THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013-2014 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface

Audience  xxi
Document Revision History  xxi
Document Conventions  xxi
Related Documentation  xxiii
Obtaining Documentation and Submitting a Service Request  xxiii

CHAPTER 1

Getting Started with Cisco ME 2600X  1

Introduction  1
Cisco IOS Software Images  1
Locating a Valid Cisco IOS Software Image  2
Manually Booting from a Cisco IOS Software Image  2
Configuring Cisco ME 2600X  3
Using Global Configuration Mode  3
Configuration Tasks  4
Configuring the Cisco ME 2600X Host Name  5
Configuring Passwords on Cisco ME 2600X  5
Setting or Changing a Static Enable Password  5
Protecting Passwords with Enable Secret  6
Setting Password for Telnet Sessions  7
Setting Password to Access the Console Terminal  8
Configuring Ethernet Access for Network Management  9
SD Flash Card Memory Tasks  10
Formatting an SD Flash Card  10
Booting from an SD Flash Card  11
Copying Files on an SD Flash Card  13
Booting from an On-Board Flash  13
Upgrading and Backing up Cisco IOS Software Images and Configuration Files  15
Selecting a Cisco IOS Image 16
Upgrading the Cisco IOS Image 16
Manually Upgrading the ROMMON 19
  Saving a Configuration File 22
  Restoring a Configuration File 22
The Software Configuration Register 23
  Description of the Software Configuration Register 23
  Boot Field Settings 24
  Configuring the Software Configuration Register 25
Troubleshooting Tips 26
  Retrieving Information from the Crashinfo File 26
Configuring Gigabit Ethernet Interfaces 28
  Configuring the Interface 28
  Enabling the Interface 30
  Setting the Speed and Duplex Mode 30
Monitoring and Maintaining Cisco ME 2600X Series 32
  Monitoring the Device Configuration 32
  Additional System Monitoring 33

CHAPTER 2 Ethernet Virtual Circuit 35
  Carrier Ethernet 35
  Prerequisites for EVC and EFP 36
  Restrictions for EVC and EFP 36
  Information About Carrier Ethernet 36
    Understanding Ethernet Virtual Circuit 37
    EVC Features 37
    EVC Types 38
    Interactions of EVC with Other Features 38
    Understanding Ethernet Flow Point 41
      Counters 42
    Understanding Bridge Domain 42
    Supported Encapsulation and Rewrite Operations 43
  How to Configure EVC 50
    Configuring an Ethernet Service Instance 50
    Configuring Layer 2 Protocol Tunneling 52
CHAPTER 3  Quality of Service  57
  Quality of Service  57
  Prerequisites for QoS  58
  Restrictions for QoS  58
  Information About QoS  58
    Advantages of QoS  60
    Cisco ME 2600X QoS  61
      Ingress QoS Functions  61
        Ingress Classification  62
        Ingress Policing  62
        Ingress Marking  63
      Egress QoS Functions  63
        Egress Classification  64
        Egress Queue Scheduling  64
        Egress LLQ  65
        Egress Bandwidth  65
        Egress Shaping  65
        Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent  65
    Hierarchical QoS  65
    EVCS QoS Support  66
    QoS Support on Port-Channel  66
    QoS Statistics  67
    Scalability  69
  How to Configure QoS  69
    Configuring QoS Features  70
    Configuring Ingress Classification  70
    Configuring Ingress Policing  73
    Attaching or Removing a Traffic Policy from the Target  78
    Configuring Ingress Marking  80
    Configuring Ingress Re-Marking  82
    Configuring Egress Classification  85
Configuring the REP Link Status Layer Ageout Timer 118
Understanding REP with EVC 119
Configuring REP over EVC 121
Configuring REP over EVC Using a Cross–Connect 121
Configuring REP over EVC Using the Bridge Domain 123
Verifying REP with EVC Configuration 125
REP with Multicast 127

CHAPTER 5
Link Aggregation Group and Link Aggregation Control Protocol 129
Understanding IEEE 802.3ad Link Bundling 129
Link Aggregation Group and Link Aggregation Control Protocol Configuration Procedures 130
Understanding LACP 130
Managing LACP 131
Configuring and Retrieving a Port Channel 131
Configuring LACP over Port Channel 133
Monitoring LACP Status 134
Understanding LACP Priority 134
Setting LACP System Priority 135
Understanding LACP 1:1 Redundancy 136
Configuring LACP 1:1 Redundancy with Fast Switchover 136
Understanding LAG 138
Managing a Channel Group 138
Configuring a Channel Group with LACP 139
Adding and Removing Interfaces from a Channel Group with LACP 140
Configuring a Channel Group with LAG 141
Adding and Removing Interfaces from a Channel Group with LAG 142
Setting a Minimum and Maximum Threshold of Active Links 144
Understanding Load Balancing 145
Configuring Manual Load Balancing with LACP 146
Configuring Manual Load Balancing with LAG 149
Show Commands 151
Interactions of LAG with Other Features 154

CHAPTER 6
MAC Learning 157
Understanding MAC Learning 157
CHAPTER 7  Multicast VLAN Registration  169
  Multicast VLAN Registration  169
  Prerequisites for MVR  170
  Restrictions for MVR  170
  Information About MVR  171
    Using MVR in a Multicast Television Application  171
  How to Configure MVR  173
    Enabling MVR in Global Configuration Mode  173
    Enabling or Disabling MVR Source and MVR Receiver on an Interface  175
    Configuring MVR Source and MVR Receiver on an Interface  175
  Verifying the MVR Configuration  177
  Configuration Examples for MVR  179
  Additional References for MVR  180

CHAPTER 8  IGMP Snooping  183
  Understanding IGMP Snooping  183
  Joining a Multicast Group  184
  Configuring IGMP Snooping  187
    Enabling or Disabling IGMP Snooping  187
  Leaving a Multicast Group  189
    Enabling or Disabling IGMP Immediate Leave  190
  IGMP Report Suppression  191
    Disabling IGMP Report Suppression  192
    Configuring a Static Multicast Port  193
    Viewing IGMP Configuration  195
CHAPTER 9  Remote Network Monitoring and Alarm Troubleshooting  205

RMON Procedures  205
Understanding RMON  205
Configuring RMON Settings  206
Displaying RMON Status  207
Alarm Troubleshooting  208

FMEA FAN Alarm  208
Clearing the FMEA FAN Alarm  208
MAC-BD-LIMT-REACHED  208
Clearing the MAC-BD-LIMT-REACHED Alarm  209
MAC-SYS-LIMT-REACHED  209
Clearing the MAC-SYS-LIMT-REACHED Alarm  209

CHAPTER 10  Authentication, Authorization, and Accounting (AAA)  211

AAA Overview  212
About AAA Security Services  212
Benefits of Using AAA  213
AAA Philosophy  213
Method Lists  213
Where to Begin  215
Overview of the AAA Configuration Process  215
Enabling AAA  215
What to Do Next  216

Configuring Authentication  217
Named Method Lists for Authentication  217
Method Lists and Server Groups  217
Method List Examples  218
AAA Authentication General Configuration Procedure  219

AAA Authentication Methods Configuration Task List  219
Configuring Login Authentication Using AAA 220
   Login Authentication Using Enable Password 222
   Login Authentication Using Line Password 222
   Login Authentication Using Local Password 222
   Login Authentication Using Group RADIUS 223
   Login Authentication Using Group TACACS+ 223
   Login Authentication Using Group Name 223
Enabling Password Protection at the Privileged Level 223
Changing the Text Displayed at the Password Prompt 225
Configuring Message Banners for AAA Authentication 226
   Configuring a Login Banner 226
   Configuring a Failed-Login Banner 227
Non-AAA Authentication Methods 228
   Configuring Line Password Protection 228
   Establishing Username Authentication 230
Authentication Examples 231
   RADIUS Authentication Examples 231
   TACACS+ Authentication Examples 232
   Login and Failed Banner Examples 233
Configuring Authorization 233
   Named Method Lists for Authorization 233
AAA Authorization Methods 234
   Method Lists and Server Groups 235
AAA Authorization Types 235
AAA Authorization Prerequisites 236
AAA Authorization Configuration Task List 236
   Configuring AAA Authorization Using Named Method Lists 236
      Authorization Types 238
      Authorization Methods 238
   Disabling Authorization for Global Configuration Commands 238
Authorization Attribute-Value Pairs 239
Authorization Configuration Examples 239
   Named Method List Configuration Example 240
   TACACS+ Authorization Example 240
   RADIUS Authorization Example 240
Configuring Accounting 241
   Named Method Lists for Accounting 241
      Method Lists and Server Groups 242
      AAA Accounting Methods 243
      EXEC Accounting 243
   AAA Session MIB 244
   AAA Accounting Prerequisites 245
   AAA Accounting Configuration Task List 246
      Configuring AAA Accounting Using Named Method Lists 246
         Accounting Type 247
         Accounting Record Types 247
         AAA Accounting Methods 247
   Accounting Attribute-Value Pairs 248
   Accounting Configuration Examples 248
      Configuring Named Method List Example 248
      AAA Session MIB Example 249
   Show Commands 249
   Additional Information 252
      Understanding Authentication 252
      Configuring Local Authentication 252
      Protecting Access to Privileged EXEC Commands 254
         Setting or Changing a Static Enable Password 254
         Protecting Passwords with Enable Password and Enabling Secret 255
         Setting or Changing a Line Password 256
   Understanding Multiple Privilege Levels 257
   Configuring Privilege Levels 257
      Setting the Privilege Level for a Command 258
      Displaying Current Privilege Levels 258
      Logging In to a Privilege Level 259
   TACACS+ Overview 259
   TACACS+ Operation 260
   TACACS+ Configuration Task List 261
   Specifying TACACS+ Authentication 261
   Specifying TACACS+ Authorization 262
   Specify TACACS+ Accounting 262
Dynamic ARP Inspection 315

Understanding DAI 315

Understanding ARP 315

Understanding ARP Spoofing Attacks 315

Understanding DAI and ARP Spoofing Attacks 316

Interface Trust States and Network Security 317

Rate Limiting of ARP Packets 318

Relative Priority of ARP ACLs and DHCP Snooping Entries 318

Logging of Dropped Packets 318

Default DAI Configuration 319
Restrictions for DAI 319
Configuring DAI 320
   Enabling DAI on Bridge Domains 320
   Configuring the DAI Interface Trust State 322
   Configuring ARP Packet Rate Limiting 323
Enabling Additional Validation 325
Configuring DAI Logging 327
   DAI Logging Overview 327
   Configuring the DAI Logging For All Packets 327
   Configuring the DAI Logging Buffer Size 328
   Configuring the DAI Logging System Messages 330
Example: DAI Configuration 331
   Configuring Switch A 331
   Configuring Switch B 335

CHAPTER 16
MAC Address Security 339
   MAC Address Security for EVC Bridge Domain 339
   Restrictions for MAC Address Security 340
   Enabling MAC Address Security for EVC Bridge Domain 340
   Disabling MAC Address Security for EVC Bridge Domain on an EFP 342
   Configuring MAC Address Whitelist on an EFP 343
   Configuring Sticky MAC Addresses on an EFP 345
   Configuring MAC Address Limiting on EFP 347
   Configuring MAC Address Limiting on a Bridge Domain 349
   Configuring Violation Response on an EFP 350
   Checking EVC State 352
   Error Recovery 352
      Manual Recovery 353
      Automatic recovery 353
   Verification 353
   Troubleshooting 356

CHAPTER 17
Layer 2 Access Control Lists on EVCs 359
   Layer 2 Access Control Lists on EVCs 359
   Finding Feature Information 359
Prerequisites for Layer 2 Access Control Lists on EVCs 360
Limitations and Restrictions for Layer 2 Access Control Lists on EVCs 360
Information About Layer 2 Access Control Lists on EVCs 360
  EVC 360
Relationship Between ACLs and Ethernet Infrastructure 361
Configuring Layer 2 Access Control Lists on EVCs 361
  Creating a Layer 2 ACL 361
  Applying a Layer 2 ACL to a Service Instance 362
  Removing a Layer 2 ACL 364
  Configuring a Layer 2 ACL with ACEs on a Service Instance 365
  Verifying the Presence of a Layer 2 ACL on a Service Instance 367
Configuration Examples for Layer 2 Access Control Lists on EVCs 368
  Example: Creating a Layer 2 ACL with ACEs 368
  Example: Applying a Layer 2 ACL to a Service Instance 368
  Example: Applying a Layer 2 ACL to Three Service Instances on the Same Interface 368
  Example: Displaying the Details of a Layer 2 ACL on a Service Instance 369
Additional References 370
  Related Documents 370
  Standards 370
  MIBs 370
  Technical Assistance 371
Feature Information for Layer 2 Access Control Lists on EVCs 371

CHAPTER 18
Layer 3 Access Control Lists on EVCs 373
Layer 3 Access Control Lists on EVCs 373
Finding Feature Information 373
Prerequisites for Layer 3 Access Control Lists on EVCs 373
Limitations and Restrictions for Layer 3 Access Control Lists on EVCs 374
Information About Layer 3 Access Control Lists on EVCs 374
Configuring Layer 3 Access Control Lists on EVCs 374
  Creating a Standard Layer 3 ACL 374
  Applying a Layer 3 ACL to a Service Instance 375
  Removing a Layer 3 ACL 377
  Creating a Layer 3 Extended ACL 378
  Applying a Layer 3 Extended ACL to a Service Instance 379
Contents

Neighbor Solicitation Messages 406
Router Advertisement Messages 407

How to Configure IPv6 408
Configuring IPv6 on an Interface 409
Configuring IPv6 on a Bridge Domain Interface 410
Configuring IPv6 Duplicate Address Detection 412
Configuring IPv6 Default and Static Routes 414
Configuring IPv6 Access Lists 415
Configuring the Neighbor Solicitation Message Interval 417
Configuring the Neighbor Reachable Time 418
Configuring the Router Advertisement Transmission Interval 419
Configuring the Router Lifetime Value 420
Configuring the IPv6 Prefix 421
Suppressing Router Advertisement Messages 422
Configuring a Static IPv6 Neighbor 423

Troubleshooting Tips 424
Configuration Examples for IPv6 425
Verifying the IPv6 Configuration 426
Additional References for IPv6 428

CHAPTER 23  SSH 431

SSH 431
Prerequisites for SSH 432
Restrictions for SSH 432
Information About SSH 432

How to Configure SSH 433
Setting Up Cisco ME 2600X to Run SSH 434
Exporting The RSA Keys to the Supervisor Using RCP 436
Importing the RSA Keys Stored on the Supervisor 437
Configuring IPv6/IPv4 Addressing and Verifying SSH 439

Troubleshooting Tips 440
Configuration Examples for SSH 441
Verifying the SSH Configuration 441
Additional References for SSH 443
CFM Messages 473
  Continuity Check Messages 473
  Loopback Messages 474
  Linktrace Messages 474
How to Configure CFM 474
  Enabling or Disabling CFM Globally 474
  Enabling or Disabling CFM on an Interface 475
  Enabling Caching of CFM Data 476
  Creating a Maintenance Domain 477
  Creating a Maintenance Association 478
  Configuring CFM Encapsulation 479
  Creating a Port MEP 480
  Creating an MEP for an EFP 481
  Defining MEPs Statically within a Maintenance Association 482
  Specifying the Number of MEPs in a Maintenance Association 483
  Creating an MIP Dynamically 485
  Configuring an MIP on a Service Instance in CFM Manually 486
  Enabling the Transmission of Continuity Check Messages 487
  Sending CFM Loopback and Linktrace Messages 489
Configuration Examples for CFM 490
Verifying the CFM Configuration 493
Additional References for CFM 499
Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecommunications technician.

• Document Revision History, page xxi
• Document Conventions, page xxi
• Related Documentation, page xxiii
• Obtaining Documentation and Submitting a Service Request, page xxiii

Document Revision History

The Document Revision History table below records technical changes to this document. The table shows the release number and document revision number for the change, the date of the change, and a brief summary of the change.

<table>
<thead>
<tr>
<th>Release No.</th>
<th>Revision</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4(3)S</td>
<td>OL-28850-04</td>
<td>July 2014</td>
<td>Added Ethernet Connectivity Fault Management (CFM) over Ethernet Virtual Connections (EVC) chapter.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>OL-28850-03</td>
<td>March 2014</td>
<td>Added Point-to-point protocol over Ethernet intermediate agent (PPPoE IA) chapter.</td>
</tr>
<tr>
<td>15.2(2)SA2</td>
<td>OL-28850-02</td>
<td>August 2013</td>
<td>Added IP Version 6 (IPv6) Support for the Management Port and Secure Shell (SSH) chapters.</td>
</tr>
<tr>
<td>15.2(2)SA</td>
<td>OL-28850-01</td>
<td>March 2013</td>
<td>First release.</td>
</tr>
</tbody>
</table>

Document Conventions

This document uses the following conventions:
<table>
<thead>
<tr>
<th><strong>Convention</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><strong>Italic</strong> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <strong>italic</strong> font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td>Bold Courier font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Reader Alert Conventions**

This document uses the following conventions for reader alerts:
Related Documentation

Use this guide in conjunction with the following referenced publications:

- Cisco ME 2600X Hardware Installation Guide
- Release Notes for Cisco ME 2600X

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
CHAPTER 1

Getting Started with Cisco ME 2600X

This chapter describes how to boot and configure Cisco ME 2600X. For information on installing your switch, see the Cisco ME 2600X Series Ethernet Access Switch Hardware Installation Guide.

- Introduction, page 1
- Cisco IOS Software Images, page 1
- Configuring Cisco ME 2600X, page 3
- Configuration Tasks, page 4
- SD Flash Card Memory Tasks, page 10
- Booting from an On-Board Flash, page 13
- Upgrading and Backing up Cisco IOS Software Images and Configuration Files, page 15
- The Software Configuration Register, page 23
- Troubleshooting Tips, page 26
- Configuring Gigabit Ethernet Interfaces, page 28
- Monitoring and Maintaining Cisco ME 2600X, page 32

Introduction

The Cisco ME 2600X is a Carrier Ethernet and FTTH based solution used as an access or an aggregation device to maximize the utility of network bandwidth. Service providers can aggregate different types of traffic (voice, video, and data) and transmit them over the core network. Cisco ME 2600X supports a wide range of FTTH and carrier ethernet features.

Cisco IOS Software Images

By default, the Cisco ME 2600X ships with a Cisco IOS software image preloaded into the SD flash card. Initially, the Cisco ME 2600X is configured to boot from this image. You can change this default setting and configure it to boot from an SD Flash card or from a TFTP server. If you specify that the device boot from
an image on a TFTP server, you must verify that you have an Ethernet connection to the URL of the TFTP server.

**Note**

When booting for the first time, you must copy the latest image from a TFTP server to an SD flash card.

Related issues are discussed in the following sections:

- Locating a Valid Cisco IOS Software Image
- Manually Booting from a Cisco IOS Software Image

### Locating a Valid Cisco IOS Software Image

If the Cisco ME 2600X does not find a valid system software image, the system enters read-only memory (ROM) monitor mode and displays the ROM monitor prompt (Rommon>). From this mode, you can use the `sddir sdflashto` command to locate a valid system image.

### Manually Booting from a Cisco IOS Software Image

If Cisco ME 2600X does not find a valid system software image, you will need to boot an image manually by using the appropriate ROM monitor mode boot command. Once you locate a software image, use one of the following forms of the boot command to boot Cisco ME 2600X:

```
rrommon 1 > set
```

PS1=rrommon ! >
PB_MODE=CPT50FTTH
IP_SUBNET_MASK=255.255.255.0
RELOAD_TYPE=1
snmpboots=1
TFTP_SERVER=202.153.144.25
DEFAULT_GATEWAY=7.6.0.1
IP_ADDRESS=7.6.11.13
BOOT=
NTPv4_Drift=0.0
CRASHINFO=ramdisk:crashinfo_19930301-000025-UTC
TFTP_FILE=/auto/tftpboot/ME2600X-universalk9-mz.152-2.SA.fc5
BSI=0
RANDOM_NUM=975074187
RELOAD_REASON=12ab34Reload Command
?=80

```
rrommon 2 > nboot
```

Using SGMII Path

link status is up!!!speed = 100, duplex = 1

Receiving /auto/tftpboot/ME2600X-universalk9-mz.152-2.SA.fc5 from 202.153.144.25
Configuring Cisco ME 2600X

You can perform a basic configuration of Cisco ME 2600X in the global configuration mode, through the Cisco IOS command line user interface (CLI).

In this method, enter configuration commands on a line-by-line basis at the console, without being prompted by a configuration script. For more information, see Using Global Configuration Mode.

Ensure you know the following before starting the configuration procedure:

- Interfaces on the device
- Protocols used on the device
- Network addressing scheme for the device
- Password scheme for your environment

Note

Before configuring Cisco ME 2600X for the first time, a mini USB should be connected to the console port. For more information on device installation, see the hardware installation guide.

You can also use the management interface to configure Cisco ME 2600X using Telnet. When using the management interface, the maximum supported interface loopback is 963120.

Using Global Configuration Mode

If you prefer not to use the interactive script of the setup facility, you can manually configure Cisco ME 2600X in the global configuration mode. The global configuration mode enables you to enter configuration commands line by line from the console terminal.

Before configuring the Cisco ME 2600X in global configuration mode, you need to be familiar with the Cisco IOS software command line interface. See the “Using the Command Line Interface” chapter in the Configuration Fundamentals Configuration Guide. It discusses the different command modes, context-sensitive help, and editing features.

To configure Cisco ME 2600X, complete the following steps:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `copy running-config startup-config` or `write memory`
### 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>Enters privileged EXEC mode on the device. Depending on the system and the software version, you may be prompted for a password. The prompt changes to Switch# in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode, from which you can enter most of the configuration commands needed to change the system configuration. The prompt changes to Switch(config)# in global configuration mode. When you are finished entering configuration commands, press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Enters interface configuration mode for the specified interface. In interface configuration mode, you can enter commands to change the interface configuration. The prompt changes to Switch(config-if)# in interface configuration mode. When you are finished entering configuration commands, press Ctrl-Z to exit the configuration mode and return to privileged EXEC mode. Use the exit command to return to global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface type slot/port</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> copy running-config startup-config or write memory</td>
<td>Saves the running configuration changes to NVRAM. If you do not save the running configuration to NVRAM, your configuration settings will be lost the next time you reload the device.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>or Switch# write memory</td>
<td></td>
</tr>
</tbody>
</table>

In global configuration mode, you will enter all the necessary commands to configure your device. The remainder of this document describes typical configuration tasks that you may need to perform. To display a list of the configuration commands available to you, enter a question mark (?) at the prompt or press the designated help key on the terminal keyboard while in configuration mode. For more information concerning Cisco IOS configuration commands, see the Cisco IOS Configuration Fundamentals Command Reference located at:


### Configuration Tasks

This section details initializing configuration tasks that should be performed on your device. Each task can be performed using either the setup command facility or the global configuration mode.
• Configuring the Cisco ME 2600X Host Name
• Configuring Passwords on Cisco ME 2600X
• Configuring Ethernet Access for Network Management

Configuring the Cisco ME 2600X Host Name

The default host name for Cisco ME 2600X is “ftth”. You can change the host name by using the `hostname name` command.

The name you assign to Cisco ME 2600X must follow the rules for ARPANET host names. It must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The name must consist of 63 or fewer characters. For more information, see Requests For Comments (RFC) 1035, Domain Names—Implementation and Specifications.

Configuring Passwords on Cisco ME 2600X

The commands available at the user EXEC level are a subset of those available at the privileged EXEC level. Many privileged EXEC commands are used to set system parameters, so you should password-protect these commands to prevent their unauthorized use. Following is a subset of the password protection commands, which are accessed via global configuration mode.

Make a note of all passwords you set and store that information in a secure location for future reference.

For more detailed information on how to establish password protection or configure privilege levels, see the Security Configuration Guide, located at:


Setting or Changing a Static Enable Password

To set or change a static enable password, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `enable password password`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Configuring Passwords on Cisco ME 2600X

#### Step 2
Enter global configuration mode.

**Command or Action:**

```
configure terminal
```

**Example:**

```
Switch# configure terminal
```

#### Step 3
Establish a new password or changes an existing password for the privileged command level.

**Command or Action:**

```
able password password
```

**Example:**

```
Switch(config)# enable password 1234abcd
```

#### Step 4
Return to privileged EXEC mode.

**Command or Action:**

```
end
```

**Example:**

```
Switch(config)# end
```

### Protecting Passwords with Enable Secret

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, use the `enable secret` command. This command allows you to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level you specify. The `enable secret` command offers better security than the `enable password` command because the `enable secret` password is stored using a nonreversible cryptographic function.

For maximum security, the enable secret and the enable passwords should be different. If you use the same password, the system accepts it but issues a warning indicating that you should enter a different password.

An enable secret password can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an enable password password can contain any number of uppercase and lowercase alphanumeric characters. You cannot use a number as the first character. Spaces, however, are valid password characters. For example, two words is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

To set or change a secret password, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `enable secret password`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Setting Password for Telnet Sessions

To configure authentication for accessing a device through incoming Telnet sessions, complete the following steps:

**SUMMARY STEPS**

1. **enable**  
2. **configure terminal**  
3. **line [vty] line-number [ending-line-number]**  
4. **login**  
5. **password password**  
6. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
**enable**  
Example:  
Switch> enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2**  
**configure terminal**  
Example:  
Switch# configure terminal | Enters global configuration mode. |
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>line [vty] line-number [ending-line-number]</code></td>
<td>Enters line configuration mode for the lines to which you want to apply the authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# line vty 0 4</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>login</code></td>
<td>Enables password checking at login.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-line)# login</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>password password</code></td>
<td>Assigns a password to a terminal or other device on a line.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-line)# password 1234abcd</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-line)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

---

### Setting Password to Access the Console Terminal

To configure authentication for accessing the console terminal, complete the following steps:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `line [console] line-number`
4. `login`
5. `password password`
6. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring Ethernet Access for Network Management

You can configure Ethernet connectivity to your FTTH for network management purposes. The RJ-45 and MII receptacles on the faceplate of the GRP and the RJ-45 receptacles on the faceplate of the PRP are IEEE 802.3u-compliant interfaces.

To configure Ethernet connectivity, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `ip address ip-address mask`
5. `end`

**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.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>interface type slot/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config)# interface GigabitEthernet 1/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>ip address ip-address mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# ip address 10.10.1.1 255.255.0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
</tbody>
</table>

### Purpose

- **Step 2**: Enters configuration mode.
- **Step 3**: Enters interface configuration mode on the Ethernet interface.
- **Step 4**: Specifies the IP address and subnet mask for the interface.
- **Step 5**: Returns to privileged EXEC mode.

### SD Flash Card Memory Tasks

The two Gigabyte SD Flash that shipped with Cisco ME 2600X contains the default Cisco IOS software image you need to boot Cisco ME 2600X. When using an SD Flash card, the Cisco IOS command to identify and access the SD Flash card is `sdflash:`.

The following sections describe common software tasks that involve an SD Flash card:

- Formatting an SD Flash card
- Booting from an SD Flash card
- Copying Files on an SD Flash card

### Formatting an SD Flash Card

To format a new SD flash card, complete the following:

**Before You Begin**

Before you use a new SD flash card, you must format it.

Caution: Formatting erases all information on an SD flash card. To prevent the loss of important data that might be stored on an SD flash card, proceed carefully. If you want to save the data contained on an SD flash card, copy the data to a server before you format the card.
SUMMARY STEPS

1. enable
2. format sdflash:
3. y

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>format sdflash:</td>
<td>Formats a new SD flash card.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# format sdflash:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>y</td>
<td>Confirms the card format.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>All sectors will be erased, proceed? [confirm]</td>
<td>y</td>
</tr>
</tbody>
</table>

The new SD flash card is now formatted and ready to use.


Booting from an SD Flash Card

To enable booting from a Cisco IOS software image file located on an SD flash card, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. boot system flash sdflash: *filename*
4. config-register 01
5. Ctrl-z
6. copy running-config startup-config or write memory
7. reload
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies that at startup, the device loads the software image named <code>filename</code>, located on the linear Flash memory card.</td>
</tr>
<tr>
<td><code>boot system flash sdflash: filename</code></td>
<td>A current image in the system will boot up.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>boot system flash sdflash: me2600X-universalk9-mz</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Disables the Break function and enables the boot system flash command.</td>
</tr>
<tr>
<td><code>config-register 01</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>config-register 01</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><code>Ctrl-z</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>Ctrl-z</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Saves the software configuration register settings to NVRAM.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code> or <code>write memory</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>copy running-config startup-config</code> or Switch# <code>write memory</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Reboots Cisco ME 2600X and uses the specified image on the SD flash card to boot the system.</td>
</tr>
<tr>
<td><code>reload</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>reload</code></td>
</tr>
</tbody>
</table>

### Note
By default, Cisco ME 2600X boots from a software image file on an SD flash card.
Copying Files on an SD Flash Card

You can copy and move files to and from an SD flash card as you would to any file system. To manipulate files on an SD flash card, use any of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dir sdflash:</code></td>
<td>Changes the present working directory you are accessing to the PCMCIA linear Flash memory card. Use disk1: to access a Flash disk of the RP.</td>
</tr>
<tr>
<td><code>delete flash1: filename</code></td>
<td>Deletes the file <code>filename</code> from a linear Flash memory card or Files that are deleted are removed from the directory list, but are not erased permanently. You can use the <code>undelete</code> command to recover deleted files.</td>
</tr>
<tr>
<td><code>delete sdflash: filename</code></td>
<td></td>
</tr>
</tbody>
</table>

Booting from an On-Board Flash

To enable booting from a Cisco IOS software image file located on an on-board flash on the Cisco ME 2600X, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `dir ramdisk`
3. `configure terminal`
4. `interface type slot/port`
5. `ip address`
6. `ip default-gateway ip-address`
7. `ip route`
8. `copy tftp: ramdisk:`
9. `test flash burn kernel ramdisk:`
10. `reload`
11. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><em>Example:</em></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dir ramdisk</td>
<td>Displays the directory content of kernel.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# dir ramdisk:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode, from which you can enter most of the configuration commands needed to change the system configuration. The prompt changes to Switch(config)# in global configuration mode. When you are finished entering configuration commands, press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface type slot/port</td>
<td>Enters interface configuration mode on the Ethernet interface.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface GigabitEthernet 1/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address and subnet mask for the interface.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip address 10.10.1.1 255.255.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip default-gateway ip-address</td>
<td>Specifies the default gateway.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip default-gateway 10.10.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip route</td>
<td>Specifies the IP route.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip route 0.0.0.0 0.0.0.0 g1/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>copy tftp: ramdisk:</td>
<td>Copies files from the TFTP server to ramdisk.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>When copying files to ramdisk, the destination filename must be 45021___KNL, otherwise the upgrade fails.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# copy tftp: ramdisk:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>test flash burn kernel ramdisk:</td>
<td>Upgrades to the new kernel version.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# test flash burn kernel ramdisk:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reload</td>
<td>Loads the new kernel version.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# reload</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 11</th>
<th>end</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config-if)# end
```

**Purpose:** Returns to privileged EXEC mode.

---

### Examples

**Switch#** `dir ramdisk:`

```
Directory of ramdisk:/

1 -rw- 131072 <no date> ngxp_rml.bin
2 -rw- 1097868 <no date> 45021____.KNL
```

**Switch#** `copy tftp: ramdisk:`

```
Address or name of remote host []? 10.1.1.1
Source filename []? me2600x-universalk9-mz.152-2.SA2-13Nov2013
Destination filename [me2600x-universalk9-mz.152-2.SA2-13Nov2013]? 45021____.KNL

Erase ramdisk: before copying? [confirm]y
Erasing the ramdisk filesystem will remove all files! Continue? [confirm]y
Erasing device... ...erased
Erase of ramdisk: complete

Loading me2600x-universalk9-mz.152-2.SA2-13Nov2013 from 10.1.1.1 (via GigabitEthernet1/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 23210060 bytes]
Verifying checksum... OK (0x6B47)
23210060 bytes copied in 75.157 secs (308821 bytes/sec)
```

**Switch#** `test flash burn kernel ramdisk:`

```
Reading ramdisk:45021____.KNL into 2367DC34. Please wait ...
23210060 bytes of image read from ramdisk:45021____.KNL
Writing 23210124 bytes of ramdisk:45021____.KNL image from 2367DBF4 writing to flash. Please wait. Flash write successful ...
```

---

### Upgrading and Backing up Cisco IOS Software Images and Configuration Files

The following sections describe common software tasks to upgrade and back up files on your device.
Selecting a Cisco IOS Image

When you select the Cisco IOS image for upgrade, consider the following:

- Memory requirement—The device should have sufficient SD flash card memory to store the Cisco IOS. The device should also have sufficient memory (DRAM) to run the Cisco IOS. If the device does not have sufficient memory (DRAM), the device will have boot problems when it boots through the new Cisco IOS.

- Software feature support—You must ensure that the new Cisco IOS supports the features used with the old Cisco IOS.

Upgrading the Cisco IOS Image

**Note**
Startup configuration is automatically restored when upgrading from:

- `me2600x-universalk9-mz.152-2.SA2` to future releases other than `me2600x-universalk9-mz.154-2.S`

**Caution**
Startup configuration is lost when upgrading from:

- `me2600x-universalk9-mz.152-2.SA2` to `me2600x-universalk9-mz.154-2.S`
- `me2600x-universalk9-mz.154-2.S` to `me2600x-universalk9-mz.154-3.S`

To retain the existing configuration, you must backup the existing configuration before upgrading and then restore it after the upgrade.

To upgrade the Cisco IOS image, complete the following steps:

1. Download the Cisco IOS software image to the TFTP server.
   Download the Cisco IOS software image onto your workstation or PC from the Download Software Area (registered customers only).

2. Identify the file system to copy the image.
   The file system type ‘sdflash’ is used to store the Cisco IOS image. The `show file system` command lists the file systems available on the device. The file system should have sufficient space to store the Cisco IOS image. You can use the `show file system` or the `dir file_system` command in order to find the free space.

   ```
   Switch# show file systems
   ```

<table>
<thead>
<tr>
<th>File Systems:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size (b)</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>62914556</td>
</tr>
<tr>
<td>20514816</td>
</tr>
</tbody>
</table>
3 Prepare for the upgrade.

Ensure the following before you upgrade the Cisco IOS:

- Store both the old Cisco IOS and the new Cisco IOS, if the device has sufficient memory. You can boot the device in the ROMMON mode and boot the old Cisco IOS, in case of boot failure with new Cisco IOS. This method saves time if you want to roll back the Cisco IOS.

- Backup the configuration from the device because some of the Cisco IOS releases add default configurations. This newly added configuration may conflict with your current configuration. Compare the configuration of the device after the Cisco IOS update with the configuration backed up before the update. If there are differences in the configuration, you must ensure they do not affect your requirements.

4 Verify that the TFTP server has IP connectivity to the device.

The TFTP server must have a network connection to the device and must be able to ping the IP address of the device targeted for a TFTP software upgrade. In order to achieve this connection, the device interface and the TFTP server must have an IP address in the same range or a default gateway configured. Check the IP address of the TFTP server in order to verify this configuration.

5 Copy the IOS Image from the TFTP server to the SD Flash card.

Before you copy the image, ensure that you have started the TFTP server software on your PC, and that you have the file name mentioned in the TFTP server root directory. Cisco recommends that you keep a backup of the device and access server configuration before you upgrade. The upgrade does not affect the configuration, which is stored in nonvolatile RAM [NVRAM]. However, this situation might happen if the right steps are not followed properly.

Switch# copy tftp: sdflash:

Address or name of remote host []? 10.105.33.135
Source filename []? ME2600X-universalk9-mz
Destination filename [ME2600X-universalk9-mz]
Accessing tftp://10.105.33.135/ME2600X-universalk9-mz...
Erase flash: before copying? [confirm]n
Loading ME2600X-universalk9-mz from 10.105.33.135 (via FastEthernet 1/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 30551884 bytes]
Verifying checksum.. OK (0xC7E6)
30551884 bytes copied in 199.636 secs (153038 bytes/sec)
Switch#
6 Verify the Cisco IOS image in the file system.

Switch# dir sdflash:

Directory of sdflash:/
1 -rw- 30551884 <no date> ME2600X-universalk9-mz
100401148 bytes total (69849200 bytes free)
Switch#

7 Verify the Configuration Register.

Use the show version command to check the config-register value. The value is displayed in the last line of the show version output. It should be set to 01.

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# config-register 01
Switch(config)# ^Z

8 Verify the Boot Variable

The device tries to boot with the first file in the SD Flash card. If the first file is not the Cisco IOS Software image, you need to configure a boot system statement in order to boot the specified image. If there is only one file in the SD Flash card and it is the Cisco IOS Software image, this step is not necessary.

Switch# show run | inc boot

boot-start-marker
boot system flash ME2600X-universalk9-mz
boot system flash sdflash:
boot system flash bootflash:
boot-end-marker
Switch#

Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no boot system
Switch(config)# boot system sdflash:ME2600X-universalk9-mz
Switch(config)# boot system sdflash:
Switch(config)# boot system bootflash:
Switch(config)# end
Switch# show run | inc boot

boot-start-marker
boot system sdflash ME2600X-universalk9-mz
boot system flash sdflash:
boot system flash bootflash:
boot-end-marker
Switch#

9 Save the configuration and reload the device.

Switch# write memory
Switch# reload

Proceed with reload? [confirm]

10 Verify the Cisco IOS upgrade.
After the reload is complete, the device should run the desired Cisco IOS Software image. Use the `show version` command in order to verify the Cisco IOS software.

Switch# show version

Cisco IOS Software, ME2600X Software (ME-UNIVERSALK9-M), Version 15.2(2)SA, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 06-Feb-13 15:15 by prod.rel_team

ROM: System Bootstrap, Version 125.7(20130201:080907) [lipxu-ROMMON_125_7_101], DEVELOPMENT SOFTWARE

Node1 uptime is 1 hour, 56 minutes
System returned to ROM by reload
System image file is "tftp://127.0.0.25//auto/tftpboot/lalishar/me2600x-universalk9-mz.152-2.SA.fc5"
Last reload type: Normal Reload
Last reload reason: Reload Command

cisco ME2600X FTTH (P2020) processor (revision A) with 2088944K bytes of memory.
Processor board ID MMMWWYYSSSS, with hardware revision
  FPGA REV = Zola 0x1.E
  CPLD REV = 0x01

Last reset from Software (Warm boot).

7K bytes of non-volatile configuration memory.
8192K bytes of processor board Hidden Config flash (Read/Write)
61440K bytes of processor board RAM Disk (Read/Write)

Configuration register is 0x1

**Manually Upgrading the ROMMON**

To manually upgrade the Cisco ME 2600X ROMMON, complete the following steps:
SUMMARY STEPS

1. enable
2. dir ramdisk
3. configure terminal
4. interface type slot/port
5. ip address
6. ip default-gateway ip-address
7. ip route
8. copy tftp: ramdisk:
9. test flash burn rommon ramdisk:
10. reload
11. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable           | Enables privileged EXEC mode.  
|      | Example: Switch> enable | • Enter your password if prompted. |
| 2    | dir ramdisk      | Displays the directory content of ROMMON. |
|      | Example: Switch# dir ramdisk: |
| 3    | configure terminal | Enters global configuration mode, from which you can enter most of the configuration commands needed to change the system configuration. The prompt changes to Switch(config)# in global configuration mode. When you are finished entering configuration commands, press Ctrl-Z to exit global configuration mode. |
|      | Example: Switch# configure terminal |
| 4    | interface type slot/port | Enters interface configuration mode on the Ethernet interface. |
|      | Example: Switch(config)# interface GigabitEthernet 1/1 |
| 5    | ip address       | Specifies the IP address and subnet mask for the interface. |
|      | Example: Switch(config-if)# ip address 10.10.1.1 255.255.0.0 |
| 6    | ip default-gateway ip-address | Specifies the default gateway. |
|      | Example: Switch(config-if)# ip default-gw 10.10.2 |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>ip route</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# ip route 0.0.0.0 0.0.0.0 g1/1</td>
</tr>
<tr>
<td></td>
<td>Specifies the IP route.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy tftp: ramdisk:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# copy tftp: ramdisk:</td>
</tr>
<tr>
<td></td>
<td>Copies files from the TFTP server to ROMMON.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>test flash burn rommon ramdisk:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# test flash burn rommon ramdisk:</td>
</tr>
<tr>
<td></td>
<td>Upgrades to the new ROMMON version.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>reload</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# reload</td>
</tr>
<tr>
<td></td>
<td>Loads the new ROMMON version.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Examples

Switch# dir ramdisk:

```
Directory of ramdisk:/
  1 -rw- 131072 <no date> ngxp_rml.bin
  2 -rw- 1097868 <no date> 4500_____BCO
```

Switch# copy tftp: ramdisk:

```
Address or name of remote host [202.153.144.25]?
Source filename [/tftpboot/ngxp_rml.bin]? /tftpboot/4500_____BCO
Destination filename [4500_____BCO]?
Accessing tftp://202.153.144.25//tftpboot/4500_____BCO...
Erase ramdisk: before copying? [confirm]n
Loading /tftpboot/4500_____BCO from 202.153.144.25 (via GigabitEthernet1/1): !!!!!
[OK - 1097868 bytes]
```
Saving a Configuration File

It is a good practice to save your configuration file, in case you need to restore it for any reason. You should save your configuration file before you make major changes to the configuration. You have two configuration files: the startup configuration file located in NVRAM and the running configuration file located in DRAM. These will generally be the same, unless you are in the process of changing the configuration.

Use the following commands to save your startup configuration file, depending on where you want to save the file:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy startup-config sdflash: filename</code></td>
<td>Copies the configuration file located in NVRAM (the system default) to the SD flash card.</td>
</tr>
<tr>
<td><code>copy startup-config tftp:</code></td>
<td>Copies the configuration file located in NVRAM (the system default) to a TFTP server on the network. You will be prompted to provide the address of the TFTP server and the file name.</td>
</tr>
</tbody>
</table>

Use the following commands to save your running configuration file, depending on where you want to save the file:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config sdflash: filename</code></td>
<td>Copies the configuration file located in DRAM (the system default) to the SD flash card.</td>
</tr>
<tr>
<td><code>copy running-config tftp:</code></td>
<td>Copies the configuration file located in DRAM (the system default) to a TFTP server on the network. You will be prompted to provide the address of the TFTP server and the file name.</td>
</tr>
</tbody>
</table>

Use the `dir` command to verify that the configuration file was copied correctly to the SD Flash card, as shown in the following example:

```
Switch# dir sdflash:
-#- -length- -----date/time------ name
1 5200084 May 10 1997 19:24:12 gsr-p-mz.112-8
3 1215 May 10 1997 20:30:52 myfile1
4 6176844 May 10 1997 23:04:10 gsr-p-mz.112-8.1
5 1186 May 10 1997 16:56:50 myfile2
9197156 bytes available (11381148 bytes used)
```

Restoring a Configuration File

To restore a configuration file from a SD flash card to NVRAM, complete the following steps:
SUMMARY STEPS

1. enable
2. copy sdflash: filename startup-config
3. copy startup-config running-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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>SWITCH&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> copy sdflash: filename startup-config</td>
<td>Copies the configuration file located in the SD Flash card to NVRAM (the system default).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>SWITCH&gt; copy sdflash: filename startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> copy startup-config running-config</td>
<td>Designates the startup configuration file stored in NVRAM to be the default running configuration file for the system.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>SWITCH&gt; copy startup-config running-config</td>
<td></td>
</tr>
</tbody>
</table>

The Software Configuration Register

Configuring the software configuration register is described in the following sections:

- Description of the Software Configuration Register
- Boot Field Settings
- Configuring the Software Configuration Register

Description of the Software Configuration Register

The software configuration register is a 16-bit register in NVRAM that you use to define specific system parameters. You can set or change the contents of this register to accomplish the following tasks:

- Define the source for the default Cisco IOS software. You can specify any of the following:
  - SD Flash card
  - TFTP server on the network
  - Boot image stored within the operating environment, which you access by using an appropriate form of the boot command entered at the ROM monitor prompt (rommon->)
• Define a default boot filename.
• Enable or disable the Break function.
• Control broadcast addresses.
• Set the console terminal baud rate.
• Recover a lost password.
• Force an automatic boot using a boot image.

When you first power on the device, a boot image called the RP ROM monitor is executed, resulting in the display of the ROM monitor prompt (Rommon>). At this prompt, you have access to a limited set of commands that enable you to set values in the software configuration register and to perform a number of other tasks.

The RP ROM monitor is loaded into the RP Flash ROM when the RP is manufactured. You can use it to boot the system from local Flash memory devices. The RP ROM monitor software can be upgraded in the field, if necessary.

• Read boot system commands from the configuration file stored in NVRAM.

The table below defines the bits in the software configuration register.

**Table 1: Software Configuration Register Bit Meanings**

<table>
<thead>
<tr>
<th>Hexadecimal Value</th>
<th>Meaning/Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Goes to ROMMON prompt</td>
</tr>
<tr>
<td>0x01</td>
<td>Boots up automatically using sdflash image</td>
</tr>
</tbody>
</table>

The factory default value for the software configuration register is 0x0102. This value is a combination of binary bit 8 = 0x0100 and binary bits 00 through 03 = 0x0002.

**Note**

Valid software configuration register values may be combinations of settings, rather than the individual settings listed in the table above. For example, the factory default value 0x0102 for the software configuration register is actually a composite of several settings.

**Boot Field Settings**

Bits 00 to 03 of the software configuration register are referred to as the boot field, which defines a source for booting the default Cisco IOS software image required to run the device. The value of the boot field is specified as a binary number, as described in the table below:
Table 2: Definition of Bits in Boot Field of Software Configuration Register

<table>
<thead>
<tr>
<th>Boot Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>On power up, the system remains at the ROM monitor prompt (rommon&gt;), awaiting a user command to boot the system manually. See Manually Booting from a Cisco IOS Software Image, on page 2.</td>
</tr>
<tr>
<td>01</td>
<td>On power up, the system automatically boots the first system image found in the onboard Flash memory SIMM on the RP.</td>
</tr>
</tbody>
</table>

Note
Cisco ME 2600X is typically delivered from the factory with an SD flash card containing a suitable working Cisco IOS image. If you discover that you need a Cisco IOS upgrade, you should download the appropriate Cisco IOS image from Cisco.com. See Upgrading and Backing up Cisco IOS Software Images and Configuration Files, on page 15.

Configuring the Software Configuration Register

To configure the software configuration register, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. config-register 0xvalue
4. ctrl-Z
5. show version
6. copy running-config startup-config or write memory
7. reload

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Password: &lt;password&gt;</td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the contents of the software configuration register, where value is a 4-bit hexadecimal number as described in Table 1-8.</td>
</tr>
<tr>
<td>config-register 0x value</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# config-register 0x value</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>ctrl-Z</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ctrl-Z</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the software configuration register value currently in effect. This is the value that would be used the next time the device reloads. The value is displayed on the last line of the display, as in the following example: Configuration register is 0x141 (will be 0x102 at next reload)</td>
</tr>
<tr>
<td>show version</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show version</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Saves the software configuration register settings to NVRAM.</td>
</tr>
<tr>
<td>copy running-config startup-config or write memory</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config or Switch# write memory</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Reboots the device. Configuration register changes take effect only after the system reloads.</td>
</tr>
<tr>
<td>reload</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# reload</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

**Retrieving Information from the Crashinfo File**

The crashinfo file is a collection of useful information related to the most recent device crash. When a device crashes as a result of data or stack corruption, additional reload information required to debug this type of crash can be found in the crashinfo file. By default, the crashinfo file is stored in the onboard Flash memory SIMM or bootflash under the name “crashinfo”.

Use any of the following commands to obtain information about or display the contents of the crashinfo file:
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir flash1</td>
<td>Displays information about the crashinfo file located in the bootflash. If a crashinfo file exists, at the end of the dir flash 1 output is a section called Information of Last System Crash that contains the name of the crashinfo file.</td>
</tr>
<tr>
<td>delete flash1:crashinfo</td>
<td>Marks the most recent crashinfo file as being deleted.</td>
</tr>
</tbody>
</table>

The following example illustrates how to view the contents of the bootflash, how to view the contents of the crashinfo file, and how to restore a previous crashinfo file and view its contents:

```
Switch# show stack

Minimum process stacks:
Free/Size Name
5056/6000 CDP BLOB
10948/12000 bcmCNTR.0
8316/12000 tBcmInit
2612/6000 hal_evc init
5004/6000 hal_fp_util init
3420/6000 NGXP L2PT INIT
4980/6000 NGXP IPSG Process
5052/6000 NGXP Bdi Init
4992/6000 NGXP_Init_P2MP_SPLIT_HORIZON_FP_APP Process
3376/6000 NGXP_EFP_FP_INIT Process
5052/6000 ngxp_p2p_rp init
5036/6000 ngxp_led_task
4996/6000 ngxp_storm_control_init
3500/6000 ngxp_copp_init
3228/6000 Dhcp Snooping Process
5056/6000 ngxp_acl_init process
5052/6000 ngxp_dai_init process
5016/6000 Autoinstall
23020/24000 Setup
20712/24000 Init
5056/6000 SASL MAIN
2048/3000 LIM WAVL
10944/12000 BootP Resolver
4628/9000 Card Agent
11036/12000 cdp init process
4848/6000 RADIUS INITCONFIG
10708/12000 DHCP Autoinstall
2052/3000 Rom Random Update Process
21188/24000 Exec

Interrupt level stacks:
Level Called Unused/Size Name
2 7562 8292/9000 ethernet channel 1 TX interrupt
5 2119438 8712/9000 Timer2 HWPoller Interrupt
6 44462 8684/9000 LBC Err Intr
7 2655317 8704/9000 M8500_TIMER_INTERRUPT
```

```
Switch# dir all-filesystems
```

```
Configuring Gigabit Ethernet Interfaces

This section explains how to configure the Gigabit Ethernet (GE) interface on Cisco ME 2600X switch.

- Configuring the Interface
- Setting the Speed and Duplex Mode
- Enabling the Interface

Configuring the Interface

To configure the GE interface, complete the following steps:
In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the Switch# prompt.

---

## Before You Begin
Cisco ME 2600X supports only the following interfaces:

- GigabitEthernet – ports 1 to 44
- TenGigabitEthernet – ports 45 to 48

---

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `cdp enable`
5. `end`

### 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>enable</strong></td>
</tr>
</tbody>
</table>
| Example: | `Switch> enable`
| Enables privileged EXEC mode. | | • Enter your password if prompted. |
| **Step 2** | **configure terminal** |
| Example: | `Switch(config)# configure terminal`
| Enters global configuration mode. |
| **Step 3** | **interface type slot/port** |
| Example: | `Switch(config)# interface gigabitethernet 0/1`
| Specifies the port adapter type and the location of the interface to be configured. The **slot** is always 0 and the **port** is the number of the port. |
| **Step 4** | **cdp enable** |
| Example: | `Switch(config-if)# cdp enable`
| Enables Cisco Discovery Protocol on the device, use the **cdp enable** command. |
| **Step 5** | **end** |
| Example: | `Switch(config-if)# end`
| Returns to privileged EXEC mode. |
Enabling the Interface

To enable the interface, complete the following steps:

In the following procedure, press the `enter` key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by using the `disable` command.

**SUMMARY STEPS**

1. `enable`
2. `interface type slot/port`
3. `no shutdown`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**       | `enable` Enables privileged EXEC mode.  
| Example:          | Switch> `enable`  
|                   | • Enter your password if prompted. |
| **Step 2**       | `interface type slot/port` Specify the port adapter type and the location of the interface to be configured. The `slot` is always 0 and the `port` is the number of the port.  
| Example:          | Switch(config)# `interface gigabitethernet 0/1` |
| **Step 3**       | `no shutdown` Enable the gigabit Ethernet interface using the `no shutdown` command.  
| Example:          | Switch(config)# `no shutdown` |
| **Step 4**       | `end` Returns to privileged EXEC mode.  
| Example:          | Switch(config)# `end` |

Setting the Speed and Duplex Mode

The Gigabit Ethernet ports of the Cisco ME 2600X switch can run in full or half-duplex mode—10 Mbps, 100 Mbps, 1000 Mbps (1 Gbps) or 10000 Mbps (10 Gbps). The Cisco ME 2600X switch has an autonegotiation feature that allows the device to negotiate the speed and duplex mode with the corresponding interface at the other end of the connection.
Autonegotiation is the default setting for the speed and transmission mode.

When you configure an interface speed and duplex mode, follow these guidelines:

• If both ends of the line support autonegotiation, use the default autonegotiation settings.
• When autonegotiation is turned on for either speed or duplex mode, it autonegotiates both speed and the duplex mode.
• If one interface supports autonegotiation, and the interface at the other end does not, configure the duplex mode and speed on both interfaces. If you use the autonegotiation setting on the supported side, the duplex mode setting is set at half-duplex.

**Note**

Speed and duplex can be configured only on the Copper gigabitethernet interfaces (0/1-44)

**Note**

In the following procedure, press the enter key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by using the disable command.

To configure speed and duplex operation, complete these steps in the interface configuration mode:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. duplex [auto | half | full]
5. speed [auto | 1000 | 100 | 10]
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`duplex [auto</td>
<td>half</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# duplex auto</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`speed [auto</td>
<td>1000</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>When the speed is configured as 10 or 100, duplex should be changed to full.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# speed auto</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring and Maintaining Cisco ME 2600X

There are a number of `show` commands that can be used to monitor Cisco ME 2600X as it runs. A subset of the most useful of these commands is described here. For a complete discussion of all available `show` commands, see the *Cisco IOS Command Reference*.

- Monitoring the Device Configuration
- Additional System Monitoring

### Monitoring the Device Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show version</code></td>
<td>Displays the Cisco IOS software version number, hardware installed in the device, the names and sources of the device image files, and the contents of the software configuration register.</td>
</tr>
<tr>
<td><code>show interfaces</code></td>
<td>Displays information about the system interfaces.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays the currently running configuration in RAM.</td>
</tr>
<tr>
<td><code>show ip interface [brief]</code></td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
</tbody>
</table>
Examples

The following sample display shows typical results from the `show version` command. Depending on the image version of the Cisco IOS software running on your device and the way the device is equipped, the command output may vary.

```shell
Switch# show version

*May 29 15:04:37.970: %SYS-5-CONFIG_I: Configured from console by console
Cisco IOS Software, ME2600X Software (ME-UNIVERSALK9-M), Version 15.2(2)SA,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 06-Feb-13 15:15 by prod_rel_team

ROM: System Bootstrap, Version 125.7(20130201:080907) [lipxu-ROMMON_125_7_101], DEVELOPMENT SOFTWARE

Node1 uptime is 1 hour, 56 minutes
System returned to ROM by reload
System image file is
"tftp://127.0.0.25//auto/tftpboot/lalishar/me2600x-universalk9-mz.152-2.SA.fc5"
Last reload type: Normal Reload
Last reload reason: Reload Command

cisco ME2600X FTTH (P2020) processor (revision A) with 2088944K bytes of memory.
Processor board ID MMMWWYYSSSS, with hardware revision
  FPGA REV  = Zola 0x1.E
  CPLD REV  = 0x01

Last reset from Software (Warm boot).
7K bytes of non-volatile configuration memory.
8192K bytes of processor board Hidden Config flash (Read/Write)
61440K bytes of processor board RAM Disk (Read/Write)

Configuration register is 0x1
```

**Additional System Monitoring**

The following additional commands can be used to monitor various system indicators:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show controllers</code></td>
<td>Displays information about the hardware.</td>
</tr>
<tr>
<td><code>show logging</code></td>
<td>Displays the state of the syslog error and event logging. Before using this command, you should configure the system to timestamp logging messages with the service <code>timestamps</code> command. To clear messages from the logging buffer, use the <code>clear logging</code> command.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show memory</td>
<td>Displays memory pool statistics, including summary information about the activities of the system memory allocator and a block-by-block listing of memory use.</td>
</tr>
<tr>
<td>show processes</td>
<td>Displays information about all active processes.</td>
</tr>
<tr>
<td>show protocols</td>
<td>Displays the configured protocols.</td>
</tr>
<tr>
<td>show stacks</td>
<td>Displays stack usage of processes and interrupt routines, including the reason for the last system reboot. This command is only useful to your technical support representative.</td>
</tr>
<tr>
<td>show tcp</td>
<td>Displays the status of TCP connections.</td>
</tr>
<tr>
<td>show tcp brief [all]</td>
<td>Displays a concise description of TCP connection endpoints.</td>
</tr>
<tr>
<td>show tech-support [page] [password]</td>
<td>Displays general information about the device when reporting a problem.</td>
</tr>
</tbody>
</table>
CHAPTER 2

Ethernet Virtual Circuit

This chapter describes Ethernet Virtual Circuit (EVC), EVC types, Ethernet Flow Point (EFP), and bridge domain. This chapter also describes procedures to configure EVC.

This chapter comprise the following topics:

- Carrier Ethernet, page 35
- Prerequisites for EVC and EFP, page 36
- Restrictions for EVC and EFP, page 36
- Information About Carrier Ethernet, page 36
- How to Configure EVC, page 50
- Verifying the EVC Configuration, page 52
- Configuration Examples for EVC, page 53
- Additional References for EVC, page 54

Carrier Ethernet

The Carrier Ethernet uses a high bandwidth Ethernet technology to deliver dedicated connectivity. It provides network connectivity by connecting to the customer site through a private Layer 2 Ethernet circuit. The available interfaces are normally 10Mbps and 100Mbps Fast Ethernet, 1000Mb/s Gigabit Ethernet and 10Gb/s Ethernet.

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 Toolkit 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.
Prerequisites for EVC and EFP

- The EFP point-to-multipoint service supports rewrite ingress with the symmetric option. It does not support the rewrite egress operation.

- Only two encapsulations are supported—untagged and default. If default is configured, configuring untagged is not required and vice versa.

- If encapsulation default is configured on an EFP, no other encapsulation match on a EFP can be configured.

- Encapsulation range limits—Only up to 4 ranges are allowed for each EFP and only up to 8 VLAN ranges are allowed for each port.

Restrictions for EVC and EFP

The following are the general restrictions for the EVC and EFP features:

- Different EFPs cannot have encapsulation for the same VLAN ID on a single interface. For example, dot1q 10 and dot1q 1-20 are not supported on a single interface because both include the same VLAN 10.

- Two different Ethernet types are not supported on a single interface. For example, encapsulations dot1q and dot1ad are not supported on the same interface.

- Rewrite Push 1 tag operation is not supported for encapsulations with double tag.

- Rewrite Push 2 tag operation is not supported for encapsulations with single or double tag.

- Rewrite pop operations are not supported for encapsulations, such as untagged, any, default, and for encapsulations involving VLAN range and list.

- Translate rewrite operations are not supported for encapsulations, such as untagged, any, default, and for encapsulations involving VLAN range and list.

- Two EFPs on the same bridge domain and on the same interface is not supported.

Information About Carrier Ethernet

The Carrier Ethernet enables you to run different services over a single connection. Next Generation Networks, VoIP, Storage, and Managed Security are some of the services that can run over a single Carrier Ethernet connection.

The Metro Ethernet Forum (MEF) defines the following five attributes to define an Ethernet as Carrier class:

- Standardized Services
- Quality of Service
- Scalability
- Service Management
• Reliability

The Carrier Ethernet can be deployed in many ways:
• Ethernet over SDH/SONET
• Ethernet over MPLS
• Native Ethernet

Note

The Cisco ME 2600X system currently supports Native Ethernet only.

Understanding Ethernet Virtual Circuit

The Ethernet Virtual Circuit (EVC) represents the service offered and is carried through the provider network. Each EVC is configured by its unique name across the provider network.

An EVC is an end-to-end representation of a single instance of a Layer 2 service that a service provider offers. It embodies the different parameters based on which the service is offered. EVC prevents data transfer between sites that are not part of the same EVC.

In simple terms, EVC is the A–Z circuit that enables you to pass customer VLANs from one port on a node to another port on another node in the network.

In the Cisco ME 2600X system, the EVC represents a Carrier Ethernet Service and is an entity that provides end-to-end connection between two or more customer end points.

EVC Attributes

Some of the global EVC attributes are:
• EVC ID—An unique identifier that identifies the EVC
• EVC Type—E-TREE
• List of associated EFPs that belong to an EVC

EVC Features

EVC in Cisco ME 2600X supports the following features:
• Create, delete, or modify EFPs
• Add EFPs as members of a bridge domain
• Map Traffic to EFPs based on:
  • 802.1q VLANS (Single VLAN, list, range)
  • Cisco Q-in-Q VLANS (Single outer and single inner VLAN)
  • Proprietary Q-in-Q VLANS (9100, 9200)
802.1ad Provider Bridges (encapsulation and rewrite)

- Map VLAN—Push, Pop, Translate Single VLAN tag
- Support for rewriting single or double VLAN tags
- Support for grouping VLANs from several UNI to a single EVC
- Support for Ethernet UNI with dual VLAN tag (Cisco-QinQ or IEEE 802.1ad)
- Support for 802.1Q VLAN ID translation on the 802.1q tagged traffic on the UNI
- Support for point-to-multipoint EVC
- Support for 1:1, 1:2, 2:1, and 2:2 VLAN translation
- EVC MAC address aging
- Flex Service Mapping (Advanced VLAN translations).
  - Support for dot1ad and Cisco Q-in-Q etype for S-tag
- Support for Layer 2 Protocol Tunneling (L2PT) for each port

**EVC Types**

Cisco ME 2600X supports Point-to-multipoint EVCs (E-LINE services):

**Ethernet Virtual Private Line**

An Ethernet Virtual Private Line (EVPL) is a point-to-multipoint EVC. EVPL is an EVC that supports communication between two UNIs. In EVPL, multiple EVCs can exist on a port and the port can have multiple EFPs. Each EFP is associated with a different bridge domain. See figure below.

*Figure 1: Ethernet Virtual Private Line*

**Interactions of EVC with Other Features**

EVC interacts with the following features.

- LAG
- REP
- Dot1ad and Layer 2 Protocol Tunneling
• MAC learning and MAC address limiting
• QoS
• MVR
• IGMP Snooping

EVC with LAG
EFPs can be configured on a channel group. The traffic, carried by the EFPs, is load balanced across the member links. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. The load balancing is achieved by distributing EFPs between the member links. The EFPs on a channel group are grouped and each group is associated with a member link. In the default load balancing mechanism, there is no control over how the EFPs are distributed together, and sometimes the EFP distribution is not ideal. The manual load balancing mechanism can be alternatively used to control the EFP grouping.

When you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.

• The number of LAGs supported is 48.
• LACP protocol is supported on the LAG.

EVC with REP
EVC supports up to 24 segments. You can configure REP over EVC using the bridge domain at the service instance level. REP is not supported on service instances configured with encapsulation untagged or default type.

REP is not supported for Ethernet Private Line and Ethernet Virtual Private Line services.

EVC with Layer 2 Protocol Tunneling
Cisco ME 2600X supports Layer 2 protocol tunneling only at the interface level. Configurations applied at the interface level are applicable to all the EFPs configured on that interface.

The following port actions are supported in this release:

• Forward—Forwards the unmodified ingress bridge protocol data units (BPDUs) on the data path.
• Drop—Drops the ingress BPDUs on the interface.
• Peer—Punts BPDUs to the local instance of the protocol.

Valid protocols include:

• Cisco discovery protocol (CDP). For more information, see Cisco Discovery Protocol, on page 267.
• Dynamic trunking protocol (DTP). If a port can become a trunk, it may also have the ability to trunk automatically, and in some cases even negotiate what type of trunking to use on the port. DTP provides this ability to negotiate the trunking method with the other device. Default behavior of DTP on interface is 'forward'.
• Link aggregation control protocol (LACP). For more information, see Link Aggregation Group and Link Aggregation Control Protocol, on page 129. Default behavior of LACP on interface is 'peer'.
• Port aggregation protocol (PAgP) aids in the automatic creation of Fast EtherChannel links. PAgP packets are sent between Fast EtherChannel-capable ports in order to negotiate the forming of a channel. Default behavior of PAgP on interface is 'forward'.

• Spanning tree protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network. Default behavior of STP on interface is 'forward'.

• VLAN trunk protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. Default behavior of VTP on interface is 'forward'.

• 802.1X defines 802.1X port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN. Default behavior of DOT1X on interface is 'forward'.

Note
The pass option, tunnel option, and Layer 2 protocol tunneling at the EFP are not supported in this release.

The following protocols are supported for each port action:

<table>
<thead>
<tr>
<th>Port Action</th>
<th>Supported Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>LACP, CDP</td>
</tr>
<tr>
<td>Drop</td>
<td>STP, VTP, DTP, PAGP, DOT1X, LACP, CDP</td>
</tr>
<tr>
<td>Forward</td>
<td>STP, VTP, DTP, PAGP, DOT1X, LACP, CDP</td>
</tr>
</tbody>
</table>

The table below lists the default port action for each protocol:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Default Port Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>Peer</td>
</tr>
<tr>
<td>VTP</td>
<td>Forward</td>
</tr>
<tr>
<td>DTP</td>
<td>Forward</td>
</tr>
<tr>
<td>STP</td>
<td>Forward</td>
</tr>
<tr>
<td>PAGP</td>
<td>Forward</td>
</tr>
<tr>
<td>LACP</td>
<td>Peer</td>
</tr>
<tr>
<td>DOT1X</td>
<td>Forward</td>
</tr>
</tbody>
</table>

See Configuring Layer 2 Protocol Tunneling, on page 52 to configure Layer 2 protocol tunneling.
EVC with MAC Learning and MAC Address Limiting

MAC learning is supported and enabled (by default) only for point–to–multipoint bridge domains. MAC learning can be enabled or disabled for point–to–multipoint bridge domains.

The MAC address limiting for bridge domains provides the capability to control the MAC address learning behavior at the bridge domain level. You can configure an upper limit on the number of MAC addresses that reside in a bridge domain. The remaining MAC addresses are dropped because they are not learned.

The MAC address limiting commands are configured under the bridge domain.

The default MAC address limit on a bridge domain is 32000. The maximum MAC address limit on a bridge domain is 32000.

Note

Both secure and non-secure EFPs cannot coexist in the same bridge domain. If MAC security is enabled on an EFP then it should be enabled on all the EFPs existing in the same bridge domain.

See MAC Learning, on page 157.

EVC with QoS

See EVCS QoS Support, on page 66.

EVC with MVR

Multicast VLAN Registration (MVR) is supported only for point–to–multipoint services. Twenty bridge domains can be configured for MVR. The multicast traffic flows from MVR source EFP to multiple MVR receiver EFPs.

See Multicast VLAN Registration, on page 169.

EVC with IGMP Snooping

Internet Group Management Protocol Snooping (IGMP snooping) is supported only for point–to–multipoint services. IGMP snooping can be enabled only at the bridge domain level. IGMP snooping can be enabled on up to 128 bridge domains.

See IGMP Snooping, on page 183.

Understanding Ethernet Flow Point

The traffic for the service needs to pass through several switches in the provider network to connect customer sites across the provider network. The instance of a specific EVC service on the physical interface of each network device through which the EVC passes through is called an Ethernet Flow Point (EFP). An EFP is a logical demarcation point of an EVC on an interface. An EFP can be associated with a bridge domain.

In simple terms, an EFP is defined as an end point of an EVC within a node. Because multiple EVCs can pass through one physical interface, the main purpose of an EFP configuration is to recognize the traffic belonging to a specific EVC on that interface and to apply the forwarding behavior and features specific to that EVC.

The EFPs on Cisco ME 2600X can be on all the ports of the Cisco ME 2600X panel.

The possible EFP administrative states are UP and DOWN. This administrative state maps to the EFP administrative state in IOS.
EFP Attributes

The key attributes of an EFP are:

• Encapsulation string—Defines the classification criteria for an incoming packet.

• Forwarding operations—Defines the forwarding operation to be applied on frames that belong to this EFP.

• Ingress rewrite operation—Defines the rewrites to be performed on the frames that belong to this EFP before proceeding with the forwarding operations.

Note

Cisco ME 2600X supports only the Ingress rewrite operation and all the rewrite operations are symmetric in nature.

For a list of supported encapsulation and ingress rewrite operations on point-to-multipoint (P2MP) EVC, see Supported Encapsulation and Rewrite Operations, on page 43.

Counters

The following counters are supported for EFPs:

• Ingress packet counts

• Egress packet counts

• Ingress bytes

• Egress bytes

For point-to-multipoint bridge domains, all the counters are enabled by default.

Understanding Bridge Domain

The bridge domain is an Ethernet broadcast domain internal to the device. The bridge domain enables you to decouple the VLAN from the broadcast domain. The bridge domain has one to many mapping with EFPs.

All the EFPs in a node for a specific EVC are grouped using the bridge domain. If EFPs belong to the same bridge domain and have the same bridge domain number, the EFPs receive traffic even if they have different VLAN numbers.

The bridge domain number is local to the node. Different nodes that are part of an EVC can have the same or different bridge domain number. However, the bridge domain number is unique for an EVC within a node.

For EVC, the bridge domain number is from 1 to 16384.

Note

The maximum supported bridge domains at any moment is 4000.
Restriction

The encapsulation and rewrite operations are not allowed if the bridge domain is configured on the EFP. Remove the existing bridge domain from the EFP and then change the encapsulation and rewrite operations.

Supported Bridge Domain

The bridge domain in Cisco ME 2600X can be configured to operate in point-to-multipoint mode only. This bridge domain can be used for Ethernet Private LAN (EPLAN) and Ethernet Virtual Private LAN (EVPLAN). Cisco ME 2600X supports up to 4000 point-to-multipoint bridge domains. MAC learning is supported for point-to-multipoint bridge domains. The point-to-multipoint bridge domain is supported over REP.

Supported Encapsulation and Rewrite Operations

The table below lists the supported encapsulation and rewrite operations for point-to-multipoint (P2MP) EVC and VPLS EFP:

<table>
<thead>
<tr>
<th>Encapsulation Criterion</th>
<th>Ingress Rewrite Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation default</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q any</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q range</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q list</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q range, list exact</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q range exact</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q list exact</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q any second-dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q range second-dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
</tbody>
</table>

Note: When using `encapsulation dot1q <vlan id> exact` command, only `vlan-type-0x8100` (default) is supported.
### Supported Encapsulation and Rewrite Operations

<table>
<thead>
<tr>
<th>Encapsulation Criterion</th>
<th>Ingress Rewrite Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q list</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad any</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad range</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; exact</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad any dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad range dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q list</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q any vlan-type &lt;type value&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q range vlan-type &lt;type value&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; exact</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q any vlan-type &lt;type value&gt; dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q range vlan-type &lt;type value&gt; dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; dot1q &lt;vlan id&gt;</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; dot1q list</td>
<td>No rewrite</td>
</tr>
<tr>
<td>encapsulation default</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q any</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q list</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>Encapsulation Criterion</td>
<td>Ingress Rewrite Action</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>encapsulation dot1q range, list exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q list exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation default</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q any</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q list</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range, list exact</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range exact</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q list exact</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation default</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q any</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q list</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation untagged, dot1q range, list</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range, list exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q range exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q list exact</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; symmetric</td>
</tr>
<tr>
<td><strong>Encapsulation Criterion</strong></td>
<td><strong>Ingress Rewrite Action</strong></td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>rewrite ingress tag push dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation untagged</td>
<td>rewrite ingress tag push dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>Encapsulation Criterion</td>
<td>Ingress Rewrite Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
</tbody>
</table>
### Supported Encapsulation and Rewrite Operations

<table>
<thead>
<tr>
<th>Encapsulation Criterion</th>
<th>Ingress Rewrite Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; exact</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 1-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-1 dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-1 dot1ad &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-1 dot1q &lt;vlan id&gt; vlan-type &lt;type-value&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>Encapsulation Criterion</td>
<td>Ingress Rewrite Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1q &lt;vlan id&gt; vlan-type &lt;type value&gt; second-dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
<tr>
<td>encapsulation dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt;</td>
<td>rewrite ingress tag translate 2-to-2 dot1ad &lt;vlan id&gt; dot1q &lt;vlan id&gt; symmetric</td>
</tr>
</tbody>
</table>
How to Configure EVC

The following tasks describe how to configure EVC on the Cisco ME 2600X device:

- Configuring an Ethernet Service Instance, on page 50
- Configuring Layer 2 Protocol Tunneling, on page 52

Configuring an Ethernet Service Instance

To configure an EVC service instance under the point–to–multipoint bridge domain, complete the following steps:

Prerequisite
Manually Booting from a Cisco IOS Software Image, on page 2

SUMMARY STEPS

1. enable
2. configure terminal
3. interface ethernet evc [evc-id]
4. interface type number
5. service instance id ethernet [evc-id]
6. encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]} second-dot1q {any | vlan-id [vlan-id [-vlan-id]]}
7. rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}} {symmetric}
8. bridge-domain bridge-id [split-horizon]
9. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface ethernet evc [evc-id]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ethernet evc evc_101</td>
</tr>
</tbody>
</table>

| Step 4 | interface type number | Specifies the interface to configure and enters interface configuration mode. |
| **Example:** | Switch(config)# interface TenGigabitEthernet 0/45 | |

| Step 5 | service instance id ethernet [evc-id] | Configures an Ethernet service instance on an interface and enters service instance configuration mode. |
| **Example:** | Switch(config-if)# service instance 101 ethernet | |

| Step 6 | encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]} second-dot1q {any | vlan-id [vlan-id [-vlan-id]]} | Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance. |
| **Example:** | Switch(config-if-srv)# encapsulation dot1q 100 second dot1q 200 | |

| Step 7 | rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} 2-to-1 dot1q vlan-id | dot1ad vlan-id} 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} [symmetric]} | Specifies the rewrite operation to be applied on the frame ingress to the service instance. |
| **Example:** | Switch(config-if-srv)# rewrite ingress tag push dot1q 20 | |

| Step 8 | bridge-domain bridge-id [split-horizon] | Binds the Ethernet service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance. The valid values for bridge-id range from 1 to 4096. |
| **Example:** | Switch(config-if-srv)# bridge-domain 12 | |

| Step 9 | exit | Exits the service instance configuration mode. |
| **Example:** | Switch(config-if-srv)# exit | |
Configuring Layer 2 Protocol Tunneling

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. l2protocol [drop|forward|peer] [cdp|dot1x|dtp|lacp|pagp|stp|vtp]
5. 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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>l2protocol [drop</td>
<td>forward</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# l2protocol forward cdp</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the EVC Configuration

Use the following show commands to verify the EVC configuration:

• show ethernet service instance
• show l2protocol interface
Ethernet Service Instance

Use the following command to show the Ethernet service instances:

```
Switch# show ethernet service instance
```

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>Interface</th>
<th>State</th>
<th>CE-Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>static</td>
<td>GigabitEthernet0/43</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>170</td>
<td>static</td>
<td>GigabitEthernet0/44</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>160</td>
<td>static</td>
<td>TenGigabitEthernet0/48</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

Layer 2 Protocol Interface

Use the following command to show the layer 2 protocol interfaces:

```
Switch# show l2protocol interface gigabitEthernet 0/25
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Drop Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp</td>
<td>0</td>
</tr>
<tr>
<td>stp</td>
<td>0</td>
</tr>
<tr>
<td>vtp</td>
<td>0</td>
</tr>
<tr>
<td>dtp</td>
<td>0</td>
</tr>
<tr>
<td>pagp</td>
<td>0</td>
</tr>
<tr>
<td>dot1x</td>
<td>0</td>
</tr>
<tr>
<td>lldp</td>
<td>0</td>
</tr>
<tr>
<td>lacp</td>
<td>41</td>
</tr>
<tr>
<td>udld</td>
<td>0</td>
</tr>
</tbody>
</table>

Configuration Examples for EVC

**Ethernet Service Instance**

The following example shows how to configure an Ethernet service instance:

```
Switch> enable
Switch# configure terminal
Switch(config)# ethernet evc evc_101
Switch(config-if)# service instance id ethernet
Switch(config-if)# encapsulation dot1q 100
Switch(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Switch(config-if-srv)# bridge-domain 12
Switch(config-if-srv)# exit
```

The following example shows how to configure a rewrite using Cisco IOS commands:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface g0/30
Switch(config-if)# no shut
Switch(config-if)# service instance 1 ethernet
Switch(config-if-srv)# encapsulation dot1q 13
Switch(config-if-srv)# bridge-domain 13
Switch(config-if-srv)# exit
```
Additional References for EVC

The following sections provide references related to the EVC feature.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
</tbody>
</table>

**RFCs**

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported, and support for existing RFCs has not been modified.</td>
<td>—</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Quality of Service

This chapter describes the Quality of Service for Cisco ME 2600X and procedures to configure Quality of Service.

- Quality of Service, page 57
- Prerequisites for QoS, page 58
- Restrictions for QoS, page 58
- Information About QoS, page 58
- How to Configure QoS, page 69
- Troubleshooting Tips, page 94
- Configuration Examples for QoS, page 94
- Verifying the QoS Configuration, page 98
- Additional References for QoS, page 100

Quality of Service

Quality of Service (QoS) refers to the ability of a network to provide improved services to selected network traffic over various underlying technologies including Ethernet and IEEE 802.1 networks.

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 Toolkit 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.
Prerequisites for QoS

The following two components are necessary to deliver QoS across a heterogeneous network:

- QoS within a single network element, which includes queuing, scheduling, and traffic shaping features.
- QoS policing and management functions to control and administer end-to-end traffic across a network.

Restrictions for QoS

The following are the general restrictions for the QoS feature:

- Policing is not supported at egress level.
- Only 0 to 6 queues can be used at egress. QoS-Group 3 is used for LLQ (Priority) traffic at egress.
- Remarking does not happen if the outer or inner VLAN is configured with ANY, LIST, or RANGE.
- COS marking fails with encapsulation VLAN range and match VLAN range.
- The police cir command is not supported at the parent level in the hierarchical quality of service (HQoS). HQoS supports only the police rate command at parent level.
- Parent level should always be class-default in HQoS.
- An ingress policer does not support more than 8 classes.
- An egress policer does not support more than 7 classes.

Information About QoS

The QoS mechanism has three basic steps. It classifies types of traffic, specifies what action to take against a type of traffic, and specifies where the action should take place. The following sections explain how the Cisco ME 2600X accomplishes these steps.

Classification Mechanism for IP and Ethernet

For any QoS service to be applied to data, there must be a way to classify an IP packet or an Ethernet frame. When identified, a specific priority can be assigned to each individual IP packet or Ethernet frame. The IP Precedence field or the IP Differentiated Services Code Point (DSCP) field can be used to classify IP packets, and the Ethernet class of service (IEEE 802.1p defined class of service [CoS]) can be used for classifying Ethernet frames. IP precedence, IP DSCP, and Ethernet CoS are further described in the following sections.

IP Precedence

Use of IP precedence enables you to specify the class of service (CoS) for a packet using the three precedence bits in the type of service (ToS) field of the IP version 4 (IPv4) header. By default, each precedence corresponds to a name. These names, which continue to evolve, are defined in RFC 791.

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>routine</td>
</tr>
</tbody>
</table>
IP precedence bit settings 6 and 7 are reserved for network control information, such as routing updates.

**IP Differentiated Services Code Point**

IP DSCP uses the six bits in the IPv4 header to specify class of service for each IP packet (IETF RFC 2474). The DSCP field classifies packets into any of the 64 possible classes. On the network edge, the IP DSCP is assigned by the client device or the switch, so that each subsequent network element can provide services based on the determined policy or the SLA.

IP Precedence and DSCP is illustrated in this figure.

*Figure 2: IP Precedence and DSCP*

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>priority</td>
</tr>
<tr>
<td>2</td>
<td>immediate</td>
</tr>
<tr>
<td>3</td>
<td>flash</td>
</tr>
<tr>
<td>4</td>
<td>flash-override</td>
</tr>
<tr>
<td>5</td>
<td>critical</td>
</tr>
<tr>
<td>6</td>
<td>internet</td>
</tr>
<tr>
<td>7</td>
<td>networks</td>
</tr>
</tbody>
</table>
**Ethernet CoS**

The Ethernet CoS refers to the three bits within a four byte IEEE 802.1Q (VLAN) header used to indicate the priority of the Ethernet frame as it passes through a switched network. The CoS bits in the IEEE 802.1Q header are commonly referred to as the IEEE 802.1p bits. There are three CoS bits that provide eight classes, matching the IP precedence number. In many real-world networks, a packet might traverse both Layer 2 and Layer 3 domains. To maintain QoS across the network, the IP ToS can be mapped to the Ethernet CoS and vice versa. For example, in a linear or one-to-one mapping where each mechanism supports eight classes. Similarly, a set of DSCP values (64 classes) can be mapped into each of the eight individual Ethernet CoS values. An IEEE 802.1Q Ethernet frame, which consists of a 2-byte Ethertype and a 2-byte tag (IEEE 802.1Q tag) on the Ethernet protocol header is shown in this figure.

**Figure 3: Ethernet Frame and the CoS Bit (IEEE 802.1p)**

---

**Advantages of QoS**

Enabling QoS in the network has the following advantages:

- **Control over resources**—You can control resources like bandwidth that is being used.
- **Tailored services**—If you are a service provider, the control and visibility that QoS provides enable you to offer carefully tailored grades of service differentiation to your customers.
- **Coexistence of mission-critical applications**:
  - Your WAN is used efficiently by mission-critical applications that are most important to your business.
  - Bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available.
  - Other applications using the link get their fair service without interfering with mission-critical traffic.
Cisco ME 2600X QoS

The Cisco ME 2600X QoS classifies each packet in the network based on its Ethernet CoS, IP precedence, IP DSCP, or VLAN ID. After they are classified into class flows, further QoS functions can be applied to each packet as it traverses the Cisco ME 2600X.

The policing feature of the Cisco ME 2600X system ensures that the attached equipment does not submit more than a predefined amount of bandwidth (Rate Limiting) into the network. The policing feature can be used to enforce the committed information rate (CIR) and the peak information rate (PIR) available to a customer at an interface. The policing action is applied per classification.

The marking feature can set the Ethernet CoS, IP precedence, or IP DSCP bits when packets enter the Cisco ME 2600X. The marking feature operates on the outer IEEE 802.1p tag, IP precedence, or IP DSCP bits and provides a mechanism for tagging packets at the ingress. The subsequent network elements can provide a QoS based only the QoS indicator that the service provider has created.

The per-class queuing allows various queuing applications to support SLA. For example, allocation of committed information rate, ensuring low latencies and rate limiting traffic to downstream nodes based on the configuration, and also enabling fair access to excess network bandwidth. The Cisco ME 2600X uses a combination of Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR) scheduling process to guarantee throughput and latency requirements and to provide fair access to excess bandwidth. The Cisco ME 2600X QoS flow is illustrated in this figure.

Figure 4: Cisco ME 2600X QoS flow

Ingress QoS Functions

Ingress QoS on the Cisco ME 2600X system involves classification, marking, and policing. The ingress card classifies the packets and assigns a traffic-class to it. The traffic-class is used for internal queuing and congestion management, as well as classification at the egress. At ingress, policy application is supported on multiple targets, which are:

- Ten Gigabit Ethernet (10 GE) and one Gigabit Ethernet (1 GE) interface
- Port-channel interface
- Port-channel member interface
- Service instance on 10 GE and 1 GE interfaces
- Service instance on port-channel
Ingress Classification

Classifying network traffic enables you to organize traffic into traffic classes or categories on the basis of whether the traffic matches specific criteria. Using the packet classification, you can partition network traffic into multiple priority levels or classes of service. Traffic is classified to determine whether it should be:

- Marked for further processing
- Policed to rate limit specific traffic types

The Cisco ME 2600X system supports ingress classification. The default class, named class-default, is the class to which any traffic that does not match any of the selection criteria in the configured class maps, is directed.

To configure ingress classification, see Configuring Ingress Classification, on page 70.

Ingress Policing

Ingress policing ensures that an attached equipment does not submit more than a predefined amount of bandwidth (Rate Limiting) into the network. The policing feature can be used to enforce the committed information rate (CIR) and the peak information rate (PIR) available to a customer at an interface or a service instance on an interface. Policing enables to limit the data flow through the Cisco ME 2600X by dropping or marking down the QoS value according to the configuration.

The Cisco ME 2600X supports ingress policing. When policing is configured, traffic is placed in one of the following categories:

- Conform
- Exceed
- Violate

Within these three categories, users can decide the actions to be applied. For instance, packets that conform to the policy rate can be configured to be transmitted, packets that exceed the policy rate can be configured to be sent with a decreased priority, and packets that violate the policy rate can be configured to be dropped.

If no actions are specified, the default conform-action is transmit, and default exceed-action or violate-action is drop.

The table below contains the list of policing actions supported at the ingress:

**Table 4: Policing Actions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit</td>
<td>Transmits the packet.</td>
</tr>
<tr>
<td>drop</td>
<td>Drops the packet.</td>
</tr>
<tr>
<td>set-cos-transmit</td>
<td>Sets the CoS value and transmits the packet.</td>
</tr>
<tr>
<td>set-dscp-transmit</td>
<td>Sets the IP DSCP value and transmit the packet.</td>
</tr>
<tr>
<td>set-precedence-transmit</td>
<td>Sets the IP precedence value and transmits the packet.</td>
</tr>
</tbody>
</table>
### Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the QoS-group value and transmits the packet.</td>
</tr>
</tbody>
</table>

The policing features supported are:

- Individual actions
- Multiple actions
- Single rate, 2-color policer
- Single rate, 3-color policer
- Dual rate, 3-color policer
- Color blind mode
- Hierarchical policing (two levels)

To create a policy-map, see Configuring Ingress Policing, on page 73.

To attach or remove a traffic policy from the interface, see Attaching or Removing a Traffic Policy from the Target, on page 78.

### Ingress Marking

Marking is a way to selectively modify QoS bits in a packet to identify traffic within the system and/or the network. The downstream devices in the network and the egress targets within the system can match the traffic based on the marking done at the ingress of the system. The Cisco ME 2600X supports ingress marking.

After you create traffic classes, configure traffic policies and traffic marking features to apply certain actions to the selected traffic in those classes.

In most cases, the purpose of a packet mark is identification. After a packet is marked, downstream devices identify traffic based on the marking and categorize the traffic according to network needs. This categorization occurs when the match commands in the traffic class are configured to identify the packets by their marking (for example, match IP precedence, match IP DSCP, match CoS, and so on). The traffic policy using this traffic class can then set the appropriate QoS features for the marked traffic.

To configure ingress marking, see Configuring Ingress Marking, on page 80.

### Egress QoS Functions

For FTTH LAG QoS, service policy application can only happen at port-channel main interface. This policy application should in turn be mapped statically to member interfaces. No egress policy-map application allowed on port-channel member interface or EFP.

**QoS for Multicast/Unicast Traffic**

While applying QOS, there is no differentiation between unicast and multicast traffic at the queue level. Both the streams are treated equally at queue level for QoS. There are no specific classes available to apply the QoS specific to multicast traffic.
Traffic Handling in the Absence of an Output Policy

If there is no output policy configured on an EVC or an interface, the unicast traffic is queued at the egress based on the traffic class set at the ingress. In the absence of an output policy, all the egress queues are treated equally and scheduled according to the Round Robin method.

Unicast QoS Restrictions

Traffic is queued in separate queues at the egress based on the traffic-class set in the frame at the ingress. This is irrespective of whether there is an egress policy applied or not.

Note: The “class-default” classification does not work at the leaf level of an output policy. This works only at a parent level in a hierarchical policy. It must be ensured that all traffic that needs to be matched using “class-default” at the leaf level is set to “qos-group 0” at the ingress, which forces the traffic-class to 0 resulting in traffic being queued in queue 0 which corresponds to the class-default.

Egress Classification

The egress classification is limited to using a traffic class field in frames to categorize the frames and make them available for QoS handling. Therefore, classification based on frame fields, such as Ethernet CoS, IP DSCP, IP precedence, and so on, should be done at ingress, and the traffic class should be assigned to the corresponding frames using the ingress marking feature.

Traffic is classified to determine whether it should be:

- Marked for further processing
- Queued and scheduled

To configure classification at the egress, see Configuring Egress Classification, on page 85.

Egress Queue Scheduling

The Cisco ME 2600X system supports Weighted Round Robin (WRR) and Low Latency Queueing (LLQ). Queueing is based on the class based classification done at egress. LLQ prioritizes and ensures low latency to the traffic in queues configured to be in LLQ, and the remaining traffic is scheduled using WRR.

Note: Queue depth is not configurable. Each queue has a minimum depth of 25600 bytes and maximum depth of 1048576 bytes.

For information on egress LLQ, see Egress LLQ, on page 65.
For information on egress bandwidth, see Egress Bandwidth, on page 65.
For information on egress shaping, see Egress Shaping, on page 65.
For information egress Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP), see Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent, on page 65.
**Egress LLQ**

Applications which are latency sensitive require handling of data with least possible delay within the system. In the Cisco ME 2600X system, low latencies are guaranteed by using strict priority scheduling at various congestion points and egress.

To configure LLQ, see Configuring Egress LLQ, on page 86.

**Egress Bandwidth**

Applications that require committed information rate (CIR) should reserve the CIR on a per-target basis at the egress. After configuring the CIR, the traffic rates are guaranteed to be met in case of congestion at the egress.

To configure the egress bandwidth, see Configuring Egress Bandwidth, on page 88.

**Egress Shaping**

Traffic shaping enables you to control the traffic going out of an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. Shaping can be used to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Shaping is the process of delaying packets in queues to make them conform to a specified profile.

To configure shaping at the egress, see Configuring Egress Shaping, on page 90.

**Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent**

Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP) specifies the ratio or percentage of the bandwidth that is divided between targets when there is congestion. BRR indicates the ratio with which the various classes are serviced when parent target is scheduled. BRP indicates the bandwidth to be allocated to each class as a percentage of the allocation done to the parent target in a hierarchical QoS model.

To configure egress BRR or BRP, see Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent, on page 92.

**Hierarchical QoS**

The Cisco ME 2600X system supports hierarchical quality-of-service (H-QoS) that includes QoS at multiple levels in a hierarchy.

**Ingress H-QoS**

An H-QoS policy can be attached to an interface or a service instance. The number of levels is limited to two for an input QoS policy, where the parent level denotes the policy target and the child level denotes the QoS traffic class:

- Only the default class, that is, **class-default** is allowed at the parent level. User-defined classes are not supported at the parent level.
Only the **police** action command is allowed at the parent level. Marking action is not supported. Also, remarking actions are not supported for the parent policer. In effect, a hierarchical policy is configured to achieve only hierarchical metering.

**EVCS QoS Support**

The Ethernet Virtual Connection Services (EVCS) uses the concept of service instances and EVC (Ethernet Virtual Circuit). A service instance is the instantiation of an EVC on a given interface on a given device. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered.

QoS works with the following EVC combinations:

- One TAG case
- Two TAG case
- One TAG to one TAG
- One TAG to two TAG
- Two TAG to one TAG
- Two TAG to two TAG
- One TAG termination
- Two TAG termination
- Tag to Tag translation

**Restrictions for QoS on EVCS**

- CoS marking or remarking is not supported for service instances defined using VLAN ranges or "encapsulation default".
- CoS marking or remarking action applies to both inner and outer tags, when inner tag is modified within the system. In all other cases, the marking or remarking action that the user specifies is limited only to the outer tag.

**Note**
For information on EVC, see Understanding Ethernet Virtual Circuit, on page 37.

**QoS Support on Port-Channel**

This section explains the QoS on the Port-Channel feature support for ingress and egress.

**QoS Support on Port-Channel at Ingress**

The QoS on the port-channel feature enables QoS service-policies to be applied at the ingress on the following targets:

- Port-channel member link
• Port-channel main interface
• Port-channel EVC

For a policy-map attached to a port-channel main interface, ingress traffic coming from any member link is subjected to the same policy-map configured on the port-channel main interface. If no policy-map is configured on the port-channel main interface, ingress traffic from the member-link is subjected to the policy-map attached to the:

- EVC through which the traffic is flowing.
- Member link.

The QoS policy can be attached to a port-channel even if the member interfaces are on different cards. Policy-maps cannot coexist on a port-channel main interface, EVC, and member link at the same time.

**Restrictions for QoS Support on Port-Channel at Ingress**

The policer configuration is enforced only on a single card and not across cards in a distributed link aggregation group (LAG). However, member links might span across cards.

**QoS Support on Port-Channel at Egress**

The QoS on port-channel feature enables QoS service-policies to be applied at the egress on the port-channel main interface.

---

**Note**

Egress service policy is not supported on the port-channel member link.

---

**Restrictions for QoS Support on Port-Channel at Egress**

A policy that is applied on a port channel is not applicable to the aggregate port channel traffic. It is applicable only on a per port-channel member basis. Therefore, if a configuration that shapes all the traffic to \( x \text{ Mbps} \) on the port-channel main interface exists, it gets translated to a configuration that shapes each member link to \( x \text{ Mbps} \). As a result, the aggregate traffic on the port channel could be up to \( n \) times \( x \text{ Mbps} \), where \( n \) is the number of links in the port-channel.

---

**QoS Statistics**

Enhanced performance monitoring displays QoS statistics on the Cisco ME 2600X interfaces. QoS statistics are supported at the 1GE interface, 10GE interface, and service instance levels. At the ingress, only byte counters are supported and at the egress, both packet and byte counters are supported.

Statistics supported at ingress are shown in the table below:
Table 5: Statistics at Ingress

<table>
<thead>
<tr>
<th>Statistics Collected</th>
<th>1GE Interface</th>
<th>10GE Interface</th>
<th>EVC</th>
<th>Port Channel Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification statistics—Packet and Byte Counters</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Marking Statistics—Byte Counters</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Marking Statistics—Packet Counters</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policing Statistics—Packet and Byte Counters</td>
<td>Supported with limitations:</td>
<td>Supported with limitations:</td>
<td>No</td>
<td>Supported with limitations:</td>
</tr>
<tr>
<td>• In a 2-color policer, both green and red byte counters are supported.</td>
<td>• In a 2-color policer, both green and red byte counters are supported.</td>
<td></td>
<td>• In a 2-color policer, both green and red byte counters are supported.</td>
<td></td>
</tr>
<tr>
<td>• In a 3-color policer, green/non-green or non-red/red are supported.</td>
<td>• In a 3-color policer, green and non-green or non-red and red are supported.</td>
<td></td>
<td>• In a 3-color policer, green/non-green or non-red/red are supported.</td>
<td></td>
</tr>
</tbody>
</table>

Statistics supported at egress are shown in this table:

Table 6: Statistics at Egress

<table>
<thead>
<tr>
<th>Statistics Collected</th>
<th>1GE Interface</th>
<th>10GE Interface</th>
<th>EVC</th>
<th>Port Channel Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification statistics - Packet and Byte Counters</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Queuing Statistics—(Accepted or Dropped) Packet and Byte Counters</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Scalability

The table below lists scalability for Cisco ME 2600X:

<table>
<thead>
<tr>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>320 x 8 policers</td>
</tr>
<tr>
<td>System supports 320 policymaps</td>
</tr>
<tr>
<td>System supports 512 unique class maps</td>
</tr>
<tr>
<td>System supports 1024 unique policymaps</td>
</tr>
<tr>
<td>160 policymaps on LAG interface</td>
</tr>
<tr>
<td>7 queues / classes per interface</td>
</tr>
</tbody>
</table>

**Note**

If all the FP entries are used under port-channel pool (LAG interface has maximum EFPs with maximum number of filters), then LAG works in double mode and you cannot apply ingress policer on any interface or service instance.

### How to Configure QoS

The following tasks describe how to configure QoS on the Cisco ME 2600X device:

- Configuring QoS Features, on page 70
- Configuring Ingress Classification, on page 70
- Configuring Ingress Policing, on page 73
- Attaching or Removing a Traffic Policy from the Target, on page 78
- Configuring Ingress Marking, on page 80
- Configuring Ingress Re-Marking, on page 82
- Configuring Egress Classification, on page 85
- Configuring Egress LLQ, on page 86
- Configuring Egress Bandwidth, on page 88
- Configuring Egress Shaping, on page 90
Configuring QoS Features

Note

Users can create traffic policies and attach these policies to targets. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

SUMMARY STEPS

1. Define a traffic class using the **class-map** command:
2. Create a traffic policy using the **policy-map** command to associate the traffic class with one or more QoS features (using the **policy-map** command):
3. Attach the traffic policy to the target using the **service-policy** command, see Attaching or Removing a Traffic Policy from the Target, on page 78.
4. Monitor and verify the QoS configuration. See Monitoring and Verifying QoS Configuration.

DETAILED STEPS

**Step 1**
Define a traffic class using the **class-map** command:
   a) To configure traffic classification at the ingress, see Configuring Ingress Classification, on page 70.
   b) To configure traffic classification at the egress, see Configuring Egress Classification, on page 85.

**Step 2**
Create a traffic policy using the **policy-map** command to associate the traffic class with one or more QoS features (using the **policy-map** command):
   a) To configure policing at the ingress, see Configuring Ingress Policing, on page 73.
   b) To configure marking at the ingress, see Configuring Ingress Marking, on page 80.
   c) To configure shaping at the egress, see Configuring Egress Shaping, on page 90.
   d) To configure the egress bandwidth, see Configuring Egress Bandwidth, on page 88.
   e) To configure low-latency queuing (LLQ), see Configuring Egress LLQ, on page 86.
   f) To configure bandwidth remaining ratio (BRR) or bandwidth remaining percent (BRP), see Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent, on page 92.

**Step 3**
Attach the traffic policy to the target using the **service-policy** command, see Attaching or Removing a Traffic Policy from the Target, on page 78.

**Step 4**
Monitor and verify the QoS configuration. See Monitoring and Verifying QoS Configuration.

Configuring Ingress Classification

- The **match** commands are used to specify various criteria for classifying packets. The packets are checked to determine whether they match the criteria specified in the **match** commands.
- The `match-all` keyword is added to the `match` command and `match-all` is the default. This classification specifies that the traffic class must match all of the specified criteria within the class-map.

- The CoS should be 0 by default for untagged traffic and it will be matched with a CoS 0 filter, if the class-map has the CoS 0 filter.

To configure ingress classification on the device, complete the following steps:

**Before You Begin**

**Note**
- Traffic classification based on multiple QoS fields (Ethernet class of service [CoS], IP precedence, and so on) for a single packet is not supported. Traffic classification is based only on the first matching parameter (in the user-specified order) of the QoS fields, if multiple match criteria are specified in a single class.

- The `match-all` cannot have more than two combinations of the classification criteria. However, the class-map can be created with more than two combinations of classification criteria. The policy with such class-map does not work and reports an error message indicating the failure. You should rectify the class-map with one classification criteria and try again.

- When using class-map, after you have added or removed a filter, do not immediately remove or add another filter as it may cause an error message to display. If you receive an error message, try again by increasing the time interval between removal or addition of the filter.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `class-map [match-any] [match-all] class-map-name`
4. `match cos cos-number`
5. `end`

### 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.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Ingress Classification

#### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>class-map [match-any] [match-all] class-map-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# class-map match-any class1</td>
</tr>
</tbody>
</table>

- **class-map**: Creates a class to be used with a class map and enters the class-map configuration mode. The class map is used for matching packets to the specified class.
  - **match-any**: Specifies that one of the match criterion must be met. Use this keyword only if you have to specify more than one match command.
  - **match-all**: Specifies that the traffic class must match all of the specified criteria.
  - **class-map-name**: Class map name. This is the name of the class map and can have a maximum of 40 alphanumeric characters.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>match cos cos-number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match cos 2</td>
</tr>
</tbody>
</table>

- **match cos**: Matches a packet on the basis of a Layer 2 CoS number.
  - **cos-number**: CoS value. The value can range from 0 to 7.

**Note**: The **match cos** command is just an example of one of the match commands that can be used. For a list of other match commands, see Table 7: Traffic Class Commands, on page 72

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# end</td>
</tr>
</tbody>
</table>

- **end**: Exits class-map configuration mode and returns to privileged EXEC mode.

---

The table below provides the traffic class commands supported at the ingress:

**Table 7: Traffic Class Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match cos cos-number</strong></td>
<td>Matches a packet on the basis of a Layer 2 CoS number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match cos 2</td>
</tr>
<tr>
<td></td>
<td>- <strong>cos-number</strong>: CoS value. The value can range from 0 to 7.</td>
</tr>
<tr>
<td><strong>match ip precedence ip-precedence-value</strong></td>
<td>Identifies the IP precedence value as match criteria.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match ip precedence 5</td>
</tr>
<tr>
<td></td>
<td>- <strong>ip-precedence-value</strong>: IP precedence value. The value can range from 0 to 7.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match ip dscp (ip-dscp-value)</td>
<td>Identifies a specific IP DSCP value as a match criterion.</td>
</tr>
<tr>
<td></td>
<td>• (ip-dscp-value) — IP DSCP value. The value can range from 0 to 63.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-cmap)# match ip dscp 6</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match vlan [vlanid ]</td>
<td>Specifies a VLAN ID or range of VLAN IDs in a class-map to match packets.</td>
</tr>
<tr>
<td></td>
<td>• (vlanid) — VLAN ID. The value can range from 0 to 4096.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-cmap)# match vlan 100</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Ingress Policing

To configure ingress policing on the device, complete the following steps:

#### Before You Begin

**Configuring Ingress Classification,** on page 70

#### Note

- In a hierarchical QoS policy, only a single-rate, 2-color policer is supported at the parent level. This should be configured using the **police \[rate\] bps-value** action command. The **police cir** command is not supported at the parent level.

- In a hierarchical QoS policy with policer configured at the parent level, only a single-rate, 2-color policer or a dual-rate, 3-color policer is supported at the child level.

### SUMMARY STEPS

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class \{class-name | class-default\}
5. police \[cir | rate\] bps-value \[bc | burst\] bc \[be | peak-burst\] be conform-action action exceed-action action violate-action action
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

- Enter your password if prompted.

### Step 2

**Command or Action:**

Example:

```
Switch> enable
```

**Purpose:**

Enters global configuration mode.

### Step 3

**Command or Action:**

Example:

```
Switch(config)# configure terminal
```

**Purpose:**

Creates or specifies the name of the traffic policy and enters the policy-map configuration mode.

- `policy-map-name`—Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.

### Step 4

**Command or Action:**

Example:

```
Switch(config-pmap)# class class1
```

**Purpose:**

Specifies the name of a traffic class to which the policy applies and enters the policy-map class configuration mode.

- `class-name`—User-defined class name to which the policy applies.
- `class-default`—Specifies that the policy applies to the default traffic class.

**Note:**

This step associates the traffic class with the traffic policy.

### Step 5

**Command or Action:**

Example:

```
Switch(config-pmap-c)# police cir 5000000 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop
```

**Purpose:**

Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm:

- `cir`—Indicates that the committed information rate (CIR) is used for policing traffic.
- `rate`—Indicates that the police rate is used for policing traffic.
- `bps value`—Average rate in bits per second. The valid values range from 8000 to 1000000000.
- `bc`—Indicates that the committed (conform) burst size is used for policing traffic.
- `be`—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000.
- `peak-burst`—Indicates that the peak-burst size is used for policing traffic.
- `be`—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• action—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 4: Policing Actions, on page 62.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>The police [cir</td>
</tr>
</tbody>
</table>

**Step 6**

| end               | Exits policy-map configuration mode and returns to privileged EXEC mode. |

Example:

Switch(config-pmap)# end

The table below provides the traffic policy commands supported at the Ingress:
### Table 8: Traffic Policy Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`police [cir</td>
<td>rate] bps-value [bc</td>
</tr>
<tr>
<td></td>
<td>• <strong>cir</strong>—Indicates that the committed information rate (CIR) is used for policing traffic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>rate</strong>—Indicates that the police rate is used for policing traffic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bps value</strong>—Average rate in bits per second. The valid values range from 8000 to 10000000000.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bc</strong>—Indicates that the committed (conform) burst size is used for policing traffic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>burst</strong>—Indicates that the burst size is used for policing traffic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bc</strong>—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000.</td>
</tr>
<tr>
<td></td>
<td>• <strong>be</strong>—Indicates that the excess burst size is used for policing traffic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>peak-burst</strong>—Indicates that the peak-burst size is used for policing traffic.</td>
</tr>
<tr>
<td></td>
<td>• <strong>be</strong>—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000.</td>
</tr>
<tr>
<td></td>
<td>• <strong>action</strong>—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 4: Policing Actions, on page 62.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config-pmap-c)# police cir 5000000 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`police [cir</td>
<td>rate] percent % [bc</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)# police cir percent 10 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit 25 violate-action drop</code></td>
<td></td>
</tr>
</tbody>
</table>

- **cir**—Indicates that the committed information rate (CIR) is used for policing traffic.
- **rate**—Indicates that the police rate is used for policing traffic.
- **percent**—Indicates that a percentage of bandwidth is used for calculating CIR or rate.
- **%**—CIR or rate bandwidth percentage. The valid values range from 1 to 100.
- **bc**—Indicates that the committed (conform) burst size is used for policing traffic.
- **burst**—Indicates that the burst size is used for policing traffic.
- **bc**—Committed (conform) burst size or burst size in mill-seconds or micro-seconds.
- **be**—Indicates that the excess burst size is used for policing traffic.
- **peak-burst**—Indicates that the peak-burst size is used for policing traffic.
- **be**—Excess burst size or peak-burst size in mill-seconds or micro-seconds.
- **action**—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 4: Policing Actions, on page 62.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>police [circuit] rate bps-value [burst] bc [peak-rate] pir [peak-burst] be conform-action action exceed-action action violate-action action</td>
<td>Configures traffic policing using two rates (CIR and PIR) where: <strong>circuit</strong>—Indicates that the committed information rate (CIR) is used for policing traffic. <strong>rate</strong>—Indicates that the peak rate is used for policing traffic. <strong>bps value</strong>—Average rate in bits per second. The valid values range from 8000 to 1000000000. <strong>bc</strong>—Indicates that the committed (conform) burst size is used for policing traffic. <strong>burst</strong>—Indicates that the burst size is used for policing traffic. <strong>bc</strong>—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. <strong>peak-rate</strong>—Indicates that the peak information rate (PIR) is used for policing traffic. <strong>peak-rate</strong>—Peak information rate or peak rate in bits per second. The valid values range from 8000 to 1000000000. <strong>be</strong>—Indicates that the excess burst size is used for policing traffic. <strong>peak-burst</strong>—Indicates that the peak-burst size is used for policing traffic. <strong>be</strong>—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. <strong>action</strong>—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 4: Policing Actions, on page 62.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config-pmap-c)# police cir 500000000 bc 200000 pir 51000000 be 400000 conform-action transmit exceed-action action set-dscp-transmit 50 violate-action action drop
```

**Attaching or Removing a Traffic Policy from the Target**

Before a traffic policy can be enabled for a class of traffic, it must be configured on a target. Use the `service-policy {input | output}` configuration command to attach a traffic policy to a target and to specify...
the direction in which the policy should be applied (either on packets entering/ingressing the target or packets exiting/egressing the target). Only one traffic policy can be applied to an interface in a given direction. Use the no form of the command, that is, no service-policy {input | output} policy-map-name to detach a traffic policy from a target.

**Before You Begin**

Complete any one of the following tasks:

- Configuring Ingress Policing, on page 73
- Configuring Ingress Marking, on page 80
- Configuring Passwords on Cisco ME 2600X, on page 5
- Configuring the Cisco ME 2600X Host Name, on page 5
- Configuring Egress Shaping, on page 90
- Configuring Egress Bandwidth, on page 88
- Configuring Egress LLQ, on page 86
- Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent, on page 92

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. service instance id ethernet
5. service-policy {input | output} policy-map-name
6. no service-policy {input | output} policy-map-name
7. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>interface type slot/port</td>
<td>Configures an interface type and enters the interface configuration</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>mode.</td>
</tr>
<tr>
<td>Switch(config)# interface TenGigabitEthernet 0/45</td>
<td>* interface-type—Interface type</td>
</tr>
<tr>
<td></td>
<td>* interface-number—Interface number.</td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

**Step 4**

`service instance id ethernet`

**Example:**

```plaintext
Switch(config-if)# service instance 100 ethernet
```

- **Purpose:** Enters the service instance mode.
  - `id`—Service instance ID.

**Step 5**

`service-policy {input | output} policy-map-name`

**Example:**

```plaintext
Switch(config-if-srv-instance)# service-policy input policy1
```

- **Purpose:** Attaches a policy map to a target.
  - Enter either the input or output keyword and the policy map name.
  - `policy-map-name`—Name of the policy map.

**Step 6**

`no service-policy {input | output} policy-map-name`

**Example:**

```plaintext
Switch(config-if-srv-instance)# no service-policy input policy1
```

- **Purpose:** Removes the policy map from the target.
  - Enter either the input or output keyword and the policy map name.

**Step 7**

`end`

**Example:**

```plaintext
Switch(config-if-srv-instance)# end
```

- **Purpose:** Exits the service instance mode.

---

### Configuring Ingress Marking

**Before You Begin**

Complete the following task:

Configuring Ingress Policing, on page 73

---

**Note**

Marking of the Layer 2 CoS bit for VPWS traffic is not supported.

---

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `policy-map policy-map-name`
4. `class {class-name | class-default}`
5. `set ip precedence ip precedence value`
6. `end`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| **Example:** Switch> enable | |
| **Step 2** configure terminal | Enters global configuration mode.  
  * commands starts the policy-map configuration mode.  
  * policy-map-name—Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters. |
| **Example:** Switch# configure terminal | |
| **Step 3** policy-map policy-map-name | Creates or specifies the name of the traffic policy and enters the policy-map configuration mode. |
| **Example:** Switch(config)# policy-map policy1 | |
| **Step 4** class {class-name | class-default} | Specifies the name of a traffic class to which the policy applies and enters the policy-map class configuration mode.  
  * Enter the previously configured class-map name.  
  * class-name—User-defined class name to which the policy applies.  
  * class-default—Specifies that the policy applies to the default traffic class. |
| **Example:** Switch(config-pmap)# class class1 | |
| **Note** This step associates the traffic class with the traffic policy. | |
| **Step 5** set ip precedence ip precedence value | Marks the precedence value in the IP header with a value between 0 to 7.  
  * ip precedence value—IP precedence value. |
| **Example:** Switch(config-pmap-c)# set ip precedence 2 | |
| **Note** The set ip precedence command is just an example of one of the marking commands that can be used. For a list of other marking commands, see Table 9: Traffic Marking Commands, on page 82. | |
| **Step 6** end | Exits policy-map configuration mode and returns to privileged EXEC mode. |
| **Example:** Switch(config-pmap)# end | |

The table below provides the traffic marking commands supported at Ingress.
Table 9: Traffic Marking Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set ip precedence ip-precedence-value</td>
<td>Marks the precedence value in the IP header with a value between 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• ip precedence value—IP precedence value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# set ip precedence 2</td>
</tr>
<tr>
<td>set cos cos-value</td>
<td>Marks the CoS value between 0 to 7 in an 802.1Q tagged frame</td>
</tr>
<tr>
<td></td>
<td>• cos-value—CoS value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# set cos 2</td>
</tr>
<tr>
<td>set ip dscp ip-dscp-value</td>
<td>Marks the IP DSCP in the ToS byte with a value between 0 to 63.</td>
</tr>
<tr>
<td></td>
<td>• ip-dscp-value—IP DSCP value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# set ip dscp 22</td>
</tr>
<tr>
<td>set qos group qos-group-value</td>
<td>Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets.</td>
</tr>
<tr>
<td></td>
<td>• qos-group-value—QoS group value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# set qos group 3</td>
</tr>
</tbody>
</table>

Configuring Ingress Re-Marking

To configure ingress re-marking on the device, complete the following steps:

**Before You Begin**

Complete the following task:

Configuring Ingress Policing, on page 73

---

**Note**

You cannot apply remarking for precedence and DSCP together.
SUMMARY STEPS

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class {class-name | class-default}
5. set ip precedence ip precedence value
6. police cir percent value
7. Confirm-action set-cos-transmit value
8. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enters your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy-map policy-map-name</td>
<td>Creates or specifies the name of the traffic policy and enters the policy-map configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# policy-map policy1</td>
<td>• policy-map-name— Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong> class {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td>Example: Switch(config-pmap)# class class1</td>
<td>• Enter the previously configured class-map name.</td>
</tr>
<tr>
<td></td>
<td>* class-name—User-defined class name to which the policy applies.</td>
</tr>
<tr>
<td></td>
<td>* class-default—Specifies that the policy applies to the default traffic class.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This step associates the traffic class with the traffic policy.</td>
</tr>
<tr>
<td><strong>Step 5</strong> set ip precedence ip precedence value</td>
<td>Marks the precedence value in the IP header with a value between 0 to 7.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# set ip precedence 2</td>
<td>• ip precedence value— IP precedence value.</td>
</tr>
</tbody>
</table>
The set ip precedence command is just an example of one of the marking commands that can be used. For a list of other marking commands, see Table 9: Traffic Marking Commands, on page 82.

### Step 6

**Police cir percent value**

**Example:**

```
Switch(config-pmap-c)# police cir percent 2
```

```
Switch(config-pmap-c)# police 100m
```

### Step 7

**Confirm-action set-cos-transmit value**

**Example:**

```
Switch(config-pmap-c-police)# Confirm-action set-cos-transmit 4
```

### Step 8

**End**

**Example:**

```
Switch(config-pmap)# end
```

The table below provides the traffic marking commands supported at Ingress:

**Table 10: Traffic Marking Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set-prec-transmit ip-precedence-value</td>
<td>Marks the precedence value in the IP header with a value between 0 to 7.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)# set-prec-transmit 2</td>
<td>• <em>ip precedence value</em>—IP precedence value.</td>
</tr>
<tr>
<td>set-cos-transmit cos-value</td>
<td>Marks the CoS value between 0 to 7 in an 802.1Q tagged frame</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)# set-cos-transmit 2</td>
<td>• <em>cos-value</em>—CoS value.</td>
</tr>
<tr>
<td>set-dscp-transmit ip-dscp-value</td>
<td>Marks the IP DSCP in the ToS byte with a value between 0 to 63.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)# set-dscp-transmit 22</td>
<td>• <em>ip-dscp-value</em>—IP DSCP value.</td>
</tr>
</tbody>
</table>
### Configuring Egress Classification

To configure egress classification on the device, complete the following steps:

#### Before You Begin

- Only one match filter is supported for each class-map.
- Only QoS-group based matching is supported for user-defined classes.
- Match based on QoS-group 3 and QoS-group 7 is used only for low latency queuing across the system.
- Match based on the class-default in the output policy suggests that matching is based on the QoS-group 0 and not the class where traffic, which does not match any selection criteria in the configured class maps, is directed.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `class-map [match-any] class-map-name`
4. `match qos-group qos-group-number`
5. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>class-map [match-any] class-map-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# class-map match-any class1</td>
</tr>
</tbody>
</table>

**Purpose:**
Creates a class to be used with a class map and enters the class-map configuration mode. The class map is used for matching packets to the specified class.

- *class-map-name*—Class name. This is the name of the class map and can have a maximum of 40 alphanumeric characters.

The **match-any** keyword specifies that one of the match criteria must be met. Use this keyword only if you have to specify more than one match command.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>match qos-group qos-group-number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match qos-group 2</td>
</tr>
</tbody>
</table>

**Purpose:**
Matches a packet on the basis of traffic class represented by the qos-group.

- *qos-group-number*—QoS-group value. The value can range from 0 to 7.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# end</td>
</tr>
</tbody>
</table>

**Purpose:**
Exits class-map configuration mode and returns to privileged EXEC mode.

### Configuring Egress LLQ

To configure egress LLQ on the device, complete the following steps:

**Before You Begin**

Complete step 1 to step 5 of Configuring Ingress Policing, on page 73

**Note**

- The **priority** command enables the rate-limit option to ensure that a particular rate is not exceeded. However, in the Cisco ME 2600X system, egress rate limiting is achieved using shapers that can cause additional delays. Therefore, it is advised to ensure that for LLQ traffic, rate limiting is done at ingress, and the rates specified at egress are just placeholders that are never exceeded. Exceeding the rate limit at egress would mean increased latencies for LLQ traffic.

- The **priority** command is supported only under class-map with qos-group 3 or 7 as the match criteria and multicast-priority class.
SUMMARY STEPS

1. enable
2. configure terminal
3. policy map policy-map-name
4. class {class-name | class-default}
5. priority bandwidth value
6. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy map policy-map-name</td>
<td>Creates or modifies a traffic policy and enters the policy-map configuration mode. The policy-map-name specifies the name of the traffic policy, which can have a maximum of 40 alphanumeric characters.</td>
</tr>
<tr>
<td>Example: Switch(config)# policy-map policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> class {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td>Example: Switch(config-pmap)# class class_qos_1</td>
<td>• class-name—Name of a predefined class included in the service policy.</td>
</tr>
<tr>
<td></td>
<td>• class-default—Specifies that the policy applies to the default traffic class.</td>
</tr>
<tr>
<td><strong>Step 5</strong> priority bandwidth value</td>
<td>Provides strict priority to a class of traffic belonging to the policy-map. Specifies the maximum bandwidth usage by a traffic class through the use of a token bucket algorithm. The bandwidth value is in kbps, and can range from 1 to 10000000.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# priority 10000</td>
<td>The priority bandwidth value command is just an example of one of the priority commands that can be used. For a list of other priority commands, see Table 11: Priority (LLQ) Commands, on page 88.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# end</td>
<td></td>
</tr>
</tbody>
</table>
The table below lists the priority commands:

**Table 11: Priority (LLO) Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>priority bandwidth value</code></td>
<td>Provides strict priority to a class of traffic belonging to the policy-map. Specifies the maximum bandwidth usage by a traffic class through the use of a token bucket algorithm. The <em>bandwidth value</em> is in kbps, and can range from 1 to 1000000.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-pmap-c)# priority 10000</code></td>
<td></td>
</tr>
<tr>
<td><code>priority</code></td>
<td>This command provides low-latency queuing without specifying the rate limiter.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-pmap-c)# priority</code></td>
<td></td>
</tr>
<tr>
<td><code>priority percent x%</code></td>
<td>Indicates that the rate of traffic that is given low latency handling is <em>x%</em> of the parent interface bandwidth or <em>x%</em> parent class CIR if policy not applied on an interface. The percentage can be a number from 1 to 100.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-pmap-c)# priority 10%</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Egress Bandwidth**

To configure egress bandwidth on the device, complete the following steps:

**Before You Begin**

Complete step 1 to step 5 of *Configuring Ingress Policing*, on page 73

**Note**

- Bandwidth action is not supported on classes with qos-group 3 or 7 as the match criteria.
- The `bandwidth` command cannot be used in combination with BRR or BRP in a class-map or a policy-map.
- The system does not validate the total CIR configured on all the targets for various congestion points. Therefore, it should be ensured that the total CIR configured does not exceed the total bandwidth available.
  - Total CIR configured for a 1 Gbps interface should not exceed 1 Gbps, which includes CIR in the policy applied on the interface and services on that interface.
  - Total CIR configured for a 10 Gbps interface should not exceed 10 Gbps, which includes CIR in the policy applied on the interface and services on that interface.
  - Total CIR for all the targets on a Cisco ME 2600X shelf should not exceed 9.882 Gbps; this is the least bandwidth for a Cisco ME 2600X shelf in a scenario where only one of the interconnects for a Cisco ME 2600X shelf is functional.
SUMMARY STEPS

1. enable
2. configure terminal
3. policy map policy-map-name
4. class {class-name | class-default}
5. bandwidth bandwidth value
6. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy map policy-map-name</td>
<td>Creates or modifies a traffic policy and enters the policy-map configuration mode. The policy-map-name specifies the name of the traffic policy that can have a maximum of 40 alphanumeric characters.</td>
</tr>
<tr>
<td>Example: Switch(config)# policy-map policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> class {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td>Example: Switch(config)# class c3</td>
<td>- class-name—User-defined class name to which the policy applies.</td>
</tr>
<tr>
<td></td>
<td>- class-default—Specifies that the policy applies to the default traffic class.</td>
</tr>
<tr>
<td><strong>Step 5</strong> bandwidth bandwidth value</td>
<td>Specifies the amount of bandwidth in kbps to be assigned to the class. Implies that the class where this is applied is given a minimum bandwidth guarantee of bandwidth value in kbps. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overheads.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# bandwidth 10000</td>
<td>Note: The bandwidth bandwidth value command is just an example of one of the bandwidth commands that can be used. For a list of other bandwidth commands, see Table 12: Bandwidth Commands, on page 90.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# end</td>
<td></td>
</tr>
</tbody>
</table>
The table below lists the bandwidth commands:

**Table 12: Bandwidth Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bandwidth</code> bandwidth-value</td>
<td>Specifies the amount of bandwidth in kbps to be assigned to the class. Implies that the class where this is applied is given a minimum bandwidth guarantee of <code>bandwidth-value</code> kbps. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# bandwidth 10000</td>
<td></td>
</tr>
<tr>
<td><code>bandwidth percent</code> %</td>
<td>Specifies the amount of bandwidth, in percentage from the available bandwidth, to be assigned to the class. The value ranges from 1 to 100.</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# bandwidth percent 20</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Egress Shaping**

To configure shaping at the egress on the device, complete the following steps:

**Before You Begin**

Complete step 1 to step 5 of *Configuring Ingress Policing*, on page 73.

**Note**

- The **shaping** command is not supported on classes with qos-group 3 or 7 as the match criteria.
- Shape on a traffic class would mean buffering of traffic in the system memory, which could result in increased latencies for these streams.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `class-map [match-any] class-map-name`
4. `policy map policy-map-name`
5. `class class-name`
6. `shape average cir value`
7. `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><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>

### Step 2

configure terminal

**Example:**

Switch# configure terminal

Enters global configuration mode.

### Step 3

class-map [match-any] class-map-name

**Example:**

Switch(config)# class-map class-interface-all

Creates a class map to be used for matching packets to a class.

### Step 4

policy map policy-map-name

**Example:**

Switch(config)# policy-map test2

policy-map-name—Name of the policy-map to configure.

### Step 5

class class-name

**Example:**

Switch(config-pmap)# class classtest

class-name—Name of a predefined class included in the service policy.

### Step 6

shape average cir value

**Example:**

Switch(config-pmap-c)# shape average 10000000

cir value—Average rate traffic shaping. The committed information rate (CIR) value ranges from 8000 to 1000000000 bps.

**Note** The **shape average cir value** command is just an example of one of the shape commands that can be used. For a list of other shape commands, see Table 13: Traffic Shaping Commands, on page 91.

### Step 7

end

**Example:**

Switch(config-pmap-c)# end

Exits the configuration mode and returns to privileged EXEC mode.

---

**Table 13: Traffic Shaping Commands**, on page 91 provides the traffic shaping commands:

**Table 13: Traffic Shaping Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shape average percent %</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# shape average percent 20</td>
<td>Shapes a class to a percent of visible bandwidth.</td>
</tr>
</tbody>
</table>

- %—Percentage. The value should range from 1 to 100.
Command | Description
---|---
**shape average cir value**  
Example:  
Switch(config-pmap-c)# shape average 10000000 | Specifies the average rate traffic shaping.  
*cir value*—CIR value in bps. The committed information rate (CIR) value ranges from 8000 to 10000000000 bps.

Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent

BRR is implemented on logical interfaces using hierarchical policy-maps.  
To configure QoS egress BRR or BRP on the device, complete the following steps:

**Before You Begin**

Complete step 1 to step 5 of Configuring Ingress Policing, on page 73

**Note**

* The **BRR and BRP** commands are not supported in combination with the **bandwidth** action in a class-map or a policy-map.  
* The **BRR and BRP** command are not supported on classes with qos-group 3 or 7 as the match criteria.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. policy map *policy-map-name*  
4. class {class-name | class-default}  
5. bandwidth remaining ratio *ratio*  
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | Enables privileged EXEC mode.  
**Example:**  
Switch> enable |  
* Enter your password if prompted.  
|
### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

Enters global configuration mode.

#### Step 3

**Policy Map Creation**

- **policy map policy-map-name**
  - **Example:**
    - Switch(config)# policy-map policy1

Creates or modifies a traffic policy and enters the policy-map configuration mode. The `policy-map-name` specifies the name of the traffic policy, which can have a maximum of 40 alphanumeric characters.

#### Step 4

**Traffic Class Configuration**

- **class {class-name | class-default}**
  - **Example:**
    - Switch(config-pmap)# class c3

Specifies the name of the predefined traffic class to which this policy applies and enters the policy-map class configuration mode, where:

- **class-name** — User-defined class name to which the policy applies.
- **class-default** — Specifies that the policy applies to the default traffic class.

#### Step 5

**Bandwidth Remaining Ratio**

- **bandwidth remaining ratio ratio**
  - **Example:**
    - Switch(config-pmap-c)# bandwidth remaining ratio 2

Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues. The value should be between 1 to 127.

**Note**

The `bandwidth remaining percent x%` command can be used instead of the `bandwidth remaining ratio ratio` command to configure BRP. For details on bandwidth remaining percent command, see Table 14: Bandwidth Remaining Ratio and Bandwidth Remaining Percent Commands, on page 93.

#### Step 6

**End Command**

- **Example:**
  - Switch(config-pmap-c)# end

Exits the configuration mode and returns to privileged EXEC mode.

---

The table below provides the bandwidth remaining ratio or percent commands:

**Table 14: Bandwidth Remaining Ratio and Bandwidth Remaining Percent Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bandwidth remaining percent x%</strong></td>
<td>Specifies that the class where the command is specified should be given x% of the excess bandwidth, where excess bandwidth is the bandwidth in excess of all the minimum bandwidth guarantees of all the classes at the same level. The value should range from 1 to 100.</td>
</tr>
</tbody>
</table>

**Example:**

- Switch(config-pmap-c)# bandwidth remaining percent 20
Troubleshooting Tips

The commands listed in this section can be used to see the policies and class-maps that are configured and applied on the Cisco ME 2600X.

Use the following commands to display configured policies and class-maps:

- Show policy-map [policy-map-name]
- Show class-map [class-map-name]

Configuration Examples for QoS

Configuring Ingress Classification

The following example shows how to configure a class-map named ipp5, and enter a match statement for IP precedence 5:

Switch> enable
Switch# configure terminal
Switch(config)# class-map ipp5
Switch(config-cmap)# match ip precedence 5
Switch(config-cmap)# exit

The following example shows how to configure a class-map on multiple match statements:

Switch> enable
Switch# configure terminal
Switch(config)# class-map match-any IPP
Switch(config-cmap)# match ip precedence 3
Switch(config-cmap)# match ip precedence 4
Switch(config-cmap)# exit

The following example shows how to configure a class-map using match-all and match-any keywords:

Switch> enable
Switch# configure terminal
Switch(config)# class-map match-any class1
Switch(config-cmap)# match vlan 100 200 400-500
Switch(config-cmap)# match cos 1
Switch(config-cmap)# exit
Switch(config)# class-map match-any class2
Switch(config-cmap)# match vlan 1000 1100-1120
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

---

**Command** | **Description**
--- | ---
bandwidth remaining ratio _ratio_ | Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non priority queues. The value should be between 1 to 127.

**Example:**
Switch(config-pmap-c)# bandwidth remaining ratio 2
The match-all criteria with multiple VLANs and CoS marking gets translated to a combination of match criteria. Therefore matching is based on the following incoming packet:

VLAN 1000 AND COS 3
VLAN 1100-1200 AND COS 3

The match-any criteria gets translated to individual match criteria. Therefore matching is based on VLAN 100, VLAN 200, VLAN 400-500, or COS 1.

The following example shows how to configure a hierarchical ingress policy:

Switch> enable
Switch# configure terminal
Switch(config)# class-map match-any childOR
Switch(config-cmap)# match cos 5
Switch(config)# policy-map testchildOR
Switch(config-pmap)# class childOR
Switch(config-pmap-c)# police cir percent 10
Switch(config)# policy-map parentOR
Switch(config-pmap-c)# class class-default
Switch(config-pmap-c)# policy rate 500000
Switch(config-pmap-c)# service-policy testchildOR
Switch(config-pmap-c)# exit

**Configuring Ingress Policing**

The following example shows how to configure policing actions:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map ABC
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police 10000000 8000 8000
Switch(config-pmap-c-policy)# conform-action set-cos-transmit 2
Switch(config-pmap-c-policy)# exceed-action set-cos-transmit 1
Switch(config-pmap-c-policy)# end

The following example shows how to configure a single rate 2-color policer:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map 1r2c
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police 2000000
Switch(config-pmap-c-policy)# conform-action transmit
Switch(config-pmap-c-policy)# exceed-action drop
Switch(config-pmap-c-policy)# end

The following example shows how to configure a single rate, 2-color policer with percent:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map 1r2c_percent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police cir percent 20
Switch(config-pmap-c-policy)# conform-action set-cos-transmit 0
Switch(config-pmap-c-policy)# exceed-action drop
Switch(config-pmap-c-policy)# end

The following example shows how to configure a dual rate, 3-color policer:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map 2r3c
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police cir 2000000 pir 3000000
Switch(config-pmap-c-policy)# conform-action set-prec-transmit 3
Switch(config-pmap-c-police)# exceed-action set-prec-transmit 2
Switch(config-pmap-c-police)# violate-action set-prec-transmit 1
Switch(config-pmap-c-police)# end

The following example shows how to configure a dual rate, 3-color policer with percent:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map 2r3c_percent
Switch(config-pmap)# class class-default
Switch(config-pmap)# police cir percent 10 pir percent 20
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# xceed-action set-cos-transmit 0
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end

The following example shows how to configure a single rate, 2-color policer in class-default and a child policy:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map police5
Switch(config-pmap)# class test18
Switch(config-pmap-c-police)# service policy child-level
Switch(config-pmap-c-police)# police cir 64000 50
Switch(config-pmap-c-police)# end

The following example shows how to configure a dual rate, 3-color policer configuration in a class and policy-map:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map test
Switch(config-pmap)# class cos2
Switch(config-pmap-c-police)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1

The following example shows how to configure a dual rate, 3-color policer in class-default with a CIR of 64 Kbps, and PIR doubled the CIR rate, a conform action of transmit, and an exceed action mark dscp af 11:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map qos_test
Switch(config-pmap)# class class-default
Switch(config-pmap-c-police)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1

The following example shows how to configure a dual rate, 3-color policer in class-default:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map qos_test
Switch(config-pmap)# class class-default
Switch(config-pmap-c-police)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1

**Attaching or Removing a QoS Traffic Policy for a Target**

The following example shows how to attach a traffic policy to a target:

Switch> enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# service instance 100 ethernet
The following example shows how to remove a traffic policy from a target:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# service instance 100 ethernet
Switch(config-if-srv-instance)# no service-policy input policy1
Switch(config-if-srv-instance)# end
```

**Configuring Ingress Marking**

The following example shows the creation of a service policy called `policy1`. This service policy is associated to a previously defined classification policy through the use of the `class` command. This example assumes that a classification policy called `class1` was previously configured. This example configures marking to set the IP precedence value:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip precedence 1
```

The following example shows how to configure marking to set the CoS value:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# policy-map test
Switch(config-pmap)# class test
Switch(config-pmap-c)# set cos 1
```

**Configuring Egress Classification**

The following example shows how to create a class map:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# class-map c1
Switch(config-cmap)# match qos-group 1
```

The following example shows how to configure priority queue at the egress:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# policy-map Test1
Switch(config-pmap)# class test
Switch(config-pmap-c)# priority 10000
```

**Configuring Egress Bandwidth**

The following example shows how to configure minimum bandwidth guarantee at the egress:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# policy-map Test
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
```
Configuring Egress Shaping

The following example shows how to shape traffic on a main interface; traffic leaving interface gi36/1 is shaped at the rate of 10 Mb/s:

Switch> enable
Switch# configure terminal
Switch(config)# class-map class-interface-all
Switch(config-cmap)# match qos-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map dts-interface-all-action
Switch(config-pmap)# class class-interface-all
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config)# interface gi36/1
Switch(config-if)# service-policy output dts-interface-all-action

Configuring Egress Bandwidth Remaining Ratio

The following example shows how to configure bandwidth remaining ratio at the egress:

Switch> enable
Switch# configure terminal
Switch(config)# policy-map BRR
Switch(config-pmap)# class Test1
Switch(config-pmap-c)# bandwidth remaining ratio 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class Test2
Switch(config-pmap-c)# bandwidth remaining ratio 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class Test3
Switch(config-pmap-c)# bandwidth remaining ratio 30
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth remaining ratio 40

Verifying the QoS Configuration

Use the following `show` commands to verify the QoS configuration:

- `show class-map`
- `show class-map class-map-name`
- `show policy-map`
- `show policy-map policy-map-name`
- `show policy-map policy-map-name class class-name`
- `show run class-map`
- `show policy-map BRR`
- `show policy-map interface interface type slot/port`
- `show policy-map interface interface type slot/port service instance number`
**Class Map**

Use the following command to show class-map information for a specific class map:

```
Switch# show class-map ipp5
```

class Map match-any ipp5 (id 1)
macth ip precedence 5

Use the following command to show class-map information for a specific class map using the `show run class-map` command:

```
Switch# show run class-map
```

Building configuration...
Current configuration : 275 bytes
!
class-map match-any EgressClassmap
match qos-group 3
class-map match-any IngressClassMap
match cos 1
end

**Policy Map**

Use the following command to show policy map information:

```
Switch# show policy-map
```

policy-map testchildOR
class childOR
police 100000000
policy-map parentOR
class class-default
police 500000000
service-policy testchildOR

Use the following command to show information for a specific policy map:

```
Switch# show policy-map ABC
```

Policy Map ABC
class class-default
police cir 100000000 bc 8000 be 8000
conform-action set-cos-transmit 2
exceed-action set-cos-transmit 1

Use the following command to verify the bandwidth remaining ratio at the egress:

```
Switch# show policy-map BRR
```

Building configuration...
Current configuration : 209 bytes
!
policy-map BRR
class Test1
bandwidth remaining ratio 10
class Test2
bandwidth remaining ratio 20
class Test3
bandwidth remaining ratio 30
class class-default
bandwidth remaining ratio 40
!
end

Additional References for QoS

The following sections provide references related to the QoS feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Quality of Service Solutions Command Reference</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Resilient Ethernet Protocol

This chapter describes Resilient Ethernet Protocol (REP), REP configuration guidelines, VLAN load balancing, REP timers, and REP over EVC. This chapter also describes procedures to configure REP.

• Understanding Resilient Ethernet Protocol, page 101
• Understanding VLAN Load Balancing, page 113
• Understanding REP Configurable Timers, page 116
• Understanding REP with EVC, page 119
• REP with Multicast, page 127

Understanding Resilient Ethernet Protocol

The Resilient Ethernet Protocol (REP) is a protocol that provides an alternative to Spanning Tree Protocol (STP) to support layer 2 resiliency, and fast switchover with Ethernet networks. REP provides a way to control network loops, handle link failures, and improve convergence time.

REP performs the following tasks:

• Controls a group of ports connected in a segment.
• Ensures that the segment does not create any bridging loops.
• Handles single link failure within the segment.
• Improves convergence time.
• Supports VLAN load balancing.

Understanding REP Segments

A 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. The two edge ports terminate the segments.
A device cannot have 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 Layer 2 interfaces.

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 (that is, the segment on the left), a single port is blocked, shown by the diagonal line. When there is a failure in the network, the blocked port returns to the forwarding state to minimize network disruption.

**Figure 5: REP Open Segments**

The segment shown in Figure 5: REP Open Segments, on page 102 is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and it is safe to connect the segment edges to any network. The traffic from a REP ring node toward the network cloud is sent to either of the edge nodes, depending on the location of the alternate port. If a failure is detected anywhere in the ring, the alternate port changes to a open port forwarding all traffic. This may cause the traffic being redirected to the other edge node depending on the fault location. It ensures that data flow is maintained between a particular REP node and the network cloud. If a failure occurs on any segment or any port on a REP segment, REP unblocks all the ports to ensure that connectivity is available through the other edge.

The segment shown in the figure below, with both edge ports located on the same device, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two devices in the segment.

**Figure 6: REP Ring Segment**
Characteristics of REP Segments

REP segments have the following characteristics:

- If all the ports in the segment are operational, one port (referred to as the alternate port) blocks traffic for each VLAN. If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity. The Failed ports are blocked for all traffic, while all the other ports in the ring stay in open state.
- In case of a link failure, the alternate ports are immediately unblocked. When the failed link comes up, a logically blocked port per VLAN is selected with minimal disruption to the network. When VLAN load balancing preemption timer is set, VLAN load balancing is automatically applied after the last failure has recovered. There are 2 alternate ports when VLAN load balancing takes effect.
- Changing the normal REP port configuration to preferred REP port with auto preemption delay configuration requires manual preemption for the first time. Subsequently when a failure occurs, auto preemption takes effect after link recovery and the port becomes the secondary port.

Understanding Link Adjacency

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. When enabled on an interface, the REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. 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. When a segment port starts, the LSL layer sends 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 under the following conditions:

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

Each port creates an adjacency with its immediate neighbor. When the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked.

Understanding Fast Convergence

A failure in a REP segment is noticed and propagated across the ring by LSL and HFL messages. LSL messages are sent hop by hop on the control plane, with each node receiving, processing, and forwarding LSL messages. This process is time-consuming.

HFL messages are flooded in the data plane across the ring on a preconfigured administrative VLAN, using a fixed multicast address. This results in each node receiving failure notifications instantaneously. Using HFL, traffic reconvergence is achieved fast, leading to insignificant loss of traffic on segment failure.
HFL messages are handled as data packets on the nodes in a ring which do not have the REP configured. The administrative VLAN is common to all the REP segments that are configured on a node. Convergence time varies depending on the type and number of nodes that are present on the ring.

**REP Edge No-Neighbor**

You can configure the non-REP switch facing ports as edge no-neighbor ports. These ports inherit the properties of edge ports, and overcome the limitation of not being able to converge quickly during a failure. You can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports as shown in the figure below. These ports inherit all the properties of edge ports. You can configure these no-neighbor ports as any other edge port and also enable the ports to send REP topology change notifications to the aggregation switch.

*Figure 7: Edge No-Neighbor Ports*

---

**Understanding REP Ports**

Ports in REP segments take one of three roles or states—Failed, Open, or Alternate.

- A port configured as a regular segment port starts as a failed port.
- When the neighbor adjacencies are determined, the port transitions to the 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 VLANs.

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.
REP Actions on Packets

REP performs specific actions depending on the type of packets. The following actions are taken by REP on packets that originate from an alternate port.

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Block/Allow (TX)</th>
<th>Action (TX)</th>
<th>Block/Allow (RX)</th>
<th>Action (RX)</th>
</tr>
</thead>
<tbody>
<tr>
<td>REP LSL packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>Punt to CPU</td>
</tr>
<tr>
<td>REP HFL packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>Punt to CPU; no forward</td>
</tr>
<tr>
<td>Tagged control packet</td>
<td>Block if VLAN is blocked on the port</td>
<td>—</td>
<td>Block if VLAN is blocked on the port</td>
<td>As per the configured protocol and EVC, if VLAN is not blocked.</td>
</tr>
<tr>
<td>Untagged control packet</td>
<td>Block</td>
<td>—</td>
<td>Block</td>
<td>—</td>
</tr>
<tr>
<td>Tagged data packet</td>
<td>Block if VLAN is blocked on the port</td>
<td>—</td>
<td>Block if VLAN is blocked on the port</td>
<td>As per EVC, if VLAN is not blocked.</td>
</tr>
<tr>
<td>Untagged data packet</td>
<td>Block</td>
<td>—</td>
<td>Block</td>
<td>—</td>
</tr>
</tbody>
</table>

REP blocks untagged packets on a port only when VLAN load balancing is not in effect. When VLAN load balancing takes effect, all the untagged packets flow across an alternate port. The following actions are taken by REP on packets that originate from an open port (a port that is not blocked by REP).

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Block/Allow (TX)</th>
<th>Action (TX)</th>
<th>Block/Allow (RX)</th>
<th>Action (RX)</th>
</tr>
</thead>
<tbody>
<tr>
<td>REP LSL packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>Punt to CPU</td>
</tr>
<tr>
<td>REP HFL packet</td>
<td>Allow only packets that originate from the node</td>
<td>—</td>
<td>Allow</td>
<td>Punt to CPU and forward as per EVC</td>
</tr>
<tr>
<td>Tagged control packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>As per the configured protocol and EVC</td>
</tr>
<tr>
<td>Untagged control packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>As per the configured protocol and EVC</td>
</tr>
<tr>
<td>Tagged data packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>As per EVC</td>
</tr>
<tr>
<td>Untagged data packet</td>
<td>Allow</td>
<td>—</td>
<td>Allow</td>
<td>As per EVC</td>
</tr>
</tbody>
</table>
Default REP Configuration

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

When REP is enabled, the sending of segment topology change notifications (STCNs) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1. When REP administrative VLAN or STCN configuration is changed, the changed configuration applies to ports.

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 action after manual preemption is to block all the VLANs at the elected alternate port.

REP Configuration Guidelines

Follow these guidelines when configuring REP:

• REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port.

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

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

• If REP is enabled on two ports on a device, both ports must be either regular segment ports or edge ports. REP ports follow these rules:
  • If only one port on a device is configured in a segment, the port should be an edge port.
  • If two ports on a device belong to the same segment, both ports must be regular segment ports.
  • If two ports on a device 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 do not forward traffic till they change to open ports through exchange of LSL HELLO messages with neighbors. You need to be aware of this to avoid sudden connection losses.

• REP configuration parameters for a port must not be changed without shutting down the port. However, the VLAN range for VLAN load balancing on primary edge port can be changed without this restriction.

• When configuring VLAN load balancing, the port selected for load balancing and the primary edge port must be on different nodes. Otherwise, it may cause HFL packets to flood, when VLAN Load Balancing is activated.

• When configuring STCN, ensure that STCN propagates across the REP segments in one direction. When STCN is sent from a segment, the STCN packet must not reach the original segment. Otherwise, it may cause an infinite loop of STCN packets flowing across the segments.

• REP is not supported on service instances configured with encapsulation, untagged, or default type.

• To avoid traffic drop after configuration change for REP Edge-NN segment, do one of the following:
  • Manually clear MAC on all the nodes.
• Shut/no-shut the REP port.

**REP Configuration Sequence**

You must perform the following tasks in this sequence to configure REP:

- Configure the REP administrative VLAN. The range of the REP admin VLAN is from 2 to 4094. The default VLAN 1 is always configured for HFL packets. However, EVC configuration must be explicitly done for VLAN 1, or any other VLAN that is selected as an administrative VLAN. See Configuring REP Administrative VLAN, on page 108.

- Enable REP on ports and assign a segment ID to it. REP is disabled on all ports by default. The range of the segment ID is from 1 to 1024. See Enabling REP on a Port, on page 109.

- Configure two edge ports in the segment; one port as the primary edge port and the other as the secondary edge port. See Enabling REP on a Port, on page 109.

If you configure two ports in a segment as the primary edge port, for example, ports on different switches, REP selects one of the ports to serve as the primary edge port based on port priority. The Primary option is enabled only on edge ports.

- Configure the primary edge port to send STCNs and VLAN load balancing to another port or to other segments. STCNs and VLAN load balancing configurations are enabled only for edge ports. See Configuring STCN on the Primary Edge Port, on page 111 and Configuring VLAN Load Balancing on the Primary Edge Port, on page 114.

**Understanding REP Administrative VLAN**

To avoid the delay introduced by relaying messages related to link-failure or VLAN-blocking notification during VLAN load balancing, REP floods packets at the HFL to a regular multicast address. HFL packets are used for fast transmission of failure notification across a REP ring by flooding a BPA on a VLAN. These messages are flooded to the whole network, not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default VLAN is VLAN 1. The default VLAN 1 is always configured.

- There can be only one administrative VLAN on a device and on a segment.

The administrative VLAN is configured at the system level. Whenever the administrative VLAN is changed, the corresponding EFP must also be manually configured to match the outer encapsulation for tagged control packets. The EFP must be associated with a bridge domain used exclusively for administrative VLAN EFPs. The VLAN marked as administrative VLAN must not be used for any other service or data traffic.

**REP Configuration Procedures**

To configure REP, complete the following procedures:

- Configuring REP Administrative VLAN, on page 108
Configuring REP Administrative VLAN

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `rep admin vlan vlan-id`
4. `end`
5. `show interface [interface-id] rep detail`

**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.</td>
</tr>
<tr>
<td><em>Example:</em> Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> rep admin vlan vlan-id</td>
<td>Configures an REP administrative VLAN. The range of the REP administrative VLAN is from 2 to 4094. The default value is VLAN 1.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# rep admin vlan 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring REP

Perform any of the following procedures as needed:

- **Enabling REP on a Port**, on page 109
- **Configuring STCN on the Primary Edge Port**, on page 111
- **Configuring Preemption Delay on the Primary Edge Port**, on page 112

### Enabling REP on a Port

**Prerequisite**

Configuring REP Administrative VLAN, on page 108

**Note**

REP can be enabled on Ten Gigabit Ethernet (10 GE) and one Gigabit Ethernet (1 GE) interface.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `rep segment segment-id [edge [no-neighbor] [primary]] [preferred]`
5. `end`
6. `show interface [interface-id] rep detail`

### Example: Configure REP Administrative VLAN

The following example shows how to configure the administrative VLAN as VLAN 100.

```
Switch> enable
Switch# configure terminal
Switch(config)# rep admin vlan 100
Switch(config)# end
```
## Enabling REP on a Port

### DETAILED STEPS

<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>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface TenGigabitEthernet 0/45</td>
</tr>
<tr>
<td></td>
<td>Specifies the interface and enters the interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# rep segment 1 edge preferred</td>
</tr>
<tr>
<td></td>
<td>Enables REP on the interface, and identifies a segment number. The segment ID range value is from 1 to 1024.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You must configure a primary and secondary edge port on each segment.</td>
</tr>
<tr>
<td></td>
<td>The following optional keywords are available.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>edge</strong> to configure the port as an edge port. Each segment has only two edge ports.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>no-neighbor</strong> to specify that the edge port must not have a neighbor port.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>primary</strong> to configure the port as the primary edge port where you can configure VLAN load balancing.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>preferred</strong> to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Configuring a port as <strong>preferred</strong> does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show interface [interface-id] rep detail</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show interface TenGigabitEthernet 0/45 rep detail</td>
</tr>
<tr>
<td></td>
<td>Displays the REP interface configuration.</td>
</tr>
</tbody>
</table>
Configuring STCN on the Primary Edge Port

Prerequisite
Enabling REP on a Port, on page 109

Note
Perform this procedure only on edge ports and not on regular segment ports.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. rep stcn {interface interface-id | segment segment-id-list}
5. end

DETAILED STEPS

<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>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface TenGigabitEthernet 0/45</td>
</tr>
<tr>
<td></td>
<td>Specifies the interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>rep stcn {interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# rep stcn segment 2-5</td>
</tr>
<tr>
<td></td>
<td>Configures the edge port to send STCNs to one or more segments or to an interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring Preemption Delay on the Primary Edge Port

Prerequisite
Enabling REP on a Port, on page 109

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. rep preempt delay value
5. end

DETAILED STEPS

<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>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface TenGigabitEthernet 0/45</td>
</tr>
<tr>
<td></td>
<td>Specifies the interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>rep preempt delay value</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# rep preempt delay 60</td>
</tr>
<tr>
<td></td>
<td>Configures a preemption time delay. Use this command if you want VLAN load balancing to automatically trigger after a link failure and recovery. The time delay range is from 15 to 300 seconds. The default action is manual preemption with no time delay.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Example: Configuring a REP Interface

The following example shows how to configure an interface as the primary edge port for segment 1, to send STCNs to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery.

```
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# rep segment 1 edge primary
Switch(config-if)# rep stcn segment 2-5
Switch(config-if)# rep block port id 0009001818D68700 vlan all
Switch(config-if)# rep preempt delay 60
Switch(config-if)# end
```

The following example shows how to configure the VLAN blocking configuration shown in the figure below. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port and all other VLANs are blocked at the primary edge port E1 (TenGigabitEthernet 0/45).

```
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# rep segment 1 edge primary
Switch(config-if)# rep block port 4 vlan 100-200
Switch(config-if)# end
```

Figure 8: Example of VLAN Blocking

Understanding VLAN Load Balancing

REP supports VLAN load balancing, controlled by the primary edge port but occurring at any port in the segment.

You must configure two edge ports in the segment for VLAN load balancing. One edge port in the REP segment acts as the primary edge port; the other edge port as the secondary edge port.

The primary edge port always participates in VLAN load balancing in the segment. REP VLAN load balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port.
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 then sends out a message to alert all interfaces in the segment about the preemption. When the message is received by the secondary edge port, it is reflected into 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 VLANs. VLAN load balancing is initiated only by the primary edge port and 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.

Configuring VLAN Load Balancing

Perform any of the following procedures as needed:

- Configuring VLAN Load Balancing on the Primary Edge Port, on page 114
- Configuring the Preemption for VLAN Load Balancing, on page 115

Configuring VLAN Load Balancing on the Primary Edge Port

Prerequisite
Enabling REP on a Port, on page 109

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
5. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3**  
interface interface-id

**Example:**
Switch(config)# interface TenGigabitEthernet 0/45

Specifies the interface and enters the interface configuration mode.

**Step 4**  
rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}

**Example:**
Switch(config-if)# rep block port id 0009001818D68700 vlan all

Configures VLAN load balancing on the primary edge port, identifies the REP alternate port, and configures the VLANs to be blocked on the alternate port.

- **id port-id** — identifies the alternate port ID. The port ID is automatically generated for each port in the segment. The `show interface interface-id rep detail` command in privileged EXEC mode displays interface port IDs.
- **neighbor-offset** number — identifies 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. Entering -1 identifies 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.

**Step 5**  
end

**Example:**
Switch(config-if)# end

Returns to privileged EXEC mode.

---

### Configuring the Preemption for VLAN Load Balancing

**Prerequisite**  
Configuring VLAN Load Balancing on the Primary Edge Port, on page 114

Ensure that all the other segment configuration has been completed before setting preemption for VLAN load balancing. When you use the `rep preempt segment segment-id` command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

If you do not use the `rep preempt delay value` interface configuration command on the primary edge port to configure a preemption time delay, the default configuration is to manually trigger VLAN load balancing on the segment. Use the `show rep topology` privileged EXEC command to see which port in the segment is the primary edge port.

Complete the following steps on the device that has the segment with the primary edge port.
SUMMARY STEPS

1. enable
2. rep preempt segment segment-id
3. show rep topology

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>rep preempt segment segment-id</td>
<td>Manually triggers VLAN load balancing on the segment.</td>
</tr>
<tr>
<td>Example: Switch# rep preempt segment 1</td>
<td>Note Confirm the action before the command is executed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>show rep topology</td>
<td>Displays the REP topology information.</td>
</tr>
<tr>
<td>Example: Switch# show rep topology</td>
<td></td>
</tr>
</tbody>
</table>

Example: Configure the Preemption for VLAN Load Balancing

The following example shows how to set the preemption for VLAN load balancing on a REP segment using Cisco IOS commands.

Switch> enable
Switch# rep preempt segment 1

Understanding REP Configurable Timers

The REP Configurable Timer (REP Fast Hellos) feature provides a fast reconvergence in a ring topology with higher timer granularity and quicker failure detection on the remote side. This feature also supports improved convergence of REP segments having nodes with copper based SFPs, where the link detection time varies between 300 ms to 700 ms.

With the REP Link Status Layer (LSL) ageout timer configuration, the failure detection time can be configured between a range of 120 to 10000 ms, in multiples of 40 ms. The result of this configuration is that, even if the copper pull takes about 700 ms to notify the remote end about the failure, the REP configurable timers process will detect it much earlier and take subsequent action for the failure recovery within 200 ms.

The LSL retries and LSL ageout timer is related in terms of LSL hello packet transmission. The LSL hello packet interval is measured by lsl_age_timer/lsl_retries value. The LSL hello packet interval value must be at least 40 ms.
Restrictions for REP timers

- While configuring REP configurable timers, we recommend that you shut the port, configure REP and only then use the **no shut** command. This prevents the REP from flapping and generating large number of internal messages.

- If incompatible switches are neighbors, configure the correct LSL Age Out value first. In some scenarios, you might not get the expected convergence range.

- While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL ageout timer value.

Configuring REP Timers

Perform any of the following procedures as needed:

- Configuring REP Link Status Layer Retries, on page 117
- Configuring the REP Link Status Layer Ageout Timer, on page 118

Configuring REP Link Status Layer Retries

**Prerequisite**

Enabling REP on a Port, on page 109

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `rep lsl-retries count`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the REP Link Status Layer Ageout Timer

**Prerequisites**
- Enabling REP on a Port, on page 109
- Configuring REP Link Status Layer Retries, on page 117

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `rep isl-age-timer value`
5. `end`

### Command or Action | Purpose
--- | ---
**Step 3** | `interface interface-id`<br>**Example:**<br>Switch(config)# interface TenGigabitEthernet 0/45<br>Specifies the interface to configure and enters interface configuration mode.

**Step 4** | `rep isl-retries count`<br>**Example:**<br>Switch(config-if)# rep isl-retries 4<br>Configures the number of retries before the REP link is disabled. The range of retries is from 3 to 10. The default number of LSL retries is 5.

**Step 5** | `end`<br>**Example:**<br>Switch(config-if)# end<br>Returns to privileged EXEC mode.

---

**Example: Configure REP Link Status Layer Retries**

The following example shows how to configure REP LSL retries using Cisco IOS commands.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# rep segment 2 edge primary
Switch(config-if)# rep isl-retries 4
Switch(config-if)# end
```
## DETAILED STEPS

<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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>rep lsl-age-timer value</td>
<td>Configures REP link status layer ageout timer value. The range of \textit{lsl-age-timer} is between 120 ms and 10000 ms, in multiples of 40 ms. The default LSL ageout timer value is 5 seconds. The recommended LSL ageout timer value is 2 seconds.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# rep lsl-age-timer 2000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Example: Configure the REP LSL Ageout Timer

The following example shows how to configure REP LSL ageout timer value using Cisco IOS commands.

```
Switch# enable 
Switch# configure terminal 
Switch(config)# interface TenGigabitEthernet 0/45 
Switch(config-if)# rep segment 1 edge primary 
Switch(config-if)# rep lsl-age-timer 2000 
Switch(config-if)# end 
```

## Understanding REP with EVC

REP can be integrated with an Ethernet Virtual Circuit (EVC) port using the REP over EVC feature. This feature allows you to configure and manage ports at the service instance level. An EVC port can have multiple service instances. Each service instance corresponds to a unique Ethernet Flow Point (EFP).

This feature allows you to configure an EVC port to participate in a REP segment. REP can selectively block or forward data traffic on particular VLANs. For an EVC, the VLAN ID refers to the outer tag of the encapsulation that is configured on a service instance.
REP is supported on an EVC cross-connect and bridge domain service. REP is not supported for Ethernet Private Line and Ethernet Virtual Private Line services.

REP does not support protection or loop prevention on ring interfaces which have one of the following EFP configurations:

- encapsulation default
- encapsulation untagged

Though a REP ring will converge with such interfaces, traffic loop can happen depending on the EVC configuration.

Using the REP over EVC feature, you can:

- Control data traffic.
- Configure VLAN load balancing.

**Restrictions for REP over EVC**

- It is recommended that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.
- REP is not supported on LACP.
- To avoid misconfiguration, you must configure all the trunk ports in the segment with the same set of allowed VLANs.
- Because REP blocks all VLANs until another REP interface sends a message to unblock it, you might lose connectivity to the port. This happens if you enable REP in a telnet session that accesses the EVC port through the same interface.
- On a device if REP is enabled on two ports for a segment, both ports must either be a regular segment ports or edge ports. REP ports follow these rules on a device:
  - If only one port is configured in a segment, the port should be an edge port.
  - If two ports belong to the same segment, both ports must be edge ports or the regular segment ports.
  - If two ports belong to the same segment and one is configured as an edge port and other as a regular segment port, the edge port is treated as a regular segment port.
  - There can be only two edge ports in a segment; if there are two edge devices in a segment, each device can have only one edge port. All the other ports on the edge device function as normal ports.
- REP interfaces come up in a blocked state and remains in a blocked state until notified that it is safe to unblock.
- REP relays all LSL Protocol Data Units (PDUs) in untagged frames and only HFL packets are relayed on the administrative VLAN.
- REP is not supported on EtherChannels. It is supported on EVC port-channels. REP is implemented on port-channels instead of its individual member links.
• In case of double VLAN tagged frame, REP is implemented only on the outer VLAN tag.

• When an edge no-neighbor is configured on a device, configuring and unconfiguring an edge port is not allowed.

## Configuring REP over EVC

Perform any of the following procedures as needed:

- Configuring REP over EVC Using a Cross–Connect, on page 121
- Configuring REP over EVC Using the Bridge Domain, on page 123

### Configuring REP over EVC Using a Cross–Connect

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `service instance id ethernet [evc-id]`
5. `encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]} second-dot1q {any | vlan-id [vlan-id [-vlan-id]]}`
6. `rewrite ingress tag {push | dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | pop {1 | 2} | translate {1-to-1 | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | 2-to-1 | dot1q vlan-id | dot1ad vlan-id | 2-to-2 | dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} [symmetric]`
7. `rep segment segment-id [edge [no-neighbor] [primary]] [preferred]`
8. `exit`

#### 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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface to configure and enters the interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>4</td>
<td><code>service instance id ethernet [evc-id]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if)# <code>service instance 101 ethernet</code></td>
</tr>
<tr>
<td>5</td>
<td>`encapsulation dot1q {any</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if-srv)# <code>encapsulation dot1q 100 second-dot1q 200</code></td>
</tr>
<tr>
<td>6</td>
<td>`rewrite ingress tag {push {dot1q vlan-id</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if-srv)# <code>rewrite ingress tag dot1q single symmetric</code></td>
</tr>
<tr>
<td>7</td>
<td><code>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if)# <code>rep segment 3 edge</code></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>4</td>
<td><code>service instance id ethernet [evc-id]</code></td>
<td>Configures an Ethernet service instance on an interface and enters the service instance configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if)# <code>service instance 101 ethernet</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>`encapsulation dot1q {any</td>
<td>vlan-id [vlan-id [-vlan-id]]} second-dot1q {any</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if-srv)# <code>encapsulation dot1q 100 second-dot1q 200</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`rewrite ingress tag {push {dot1q vlan-id</td>
<td>dot1q vlan-id second-dot1q vlan-id</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if-srv)# <code>rewrite ingress tag dot1q single symmetric</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</code></td>
<td>Configures REP over EVC. The segment ID range is from 1 to 1024. <strong>Note</strong> You must configure a primary and secondary edge port on each segment. The following optional keywords are available.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if)# <code>rep segment 3 edge</code></td>
<td>Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.</td>
</tr>
</tbody>
</table>
### Configuring REP over EVC Using the Bridge Domain

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `service instance id ethernet [evc-id]`
5. `encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]} second-dot1q {any | vlan-id [vlan-id [-vlan-id]]}`
6. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}} {symmetric}`
7. `bridge-domain bridge-id [split-horizon]`
8. `exit`
9. `rep segment segment-id [edge [no-neighbor] [primary]] [preferred]`
10. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> <code>exit</code></td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config-if)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface interface-id</code></td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# interface TenGigabitEthernet 0/45</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td>service instance id ethernet [evc-id]</td>
<td>Configures an Ethernet service instance on an interface and enters service instance configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
Switch(config-if)# service instance 101 ethernet

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation dot1q {any</td>
<td>vlan-id [vlan-id [vlan-id]]}</td>
<td>Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
</tbody>
</table>

**Example:**
Switch(config-if-srv)# encapsulation dot1q 100 second dot1q 200

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>rewrite ingress tag {push</td>
<td>dot1q vlan-id</td>
<td>dot1q vlan-id</td>
</tr>
</tbody>
</table>

**Step 7**
bridge-domain bridge-id [split-horizon]

**Example:**
Switch(config-if-srv)# bridge-domain 10

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits service instance configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**
Switch(config-if-srv)# exit

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</td>
<td>Configures REP over EVC. The segment ID range is from 1 to 1024.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
You must configure a primary and secondary edge port on each segment.

The following optional keywords are available.

- **edge** to configure the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports.
- **no-neighbor** to specify that the edge port must not have a neighbor port.

**Example:**
Switch(config-if)# rep segment 2 edge primary
Resilient Ethernet Protocol

Verifying REP with EVC Configuration

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter primary to configure the port as the primary edge port where you can configure VLAN load balancing.</td>
<td></td>
</tr>
<tr>
<td>• Enter preferred to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.</td>
<td></td>
</tr>
</tbody>
</table>

Step 10

<table>
<thead>
<tr>
<th>Step 10</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# exit</td>
</tr>
<tr>
<td>Exits interface configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

Example: Configure REP over EVC Using the Bridge Domain

The following example shows how to configure REP over EVC using the bridge domain.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 10
Switch(config-if-srv)# rewrite ingress tag push dot1q 10 symmetric
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# exit
Switch(config-if)# rep segment 2 edge
Switch(config-if)# end
```

Verifying REP with EVC Configuration

You can use the `show rep topology`, `show rep topology detail` and `show interface rep` commands to verify REP over EVC configuration.

Example of the show rep topology Command

```
Switch# show rep topology
```

<table>
<thead>
<tr>
<th>REP Segment 2</th>
<th>PortName</th>
<th>Edge</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge</td>
<td>Gi0/2</td>
<td>Pri</td>
<td>Open</td>
</tr>
<tr>
<td>ME2600X-2</td>
<td>Gi0/2</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>ME2600X-2</td>
<td>Gi0/1</td>
<td></td>
<td>Open</td>
</tr>
<tr>
<td>ME2600X-1</td>
<td>Gi0/1</td>
<td></td>
<td>Open</td>
</tr>
</tbody>
</table>
### Example of the show rep topology detail Command

```
Switch# show rep topology detail
REP Segment 2
Edge, Gi0/2 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 108c.8370.3000
  Port Number: 005
  Port Priority: 000
  Neighbor Number: 1 / [-6]
ME2600X-2, Gi0/2 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 108c.8370.2000
  Port Number: 005
  Port Priority: 000
  Neighbor Number: 2 / [-5]
ME2600X-2, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 108c.8370.2000
  Port Number: 004
  Port Priority: 000
  Neighbor Number: 3 / [-4]
ME2600X-1, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 108c.8370.1000
  Port Number: 004
  Port Priority: 000
  Neighbor Number: 4 / [-3]
ME2600X-1, Gi0/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 108c.8370.1000
  Port Number: 006
  Port Priority: 000
  Neighbor Number: 5 / [-2]
Edge, Gi0/3 (Secondary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 108c.8370.3000
  Port Number: 006
  Port Priority: 010
  Neighbor Number: 6 / [-1]
```

### Example of the show interface rep detail Command

```
Switch# show interfaces gigabitEthernet 0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Primary Edge)
PortID: 0005108C83703000
Preferred flag: No
Operational Link Status: TWO WAY
Current Key: 006108C83703000E83D
```
REP with Multicast

REP supports up to 24 segments in each node.

In an REP ring, the multicast traffic may not flow across all the elements on the ring; the traffic depends on the path taken from the multicast device to the client. The elements that do not form the multicast path do not become members of the multicast group.

When there is a failure in an REP ring, it is possible that the new path between the multicast device and the client may traverse elements which were previously not part of the multicast traffic path. These elements do not forward multicast traffic till they see a query from multicast device and a join from the client. A multicast device may only send query after long intervals, which results in a large traffic hit. All the ports that are enabled with REP must be configured as static multicast device ports to solve this issue.
Resilient Ethernet Protocol

REP with Multicast
Link Aggregation Group and Link Aggregation Control Protocol

This chapter describes Link Aggregation Group, Link Aggregation Control Protocol, and manual load balancing. This chapter also describes the configuration procedures.

This chapter includes the following topics.

- Understanding IEEE 802.3ad Link Bundling, page 129
- Link Aggregation Group and Link Aggregation Control Protocol Configuration Procedures, page 130
- Understanding LACP, page 130
- Understanding LACP Priority, page 134
- Understanding LACP 1:1 Redundancy, page 136
- Understanding LAG, page 138
- Understanding Load Balancing, page 145
- Show Commands, page 151
- Interactions of LAG with Other Features, page 154

Understanding IEEE 802.3ad Link Bundling

The IEEE 802.3ad link bundling feature provides a method for aggregating multiple Ethernet links into a single logical channel based on the IEEE 802.3ad standard. This feature helps improve the cost effectiveness of a device by increasing cumulative bandwidth without necessarily requiring hardware upgrades. In addition, the IEEE 802.3ad link bundling feature provides a capability to dynamically provision, manage, and monitor various aggregated links and enables interoperability between various Cisco devices and devices of third-party vendors.

Benefits of Link Bundling

The IEEE 802.3ad link bundling feature provides the following benefits:

- Increased network capacity without changing physical connections or upgrading hardware.
• Cost savings resulting from use of existing hardware and software for additional functions.
• A standard solution that enables interoperability of network devices.
• Port redundancy without user intervention when an operational port fails.

**Link Aggregation Group and Link Aggregation Control Protocol**

**Configuration Procedures**

To configure Link Aggregation Group (LAG) and Link Aggregation Control Protocol (LACP) using Cisco IOS commands, complete the following procedures:

• Configuring and Retrieving a Port Channel, on page 131
• Configuring LACP over Port Channel, on page 133
• Monitoring LACP Status, on page 134
• Setting LACP System Priority, on page 135
• Configuring LACP 1:1 Redundancy with Fast Switchover, on page 136
• Configuring a Channel Group with LACP, on page 139
• Adding and Removing Interfaces from a Channel Group with LAG, on page 142
• Setting a Minimum and Maximum Threshold of Active Links, on page 144
• Configuring Manual Load Balancing with LAG, on page 149

**Understanding LACP**

The LACP is part of the IEEE802.3ad standard that enables you to bundle several physical ports together to form a single logical channel. LACP enables a network device, such as a switch, to negotiate an automatic bundling of links by sending LACP packets to the peer device. The LACP is a control protocol over LAG to check for any LAG misconfigurations.

LACP enables you to form a single Layer 2 link automatically from two or more Ethernet links. This protocol ensures that both ends of the Ethernet link are functional and agree to be members of the aggregation group. LACP must be enabled at both ends of the link to be operational.

For more information on LACP, see the IEEE802.3ad standard document.

**LACP Advantages**

LACP provides high reliability and redundancy. If a port fails, traffic continues on the remaining ports.

**LACP Functions**

LACP performs the following functions in the system:

• Maintains configuration information to control aggregation.
• Exchanges configuration information with other peer devices.
Attaches or detaches ports from the LAG based on the exchanged configuration information.

**LACP Modes**

LACP can be configured in the following modes:

- **Active**—In this mode, the ports send LACP packets at regular intervals to the partner ports.
- **Passive**—In this mode, the ports do not send LACP packets until the partner port sends LACP packets. After receiving the LACP packets from the partner port, the ports send LACP packets to the partner port.

---

**Note**

When you enable LACP on the channel group, LACP exchanges Protocol Data Units (PDU) of size 128 bytes. Hence, if the Maximum Transmission Unit (MTU) size of the channel group is set to a value less than 128 bytes, the protocol data units are dropped and the channel group interface goes down.

A maximum of 8 member links are supported per port channel. A member link cannot belong to more than one port channel at the same time.

---

**Managing LACP**

Perform any of the following procedures as needed:

- Configuring and Retrieving a Port Channel, on page 131
- Configuring LACP over Port Channel, on page 133
- Monitoring LACP Status, on page 134

---

**Configuring and Retrieving a Port Channel**

**Note**

You must manually create a port channel logical interface. Configuring the IP address on the port channel interface is not supported.

---

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface port-channel *channel-number*
4. end
5. show running-config interface port-channel *channel-number*
6. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Identifies the interface port channel and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface port-channel channel-number</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>interface port-channel 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the port channel configuration.</td>
</tr>
<tr>
<td><code>show running-config interface port-channel channel-number</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>show running-config interface port-channel 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Ends the current configuration session.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Example: Verify the Port Channel Configuration

The following example shows how to verify the port channel configuration using Cisco IOS commands.

```
Switch# `show running-config interface port-channel 100`
```

```
Building configuration...

Current configuration : 139 bytes
!
  interface Port-channel100
    no ip address
    carrier-delay msec 0
    l2protocol peer cdp lacp
    l2protocol forward stp vtp dtp pagp dot1x
end
```
Configuring LACP over Port Channel

SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel channel-number
4. exit
5. interface type number
6. channel-group channel-number mode {active | passive}
7. end

DETAILED STEPS

<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>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface port-channel channel-number</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface port-channel 10</td>
</tr>
<tr>
<td></td>
<td>Identifies the interface port channel and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# exit</td>
</tr>
<tr>
<td></td>
<td>Returns to interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>interface type number</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface TenGigabitEthernet 0/45</td>
</tr>
<tr>
<td></td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>channel-group channel-number mode {active</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# channel-group 10 mode active</td>
</tr>
<tr>
<td></td>
<td>Configures the interface in a channel group and sets the lacp mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Monitoring LACP Status

For examples of `show lacp` commands, see Show Commands, on page 151.

SUMMARY STEPS

1. enable
2. show lacp `{channel-group-number | counters | internal [detail] | neighbor [detail] | sys-id}
3. end

DETAILED STEPS

<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>Example:</td>
<td><code>Switch&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
| **Step 2** | show lacp `{channel-group-number | counters | internal [detail] | neighbor [detail] | sys-id}
| Example: | `Switch# show lacp internal` |
| | Displays LACP information. |
| **Step 3** | end |
| Example: | `Switch# end` |
| | Ends the current configuration session. |

Understanding LACP Priority

LACP uses the following parameters to control aggregation:

- LACP system priority—The system priority can be configured automatically or through the CLI. LACP uses the system priority with the device MAC address to form the system ID and also during negotiations with other systems. The range of LACP system priority is from 0 to 65535. The default value is 32768.

- LACP port priority—The port priority can be configured automatically or through the CLI. LACP uses the port priority to decide which ports must be placed first in aggregation. LACP also uses the port priority with the port number to form the port identifier. The range of LACP port priority is from 0 to 65535. The default value is 32768.
• LACP administrative key—LACP automatically configures an administrative key value on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. The ability of the port to aggregate with the other ports is determined by the following:
  * Port physical characteristics such as data rate, duplex capability, and point-to-point or shared medium.
  * Configuration restrictions that you establish.

### Setting LACP System Priority

#### SUMMARY STEPS

1. enable
2. configure terminal
3. lacp system-priority *priority*
4. end
5. show lacp {channel-group-number | counters | internal [detail] | neighbor [detail] | sys-id}
6. end

#### 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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> lacp system-priority <em>priority</em></td>
<td>Sets the system priority. The range of the LACP system priority is from 0 to 65535. The default value is 32768.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# lacp system-priority 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show lacp {channel-group-number</td>
<td>counters</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show lacp sys-id</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose |
--- | --- |
**Step 6** | **end** | Ends the current configuration session. |

**Example:**

```
Switch# end
```

---

### Understanding LACP 1:1 Redundancy

The LACP 1:1 redundancy feature provides an EtherChannel configuration with one active link and fast switchover to a hot standby link.

To use the LACP 1:1 redundancy feature, configure the LACP EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot standby link. When the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link.

For the LACP 1:1 redundancy feature to work correctly, especially the fast switchover capability, the feature needs to be enabled at both ends of the link.

### Configuring LACP 1:1 Redundancy with Fast Switchover

For the LACP 1:1 redundancy feature, the channel group must contain two links, of which only one is active. The link with the lower port priority number (and therefore a higher priority) becomes the active link, and the other link moves to a hot standby state. The maximum number of active member ports (`lacp max-bundle`) must be set to 1.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface port-channel channel-number`
4. `lacp fast-switchover`
5. `lacp max-bundle number`
6. `end`
7. `show running-config interface port-channel channel-number`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
</tbody>
</table>
### Command or Action

**Example:**

Switch> **enable**

- Enter your password if prompted.

### Step 2

**configure terminal**

*Example:*  
Switch# **configure terminal**

Enters global configuration mode.

### Step 3

**interface port-channel channel-number**

*Example:*  
Switch(config)# **interface port-channel 10**

Identifies the interface port channel and enters interface configuration mode.

### Step 4

**lacp fast-switchover**

*Example:*  
Switch(config-if)# **lacp fast-switchover**

Enables the fast switchover feature for this channel group.

### Step 5

**lacp max-bundle number**

*Example:*  
Switch(config-if)# **lacp max-bundle 1**

Sets the maximum number of active member ports in the channel group to 1.

### Step 6

**end**

*Example:*  
Switch(config-if)# **end**

Returns to privileged EXEC mode.

### Step 7

**show running-config interface port-channel channel-number**

*Example:*  
Switch# **show running-config interface port-channel 10**

Displays the port channel configuration.

---

**Example: Configure LACP 1:1 Redundancy with Fast Switchover**

The following example shows how to configure the LACP channel group with 1:1 redundancy using Cisco IOS commands. Because the Ten Gigabit Ethernet port 0/45 is configured with a higher port priority number (and therefore a lower priority) than the default value of 32768, it becomes the standby port.

```
Switch> **enable**  
Switch# **configure terminal**  
Switch(config)# **lacp system-priority 33000**  
Switch(config)# **interface TenGigabitEthernet 0/45**  
Switch(config-if)# **channel-group 1 mode active**  
Switch(config)# **interface TenGigabitEthernet 0/45**  
Switch(config-if)# **lacp port-priority 33000**  
Switch(config)# **interface port-channel 1**  
Switch(config-if)# **lacp fast-switchover**  
Switch(config-if)# **lacp max-bundle 1**  
Switch(config-if)# **end**  
Switch(config)# **show run interface port-channel 1**
```
Understanding LAG

The LAG or an EtherChannel, bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links. When an Ethernet Flow Point is configured on LAG, the EFP is protected against link failures.

When a link within an EtherChannel fails, the traffic previously carried over the failed link switches to the remaining links within that EtherChannel.

LAG supports manual load balancing and platform default load balancing. LAG supports Ethernet services.

Restrictions for LAG

- All the member links of LAG must be connected to the same Cisco ME 2600X system and must be of the same interface type (10GE or 1GE). For example, one member link can be present in one Cisco ME 2600X and another member link can be present in another Cisco ME 2600X. These two Cisco ME 2600X panels must be connected to the same Cisco ME 2600X system.
- All the member links of LAG must operate at the same link speed and in full-duplex mode. LACP does not support the half-duplex mode.
- Member links with varying speed can be added to the same port-channel with LAG.
- If you configure a physical port as part of LAG, you cannot configure Ethernet Virtual Circuits (EVCs) under that physical port.
- Maximum of 8 member links are supported per LAG. A member link cannot belong to more than one LAG at the same time.
- Maximum number of port channel interfaces supported are 64.
- If you remove a member from a port-channel configured with a low value carrier delay, all other links in the port-channel flap.

Managing a Channel Group

Perform any of the following procedures as needed:

- Configuring a Channel Group with LACP, on page 139
- Adding and Removing Interfaces from a Channel Group with LAG, on page 142
- Setting a Minimum and Maximum Threshold of Active Links, on page 144
Configuring a Channel Group with LACP

SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel channel-number
4. interface type number
5. channel-group channel-number mode {active | passive}
6. 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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface port-channel channel-number</td>
<td>Identifies the interface port channel.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface port-channel 5</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>interface type number</td>
<td>Configures a member interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>channel-group channel-number mode {active</td>
<td>passive}</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# channel-group 5 mode active</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
**Example: Configure a Channel Group with LACP**

The following example shows how to configure the channel group number 5 using Cisco IOS commands.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# channel-group 5 mode active
Switch(config-if)# exit
```

**Adding and Removing Interfaces from a Channel Group with LACP**

**Prerequisite**

*Configuring and Retrieving a Port Channel, on page 131*

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `channel-group channel-group-number mode {active | passive}`
5. `no channel-group channel-group-number`
6. `end`

**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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Configures a member interface and enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> channel-group channel-group-number mode {active</td>
<td>passive}</td>
</tr>
<tr>
<td>Example: Switch(config-if)# channel-group 5 mode active</td>
<td></td>
</tr>
</tbody>
</table>
Example: Add and Remove Interface from a Channel Group

The following example shows how to add an interface to a channel group using Cisco IOS commands:

Switch> enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# channel-group 5 mode active
Switch(config-if)# exit

The following example shows how to remove an interface from a channel group using Cisco IOS commands:

Switch> enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# no channel-group 5
Switch(config-if)# exit

Configuring a Channel Group with LAG

SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel channel-number
4. interface type number
5. channel-group channel-number
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Adding and Removing Interfaces from a Channel Group with LAG

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface port-channel channel-number</td>
<td>Identifies the interface port channel.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface port-channel 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type number</td>
<td>Configures a member interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> channel-group channel-number</td>
<td>Configures the channel group with the LACP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# channel-group 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Configure a Channel Group with LAG**

The following example shows how to configure the channel group number 5 using Cisco IOS commands.

Switch> enable
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# channel-group 5
Switch(config-if)# exit

**Adding and Removing Interfaces from a Channel Group with LAG**

**Prerequisite**

*Configuring and Retrieving a Port Channel*, on page 131
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `channel-group channel-group-number`
5. `no channel-group channel-group-number`
6. `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><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>2</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>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>interface type number</code></td>
<td>Configures a member interface and enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>interface TenGigabitEthernet 0/45</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>channel-group channel-group-number</code></td>
<td>Adds a Ten Gigabit Ethernet interface to a channel group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# <code>channel-group 5</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>no channel-group channel-group-number</code></td>
<td>Removes the Ten Gigabit Ethernet interface from the channel group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# <code>no channel-group 5</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example: Add and Remove Interface from a Channel Group**

The following example shows how to add an interface to a channel group using Cisco IOS commands:

Switch> `enable`
Switch# `configure terminal`
Switch(config)# `interface TenGigabitEthernet 0/45`
Switch(config-if)# channel-group 5
Switch(config-if)# exit

The following example shows how to remove an interface from a channel group using Cisco IOS commands:

Switch> enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# no channel-group 5
Switch(config-if)# exit

### Setting a Minimum and Maximum Threshold of Active Links

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel channel-number
4. lACP min-bundle min-bundle-number
5. lACP max-bundle max-bundle-number
6. 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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface port-channel channel-number</td>
<td>Creates a port channel virtual interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface port-channel 1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>lACP min-bundle min-bundle-number</td>
<td>Sets the minimum threshold of active member links allowed in the LACP bundle. The range is 1 to 8.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# lACP min-bundle 5</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>lACP max-bundle max-bundle-number</td>
<td>Sets the maximum threshold of active member links allowed in the LACP bundle. The range is 1 to 8. The maximum threshold value must be greater than or equal to the minimum threshold value.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# lACP max-bundle 7</td>
<td></td>
</tr>
</tbody>
</table>
Example: Set a Minimum Threshold of Active Links

The following example shows how to set a minimum threshold of active member links using Cisco IOS commands:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface port-channel 1
Switch(config-if)# lacp min-bundle 5
Switch(config-if)# end
```

Understanding Load Balancing

Manual load balancing enables you to manually specify which member link a service instance must use for its egress traffic. This allows you, who has knowledge about the type of traffic traversing an EFP, to equally distribute EFPs.

---

**Note**

The ingress traffic for any EFP can arrive on any member link of the LAG. All the egress traffic for the EFP must use only one of the member links.

EFPs can be configured on a channel group. The traffic, carried by the EFPs, is load balanced across the member links. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. The load balancing is achieved by distributing EFPs between the member links. The EFPs on a channel group are grouped and each group is associated with a member link. The manual load balancing mechanism can be used to control the EFP grouping.

---

**Note**

Cisco ME 2600X supports manual load balancing and platform default load balancing. Cisco ME 2600X does not support weighted load balancing in this release. When manual load balancing is not configured and applied to the service instance, the default platform load balancing mechanism is used.

**Default Load Balancing**

In the default load balancing mechanism, the EFP traffic is distributed based on a hashing algorithm that is determined by the service instance ID and the number of active members in the channel group. The default load balancing algorithm is explained below.

\[(\text{Service-instance ID}) \div \text{max_num_links}\]
The maximum number of member links (max_num_links) supported in Cisco ME 2600X is 8. Hence, 
(Service-instance ID) ÷ max_num_links value provides a hash bit value from 0 to 7. This value is then compared 
with the load share of each member link.

The load share is allocated for each active member link based on the number of active member links in the 
channel group. The member link whose load share contains the hash bit is selected as the egress link.

The load share derivation is as follows:
The default load share allocation algorithm allocates the load share bits sequentially to the member links.

Let us consider that we have 4 active links as follows. The load share calculation varies based on the link ids 
defined.

Member-1:4/1- 0 0 0 1 0 0 0 1 = 0x11
Member-2:4/2- 0 0 1 0 0 0 1 0 = 0x22
Member-3:4/3- 0 1 0 0 0 1 0 0 = 0x44
Member-4:4/4- 1 0 0 0 1 0 0 0 = 0x88

**Configuring Load Balancing**

1. Create a channel group and add 4 member links (4/1, 4/2, 4/3, and 4/4).
2. The load share is calculated for the active member links.
3. Create a service with ID10 on the channel group.
4. On applying the algorithm: (Service-instance ID) ÷ max_num_links, we get 10 ÷ 8 = 2 (hash bit).
5. In the loadshare derived above, the hash bit = 2 is set for the port 4/3 and hence 4/3 is chosen as the egress 
   port for the service 10.
6. The same procedure is repeated when services are added to obtain the egress port.

---

**Configuring Manual Load Balancing with LACP**

**Prerequisite**

Configuring a Channel Group with LACP, on page 139
SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel channel-number
4. service instance id ethernet
5. encapsulation untagged, dot1q {any | vlan-id} second-dot1q {any | vlan-id}
6. bridge-domain bridge-id
7. exit
8. port-channel load-balance {link link-id}
9. backup link link-id
10. service-instance id
11. exit
12. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: R Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface port-channel channel-number</td>
<td>Creates a port channel virtual interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface port-channel 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface and enters service instance configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# service instance 100 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation untagged, dot1q {any</td>
<td>vlan-id} second-dot1q {any</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# encapsulation dot1q 100</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Step 6</td>
<td>bridge-domain bridge-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-srv)# bridge-domain 100</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-srv)# exit</td>
</tr>
<tr>
<td>Step 8</td>
<td>port-channel load-balance {link link-id}</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# port-channel load-balance link 1</td>
</tr>
<tr>
<td>Step 9</td>
<td>backup link link-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-lb)# backup link 2,3,4</td>
</tr>
<tr>
<td>Step 10</td>
<td>service-instance id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-lb)# service-instance 100</td>
</tr>
<tr>
<td>Step 11</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-lb)# exit</td>
</tr>
<tr>
<td>Step 12</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
</tbody>
</table>

**Example: Configuring Manual Load Balancing with LACP**

The following example shows how the service instances 100 and 101 are manually assigned to link 1 on Ten Gigabit Ethernet interface 0/45. The service instances are also assigned backup links 2, 3, and 4.

Switch# configure terminal
Switch(config)# interface port-channel 10
Switch(config-if)# service instance 100 ethernet
Switch(config-if-srv)# encapsulation dot1q 100
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# exit
Switch(config-if)# service instance 101 ethernet
Switch(config-if-srv)# encapsulation dot1q 101
Switch(config-if-srv)# bridge-domain 101
Switch(config-if-srv)# exit
Switch(config-if)# port-channel load-balance link 1
Switch(config-if-lb)# backup link 2,3,4
Switch(config-if-lb)# service-instance 100,101
Switch(config-if-lb)# exit
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# channel-group 10 mode active link 1
Switch(config-if)# exit

Configuring Manual Load Balancing with LAG

Prerequisite
Configuring a Channel Group with LAG, on page 141

SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel channel-number
4. service instance id ethernet
5. encapsulation untagged, dot1q {any | vlan-id} second-dot1q {any | vlan-id}
6. bridge-domain bridge-id
7. exit
8. port-channel load-balance {link link-id}
9. backup link link-id
10. service-instance id
11. exit
12. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface port-channel channel-number</td>
<td>Creates a port channel virtual interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface port-channel 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface and enters service instance configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# service instance 100 ethernet</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 5    | encapsulation untagged, dot1q \{any | vlan-id\}  
second-dot1q \{any | vlan-id\} | Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance. |
|      | Example:  
Switch(config-if-srv)# encapsulation dot1q 100 | |
| 6    | bridge-domain bridge-id | Binds the Ethernet service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance. |
|      | Example:  
Switch(config-if-srv)# bridge-domain 100 | |
| 7    | exit | Exits the service instance configuration mode. |
|      | Example:  
Switch(config-if-srv)# exit | |
| 8    | port-channel load-balance \{link link-id\} | Configures the primary load balanced link. |
|      | Example:  
Switch(config-if)# port-channel load-balance link 1 | |
| 9    | backup link link-id | Configures the back up links under the primary link. |
|      | Example:  
Switch(config-if-lb)# backup link 2,3,4 | |
| 10   | service-instance id | Assigns a service instance to a member link for manual load balancing |
|      | Example:  
Switch(config-if-lb)# service-instance 100 | |
| 11   | exit | Returns to interface configuration mode. |
|      | Example:  
Switch(config-if-lb)# exit | |
| 12   | end | Returns to privileged EXEC mode. |
|      | Example:  
Switch(config-if)# end | |

**Example: Configuring Manual Load Balancing with LAG**

The following example shows how the service instances 100 and 101 are manually assigned to link 1 on Ten Gigabit Ethernet interface 0/45. The service instances are also assigned backup links 2, 3, and 4.

```
Switch# configure terminal  
Switch(config)# interface port-channel 10  
Switch(config-if)# service instance 100 ethernet  
Switch(config-if-srv)# encapsulation dot1q 100  
Switch(config-if-srv)# bridge-domain 100  
Switch(config-if-srv)# exit
```
Show Commands

Display Port Channel Statistics

The following example shows how to view port channel statistics.

Switch# show interfaces stats

<table>
<thead>
<tr>
<th>GigabitEthernet 0/1</th>
<th>Pkts In</th>
<th>Chars In</th>
<th>Pkts Out</th>
<th>Chars Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>108470</td>
<td>31042570</td>
<td>82259</td>
<td>1425549</td>
</tr>
<tr>
<td>Route cache</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>108470</td>
<td>31042570</td>
<td>82259</td>
<td>1425549</td>
</tr>
<tr>
<td>GigabitEthernet 0/2</td>
<td>Pkts In</td>
<td>Chars In</td>
<td>Pkts Out</td>
<td>Chars Out</td>
</tr>
<tr>
<td>Processor</td>
<td>15979</td>
<td>19073260</td>
<td>15192</td>
<td>1325713</td>
</tr>
<tr>
<td>Route cache</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>15979</td>
<td>19073260</td>
<td>15192</td>
<td>1325713</td>
</tr>
<tr>
<td>Port-channel15</td>
<td>Pkts In</td>
<td>Chars In</td>
<td>Pkts Out</td>
<td>Chars Out</td>
</tr>
<tr>
<td>Processor</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Route cache</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Switch# show interfaces port-channel 2 stats

<table>
<thead>
<tr>
<th>Port-channel2</th>
<th>Pkts In</th>
<th>Chars In</th>
<th>Pkts Out</th>
<th>Chars Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>570546645</td>
<td>295127854241</td>
<td>557694541</td>
<td>291427545417</td>
</tr>
<tr>
<td>Route cache</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>570546645</td>
<td>295127854241</td>
<td>557694541</td>
<td>291427545417</td>
</tr>
</tbody>
</table>

Display Port Channel Interface

The following example shows how to view the information for a port channel interface. channel-id is an integer value between 1 to 64.

Switch# show interfaces port-channel channel-id

Switch# show interfaces port-channel 20
Port-channel20 is up, line protocol is up
Hardware is GEChannel, address is 0002.0415.0002 (bia 0000.0000.0000)
MTU 9600 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
   No. of active members in this channel: 1
   Member 0 : TenGigabitEthernet 0/45 , Full-duplex, 10000Mb/s
   No. of passive members in this channel: 0
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   37 packets input, 7820 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   39 packets output, 8088 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out

Display EFP Statistics
The following example shows how to view EFP statistics.

Switch> show ethernet service instance stats

System maximum number of service instances: 32768
Service Instance 2, Interface TenGigabitEthernet 0/45
   Pkts In      Bytes In      Pkts Out      Bytes Out
   0           0              0           0
Service Instance 2, Interface Port-channel15
   Pkts In      Bytes In      Pkts Out      Bytes Out
   0           0              0           0

Display LACP Activity
The following examples show how to view LACP activity in the network.

Switch# show lacp internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode        P - Device is in Passive mode

Channel group 20
### Show Commands

Switch# `show lacp 20 counters`

<table>
<thead>
<tr>
<th>Port</th>
<th>LACP port</th>
<th>Priority</th>
<th>Admin Key</th>
<th>Oper Key</th>
<th>Port Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te4/2</td>
<td>SA bndl</td>
<td>32768</td>
<td>0x5</td>
<td>0x5</td>
<td>0x42</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

Switch# `show lacp 20 internal`

Flags:  
- **S** - Device is requesting Slow LACPDUs  
- **F** - Device is requesting Fast LACPDUs  
- **A** - Device is in Active mode  
- **P** - Device is in Passive mode  

Switch# `show lacp 20 neighbor`

Flags:  
- **S** - Device is requesting Slow LACPDUs  
- **F** - Device is requesting Fast LACPDUs  
- **A** - Device is in Active mode  
- **P** - Device is in Passive mode  

Partner's information:

<table>
<thead>
<tr>
<th>Partner</th>
<th>Partner</th>
<th>LACP Port</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Flags</td>
<td>State</td>
<td>Port</td>
<td>Priority</td>
<td>Admin Key</td>
<td>Oper Key</td>
</tr>
<tr>
<td>Te4/2</td>
<td>SA</td>
<td>32768</td>
<td>0011.2026.7300</td>
<td>11s</td>
<td>0x1</td>
<td>0x14</td>
</tr>
</tbody>
</table>

Switch# `show lacp 20 counters`

<table>
<thead>
<tr>
<th>Channel group: 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te4/2</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>31</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

Switch# `show lacp sys-id`

```
32768,0005.9b2e.18e0
```
Display Manual Load Balancing Configuration

Switch# show ethernet service instance load-balance

Manually Assigned Load-Balancing Status for Port-channel1

Link ID 1: TenGigabitEthernet 0/45 (Active)
Backup: Link ID 2 TenGigabitEthernet 0/45
Service instances: 10

Link ID 2: TenGigabitEthernet 0/46 (Active)
Backup: Link ID 1 TenGigabitEthernet 0/46
Service instances: 20

Switch# show ethernet service instance platform

Displays the port channel EFPs that are currently using the manual or platform load balancing and the egress link.

EFP id: 10 Interface Port-channel1
Load balancing type: Manual
Associated Egress Interface: TenGigabitEthernet 0/45
EFP id: 20 Interface Port-channel1
Load balancing type: Manual
Associated Egress Interface: TenGigabitEthernet 0/46
EFP id: 10 Interface Port-channel2
Load balancing type: Manual
Associated Egress Interface: TenGigabitEthernet 0/47
EFP id: 20 Interface Port-channel2
Load balancing type: Platform
Associated Egress Interface: TenGigabitEthernet 0/48

Interactions of LAG with Other Features

LAG interacts with the following features:

• EVC
• QoS
• IGMP Snooping

LAG with EVC

EFPs can be configured on a channel group. The traffic, carried by the EFPs, is load balanced across the member links. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. The load balancing is achieved by distributing EFPs between the member links. The EFPs on a channel group are grouped and each group is associated with a member link.

In the default load balancing mechanism, there is no control over how the EFPs are distributed together, and sometimes the EFP distribution is not ideal. The manual load balancing mechanism can be alternatively used to control the EFP grouping.

When you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.
LAG can be configured for both point-to-point and point-to-multipoint bridge domains.

---

**Note**

The system will support a maximum of 256 EFPs on all the configured port channels.

---

**LAG with QoS**

See QoS Support on Port-Channel, on page 66.

**LAG with IGMP Snooping**

See IGMP Snooping Interaction with LAG, on page 200.

**LAG with REP**

REP is not supported on member links that are part of a channel group.
MAC Learning

This chapter describes MAC learning, MAC address limiting, and static MAC address. This chapter also describes the configuration procedures.

- Understanding MAC Learning, page 157
- Understanding MAC Address Limiting, page 160
- Understanding the Static MAC Address, page 162
- Removing a MAC Address, page 164
- Displaying Information About the MAC Address Table, page 165

Understanding MAC Learning

A software MAC address table is maintained on the Cisco ME 2600X. This MAC address table contains the MAC addresses learned on all the interfaces of Cisco ME 2600X.

Note
By default, MAC address learning is enabled only for point-to-multipoint bridge domains and can also be disabled.

MAC Address Aging

Dynamically learned MAC addresses are deleted after the MAC address age out value. This frees up unused addresses from the MAC address table for other active subscribers. In Cisco ME 2600X, the default value for MAC address aging is 300 seconds and cannot be changed. The expected MAC address age out timer is between 300 to 600 seconds depending on the number of MAC addresses learned.

Dynamic MAC Address Learning

Dynamic MAC address learning occurs when the bridging data path encounters an ingress frame whose source address is not present in the MAC address table for the ingress service instance. The learned MAC addresses are distributed to the other cards with Ethernet Flow Points (EFPs) in the same bridge domain.
**MAC Move**

A MAC move occurs when the same MAC address is re-learned on a different port. When a MAC move is detected, a transient event is generated to inform the user about the MAC move.

**MAC Learning on LAG**

MAC learning is enabled on the LAG interface, if the Link Aggregation Group (LAG) interface is part of the point-to-multipoint bridge domain. The MAC addresses are learned on the LAG interface instead of the physical interface.

**MAC Learning Actions**

The table below describes the various scenarios and the actions taken on MAC addresses for each scenario.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A bridge domain is created.</td>
<td>The MAC learning is enabled by default in point-to-multipoint bridge domains. The MAC learning is not supported in point-to-point bridge domains.</td>
</tr>
<tr>
<td>A bridge domain is deleted.</td>
<td>The MAC addresses learned on the bridge domain are removed from the software MAC address table that is maintained on the interface on Cisco ME 2600X.</td>
</tr>
<tr>
<td>An EFP is added and is the first EFP on a bridge domain on an interface of Cisco ME 2600X.</td>
<td>All the MAC addresses learned on the bridge domain are sent to this new interface on Cisco ME 2600X.</td>
</tr>
<tr>
<td>An EFP is added and is not the first EFP on a bridge domain.</td>
<td>Nothing needs to be done as the MAC addresses learned on the bridge domain are already present.</td>
</tr>
<tr>
<td>An EFP is deleted.</td>
<td>All the MAC addresses learned on that EFP are deleted.</td>
</tr>
<tr>
<td>An EFP admin state is UP.</td>
<td>When the EFP is the first EFP on the bridge domain on the Cisco ME 2600X, all the MAC addresses learned on the bridge domain are sent to this new interface on Cisco ME 2600X. When the EFP is not the first EFP on the bridge domain on the interface, nothing needs to be done as the MAC addresses learned on the bridge domain are already present.</td>
</tr>
<tr>
<td>An EFP admin state is DOWN.</td>
<td>All the MAC addresses learned on that EFP are deleted.</td>
</tr>
<tr>
<td>The port goes down.</td>
<td>All the MAC addresses learned on the port on all the bridge domains are deleted.</td>
</tr>
</tbody>
</table>

**MAC Learning Configuration Procedures**

The following procedures can be performed using Cisco IOS commands to configure MAC learning and MAC address limiting:
Re-enabling or Disabling MAC Learning on a Bridge Domain

MAC learning is enabled on the point-to-multipoint bridge domains by default.

SUMMARY STEPS

1. enable
2. configure terminal
3. bridge-domain bridge-id
4. mac learning
5. no mac learning
6. end

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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> bridge-domain bridge-id</td>
<td>Configures components on a bridge domain and enters bridge domain configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# bridge-domain 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mac learning</td>
<td>Re-enables MAC learning on this bridge domain.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-bdomain)# mac learning</td>
<td></td>
</tr>
</tbody>
</table>
### Understanding MAC Address Limiting

The MAC Address Limiting for bridge domains provides the capability to control the MAC addresses learnt on the bridge domain. You can configure an upper limit on the number of MAC addresses that can be learnt in a bridge domain. If an Ethernet frame with an unknown MAC address is received, it is flooded in the bridge domain. The MAC address limiting commands are configured under the bridge domain.

**Note**

The maximum MAC address limit on a bridge domain is 32000.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5**  
no mac learning | Disables MAC learning on this bridge domain.  
Example:  
Switch(config-bdomain)# no mac learning |
| **Step 6**  
end | Exits bridge domain configuration mode and returns to privileged EXEC mode.  
Example:  
Switch(config-bdomain)# end |

---

**Example: Re-enable or Disable MAC Learning on a Bridge Domain**

The following example shows how to re-enable MAC learning on a bridge domain using Cisco IOS commands:

```
Switch> enable  
Switch# configure terminal  
Switch(config)# bridge-domain 100  
Switch(config-bdomain)# mac learning  
Switch(config-bdomain)# end
```

The following example shows how to disable MAC learning on a bridge domain using Cisco IOS commands:

```
Switch> enable  
Switch# configure terminal  
Switch(config)# bridge-domain 100  
Switch(config-bdomain)# no mac learning  
Switch(config-bdomain)# end
```
Configuring MAC Address Limit on a Bridge Domain

SUMMARY STEPS

1. enable
2. configure terminal
3. bridge-domain bridge-id
4. mac limit maximum addresses maximum-addresses
5. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> bridge-domain bridge-id</td>
<td>Configures components on a bridge domain and enters bridge domain configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# bridge-domain 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mac limit maximum addresses maximum-addresses</td>
<td>Sets an upper limit on the number of MAC addresses that reside in a bridge domain.</td>
</tr>
<tr>
<td>Example: Switch(config-bdomain)# mac limit maximum addresses 200</td>
<td><strong>Note</strong> Use the no mac limit command to restore the default MAC address limit.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits bridge domain configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-bdomain)# end</td>
<td></td>
</tr>
</tbody>
</table>

Example: Configure MAC Address Limit on a Bridge Domain

The following example shows how to configure MAC address limiting on a bridge domain using Cisco IOS commands:

```
Switch> enable
Switch# configure terminal
Switch(config)# bridge-domain 100
```
Understanding the Static MAC Address

You can configure static MAC addresses on a service instance. Static MAC address configuration on service instances eliminates the need for MAC address learning, which is required for traffic forwarding. Without MAC address learning, MAC address table resources can be conserved and network resources can be optimized.

Note
Static MAC address configuration does not apply to the MVR bridge domain.

Benefits
Static MAC address support on service instances provides the following benefits:

• Facilitates optimization of network resources.
• Conserves MAC table resources when used for upstream traffic.

Restrictions for Static MAC Address

• Multicast static MAC addresses are not allowed in MAC address configurations.
• Unicast MAC addresses can be statically configured.

Configuring a Static MAC Address on a Service Instance

Prerequisite
Configuring an Ethernet Service Instance, on page 50

Note
Use the no mac static address mac-addr command to remove the statically added unicast MAC address.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. service instance id ethernet [eve-id]
5. mac static address mac-address
6. exit
7. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| `enable` |  |
| Example:  
  Switch> enable |  |
| **Step 2** | Enters global configuration mode. |
| `configure terminal` |  |
| Example:  
  Switch# configure terminal |  |
| **Step 3** | Configures a Ten Gigabit Ethernet interface and enters interface configuration mode. |
| `interface type number` |  |
| Example:  
  Switch(config)# interface TenGigabitEthernet 0/45 |  |
| **Step 4** | Configures an Ethernet service instance on an interface and enters service instance configuration mode. |
| `service instance id ethernet [evc-id]` |  |
| Example:  
  Switch(config-if)# service instance 1 ethernet |  |
| **Step 5** | Configures a static MAC address on a service instance. |
| `mac static address mac-address` |  |
| Example:  
  Switch(config-if-srv)# mac static address 0000.bbbb.cccc |  |
| **Step 6** | Returns to interface configuration mode. |
| `exit` |  |
| Example:  
  Switch(config-if-srv)# exit |  |
| **Step 7** | Returns to privileged EXEC mode. |
| `end` |  |
| Example:  
  Switch(config-if)# end |  |

#### Example: Configure a Static MAC Address on a Service Instance

The following example shows how to configure a static MAC address on a service instance using Cisco IOS commands:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# service instance 1 ethernet
Switch(config-if-srv)# encapsulation dot1q 100
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# mac static address 0000.bbbb.cccc
Switch(config-if-srv)# exit
Switch(config-if)# end
```
Removing a MAC Address

Note
This procedure removes only dynamically added MAC addresses. To remove the statically added MAC addresses, use the no mac static address mac-addr command.

SUMMARY STEPS

1. enable
2. configure terminal
3. clear mac-address-table [address mac-address] [interface type number] [bridge-domain bridgedomain-id]
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2 configure terminal | Enters global configuration mode. |
| Example:                  |        |
| Switch# configure terminal|         |

| Step 3 clear mac-address-table [address mac-address] [interface type number] [bridge-domain bridgedomain-id] | Removes the dynamic MAC address from the MAC address table on a bridge domain. The bridgedomain-id is the bridge domain number. |
| Example: | Switch(config)# clear mac-address-table address 0000.bbbb.cccc interface TenGigabitEthernet 0/45 bridge-domain 100 |

| Step 4 exit | Exits global configuration mode. |
| Example: | Switch(config)# exit |

Example: Remove a MAC Address

The following example shows how to remove a MAC address from the MAC address table on a bridge domain using Cisco IOS commands:

Switch> enable
Switch# configure terminal
Switch(config)# clear mac-address-table address 0000.bbbb.cccc interface TenGigabitEthernet 0/45 bridge-domain 100
Switch(config)# exit

The following example shows how to remove a MAC address from the MAC address table on all the bridge domains using Cisco IOS commands:

Switch> enable
Switch# configure terminal
Switch(config)# clear mac-address-table address 0000.bbbb.cccc
Switch(config)# exit

## Displaying Information About the MAC Address Table

### SUMMARY STEPS

1. enable
2. show mac-address-table address *mac-addr*
3. show mac-address-table bridge-domain *bridge-domain-id*
4. show mac-address-table interface *type number*

### 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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show mac-address-table address <em>mac-addr</em></td>
<td>Displays information about the MAC address table for a specific MAC address. The <em>mac-addr</em> is a 48-bit MAC address and the valid format is H.H.H.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show mac-address-table address 0050.3e8d.6400</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show mac-address-table bridge-domain <em>bridge-domain-id</em></td>
<td>Displays information about the MAC address table for a specific bridge domain. The <em>bridge-domain-id</em> is the bridge domain number.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show mac-address-table bridge-domain 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show mac-address-table interface <em>type number</em></td>
<td>Displays information about the MAC address table for a specific interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show mac-address-table interface TenGigabitEthernet 0/45</td>
<td></td>
</tr>
</tbody>
</table>
Example: Display Information About the MAC Address Table

The following example shows how to display the MAC address table information:

Switch# show mac-address-table

<table>
<thead>
<tr>
<th>Bridge Domain Index</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0000.1000.001e</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001d</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001c</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>200</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>Te4/1</td>
</tr>
<tr>
<td>100</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>Te4/1</td>
</tr>
<tr>
<td>5</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>Te4/1</td>
</tr>
<tr>
<td>4</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>Te4/1</td>
</tr>
<tr>
<td>1</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>Te4/1</td>
</tr>
</tbody>
</table>

The following example shows how to display the MAC address table information for a specific MAC address:

Switch# show mac-address-table address 0000.1000.0001

<table>
<thead>
<tr>
<th>Bridge Domain Index</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0000.1000.0001</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
</tbody>
</table>

The following example shows how to display the MAC address table information for a specific bridge domain:

Switch# show mac-address-table bridge-domain 2

<table>
<thead>
<tr>
<th>Bridge Domain Index</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0000.1000.001e</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001d</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001c</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001b</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001a</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.0019</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
</tbody>
</table>

The following example shows how to display the MAC address table information for a specific interface:

Switch# show mac-address-table interface tenGigabitEthernet 0/45

<table>
<thead>
<tr>
<th>Bridge Domain Index</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0000.1000.001e</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001d</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001c</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001b</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.001a</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
<tr>
<td>2</td>
<td>0000.1000.0019</td>
<td>dynamic</td>
<td>Te4/2</td>
</tr>
</tbody>
</table>

The following example shows how to display the MAC address table information for a LAG interface (Po9):

Switch# show mac-address-table
<table>
<thead>
<tr>
<th>Bridge Domain Index</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0000.0300.0900</td>
<td>dynamic</td>
<td>Te4/1</td>
</tr>
<tr>
<td>2</td>
<td>0000.0300.1000</td>
<td>dynamic</td>
<td>Po9</td>
</tr>
</tbody>
</table>
Multicast VLAN Registration

This chapter describes Multicast VLAN Registration and procedures to configure Multicast VLAN Registration.

- Multicast VLAN Registration, page 169
- Prerequisites for MVR, page 170
- Restrictions for MVR, page 170
- Information About MVR, page 171
- How to Configure MVR, page 173
- Verifying the MVR Configuration, page 177
- Configuration Examples for MVR, page 179
- Additional References for MVR, page 180

Multicast VLAN Registration

In multicast VLAN networks, subscribers to a multicast group can exist in more than one VLAN. If the VLAN boundary restrictions in a network consist of Layer 2 switches, it might be necessary to replicate the multicast stream to the same group in different subnets, even if they are on the same physical network. Multicast VLAN Registration (MVR) routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when MVR is enabled.

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 Toolkit 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.
Prerequisites for MVR

- It is mandatory to untag the packets before they enter the bridge domain. For an MVR source and receiver, the packets are untagged using the rewrite pop configuration at the EFP level.
  - For a single tagged packet, the tag is removed using the `rewrite ingress tag pop 1 symmetric` command at the EFP level.
  - For a double tagged packet, the tag is removed using the `rewrite ingress tag pop 2 symmetric` command at the EFP level.
  - For an untagged packet, a rewrite operation is not required.
- Only one MVR VLAN can be present in a router, and the same VLAN must be configured as the MVR VLAN for all the routers in the same network.
- Source ports must be in the MVR VLAN.
- Receiver ports of the VLAN must either have a snooping querier or a layer 3 switch virtual interfaces (SVI) to generate an IGMP query on that VLAN.
- The MVR VLAN must not be a reverse path forwarding (RPF) interface for any multicast route.
- VLAN Trunk Protocol (VTP) pruning must be disabled if the MVR VLAN number is between 1 and 1000.

Restrictions for MVR

- Do not connect a multicast router to a receiver port.
- Receiver ports can only be access ports; they cannot be trunk ports.
- MVR is available only on native systems.
- MVR cannot coexist with storm control on ES-20 ports.
- When Layer 2 port-channel is configured as MVR receiver port, multicast data traffic from MVR group is not forwarded out of the member links.
- MVR data received on an MVR receiver port cannot be forwarded to MVR source ports.
- MVR with IGMP on REP segment results in a stale entry in the IGMP snooping table when REP state changes.
- When using private VLANs, you cannot configure a primary or secondary VLAN as the MVR VLAN.
- The maximum number of multicast entries (MVR group addresses) on a router (maximum number of television channels received) is 2000.
- Receiver ports on a router can be in different VLANs, but must not be in the MVR VLAN.
Information About MVR

In a typical Layer 2 multi-VLAN network, subscribers to a multicast group can be on multiple VLANs. To maintain data isolation between these VLANs, the multicast stream on the source VLAN must be passed to a router, which replicates the stream on all subscriber VLANs, thereby wasting upstream bandwidth.

Multicast VLAN Registration (MVR) allows a Layer 2 switch to forward the multicast data from a source on a common assigned VLAN to the subscriber VLANs, conserving upstream bandwidth by bypassing the router. The switch will forward multicast data for MVR IP multicast streams only to MVR ports on which hosts have joined, either by IGMP reports or by MVR static configuration. The switch will forward IGMP reports received from MVR hosts only to the source port. MVR supports IGMPv3 messages. For other traffic, VLAN isolation is preserved.

MVR requires at least one VLAN to be designated as the common VLAN to carry the multicast stream from the source. More than one such multicast VLAN (MVR VLAN) can be configured in the system, and a global default MVR VLAN as well as interface-specific default MVR VLANs can also be configured.

MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the MVR VLAN by sending IGMP join and leave messages. IGMP leave messages from an MVR group are handled according to the IGMP configuration of the VLAN on which the leave message is received. If IGMP fast leave is enabled on the VLAN, the port is removed immediately; otherwise an IGMP query is sent to the group to determine whether other hosts are present on the port.

MVR can coexist with IGMP snooping on a router.

Using MVR in a Multicast Television Application

In a multicast television application, a Personal Computer (PC) or a television with a set-top box, can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is an EFP configured as the MVR receiver. The figure below is an example configuration. The DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to the Cisco ME 2600X Series Ethernet Access Switch to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the Cisco ME 2600X Series Ethernet
Access Switch modifies the hardware address table to include this receiver EFP and bridge-domain as a forwarding destination of the specified multicast stream when it is received from the multicast bridge-domain.

Figure 9: Multicast Bridge-Domain Registration Example

When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The Cisco ME 2600X Series Ethernet Access Switch sends a MAC-based general query through the receiver EFP bridge-domain. If there is another set-top box in the bridge-domain still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the Cisco ME 2600X Series Ethernet Access Switch does not receive a response, it eliminates the receiver EFP as a forwarding destination for this group.

If the Immediate Leave feature is enabled on a receiver EFP, the EFP leaves a multicast group quicker.
Without Immediate Leave, when the Cisco ME 2600X Series Ethernet Access Switch receives an IGMP leave message from a subscriber on a receiver EFP, it sends out an IGMP group specific query on that EFP and waits for the IGMP group membership reports. If no reports are received in the configured time period, the receiver EFP is removed from the multicast group membership.

With Immediate Leave, an IGMP query is not sent from the receiver EFP where the IGMP leave was received. As soon as the leave message is received, the receiver EFP is removed from the multicast group membership, which speeds up leave latency.

Enable the Immediate Leave feature only on receiver EFPs to which a single receiver device is connected. MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each bridge-domain. Multicast traffic for all channels is only sent around the bridge domain source EFPs—only on the multicast bridge-domain. The IGMP leave and join messages are in the bridge-domain to which the subscriber port is assigned. These messages dynamically register for streams of multicast traffic in the multicast bridge-domain on the Layer 3 device. The Cisco ME 2600X Series Ethernet Access Switch modifies the forwarding behavior to allow the traffic to be forwarded from the multicast bridge domain to the subscriber port in a different bridge-domain, thereby selectively allowing traffic to cross between the two bridge-domains.

IGMP reports are sent to the same IP multicast group address as the multicast data. The Cisco ME 2600X Series Ethernet Access Switch must capture all IGMP join and leave messages from the receiver EFPs and forward them to the multicast bridge domain of the source EFP.

How to Configure MVR

The following tasks describe how to configure MVR on the Cisco ME 2600X device:

- Enabling MVR in Global Configuration Mode, on page 173
- Enabling or Disabling MVR Source and MVR Receiver on an Interface, on page 175
- Configuring MVR Source and MVR Receiver on an Interface, on page 175

Enabling MVR in Global Configuration Mode

SUMMARY STEPS

1. enable
2. configure terminal
3. bridge-domain bridge-domain id
4. exit
5. mvr
6. mvr max-groups max-groups
7. mvr group ip-address [count count | [mask mask]]
8. mvr vlan vlan-id
9. end
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>enters the bridge-domain configuration mode.</td>
</tr>
<tr>
<td>bridge-domain bridge-domain id</td>
<td>Enters the bridge-domain configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# bridge-domain 100</td>
<td>bridge-domain id—Numerical identifier for the bridge domain instance. The range is an integer from 1 to 4096.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-bdomain)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>enables MVR globally. The no form of the command disables MVR.</td>
</tr>
<tr>
<td>mvr</td>
<td>Enables MVR globally. The no form of the command disables MVR.</td>
</tr>
<tr>
<td>Example: Switch(config)# mvr</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>specifies the maximum number of MVR groups.</td>
</tr>
<tr>
<td>mvr max-groups max-groups</td>
<td>Specifies the maximum number of MVR groups.</td>
</tr>
<tr>
<td>Example: Switch(config)# mvr max-groups 2000</td>
<td>max-groups—The number of groups can be from 1 to 2000. The default number of max-groups is 2000.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>configures an IP multicast address on the router or uses the count parameter to configure a contiguous series of MVR group addresses.</td>
</tr>
<tr>
<td>mvr group ip-address [count count] [mask mask]</td>
<td>Configures an IP multicast address on the router or uses the count parameter to configure a contiguous series of MVR group addresses.</td>
</tr>
<tr>
<td>Example: Switch(config)# mvr group 225.1.1.1 5</td>
<td>count—The range for count is 1 to (max-groups current-count); the default is 1. Any multicast data sent to this address is sent to all source ports on the router, and all receiver ports that have elected to receive data on that multicast address. Each multicast address corresponds to one television channel.</td>
</tr>
<tr>
<td></td>
<td>mask—Specifies the IP mask for MVR group addresses.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>specifies the VLAN in which multicast data is received; all source ports must belong to this VLAN.</td>
</tr>
<tr>
<td>mvr vlan vlan-id</td>
<td>Specifies the VLAN in which multicast data is received; all source ports must belong to this VLAN.</td>
</tr>
<tr>
<td>Example: Switch(config)# mvr vlan 100</td>
<td>vlan-id—The VLAN range is 1 to 1001 and 1006 to 4094. The default value is 1. Use the no form of the command to clear the MVR VLAN.</td>
</tr>
</tbody>
</table>
Enabling or Disabling MVR Source and MVR Receiver on an Interface

MVR source and MVR receiver are configured on the interface and are mapped to the efpid of the service instance created on that port.

The `mvr type {source | receiver} efpid {ethernet service instance}` command is used to configure the MVR source or receiver on the interface.

**Note**

The service instance number of the EFP created on the port where MVR receiver is configured must be same as the service instance number of the EFP created on the port where MVR source is configured.

To configure MVR source and receiver on the interface level, see Configuring MVR Source and MVR Receiver on an Interface, on page 175

Configuring MVR Source and MVR Receiver on an Interface

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `service instance id ethernet`
5. `encapsulation dot1q vlan-id`
6. `rewrite ingress tag pop {1|2} symmetric`
7. `bridge-domain bridge-domain id`
8. `exit`
9. `mvr type {source | receiver} efpid {ethernet service instance}`
10. `end`

**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.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type slot/port</td>
<td>Specifies the type and location of the interface to configure, where:</td>
</tr>
<tr>
<td>Example:</td>
<td>• type—Specifies the type of the interface.</td>
</tr>
<tr>
<td>Switch(config)# interface</td>
<td>• slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td>TenGigabitEthernet 0/4</td>
<td></td>
</tr>
<tr>
<td>Step 4 service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>• id—Integer from 1 to 4294967295 that uniquely identifies a service instance on an interface.</td>
</tr>
<tr>
<td>Switch(config-if)# service instance</td>
<td></td>
</tr>
<tr>
<td>TenGigabitEthernet 0/4</td>
<td></td>
</tr>
<tr>
<td>1 ethernet</td>
<td></td>
</tr>
<tr>
<td>Step 5 encapsulation dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td>• vlan-id—VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs.</td>
</tr>
<tr>
<td>Switch(config-if-srv)# encapsulation</td>
<td></td>
</tr>
<tr>
<td>dot1q 100</td>
<td></td>
</tr>
<tr>
<td>Step 6 rewrite ingress tag pop {1</td>
<td>2} symmetric</td>
</tr>
<tr>
<td>Example:</td>
<td>• pop {1 | 2}—One or two tags are removed from the packet. This command can be combined with a push (pop N and subsequent push vlan-id).</td>
</tr>
<tr>
<td>Switch(config-if-srv)# rewrite ingress</td>
<td>• symmetric—(Optional) A rewrite operation is applied on both ingress and egress. The operation on egress is the inverse operation as ingress.</td>
</tr>
<tr>
<td>tag pop 1 symmetric</td>
<td></td>
</tr>
<tr>
<td>Step 7 bridge-domain bridge-domain id</td>
<td>Enters the bridge-domain.</td>
</tr>
<tr>
<td>Example:</td>
<td>• bridge-domain id—Numerical identifier for the bridge domain instance. The range is an integer from 1 to 4096.</td>
</tr>
<tr>
<td>Switch(config-if-srv)# bridge-domain</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Step 8 exit</td>
<td>Exits the service instance mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-srv)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 9 mvr type {source</td>
<td>receiver}efp_id</td>
</tr>
<tr>
<td>{ethernet service instance}</td>
<td>• source—Configures uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source</td>
</tr>
</tbody>
</table>
Verifying the MVR Configuration

Use the following show commands to verify the MVR configuration:

- `show mvr receiver-ports`
- `show mvr source-ports`
- `show mvr groups`
- `show ip igmp snooping groups`
- `show ip igmp snooping querier`
- `show mvr`
- `show ip igmp snooping mrouter`

**MVR Receiver Port**

The following command displays the MVR receiver port configuration.

```
Switch# show mvr receiver-ports
```

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
<th>Status</th>
<th>Immediate Leave</th>
<th>Joins (v1,v2,v3)</th>
<th>Joins (v3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Po10</td>
<td>100</td>
<td>ACTIVE</td>
<td>/UP</td>
<td>DISABLED</td>
<td>0</td>
</tr>
<tr>
<td>Gi0/2</td>
<td>100</td>
<td>ACTIVE</td>
<td>/UP</td>
<td>DISABLED</td>
<td>0</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config-if)# mvr type source
Switch(config-if)# efp_id 1
```

- **Purpose**: All source ports on a router belong to the single multicast VLAN.
- **receiver**—Configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN. If you attempt to configure a non-MVR port with MVR configurations, the operation fails. The default configuration is as a non-MVR port.

**Step 10**

- **end**

  Returns to privileged EXEC mode.

```
Switch(config-if)# end
```

**Example:**

```
Switch(config-if)#
```
Po10 200 ACTIVE /UP DISABLED 0 0
Gi0/2 101 ACTIVE /UP DISABLED 0 0

**MVR Source Port**
The following command displays the MVR source port configuration:

```
Switch# show mvr source-ports
```

J o i n s :  v 1 , v 2 , v 3 c o u n t e r s h o w s t o t a l I G M P j o i n s
v 3 c o u n t e r s h o w s I G M P j o i n s r e c e i v e d w i t h b o t h M V R a n d n o n - M V R
g r o u p s
<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
<th>Status</th>
<th>Immediate Leave</th>
<th>Joins (v1,v2,v3)</th>
<th>Joins (v3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>1</td>
<td>ACTIVE /UP</td>
<td>DISABLED</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi0/1</td>
<td>2</td>
<td>ACTIVE /UP</td>
<td>DISABLED</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**MVR Group**
The following command displays the MVR group details:

```
Switch# show mvr groups
```

M V R m u l t i c a s t V L A N : 1
M V R m a x M u l t i c a s t G r o u p s a l l o w e d : 2000
M V R c u r r e n t m u l t i c a s t g r o u p s : 60
M V R g r o u p s :

```
224.1.1.1 224.1.1.20 count 20
225.1.1.1 225.1.1.20 count 20
229.1.1.1 229.1.1.10 count 10
230.1.1.1 230.1.1.10 count 10
```

M V R m u l t i c a s t V L A N : 2
M V R m a x M u l t i c a s t G r o u p s a l l o w e d : 2000
M V R c u r r e n t m u l t i c a s t g r o u p s : 60
M V R g r o u p s :

```
224.1.1.1 224.1.1.20 count 20
225.1.1.1 225.1.1.20 count 20
229.1.1.1 229.1.1.10 count 10
230.1.1.1 230.1.1.10 count 10
```

**Snooping**
The following command displays the snooping details:

```
Switch# show ip igmp snooping groups
```

Fl a g s : I -- I G M P s n o o p i n g , S -- S t a t i c , P -- P I M s n o o p i n g , A -- A S M m o d e
<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group/source</th>
<th>Type</th>
<th>Version</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>229.1.1.1</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.2</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.3</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.4</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.5</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.6</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.7</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.8</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.9</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
<tr>
<td>1</td>
<td>229.1.1.10</td>
<td>I</td>
<td>v3</td>
<td>Po10 G10/2</td>
</tr>
</tbody>
</table>

**Querier**

The following command displays the querier details:

Switch# `show ip igmp snooping querier`

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>IGMP Version</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12.12.12.12</td>
<td>v3</td>
<td>G10/1</td>
</tr>
</tbody>
</table>

**Generic MVR**

The following command displays the generic MVR details:

Switch# `show mvr`

MVR Running: TRUE
MVR multicast VLAN: 2
MVR Max Multicast Groups: 2000
MVR Current multicast groups: 100
MVR Global query response time: 5 (tenths of sec)

**Mrouter**

The following command displays the mrouter details:

Switch# `show ip igmp snooping mrouter`

<table>
<thead>
<tr>
<th>Vlan</th>
<th>ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>G10/1(dYNAMIC)</td>
</tr>
</tbody>
</table>

**Configuration Examples for MVR**

The following example shows how to enable MVR:

Switch> `enable`
Switch# `configure terminal`
Switch(config)# `mvr`
Switch(config)# `mvr groups 225.1.1.1 5`
Switch(config)# `bridge-domain 100`
Switch(config-bdomain)# `exit`
Switch(config)# `mvr vlan 100`
Switch(config)# `exit`
The following examples show how to configure MVR source on the interface:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface g0/4
Switch(config-if)# service instance 1 ethernet
Switch(config-if-srv)# encapsulation dot1q 100
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# exit
Switch(config-if)# mvr type source efp_id 1
Switch(config-if)# end
```

The following example shows how to configure MVR receiver on the interface:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface g0/45
Switch(config-if)# service instance 1 ethernet
Switch(config-if-srv)# encapsulation dot1q 100
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 50
Switch(config-if-srv)# exit
Switch(config-if)# mvr type receiver efp_id 1
Switch(config-if)# end
```

### Additional References for MVR

The following sections provide references related to the MVR feature.

#### Related Documents

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

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
</tbody>
</table>
### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported, and support for existing RFCs has not been modified.</td>
<td>—</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Additional References for MVR
CHAPTER 8

IGMP Snooping

This chapter describes IGMP Snooping and procedures to configure IGMP Snooping.

- Understanding IGMP Snooping, page 183
- Joining a Multicast Group, page 184
- Configuring IGMP Snooping, page 187
- Leaving a Multicast Group, page 189
- IGMP Report Suppression, page 191
- IGMP Proxy Reporting, page 199
- L2 Address Aliasing Issue, page 200
- IGMP Snooping Interaction with LAG, page 200
- IGMP Statistics and Counters, page 201
- Alarms, page 203

Understanding IGMP Snooping

As networks increase in size, multicast routing becomes critically important as a means to determine which segments require multicast traffic and which do not. IP multicasting enables IP traffic to be propagated from one source to a number of destinations, or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to the multicast group identified by a single IP destination group address.

Internet Group Management Protocol (IGMP) snooping restricts flooding of multicast traffic by sending multicast traffic only to the interfaces that are subscribed to a particular multicast group.

The Cisco ME 2600X system can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the Cisco ME 2600X system to snoop on the IGMP transmissions between the host and the device and to keep track of multicast groups and member ports. When the Cisco ME 2600X system receives an IGMP report from a host for a particular multicast group, the Cisco ME 2600X system adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table.
entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Note
For more information on IP multicast and IGMP, see RFC 1112, RFC 2236, and RFC 3376.

The Cisco ME 2600X system forwards periodic general queries received from the multicast device in the bridge domain where IGMP snooping is enabled. All hosts interested in this multicast group send join requests and are added to the forwarding table entry. The Cisco ME 2600X system creates one entry per bridge domain in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The IP multicast groups learned through IGMP snooping are dynamic.

If a port interface, EFP, and bridge domain state changes, the IGMP snooping-learned multicast groups from this port, EFP, and bridge domain in the bridge domain are deleted.

IGMP Versions
The Cisco ME 2600X system supports IGMP version 1, IGMP version 2, and IGMP version 3 on a bridge domain level. The Cisco ME 2600X system does snooping using L2 multicast address and not L3 IP address.

Note
The Cisco ME 2600X system supports IGMPv3 snooping based only on the destination multicast MAC address and not on the the source IP address or on proxy reports.

An IGMPv3 Cisco ME 2600X system provides Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when the network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv1 or IGMPv2 hosts.

Joining a Multicast Group

When a host connected to the Cisco ME 2600X wants to join an IP multicast group and it is an IGMP version 2 or version 3 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the Cisco ME 2600X receives a general query from the router, it forwards the query to all the EFPs in the bridge domain. IGMP hosts wanting to join the multicast group respond by sending a join message to the Cisco ME 2600X. The Cisco ME 2600X CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received.
to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group. See the figure below.

Figure 10: Initial IGMP Join Message

Router A sends a general query to the Cisco ME 2600X, which forwards the query to ports 2 through 5, which have EFPs configured in the same bridge domain. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. The Cisco ME 2600X CPU uses the information in the IGMP report to set up a forwarding-table entry as shown in the table below, which includes the port numbers connected to Host 1 and the router.

Table 16: IGMP Snooping Forwarding Table

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

The Cisco ME 2600X hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table enables the switching engine to send frames addressed to the 224.1.2.3 multicast IP address, which are not IGMP packets, to the router and to the host that has joined the group.

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group, as shown in the figure below, the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in the table below. Note that because the forwarding table directs IGMP messages only to the CPU,
the message is not flooded to other ports on the Cisco ME 2600X. Any known multicast traffic is forwarded
to the group and not to the CPU.

*Figure 11: Second Host Joining a Multicast Group*

![Diagram showing second host joining a multicast group]

*Table 17: Updated IGMP Snooping Forwarding Table*

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2, 5</td>
</tr>
</tbody>
</table>

*Restrictions for IGMP Snooping*

- On a Cisco ME 2600X, IGMP snooping can be configured at the bridge domain level.
- IGMP immediate-leave and IGMP report-suppression commands can be configured at the bridge domain level.
- Static multicast device can be configured at the EFP level.
- It is mandatory to untag the packets before they enter the bridge domain. This is achieved using the rewrite pop configuration at the EFP level.
- For a single tagged packet, the tag is removed using the `rewrite ingress tag pop 1 symmetric` command at the EFP level.
- For a double tagged packet, the tag is removed using the `rewrite ingress tag pop 2 symmetric` command at the EFP level.
- For an untagged packet, a rewrite operation is not required.
- Maximum bridge domains supported are 128, with a maximum of 2000 per group.
Configuring IGMP Snooping

To configure IGMP snooping, complete the following procedures:

1. Enabling or Disabling IGMP Snooping, on page 187
2. Complete the following tasks as necessary:
   - Enabling or Disabling IGMP Immediate Leave, on page 190
   - Disabling IGMP Report Suppression, on page 192
   - Configuring a Static Multicast Port, on page 193
3. (Optional) Viewing IGMP Configuration, on page 195

Enabling or Disabling IGMP Snooping

**SUMMARY STEPS**

1. enable
2. configure terminal
3. bridge domain bridge-domain value
4. [no] ip igmp snooping
5. end
6. 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></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>bridge domain bridge-domain value</td>
<td>Enters the bridge domain.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# bridge-domain 22</td>
<td></td>
</tr>
</tbody>
</table>
Enabling or Disabling IGMP Snooping

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] ip igmp snooping</td>
<td>Enables IGMP snooping on the bridge-domain. The <code>no</code> form of the command disables this function.</td>
</tr>
</tbody>
</table>

**Step 4**

**Example:**

```
Switch(config-bdomain)# ip igmp snooping
```

**Step 5**

**Example:**

```
Switch(config-bdomain)# end
```

**Step 6**

**Example:**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

**Examples:**

The following example shows how to enable IGMP snooping on untagged Ethernet traffic on the bridge domain and how to configure the source and host ports:

**Configuration on the bridge-domain**

```
Switch(config)# bridge-domain 30
Switch(config-bdomain)# ip igmp snooping
```

**Configuration on port 1**

```
Switch(config)# interface gi 0/1
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation untagged
Switch(config-if-srv)# bridge-domain 30
```

**Configuration on port 2**

```
Switch(config)# interface gi 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation untagged
Switch(config-if-srv)# bridge-domain 30
```

**Configuration on port 3**

```
Switch(config)# interface gi 0/10
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation untagged
Switch(config-if-srv)# bridge-domain 30
```

The following example shows how to enable IGMP snooping on single and double tagged Ethernet traffic on the bridge domain and how to configure the source and host ports:

**Configuration on the bridge-domain**

```
Switch(config)# bridge-domain 30
Switch(config-bdomain)# ip igmp snooping
```

**Configuration on port 1**

```
Switch(config)# interface gi 0/1
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 50 second-dot1q 10
Switch(config-if-srv)# rewrite ingress pop 2 symmetric
Switch(config-if-srv)# bridge-domain 30
```
The following example shows how to enable IGMP snooping on double tagged Ethernet traffic on the bridge domain and how to configure the source and host ports:

**Configuration on the bridge-domain**

```
Switch(config)# bridge-domain 30
Switch(config-bdomain)# ip igmp snooping
```

**Configuration on port 1**

```
Switch(config)# interface gi 0/1
Switch(config-if)# service instance 10 ethernet
Switch(config-if-serv)# encapsulation dot1q 10 second-dot1q 20
Switch(config-if-serv)# rewrite ingress pop 2 symmetric
Switch(config-if-serv)# bridge-domain 30
```

**Configuration on port 2**

```
Switch(config)# interface gi 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-serv)# encapsulation dot1q 100 second-dot1q 20
Switch(config-if-serv)# rewrite ingress pop 2 symmetric
Switch(config-if-serv)# bridge-domain 30
```

**Configuration on port 3**

```
Switch(config)# interface gi 0/6
Switch(config-if)# service instance 10 ethernet
Switch(config-if-serv)# encapsulation dot1q 101 second-dot1q 20
Switch(config-if-serv)# rewrite ingress pop 2 symmetric
Switch(config-if-serv)# bridge-domain 30
```

**What to Do Next**

**Verification**

To verify if the IGMP snooping is enabled on the Ethernet traffic, run the following command:

```
show ip igmp snooping vlan 30
```

## Leaving a Multicast Group

The router sends periodic multicast general queries, and the Cisco ME 2600X system forwards these queries through all ports in the bridge domain. Interested hosts respond to the queries. If at least one host in the bridge domain wants to receive multicast traffic, the router continues forwarding the multicast traffic to the bridge domain. The Cisco ME 2600X system forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.

When hosts want to leave a multicast group, they can leave without sending a message, or they can send a leave message. When the Cisco ME 2600X system receives a leave message from a host, it sends a group-specific query to learn if any other devices connected to that interface are interested in traffic for the specific multicast group. The Cisco ME 2600X system then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table.
If the router receives no reports from a bridge domain, it removes the group for the bridge domain from its IGMP cache.

**Immediate Leave**

The Immediate Leave feature is only supported on IGMP version 2 hosts. The Cisco ME 2600X system uses IGMP Snooping Immediate Leave feature to remove an interface from the forwarding table, which sends a leave message without the Cisco ME 2600X system sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. The Immediate Leave feature ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

---

*Note*

You should only use the Immediate Leave feature on bridge domains where a single host is connected to each port. If this feature is enabled on bridge domains where more than one host is connected to a port, some hosts might get dropped.

---

**Enabling or Disabling IGMP Immediate Leave**

When you enable the IGMP Immediate Leave feature, the Cisco ME 2600X system immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate Leave feature only when there is a single receiver present on every port in the bridge domain.

---

*Note*

The Immediate Leave feature is supported only on IGMP version 2 hosts.

---

**Prerequisite**

Enabling or Disabling IGMP Snooping, on page 187

---

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `bridge domain bridge-domain value`
4. `[no] ip igmp snooping immediate-leave`
5. `end`
6. `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.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>* Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters the bridge domain configuration mode.</td>
</tr>
<tr>
<td><code>bridge domain bridge-domain value</code></td>
<td>• Enter the value of the bridge domain.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>bridge-domain 22</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables the IGMP Immediate Leave feature on the bridge domain. The <code>no</code> form of the command disables this function.</td>
</tr>
<tr>
<td><code>[no] ip igmp snooping immediate-leave</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-bdomain)# <code>ip igmp snooping immediate-leave</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-bdomain)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

To disable the IGMP Immediate Leave feature on a bridge domain, use the `no ip igmp snooping immediate-leave` in the bridge-domain configuration mode.

**Examples:**
The following example shows how to enable IGMP Immediate Leave feature for bridge-domain130:

```
Switch# `configure terminal` 
Switch(config)# `bridge-domain 130` 
Switch(config-bdomain)# `ip igmp snooping immediate-leave` 
Switch(config-bdomain)# `end`
```

**IGMP Report Suppression**

**Note**  
IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The Cisco ME 2600X system uses IGMP report suppression to forward only one IGMP report per multicast query, to multicast devices. When IGMP suppression is enabled (the default), the Cisco ME 2600X system sends the first IGMP report from all hosts for a group, to all the multicast devices. The Cisco ME 2600X
Disabling IGMP Report Suppression

**Note**
IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

IGMP report suppression is enabled by default. When it is enabled, the Cisco ME 2600X system forwards only one IGMP report per multicast query. When report suppression is disabled, all IGMP reports are forwarded to the multicast devices. To re-enable IGMP report suppression, use the `ip igmp snooping report-suppression` command in the bridge domain configuration mode.

**Prerequisite**
Enabling or Disabling IGMP Snooping, on page 187

**SUMMARY STEPS**

1. enable
2. configure terminal
3. bridge domain *bridge-domain value*
4. no ip igmp snooping report-suppression
5. end
6. 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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 3**

Enter the bridge domain configuration mode.

Example:

```bash
Switch(config)# bridge-domain 22
```

**Purpose**

- Enters the bridge domain configuration mode.

**Step 4**

Disables IGMP report suppression.

Example:

```bash
Switch(config-bdomain)# no ip igmp snooping report-suppression
```

**Step 5**

Returns to the privileged EXEC mode.

Example:

```bash
Switch(config-bdomain)# end
```

**Step 6**

(Optional) Saves your entries in the configuration file.

Example:

```bash
Switch# copy running-config startup-config
```

### Examples:

The following example shows how to re-enable IGMP report suppression for bridge-domain 130:

```bash
Switch# configure terminal
Switch(config-bdomain)# bridge-domain 130
Switch(config-bdomain)# ip igmp snooping report-suppression
Switch(config-bdomain)# end
```

### Configuring a Static Multicast Port

To add a static connection to a multicast port, use the `ip igmp snooping mrouter` EFP configuration command on the Cisco ME 2600X system. To remove a static multicast port from the bridge domain, use the `no ip igmp snooping mrouter` configuration command.

**Note**

Static connections to multicast devices are supported only at the EFP.

**Prerequisite**

Enabling or Disabling IGMP Snooping, on page 187
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. service instance id ethernet
5. encapsulation dot1q id
6. rewrite ingress tag pop 1 symmetric
7. bridge domain bridge-domain value
8. [no] ip igmp snooping mrouter
9. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Specifies the type and location of the interface to configure, where:</td>
</tr>
<tr>
<td>Example: Switch(config)# interface TenGigabitEthernet 0/45</td>
<td>• type—Specifies the type of interface.</td>
</tr>
<tr>
<td></td>
<td>• slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td>The interface can be a physical interface or a port channel. The port-channel range is 1 to 128.</td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# service instance 10 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q id</td>
<td>Defines the encapsulation format as IEEE 802.1Q (dot1q) and specifies the identifier. The identifier indicates the CVLAN with which the packet is received on the interface.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# encapsulation dot1q 10</td>
<td>• Enter the value of the identifier.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 6**

`rewrite ingress tag pop 1 symmetric`

*Example:*

```
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
```

Specifies the rewrite operation.

**Step 7**

`bridge domain bridge-domain value`

*Example:*

```
Switch(config-if-srv)# bridge-domain 22
```

Specifies the multicast bridge domain ID. The bridge domain ID range is from 1 to 16384

- Enter the value of the bridge domain.

**Step 8**

`[no] ip igmp snooping mrouter`

*Example:*

```
Switch(config-if-srv)# ip igmp snooping mrouter
```

Adds a static connection to the multicast device. The `no` form of the command removes the static multicast port from the bridge domain.

**Step 9**

`end`

*Example:*

```
Switch(config-if-srv)# end
```

Returns to the privileged EXEC mode.

### Examples:

The following example shows how to enable a static connection to a multicast device:

```
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# service instance 20 ethernet
Switch(config-if-srv)# encapsulation dot1q 10
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 20
Switch(config-if-srv)# ip igmp snooping mrouter
```

The following example shows how to disable a static connection to a multicast device:

```
Switch(config)# interface TenGigabitEthernet 0/45
Switch(config-if)# service instance 20 ethernet
Switch(config-if-srv)# no ip igmp snooping mrouter
```

### Viewing IGMP Configuration

**SUMMARY STEPS**

1. `enable`
2. `show ip igmp snooping [groups [count | vlan bridge-domain ID [ ip-address | count | dynamic [count] | user [count] ]] | mrouter [vlan bridge-domain ID] querier | vlan bridge-domain ID]`
3. `show ip igmp snooping querier [vlan bridge-domain ID ]`
### 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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show ip igmp snooping [groups [count</td>
<td>vlan bridge-domain ID [ip-address [count</td>
</tr>
<tr>
<td>Example: Switch# show ip igmp snooping vlan 22</td>
<td>• groups—(Optional) Displays group information.</td>
</tr>
<tr>
<td></td>
<td>• count—(Optional) Displays the number of multicast groups learned by IGMP snooping.</td>
</tr>
<tr>
<td></td>
<td>• vlan bridge-domain ID—(Optional) Specifies a bridge domain.</td>
</tr>
<tr>
<td></td>
<td>• bridge-domain ID— Bridge domain ID. Valid values are from 1 to 16384.</td>
</tr>
<tr>
<td></td>
<td>• ip-address—(Optional) Displays information about the specified group.</td>
</tr>
<tr>
<td></td>
<td>• count—(Optional) Displays the group count inside a bridge domain.</td>
</tr>
<tr>
<td></td>
<td>• dynamic—(Optional) Displays dynamic entries learned through IGMP snooping.</td>
</tr>
<tr>
<td></td>
<td>• count—(Optional) Displays the number of dynamic entries.</td>
</tr>
<tr>
<td></td>
<td>• user—(Optional) Displays only the user-configured multicast entries.</td>
</tr>
<tr>
<td></td>
<td>• count—(Optional) Displays the number of user-configured multicast entries.</td>
</tr>
<tr>
<td></td>
<td>• mrouter—(Optional) Displays information about dynamically learned and manually configured multicast ports.</td>
</tr>
<tr>
<td></td>
<td>• querier—(Optional) Displays IGMP querier information.</td>
</tr>
<tr>
<td><strong>Step 3</strong> show ip igmp snooping querier [vlan bridge-domain ID ]</td>
<td>Displays information about the IP address and the receiving port for the recently received IGMP query messages.</td>
</tr>
<tr>
<td>Example: Switch# show ip igmp snooping querier vlan 22</td>
<td>• vlan bridge-domain ID —(Optional) Specifies a bridge domain.</td>
</tr>
<tr>
<td></td>
<td>• bridge-domain ID— Bridge domain ID. Valid values are from 1 to 16384.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the output of the **show ip igmp snooping [vlan bridge-domain ID]** command.

Switch# show ip igmp snooping vlan 2
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression : Enabled
TCN solicit query : Disabled
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000
Check TTL=1 : No
Check Router-Alert-Option : No

Vlan 2
-----------------------
IGMP snooping Admin State : Enabled
IGMP snooping Oper State : Enabled
IGMPv2 immediate leave : Disabled
Report suppression : Enabled
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000
Check TTL=1 : Yes
Check Router-Alert-Option : Yes
Query Interval : 0
Max Response Time : 10000

The following example displays the output of the `show ip igmp snooping groups` command.

Switch# show ip igmp snooping groups

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group/source</th>
<th>Type</th>
<th>Version</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>225.10.10.10</td>
<td>I</td>
<td>v2</td>
<td>Te0/45</td>
</tr>
</tbody>
</table>

The following example displays the output of the `show ip igmp snooping groups count` command.

Switch# show ip igmp snooping groups count

Total number of groups: 1

The following example displays the output of the `show ip igmp snooping groups dynamic` command.

Switch# show ip igmp snooping groups dynamic

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group/source</th>
<th>Type</th>
<th>Version</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>225.10.10.10</td>
<td>I</td>
<td>v2</td>
<td>Te0/45</td>
</tr>
</tbody>
</table>

The following example displays the output of the `show ip igmp snooping groups dynamic count` command.

Switch# show ip igmp snooping groups dynamic count

Total number of groups: 1

The following example displays the output of the `show ip igmp snooping groups user` command.

Switch# show ip igmp snooping groups user
The following example displays the output of the `show ip igmp snooping groups user count` command.

```
Switch# show ip igmp snooping groups user count
Total number of groups: 1
```

The following example displays the output of the `show ip igmp snooping groups vlan` command.

```
Switch# show ip igmp snooping groups vlan 22

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
Vlan Group/source Type Version Port List
-------------------------- -------------------- ---- ----- -------
22 225.10.10.10 I v2 Te0/45
```

The following example displays the output of the `show ip igmp snooping groups vlan bridge-domain ID [ip_address]` command.

```
Switch# show ip igmp snooping groups vlan 22 225.10.10.10

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
Vlan Group/source Type Version Port List
-------------------------- -------------------- ---- ----- -------
22 225.10.10.10 I v2 Te0/45
```

The following example displays the output of the `show ip igmp snooping groups vlan bridge-domain ID [count]` command.

```
Switch# show ip igmp snooping groups vlan 22 count
Total number of groups in Bridge-Domain Index 22: 1
```

The following example displays the output of the `show ip igmp snooping groups vlan bridge-domain ID [dynamic]` command.

```
Switch# show ip igmp snooping groups vlan 22 dynamic

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
Vlan Group/source Type Version Port List
-------------------------- -------------------- ---- ----- -------
22 225.10.10.10 I v2 Te0/45
```

The following example displays the output of the `show ip igmp snooping groups vlan bridge-domain ID [dynamic count]` command.

```
Switch# show ip igmp snooping groups vlan 22 dynamic count
Total number of groups in Bridge-Domain Index 22: 1
```

The following example displays the output of the `show ip igmp snooping groups vlan bridge-domain ID [user]` command.

```
Switch# show ip igmp snooping groups vlan 22 user
```
Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan | Group/source | Type | Version | Port List
-----|--------------|------|---------|-------------------
22  | 225.10.10.10 | I    | v2      | Te0/45

The following example displays the output of the `show ip igmp snooping mrouter` command.

Switch# `show ip igmp snooping mrouter`

Vlan | ports
-----|-----
2   | Te0/45(dynamic)

The following example displays the output of the `show ip igmp snooping mrouter vlan 2` command.

Switch# `show ip igmp snooping mrouter vlan 2`

Vlan | ports
-----|-----
2   | Te0/45(dynamic)

The following example shows the output of the `show ip igmp snooping querier` command.

Switch# `show ip igmp snooping querier`

Vlan | IP Address | IGMP Version | Port
-----|------------|--------------|-----
2   | 10.10.10.1  | v2           | Te0/45

The following example shows the output of the `show ip igmp snooping querier [vlan bridge-domain ID]` command.

Switch# `show ip igmp snooping querier vlan 22`

IP address : 1.1.1.1
IGMP version : v2
Port : Gi0/41
Max response time : 10s

**IGMP Proxy Reporting**

IGMP supports proxy reporting for IGMPv1 and IGMPv2 messages to handle group-specific queries. These queries are not sent downstream, but the Cisco ME 2600X system does respond to them directly. When the Cisco ME 2600X system receives a group-specific query, the Cisco ME 2600X system terminates the query and sends an IGMP proxy report if there is a receiver for the group. There is no proxy reporting for IGMPv3 messages. For IGMPv3, a group-specific query or a group source-specific query is flooded to all VLAN member ports. The database for the IGMPv3 membership report is built based on the reports received.

Host reports responding to a specific query can be suppressed by the report suppression feature. Report suppression is supported for IGMPv1, IGMPv2 and IGMPv3 messages. With report suppression enabled (by default), when the Cisco ME 2600X system receives a general query, the Cisco ME 2600X system starts a suppression cycle for reports from all hosts to each group or channel. Only the first report to the discovered multicast devices are forwarded; the rest of the reports are suppressed. For IGMPv1 and IGMPv2, the time of suppression is the report response time indicated in the general query message. For IGMPv3, suppression occurs for the entire general query interval.
• Source-based filtering for IGMP version 3 reports is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection. The source-only entries are deleted every 5 minutes and relearned to ensure that they are still valid.

• Turning off explicit host tracking disables fast-leave processing and proxy reporting.

L2 Address Aliasing Issue

The IGMP snooping forwarding table is based on L2 address. Since multiple IP addresses can map to the same L2 address, an L2 address aliasing can occur. For example, IP addresses 225.1.1.1 and 226.1.1.1 map to the same MAC address 01005E010101 which results in L2 address aliasing.

IGMP Snooping Interaction with LAG

A link aggregation (LAG) interface can be added to a bridge domain, which has IGMP snooping enabled.

The following example shows how to configure the source port, which is part of the LAG interface that is a member of the bridge domain that has IGMP snooping enabled.

Configuration on the bridge-domain

Switch(config)# bridge-domain 30
Switch(config-bdomain)# ip igmp snooping

Configuration on port 1

Switch(config)# interface port-channel 10
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 10
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 30
Switch(config)# interface gi0/25
Switch(config-if)# channel-group 10
Switch(config)# interface gi0/26
Switch(config-if)# channel-group 10

Configuration on port 2

Switch(config)# interface gi0/1
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 20 second-dot1q 30
Switch(config-if-srv)# rewrite ingress pop 2 symmetric
Switch(config-if-srv)# bridge-domain 30

Configuration on port 3

Switch(config)# interface gi0/2
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 40
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 30

The following example shows how to configure the receiver port, which is part of the LAG interface that is a member of the bridge domain that has IGMP snooping enabled.

Configuration on the bridge-domain

Switch(config)# bridge-domain 30
Switch(config-bdomain)# ip igmp snooping
Configuration on port 1

Switch(config)# interface ten 0/45
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 10 second-dot1q 30
Switch(config-if-srv)# rewrite ingress pop 2 symmetric
Switch(config-if-srv)# bridge-domain 30

Configuration port 2

Switch(config)# interface port-channel 10
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 10
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 30
Switch(config-if)# interface gi0/25
Switch(config-if)# channel-group 10
Switch(config-if)# interface gi0/26
Switch(config-if)# channel-group 10

Configuration on port 3

Switch(config)# interface gi0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 40
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 30

IGMP Statistics and Counters

An entry in a counter contains multicasting statistical information for the IGMP snooping capable Cisco ME 2600X system. The equivalent IOS command to retrieve statistical information is `show ip igmp snooping counters`.

This information can be stored in the following counters:

- **Tx General Queries**—Number of general queries transmitted through an interface.
- **Tx Group Specific Queries**—Total group specific queries transmitted through an interface.
- **Tx Reports**—Total membership reports transmitted through an interface.
- **Tx Leaves**—Total leave messages transmitted through an interface.
- **Rx General Queries**—Total general queries received at an interface.
- **Rx Group Specific Queries**—Total group specific queries received at an interface.
- **Rx Reports**—Total membership reports received at an interface.
- **Rx Leaves**—Total leave messages received at an interface.
- **Rx Valid Packets**—Total valid IGMP packets received at an interface.
- **Rx Invalid Packets**—Total number of invalid IGMP packets that are received at an interface.

The following example shows the statistical information using the `show ip igmp snooping counters` command.

```
Switch> show ip igmp snooping counters
packet queue maximum size: 20000
packet queue current size: 0
packet queue peak size: 0
packet queue drop count: 0
```
### Vlan 1

#### IGMP Snooping Counters

Overall there are 15 counters

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Ovr</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX processed Query Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed Group Specific Query</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed Join</td>
<td>787120</td>
<td></td>
</tr>
<tr>
<td>RX processed Leave</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed Total Valid Packets</td>
<td>782</td>
<td></td>
</tr>
<tr>
<td>RX processed Other Packets</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX Packets dropped for sanity errors</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX Packets dropped for checksum errors</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX Packets dropped for header length errors</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX Packets dropped for other errors</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed Topology change notification</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

#### IGMP Snooping V3 Counters

Overall there are 18 counters

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Ovr</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX processed V3 ALLOW NEW</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed V3 BLOCK OLD</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed V3 MODE IS INCLUDE</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed V3 MODE IS EXCLUDE</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed V3 CHANGE TO INCLUDE</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed V3 CHANGE TO EXCLUDE</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RX processed V3 Query</td>
<td>782</td>
<td></td>
</tr>
</tbody>
</table>
## Alarms

The MCAST-MAC-TABLE-FULL condition is raised from IGMP snooping at Cisco ME 2600X. The Cisco ME 2600X supports a maximum of 2000 multicast groups. The MCAST-MAC-TABLE-FULL condition is raised when the multicast table is full and a new join request is received. This table is cleared when at least one entry gets cleared from the multicast table after the alarm is raised.
Alarms
Remote Network Monitoring and Alarm Troubleshooting

This chapter describes remote network monitoring (RMON) and alarm troubleshooting.

- RMON Procedures, page 205
- Understanding RMON, page 205
- Alarm Troubleshooting, page 208

RMON Procedures

To configure RMON using Cisco IOS commands, complete the following procedures:

- Configuring RMON Settings, on page 206
- Displaying RMON Status, on page 207

Understanding RMON

RMON is a standard monitoring feature that allows various network agents and console systems to exchange network monitoring data. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information. You can use the RMON feature with the Simple Network Management
Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments as shown in the figure below.

*Figure 12: Remote Monitoring Example*

![Remote Monitoring Example Diagram](image)

**Default RMON Configuration**

RMON is disabled by default; no alarms or events are configured.

**Configuring RMON Settings**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. rmon alarm number variable interval {delta | absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]
4. rmon event number [log] [trap community] [description string] [owner string]
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
---|---
Example: Switch# enable | • Enter your password if prompted.
Step 2 configure terminal | Enters global configuration mode.
Example: Switch# configure terminal | Sets a RMON alarm on a MIB object.
Step 3 rmon alarm number variable interval {delta | absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string] | This example configures RMON alarm number 10. The alarm monitors the MIB variable ifEntry.20.1 once every 20 seconds until the alarm is disabled, and checks the change in the rise or fall of the variable. If the ifEntry.20.1 value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the rmon event command. The possible events include a log entry or an SNMP trap. If the ifEntry.20.1 value changes by 0, the alarm is reset and can be triggered again.
Example: Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner user1 | Sets a RMON alarm on a MIB object.
Step 4 rmon event number [log] [trap community] [description string] [owner string] | Adds or removes an event in the RMON event table that is associated with an RMON event number.
Example: Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner user | Adds or removes an event in the RMON event table that is associated with an RMON event number.
Step 5 exit | Exits configuration mode.
Example: Switch(config)# exit | Exits configuration mode.

Displaying RMON Status

To display the current RMON agent status on the device, use one or more of the privileged EXEC commands described in Table 18: Commands for Displaying RMON Status, on page 207.

Table 18: Commands for Displaying RMON Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon alarms</td>
<td>Displays the RMON alarm table.</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays the RMON event table.</td>
</tr>
</tbody>
</table>
Alarm Troubleshooting

This section gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ME 2600X alarm and condition.

FMEA FAN Alarm

Default Severity: Critical (CR), Service-Affecting (SA)
This alarm gets raised when a power failure has encountered in any of the fan modules.

Precondition:
Make sure FMEA is enabled on Cisco ME 2600X. If not issue ‘fmea enable 1’ on Cisco ME 2600X.

Clearing the FMEA FAN Alarm

SUMMARY STEPS

1. Check all connections are intact inside the module and replace the fan module.

DETAILED STEPS

Check all connections are intact inside the module and replace the fan module.
Sample output for FMEA:

```
Fault Desc:FAN.01:FAN alarm with Timestamp:14:04:23 UTC 2012-11-28
```

To view the last occurrence of FMEA alarm:

```
Switch# fmea alarms
```

```
Alarm raised:Count:1 Index:23=>FAN.01:FAN alarm
```

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MAC-BD-LIMT-REACHED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)
The MAC Bridge Domain Limit Reached (MAC-BD-LIMT-REACHED) alarm is raised when the MAC address learnt on the bridge domain has reached a limit of 32,000.
Clearing the MAC-BD-LIMT-REACHED Alarm

SUMMARY STEPS

1. Reduce the MAC address size on the bridge domain.

DETAILED STEPS

Reduce the MAC address size on the bridge domain. If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MAC-SYS-LIMT-REACHED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

The MAC System Limit Reached (MAC-SYS-LIMT-REACHED) alarm is raised when the system MAC address limit of 32,000 is reached.

Clearing the MAC-SYS-LIMT-REACHED Alarm

SUMMARY STEPS

1. Reduce the system MAC address size to less than 32,000.

DETAILED STEPS

Reduce the system MAC address size to less than 32,000. If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).
Authentication, Authorization, and Accounting (AAA)

This chapter describes Authentication, Authorization, and Accounting (AAA).

- AAA Overview, page 212
- Configuring Authentication, page 217
- AAA Authentication Methods Configuration Task List, page 219
- Non-AAA Authentication Methods, page 228
- Authentication Examples, page 231
- Configuring Authorization, page 233
- Named Method Lists for Authorization, page 233
- AAA Authorization Methods, page 234
- Method Lists and Server Groups, page 235
- AAA Authorization Types, page 235
- AAA Authorization Prerequisites, page 236
- AAA Authorization Configuration Task List, page 236
- Authorization Attribute-Value Pairs, page 239
- Authorization Configuration Examples, page 239
- Configuring Accounting, page 241
- Named Method Lists for Accounting, page 241
- AAA Session MIB, page 244
- AAA Accounting Prerequisites, page 245
- AAA Accounting Configuration Task List, page 246
- Accounting Attribute-Value Pairs, page 248
- Accounting Configuration Examples, page 248
Access control is the way you control who is allowed access to the network server and what services the security services provide the primary framework through which you set up access control on your device or access server.

About AAA Security Services

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

• **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

  Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

  All authentication methods, except for line password and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, see Configuring Authentication, on page 217.

• **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP and Telnet.

  AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user’s actual capabilities and restrictions. The database can be located locally on the device or access server or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

  As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces. For information about configuring authorization using AAA, see Configuring Authorization, on page 233.

• **Accounting**—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times.

  Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting
AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces. For information about configuring accounting using AAA, see Configuring Accounting, on page 241.

In many circumstances, AAA uses protocols such as RADIUS or TACACS+ to administer its security functions. If your device or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+ security server.

Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA, such as line password authentication and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS and TACACS+
- Multiple backup systems

AAA Philosophy

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

For information about applications that use AAA, such as per-user configuration and virtual profiles, see the chapters “Configuring Per-User Configuration” and “Configuring Virtual Profiles” in the Cisco IOS Dial Technologies Configuration Guide, Release 12.2.

Method Lists

A method list is a sequential list that defines the authentication methods used to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, Cisco IOS software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.
Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers.

**Figure 13: Typical AAA Network Configuration**

Suppose the system administrator has defined a method list where R1 is contacted first for authentication information, then R2, T1, T2, and finally the local username database on the access server itself. When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated. If all of the authentication methods return errors, the network access server will process the session as a failure, and the session is terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.
Where to Begin

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack. Cisco recommends that you use AAA, no matter how minor your security needs might be.

Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco device or access server using AAA, follow this process:

• Enable AAA by using the `aaa new-model` global configuration command.

  **Note** Once enabled AAA cannot be disabled.

• If you decide to use a separate security server, configure security protocol parameters, such as RADIUS and TACACS+.

• Define the method lists for authentication by using an AAA authentication command.

• Apply the method lists to a particular interface or line, if required.

• (Optional) Configure authorization using the `aaa authorization` command.

• (Optional) Configure accounting using the `aaa accounting` command.

For a complete description of the commands used in this chapter, see the chapter “Authentication Commands” of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Enabling AAA

Before you can use any of the services AAA network security services provide, you must enable AAA.

To enable AAA, perform the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
What to Do Next

Once you have enabled AAA, you are ready to configure the other elements relating to your selected security solution. The table below describes AAA configuration tasks and where to find more information.

Table 19: AAA Access Control Security Solutions Methods

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring local login authentication</td>
<td>Configuring Authentication, on page 217</td>
</tr>
<tr>
<td>Controlling login using security server</td>
<td>Configuring Authentication, on page 217</td>
</tr>
<tr>
<td>authentication</td>
<td>Configuring Authentication, on page 217</td>
</tr>
<tr>
<td>Defining method lists for authentication</td>
<td>Configuring Authentication, on page 217</td>
</tr>
<tr>
<td>Applying method lists to a particular</td>
<td>Configuring Authentication, on page 217</td>
</tr>
<tr>
<td>interface or line</td>
<td>Configuring Authentication, on page 217</td>
</tr>
<tr>
<td>Configuring RADIUS security protocol parameters</td>
<td>Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263</td>
</tr>
<tr>
<td>Configuring TACACS+ security protocol</td>
<td>TACACS+ Configuration Task List, on page 261</td>
</tr>
<tr>
<td>parameters</td>
<td></td>
</tr>
<tr>
<td>Enabling TACACS+ authorization</td>
<td>Configuring Authorization, on page 233</td>
</tr>
<tr>
<td>Enabling accounting</td>
<td>Configuring Accounting, on page 241</td>
</tr>
</tbody>
</table>

If you have elected not to use the AAA security services, see Configuring Authentication, on page 217 for the non-AAA configuration task “Configuring Login Authentication.”
Configuring Authentication

Authentication verifies users before they are allowed access to the network and network services. The Cisco IOS software implementation of authentication is divided into two main categories:

- AAA Authentication Methods Configuration Task List, on page 219
- Non-AAA Authentication Methods, on page 228

Authentication, for the most part, is implemented through the AAA security services. Cisco recommends that, whenever possible, AAA be used to implement authentication.

This chapter describes both AAA and non-AAA authentication methods. For authentication configuration examples, see Authentication Examples, on page 231. For a complete description of the AAA commands used in this chapter, see the "Authentication, Authorization, and Accounting (AAA)" part of the Cisco IOS Security Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature, or see the software release notes for a specific release.

Named Method Lists for Authentication

To configure AAA authentication, you must first define a named list of authentication methods, and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first listed method to authenticate users. If that method fails to respond, the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted.

It is important to note that the Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are
RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS server. T1 and T2 make up the group of TACACS+ servers.

**Figure 14: Typical AAA Network Configuration**

![Typical AAA Network Configuration Diagram]

Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as a server group, and define T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for login authentication.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263 or TACACS+ Configuration Task List, on page 261.

**Method List Examples**

Suppose the system administrator has decided on a security solution where all interfaces will use the same authentication methods to authenticate login connections. In the RADIUS group, R1 is contacted first for authentication information, then if there is no response, R2 is contacted. If R2 does not respond, T1 in the TACACS+ group is contacted; if T1 does not respond, T2 is contacted. If all designated servers fail to respond, authentication falls to the local username database on the access server itself. To implement this solution, the system administrator would create a default method list by entering the following command:

```
aaa authentication login default group radius group tacacs+ local
```
In this example, "default" is the name of the method list. The protocols included in this method list are listed after the name, in the order they are to be queried. The default list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern would continue through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

It is important to remember that a FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

In the following example, the system administrator uses server groups to specify that only R2 and T2 are valid servers for login authentication. To perform this task, the administrator must define specific server groups whose members are R2 (172.16.2.7) and T2 (172.16.2.77), respectively. In this example, the RADIUS server group "rad2only" is defined as follows using the `aaa group server` command:

```bash
group server radius rad2only
    server-private 172.16.2.7 key helloworld
```

The TACACS+ server group "tac2only" is defined as follows using the `aaa group server` command:

```bash
group server tacacs tac2only
    server-private 172.16.2.77 key cisco
```

The administrator then applies login authentication using the server groups. In this example, the default methods list for login authentication follows this order: group rad2only, group tac2only, and local:

```bash
aaa authentication login default group rad2only group tac2only local
```

### AAA Authentication General Configuration Procedure

To configure AAA authentication, perform the following tasks:

- Enable AAA by using the `aaa new-model` global configuration command. For more information about configuring AAA, see **AAA Overview**, on page 212.

- Configure security protocol parameters, such as RADIUS or TACACS+ if you are using a security server. For more information about RADIUS, see **Configuring Cisco ME 2600X to RADIUS Server Communication**, on page 263. For more information about TACACS+, see **TACACS+ Configuration Task List**, on page 261.

- Define the method lists for authentication by using an AAA authentication command.

- Apply the method lists to a particular interface or line, if required.

### AAA Authentication Methods Configuration Task List

This section discusses the following AAA authentication methods:

- Configuring Login Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Changing the Text Displayed at the Password Prompt
Configuring Message Banners for AAA Authentication

Note
AAA features are not available for use until you enable AAA globally by issuing the `aaa new-model` command. For more information about enabling AAA, see AAA Overview, on page 212.

For authentication configuration examples using the commands in this chapter, see Authentication Examples, on page 231.

## Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the `aaa authentication login` command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the `aaa authentication login` command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the `login authentication` line configuration command.

To configure login authentication using AAA, complete the following steps:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login {default | list-name} method1 [method2...]`
5. `line {aux | console | tty | vty} line-number [ending-line-number]`
6. `login authentication {default | list-name}`
7. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
**Example:**  
Switch> enable  
• Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
**Example:**  
Switch# configure terminal |
| **Step 3** aaa new-model | Enables AAA globally.  
**Example:**  
Switch(config)# aaa new-model |
### Configuring Login Authentication Using AAA

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authentication login {default</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authentication login test local</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>line [aux</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# line vty 0</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>login authentication {default</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-line)# login authentication test</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-line)# end</td>
</tr>
</tbody>
</table>

The list-name is a character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, use the following command:

```shell
aaa authentication login default group tacacs+ none
```

**Note**

Because the **none** keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

The table below lists the supported login authentication methods.

### Table 20: AAA Authentication Login Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>
Configuring Login Authentication Using AAA

Use the list of all RADIUS servers for authentication.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.</td>
</tr>
</tbody>
</table>

The `login` command only changes username and privilege level but does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the device (loop-back). Make sure that the device has been configured for secure Telnet sessions if you choose to implement autocommands this way.

## Login Authentication Using Enable Password

Use the `aaa authentication login` command with the `enable method` keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default enable
```

Before you can use the enable password as the login authentication method, you need to define the enable password. For more information about defining enable passwords, see Configuring Passwords on Cisco ME 2600X, on page 5.

## Login Authentication Using Line Password

Use the `aaa authentication login` command with the `line method` keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you need to define a line password. For more information about defining line passwords, see Configuring Line Password Protection, on page 228.

## Login Authentication Using Local Password

Use the `aaa authentication login` command with the `local method` keyword to specify that the Cisco device or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default local
```

For information about adding users into the local username database, see Establishing Username Authentication, on page 230.
Login Authentication Using Group RADIUS

Use the `aaa authentication login` command with the `group radius` method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, use the following command:

```bash
aaa authentication login default group radius
```

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, see Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263.

Login Authentication Using Group TACACS+

Use the `aaa authentication login` command with the `group tacacs+` method to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, use the following command:

```bash
aaa authentication login default group tacacs+
```

Before you can use TACACS+ as the login authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, see TACACS+ Configuration Task List, on page 261.

Login Authentication Using Group Name

Use the `aaa authentication login` command with the `group group-name` method to specify a subset of RADIUS or TACACS+ servers to use as the login authentication method. To specify and define the group name and the members of the group, use the `aaa group server` command. For example, use the `aaa group server` command to first define group `loginrad`:

```bash
aaa group server radius loginrad
server-private 172.16.2.3 key test
server-private 172.16.2.17 key hello
server-private 172.16.2.32 key admin
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group `loginrad`.

To specify `group loginrad` as the method of user authentication at login when no other method list has been defined, use the following command:

```bash
aaa authentication login default group loginrad
```

Before you can use a group name as the login authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS or TACACS+ security server, see Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263 or TACACS+ Configuration Task List, on page 261.

Enabling Password Protection at the Privileged Level

Use the `aaa authentication enable default` command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line.

To enable password protection at the privileged level, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. aaa authentication enable default method1 [method2...]
4. end

DETAILED STEPS

<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>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa authentication enable default method1 [method2...]</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authentication enable default group radius group tacacs+ local</td>
</tr>
<tr>
<td></td>
<td>Enables user ID and password checking for users requesting privileged EXEC level.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> All aaa authentication enable default requests sent by the device to a RADIUS server include the username “Senab15$.” Requests sent to a TACACS+ server will include the username that is entered for login authentication.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered. Table 8 lists the supported enable authentication methods.

Table 21: AAA Authentication Enable Default Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS hosts for authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The RADIUS method does not work on a per-username basis.</td>
</tr>
</tbody>
</table>
### Changing the Text Displayed at the Password Prompt

Use the `aaa authentication password-prompt` command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The `no` form of this command returns the password prompt to the following default value:

```
Password:
```

The `aaa authentication password-prompt` command works when RADIUS is used as the login method. You can see the password prompt defined in the command shown even when the RADIUS server is unreachable. The `aaa authentication password-prompt` command does not work with TACACS+. TACACS+ supplies the NAS with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the `aaa authentication password-prompt` command. If the TACACS+ server is not reachable, the password prompt defined in the `aaa authentication password-prompt` command may be used.

To change the text displayed at the password prompt, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa authentication password-prompt` *text-string*
4. `end`

**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.</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>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that are displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

This section includes the following sections:

- Configuring a Login Banner
- Configuring a Failed-Login Banner

#### Configuring a Login Banner

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

To configure a banner that is displayed whenever a user logs in (replacing the default message for login), complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication banner delimiter string delimiter`
5. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Creates a personalized login banner.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa authentication banner delimiter string delimiter &quot;Unauthorized use is prohibited.&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

The maximum number of characters that can be displayed in the login banner is 2996 characters.

### Configuring a Failed-Login Banner

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the failed-login banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

To configure a message that is displayed whenever a user fails login (replacing the default message for failed login), complete the following steps:

### SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication fail-message delimiter string delimiter
5. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| Example: | Switch> enable | |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Switch# configure terminal | |
| Step 3 | aaa new-model | Enables AAA. |
| Example: | Switch(config)# aaa new-model | |
| Step 4 | aaa authentication fail-message delimiter string delimiter | Creates a message to be displayed when a user fails login. |
| Example: | Switch(config)# aaa authentication fail-message delimiter *Failed login. Try again.* | |
| Step 5 | end | Returns to privileged EXEC mode. |
| Example: | Switch(config)# end | |

The maximum number of characters that can be displayed in the failed-login banner is 2996 characters.

### Non-AAA Authentication Methods

This section discusses the following non-AAA authentication tasks:

- Configuring Line Password Protection
- Establishing Username Authentication

### Configuring Line Password Protection

You can provide access control on a terminal line by entering the password and establishing password checking.
SUMMARY STEPS

1. enable
2. configure terminal
3. line [aux | console | tty | vty] line-number [ending-line-number]
4. password password
5. login
6. no login
7. end

DETAILED STEPS

<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>
</tbody>
</table>
| Example: Switch> enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Step 2** | configure terminal |
| Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 3** | line [aux | console | tty | vty] line-number [ending-line-number] |
| Example: Switch(config)# line vty 0 | Enters line configuration mode for the lines to which you want to apply the authentication list. |
| **Step 4** | password password |
| Example: Switch(config-line)# password 1234abcd | Assigns a password to a terminal or other device on a line. |
| **Step 5** | login |
| Example: Switch(config-line)# login | Enables password checking at login.  
The password checker is case sensitive and can include spaces; for example, the password “Secret” is different from the password “secret,” and “two words” is an acceptable password.  
You can disable line password verification by disabling password checking. To perform this task, use the following command in line configuration mode: |
| **Step 6** | no login |
| Example: Switch(config-line)# no login | Disables password checking or allow access to a line without password verification. |
Establishing Username Authentication

If you configure line password protection and then configure TACACS or extended TACACS, the TACACS username and password take precedence over line passwords. If you have not yet implemented a security policy, we recommend that you use AAA.

The `login` command only changes username and privilege level but it does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the device (loop-back). Make sure that the device has been configured for secure Telnet sessions if you choose to implement autocommands this way.

### Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:

- To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS
- To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and "no escape" situations

To establish username authentication, use the following commands as needed for your system configuration:

### SUMMARY STEPS

1. enable
2. configure terminal
3. `username name [nopassword | password password | password encryption-type encrypted password]` or `username name [access-class number]`
4. `username name [privilege level]`
5. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example: Switch&gt; <strong>enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> username <em>name</em> [nopassword</td>
<td>Establishes username authentication with encrypted passwords.</td>
</tr>
<tr>
<td>password <em>password</em></td>
<td>or username <em>name</em> [access-class <em>number</em>]</td>
</tr>
<tr>
<td>Example: Switch(config)# username <em>user</em> password 1234abcd</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> username <em>name</em> [privilege <em>level</em>]</td>
<td>(Optional) Sets the privilege level for the user.</td>
</tr>
<tr>
<td>Example: Switch(config)# username <em>user</em> privilege 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Authentication Examples**

The following sections provide authentication configuration examples:

- RADIUS Authentication Examples
- TACACS+ Authentication Examples
- Login and Failed Banner Examples

**RADIUS Authentication Examples**

This section provides two sample configurations using RADIUS.

The following example shows how to configure the device to authenticate and authorize using RADIUS:

```plaintext
aaa authentication login radius-login group radius local
aaa authorization exec default group radius if-authenticated
line 3
login authentication radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:
• The **aaa authentication login radius-login group radius local** command configures the device to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.

• The **aaa authorization exec default group radius if-authenticated** command queries the RADIUS database for information that is used during EXEC authorization, such as autocommands and privilege levels, but only provides authorization if the user has successfully authenticated.

• The **login authentication radius** command enables the radius method list for line 3.

The following example shows how to configure the device to prompt for and verify a username and password, authorize the user’s EXEC level, and specify it as the method of authorization for privilege level 2. In this example, if a local username is entered at the username prompt, that username is used for authentication.

If the user is authenticated using the local database, EXEC authorization using RADIUS will fail because no data is saved from the RADIUS authentication. The method list also uses the local database to find an autocommand. If there is no autocommand, the user becomes the EXEC user. If the user then attempts to issue commands that are set at privilege level 2, TACACS+ is used to attempt to authorize the command.

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius server radius
address ipv4 72.163.191.63 auth-port 1645 acct-port 1646
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

• The **aaa authentication login default group radius local** command specifies that the username and password are verified by RADIUS or, if RADIUS is not responding, by the device’s local user database.

• The **aaa authorization exec default group radius local** command specifies that RADIUS authentication information be used to set the user’s EXEC level if the user authenticates with RADIUS. If no RADIUS information is used, this command specifies that the local user database be used for EXEC authorization.

• The **aaa authorization command 2 default group tacacs+ if-authenticated** command specifies TACACS+ authorization for commands set at privilege level 2, if the user has already successfully authenticated.

• The **radius server radius address ipv4 72.163.191.63 auth-port 1645 acct-port 1646** command specifies the IP address of the RADIUS server host, the UDP destination port for authentication requests, and the UDP destination port for accounting requests.

### TACACS+ Authentication Examples

The following example shows how to configure TACACS+ as the security protocol to be used for login authentication:

```
aaa new-model
aaa authentication login test group tacacs+ local
tacacs server tacacs+
address ipv4 10.1.2.3
key goaway
```

The lines in this sample TACACS+ authentication configuration are defined as follows:

• The **aaa new-model** command enables the AAA security services.

• The **aaa authentication** command defines a method list, “test,” to be used on serial interfaces running login. The group tacacs+ keywords means that authentication is done through TACACS+. If TACACS+
returns an ERROR of some sort during authentication, the local keyword indicates that authentication is attempted using the local database on the network access server.

- The `tacacs server tacacs+ address ipv4 10.1.2.3` command identifies the TACACS+ daemon as having an IP address of 10.1.2.3.

- The `tacacs server key` command defines the shared encryption key to be “goaway.”

### Login and Failed Banner Examples

The following example shows how to configure a login banner (in this case, the phrase “Unauthorized Access Prohibited”) that is displayed when a user logs in to the system. The asterisk (*) is used as the delimiting character. (RADIUS is specified as the default login authentication method.)

```plaintext
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized Access Prohibited
Username:
```

The following example shows how to additionally configure a failed login banner (in this case, the phrase “Failed login. Try again.”) that is displayed when a user tries to log in to the system and fails. The asterisk (*) is used as the delimiting character. (RADIUS is specified as the default login authentication method.)

```plaintext
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

### Configuring Authorization

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user’s profile, which is located either in the local user database or on the security server, to configure the user’s session. Once this is done, the user is granted access to a requested service only if the information in the user profile allows it.

For a complete description of the authorization commands used in this chapter, see the chapter “Authorization Commands” in the Cisco IOS Security Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or see the software release notes for a specific release.

### Named Method Lists for Authorization

Method lists for authorization define the ways in which authorization is performed and the sequence in which these methods are performed. A method list is simply a named list describing the authorization methods to
be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

Method lists are specific to the authorization type requested:

- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods is performed. The only exception is the default method list (which is named "default"). If the `aaa authorization` command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, local authorization takes place by default.

### AAA Authorization Methods

AAA supports five different methods of authorization:

- **TACACS+**—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- **If-Authenticated**—The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None**—The network access server does not request authorization information; authorization is not performed over this line or interface.
- **Local**—The device or access server consults its local database, as defined by the username command, for example, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- **RADIUS**—The network access server requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS server. T1 and T2 make up the group of TACACS+ servers.

Figure 15: Typical AAA Network Configuration

Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as a server group, and define T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for login authentication.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263 or TACACS+ Configuration Task List, on page 261.

AAA Authorization Types

Cisco IOS software supports two different types of authorization:
• Commands—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.

• EXEC—Applies to the attributes associated with a user EXEC terminal session.

### AAA Authorization Prerequisites

Before configuring authorization using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server. For more information about enabling AAA on your Cisco device or access server, see **AAA Overview**, on page 212.

- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly. For more information about AAA authentication, see **Configuring Authentication**, on page 217.

- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS or TACACS+ security server, see **Configuring Cisco ME 2600X to RADIUS Server Communication**, on page 263 or **TACACS+ Configuration Task List**, on page 261.

- Define the rights associated with specific users by using the `username` command if you are issuing local authorization. For more information about the `username` command, see the **Cisco IOS Security Command Reference**.

### AAA Authorization Configuration Task List

This section describes the following configuration tasks:

- Configuring AAA Authorization Using Named Method Lists
- Disabling Authorization for Global Configuration Commands

For authorization configuration examples using the commands in this chapter, see **Authorization Configuration Examples**, on page 239.

### Configuring AAA Authorization Using Named Method Lists

To configure AAA authorization using named method lists, complete the following steps:
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [method2...]]`
4. `line [aux | console | tty | vty] line-number [ending-line-number] or interface type slot/port`
5. `authorization commands {arap | commands level | connection | exec} {default | list-name}`
6. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Switch# configure terminal |
| **Step 3** aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [method2...]] | Creates an authorization method list for a particular authorization type and enable authorization. |
| Example: Switch(config)# aaa authorization commands 7 tacauth group tacacs+ |
| **Step 4** line [aux | console | tty | vty] line-number [ending-line-number] or interface type slot/port | Enters the line configuration mode for the lines to which you want to apply the authorization method list.  
Alternately, enters the interface configuration mode for the interfaces to which you want to apply the authorization method list. |
| Example: Switch(config)# line vty 0 |
| **Step 5** authorization commands {arap | commands level | connection | exec} {default | list-name} | |
| Example: Switch(config-line)# authorization commands 7 tacauth |
| **Step 6** exit | Returns to privileged EXEC mode. |
| Example: Switch(config-line)# exit |
Authorization Types

Named authorization method lists are specific to the indicated type of authorization.

To create a method list to enable authorization for all network-related service requests (including SLIP and login), use the network keyword.

To create a method list to enable authorization to determine if a user is allowed to run an EXEC shell, use the exec keyword.

To create a method list to enable authorization for specific, individual EXEC commands associated with a specific privilege level, use the commands keyword. (This allows you to authorize all commands associated with a specified command level from 0 to 15.)

To create a method list to enable authorization for reverse Telnet functions, use the `reverse-access` keyword.

For information about the types of authorization supported by the Cisco IOS software, see AAA Authorization Types, on page 235.

Authorization Methods

To have the network access server request authorization information via a TACACS+ security server, use the `aaa authorization` command with the `group tacacs+` method keyword. For more specific information about configuring authorization using a TACACS+ security server, see TACACS+ Configuration Task List, on page 261. For an example of how to enable a TACACS+ server to authorize the use of network services, including login, see TACACS+ Authorization Example, on page 240.

To allow users to have access to the functions they request as long as they have been authenticated, use the `aaa authorization` command with the `if-authenticated` method keyword. If you select this method, all requested functions are automatically granted to authenticated users.

There may be times when you do not want to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the `none` method keyword. If you select this method, authorization is disabled for all actions.

To select local authorization, which means that the device or access server consults its local user database to determine the functions a user is permitted to use, use the `aaa authorization` command with the `local` method keyword. The functions associated with local authorization are defined by using the `username` global configuration command. For a list of permitted functions, see Configuring Authentication, on page 217.

Note

Authorization method lists for SLIP follow whatever is configured for login on the relevant interface. If no lists are defined and applied to a particular interface (or no login settings are configured), the default setting for authorization applies.

Disabling Authorization for Global Configuration Commands

The `aaa authorization` command with the commands keyword attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using `no aaa authorization config-commands` stops the network access server from attempting configuration command authorization.

To disable AAA authorization for all global configuration commands, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. no aaa authorization config-commands
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
Example:  
Switch> enable |  
• Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode.  
Example:  
Switch# configure terminal |
| Step 3 | no aaa authorization config-commands | Disables authorization for all global configuration commands.  
Example:  
Switch(config)# no aaa authorization config-commands |
| Step 4 | end | Returns to privileged EXEC mode.  
Example:  
Switch(config)# end |

Authorization Attribute-Value Pairs

RADIUS and TACACS+ authorization both define specific rights for users by processing attributes, which are stored in a database on the security server. For both RADIUS and TACACS+, attributes are defined on the security server, associated with the user, and sent to the network access server where they are applied to the user’s connection.

Authorization Configuration Examples

The following sections provide authorization configuration examples.
Named Method List Configuration Example

The following example shows how to configure a Cisco ME 2600X (enabled for AAA and communication with a RADIUS security server) for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```plaintext
aaa new-model
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius group tacacs+
radius server radius
    address ipv4 72.163.191.63 auth-port 1645 acct-port 1646
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The `aaa new-model` command enables AAA network security services.
- The `aaa authorization exec default start-stop group radius group tacacs+` command defines the network accounting method list named charley, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using login.

TACACS+ Authorization Example

The following example shows how to allow network authorization using TACACS+:

```plaintext
aaa authorization commands 15 default group tacacs+
```

Note RADIUS Authorization is not supported using "commands" authorization.

RADIUS Authorization Example

The following example shows how to configure the device to authorize using RADIUS:

```plaintext
aaa new-model
aaa authorization exec default group radius if-authenticated
```

The lines in this sample RADIUS authorization configuration are defined as follows:

- The `aaa authorization exec default group radius if-authenticated` command configures the network access server to contact the RADIUS server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the RADIUS server, the fallback method is to permit the CLI to start, provided the user has been properly authenticated.

The RADIUS information returned may be used to specify an autocmd or a connection access list be applied to this connection.

Note Because no fallback method is specified in this example, authorization will fail if, for any reason, there is no response from the RADIUS server.
Configuring Accounting

The AAA accounting feature enables you to track the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

For a complete description of the accounting commands used in this chapter, see the chapter "Accounting Commands" in the Cisco IOS Security Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release.

Named Method Lists for Accounting

Like authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for accounting services. The only exception is the default method list (which, by coincidence, is named "default"). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.

Note

The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle—meaning that the security server responds by denying the user access—the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports Exec accounting. EXEC provides information about user EXEC terminal sessions of the network access server.
System accounting does not use named accounting lists; you can only define the default list for system accounting.

Once again, when you create a named method list, you are defining a particular list of accounting methods for the indicated accounting type.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named “default”). If the aaa accounting command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

**Method Lists and Server Groups**

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS server. T1 and T2 make up the group of TACACS+ servers.

**Figure 16: Typical AAA Network Configuration**

Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as a server group, and define T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for login authentication.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address.
address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263 or TACACS+ Configuration Task List, on page 261.

AAA Accounting Methods

Cisco IOS supports the following two methods for accounting:

- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

EXEC Accounting

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

```
Wed Jun 27 04:26:23 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "fgeorge"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Delay-Time = 0
User-Id = "fgeorge"
NAS-Identifier = "172.16.25.15"

NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "fgeorge"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Session-Time = 62
Acct-Delay-Time = 0
```
User-Id = “fgeorge”
NAS-Identifier = “172.16.25.15”
The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

Wed Jun 27 03:46:21 2001 172.16.25.15 fgeorge tty3 5622329430/4327528
start task_id=2 service=shell
Wed Jun 27 04:08:55 2001 172.16.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=2 service=shell elapsed_time=1354

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

NAS-IP-Address = “172.16.25.15”
NAS-Port = 26
User-Name = “fgeorge”
Caller-ID = “171.68.202.158”
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = “00000010”
Acct-Delay-Time = 0
User-Id = “fgeorge”
NAS-Identifier = “172.16.25.15”

NAS-IP-Address = “172.16.25.15”
NAS-Port = 26
User-Name = “fgeorge”
Caller-ID = “171.68.202.158”
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = “00000010”
Acct-Session-Time = 14
Acct-Delay-Time = 0
User-Id = “fgeorge”
NAS-Identifier = “172.16.25.15”

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

start task_id=41 service=shell
Wed Jun 27 04:07:02 2001 172.16.25.15 fgeorge tty26 171.68.202.158
stop task_id=41 service=shell elapsed_time=9

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the show radius statistics command)
- Status of servers providing AAA functions
- Identities of external AAA servers
- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call
The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

**Table 22: SNMP End-User Data Objects**

<table>
<thead>
<tr>
<th>SessionId</th>
<th>The session identification used by the AAA accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserId</td>
<td>The user login ID or zero-length string if a login is unavailable.</td>
</tr>
<tr>
<td>IpAddr</td>
<td>The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.</td>
</tr>
<tr>
<td>IdleTime</td>
<td>The elapsed time in seconds that the session has been idle.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>The session termination object used to disconnect the given client.</td>
</tr>
<tr>
<td>CallId</td>
<td>The entry index corresponding to this accounting session that the Call Tracker record stored.</td>
</tr>
</tbody>
</table>

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

**Table 23: SNMP AAA Session Summary**

<table>
<thead>
<tr>
<th>ActiveTableEntries</th>
<th>Number of sessions currently active.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveTableHighWaterMark</td>
<td>Maximum number of sessions present at once since last system reinstallation.</td>
</tr>
<tr>
<td>TotalSessions</td>
<td>Total number of sessions since last system reinstallation.</td>
</tr>
<tr>
<td>DisconnectedSessions</td>
<td>Total number of sessions that have been disconnected using since last system reinstallation.</td>
</tr>
</tbody>
</table>

### AAA Accounting Prerequisites

Before configuring accounting using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server. For more information about enabling AAA on your Cisco device or access server, see [AAA Overview](page212).
- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS or TACACS+ security server, see [Configuring Cisco ME 2600X to RADIUS Server Communication](page263) or [TACACS+ Configuration Task List](page261).
AAA Accounting Configuration Task List

This section describes the following configuration tasks:

- Configuring AAA Accounting Using Named Method Lists
- Suppressing Generation of Accounting Records for Null Username Sessions
- Configuring AAA Resource Accounting for Start-Stop Records
- Configuring AAA Resource Failure Stop Accounting
- Configuring AAA Session MIB

For accounting configuration examples using the commands in this chapter, see Accounting Configuration Examples, on page 248.

Configuring AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [method1 [method2...]]
4. line [aux | console | tty | vty] line-number [ending-line-number] or interface interface-type interface-number
5. accounting {arap | commands level | connection | exec} {default | list-name}
6. exit

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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 3 | aaa accounting \{system | network | exec | connection | commands level\} \{default | list-name\} \{start-stop | stop-only | none\} \{method1 [method2...]\] |
| Purpose | Creates an accounting method list and enables accounting. The argument list-name is a character string used to name the list you are creating. |
| Example: | Switch(config)# aaa accounting commands 7 tacacctcomm start-stop group tacacs+ |

| Step 4 | line \{aux | console | tty | vty\} line-number \{ending-line-number\} or interface interface-type interface-number |
| Purpose | Enters the line configuration mode for the lines to which you want to apply the accounting method list. or |
| Example: | Switch(config)# line vty 0 |

| Step 5 | accounting \{arap | commands level | connection | exec\} \{default | list-name\} |
| Purpose | Applies the accounting method list to a line or set of lines. |
| Example: | Switch(config-line)# accounting commands 7 tacacctcomm |

| Step 6 | exit |
| Purpose | Returns to privileged EXEC mode. |
| Example: | Switch(config-line)# exit |

### Accounting Type

Named accounting method list is specific to the indicated type of accounting.

- **exec**—To create a method list that provides accounting records about user EXEC terminal sessions on the network access server, including username, date, start and stop times, use the exec keyword.

### Accounting Record Types

For minimal accounting, use the stop-only keyword, which instructs the specified method (RADIUS or TACACS+) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the start-stop keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the none keyword.

### AAA Accounting Methods

Cisco IOS supports the following two methods for accounting:
TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

## Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ attribute-value (AV) pairs or RADIUS attributes, depending on which security method you have implemented.

---

**Note**

Only priv-lvl AV-Pair is supported.

---

## Accounting Configuration Examples

This section contains the following examples:

- Configuring Named Method List Example
- AAA Session MIB Example

### Configuring Named Method List Example

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database are queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```plaintext
aaa accounting exec default start-stop group tacacs+ group radius
```

For more information, see Configuring Cisco ME 2600X to RADIUS Server Communication, on page 263 or TACACS+ Configuration Task List, on page 261.

The `show accounting` command yields the following output for the preceding configuration:

```plaintext
Active Accounted actions on tty1, User rubble Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service-login protocol-ip address=10.0.0.98
```

The table below describes the fields contained in the preceding output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Accounted actions on</td>
<td>Terminal line or interface name user with which the user logged in.</td>
</tr>
<tr>
<td>User</td>
<td>User’s ID.</td>
</tr>
</tbody>
</table>

---
### AAA Session MIB Example

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for login users:

```
aaa new-model
aaa authentication login default group radius
```

### Show Commands

The following AAA show commands are available:

#### Examples

```
Switch#show aaa servers

RADIUS: id 6050, priority 0, host 72.163.210.36, auth-port 1645, acct-port 1646
  State: current UP, duration 99643s, previous duration 0s
  Dead: total time 0s, count 0
  Quarantined: No
  Authen: request 0, timeouts 0, failover 0, retransmission 0
    Response: accept 0, reject 0, challenge 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Author: request 0, timeouts 0, failover 0, retransmission 0
    Response: accept 0, reject 0, challenge 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Account: request 0, timeouts 0, failover 0, retransmission 0
    Request: start 0, interim 0, stop 0
    Response: start 0, interim 0, stop 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms

Elapsed time since counters last cleared: 1d3h40m
Estimated Outstanding Access Transactions: 0
```
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0

Requests per minute past 24 hours:
  high - 3 hours, 41 minutes ago: 0
  low - 3 hours, 41 minutes ago: 0
  average: 0

Switch#show tacacs

Tacacs+ Server - private :
  Server address: 72.163.210.36
  Server port: 49
  Socket opens: 0
  Socket closes: 0
  Socket aborts: 0
  Socket errors: 0
  Socket Timeouts: 0
  Failed Connect Attempts: 0
  Total Packets Sent: 0
  Total Packets Recv: 0

Switch#show users

<table>
<thead>
<tr>
<th>Line</th>
<th>User</th>
<th>Host(s)</th>
<th>Idle</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 0</td>
<td>con</td>
<td>idle</td>
<td>00:00:00</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>vty</td>
<td>admin</td>
<td>idle</td>
<td>1d02h 64.103.217.21</td>
</tr>
</tbody>
</table>

Switch#show aaa user all

Unique id 11 is currently in use.
No data for type 0
No data for type EXEC
No data for type CONN
NET: Username=(n/a)  
  Session Id=00000001 Unique Id=0000000B
  Start Sent=0 Stop Only=N
  stop_has_been_sent=N
  Method List=0
  Attribute list:  
 2481FB5C 0 00000001 session-id(408) 4 1(1)

No data for type CMD
No data for type SYSTEM
No data for type VRRS
No data for type RM CALL
No data for type RM VPDN
No data for type AUTH PROXY
No data for type DOT1X
No data for type CALL
No data for type VPDN-TUNNEL
No data for type VPDN-TUNNEL-LINK
No data for type IPSEC-TUNNEL
No data for type MCAST
No data for type RESOURCE
No data for type SSG
No data for type IDENTITY
No data for type ConnectedApps

Accounting:
    log=0x18001
    Events recorded:
        CALL START
        INTERIM START
        INTERIM STOP
    update method(s):
        NONE
    update interval = 0
    Outstanding Stop Records : 0

Dynamic attribute list:
    2481FB5C 0 00000001 connect-progress(75) 4 Term Serv Auth
    2481FB90 0 00000001 pre-session-time(334) 4 99818(185EA)
    2481FBC4 0 00000001 elapsed_time(414) 4 0(0)
    2481FBD8 0 00000001 pre-bytes-in(330) 4 0(0)
    2481FC2C 0 00000001 pre-bytes-out(331) 4 0(0)
    2481FA4C 0 00000001 pre-paks-in(332) 4 0(0)
    2481FA80 0 00000001 pre-paks-out(333) 4 0(0)

Debg: No data available
Radi: No data available

Interface:
    TTY Num = 0
    Stop Received = 0

Byte/Packet Counts till Call Start:
    Start Bytes In = 0         Start Bytes Out = 0
    Start Paks In = 0          Start Paks Out = 0

Byte/Packet Counts till Service Up:
    Pre Bytes In = 0           Pre Bytes Out = 0
    Pre Paks In = 0            Pre Paks Out = 0

Cumulative Byte/Packet Counts:
    Bytes In = 0                Bytes Out = 0
    Paks In = 0                 Paks Out = 0

    StartTime = 12:42:12 UTC Sep 11 1900
    Component = Exec

Authen: service=LOGIN type=ASCII method=NONE
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.

General:
    Unique Id = 0000000B
    Session Id = 00000001
    Attribute List:
        2481FA4C 0 00000081 interface(221) 4 tty0
        2481FA80 0 00000001 port-type(225) 4 Async
        2481FAB4 0 00000081 clid(36) 5 async

PerU: No data available
Service Profile: No Service Profile data.

Switch#show aaa local user lockout

<table>
<thead>
<tr>
<th>Local-user</th>
<th>Lock time</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco</td>
<td>16:28:00 UTC Wed Sep 12 1900</td>
</tr>
</tbody>
</table>

Switch#show aaa sessions
Total sessions since last reload: 7
Session Id: 7
  Unique Id: 17
  User Name: admin
  IP Address: 64.103.217.21
  Idle Time: 0
  CT Call Handle: 0

Switch#show running-config aaa

authentication login default group taclogin local
aaa authentication login fail-message "Check your username and password...!"
aaa authentication attempts login 5
aaa authorization exec default group taclogin if-authenticated
aaa accounting exec default start-stop group taclogin group radlogin
username admin privilege 15 password 0 admin

aaa group server radius radlogin
  server-private 72.163.210.36 key helloworld
  server-private 72.163.191.69 key helloworld

aaa group server tacacs+ taclogin
  server-private 72.163.210.36 key helloworld
  server-private 72.163.191.69 key helloworld

aaa local authentication attempts max-fail 2
aaa new-model
aaa session-id common

Additional Information

This chapter provides additional security information on the following topics:

- Local Authentication
- TACACS+
- RADIUS

Understanding Authentication

Access control enables you to restrict access to the network server and its services to a specific group of users. The authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you can set up access control on your device or access server.

Authentication is a way of identifying a user before permitting access to the network and network services. The Cisco ME 2600X supports local authentication mechanism to administer its security functions.

Configuring Local Authentication

The only supported login authentication method in Cisco ME 2600X is local authentication.
SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login default methodname
5. line [aux | console | tty | vty] line-number [ending-line-number]
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| Example: Switch> enable | • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Switch(config)# configure terminal | |
| **Step 3** aaa new-model | Enables authentication, authorization, and accounting (AAA) globally. |
| Example: Switch(config)# aaa new-model | |
| **Step 4** aaa authentication login default methodname | Creates the default local authentication list. |
| Example: Switch(config-if)# aaa authentication login default local | |
| **Step 5** line [aux | console | tty | vty] line-number [ending-line-number] | Enters line configuration mode for the lines to which you want to apply the authentication list. |
| Example: Switch(config)# line vty 0 4 | |
| **Step 6** end | Returns to global configuration mode. |
| Example: Switch(config-line)# end | |

**Example: Configure Local Authentication**

The following example shows how to configure local authentication using Cisco IOS commands:

Switch> enable
Switch# configure terminal
## Setting or Changing a Static Enable Password

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `username user password password`
4. `enable password password`
5. `end`

### 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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt;</code> enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> username user password password</td>
<td>Sets the user name and password.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# username user1 password pwd</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enable password password</td>
<td>Enables a new password or changes an existing password for the privileged command level.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# enable password user1</code></td>
<td></td>
</tr>
</tbody>
</table>
Protecting Passwords with Enable Password and Enabling Secret

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the `enable password` or `enable secret` commands. Both commands accomplish the same thing; that is, they allow you to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level you specify.

We recommend that you use the `enable secret` command because it uses an improved encryption algorithm. If you configure the `enable secret` command, it takes precedence over the `enable password` command; the two commands cannot be in effect simultaneously.

If neither the `enable password` command nor the `enable secret` command is configured, and if there is a line password configured for the console, the console line password serves as the enable password for all VTY sessions.

Use the `enable password` or `enable secret` commands with the `level` keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the `privilege level` configuration command to specify the commands accessible at various levels.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `username user password password`
4. `enable password [level level-number] {password | encryption-type encrypted-password}`
5. `enable secret [level level-number] {password | encryption-type encrypted-password}`
6. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
---|---
**Step 2**  
configure terminal | Enters global configuration mode.

**Step 3**  
username *user* password *password* | Sets the user name and password.

**Step 4**  
enable password [level *level-number*] {password | encryption-type encrypted-password} | Enables a password for a privilege command mode.

**Step 5**  
enable secret [level *level-number*] {password | encryption-type encrypted-password} | Specifies a secret password, saved using a non-reversible encryption method. If both enable password and enable secret commands are set, the user must use the enable secret password.

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

### Setting or Changing a Line Password

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. password *password_new*  
4. end

**DETAILED STEPS**

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

Example:

Switch> enable

---

**Cisco ME 2600X Series Ethernet Access Switch Software Configuration Guide**

OL-28850-04
## Understanding Multiple Privilege Levels

Cisco ME 2600X supports multiple privilege levels, which provide access to commands. By default, there are two levels of access to commands:

- User EXEC mode (level 1)
- Privileged EXEC mode (level 15)

You can configure additional levels of access to commands, called privilege levels, to meet the needs of users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured from level 0, which is the most restricted level, to level 15, which is the least restricted level.

The access to each privilege level is enabled through separate passwords, which you can specify when configuring the privilege level.

For example, if you want a certain set of users to be able to configure only certain interfaces and configuration options, you could create a separate privilege level only for specific interface configuration commands and distribute the password for that level to those users.

## Configuring Privilege Levels

Perform any of these procedures as needed.

- Setting the Privilege Level for a Command, on page 258
- Displaying Current Privilege Levels, on page 258
- Logging In to a Privilege Level, on page 259
## Setting the Privilege Level for a Command

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `privilege mode level level_number command-string`
4. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>privilege mode level level_number command-string</code></td>
<td>Configures the specified privilege level to</td>
</tr>
<tr>
<td>Example:</td>
<td>allow access to the specified command.</td>
</tr>
<tr>
<td><code>Switch(config)# privilege exec level 14 configure</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits global configuration mode and returns</td>
</tr>
<tr>
<td>Example:</td>
<td>to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Switch(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

## Displaying Current Privilege Levels

### SUMMARY STEPS

1. `enable`
2. `show privilege`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
---|---
**Example:** Switch> enable | • Enter your password if prompted.

### Step 2

Command or Action | Purpose
---|---
**Example:** Switch# show privilege | Displays the current privilege level you can access based on the password you used.

---

### Logging In to a Privilege Level

**SUMMARY STEPS**

1. enable
2. enable level

**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 your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> enable level</td>
<td>Logs in to a specified privilege level.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# enable 12</td>
<td></td>
</tr>
</tbody>
</table>

---

### TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a device or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—indepedently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.
The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and devices and the Cisco IOS user interface (for both devices and access servers) can be network access servers.

The TACACS+ protocol provides authentication between the network access server and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between a network access server and a TACACS+ daemon are encrypted.

You need a system running TACACS+ daemon software to use the TACACS+ functionality on your network access server.

**TACACS+ Operation**

When a user attempts a simple ASCII login by authenticating to a network access server using TACACS+, the following process typically occurs:

1. When the connection is established, the network access server contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the network access server then contacts the TACACS+ daemon to obtain a password prompt. The network access server displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

   **Note**

   TACACS+ allows an arbitrary conversation to be held between the daemon and the user until the daemon receives enough information to authenticate the user. This is usually done by prompting for a username and password combination, but may include other items, such as mother’s maiden name, all under the control of the TACACS+ daemon.

2. The network access server eventually receives one of the following responses from the TACACS+ daemon:
   - ACCEPT—The user is authenticated and service may begin. If the network access server is configured to require authorization, authorization begins at this time.
   - REJECT—The user has failed to authenticate. The user may be denied further access, or is prompted to retry the login sequence depending on the TACACS+ daemon.
   - ERROR—An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the network access server. If an ERROR response is received, the network access server typically tries to use an alternative method for authenticating the user.
   - CONTINUE—The user is prompted for additional authentication information.

3. Following authentication, the user will also be required to undergo an additional authorization phase, if authorization has been enabled on the network access server. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

4. If TACACS+ authorization is required, the TACACS+ daemon is again contacted and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response will contain data in the form of attributes that are used to direct the EXEC session for that user, determining services that the user can access.

   Services include the following:
• Telnet, rlogin, or EXEC services
• Connection parameters, including the host or client IP address, access list, and user timeouts

TACACS+ Configuration Task List

To configure your device to support TACACS+, you must perform the following tasks:

• Use the `aaa new-model` global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+. For more information about using the `aaa new-model` command, see AAA Overview, on page 212.

• Use the `tacacs-server host` command to specify the IP address of one or more TACACS+ daemons. Use the `tacacs-server key` command to specify an encryption key that is used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon.

• Use the `aaa authentication` global configuration command to define method lists that use TACACS+ for authentication. For more information about using the `aaa authentication` command, see Configuring Authentication, on page 217.

• Use the `line` and `interface` commands to apply the defined method lists to various interfaces. For more information, see Configuring Authentication, on page 217.

• If needed, use the `aaa authorization` global command to configure authorization for the network access server. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire network access server. For more information about using the `aaa authorization` command, see Configuring Authorization, on page 233.

• If needed, use the `aaa accounting` command to enable accounting for TACACS+ connections. For more information about using the `aaa accounting` command, see Configuring Accounting, on page 241.

To configure TACACS+, perform the tasks in the following sections:

• Set the TACACS+ Authentication Key
• Specify TACACS+ Authentication
• Specify TACACS+ Accounting

For TACACS+ configuration examples using the commands in this chapter, see TACACS+ Authentication, Authorization, and Accounting Example, on page 262.

Specifying TACACS+ Authentication

After you have identified the TACACS+ daemon and defined an associated TACACS+ encryption key, you need to define method lists for TACACS+ authentication. Because TACACS+ authentication is operated via AAA, you need to issue the `aaa authentication` command, specifying TACACS+ as the authentication method. For more information, see Configuring Authentication, on page 217.
Specifying TACACS+ Authorization

AAA authorization enables you to set parameters that restrict a user’s network access. Authorization via TACACS+ may be applied to commands, network connections, and EXEC sessions. Because TACACS+ authorization is facilitated through AAA, you need to issue the `aaa authorization` command, specifying TACACS+ as the authorization method. For more information, see Configuring Authorization, on page 233.

Specify TACACS+ Accounting

AAA accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because TACACS+ accounting is facilitated through AAA, you need to issue the `aaa accounting` command, specifying TACACS+ as the accounting method. For more information, see Configuring Accounting, on page 241.

TACACS+ Authentication, Authorization, and Accounting Example

The following example shows the configuration for a TACACS+ daemon with an IP address of 10.2.3.4 and an encryption key of "apple."

```
aaa new-model
aaa authentication login default tacacs+ local
  tacacs-server host 10.2.3.4
  tacacs-server key apple
aaa authorization exec default group tacacs+ if-authenticated
  aaa authorization commands 7 default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```

In this example:

- The `aaa new-model` command enables the AAA security services.
- The `aaa authentication` command defines the default method method list. Incoming ASCII logins on all interfaces (by default) will use TACACS+ for authentication. If no TACACS+ server responds, then the network access server will use the information contained in the local username database for authentication.
- The `tacacs-server host` command identifies the TACACS+ daemon as having an IP address of 10.2.3.4. The `tacacs-server key` command defines the shared encryption key to be "apple."
- The `aaa authorization` command configures network authorization via TACACS+. Unlike authentication lists, this authorization list always applies to all incoming network connections made to the network access server.
- The `aaa accounting` command configures network accounting via TACACS+. In this example, whenever a network connection terminates, accounting records describing the session that just terminated are sent to the TACACS+ daemon.

About RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.
RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

Cisco supports RADIUS under its AAA security paradigm. RADIUS can be used with other AAA security protocols, such as TACACS+ and local username lookup. RADIUS is supported on all Cisco platforms, but some RADIUS-supported features run only on specified platforms.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database.

### Configuring Cisco ME 2600X to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (CiscoSecure ACS), Livingston, Merit, Microsoft, or another software provider. Configuring Cisco ME 2600X to RADIUS server communication can have several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string

RADIUS security servers are identified on the basis of their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

A RADIUS server and a Cisco ME 2600X use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the Cisco ME 2600X.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the Cisco ME 2600X, use the three unique global commands: `radius-server timeout`, and `radius-server retransmit`. To apply these values on a specific RADIUS server, use the `radius-server host` command.
You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Cisco network access server. If both global and per-server functions are configured on a Cisco ME 2600X, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

To configure per-server RADIUS server communication, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `radius server {hostname}`
4. `radius server [address | automate-tester | backoff | exit | key | no | non-standard | pac | retransmit | timeout]`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>radius server {hostname}</code></td>
<td>Enters the radius server configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius server cisco_radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `radius server [address</td>
<td>automate-tester</td>
</tr>
<tr>
<td>Example: Switch(config-radius-server)# address ipv4 172.26.106.10 Switch(config-radius-server)# key ciscokey</td>
<td>• address—specifies the radius server address</td>
</tr>
<tr>
<td></td>
<td>• automate-tester—configures server automated testing</td>
</tr>
<tr>
<td></td>
<td>• backoff—retries backoff pattern (default is retransmits with constant delay)</td>
</tr>
<tr>
<td></td>
<td>• exit—exits from RADIUS server configuration mode</td>
</tr>
<tr>
<td></td>
<td>• key—per-server encryption key</td>
</tr>
<tr>
<td></td>
<td>• no—negates a command or set its defaults</td>
</tr>
<tr>
<td></td>
<td>• non-standard—attributes to be parsed that violate RADIUS standard</td>
</tr>
</tbody>
</table>
Configuring Global Communication Settings Between Cisco ME 2600X and a RADIUS Server

To configure global communication settings between the Cisco ME 2600X and a RADIUS server, use the following `radius-server` commands in global configuration mode:

**SUMMARY STEPS**

1. `radius-server retransmit retries`
2. `radius-server timeout seconds`
3. `radius-server deadtime minutes`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server retransmit retries</code></td>
<td>Specifies how many times the Cisco ME 2600X transmits each RADIUS request to the server before giving up (the default is 3).</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# radius-server 10</code></td>
<td></td>
</tr>
<tr>
<td><code>radius-server timeout seconds</code></td>
<td>Specifies for how many seconds a Cisco ME 2600X waits for a reply to a RADIUS request before retransmitting the request.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# radius-server 60</code></td>
<td></td>
</tr>
<tr>
<td><code>radius-server deadtime minutes</code></td>
<td>Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# radius-server 2</code></td>
<td></td>
</tr>
</tbody>
</table>
RADIUS Authentication and Accounting Example

The following example shows a general configuration using RADIUS with the AAA command set:

```plaintext
radius server radius
address ipv4 123.45.1.2 auth-port 1645 acct-port 1646
key key
username root password ALongPassword
aaa authentication login default group radius local
aaa authorization exec default local
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The `radius server radius address ipv4 123.45.1.2 auth-port 1645 acct-port 1646` command defines the IP address of the RADIUS server host.
- The `radius server key key` command defines the shared secret text string between the network access server and the RADIUS server host.
- The `aaa authentication login default group radius local` command defines the authentication method list “default,” which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using login.

RADIUS Server Group Example

The following example shows how to create server group radgroup1 with three different RADIUS server members, each using the default authentication port (1645) and accounting port (1646):

```plaintext
aaa group server radius radgroup1
    server-private 172.16.1.11 key hello
    server-private 172.17.1.21 key test
    server-private 172.18.1.31 key cisco
```
Cisco Discovery Protocol

This chapter describes Cisco Discovery Protocol (CDP) and the configuration examples.

- Understanding CDP, page 267
- Configuring CDP, page 267
- Show Commands, page 268

Understanding CDP

Cisco Discovery Protocol (CDP) is used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your device uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Use of SNMP with the CDP Management Information Base (MIB) allows network management applications to learn the device type and the SNMP agent address of neighboring devices, and to send SNMP queries to those devices. Cisco Discovery Protocol uses the CISCO-CDP-MIB.

CDP is enabled on the system and on the interfaces by default. If you prefer not to use the CDP device discovery capability, you can disable it with the `no cdp run` command at the system level and `no cdp enable` command at the interface level.

Configuring CDP

SUMMARY STEPS

1. enable
2. configure terminal
3. [no] cdp run
4. interface type number
5. [no] cdp enable
6. end
### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode. |
| Step 3 | [no] cdp run | Re-enables or disables CDP on the system. |
| Step 4 | interface type number | Configures a Ten Gigabit Ethernet interface and enters interface configuration mode. |
| Step 5 | [no] cdp enable | Re-enables or disables CDP on the interface. |
| Step 6 | end | Returns to privileged EXEC mode. |

### Show Commands

The following Cisco Discovery Profile show commands are available. Use the `show cdp ?` command to see all the commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>entry</td>
<td>Information for specific neighbor entry</td>
</tr>
<tr>
<td>interface</td>
<td>CDP interface status and configuration</td>
</tr>
<tr>
<td>neighbors</td>
<td>CDP neighbor entries</td>
</tr>
<tr>
<td>traffic</td>
<td>CDP statistics</td>
</tr>
</tbody>
</table>
Examples

Switch#show cdp entry ?

* all CDP neighbor entries

Switch#show cdp entry *

Device ID: Switch
Entry address(es):
  IP address: 10.64.106.180
Platform: cisco ME2600X Switch, Capabilities: Switch IGMP
Interface: TenGigabitEthernet 0/47, Port ID (outgoing port):
  TenGigabitEthernet 0/48
Holdtime: 135 sec

Version :
Cisco IOS Software, ME2600X Software (ME-UNIVERSALK9-M), Version 15.2(2)SA,
  RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 06-Feb-13 15:15 by prod_rel_team

advertisement version: 2
Management address(es):
  IP address: 10.64.106.180

Device ID: Switch
Entry address(es):

Switch#show cdp int g0/5

GigabitEthernet 0/5 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Switch#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
  D - Remote, C - CVTA, M - Two-port Mac Relay

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local Intrfce</th>
<th>Holdtme</th>
<th>Capability</th>
<th>Platform</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>Ten 0/47</td>
<td>149</td>
<td>S I</td>
<td>ME2600X</td>
<td>FT</td>
</tr>
<tr>
<td>Ten 0/48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Ten 0/48</td>
<td>162</td>
<td>S I</td>
<td>ME2600X</td>
<td>FT</td>
</tr>
<tr>
<td>Ten 0/47</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Gig 0/19</td>
<td>135</td>
<td>S I</td>
<td>ME2600X</td>
<td>FT</td>
</tr>
<tr>
<td>Gig 0/20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Gig 0/20</td>
<td>127</td>
<td>S I</td>
<td>ME2600X</td>
<td>FT</td>
</tr>
<tr>
<td>Gig 0/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Gig 0/11</td>
<td>149</td>
<td>S I</td>
<td>ME2600X</td>
<td>FT</td>
</tr>
<tr>
<td>Gig 0/12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td>Gig 0/12</td>
<td>178</td>
<td>S I</td>
<td>ME2600X</td>
<td>FT</td>
</tr>
<tr>
<td>Gig 0/11</td>
<td>Switch</td>
<td>Gig 0/9</td>
<td>158</td>
<td>S</td>
<td>I</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>-----</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Gig 0/10</td>
<td>Switch</td>
<td>Gig 0/10</td>
<td>167</td>
<td>S</td>
<td>I</td>
</tr>
<tr>
<td>Gig 0/9</td>
<td>Switch</td>
<td>Gig 0/5</td>
<td>169</td>
<td>S</td>
<td>I</td>
</tr>
<tr>
<td>Gig 0/6</td>
<td>Switch</td>
<td>Gig 0/6</td>
<td>130</td>
<td>S</td>
<td>I</td>
</tr>
<tr>
<td>Gig 0/5</td>
<td>SW-OTBU-F23</td>
<td>Gig 1/1</td>
<td>140</td>
<td>S</td>
<td>I</td>
</tr>
</tbody>
</table>

Switch#show cdp traffic

CDP counters:
- Total packets output: 42276, Input: 38430
-Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
-No memory: 0, Invalid packet: 0,
-CDP version 1 advertisements output: 0, Input: 0
-CDP version 2 advertisements output: 42276, Input: 38430
This chapter explains Simple Network Management Protocol (SNMP) as implemented by Cisco ME 2600X.

**SNMP**

This chapter explains Simple Network Management Protocol (SNMP) as implemented by Cisco ME 2600X.

- Understanding SNMP, page 271
- Understanding SNMP Components, page 272
- Understanding MIB, page 274
- Understanding SNMP Traps, page 277
- Understanding SNMP Community Names, page 279
- Understanding SNMP Messages, page 279

### Understanding SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by Cisco ME 2600X. SNMP is an application–layer communication protocol that allows network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth. SNMP makes network monitoring more cost effective and allows your network to be more reliable.

Cisco ME 2600X supports SNMP Version 2c (SNMPv2c). As compared to SNMPv1, SNMPv2c includes additional protocol operations and 64–bit performance monitoring support.
The figure below illustrates the basic layout idea of an SNMP-managed network.

Figure 17: Basic Network Managed by SNMP

The advantages of SNMP are as follows:

- SNMP is LAN based.
- SNMP is an open standard.
- SNMP can be easily extended.
- SNMP provides a common management platform for many different devices.

Understanding SNMP Components

An SNMP-managed network consists of a manager, agents, and managed devices.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device being managed.

Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or several management systems.
The figure below illustrates the relationship between the network manager, the SNMP agent, and the managed devices.

Figure 18: Example of the Primary SNMP Components

An agent residing on each managed device translates local management information data—such as performance information or event and error information—caught in software traps, into a readable form for the management system.

The figure below illustrates SNMP agent get–request that transport data to the network management software.

Figure 19: Agent Gathering Data from a MIB and Sending Traps to the Manager

The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.
It is recommended that the SNMP Manager timeout value be set to 60 seconds. Under certain conditions, if this value is lower than the recommended time, the TNC/TSC card can be reset. However, the response time depends on various parameters such as object being queried, complexity, number of hops in the node and so on.

Understanding MIB

The Management Information Base (MIB) is a data structure that describes SNMP network elements as a list of data objects. The SNMP manager must compile the MIB file for each equipment type in the network to monitor SNMP devices.

The manager and agent use a MIB and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables being represented as leaves on the branches. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages. The MIB associates each OID with a readable label and various other parameters related to the object. The MIB then serves as a data dictionary or codebook that is used to assemble and interpret SNMP messages.

When the SNMP manager wants to know the value of an object, such as the state of an alarm point, the system name, or the element uptime, it will assemble a GET packet that includes the OID for each object of interest. The element receives the request and looks up each OID in its code book (MIB). If the OID is found (the object is managed by the element), a response packet is assembled and sent with the current value of the object included. If the OID is not found, a special error response is sent that identifies the unmanaged object.

MIBs Supported in Cisco ME 2600X

The table below lists the MIBs supported in Cisco ME 2600X.

<table>
<thead>
<tr>
<th>MIB Module</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTITY-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td>Generic</td>
</tr>
</tbody>
</table>

Note: The following objects do not return any value:
- snmpTrap
- snmpTraps
- sysORTable
- sysORIndex
- sysORID
- sysORDescr
- sysORUpTime

Table 25: MIBs Supported in Cisco ME 2600X
### MIB Module

<table>
<thead>
<tr>
<th>MIB Module</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-CDP-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>CISCO-IETF-IP-FORWARD-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>CISCO-IETF-IP-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>IF-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>RMON-MIB</td>
<td>Generic</td>
</tr>
</tbody>
</table>

#### Note

The following objects do not return any value:
- `rmonEventsV2`
- `etherStatsTable`
- `historyControlTable`
- `etherHistoryTable`
- `hosts`
- `hostTopN`
- `matrix`
- `filter`
- `capture`
- `logTable`
<table>
<thead>
<tr>
<th>MIB Module</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>UDP-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>RMON-MIB-V1SMI/HC-RMON-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>Ether-Like-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>CISCO-PROCESs-MIB</td>
<td>Generic</td>
</tr>
<tr>
<td>OLD-CISCO-MEMORY</td>
<td>Generic</td>
</tr>
<tr>
<td>CISCO-AAA-SERVER-MIB</td>
<td>Feature</td>
</tr>
<tr>
<td>CISCO-AAA-SESSION-MIB</td>
<td>Feature</td>
</tr>
<tr>
<td>CISCO-EVC-MIB</td>
<td>Feature</td>
</tr>
<tr>
<td>CISCO-CLASS-BASED-QOS-MIB</td>
<td>Feature</td>
</tr>
<tr>
<td>CISCO-IGMP-SNOOPING-MIB</td>
<td>Feature</td>
</tr>
<tr>
<td>IEEE8023-LAG-MIB</td>
<td>Feature</td>
</tr>
</tbody>
</table>
The following generic MIBs are not supported in Cisco ME 2600X:

- BRIDGE-MIB
- ENTITY-STATE-MIB
- CISCO-IETF-ISDN-CAPABILITY
- CISCO-OTN-IF-MIB

Each MIB includes compliance and conformance groups—these are not expected to return any output.

ENTITY-MIB—This is used for entity mapping. There is only one entity in ME2600X and therefore no entity is mapped. As a result, this table does not respond with any data.

IP-MIB—ipNetToMediaTable, ipNetToPhysicalTable, ipDefaultRouterTable, and ipv6 related tables are not supported.

TCP-MIB—tcpListenerTable is not supported.

The following feature MIBs are not supported in Cisco ME 2600X:

- AAA
  - CISCO-RADIUS-MIB
  - CISCO-AAA-SERVER-EXT-MIB
  - CISCO-RADIUS-EXT-MIB

- IGMP
  - IGMP-MIB.my

---

**Note**

Access tables with table name are not supported.

---

### Understanding SNMP Traps

Cisco ME 2600X uses SNMP traps to generate all the alarms and events. The traps contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity.
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service-affecting).
- Date and time stamp showing when the alarm occurred.

### Generic IETF Traps

Cisco ME 2600X supports the generic IETF traps listed in the table below.
Table 26: Supported Generic IETF Traps

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldStart</td>
<td>Agent up, cold start.</td>
</tr>
<tr>
<td>warmStart</td>
<td>Agent up, warm start.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Community string does not match.</td>
</tr>
<tr>
<td>linkdown</td>
<td>Test linkdown trap.</td>
</tr>
<tr>
<td>linkup</td>
<td>Test linkup trap.</td>
</tr>
</tbody>
</table>

Examples of IETF Traps

coldStart

DISMAN-EVENT-MIB::sysUpTimeInstance = 21775
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::coldStart
CERENT-454-MIB::cerent454NodeId.0 = 20110705135346D
CERENT-454-MIB::cerent454AlarmState.1.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"

warmStart

DISMAN-EVENT-MIB::sysUpTimeInstance = 21775
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::warmStart
CERENT-454-MIB::cerent454NodeId.0 = 20110705135346D
CERENT-454-MIB::cerent454AlarmState.1.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"

Authentication

DISMAN-EVENT-MIB::sysUpTimeInstance = 6335948
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::Authentication
CERENT-454-MIB::cerent454NodeId.0 = 20110705121300D
CERENT-454-MIB::cerent454AlarmState.1.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"

linkup, linkdown

Snmptrap sample for mgmt. i/f shut/noshut

blirst-ong-lnx1:168> snmptrapd -f -Lo -Oq -Ot -F "%V
%B
%N
%w
%q
%P
%v

" 40000
2012-09-10 16:32:32 NET-SNMP version 5.1.2 Started.
10.64.106.180
0
0
TRAP2, SNMP v2c, community public
DISMAN-EVENT-MIB::sysUpTimeInstance = 255394
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::enterprises.9.9.43.2.0.1
SNMPv2-SMI::enterprises.9.9.43.1.1.6.1.3.2 = 1
SNMPv2-SMI::enterprises.9.9.43.1.1.6.1.4.2 = 2
SNMPv2-SMI::enterprises.9.9.43.1.1.6.1.5.2 = 3
10.64.106.180
0
0
TRAP2, SNMP v2c, community public
DISMAN-EVENT-MIB::sysUpTimeInstance = 256172
Understanding SNMP Community Names

Community names are used to group SNMP trap destinations.

Understanding SNMP Messages

SNMP uses the following messages to communicate between the manager and the agent.

- Get
- GetNext
- GetResponse
- Set
- Trap

The Get and GetNext messages allow the manager to request information for a specific variable. The agent, upon receiving a Get or GetNext message, will issue a GetResponse message to the manager with either the information requested or an error indication as to why the request cannot be processed.

A Set message allows the manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. The agent will then respond with a GetResponse message indicating the change has been made or an error indication as to why the change cannot be made.

The Trap message allows the agent to inform the manager of an important event. An SNMP Trap is a change–of–state (COS) message—it could mean an alarm, a clear or simply a status message.
This chapter describes IP Source Guard for Service Instance and procedures to configure IP Source Guard for Service Instance.

- IP Source Guard for Service Instance, page 281
- Restrictions for IP Source Guard, page 281
- Configuring IP Source Guard for a Service Instance, page 282
- Configuring IP Source Guard With Static IP, page 284
- Example, page 284
- Verification, page 285
- Troubleshooting, page 286

**IP Source Guard for Service Instance**

An IP source guard filters a source IP address on a layer 2 port and prevents malicious hosts from impersonating a legitimate host. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted layer 2 access ports.

Initially, all IP traffic on the service instance is blocked except for DHCP packets that are captured by DHCP snooping. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, the IP source guard for service instance feature automatically creates an access control list (ACL) to permit that traffic. Traffic from other hosts is denied. This filtering limits the ability of a host to attack the network by claiming the IP address of a neighbor host.

Cisco ME 2600X supports a maximum of 511 static IP clients.

**Restrictions for IP Source Guard**

- The number of ACLs and ACEs that can be configured as part of IP source guard are bounded by the hardware resources on the line card.
The IP source guard is meant to verify host source IP information. Only ingress traffic is filtered. It is not applicable to egress direction.

The IP source guard is not effective for software forwarded packets. When a non-recoverable TCAM exception occurs for the IP source guard, the IP filtering is not effective and packets are permitted.

IP source guard is supported on port-channel service instances.

IP source guard is not supported over management interface.

IP source guard should be enabled on only 128 Bridge-domains.

Static IP source guard entry gets priority over the dynamic DHCP snooping.

Renewing the DHCP client IP address after removing the static IP source address results in a stale entry in the IP source guard table.

## Configuring IP Source Guard for a Service Instance

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port` or `interface port-channel` `type`
4. `ip verify source bridge-domain dhcp-snooping`
5. `[no] service instance id ethernet [service-name]`
6. `encapsulation dot1q vlan-id`
7. `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 2-to-1 dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id}} {symmetric}`
8. `[no] bridge-domain bridge-id`
9. `exit`
10. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2. configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### IP Source Guard for Service Instance

#### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | Specifies the interface to configure.  
  - `slot/port` - Specifies the location of the interface.  
  - `type` - Specifies the port channel interface. |
| `interface gigabitethernet slot/port` or `interface tengigabitethernet slot/port` or `interface port-channel type` | Example:  
  `Switch(config)# interface gigabitethernet 0/1` |
| **Step 4** | Enables the IP source guard states. The `dhcp-snooping` option applies the feature to all VLANs on the interface that have DHCP snooping enabled. |
| `ip verify source bridge-domain dhcp-snooping` | Example:  
  `Switch(config-if)# ip verify source bridge-domain dhcp-snooping` |
| **Step 5** | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| `[no] service instance id ethernet [service-name]` | Example:  
  `Switch(config-if)# service instance 101 ethernet` |
| **Step 6** | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| `encapsulation dot1q vlan-id` | Example:  
  `Switch(config-if-srv)# encapsulation dot1q 13` |
| **Step 7** | Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.  
  **Note** In order for the device to distinguish if the packet is DHCP, all tags must be in pop state; push and translate states are not supported. |
| `rewrite ingress tag {push {dot1q vlan-id | dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id | dot1q vlan-id dot1q vlan-id} | pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-id} | 1-to-2 {dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-1 {dot1q vlan-id second-dot1q vlan-id} | 2-to-2 {dot1q vlan-id second-dot1q vlan-id}} symmetric` | Example:  
  `Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric` |
| **Step 8** | Binds the service instance to a bridge domain instance where `bridge-id` is the identifier for the bridge domain instance. |
| `[no] bridge-domain bridge-id` | Example:  
  `Switch(config-if-srv)# bridge-domain 12` |
| **Step 9** | Exits service instance configuration mode. |
| `exit` | Example:  
  `Switch(config-if-srv)# exit` |
| **Step 10** | Exits configuration mode. |
| `end` | Example:  
  `Switch(config)# end` |
Configuring IP Source Guard With Static IP

### SUMMARY STEPS
1. enable
2. configure terminal
3. ip source binding mac-address bridge-domain bridge-id interface type mod /port
4. end

### 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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip source binding mac-address bridge-domain bridge-id interface type mod /port</td>
<td>Adds the static entry.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip source binding 0000.0000.0163 bridge-domain 52 1.1.1.163 interface Gi0/18 efp 163</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Example

This example shows how to configure IP source guard for a service instance with single tag (Dot1q) encapsulation.

Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# service instance 71 ethernet
Switch(config-if-srv)# encapsulation dot1q 71
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# exit
Switch(config-if)# ip verify source bridge-domain dhcp-snooping
This example shows how to configure IP source guard for a service instance with double tag (QinQ) encapsulation.

Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# service instance 71 ethernet
Switch(config-if-srv)# encapsulation dot1q 71 second-dot1q 100
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# exit
Switch(config-if)# ip verify source bridge-domain dhcp-snooping

This example shows how to configure IP source guard for a service instance with untagged encapsulation.

Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# service instance 71 ethernet
Switch(config-if-srv)# encapsulation dot1q 71
Switch(config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# exit
Switch(config-if)# ip verify source bridge-domain dhcp-snooping

This example shows how to configure IP source guard for a service instance with default encapsulation.

Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# service instance 71 ethernet
Switch(config-if-srv)# encapsulation default
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# exit
Switch(config-if)# ip verify source bridge-domain dhcp-snooping

This example shows how to configure IP source guard for a service instance with single tag encapsulation on a port-channel interface.

Switch# enable
Switch# configure terminal
Switch(config)# interface port-channel 2
Switch(config-if)# service instance 71 ethernet
Switch(config-if-srv)# encapsulation dot1q 100
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# exit
Switch(config-if)# ip verify source bridge-domain dhcp-snooping

Verification

Use the **show ip verify source** to verify the configuration:

```
Switch# show ip verify source
Interface Filter-type Filter-mode IP-address Mac-address Vlan
----------- ----------- ----------- ---------------
Gi0/1 ip active 123.1.1.1 100
Gi0/1 ip active 123.1.1.2 100
Gi0/1 ip active 123.1.1.3 100
```
Mac filtering not supported for IP source guard.

Troubleshooting

Troubleshooting Scenarios for IP Source Guard feature

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP source guard not enabled</td>
<td>Use <code>show ip verify source</code> command to check if the entries exist.</td>
</tr>
<tr>
<td>DHCP snooping failures</td>
<td>1  Verify whether or not the issues are specific to DHCP snooping or IP source guard. Use the show <code>ip dhcp snooping binding</code> command to check the DHCP snooping bindings on the Cisco ME 2600X. If the expected entry is missing on Cisco ME 2600X, debug the DHCP snooping sessions and share the output with TAC.</td>
</tr>
<tr>
<td></td>
<td>2  If the entry is displayed on the Cisco ME 2600X then check IP source guard configuration on the interface. If the issue persists, contact TAC.</td>
</tr>
</tbody>
</table>
CHAPTER 14

DHCP Snooping

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping in Cisco IOS Release 12.2SX.

Note

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, located at:

- Understanding DHCP Snooping, page 287
- Default Configuration for DHCP Snooping, page 293
- Restrictions for DHCP Snooping, page 293
- Configuring DHCP Snooping, page 295
- Configuration Examples for the Database Agent, page 308
- Displaying a Binding Table, page 312

Understanding DHCP Snooping

Overview of DHCP Snooping

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.
Other security features, such as dynamic ARP inspection (DAI), also use information stored in the DHCP snooping binding database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

The DHCP snooping feature is implemented in software on the route processor (RP). Therefore, all DHCP messages for enabled VLANs are intercepted in the PFC and directed to the RP for processing.

**Trusted and Untrusted Sources**

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.

In an enterprise network, devices under your administrative control are trusted sources. These devices include the switches, routers, and servers in your network. Any device beyond the firewall or outside your network is an untrusted source. Host ports and unknown DHCP servers are generally treated as untrusted sources.

A DHCP server that is on your network without your knowledge on an untrusted port is called a *spurious DHCP server*. A spurious DHCP server is any piece of equipment that is loaded with DHCP server enabled. Some examples are desktop systems and laptop systems that are loaded with DHCP server enabled, or wireless access points honoring DHCP requests on the wired side of your network. If spurious DHCP servers remain undetected, you will have difficulties troubleshooting a network outage. You can detect spurious DHCP servers by sending dummy DHCPDISCOVER packets out to all of the DHCP servers so that a response is sent back to the switch.

In a service provider environment, any device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In the switch, you indicate that a source is trusted by configuring the trust state of its connecting interface. The default trust state of all interfaces is untrusted. You must configure DHCP server interfaces as trusted. You can also configure other interfaces as trusted if they connect to devices (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces, as untrusted DHCP messages are forwarded only to trusted interfaces.

**DHCP Snooping Binding Database**

The DHCP snooping binding database is also referred to as the DHCP snooping binding table.

The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces.

The DHCP snooping feature updates the database when the switch receives specific DHCP messages. For example, the feature adds an entry to the database when the switch receives a DHCPACK message from the server. The feature removes the entry in the database when the IP address lease expires or the switch receives a DHCPRELEASE message from the host.
Each entry in the DHCP snooping binding database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

Packet Validation

The switch validates DHCP packets received on the untrusted interfaces of VLANs with DHCP snooping enabled. The switch forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

- The switch receives a packet (such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet) from a DHCP server outside the network or firewall.
- The switch receives a packet on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match. This check is performed only if the DHCP snooping MAC address verification option is turned on.
- The switch receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.
- The switch receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0 in giaddr.

To support trusted edge switches that are connected to untrusted aggregation-switch ports, you can enable the DHCP option-82 on untrusted port feature, which enables untrusted aggregation-switch ports to accept DHCP packets that include option-82 information. Configure the port on the edge switch that connects to the aggregation switch as a trusted port.

Note

With the DHCP option-82 on untrusted port feature enabled, use dynamic ARP inspection on the aggregation switch to protect untrusted input interfaces.

DHCP Snooping Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP snooping option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The figure below is an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent is configured.
with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

*Figure 20: DHCP Relay Agent in a Metropolitan Ethernet Network*

![Diagram showing DHCP Relay Agent in a Metropolitan Ethernet Network]

When you enable the DHCP snooping information option-82 on the switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit ID suboption).
- If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, or the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. The DHCP server then echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

When the previously described sequence of events occurs, the values in these fields in the figure below do not change:

- Circuit ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit ID type
  - Length of the circuit ID type

- Remote ID suboption fields
Suboption type
Length of the suboption type
Remote ID type
Length of the circuit ID type

The figure below shows the packet formats for the remote ID suboption and the circuit ID suboption. The switch uses the packet formats when DHCP snooping is globally enabled and when the ip dhcp snooping information option global configuration command is entered. For the circuit ID suboption, the module field is the slot number of the module.

Figure 21: Suboption Packet Formats

Circuit ID Suboption Frame Format

Remote ID Suboption Frame Format

Overview of the DHCP Snooping Database Agent

To retain the bindings across reloads, you must use the DHCP snooping database agent. Without this agent, the bindings established by DHCP snooping are lost upon reload, and connectivity is lost as well.

The database agent stores the bindings in a file at a configured location. Upon reload, the switch reads the file to build the database for the bindings. The switch keeps the file current by writing to the file as the database changes.

The format of the file that contains the bindings is as follows:

```xml
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...```
Each entry in the file is tagged with a checksum that is used to validate the entries whenever the file is read. The initial-checksum entry on the first line helps distinguish entries associated with the latest write from entries that are associated with a previous write.

This is a sample bindings file:

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
  1.1.1.1 512 0001.0001.0005 3EBE2881 Gi1/1 e5e1e733
  1.1.1.1 512 0001.0001.0002 3EBE2881 Gi1/1 4b3486ec
  1.1.1.1 1536 0001.0001.0004 3EBE2881 Gi1/1 f0e02872
  1.1.1.1 1024 0001.0001.0003 3EBE2881 Gi1/1 ac41adf9
  1.1.1.1 1 0001.0001.0001 3EBE2881 Gi1/1 34a3273e
END
```

Each entry holds an IP address, VLAN, MAC address, lease time (in hex), and the interface associated with a binding. At the end of each entry is a checksum that is based on all the bytes from the start of the file through all the bytes associated with the entry. Each entry consists of 72 bytes of data, followed by a space, followed by a checksum.

Upon bootup, when the calculated checksum equals the stored checksum, the switch reads entries from the file and adds the bindings to the DHCP snooping database. If the calculated checksum does not equal the stored checksum, the entry read from the file is ignored and so are all the entries following the failed entry. The switch also ignores all those entries from the file whose lease time has expired. (This is possible because the lease time might indicate an expired time.) An entry from the file is also ignored if the interface referred to in the entry no longer exists on the system, or if it is a device port or a DHCP snooping-trusted interface.

When the switch learns of new bindings or when it loses some bindings, the switch writes the modified set of entries from the snooping database to the file. The writes are performed with a configurable delay to batch as many changes as possible before the actual write happens. Associated with each transfer is a timeout after which a transfer is aborted if it is not completed. These timers are referred to as the write delay and abort timeout.

**DHCP Snooping Host Tracking**

The DHCP snooping host tracking feature implements a cache to learn VLAN and MAC addresses to port the mapping of clients from snooped DHCP request packets and uses this information to forward snooped DHCP reply packets.

This feature improves DHCP snooping packet processing performance for DHCP reply packets by not needing to lookup the hardware VLAN and MAC address table in order to determine the port on which to send the DHCP reply packets. This feature is useful in deployments where it is not possible to use the DHCP snooping information option along with DHCP (for example, when the server does not support DHCP information option). If DHCP is configured it takes higher precedence than the DHCP snooping host tracking feature in determining the port on which to forward reply packets.

The DHCP snooping host tracking feature is off by default (see Enabling DHCP Snooping Host Tracking, on page 298).
Default Configuration for DHCP Snooping

Table 27: Default Configuration Values for DHCP Snooping

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value/State</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping host tracking feature</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping information option</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP option-82 on untrusted port feature</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping limit rate</td>
<td>None</td>
</tr>
<tr>
<td>DHCP snooping trust</td>
<td>Untrusted</td>
</tr>
<tr>
<td>DHCP snooping vlan</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping spurious server detection</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping detect spurious interval</td>
<td>30 minutes</td>
</tr>
</tbody>
</table>

Restrictions for DHCP Snooping

When configuring DHCP snooping, note these restrictions:

- The DHCP snooping database stores at least 8,000 bindings.
- Two Snooping devices are not supported. Snooping device should always face the client.
- When a large number of clients try to establish bindings simultaneously and the packets pass through a relay agent, it may result in a slow binding.
- Maximum number of supported DHCP binding entries on an interface is 512.

When configuring DHCP snooping, follow these guidelines:

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the `ip dhcp snooping trust` interface configuration command.

If a Layer 2 LAN port is connected to a DHCP client, configure the port as untrusted by entering the `no ip dhcp snooping trust` interface configuration command.

If DHCP snooping information option is configured, it takes higher precedence than the DHCP snooping host tracking feature in determining the port on which to forward reply packets.

Minimum DHCP Snooping Configuration

The minimum configuration steps for the DHCP snooping feature are as follows:

1. Define and configure the DHCP server.

2. Enable DHCP snooping on at least one VLAN.
   
   By default, DHCP snooping is inactive on all VLANs. See Enabling DHCP Snooping on a Bridge Domain, on page 301.

3. Ensure that DHCP server is connected through a trusted interface.
   
   By default, the trust state of all interfaces is untrusted. See Configuring the DHCP Trust State on Layer 2 LAN Interfaces, on page 302.

4. Configure the DHCP snooping database agent.
   
   This step ensures that database entries are restored after a restart or switchover. See Configuring the DHCP Snooping Database Agent, on page 305.

5. Enable DHCP snooping globally.
   
   The feature is not active until you complete this step. See Enabling DHCP Snooping Globally, on page 295.

If you are configuring the switch for DHCP relay, the following additional steps are required:

1. Define and configure the DHCP relay agent IP address.
   
   If the DHCP server is in a different subnet from the DHCP clients, configure the server IP address in the helper address field of the client side VLAN.

2. Configure DHCP option-82 on untrusted port.
   
   See Enabling the DHCP Option-82 on Untrusted Port Feature, on page 297.
Configuring DHCP Snooping

Enabling DHCP Snooping Globally

Note
Configure this command as the last configuration step (or enable the DHCP feature during a scheduled maintenance period) because after you enable DHCP snooping globally, the switch drops DHCP requests until you configure the ports.

To enable DHCP snooping globally, complete the following steps:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip dhcp snooping`
4. `do show ip dhcp snooping`
5. `exit`

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.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp snooping</td>
<td>Enables DHCP snooping globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> do show ip dhcp snooping</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# do show ip dhcp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>
This example shows how to enable DHCP snooping globally:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# do show ip dhcp snooping
Switch DHCP snooping is enabled
Switch(config)#
```

When DHCP snooping is disabled and DAI is enabled, the switch shuts down all the hosts because all ARP entries in the ARP table are checked against a nonexistent DHCP database. When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny ARP packets.

---

### Enabling DHCP Option-82 Data Insertion

To enable DHCP option-82 data insertion, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip dhcp snooping information option`
4. `do show ip dhcp snooping | include 82`
5. `exit`

**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.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp snooping information option</td>
<td>Enables DHCP option-82 data insertion</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# ip dhcp snooping information option</code></td>
<td></td>
</tr>
</tbody>
</table>

---

Note: This information is from the Cisco ME 2600X Series Ethernet Access Switch Software Configuration Guide, page 296.
### Enabling the DHCP Option-82 on Untrusted Port Feature

To enable untrusted ports to accept DHCP packets that include option-82 information, perform this task:

**Before You Begin**

- With the DHCP option-82 on untrusted port feature enabled, the switch does not drop DHCP packets that include option-82 information that are received on untrusted ports. Do not use the `ip dhcp snooping information option allowed-untrusted` command on an aggregation switch to which any untrusted devices are connected.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip dhcp snooping information option allow-untrusted`
4. `do show ip dhcp snooping`
5. `exit`
Enabling DHCP Snooping Host Tracking

To configure the DHCP Snooping Host Tracking feature, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. ip dhcp snooping track host
4. clear ip dhcp snooping track host
5. exit
**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. Enters global configuration mode.</td>
</tr>
</tbody>
</table>

- **Example:**
  ```
  Switch> enable
  ```

<table>
<thead>
<tr>
<th><strong>Step 2</strong> configure terminal</th>
<th>Enables the DHCP snooping host tracking feature.</th>
</tr>
</thead>
</table>

- **Example:**
  ```
  Switch# configure terminal
  ```

<table>
<thead>
<tr>
<th><strong>Step 3</strong> ip dhcp snooping track host</th>
<th>Clears the DHCP snooping host track cache.</th>
</tr>
</thead>
</table>

- **Example:**
  ```
  Switch(config)# ip dhcp snooping track host
  ```

<table>
<thead>
<tr>
<th><strong>Step 4</strong> clear ip dhcp snooping track host</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
</table>

- **Example:**
  ```
  Switch(config)# clear ip dhcp snooping track host
  ```

<table>
<thead>
<tr>
<th><strong>Step 5</strong> exit</th>
<th></th>
</tr>
</thead>
</table>

- **Example:**
  ```
  Switch(config)# exit
  ```

This example shows how to enable the DHCP snooping host tracking feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no ip dhcp snooping information option
Switch(config)# ip dhcp snooping track host
Switch(config)# exit
```

This example shows how to display the contents of the DHCP snooping host tracking cache:

```
Switch# show ip dhcp snooping track host
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>interface</th>
<th>mac</th>
<th>time left</th>
</tr>
</thead>
<tbody>
<tr>
<td>203</td>
<td>G13/47</td>
<td>000a.cb00.126d</td>
<td>expired</td>
</tr>
<tr>
<td>204</td>
<td>G11/47</td>
<td>000a.cc00.1262</td>
<td>expired</td>
</tr>
<tr>
<td>202</td>
<td>G12/47</td>
<td>000a.ca00.125d</td>
<td>expired</td>
</tr>
<tr>
<td>204</td>
<td>G11/47</td>
<td>000a.cc00.1263</td>
<td>expired</td>
</tr>
<tr>
<td>203</td>
<td>G13/47</td>
<td>000a.cb00.1276</td>
<td>expired</td>
</tr>
<tr>
<td>201</td>
<td>G11/47</td>
<td>000a.c900.1273</td>
<td>expired</td>
</tr>
</tbody>
</table>

---

**Enabling DHCP Snooping MAC Address Verification**

With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The
source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet.

To enable DHCP snooping MAC address verification, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip dhcp snooping verify mac-address
4. do show ip dhcp snooping | include hwaddr
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

   enable

   Example: Switch> enable

- Enables privileged EXEC mode.
  - Enter your password if prompted.

| **Step 2**

   configure terminal

   Example: Switch# configure terminal

- Enters global configuration mode.

| **Step 3**

   ip dhcp snooping verify mac-address

   Example: Switch(config)# ip dhcp snooping verify mac-address

- Enables DHCP snooping MAC address verification.

| **Step 4**

   do show ip dhcp snooping | include hwaddr

   Example: Switch(config)# do show ip dhcp snooping | include hwaddr

- Verifies the configuration.

| **Step 5**

   exit

   Example: Switch(config)# exit

- Returns to privileged EXEC mode.

This example shows how to disable DHCP snooping MAC address verification:

Switch(config)# no ip dhcp snooping verify mac-address
Switch(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is disabled
Switch(config)#

This example shows how to enable DHCP snooping MAC address verification:

Switch(config)# ip dhcp snooping verify mac-address
Switch(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is enabled
Switch(config)#
Enabling DHCP Snooping on a Bridge Domain

By default, the DHCP snooping feature is inactive on all Bridge Domains. You may enable the feature on a single Bridge Domain or a range of Bridge Domains.

When enabled on a Bridge Domain, the DHCP snooping feature creates four entries in the VACL table in the MFC3. These entries cause the PFC3 to intercept all DHCP messages on this Bridge Domain and send them to the RP. The DHCP snooping feature is implemented in software on the RP.

To enable DHCP snooping on bridge domains, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip dhcp snooping bridge-domain {{bridge-domain_ID [bridge-domain_ID]} | {bridge-domain_range}}
4. do show ip dhcp snooping
5. exit

**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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp snooping bridge-domain {{bridge-domain_ID [bridge-domain_ID]}</td>
<td>{bridge-domain_range}}</td>
</tr>
<tr>
<td>Example: Switch(config)# ip dhcp snooping bridge-domain 1 or Switch(config)# ip dhcp snooping bridge-domain 1-10,40-50,61</td>
<td>Note: Do not use this command to configure the second node (server side). You can configure DHCP snooping for a single Bridge Domain or a range of Bridge Domains:</td>
</tr>
<tr>
<td></td>
<td>• To configure a single Bridge Domain, enter a single Bridge Domain number.</td>
</tr>
<tr>
<td></td>
<td>• To configure a range of Bridge Domains, enter a beginning and an ending Bridge Domain number or a dash-separated pair of Bridge Domain numbers.</td>
</tr>
<tr>
<td></td>
<td>• You can enter a comma-separated list of Bridge Domain numbers and dash-separated pairs of Bridge Domain numbers.</td>
</tr>
</tbody>
</table>
### Configuring the DHCP Trust State on Layer 2 LAN Interfaces

To configure DHCP trust state on a Layer 2 LAN interface, complete the following steps:

#### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>do show ip dhcp snooping</code></td>
<td>Verifies the configuration.</td>
</tr>
</tbody>
</table>
|      | **Example:**  
|      | `Switch(config)# do show ip dhcp snooping` | |
| 5    | `exit` | Returns to privileged EXEC mode. |
|      | **Example:**  
|      | `Switch(config)# exit` | |

This example shows how to enable DHCP snooping on Bridge Domains 10 through 12:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping bridge-domain 10 12
```

This example shows another way to enable DHCP snooping on Bridge Domains 10 through 12:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping bridge-domain 10-12
```

This example shows another way to enable DHCP snooping on Bridge Domains 10 through 12:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping bridge-domain 10,11,12
```

This example shows how to enable DHCP snooping on Bridge Domains 10 through 12 and Bridge Domain 15:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping bridge-domain 10-12,15
```

This example shows how to verify the configuration:

```
Switch(config)# do show ip dhcp snooping
```

DHCP snooping is enabled
DHCP snooping is configured on following bridge-domains: 10-12,15
DHCP snooping is operational on following bridge-domains: none
DHCP snooping is configured on the following Interfaces:

```
Insertion of option 82 is enabled
Verification of hwaddr field is enabled
Interface       Trusted       Rate limit (pps)
------------------------- ------ ----------------
Switch#```
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface \{type slot/port | port-channel number\}
4. ip dhcp snooping trust
5. do show ip dhcp snooping | begin pps
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  * Enter your password if prompted.  |
| **Example:** Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode.  |
| **Example:** Switch# configure terminal |
| **Step 3** interface \{type slot/port | port-channel number\} | Selects the interface to configure.  |
| **Example:**  
  Switch(config)# interface port-channel 1  
  or  
  Switch(config)# interface GigabitEthernet 0/1 |
| **Step 4** ip dhcp snooping trust | Configures the interface as trusted.  |
| **Example:**  
  Switch(config-if)# ip dhcp snooping trust |
| **Step 5** do show ip dhcp snooping | Verifies the configuration.  |
| **Example:**  
  Switch(config-if)# do show ip dhcp snooping | begin pps |
| **Step 6** end | Returns to privileged EXEC mode.  |
| **Example:**  
  Switch(config-if)# end |

This example shows how to configure Fast Ethernet port 5/12 as trusted:

Switch# configure terminal  
Switch(config)# interface FastEthernet5/12  
Switch(config-if)# ip dhcp snooping trust  
Switch(config-if)# do show ip dhcp snooping | begin pps
Configuring DHCP Snooping Rate Limiting on Layer 2 LAN Interfaces

To configure DHCP snooping rate limiting on a Layer 2 LAN interface, complete the following steps:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface {type slot/port | port-channel number}`
4. `ip dhcp snooping limit rate rate`
5. `do show ip dhcp snooping | begin pps`
6. `end`

### 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>enable</strong>&lt;br&gt;Example: Switch&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Example: Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**interface {type slot/port</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip dhcp snooping limit rate <em>rate</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# ip dhcp snooping limit rate 10</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>do show ip dhcp snooping</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# do show ip dhcp snooping</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
</tbody>
</table>

**What to Do Next**

When configuring DHCP snooping rate limiting on a Layer 2 LAN interface, note the following information:

- We recommend an untrusted rate limit of not more than 100 packets per second (pps).
- If you configure rate limiting for trusted interfaces, you might need to increase the rate limit on trunk ports carrying more than one VLAN on which DHCP snooping is enabled.
- When you configure rate limit as 1 pps, the interface immediately goes to error disable state on receiving a DHCP packet.
- DHCP snooping puts ports where the rate limit is exceeded into the error-disabled state.

This example shows how to configure DHCP packet rate limiting to 100 pps on Fast Ethernet port 5/12:

```
Switch# configure terminal
Switch(config)# interface FastEthernet 5/12
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# do show ip dhcp snooping | begin pps
Interface Trusted Rate limit (pps)
------------------------ ------- ----------------
FastEthernet5/12 no 100
Switch#
```

**Configuring the DHCP Snooping Database Agent**

To configure the DHCP snooping database agent, complete one or more of the following steps:

- **Note** The URL in the following task indicates either TFTP:filename or SD flash:filename.
**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip dhcp snooping database { _url | write-delay seconds | timeout seconds }`
4. `clear ip dhcp snooping database statistics`
5. `renew ip dhcp snooping database [validation none] [url]`
6. `ip dhcp snooping binding mac address bridge-domain <bridge-domain_id> ip_address interface <ifname> efp_id <efp-id> expiry <sec>`
7. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt;</code> <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch#</code> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `ip dhcp snooping database { _url</td>
<td>write-delay seconds</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)#</code> <code>ip dhcp snooping database tftp://202.153.144.25//auto/tftp-abc-user1/name/DHCP_Database/name_database_xyz</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#</code> <code>ip dhcp snooping database timeout 10</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#</code> <code>ip dhcp snooping database write-delay 30</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>clear ip dhcp snooping database statistics</code></td>
<td>Clears the statistics associated with the database agent.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)#</code> <code>clear ip dhcp snooping database statistics</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>renew ip dhcp snooping database [validation none] [url]</code></td>
<td>Requests the read entries from a file at the given URL.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)#</code> <code>renew ip dhcp snooping database validation none tftp://202.153.144.25//auto/tftp-abc-user1/name/DHCP_Database/name_database_xyz</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>ip dhcp snooping binding mac address bridge-domain &lt;bridge-domain_id&gt; ip_address interface &lt;ifname&gt; efp_id &lt;efp-id&gt; expiry &lt;sec&gt;</code></td>
<td>Adds bindings to the snooping database.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)#</code> <code>ip dhcp snooping binding 0000.1111.2222 bridge-domain 1 1.1.1.1 int gi0 efp_id 1 expiry 100</code></td>
<td></td>
</tr>
</tbody>
</table>
When configuring the DHCP snooping database agent, note the following information:

- The DHCP snooping database stores at least 8,000 bindings.
- Store the file on a TFTP server to avoid consuming storage space on the switch storage devices.
- Network-based URLs (such as TFTP and FTP) require that you create an empty file at the configured URL before the switch can write the set of bindings for the first time.

This example shows how to verify the configuration:

```
Switch# show ip dhcp snooping database [detail]
```

```
Agent URL :
tftp://202.153.144.25//auto/tftp-abc-user1/name/DHCP_Database/name_database_xyz
Write delay Timer : 30 seconds
Abort Timer : 10 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeeded Time : None
Last Failed Time : 23:40:32 IST Sat Sep 11 1993
Last Failed Reason : Expected more data on read.

Total Attempts : 1 Startup Failures : 0
Successful Transfers : 0 Failed Transfers : 1
Successful Reads : 0 Failed Reads : 1
Successful Writes : 0 Failed Writes : 0
Media Failures : 0
First successful access: Read

Last ignored bindings counters :
Binding Collisions : 0 Expired leases : 0
Invalid interfaces : 0 Unsupported vlans : 0
Parse failures : 0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions : 0 Expired leases : 0
Invalid interfaces : 0 Unsupported vlans : 0
Parse failures : 0
```
**Configuration Examples for the Database Agent**

**Example 1: Enabling the Database Agent**

The following example shows how to configure the DHCP snooping database agent to store the bindings at a given location and to view the configuration and operating state:

```
Switch> enable
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
Switch#
```

Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

<table>
<thead>
<tr>
<th>Total Attempts</th>
<th>21</th>
<th>Startup Failures</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Transfers</td>
<td>0</td>
<td>Failed Transfers</td>
<td>21</td>
</tr>
<tr>
<td>Successful Reads</td>
<td>0</td>
<td>Failed Reads</td>
<td>0</td>
</tr>
<tr>
<td>Successful Writes</td>
<td>0</td>
<td>Failed Writes</td>
<td>21</td>
</tr>
<tr>
<td>Media Failures</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

First successful access: Read

<table>
<thead>
<tr>
<th>Last ignored bindings counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding Collisions</td>
</tr>
<tr>
<td>Expired leases</td>
</tr>
<tr>
<td>Invalid interfaces</td>
</tr>
<tr>
<td>Unsupported Bridge Domains</td>
</tr>
<tr>
<td>Parse failures</td>
</tr>
<tr>
<td>Last Ignored Time</td>
</tr>
</tbody>
</table>

The first three lines of output show the configured URL and related timer-configuration values. The next three lines show the operating state and the amount of time left for expiry of write delay and abort timers.

Among the statistics shown in the output, startup failures indicate the number of attempts to read or create the file that failed on bootup.

Create a temporary file on the TFTP server with the `touch` command in the TFTP server daemon directory. With some UNIX implementations, the file should have full read and write access permissions (777).
DHCP snooping bindings are keyed on the MAC address and Bridge Domain combination. If an entry in the remote file has an entry for a given MAC address and Bridge Domain set for which the switch already has a binding, the entry from the remote file is ignored when the file is read. This condition is referred to as the binding collision.

An entry in a file may no longer be valid because the lease indicated by the entry may have expired by the time it is read. The expired leases counter indicates the number of bindings that are ignored because of this condition. The Invalid interfaces counter refers to the number of bindings that have been ignored when the interface referred by the entry either does not exist on the system or is a router or DHCP snooping trusted interface (if it exists) when the read happened. Unsupported Bridge Domains refers to the number of entries that have been ignored because the indicated Bridge Domain is not supported on the system. The Parse failures counter provides the number of entries that have been ignored when the switch is unable to interpret the meaning of the entries from the file.

The switch maintains two sets of counters for these ignored bindings. One provides the counters for a read that has at least one binding ignored by at least one of these conditions. These counters are shown as the “Last ignored bindings counters.” The total ignored bindings counters provides a sum of the number of bindings that have been ignored because of all the reads since the switch bootup. These two sets of counters are cleared by the clear command. The total counter set may indicate the number of bindings that have been ignored since the last clear.

### Example 2: Reading Binding Entries from a TFTP File

To manually read the entries from a TFTP file, complete the following steps:

#### SUMMARY STEPS

1. enable
2. show ip dhcp snooping database
3. renew ip dhcp snoop data url
4. show ip dhcp snoop data
5. show ip dhcp snoop bind

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>show ip dhcp snooping database</td>
<td>Displays the DHCP snooping database agent statistics.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip dhcp snooping database</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>renew ip dhcp snoop data url</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Switch# renew ip dhcp snooping database validation none tftp://202.153.144.25//auto/tftp-abc-user1/name/DHCP_Database/name_database_xyz</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show ip dhcp snoop data</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Switch# show ip dhcp snoop data</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>show ip dhcp snoop bind</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Switch# show ip dhcp snoop bind</strong></td>
</tr>
</tbody>
</table>

This is an example of how to manually read entries from the tftp://10.1.1.1/directory/file:

```plaintext
Switch# show ip dhcp snooping database

Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts : 0 Startup Failures : 0
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
Media Failures : 0

Switch# renew ip dhcp snoop data tftp://10.1.1.1/directory/file
Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !
[OK - 457 bytes]
Database downloaded successfully.

Switch#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read succeeded.

Switch# show ip dhcp snoop data

Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
```
Example 3: Adding Information to the DHCP Snooping Database

To manually add a binding to the DHCP snooping database, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `show ip dhcp snooping binding`
3. `ip dhcp snooping binding binding_id bridge-domain bridge-domain_id interface interface efp_id expiry lease_time`
4. `show ip dhcp snooping binding`
## Displaying a Binding Table

The DHCP snooping binding table for each switch contains binding entries that correspond to untrusted ports. The table does not contain information about hosts interconnected with a trusted port because each interconnected switch will have its own DHCP snooping binding table.
This example shows how to display the DHCP snooping binding information for a switch:

```
Switch# show ip dhcp snooping binding
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IP Address</th>
<th>Lease (sec)</th>
<th>Type</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:B3:3F:3B:99</td>
<td>55.5.5.2</td>
<td>6943</td>
<td>dhcp-snooping</td>
<td>10</td>
</tr>
</tbody>
</table>

**FastEthernet6/10**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Client hardware MAC address</td>
</tr>
<tr>
<td>IP Address</td>
<td>Client IP address assigned from the DHCP server</td>
</tr>
<tr>
<td>Lease (seconds)</td>
<td>IP address lease time</td>
</tr>
<tr>
<td>Type</td>
<td>Binding type: dynamic binding learned by DHCP snooping or statically-configured binding</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN number of the client interface</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface that connects to the DHCP client host</td>
</tr>
</tbody>
</table>
Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) in Cisco IOS Release 12.2SX

- Understanding DAI, page 315
- Default DAI Configuration, page 319
- Restrictions for DAI, page 319
- Configuring DAI, page 320
- Example: DAI Configuration, page 331

Understanding DAI

Understanding ARP

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address.

Understanding ARP Spoofing Attacks

ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker’s computer and then to the router, switch, or host.
An ARP spoofing attack can target hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. The figure below shows an example of ARP cache poisoning.

**Figure 22: ARP Cache Poisoning**

Hosts A, B, and C are connected to the switch on interfaces A, B, and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch for Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, which is the topology of the classic *man-in-the-middle* attack.

### Understanding DAI and ARP Spoofing Attacks

DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

DAI ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the bridge domains and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

The switch logs dropped packets (see [Logging of Dropped Packets](#), on page 318).
You can configure DAI to drop ARP packets when the IP addresses in the packets are invalid or when the
MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header
(see Enabling Additional Validation, on page 325).

Interface Trust States and Network Security

DAI associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass
all DAI validation checks, and those arriving on untrusted interfaces undergo the DAI validation process.

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and
configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering
the network from a given switch bypass the security check. No other validation is needed at any other place
in the bridge domain or in the network. You configure the trust setting by using the `ip arp inspection trust`
interface configuration command.

Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted
can result in a loss of connectivity.

In the figure below, assume that both Switch A and Switch B are running DAI on the bridge domain that
includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected
to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch
A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between
Host 1 and Host 2 is lost.

**Figure 23: ARP Packet Validation on a Bridge Domain Enabled for DAI**

Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If
Switch A is not running DAI, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link
between the switches is configured as trusted). This condition can occur even though Switch B is running
DAI.

DAI ensures that hosts (on untrusted interfaces) connected to a switch running DAI do not poison the ARP
caches of other hosts in the network. However, DAI does not prevent hosts in other portions of the network
from poisoning the caches of the hosts that are connected to a switch running DAI.
In cases in which some switches in a bridge domain run DAI and other switches do not, configure the interfaces connecting such switches as untrusted. However, to validate the bindings of packets from switches where DAI is not configured, configure ARP ACLs on the switch running DAI. When you cannot determine such bindings, isolate switches running DAI at Layer 3 from switches not running DAI.

Note
Depending on the setup of the DHCP server and the network, it might not be possible to validate a given ARP packet on all switches in the bridge domain.

Rate Limiting of ARP Packets

The switch performs DAI validation checks, which rate limits incoming ARP packets to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate limited. You can change this setting by using the `ip arp inspection limit` interface configuration command.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you intervene. You can use the `errdisable recovery` global configuration command to enable error disable recovery so that ports automatically emerge from this state after a specified timeout period.

For configuration information, see Configuring ARP Packet Rate Limiting, on page 323.

Relative Priority of ARP ACLs and DHCP Snooping Entries

DAI uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the `ip arp inspection filter` global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Logging of Dropped Packets

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving bridge domain, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You use the `ip arp inspection log-buffer` global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. You specify the type of packets that are logged by using the `ip arp inspection bridge domain logging` global configuration command. For configuration information, see Configuring DAI Logging, on page 327.
Default DAI Configuration

The table below shows the default DAI configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAI</td>
<td>Disabled on all bridge domains.</td>
</tr>
<tr>
<td>Interface trust state</td>
<td>All interfaces are untrusted.</td>
</tr>
<tr>
<td>Rate limit of incoming ARP</td>
<td>The rate is 15 pps on untrusted interfaces, assuming that the network is a Layer</td>
</tr>
<tr>
<td>packets</td>
<td>2-switched network with a host connecting to as many as 15 new hosts per second.</td>
</tr>
<tr>
<td></td>
<td>The rate is unlimited on all trusted interfaces.</td>
</tr>
<tr>
<td></td>
<td>The burst interval is 1 second.</td>
</tr>
<tr>
<td>ARP ACLs for non-DHCP</td>
<td>No ARP ACLs are defined.</td>
</tr>
<tr>
<td>environments</td>
<td></td>
</tr>
<tr>
<td>Validation checks</td>
<td>No checks are performed.</td>
</tr>
<tr>
<td>Log buffer</td>
<td>When DAI is enabled, all denied or dropped ARP packets are logged.</td>
</tr>
<tr>
<td></td>
<td>The number of entries in the log is 32.</td>
</tr>
<tr>
<td></td>
<td>The number of system messages is limited to 5 per second.</td>
</tr>
<tr>
<td></td>
<td>The logging-rate interval is 1 second.</td>
</tr>
<tr>
<td>Per-bridge domain logging</td>
<td>All denied or dropped ARP packets are logged.</td>
</tr>
</tbody>
</table>

Restrictions for DAI

- DAI is an ingress security feature; it does not perform any egress checking.
- DAI is not effective for hosts connected to switches that do not support DAI or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with DAI checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for DAI.
- DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. For configuration information, see Configuring DHCP Snooping, on page 295.
- When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.
Dynamic ARP Inspection

Configuring DAI

Enabling DAI on Bridge Domains

You can enable DAI on a single bridge domain or a range of bridge domains:

• To enable a single bridge domain, enter a single bridge domain number.
• To enable a range of bridge domains, enter a dash-separated pair of bridge domain numbers.
• You can enter a comma-separated list of bridge domain numbers and dash-separated pairs of bridge domain numbers

To enable DAI on bridge domains, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. ip arp inspection bridge domain \{bridge-domain_ID | bridge-domain_range\}
4. do show ip arp inspection bridge-domain \{bridge-domain_ID\}
5. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Step 2 configure terminal | Enters global configuration mode. |
| Step 3 ip arp inspection bridge domain `{bridge-domain_ID | Enables DAI on bridge domains.  
  bridge-domain_range}` |
| Step 4 do show ip arp inspection bridge-domain `{bridge-domain_ID` | Verifies the configuration. |
| Step 5 end        | Returns to privileged EXEC mode. |

### Examples

This example shows how to enable DAI on bridge domains 10 through 12

```
Switch# configure terminal
Switch(config)# ip arp inspection bridge-domain 10-12
```

This example shows another way to enable DAI on bridge domains 10 through 12

```
Switch# configure terminal
Switch(config)# ip arp inspection bridge-domain 10,11,12
```

This example shows how to enable DAI on bridge domains 10 through 12 and bridge domain 15

```
Switch# configure terminal
Switch(config)# ip arp inspection bridge-domain 10-12,15
```

This example shows how to verify the configuration

```
Switch(config)# $arp inspection bridge-domain 1 | begin BD
```

<table>
<thead>
<tr>
<th>BD</th>
<th>Configuration</th>
<th>Operation</th>
<th>ACL Match</th>
<th>Static ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD</td>
<td>ACL Logging</td>
<td>DHCP Logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Deny</td>
<td>Deny</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the DAI Interface Trust State

The switch forwards ARP packets that it receives on a trusted interface, but does not check them. On untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the `ip arp inspection bridge domain logging` global configuration command. For more information, see Configuring DAI Logging, on page 327.

To configure the DAI interface trust state, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface {type1 slot/port | port-channel number}`
4. `ip arp inspection trust`
5. `do show ip arp inspection interfaces`
6. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code> Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code> Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`interface {type1 slot/port</td>
</tr>
<tr>
<td></td>
<td>Example: `Switch(config)# interface {type1 slot/port</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip arp inspection trust</code> Configures the connection between switches as trusted.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# ip arp inspection trust</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>do show ip arp inspection interfaces</code> Verifies the DAI configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# do show ip arp inspection interfaces</code></td>
</tr>
</tbody>
</table>
### Configuring ARP Packet Rate Limiting

When DAI is enabled, the switch performs ARP packet validation checks, which makes the switch vulnerable to an ARP-packet denial-of-service attack. ARP packet rate limiting can prevent an ARP-packet denial-of-service attack.

To configure ARP packet rate limiting on a port, perform this task:

#### Before You Begin

When configuring ARP packet rate limiting, note the following information:

- The default rate is 15 pps on untrusted interfaces and unlimited on trusted interfaces
- For rate pps, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps.
- The rate none keywords specify that there is no upper limit for the rate of incoming ARP packets that can be processed.
- (Optional) For burst interval seconds (default is 1), specify the consecutive interval, in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15.
- When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in the error-disabled state until you enable error-disabled recovery, which allows the port to emerge from the error-disabled state after a specified timeout period.
- Unless you configure a rate-limiting value on an interface, changing the trust state of the interface also changes its rate-limiting value to the default value for the configured trust state. After you configure the rate-limiting value, the interface retains the rate-limiting value even when you change its trust state. If you use the no ip arp inspection limit interface configuration command, the interface reverts to its default rate-limiting value.
For configuration guidelines about limiting the rate of incoming ARP packets on trunk ports and EtherChannel ports, see Restrictions for DAI, on page 319.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface {type slot/port | port-channel number}`
4. `ip arp inspection limit {rate pps [burst interval seconds] | none}`
5. `do show ip arp inspection interfaces`
6. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; <code>enable</code></td>
<td>Complete with your password.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`interface {type slot/port</td>
<td>port-channel number}`</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>interface GigabitEthernet 0/12</code></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>interface port-channel 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Configures ARP packet rate limiting.</td>
</tr>
<tr>
<td>`ip arp inspection limit {rate pps [burst interval seconds]</td>
<td>none}`</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <code>ip arp inspection limit rate 20 burst interval 2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>do show ip arp inspection interfaces</code></td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <code>do show ip arp inspection interfaces</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>
Example

This example shows how to configure ARP packet rate limiting on Gigabit Ethernet port 0/14:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 0/14
Switch(config-if)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if)# do show ip arp inspection interfaces | include Int|--|0/14

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate (pps)</th>
<th>Burst Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/14</td>
<td>Untrusted</td>
<td>20</td>
<td>2</td>
</tr>
</tbody>
</table>

Enabling Additional Validation

DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can enable additional validation on the destination MAC address, the sender and target IP addresses, and the source MAC address.

The additional validations do the following:

- **dst-mac**—Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

- **ip**—Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

- **src-mac**—Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling additional validation, note the following information:

- You must specify at least one of the keywords.
- Each `ip arp inspection validate` command overrides the configuration from any previous commands. If an `ip arp inspection validate` command enables `src-mac` and `dst-mac` validations, and a second `ip arp inspection validate` command enables IP validation only, the `src-mac` and `dst-mac` validations are disabled as a result of the second command.

To enable additional validation, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip arp inspection validate {[dst-mac] [ip] [src-mac]}
4. do show ip arp inspection | include abled$
5. exit
## Dynamic ARP Inspection

### Enabling Additional Validation

<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><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch&gt; enable</code></td>
<td>· Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`ip arp inspection validate {dst-mac</td>
<td>ip</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# ip arp inspection validate dst-mac</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip arp inspection validate ip</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip arp inspection validate src-mac</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`do show ip arp inspection</td>
<td>include abled$`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>`Switch(config)# do show ip arp inspection</td>
<td>include abled$`</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>exit</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

### Examples

This example shows how to enable src-mac additional validation:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection validate src-mac
Switch(config)# do show ip arp inspection | include abled$
```

<table>
<thead>
<tr>
<th>Source Mac Validation</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Mac Validation</td>
<td>Disabled</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

This example shows how to enable dst-mac additional validation:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection validate dst-mac
Switch(config)# do show ip arp inspection | include abled$
```

<table>
<thead>
<tr>
<th>Source Mac Validation</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Mac Validation</td>
<td>Enabled</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
This example shows how to enable ip additional validation:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection validate ip
Switch(config)# do show ip arp inspection | include abled$

<table>
<thead>
<tr>
<th>Source Mac Validation</th>
<th>: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Mac Validation</td>
<td>: Disabled</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>: Enabled</td>
</tr>
</tbody>
</table>

This example shows how to enable src-mac and dst-mac additional validation:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection validate src-mac dst-mac
Switch(config)# do show ip arp inspection | include abled$

<table>
<thead>
<tr>
<th>Source Mac Validation</th>
<th>: Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Mac Validation</td>
<td>: Enabled</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>: Disabled</td>
</tr>
</tbody>
</table>

This example shows how to enable src-mac, dst-mac, and ip additional validation:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection validate src-mac dst-mac ip
Switch(config)# do show ip arp inspection | include abled$

<table>
<thead>
<tr>
<th>Source Mac Validation</th>
<th>: Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Mac Validation</td>
<td>: Enabled</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>: Enabled</td>
</tr>
</tbody>
</table>

## Configuring DAI Logging

### DAI Logging Overview

When DAI drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, DAI clears the entry from the log buffer. Each log entry contains flow information, such as the receiving bridge domain, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

A log-buffer entry can represent more than one packet. For example, if an interface receives many packets on the same bridge domain with the same ARP parameters, DAI combines the packets as one entry in the log buffer and generates a single system message for the entry.

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the `show ip arp inspection log` privileged EXEC command is affected. Two dashes ("--") appear instead of data except for the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer or increase the logging rate.

### Configuring the DAI Logging For All Packets

To configure the DAI logging for all packets, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. ip arp inspection bridge-domain range logging \{acl-match | dhcp-bindings\} \{all | none | permit\}
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ip arp inspection bridge-domain range logging</td>
<td>Configures the DAI logging for all packets (DHCP permit and deny).</td>
</tr>
<tr>
<td>{acl-match</td>
<td>dhcp-bindings} {all</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip arp inspection bridge-domain 200</td>
<td></td>
</tr>
<tr>
<td>logging dhcp-bindings all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Example

This example shows how to configure the DAI logging for all packets:

```bash
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection bridge-domain 200 logging dhcp-bindings all
```

Configuring the DAI Logging Buffer Size

To configure the DAI logging buffer size, complete the following steps:
Summary Steps

1. enable
2. configure terminal
3. ip arp inspection log-buffer entries number
4. do show ip arp inspection log | include Size
5. exit

Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip arp inspection log-buffer entries number</td>
<td>Configures the DAI logging buffer size (range is 0 to 1024).</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ip arp inspection log-buffer entries 100</td>
</tr>
<tr>
<td>Step 4 do show ip arp inspection log</td>
<td>include Size</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# do show ip arp inspection log</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# exit</td>
</tr>
</tbody>
</table>

Example

This example shows how to configure the DAI logging buffer for 64 messages:

Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)# do show ip arp inspection log | include Size

Total Log Buffer Size : 64
Configuring the DAI Logging System Messages

When configuring the DAI logging system messages, note the following information:

- For **logs number_of_messages** (default is 5), the range is 0 to 1024. A 0 value means that the entry is placed in the log buffer, but a system message is not generated.
- For **interval length_in_seconds** (default is 1), the range is 0 to 86400 seconds (1 day). A 0 value means that a system message is immediately generated (and the log buffer is always empty). An interval setting of 0 overrides a log setting of 0.
- System messages are sent at the rate of **number_of_messages per length_in_seconds**.

To configure the DAI logging system messages, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. **ip arp inspection log-buffer logs number_of_messages interval length_in_seconds**
4. do show ip arp inspection log
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ip arp inspection log-buffer logs number_of_messages interval length_in_seconds</strong></td>
<td>Configures the DAI logging buffer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ip arp inspection log-buffer logs 100 interval 860</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>do show ip arp inspection log</strong></td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# do show ip arp inspection log</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>exit</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Example

This example shows how to configure DAI logging to send 12 messages every 2 seconds:

Switch# configure terminal
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
Switch(config)# do show ip arp inspection log | include Syslog

Syslog rate : 12 entries per 2 seconds.

This example shows how to configure DAI logging to send 20 messages every 60 seconds

Switch# configure terminal
Switch(config)# ip arp inspection log-buffer logs 20 interval 60
Switch(config)# do show ip arp inspection log | include Syslog

Syslog rate : 20 entries per 60 seconds.

Example: DAI Configuration

This procedure shows how to configure DAI when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B as shown in Figure 1-2 on page 1-3. Both switches are running DAI on bridge domain 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2. Switch A Gigabit Ethernet port 0/3 is connected to the Switch B Gigabit Ethernet port 0/3.

Note

- DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. For configuration information, see DHCP Snooping, on page 287.

- This configuration does not work if the DHCP server is moved from Switch A to a different location.

- To ensure that this configuration does not compromise security, configure Gigabit Ethernet port 0/3 on Switch A and Gigabit Ethernet port 0/3 on Switch B as trusted.

Configuring Switch A

To enable DAI and configure Gigabit Ethernet port 0/3 on Switch A as trusted, complete the following steps:
SUMMARY STEPS

1. enable
2. show cdp neighbors
3. configure terminal
4. configure terminal
5. exit
6. show ip dhcp snooping binding
7. show ip arp inspection statistics bridge-domain 1

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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show cdp neighbors</td>
<td>Verifies the connection between Switch A and Switch B.</td>
</tr>
<tr>
<td><strong>Example:</strong> SwitchA# show cdp neighbors</td>
<td></td>
</tr>
<tr>
<td>Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone</td>
<td></td>
</tr>
<tr>
<td>Device ID Port ID Local Intrfce Holdtme Capability Platform</td>
<td></td>
</tr>
<tr>
<td>SwitchB Gi 0/3 177 R S I WS-C6506</td>
<td></td>
</tr>
<tr>
<td>SwitchA#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>Enables DAI on bridge domain 1 and verifies the configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> SwitchA (config) # configure terminal</td>
<td></td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
<td></td>
</tr>
<tr>
<td>SwitchA(config)# ip arp inspection bridge-domain 1</td>
<td></td>
</tr>
<tr>
<td>SwitchA(config)# do sh ip arp ins bridge-domain 1</td>
<td></td>
</tr>
<tr>
<td>Source Mac Validation : Enabled</td>
<td></td>
</tr>
<tr>
<td>Destination Mac Validation : Disabled</td>
<td></td>
</tr>
<tr>
<td>IP Address Validation : Disabled</td>
<td></td>
</tr>
<tr>
<td>BD Configuration Operation ACL Match Static</td>
<td></td>
</tr>
<tr>
<td>ACL</td>
<td></td>
</tr>
</tbody>
</table>
### Dynamic ARP Inspection

#### Configuring Switch A

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>---</strong></td>
<td><strong>---</strong></td>
</tr>
<tr>
<td>1 Enabled</td>
<td>Active</td>
</tr>
<tr>
<td>BD</td>
<td>ACL Logging</td>
</tr>
<tr>
<td>1 Deny</td>
<td>Deny</td>
</tr>
</tbody>
</table>

#### Step 4

**configure terminal**

Example:

```
SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA#(config)# int gi 0/3
SwitchA#(config-if)# ip arp ins
SwitchA#(config-if)# ip arp inspection tr
SwitchA#(config-if)# ip arp inspection trust
SwitchA#(config-if)# end
SwitchA# sh ip arp inspection interfaces gigabitEthernet 0/3
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate (pps)</th>
<th>Burst Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/3</td>
<td>Trusted</td>
<td>None</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Step 5

**exit**

Example:

```
Switch(config)# exit
```

#### Step 6

**show ip dhcp snooping binding**

Example:

```
SwitchA# show ip dhcp snooping binding
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IpAddress</th>
<th>Lease(sec)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:00:02:00:02</td>
<td>1.1.1.2</td>
<td>4993</td>
<td>dhcp-snooping</td>
</tr>
</tbody>
</table>

#### Step 7

**show ip arp inspection statistics bridge-domain 1**

Example:

```
SwitchA# show ip arp inspection statistics bridge-domain 1
```

<table>
<thead>
<tr>
<th>BD</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD DHCP Permits</td>
<td>ACL Permits</td>
<td>Source MAC Failures</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>BD Dest MAC Failures</td>
<td>IP Validation Failures</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SwitchA#

If Host 1 then sends out two ARP requests with an IP address of 1.1.1.2 and a MAC address of 0002.0002.0002, both requests are permitted, as reflected in the following statistics:

SwitchA# show ip arp inspection statistics bridge-domain 1

<table>
<thead>
<tr>
<th>BD</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SwitchA#

If Host 1 then tries to send an ARP request with an IP address of 1.1.1.3, the packet is dropped and an error message is logged:

00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa6/4, bridge-domain 1.([0002.0002.0002/1.1.1.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Tue Jul 10 2001])

SwitchA# show ip arp inspection statistics bridge domain 1

SwitchA#

The statistics will display as follows:

<table>
<thead>
<tr>
<th>BD</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

SwitchA#
Configuring Switch B

To enable DAI and configure Fast Ethernet port 3/3 on Switch B as trusted, complete the following steps:

**SUMMARY STEPS**

1. **enable**
2. **show cdp neighbors**
3. **configure terminal**
4. **configure terminal**
5. **exit**
6. **show ip dhcp snooping binding**
7. **show ip arp inspection statistics bridge-domain 1**

**DETAILED STEPS**

<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><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show cdp neighbors</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>SwitchA# show cdp neighbors</td>
</tr>
<tr>
<td></td>
<td>Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone</td>
</tr>
<tr>
<td></td>
<td>Device ID</td>
</tr>
<tr>
<td></td>
<td>Port ID</td>
</tr>
<tr>
<td></td>
<td>SwitchB#</td>
</tr>
<tr>
<td></td>
<td>Verifies the connectivity.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>SwitchB# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>Enables DAI on bridge domain 1, and verifies the configuration.</td>
</tr>
</tbody>
</table>
### Configuring Switch B

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SwitchB(config)# ip arp inspection bridge-domain 1</td>
<td></td>
</tr>
<tr>
<td>SwitchB(config)# end</td>
<td></td>
</tr>
<tr>
<td>SwitchB# show ip arp inspection bridge-domain 1</td>
<td></td>
</tr>
<tr>
<td>Source Mac Validation : Disabled</td>
<td></td>
</tr>
<tr>
<td>Destination Mac Validation : Disabled</td>
<td></td>
</tr>
<tr>
<td>IP Address Validation : Disabled</td>
<td></td>
</tr>
<tr>
<td>BD Configuration Operation ACL Match Static</td>
<td></td>
</tr>
<tr>
<td>ACL</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------</td>
</tr>
<tr>
<td>1  Enabled</td>
<td>Active</td>
</tr>
<tr>
<td>BD ACL Logging DHCP Logging</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------</td>
</tr>
<tr>
<td>1 Deny</td>
<td>Deny</td>
</tr>
<tr>
<td>SwitchB#</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 4 configure terminal

**Example:**

SwitchB# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SwitchB(config)# interface GigabitEthernet 0/3

SwitchB(config-if)# ip arp inspection trust

SwitchB(config-if)# end

SwitchB# show ip arp inspection interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/2</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/3</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/4</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/5</td>
<td>Trusted</td>
<td>None</td>
</tr>
<tr>
<td>Gi0/6</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/7</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/8</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi0/9</td>
<td>Untrusted</td>
<td>15</td>
</tr>
</tbody>
</table>

<output truncated>

SwitchB#

#### Step 5 exit

**Example:**

Switch(config)# exit

Returns to privileged EXEC mode.

#### Step 6 show ip dhcp snooping binding

**Example:**

SwitchB# show ip dhcp snooping binding

Verifies the list of DHCP snooping bindings.
### Dynamic ARP Inspection

#### Configuring Switch B

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacAddress</td>
<td>IpAddress</td>
</tr>
<tr>
<td>BD Interface</td>
<td>-------------------</td>
</tr>
<tr>
<td>00:01:00:01:00:01</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>1 GigabitEthernet 0/4</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**  
`show ip arp inspection statistics bridge-domain 1`

**Example:**

```
SwitchB# show ip arp inspection statistics bridge-domain 1
```

<table>
<thead>
<tr>
<th>BD</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Source MAC Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>Dest MAC Failures</th>
<th>IP Validation Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SwitchB#

If Host 2 then sends out an ARP request with the IP address 1.1.1.1 and the MAC address 0001.0001.0001, the packet is forwarded and the statistics are updated appropriately:

```
SwitchB# show ip arp inspection statistics bridge-domain 1
```

<table>
<thead>
<tr>
<th>BD</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Source MAC Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>Dest MAC Failures</th>
<th>IP Validation Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SwitchB#

If Host 2 attempts to send an ARP request with the IP address 1.1.1.2, DAI drops the request and logs a system message:

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/4, bridge-domain 1.([0001.0001.0001/1.1.1.2/0000.0000.0000/0.0.0.0/01:53:21 UTC
```

Checks the statistics before and after DAI processes any packets.
Fri May 23 2003]
SwitchB#

The statistics display as follows:
SwitchB# show ip arp inspection statistics bridge domain 1

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Source MAC Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BD</th>
<th>Dest MAC Failures</th>
<th>IP Validation Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SwitchB#
MAC Address Security

This chapter describes MAC Address Security and procedures to configure MAC Address Security.

- MAC Address Security for EVC Bridge Domain, page 339
- Restrictions for MAC Address Security, page 340
- Enabling MAC Address Security for EVC Bridge Domain, page 340
- Disabling MAC Address Security for EVC Bridge Domain on an EFP, page 342
- Configuring MAC Address Whitelist on an EFP, page 343
- Configuring Sticky MAC Addresses on an EFP, page 345
- Configuring MAC Address Limiting on EFP, page 347
- Configuring MAC Address Limiting on a Bridge Domain, page 349
- Configuring Violation Response on an EFP, page 350
- Checking EVC State, page 352
- Error Recovery, page 352
- Verification, page 353
- Troubleshooting, page 356

MAC Address Security for EVC Bridge Domain

The Media Access Control (MAC) Address Security for EVC Bridge Domain feature addresses port security with EVCs by providing the capability to control and filter MAC address learning behavior at the granularity of a per-EFP basis. For instance, when a violation requires a shutdown, only the customer assigned to a given EFP is affected rather than all customers using the port.

Cisco IOS Release 12.2(33)SRE adds support for MAC address security on EVC port-channels. This feature operates on a port-channel interface in a similar manner to how it works on a physical port. In each case, MAC security is configured on a service instance associated with a bridge domain.

Mac Address Security does not work with a mix of secure and nonsecure EFPs in same bridge domain. For more information, see CSCuc55613.
Using MAC Address Security feature 10% of the traffic is dropped after clear MAC, until traffic is learnt on both EFPs. For more information, see CSCuc50540.

Aging time configuration is not supported. Even the show command for aging time does not retrieve any output due to hardware limitation. Aging time varies between 5mins-10mins. For more information, see CSCuc31405 and CSCua99729.

Restrictions for MAC Address Security

- System wide, the following limits apply to the total configured whitelist and learned MAC addresses:
  - Total number of MAC addresses supported under MAC Security is limited to 32K.
  - Total number of secure EFPs in the system is limited to 256.
  - Total number of MAC addresses supported under MAC Security, per EFP, is limited to 48.

- You can configure or remove the various MAC security elements irrespective of whether MAC security is enabled on the EFP. However, these configurations become operational only after MAC security is enabled.

- It is recommended that you enable MAC address security feature on all the EFPs in a bridge-domain.

- When you enable the MAC address security for EVC bridge domain feature, existing MAC address table entries on the EFP are removed.

- When you enable the MAC address security, the traffic is forwarded once the switch learns the MAC address.

- The MAC address security for EVC bridge domain feature can be configured on an EFP only if the EFP is a member of a bridge domain.

- If you disassociate the EFP from the BD, the MAC security feature is completely removed.

- For port-channel, this configuration is propagated to all member links in the port-channel. Consistent with the already implemented bridge domain EVC port-channel functionality, packets on a secured EFP are received on any member link, but all the egress packets are sent out to one of the selected member links.

- System does not permit addition of multicast/broadcast MAC address as a permit address. However, addition of multicast/broadcast MAC address is allowed in deny address configuration to verify such invalid packets.

- When EVC with the same EFP or service instance is created between ports 1 and 2 and MAC address m1 is configured as permit address (whitelist) on port1, the same MAC address can be configured as deny address (blacklist) on port2 and vice versa.

Enabling MAC Address Security for EVC Bridge Domain

This section describes how to enable MAC address security for EVC bridge domain.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security or no mac security

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface gigabitethernet slot/subslot/port or</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit</td>
</tr>
<tr>
<td>interface tengigabitethernet slot/subslot/port or</td>
<td>Ethernet or the port-channel interface to</td>
</tr>
<tr>
<td>interface port-channel number</td>
<td>configure.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 0/5</td>
<td></td>
</tr>
<tr>
<td>Step 4 service instance id Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC)</td>
</tr>
<tr>
<td>Example: Switch(config-if)# service instance 101 ethernet</td>
<td>on an interface and sets the device into the</td>
</tr>
<tr>
<td></td>
<td>config-if-srv submode.</td>
</tr>
<tr>
<td>Step 5 encapsulation dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# encapsulation dot1q 13</td>
<td>to map ingress dot1q frames on an interface to</td>
</tr>
<tr>
<td></td>
<td>the appropriate service instance.</td>
</tr>
<tr>
<td>Step 6 bridge-domain bridge-id</td>
<td>Binds the service instance to a bridge domain</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# bridge-domain 12</td>
<td>instance where bridge-id is the identifier for</td>
</tr>
<tr>
<td></td>
<td>the bridge domain instance.</td>
</tr>
<tr>
<td>Step 7 mac security or no mac security</td>
<td>Enables or disables the MAC Security on the EFP.</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# mac security or</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-srv)# no mac security</td>
<td></td>
</tr>
</tbody>
</table>
Examples

This example shows how to enable MAC address security for EVC bridge domain.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-srv)# encapsulation dot1q 20
Switch(config-srv)# bridge-domain 100
Switch(config-srv)# mac security
```

This example shows how to disable MAC address security for EVC bridge domain.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# no mac security
```

Disabling MAC Address Security for EVC Bridge Domain on an EFP

This section describes how to disable MAC address security for EVC bridge domain.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet` `slot/subslot/port` or `interface tengigabitethernet` `slot/subslot/port` or `interface port-channel` `number`
4. `service instance id Ethernet` `[service-name]`
5. `no mac security`
6. `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><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
**Command or Action** | **Purpose**
--- | ---
**Step 3** | **interface gigabitethernet** slot/subslot/port or **interface tengigabitethernet** slot/subslot/port or **interface port-channel** number
*Example:* Switch(config)# interface GigabitEthernet 0/5
| Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.

**Step 4** | **service instance** *id* **Ethernet** [service-name]
*Example:* Switch(config-if)# service instance 101 ethernet
| Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.

**Step 5** | **no mac security**
*Example:* Switch(config-if-srv)# no mac security
| Disables MAC Security on the EFP.

**Step 6** | **end**
*Example:* Switch(config-if-srv)# end
| Returns to privileged EXEC mode.

**Example**

This example shows how to disable MAC address security for EVC bridge domain.

Switch# enable  
Switch# configure terminal 
Switch(config)# interface GigabitEthernet 0/5 
Switch(config-if)# service instance 10 ethernet 
Switch(config-if-srv)# no mac security

**Configuring MAC Address Whitelist on an EFP**

A permit list is a set of MAC addresses that are permitted on a service instance. Permitted addresses are permanently configured into the MAC address table of the service instance as static entries.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security
8. mac security address permit H.H.H
9. no mac security
10. no mac security address permit H.H.H
11. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  **Example:**  
  Switch# enable  
  • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
  **Example:**  
  Switch# configure terminal |
| **Step 3** interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number | Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.  
  **Example:**  
  Switch(config)# interface GigabitEthernet 0/5 |
| **Step 4** service instance id Ethernet [service-name] | Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.  
  **Example:**  
  Switch(config-if)# service instance 101 ethernet |
| **Step 5** encapsulation dot1q vlan-id | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.  
  **Example:**  
  Switch(config-if-srv)# encapsulation dot1q 13 |
| **Step 6** bridge-domain bridge-id | Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.  
  **Example:**  
  Switch(config-if-srv)# bridge-domain 12 |
### Configuring Sticky MAC Addresses on an EFP

MAC addresses learned dynamically on the EFP after `mac security sticky` is configured are retained during a link-down condition and device reload. Sticky Mac is shown in the MAC table as static addresses. However, you should copy the running configuration details to retain the mac address details.

When sticky addresses are added or removed from the service instance, existing dynamically learned MAC addresses remain unchanged. All new addresses learned become "sticky" addresses. Disabling sticky addresses causes all sticky secure MAC addresses on the service instance to be removed from the MAC address table and from the running-configuration.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>mac security</strong> Enables MAC Security on the EFP</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-if-srv)# mac security</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>mac security address permit H.H.H</strong> Adds the specified MAC Address as a whitelist (&quot;permit&quot;) MAC Address for the EFP</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-if-srv)# mac security address permit H.H.H</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>no mac security</strong> Disables MAC Security on the EFP</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-if-srv)# no mac security</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>no mac security address permit H.H.H</strong> Removes the specified MAC Address as a whitelist (&quot;permit&quot;) MAC Address for the EFP</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-if-srv)# no mac security address permit H.H.H</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>end</strong> Returns to privileged EXEC mode</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-if-srv)# end</code></td>
</tr>
</tbody>
</table>

---

**Example**

This example shows how to configure whitelisted MAC addresses on an EFP that is a member of a bridge domain.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if)# encapsulation dot1q 20
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# mac security address permit 0000.1111.2222
Switch(config-if-srv)# mac security
```
This section describes how to configure sticky MAC addresses on an EFP.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security sticky
8. mac security
9. no mac security
10. no mac security sticky

**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.</td>
</tr>
<tr>
<td>Example: Switch# enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number</td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 0/5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id Ethernet [service-name]</td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# service instance 101 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> encapsulation dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# encapsulation dot1q 13</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>bridge-domain</strong> bridge-id</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if-srv)# bridge-domain 12</td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>mac security sticky</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if-srv)# mac security sticky</td>
<td>Enables Sticky feature causing all dynamic secure MAC addresses to become sticky MAC addresses. Any new MAC address learnt becomes sticky.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To retain the sticky MAC addresses across reloads, ensure that you save the running configuration to the start up configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>mac security</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if-srv)# mac security</td>
<td>Enables MAC Security on the EFP.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>no mac security</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if-srv)# no mac security</td>
<td>Disables the MAC Security on the EFP.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>no mac security sticky</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if-srv)# no mac security sticky</td>
<td>Disables the MAC Security Sticky on the EFP.</td>
</tr>
</tbody>
</table>

**Example**

This example configures sticky MAC addresses on an EFP.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 20
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# mac security sticky
Switch(config-if-srv)# mac security
```

**Configuring MAC Address Limiting on EFP**

This section describes how to configure an upper limit for the number of secured MAC addresses allowed on an EFP. This includes addresses added as part of a whitelist, as well as dynamically learned MAC addresses. If the upper limit is decreased, one or more learned MAC entries may be removed. The default limit is 1. However, it can be set to a maximum of 48 addresses per EFP.
When both mac address limiting on a bridge domain and maximum mac address per EFP are configured, the lower value of the two takes higher priority.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface gigabitethernet slot/subslot/port` or `interface tengigabitethernet slot/subslot/port` or `interface port-channel number`
4. `service instance id Ethernet [service-name]`
5. `encapsulation dot1q vlan-id`
6. `bridge-domain bridge-id`
7. `mac security maximum addresses 'n'`
8. `mac security`
9. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code>&lt;br&gt;Example:&lt;br&gt;<code>Switch&gt; enable</code>&lt;br&gt;Enables privileged EXEC mode.&lt;br&gt;* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code>&lt;br&gt;Example:&lt;br&gt;<code>Switch# configure terminal</code>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface gigabitethernet slot/subslot/port</code> or <code>interface tengigabitethernet slot/subslot/port</code> or <code>interface port-channel number</code>&lt;br&gt;Example:&lt;br&gt;<code>Switch(config)# interface GigabitEthernet 0/5</code>&lt;br&gt;Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>service instance id Ethernet [service-name]</code>&lt;br&gt;Example:&lt;br&gt;<code>Switch(config-if)# service instance 101 ethernet</code>&lt;br&gt;Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>encapsulation dot1q vlan-id</code>&lt;br&gt;Example:&lt;br&gt;<code>Switch(config-if-srv)# encapsulation dot1q 13</code>&lt;br&gt;Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
</tbody>
</table>
### Purpose

- **Command or Action**
- **Purpose**

#### Step 6

**bridge-domain** bridge-id

*Example:
Switch(config-if-srv)# bridge-domain 12

Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.

#### Step 7

**mac security maximum addresses ’n’**

*Example:
Switch(config-if-srv)# mac security maximum addresses 10

Sets (or changes) the maximum number of secure addresses permitted on the EFP to the integer value n. The acceptable range for secure addresses ’n’ is 1–48.

#### Step 8

**mac security**

*Example:
Switch(config-if-srv)# mac security

Enables MAC Security on the EFP.

#### Step 9

**end**

*Example:
Switch(config-if-srv)# end

Returns to privileged EXEC mode.

### Example

This example configures an upper limit of 10 for the number of secured MAC addresses allowed on an EFP.

```
Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 20
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# mac security maximum addresses 10
Switch(config-if-srv)# mac security
```

### Configuring MAC Address Limiting on a Bridge Domain

This section describes how to configure an upper limit for the number of secured MAC addresses located on the bridge domain.

### SUMMARY STEPS

1. enable
2. configure terminal
3. bridge-domain vlan-id [access | dot1q [tag] | dot1q-tunnel] [broadcast] [ignore-bpdu-pid] [pvst-tlv CE-vlan] [increment] [lan-fcs] [split-horizon]
4. mac limit maximum addresses [n]
5. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** Switch# enable |  |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Switch# configure terminal |  |
| **Step 3** bridge-domain vlan-id [access | Sets the limit for maximum addresses. The default value is 10240. |
  | dot1q [tag] | [n] |
  | dot1q-tunnel] [broadcast] [ignore-bpdu-pid] [pvst-tlv CE-vlan] [increment] [lan-fcs] [split-horizon] |  |
  | **Example:** Switch(config)# bridge-domain 12 |  |
| **Step 4** mac limit maximum addresses [n] |  |
| **Example:** Switch(config-bdomain)# mac limit maximum addresses 1000 |  |
| **Step 5** end | Returns to privileged EXEC mode. |
| **Example:** Switch(config-bdomain)# end |  |

**Example**

This example configures an upper limit of 1000 for the number of secured MAC addresses.

```
Switch# enable
Switch# configure terminal
Switch(config)# bridge-domain 100
Switch(config-if-srv)# mac limit maximum address 1000
```

## Configuring Violation Response on an EFP

This section describes how to specify the expected behavior of the device when an attempt to dynamically learn a MAC address fails because of a violation of the configured MAC Security policy on the EFP. The default violation behavior is termed as an EFP shutdown.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number
4. service instance id Ethernet [service-name]
5. encapsulation dot1q vlan-id
6. bridge-domain bridge-id
7. mac security violation restrict or mac security violation protect
8. mac security
9. end

DETAILED STEPS

<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>Example:</td>
<td>Switch# enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface gigabitethernet slot/subslot/port or interface tengigabitethernet slot/subslot/port or interface port-channel number</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface GigabitEthernet 0/5</td>
</tr>
<tr>
<td></td>
<td>Specifies the Gigabit Ethernet or the Ten Gigabit Ethernet or the port-channel interface to configure.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>service instance id Ethernet [service-name]</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# service instance 101 ethernet</td>
</tr>
<tr>
<td></td>
<td>Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv submode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>encapsulation dot1q vlan-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-srv)# encapsulation dot1q 13</td>
</tr>
<tr>
<td></td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>bridge-domain bridge-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-srv)# bridge-domain 12</td>
</tr>
<tr>
<td></td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.</td>
</tr>
</tbody>
</table>
### Checking EVC State

The following commands can be used to check whether the EVC is in Errdisabled (shutdown) state or UP:

- `show ethernet service instance id <> int <>`
- `show ethernet service instance int <>`
- `show ethernet service instance detail`

### Error Recovery

This section describes how to recover from violation causing an EFP shutdown (default violation response) and contains the following sections:

- Manual Recovery
- Automatic Recovery
Manual Recovery

For manual recovery, use the `clear ethernet service instance id id interface interface-name errdisable` command to bring the service instance out of an error disabled state as shown below:

Switch# enable
Switch# configure terminal
Switch# clear ethernet service instance id 10 interface GigabitEthernet 0/5

Automatic recovery

For automatic recovery, use the `errdisable recovery cause mac security` command. You must specify the timer interval. The valid value is from 30 to 86400 second. In the configuration example that follows, the EFP recovers 60 seconds after the violation causes the shutdown.

Switch# enable
Switch# configure terminal
Switch(config)# interface GigabitEthernet 0/5
Switch(config-if)# service instance 10 ethernet
Switch(config-if-srv)# encapsulation dot1q 10
Switch(config-if-srv)# bridge-domain 100
Switch(config-if-srv)# mac security
Switch(config-if-srv)# errdisable recovery cause mac-security 60

Verification

Use the following commands to verify operation.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet service instance id &lt;id&gt; interface &lt;interface-id&gt; mac security address</code></td>
<td>Displays the secure addresses on the specified EFP.</td>
</tr>
<tr>
<td><code>show ethernet service instance id &lt;id&gt; interface &lt;interface-id&gt; mac security last violation</code></td>
<td>Displays the last violation recorded on the specified EFP.</td>
</tr>
<tr>
<td><code>show ethernet service instance id &lt;id&gt; interface &lt;interface-id&gt; mac security statistics</code></td>
<td>Displays the number of allowed and actual secured address and the number of violations recorded on the EFP.</td>
</tr>
<tr>
<td><code>show ethernet service instance id &lt;id&gt; interface &lt;interface-id&gt; mac security</code></td>
<td>Displays the MAC Security status of the specified EFP.</td>
</tr>
<tr>
<td><code>show ethernet service instance mac security address</code></td>
<td>Displays the secure addresses on all the EFPs in the system.</td>
</tr>
<tr>
<td><code>show ethernet service instance mac security last violation</code></td>
<td>Displays information about the last violation recorded on the device (across all service instances) and information about the last violation recorded on each of the service instances.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>show ethernet service instance mac security statistics</td>
<td>Displays the number of allowed and actual secured addresses, as well as the number of violations recorded on all the EFPs in the system.</td>
</tr>
<tr>
<td>show ethernet service instance mac security</td>
<td>Displays all the EFPs in the system that have MAC Security enabled.</td>
</tr>
<tr>
<td>show bridge-domain id mac security address</td>
<td>Displays the secure addresses on all EFPs belonging to the specified bridge domain.</td>
</tr>
<tr>
<td>show bridge-domain id mac security last violation</td>
<td>Displays information about the last violation recorded on each of the service instances belonging to the bridge domain.</td>
</tr>
<tr>
<td>show bridge-domain id mac security statistics</td>
<td>Displays the number of allowed and actual secured addresses, as well as the number of violations recorded on all the EFPs that belong to the specified bridge domain.</td>
</tr>
<tr>
<td>show bridge-domain id mac security</td>
<td>Displays all the EFPs that belong to the specified bridge domain, and that have MAC Security enabled.</td>
</tr>
</tbody>
</table>

**Example: Displaying the MAC Addresses on a Specific Secure Service Instance**

Switch# `show ethernet service instance id 501 interface gigabitethernet 0/5 mac security address`

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001.0001.0001</td>
<td>static</td>
</tr>
<tr>
<td>0001.0001.0002</td>
<td>static</td>
</tr>
<tr>
<td>0001.0001.aaaa</td>
<td>dynamic</td>
</tr>
<tr>
<td>0001.0001.aaab</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

The table below describes the significant fields in the output:

**Table 29: MAC Addresses on a Specific Service Instance: Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the MAC addresses on the service instance.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of MAC address by declaring if it was statically configured (static) or dynamically learned (dynamic).</td>
</tr>
</tbody>
</table>

**Example: Displaying the Last Violation on a Specific Service Instance**

Switch# `show ethernet service instance mac security last violation`

```
Gi0/25 ServInst 25 (bridge-domain 25)
Last violation at: 00:01:51
Source MAC address: 0000.0000.0001
```
Example: Displaying the MAC Security Status of a Specific Service Instance

Switch# show ethernet service instance id 501 interface gigabitethernet 0/5 mac security

MAC Security: enabled

Example: Displaying the MAC Addresses of All Secured Service Instances

Switch# show ethernet service instance mac security address

<table>
<thead>
<tr>
<th>Port</th>
<th>Bridge-domain</th>
<th>MAC Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>g0/1</td>
<td>ServInst 1</td>
<td>0001.0001.0001</td>
<td>static</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 1</td>
<td>0001.0001.0002</td>
<td>static</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 1</td>
<td>0001.0001.aaaa</td>
<td>dynamic</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 1</td>
<td>0001.0001.aaab</td>
<td>dynamic</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 2</td>
<td>0002.0002.0002</td>
<td>static</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 2</td>
<td>0002.0002.0003</td>
<td>static</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 2</td>
<td>0002.0002.0004</td>
<td>static</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 2</td>
<td>0002.0002.aaaa</td>
<td>dynamic</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 2</td>
<td>0002.0002.bbbb</td>
<td>dynamic</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 2</td>
<td>0002.0002.cccc</td>
<td>dynamic</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 10</td>
<td>0003.0003.0001</td>
<td>static</td>
</tr>
<tr>
<td>g0/1</td>
<td>ServInst 10</td>
<td>0003.0003.0002</td>
<td>static</td>
</tr>
</tbody>
</table>

The table below describes the significant fields in the output:

**Table 30: MAC Addresses of All Service Instances: Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Displays the service instance ID number and its interface type and number.</td>
</tr>
<tr>
<td>Bridge-Domain</td>
<td>Displays the bridge-domain ID number for each service instance listed.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the MAC addresses on the service instance.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of MAC address by declaring if it was statically configured (static) or dynamically learned (dynamic).</td>
</tr>
</tbody>
</table>
Example: Displaying the MAC Security Statistics of All Service Instances

In the following example, the numbers of allowed and actual secured addresses recorded on the service instance are displayed.

Switch# show ethernet service instance mac security statistics

<table>
<thead>
<tr>
<th>Service Instance</th>
<th>Current Secure Addresses</th>
<th>Permitted Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/41 ServInst 1 (bridge-domain 1)</td>
<td>0</td>
<td>48</td>
</tr>
<tr>
<td>Gi0/41 ServInst 10 (bridge-domain 10)</td>
<td>0</td>
<td>48</td>
</tr>
<tr>
<td>Gi0/41 ServInst 100 (bridge-domain 100)</td>
<td>0</td>
<td>48</td>
</tr>
<tr>
<td>Gi0/41 ServInst 101 (bridge-domain 101)</td>
<td>0</td>
<td>48</td>
</tr>
</tbody>
</table>

Example: Displaying the MAC Addresses on All Service Instances for a Bridge Domain

Switch# show bridge-domain 730 mac security address

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/1 ServInst 1</td>
<td>0001.0001.0001</td>
<td>static</td>
</tr>
<tr>
<td>G0/1 ServInst 1</td>
<td>0001.0001.0002</td>
<td>static</td>
</tr>
<tr>
<td>G0/1 ServInst 1</td>
<td>0001.0001.aaaa</td>
<td>dynamic</td>
</tr>
<tr>
<td>G0/1 ServInst 1</td>
<td>0001.0001.aaab</td>
<td>dynamic</td>
</tr>
<tr>
<td>G0/1 ServInst 2</td>
<td>0002.0002.0002</td>
<td>static</td>
</tr>
<tr>
<td>G0/1 ServInst 2</td>
<td>0002.0002.0003</td>
<td>static</td>
</tr>
<tr>
<td>G0/1 ServInst 2</td>
<td>0002.0002.aaaaa</td>
<td>dynamic</td>
</tr>
<tr>
<td>G0/1 ServInst 2</td>
<td>0002.0002.bbbbb</td>
<td>dynamic</td>
</tr>
<tr>
<td>G0/1 ServInst 2</td>
<td>0002.0002.ccccc</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

Example: Displaying the Secured Service Instances for a Specific Bridge Domain

Switch# show bridge-domain 730 mac security

G0/1 ServInst 1
MAC Security enabled: yes
G0/2 ServInst 2
MAC Security enabled: yes

Troubleshooting

Troubleshooting Scenarios for MAC Security feature

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFP is disabled and is unable to automatically recover from error disable state</td>
<td>Use the errdisable recovery cause mac-security interval or clear ethernet service instance id id interface interface-name errdisable commands to re-enable the EFP.</td>
</tr>
</tbody>
</table>
### Problem
MAC security errors or events

### Solution
Use the `debug ethernet service instance mac security errors|events` and `debug ethernet service instance mac table errors|events` commands to troubleshoot mac security issues. For example:

```
Switch# debug ethernet service instance id 45 interface tengigabitethernet 0/45 mac security ?
```

errors MAC Security errors

events MAC Security events

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| MAC security errors or events | Use the `debug ethernet service instance mac security errors|events` and `debug ethernet service instance mac table errors|events` commands to troubleshoot mac security issues. For example:  
`Switch# debug ethernet service instance id 45 interface tengigabitethernet 0/45 mac security ?`  
errors MAC Security errors  
events MAC Security events |
Layer 2 Access Control Lists on EVCs

This chapter describes how to implement ACLs on EVCs.

- Layer 2 Access Control Lists on EVCs, page 359
- Finding Feature Information, page 359
- Prerequisites for Layer 2 Access Control Lists on EVCs, page 360
- Limitations and Restrictions for Layer 2 Access Control Lists on EVCs, page 360
- Information About Layer 2 Access Control Lists on EVCs, page 360
- Configuring Layer 2 Access Control Lists on EVCs, page 361
- Configuration Examples for Layer 2 Access Control Lists on EVCs, page 368
- Additional References, page 370
- Feature Information for Layer 2 Access Control Lists on EVCs, page 371

Layer 2 Access Control Lists on EVCs

The ability to filter packets in a modular and scalable way is important for both network security and network management. Access Control Lists (ACLs) provide the capability to filter packets at a fine granularity. In Metro Ethernet networks, ACLs are directly applied on Ethernet virtual circuits (EVCs).

Layer 2 Access Control Lists on EVCs is a security feature that allows packet filtering based on MAC addresses. This module describes how to implement ACLs on EVCs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 Feature Information for Layer 2 Access Control Lists on EVCs, on page 371.

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/. An account on Cisco.com is not required.
Prerequisites for Layer 2 Access Control Lists on EVCs

• Knowledge of how service instances must be configured.
• Knowledge of extended MAC ACLs and how they must be configured.

Limitations and Restrictions for Layer 2 Access Control Lists on EVCs

• Supported access control entries (ACEs) are:
  ◦ Up to 128 ACE, one ACE per MAC ACL
  ◦ Up to 255 ACE, on a single MAC ACL

Note
MAC ACL can be configured for up to \((N+1)\times M=256\), where \(N\) is the number of ACE and \(M\) is the number of MAC ACLs.

• Layer 2 ACLs function inbound only.
• For ACL with port channel and untagged EFP, you must include the permit action for lag control packets.
• Default encapsulation traffic must match with the tag protocol identifier (TPID) 0x8100, otherwise the traffic drops.
• To remove a filter you created in MAC ACL, do one of the following:
  ◦ Apply a no <filter> and then exit. Go back to the filter and then deny the filter.
  ◦ Wait for more than 10 minutes after applying the filter and then deny the filter.

Note
Filtering is applied to both, control packets and data packets.
ACEs is applied to control packets along with data packets.
If there are no ACEs, default is to deny all packets.

Information About Layer 2 Access Control Lists on EVCs

EVC

An EVC as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. It is an end-to-end representation of a single instance of a Layer 2 service being offered by a
Layer 2 Access Control Lists on EVCs

Relationship Between ACLs and Ethernet Infrastructure

The following points capture the relationship between ACLs and Ethernet Infrastructure (EI):

- ACLs can be directly applied on an EVC using the command-line interface (CLI). An ACL is applied to a service instance, which is the instantiation of an EVC on a given port.
- One ACL can be applied to more than one service instance at any time.
- One service instance can have one ACL at most applied to it at any time. If a Layer 2 ACL is applied to a service instance that already has a Layer 2 ACL, the new one replaces the old one.
- Only named ACLs can be applied to service instances. The command syntax ACLs is retained; the `mac access-list extended` command is used to create an ACL.
- The `show ethernet service instance` command can be used to provide details about ACLs on service instances.

Configuring Layer 2 Access Control Lists on EVCs

Creating a Layer 2 ACL

To create a Layer 2 ACL with a single ACE, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. mac access-list extended name
4. permit {{src-mac mask | any | host} {dest-mac mask | any | host} [protocol [cos value]]}
5. deny {{src-mac mask | any | host} {dest-mac mask | any | host} [protocol [cos value]]}
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Applying a Layer 2 ACL to a Service Instance

To apply a Layer 2 ACL to a service instance, complete the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mac access-list extended name</td>
<td>Defines an extended MAC ACL and enters mac access list control configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# mac access-list extended test-12-acl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> permit {{src-mac mask</td>
<td>any</td>
</tr>
<tr>
<td>Example: Switch(config-ext-macl)# permit host 00aa.00bb.00cc any</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> deny {{src-mac mask</td>
<td>any</td>
</tr>
<tr>
<td>Example: Switch(config-ext-macl)# deny host 00aa.00bb.01cc any</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-ext-macl)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Packet Filtering

Packet filtering takes place only after the ACL has been created and applied to the service instance.

### Before You Begin

Before applying an ACL to a service instance, you must create it using the `mac access-list extended` command. See Creating a Layer 2 ACL, on page 361.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. service instance id ethernet
5. encapsulation dot1q vlan-id
6. mac access-group access-list-name in
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode. |-)
| Example: Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Switch# configure terminal |
| **Step 3** interface type number | Specifies the type and location of the interface to configure, where: |
| Example: Switch(config)# interface GigabitEthernet 0/10 |
| • type — Specifies the type of the interface. |
| • number — Specifies the location of the interface. |
| **Step 4** service instance id ethernet | Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode. |
| Example: Switch(config-if)# service instance 100 ethernet |
| **Step 5** encapsulation dot1q vlan-id | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance. |
| Example: Switch(config-if-srv)# encapsulation dot1q 100 |
| **Step 6** mac access-group access-list-name in | Applies a MAC ACL to control incoming traffic on the interface. |
| Example: Switch(config-if-srv)# mac access-group test-12-acl in |
| **Step 7** end | Returns to privileged EXEC mode. |
| Example: Switch(config-if-srv)# end |
Removing a Layer 2 ACL

To remove a Layer 2 ACL, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `service instance id ethernet`
5. `no mac access-group test-l2-acl in`
6. `no mac access-list name`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td><code>interface type slot/port</code></td>
<td>Switch(config)# interface GigabitEthernet 0/10</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters the interface configuration mode with the service instance.</td>
</tr>
<tr>
<td><code>service instance id ethernet</code></td>
<td>Switch(config-if)# service instance 100 ethernet</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Removes the ACL from the service instance.</td>
</tr>
<tr>
<td><code>no mac access-group test-l2-acl in</code></td>
<td>Switch(config-if-srv)# no mac access-group test-l2-acl in</td>
</tr>
</tbody>
</table>
### Configuring a Layer 2 ACL with ACEs on a Service Instance

To configure the same ACL with three ACEs and stop all other traffic on a service instance, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `mac access-list extended name`
4. `permit {src-mac mask | any | host} {dest-mac mask | any | host}`
5. `permit {src-mac mask | any | host} {dest-mac mask | any | host}`
6. `permit {src-mac mask | any | host} {dest-mac mask | any | host}`
7. `exit`
8. `interface type number`
9. `service instance id ethernet`
10. `encapsulation dot1q vlan-id`
11. `mac access-group access-list-name in`
12. `end`

**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.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>no mac access-list name</code></td>
<td>Removes the Layer 2 ACL that you specify by name from the running configuration.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-if-srv)# no mac access-list acl-mac-01</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-if-srv)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>mac access-list extended name</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mac access list extended test-12-acl</td>
</tr>
<tr>
<td>4</td>
<td>permit {src-mac mask</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ext-macl)# permit host 00aa.bbcc.ddea any</td>
</tr>
<tr>
<td>5</td>
<td>permit {src-mac mask</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ext-macl)# permit host 00aa.bbcc.ddeb any</td>
</tr>
<tr>
<td>6</td>
<td>permit {src-mac mask</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ext-macl)# permit host 00aa.bbcc.ddec any</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ext-macl)# exit</td>
</tr>
<tr>
<td>8</td>
<td>interface type number</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface GigabitEthernet 0/10</td>
</tr>
<tr>
<td>9</td>
<td>service instance id ethernet</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# service instance 200 ethernet</td>
</tr>
<tr>
<td>10</td>
<td>encapsulation dot1q vlan-id</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if-srv)# encapsulation dot1q 100</td>
</tr>
</tbody>
</table>
### Layer 2 Access Control Lists on EVCs

#### Verifying the Presence of a Layer 2 ACL on a Service Instance

Perform this task to verify that a Layer 2 ACL is present on an EVC. This verification task can be used after an ACL has been configured to confirm its presence.

**SUMMARY STEPS**

1. **enable**
2. **show ethernet service instance id** *id* **interface** *type* *number* **detail**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>show ethernet service instance id</strong> <em>id</em> <strong>interface</strong> <em>type</em> <em>number</em> <strong>detail</strong></td>
<td>Displays detailed information about Ethernet customer service instances.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <strong>show ethernet service instance id</strong> 100 <strong>interface</strong> gigabitethernet 0/10 <strong>detail</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Layer 2 Access Control Lists on EVCs

Example: Creating a Layer 2 ACL with ACEs

The following example shows how to create a Layer 2 ACL called mac-11-acl with two permitted ACEs:

```
enable
configure terminal
mac access-list extended mac-11-acl
    permit host 00aa.00bb.00cc any
    permit host 00aa.00bb.01cc any
```

Example: Applying a Layer 2 ACL to a Service Instance

The following example shows how to apply a Layer 2 ACL called mac-20-acl to a service instance. The ACL has five permitted ACEs and all other traffic is not allowed.

```
enable
configure terminal
mac access-list extended mac-20-acl
    permit host 00aa.bbcc.adec any
    permit host 00aa.bbcc.bdec any
    permit host 00aa.bbcc.cdec any
    permit host 00aa.bbcc.edec any
    permit host 00aa.bbcc.fdec any
exit
interface gigabitethernet 0/10
    service instance 100 ethernet
    encapsulation dot1q 100
    mac access-group mac-20-acl in
```

Example: Applying a Layer 2 ACL to Three Service Instances on the Same Interface

The following example shows how to apply a Layer 2 ACL called mac-07-acl to three service instances on the same interface:

```
enable
configure terminal
mac access-list extended mac-07-acl
    permit host 00aa.bbcc.adec any
    permit host 00aa.bbcc.bdec any
    permit host 00aa.bbcc.cdec any
exit
interface gigabitethernet 0/10
    service instance 100 ethernet
    encapsulation dot1q 100
    mac access-group mac-07-acl in
```
```
interface gigabitethernet 0/10
    service instance 101 ethernet
    encapsulation dot1q 101
    mac access-group mac-07-acl in
```
```
interface gigabitethernet 0/10
    service instance 102 ethernet
    encapsulation dot1q 102
    mac access-group mac-07-acl in
```
Example: Displaying the Details of a Layer 2 ACL on a Service Instance

The following sample output displays the details of a Layer 2 ACL called test-acl on a service instance.

```
Switch# show ethernet service instance id 100 interface ethernet0/0 detail
```

<table>
<thead>
<tr>
<th>Service Instance ID: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 ACL (inbound): test-acl</td>
</tr>
<tr>
<td>Associated Interface: Ethernet0/0</td>
</tr>
<tr>
<td>Associated EVC: test</td>
</tr>
<tr>
<td>L2 protocol drop</td>
</tr>
<tr>
<td>CEVlans:</td>
</tr>
<tr>
<td>Interface Dot1q Tunnel Ethertype: 0x8100</td>
</tr>
<tr>
<td>State: Up</td>
</tr>
<tr>
<td>L2 ACL permit count: 10255</td>
</tr>
<tr>
<td>L2 ACL deny count: 53</td>
</tr>
</tbody>
</table>

The table below describes the significant fields in the output.

**Table 31: show ethernet service instance Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Instance ID</td>
<td>Displays the service instance ID.</td>
</tr>
<tr>
<td>L2 ACL (inbound):</td>
<td>Displays the ACL name.</td>
</tr>
<tr>
<td>Associated Interface:</td>
<td>Displays the interface details of the service instance.</td>
</tr>
<tr>
<td>Associated EVC:</td>
<td>Displays the EVC with which the service instance is associated</td>
</tr>
<tr>
<td>CEVlans:</td>
<td>Displays details of the associated VLAN ID.</td>
</tr>
<tr>
<td>State:</td>
<td>Displays whether the service instance is in an up or down state.</td>
</tr>
<tr>
<td>L2 ACL permit count:</td>
<td>Displays the number of packet frames allowed to pass on the service instance by the ACL.</td>
</tr>
<tr>
<td>L2 ACL deny count</td>
<td>Displays the number of packet frames not permitted to pass on the service instance by the ACL.</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 Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Carrier Ethernet Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands: master list of commands with complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEF 6.1</td>
<td>Metro Ethernet Services Definitions Phase 2 (PDF 6/08)</td>
</tr>
<tr>
<td>MEF 10.1</td>
<td>Ethernet Services Attributes Phase 2 (PDF 10/06)</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Layer 2 Access Control Lists on EVCs

The table below lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 32: Feature Information for Layer 2 Access Control Lists on EVCs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Access Control Lists on EVCs</td>
<td>12.2(33)SRD 15.0(1)S</td>
<td>The Layer 2 Access Control Lists on EVCs feature introduces ACLs on EVCs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The following commands were introduced or modified: interface, mac access-group in, mac access-list extended, show ethernet service instance.</td>
</tr>
</tbody>
</table>
Layer 3 Access Control Lists on EVCs

This chapter describes how to implement ACLs on EVCs.

- Layer 3 Access Control Lists on EVCs, page 373
- Finding Feature Information, page 373
- Prerequisites for Layer 3 Access Control Lists on EVCs, page 373
- Limitations and Restrictions for Layer 3 Access Control Lists on EVCs, page 374
- Information About Layer 3 Access Control Lists on EVCs, page 374
- Configuring Layer 3 Access Control Lists on EVCs, page 374

Layer 3 Access Control Lists on EVCs

The ability to filter packets in a modular and scalable way is important for both network security and network management. Access Control Lists (ACLs) provide the capability to filter packets at a fine granularity. In Metro Ethernet networks, ACLs are directly applied on Ethernet virtual circuits (EVCs).

Layer 3 Access Control Lists on EVCs is a security feature that allows packet filtering based on IP addresses. This module describes how to implement ACLs on EVCs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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/. An account on Cisco.com is not required.

Prerequisites for Layer 3 Access Control Lists on EVCs

- Knowledge of service instances configuration.
- Knowledge of extended IP ACLs and configuration.
Limitations and Restrictions for Layer 3 Access Control Lists on EVCs

- Supported access control entries (ACEs) are
  - up to 256 ACE, one ACE per IP ACL.
  - up to 511 ACE, on a single IP ACL

---

**Note**

IP ACL can be configured for up to \((N+1) \times M = 512\), where \(N\) is the number of ACE and \(M\) is the number of IP ACLs.

---

**Note**

Filtering is applied to both, control packets and data packets.
ACEs are applied to control packets along with data packets.
If there are no ACEs default is deny all packets.

When you configure IP ACL with Not-equal to <value>, Greater than <value>, Less than <value>, Range <lower bound, higher bound>, each filter is considered as 1 range value per ethernet flow point (EFP).
Maximum supported ACL configuration range check is 60.

Information About Layer 3 Access Control Lists on EVCs

Layer 3 ACLs are of two types:
- Standard
- Extended

The ACLs can be either named or numbered.

Configuring Layer 3 Access Control Lists on EVCs

Creating a Standard Layer 3 ACL

To create a Layer 3 ACL with a single ACE, complete the following steps.
### Summary Steps

1. `enable`
2. `configure terminal`
3. `ip access-list standard 99 number`
4. `permit ?`
5. `end`

### 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>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; <code>enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip access-list standard 99 number</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# ip access-list standard 99 number</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>permit ?</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-std-nacl)# permit host 10.1.1.1</code></td>
</tr>
<tr>
<td></td>
<td><code>any</code></td>
</tr>
<tr>
<td></td>
<td><code>host</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-std-nacl)# end</code></td>
</tr>
</tbody>
</table>

### Applying a Layer 3 ACL to a Service Instance

To apply a Layer 3 ACL to a service instance, complete the following steps.

**Note**

Packet filtering takes place only after the ACL has been created and applied to the service instance.
Before You Begin

Before applying an ACL to a service instance, you must create it using the `ip access-list extended` command. See Creating a Standard Layer 3 ACL, on page 374.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `service instance id ethernet`
5. `encapsulation dot1q vlan-id`
6. `ip access-group access-list-name in`
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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type number</td>
<td>Specifies the type and location of the interface to configure, where:</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface GigabitEthernet 0/10</td>
<td>• type — Specifies the type of the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• number — Specifies the location of the interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# service instance 100 ethernet</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>encapsulation dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-srv)# encapsulation dot1q 100</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>ip access-group access-list-name in</td>
<td>Applies a IP ACL to control incoming traffic on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if-srv)# ip access-group test-12-acl in</td>
<td></td>
</tr>
</tbody>
</table>
Removing a Layer 3 ACL

To remove a Layer 3 ACL, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `service instance id ethernet`
5. `no ip access-group <acl-number> in|out`
6. `no ip access-list name`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td><code>interface type slot/port</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#interface GigabitEthernet 0/10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters the interface configuration mode with the service instance.</td>
</tr>
<tr>
<td><code>service instance id ethernet</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# service instance 100 ethernet</code></td>
<td></td>
</tr>
</tbody>
</table>
Creating a Layer 3 Extended ACL

To create a Layer 3 extended ACL with a single ACE, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip access-list extended name`
4. `permit tcp host 10.1.1.1 any`
5. `deny tcp host 10.1.1.0 any`
6. `end`

**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.</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>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Layer 3 Access Control Lists on EVCs

#### Applying a Layer 3 Extended ACL to a Service Instance

To apply a Layer 3 Extended ACL to a service instance, complete the following steps:

**Note**

Packet filtering takes place only after the ACL has been created and applied to the service instance.

**Before You Begin**

Before applying an ACL to a service instance, you must create it using the `ip access-list extended` command. See [Creating a Standard Layer 3 ACL](#), on page 374.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `service instance id ethernet`
5. `encapsulation dot1q vlan-id`
6. `ip access-group access-list-name in`
7. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
  **Example:**
  ```
  Switch> enable
  ```  
  - Enter your password if prompted. |
| **Step 2** | configure terminal | Enters global configuration mode.  
  **Example:**
  ```
  Switch# configure terminal
  ``` |
| **Step 3** | interface type number | Specifies the type and location of the interface to configure,  
  where:  
  **Example:**
  ```
  Switch(config)# interface GigabitEthernet 0/10
  ```  
  - type—Specifies the type of the interface.  
  - number—Specifies the location of the interface. |
| **Step 4** | service instance id ethernet | Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.  
  **Example:**
  ```
  Switch(config-if)# service instance 100 ethernet
  ``` |
| **Step 5** | encapsulation dot1q vlan-id | Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.  
  **Example:**
  ```
  Switch(config-if-srv)# encapsulation dot1q 100
  ``` |
| **Step 6** | ip access-group access-list-name in | Applies a IP ACL to control incoming traffic on the interface.  
  **Example:**
  ```
  Switch(config-if-srv)# ip access-group test-l3-ext in
  ``` |
| **Step 7** | end | Returns to privileged EXEC mode.  
  **Example:**
  ```
  Switch(config-if-srv)# end
  ``` |

### Removing a Layer 3 Extended ACL

To remove a Layer 3 extended ACL, complete the following steps:
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `service instance id ethernet`
5. `no ip access-group <acl-number> in|out`
6. `no ip access-list extended name`
7. `exit`

### 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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>![Example](Switch&gt; enable)</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td>![Example](Switch# configure terminal)</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)#interface GigabitEthernet 0/10</td>
<td>![Example](switch(config)#interface GigabitEthernet 0/10)</td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id ethernet</td>
<td>Enters the interface configuration mode with the service instance.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-if)# service instance 100 ethernet</td>
<td>![Example](switch(config-if)# service instance 100 ethernet)</td>
</tr>
<tr>
<td><strong>Step 5</strong> no ip access-group &lt;acl-number&gt; in</td>
<td>out</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config-if-srv)# no ip access-group test-12-acl in</td>
<td>![Example](switch(config-if-srv)# no ip access-group test-12-acl in)</td>
</tr>
<tr>
<td><strong>Step 6</strong> no ip access-list extended name</td>
<td>Removes the Layer 3 extended ACL that you specify by name from the running configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# no ip access-list extended acl-mac-01</td>
<td>![Example](switch(config)# no ip access-list extended acl-mac-01)</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# exit</td>
<td>![Example](Switch(config)# exit)</td>
</tr>
</tbody>
</table>
Removing a Layer 3 Extended ACL
This chapter describes Storm Control over EVC and procedures to configure Storm Control over EVC.

- Storm Control over EVC, page 383
- Restrictions for Storm Control over EVC, page 383
- Configuring Storm Control over EVC, page 384
- Examples, page 385
- Verification, page 387

Storm Control over EVC

Storm control prevents traffic on a LAN from being disrupted by a broadcast, a multicast, or a unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic, and degrading network performance.

Storm-control is supported at EFP level and policing can be applied at the EFP level. Storm control is supported on port channel EVCs. When an EVC moves to the error-disable state, auto-recovery can be configured for storm control after a certain pre-determined interval.

Table 33: EFPs Supported

<table>
<thead>
<tr>
<th>Condition</th>
<th>Maximum Supported EFPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both Broadcast and Multicast is applied on same EFP</td>
<td>128</td>
</tr>
<tr>
<td>Only Broadcast</td>
<td>256</td>
</tr>
<tr>
<td>Only Multicast</td>
<td>256</td>
</tr>
</tbody>
</table>

Restrictions for Storm Control over EVC

- Storm control over EVC can be configured on connect, cross connect and bridge-domain interfaces.
• Storm control is supported on port channel EVCs.
• Storm control over EVC can be configured only for broadcast or multicast packets, not for unicast packets.
• If storm control is already configured at the port level, you cannot configure storm control over EVC and vice versa.
• When an EVC moves to the error-disable state, auto-recovery can be configured for storm-control after a certain pre-determined interval.
• SNMP trap is not supported.
• If storm control is enabled on a port channel EVC, the configuration is applied per network processor (NP).
• Only 256 policer profiles are supported per network processor.
• QoS and storm-control share the same hardware policer resources.

### Configuring Storm Control over EVC

Perform these steps to configure storm control over EVC feature.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel
4. service instance id Ethernet
5. encapsulation dot1q vlan-id
6. storm-control {broadcast | multicast} cir cir-value | action shutdown
7. bridge-domain bridge-id
8. end

#### 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.</td>
</tr>
<tr>
<td>Example: Switch# enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Cisco ME 2600X Series Ethernet Access Switch Software Configuration Guide
<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface gigabitethernet slot/port or interface tengigabitethernet slot/port or interface port-channel</td>
<td>Specifies the gigabit ethernet or the ten gigabit ethernet interface, or port channel to configure.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td>- slot/port—Specifies the location of the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- number—Specifies the port channel interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>service instance id Ethernet</td>
<td>Creates a service instance (an instantiation of an EVC) on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# service instance 101 ethernet</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>encapsulation dot1q vlan-id</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if-srv)# encapsulation dot1q 100</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>storm-control {{broadcast</td>
<td>multicast} cir cir-value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cir-value - The acceptable range is 10000000-100000000 for a gigabit ethernet interface, and 100000000-1000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent</td>
</tr>
<tr>
<td></td>
<td>action shutdown}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if-srv)# storm-control broadcast cir 11000000</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>bridge-domain bridge-id</td>
<td>Binds the service instance to a bridge domain instance where bridge-id is the identifier.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if-srv)# bridge-domain 12</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if-srv)# end</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the ingress packets exceed the configured rate, the EVC moves to error-disable state if the action is configured as shutdown. You can configure the EVC to move to up state after a certain interval using errdisable recovery cause storm-control interval command. The accepted interval varies from 30 to 86400 seconds.</td>
<td></td>
</tr>
</tbody>
</table>
Switch(config-if-srv)# bridge-domain 12

Switch# sh running-config interface g0/30

Building configuration...

Current configuration : 347 bytes
!
interface GigabitEthernet0/30
  no ip address
  speed auto
  duplex auto
  negotiation auto
  soak link notification 0
  l2protocol peer cdp lacp
  l2protocol forward stp vtp dtp pagp dot1x
  service instance 1 ethernet
  encapsulation dot1q 100
  storm-control broadcast cir 10000000
  storm-control multicast cir 10000000
  bridge-domain 12

If action -shut is used errdisable needs to be configured.

Note no storm-control action shutdown is not supported.

The following example shows how to configure ERR disable:

Switch(config)# interface g0/30
Switch(config-if)# no shut
Switch(config-if-srv)# encapsulation dot1q 100
Switch(config-if-srv)# storm-control broadcast cir 10m
Switch(config-if-srv)# storm-control multicast cir 10m
Switch(config-if-srv)# storm-control action shutdown
Switch(config-if-srv)# errdisable recovery cause storm-control 30
Switch(config-if-srv)# bridge-domain 12

Switch# sh running-config interface g0/30

Building configuration...

Current configuration : 425 bytes
!
interface GigabitEthernet0/30
  no ip address
  speed auto
  duplex auto
  negotiation auto
  soak link notification 0
  l2protocol peer cdp lacp
  l2protocol forward stp vtp dtp pagp dot1x
  service instance 1 ethernet
  encapsulation dot1q 100
  storm-control action shutdown
  storm-control broadcast cir 10000000
  storm-control multicast cir 10000000
  errdisable recovery cause storm-control 30
  bridge-domain 12
!
Verification

Use the `show ethernet service instance id id interface type slot/port stats` command to verify the storm control over EVC configuration.

```
Switch# show ethernet service instance id 1204 interface gigabit ethernet 2/7 stats
```

- Port maximum number of service instances: 8000
- Service Instance 1204, Interface GigabitEthernet2/7
  - Pkts In  Bytes In  Pkts Out  Bytes Out
    - 2262238  452447600  150570  30114000
- Storm Control Discard Pkts: 1809909
Control Plane Policing

This chapter describes Control Plane Policing and procedures to configure Control Plane Policing.

- Control Plane Policing, page 389
- Finding Feature Information, page 389
- Restrictions for Control Plane Policing, page 390
- Benefits of Control Plane Policing, page 391
- Defining Control Plane Services, page 391
- Verifying Control Plane Services, page 392
- Configuration Examples for Control Plane Policing, page 394
- Technical Assistance, page 394

Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS devices and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE Software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for Control Plane Policing

Output Rate-Limiting Support
Output rate-limiting is performed in the silent (packet discard) mode. Silent mode enables a device to silently discard packets using policy maps applied to output control plane traffic with the service-policy output command.

MQC Restrictions
The Control Plane Policing feature requires the MQC to configure packet classification, packet marking, and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing. Only two MQC actions are supported in policy maps—police and set.

Only permit any any is supported.
The Control Plane Policing feature supports IP, IGMP, OSPF and ARP.

OSPF Restrictions
• Hardware based layer 3 forwarding is not supported.
• The maximum layer 3 traffic line rate supported is 3 Mbps. When the traffic line rate exceeds 3 Mbps, all layer 3 protocols fail.

Policer Support
• Only 3Mbps policer is supported.
• More than 3Mbps policer cannot be attached to the control plane.
• Only input policer is supported.
• If any control packet is configured for 3Mbps rate limit, all the remaining control packets are dropped.
• There is no priority method for control-packets.

We recommend that you configure support control packets within 2Mbps and spare 1Mbps for class-default.

Match Criteria Support and Restrictions
The following classification (match) criteria are supported:

• Standard and extended IP access control lists (ACLs).

Note
In extended IP access control list only IGMP and ospf is supported.

• In class-map configuration mode, match criteria specified by the following commands:
  • match protocol ip
Benefits of Control Plane Policing

Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

Defining Control Plane Services

Restrictions for Control Plane Services

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

Before You Begin

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

SUMMARY STEPS

1. enable
2. configure terminal
3. control-plane
4. service-policy {input} policy-map-name
5. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
  * Example:  
  Switch> enable  
  - Enter your password if prompted. |
| **Step 2** | configure terminal | Enters global configuration mode.  
  * Example:  
  Switch# configure terminal |
| **Step 3** | control-plane | Enters control-plane configuration mode (a prerequisite for Step 4)  
  * Example:  
  Switch(config)# control-plane |
| **Step 4** | service-policy {input} policy-map-name | Attaches a QoS service policy to the control plane. Note the following points:  
  * input—Applies the specified service policy to packets received on the control plane.  
  * policy-map-name—Name of a service policy map (created using the policy-map command) to be attached.  
  * Example:  
  Switch(config-cp)# service-policy input control-plane-policy |
| **Step 5** | end | (Optional) Returns to privileged EXEC mode.  
  * Example:  
  Switch(config-cp)# end |

### Verifying Control Plane Services

#### SUMMARY STEPS

1. enable
2. show policy-map control-plane
3. exit

#### DETAILED STEPS

<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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter your password if prompted.</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <strong>enable</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>show policy-map control-plane</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# <strong>show policy-map control-plane all</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# <strong>exit</strong></td>
</tr>
</tbody>
</table>

### Examples

The following example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class map TEST, while allowing all other traffic (that matches the class map "class-default") to go through as is.

```
Switch# sh policy-map control-plane
```

Limited counter support. Refer documentation for details.

**Control Plane**

Service-policy input: pigmp

```
Class-map: igmp (match-all)
  108210 packets, 6925376 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group 100
police:
  cir 2000000 bps, bc 62500 bytes
  conformed 98551 packets, 6307200 bytes; actions:
    transmit
  exceeded 9659 packets, 618176 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  17 packets, 5959 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
police:
  cir 1000000 bps, bc 31250 bytes
  conformed 17 packets, 5959 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps
```
Configuration Examples for Control Plane Policing

The following example shows how to configure control plane policing:

```
Switch(config)# access-list 101 permit ospf any any
Switch(config)# class-map ospf
Switch(config-cmap)# match access-group 101
Switch(config)# policy-map pospf
Switch(config-pmap)# class ospf
Switch(config-pmap-c)# police cir 2m
Switch(config-pmap-c-police)# control-plane
Switch(config-cp)# service-policy input pospf
```

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
CHAPTER 21

ICMP Unreachable Rate Limiting User Feedback

This chapter describes ICMP Unreachable Rate Limiting User Feedback and procedures to configure ICMP Unreachable Rate Limiting User Feedback.

- Configuring ICMP Unreachable Rate Limiting User Feedback, page 395
- Configuring ICMP Unreachable Rate Limiting User Feedback, page 396
- ICMP Unreachable Destination Counters, page 397
- ICMP Overview, page 398
- Denial of Service Attack, page 398
- Clearing the ICMP Unreachable Destination Packet Statistics, page 398
- Configuring ICMP Unreachable Destination Counters and Logging Intervals, page 399
- Displaying the ICMP Unreachable Destination Packets, page 401

Configuring ICMP Unreachable Rate Limiting User Feedback

Perform this task to clear all of the unreachable destination packet statistics and to specify an interval number for unreachable destination messages. This task also configures a packet counter (threshold) and interval to trigger a logging message to a console. This task is beneficial to begin a new log after the thresholds have been set.
## Configuring ICMP Unreachable Rate Limiting User Feedback

### SUMMARY STEPS

1. enable
2. clear ip icmp rate-limit [interface-type interface-number]
3. configure terminal
4. ip icmp rate-limit unreachable [df][ms] [log [packets] [interval-ms]]
5. exit
6. show ip icmp rate-limit [interface-type interface-number]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** Switch> enable |

| **Step 2** clear ip icmp rate-limit [interface-type interface-number] | Clears all current ICMP unreachable statistics for all configured interfaces.  
The optional interface-type and interface-number arguments clear the statistics for only one interface. |
| **Example:** Switch# clear ip icmp rate-limit GigabitEthernet 0/3 |

| **Step 3** configure terminal | Enters global configuration mode |
| **Example:** Switch# configure terminal |

| **Step 4** ip icmp rate-limit unreachable [df][ms] [log [packets] [interval-ms]] | Specifies the rate limitation of ICMP unreachable destination messages and the error message log threshold for generating a message. The default is no unreachable messages are sent more often than once every half second. |
| **Example:** Switch(config)# ip icmp rate-limit unreachable df log 1100 12000 |

The arguments and keywords are as follows:

- **df** --(Optional) When "don't fragment" (DF) bit is set in the ICMP header, a datagram cannot be fragmented. If the df keyword is not specified, all other types of destination unreachable messages are sent.
- **ms** --(Optional) Interval at which unreachable messages are generated. The valid range is from 1 to 4294967295.
- **log** --(Optional) List of error messages. The arguments are as follows:
  - **packets** --(Optional) Number of packets that determine a threshold for generating a log. The default is 1000.
**ICMP Unreachable Rate Limiting User Feedback**

**Command or Action | Purpose**
--- | ---

|  | “interval-ms” *(Optional)* Time limit for an interval for which a logging message is triggered. The default is 60000, which is 1 minute. |

**Note**
Counting begins as soon as this command is configured.

**Step 5**

**exit**

*Example:*

Switch(config)# exit

Exits to privileged EXEC mode.

**Step 6**

**show ip icmp rate-limit [interface-type interface-number]**

*Example:*

Switch# show ip icmp rate-limit ethernet 2/3

(Optional) Displays all current ICMP unreachable statistics for all configured interfaces. The optional interface-type and interface-number arguments display the statistics for only one interface.

**Examples:**

The following output using the `show ip icmp rate-limit` command displays the unreachable destinations by interface:

```
Switch# show ip icmp rate-limit

DF bit unreachables   All other unreachables
--------------------------------------------
Interval (millisecond) 500 # DF bit unreachables  500 # All other
Interface unreachables
--------------------------------------------
Ethernet0/0            0
Ethernet0/2            0
Serial3/0/3            0 19
```

The greatest number of unreachables is on serial interface 3/0/3

---

**ICMP Unreachable Destination Counters**

The ICMP Unreachable Destination Counters feature enables you to clear and display packets that have been discarded because of an unreachable destination, and to configure a threshold interval for triggering error messages. When message logging is generated, it displays on your console.
Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at [http://www.cisco.com/go/fn](http://www.cisco.com/go/fn). You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

ICMP Overview

Originally created for the TCP/IP suite in RFC 792, the Internet Control Message Protocol (ICMP) was designed to report a small set of error conditions. ICMP also can report a wide variety of error conditions, provide feedback and testing capabilities. It is a valuable support tool because each message uses a common format and is sent and received by using the same protocol rules.

ICMP enables IP to perform addressing, datagram packaging, and routing by allowing encapsulated messages to be sent and received between IP devices. These messages are encapsulated in IP datagrams just like any other IP message. When the message is generated, the original IP header is encapsulated in the ICMP message and these two pieces are encapsulated within a new IP header to be returned as an error report to the sending device.

ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. To avoid the infinite regress of messages about messages, no ICMP messages are sent about ICMP messages.

ICMP does not make IP reliable or ensure the delivery of datagrams or the return of a control message. Some datagrams may be dropped without any report of their loss. The higher-level protocols that use IP must implement their own reliability procedures if reliable communication is required.

For information about IPv6 and ICMP, see the [Cisco IOS IPv6 Configuration Guide, Release 12.4](http://www.cisco.com) and [Cisco IOS IPv6 Command Reference, Release 12.4](http://www.cisco.com).

Denial of Service Attack

A DoS attack occurs when a stream of ICMP echo requests (pings) are broadcast to a destination subnet. The source addresses of these requests are falsified to be the source address of the target. For each request sent by the attacker, many hosts on the subnet will respond flooding the target and wasting bandwidth. The most common DoS attack is called a "smurf" attack, named after an executable program and is in the category of network-level attacks against hosts. DoS attacks can be easily detected when error-message logging of the ICMP Unreachable Destination Counters feature is enabled.

Clearing the ICMP Unreachable Destination Packet Statistics

Perform this task to clear all of the unreachable destination packet statistics. This task is beneficial to begin a new log after the thresholds have been set.
SUMMARY STEPS

1. enable
2. clear ip icmp rate-limit [interface-type interface-number]
3. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> clear ip icmp rate-limit [interface-type interface-number]</td>
<td>Clears all current ICMP unreachable statistics for all configured interfaces. The optional interface-type and interface-number arguments clear the statistics for only one interface.</td>
</tr>
<tr>
<td>Example: Switch# clear ip icmp rate-limit GigabitEthernet 0/3</td>
<td>Note See the interface command in the Cisco IOS Interface and Hardware Component Command Reference, Release 12.4 for valid interface types.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Exits to user EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring ICMP Unreachable Destination Counters and Logging Intervals

Perform this task to specify an interval number for unreachable destination messages and a packet counter (threshold) and interval to trigger a logging message to a console. Counting begins as soon as the ip icmp rate-limit unreachable command is configured.

Before You Begin
Clearing the ICMP Unreachable Destination Packet Statistics, on page 398

When Cisco ME 2600X is configured with a default static route such as IP route 0.0.0.0 0.0.0.0 g1/1 then for any destination IP destination unreachable counters do not increase.
SUMMARY STEPS

1. enable
2. configure terminal
3. ip icmp rate-limit unreachable [df] [ms] [log] [packets] [interval-ms]
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip icmp rate-limit unreachable [df] [ms] [log] [packets] [interval-ms]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ip icmp rate-limit unreachable df log 1100 12000</td>
</tr>
<tr>
<td>Note</td>
<td>Counting begins as soon as this command is configured.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# exit</td>
</tr>
</tbody>
</table>
Displaying the ICMP Unreachable Destination Packets

Perform this optional task to display all of the unreachable destination packet statistics, which include dropped packets. Counting begins as soon as the `ip icmp rate-limit unreachable` command is configured.

**SUMMARY STEPS**

1. `enable`
2. `show ip icmp rate-limit [interface-type interface-number]`
3. `end`

**DETAILED STEPS**

<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><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show ip icmp rate-limit [interface-type interface-number]</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show ip icmp rate-limit GigabitEthernet 0/3</td>
</tr>
<tr>
<td></td>
<td>Displays all current ICMP unreachable statistics for all configured interfaces. The optional <code>interface-type</code> and <code>interface-number</code> arguments displays the statistics for only one interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> See the <code>interface</code> command in the <em>Cisco IOS Interface and Hardware Component Command Reference</em>, Release 12.4 for valid interface types</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# end</td>
</tr>
</tbody>
</table>

**Example**

The following output using the `show ip icmp rate-limit` command displays the unreachable destinations by interface:

```
Switch# show ip icmp rate-limit

+-----------------+-----------------+-----------------+
| DF bit unreachables | All other unreachables | 
| Interval (millisecond) | 500 | 500 |
| Interface unreachables | # DF bit unreachables | # All other unreachables |
| Ethernet0/0 | 0 | 0 |
| Ethernet0/2 | 0 | 0 |
```

Cisco ME 2600X Series Ethernet Access Switch Software Configuration Guide
The greatest number of unreachables is on serial interface 3/0/3.
CHAPTER 22

IP Version 6 Support for the Management Port

This chapter describes IP Version 6 (IPv6) Support for the Management Port and procedures to configure IPv6 for the Management Port.

- IP Version 6 Support for the Management Port, page 403
- Prerequisites for IPv6, page 404
- Restrictions for IPv6, page 404
- Information About IPv6, page 404
- How to Configure IPv6, page 408
- Troubleshooting Tips, page 424
- Configuration Examples for IPv6, page 425
- Verifying the IPv6 Configuration, page 426
- Additional References for IPv6, page 428

IP Version 6 Support for the Management Port

IP version 6 is a new IP protocol designed to replace IP version 4, the Internet protocol that is extensively used throughout the world.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see the Bug Toolkit and 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 the 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.
Prerequisites for IPv6

- You must be familiar with IPv6 basics such as IPv6 addressing, IPv6 header information, ICMPv6, and the IPv6 Neighbor Discovery (ND) Protocol.
- Ensure that you follow the memory and/or processing guidelines when you convert a device to a dual-stack device (IPv4/IPv6).

Restrictions for IPv6

- IPv6 packets are transparent to Layer 2 LAN switches because the switches do not examine Layer 3 packet information before forwarding IPv6 frames. IPv6 hosts can be directly attached to Layer 2 LAN switches.
- You can configure multiple IPv6 global addresses within the same prefix on an interface. However, multiple IPv6 link-local addresses on an interface are not supported.
- Because RFC 3879 deprecates the use of site-local addresses, you should configure private IPv6 addresses according to the recommendations of unique local addressing (ULA) in RFC 4193.

Information About IPv6

IPv6 increases the number of network address bits from 32 bits (in IPv4) to 128 bits. IPv6 is based on IPv4 but it includes a much larger address space and other improvements such as a simplified main header and extension headers.

The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently. The flexibility of the IPv6 address space reduces the need for private addresses and the use of Network Address Translation (NAT), which translates private (not globally unique) addresses into a limited number of public addresses. IPv6 enables new application protocols that do not require special processing by border routers at the edge of networks.

IPv6 functionalities such as prefix aggregation, simplified network renumbering, and IPv6 site multihoming capabilities, enable more efficient routing. IPv6 supports Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF) for IPv6, and multiprotocol Border Gateway Protocol (BGP).

IPv6-Enabled Commands

The following Cisco Firewall Services Module (FWSM) commands can accept and display IPv6 addresses:

- capture
- configure
- copy
- http
- name
Failover does not support IPv6. The `ipv6 address` command does not support setting standby addresses for failover configurations. The `failover interface ip` command does not support using IPv6 addresses on the failover and stateful failover interfaces.

When entering IPv6 addresses in commands that support them, simply enter the IPv6 address using standard IPv6 notation; for example `fe80::2e0:b6ff:fe01:3b7a` or `[fe80::2e0:b6ff:fe01:3b7a]`. The Cisco ME 2600X device supports both notations (IPv6 addresses with or without the square brackets).

The following commands were modified to work for IPv6:

- `debug`
- `fragment`
- `ip`
- `verify`
- `mtu icmp` (entered as `ipv6 icmp`)

The following inspection engines support IPv6:

- FTP
- HTTP
- ICMP
- SMTP
- TCP
- UDP
IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to
determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a
neighbor, and keep track of neighboring devices.

These topics contain more information:

• Neighbor Solicitation Messages
• Router Advertisement Messages

Neighbor Solicitation Messages

Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address
of another node on the same local link (see the figure below). When a node wants to determine the link-layer
address of another node, the source address in a neighbor solicitation message is the IPv6 address of the node
sending the neighbor solicitation message. The destination address in the neighbor solicitation message is the
solicited-node multicast address that corresponds to the IPv6 address of the destination node. The neighbor
solicitation message also includes the link-layer address of the source node.

![IPv6 Neighbor Discovery—Neighbor Solicitation Message](image)

After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement
message (ICMPv6 Type 136) on the local link. The source address in the neighbor advertisement message is
the IPv6 address of the node sending the neighbor advertisement message; the destination address is the IPv6
address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement
message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement message, the source node communicates with the
destination node. The figure above shows the neighbor solicitation and response process.
Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. When there is such a change, the destination address for the neighbor advertisement is the all-nodes multicast address.

You can configure the neighbor solicitation message interval and neighbor reachable time on a per-interface basis. These topics contain more information:

- Configuring the Neighbor Solicitation Message Interval
- Configuring the Neighbor Reachable Time

**Router Advertisement Messages**

Router advertisement messages (ICMPv6 Type 134) are periodically sent to each IPv6 configured interface of FWSM. The router advertisement messages are sent to the all-nodes multicast address.

*Figure 25: IPv6 Neighbor Discovery—Router Advertisement Message*

Router advertisement messages include the following information:

- One or more IPv6 prefix that nodes on the local link can use to automatically configure their IPv6 addresses.
- Lifetime information for each prefix included in the advertisement.
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed.
- Default router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time (in seconds) the router should be used as a default router).
- Additional information for hosts, such as the hop limit and MTU a host should use in packets that it originates.
- The amount of time between neighbor solicitation message retransmissions on a given link.
- The amount of time a node considers a neighbor reachable.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without waiting for the next scheduled router advertisement message. Because router solicitation messages are usually
sent by hosts, and the host does not have a configured unicast address, the source address in router solicitation messages is usually the unspecified IPv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When a router advertisement is sent in response to a router solicitation, the destination address in the router advertisement message is the unicast address of the source of the router solicitation message.

You can configure the following settings for router advertisement messages:

- The time interval between periodic router advertisement messages.
- The router lifetime value, which indicates the amount of time IPv6 nodes should consider for the FWSM to be the default router.
- The IPv6 network prefixes in use on the link.
- Whether or not an interface transmits router advertisement messages.

Unless otherwise noted, the router advertisement message settings are specific to an interface and are entered in interface configuration mode. These topics contain information about changing the router settings:

- Configuring the Router Advertisement Transmission Interval
- Configuring the Router Lifetime Value
- Configuring the IPv6 Prefix
- Suppressing Router Advertisement Messages

How to Configure IPv6

The following tasks describe how to configure IPv6 on the Cisco ME 2600X device:

- Configuring IPv6 on an Interface, on page 409
- Configuring IPv6 Duplicate Address Detection, on page 412
- Configuring IPv6 Default and Static Routes, on page 414
- Configuring IPv6 Access Lists, on page 415
- Configuring the Neighbor Solicitation Message Interval, on page 417
- Configuring the Neighbor Reachable Time, on page 418
- Configuring the Router Advertisement Transmission Interval, on page 419
- Configuring the Router Lifetime Value, on page 420
- Configuring the IPv6 Prefix, on page 421
- Suppressing Router Advertisement Messages, on page 422
- Configuring a Static IPv6 Neighbor, on page 423
Configuring IPv6 on an Interface

FWSM supports dual IP stack. You can configure both IPv6 and IPv4 on an interface. You do not need to enter any special commands to do so; simply enter the IPv4 configuration commands and IPv6 configuration commands as you normally would. Make sure you configure the default route for both IPv4 and IPv6.

Note

You cannot configure IPv6 on an interface that is used by more than one context (a shared VLAN).

To configure IPv6 on an interface, complete the following steps:

**Before You Begin**

At a minimum, each interface needs to be configured with an IPv6 link-local address. Additionally, you can add a site-local and global addresses to an interface.

**Note**

FWSM does not support IPv6 anycast addresses.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface type slot/port**
4. **ipv6 address autoconfig** or **ipv6 address ipv6-address link-local** or **ipv6 enable** or **ipv6 address ipv6-address [eui-64]** or **ipv6 nd suppress-ra**
5. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| Example: Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Switch# configure terminal |
| **Step 3** interface type slot/port | Configures an IPv6 address for the interface. You can assign several IPv6 addresses to an interface, such as an IPv6 link-local, site-local, and global address. However, at a minimum, you must configure a link-local address.  
  There are several methods for configuring IPv6 addresses for an interface. Pick the method that suits your needs from the next step. |
| Example: Switch(config)# interface GigabitEthernet 0/1 |
### Configuring IPv6 on a Bridge Domain Interface

To configure IPv6 on a bridge domain interface, complete the following steps:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 address autoconfig or ipv6 address ipv6-address link-local or ipv6 enable or ipv6 address ipv6-address [eui-64] or ipv6 nd suppress-ra</td>
<td>Configures the following:</td>
</tr>
<tr>
<td></td>
<td>• Autoconfig:</td>
</tr>
<tr>
<td></td>
<td>Enables stateless autoconfiguration on the interface. Enabling stateless autoconfiguration configures IPv6 addresses based on prefixes received in Router Advertisement messages. A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Link-local address:</td>
</tr>
<tr>
<td></td>
<td>Configures a link-local address on the interface. If you do not assign any other IPv6 addresses to the interface, you can manually define the link-local address or generating one based on the interface MAC address (Modified EUI-64 format).</td>
</tr>
<tr>
<td></td>
<td>• IPv6 on the interface:</td>
</tr>
<tr>
<td></td>
<td>Enables IPv6 on the interface and automatically generate the link-local address using the Modified EUI-64 interface ID based on the interface MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You do not need to use the ipv6 enable command if you enter any other ipv6 address commands on an interface; IPv6 support is automatically enabled as soon as you assign an IPv6 address to the interface.</td>
</tr>
<tr>
<td></td>
<td>• Site-local or global address:</td>
</tr>
<tr>
<td></td>
<td>Assigns a site-local or global address to the interface. When you assign a site-local or global address, a link-local address is automatically created. Use the optional eui-64 keyword to use the Modified EUI-64 interface ID in the low order 64 bits of the address.</td>
</tr>
<tr>
<td></td>
<td>• Suppress Router Advertisement messages:</td>
</tr>
<tr>
<td></td>
<td>By default, router advertisement messages are automatically sent in response to router solicitation messages. You may want to disable these messages on interfaces for which you do not want FWSM to supply the IPv6 prefix (for example, the outside interface).</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring IPv6 on a Bridge Domain Interface

To configure IPv6 on a bridge domain interface, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. service instance id ethernet [evc-id]
5. encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]}
6. bridge-domain bridge-id
7. exit
8. no shutdown
9. exit
10. interface BDI interface number
11. ipv6 address {X:X:X::X link-local | X:X:X::X/prefix [anycast | eui-64] | autoconfig [default]} or ip address ip-address mask
12. no shutdown
13. 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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>interface type slot/port</td>
<td>Specifies the port adapter type and the location of the interface to be configured. The slot is always 0 and the port is the number of the port.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>service instance id ethernet [evc-id]</td>
<td>Configures an Ethernet service instance on an interface and enters service instance configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# service instance 100 ethernet</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>encapsulation dot1q {any</td>
<td>vlan-id [vlan-id [-vlan-id]]}</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if-srv)# encapsulation dot1q 100</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 6   bridge-domain bridge-id</td>
<td>Binds the Ethernet service instance to a bridge domain instance where <em>bridge-id</em> is the identifier for the bridge domain instance. The valid values for <em>bridge-id</em> range from 1 to 4096.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# bridge-domain 3000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7   exit</td>
<td>Exits the service instance configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8   no shutdown</td>
<td>Enables an interface.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# no shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 9   exit</td>
<td>Exits the interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 10  interface BDI interface number</td>
<td>Specifies a bridge domain interface. <em>Note</em> The <em>interface number</em> must be same as the <em>bridge-id</em>.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# interface bdi 3000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 11  ipv6 address {X:X:X::X} link-local</td>
<td>Specifies the IPv6 or IPv4 address for the bridge domain interface.</td>
<td></td>
</tr>
<tr>
<td>X:X:X::X/prefix [anycast</td>
<td>eui-64]</td>
<td>autoconfig [default]</td>
</tr>
<tr>
<td>Example: Switch(config-if)# ipv6 address 20::1/64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip address 20.1.1.1 255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 12  no shutdown</td>
<td>Enables an interface.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# no shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 13  end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring IPv6 Duplicate Address Detection

During the stateless autoconfiguration process, duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection is first performed on the...
new link-local address. And only when the link local address is verified as unique, duplicate address detection is performed on all the other IPv6 unicast addresses on the interface.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state. An interface returning to an administratively up state restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

When a duplicate address is identified, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is issued. If the duplicate address is a global address of the interface, the address is not used and an error message is issued. However, all configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

FWSM uses neighbor solicitation messages to perform duplicate address detection. By default, the number of times an interface performs duplicate address detection is 1.

To change the number of duplicate address detection attempts and the neighbor solicitation message interval, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd dad attempts value
5. ipv6 nd ns-interval value
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  Example: Switch> enable  
  • Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode.  
  Example: Switch# configure terminal |
| Step 3 | interface type slot/port | Enters interface configuration mode.  
  Example: Switch(config)# interface GigabitEthernet 0/1 |
| Step 4 | ipv6 nd dad attempts value | Changes the number of duplicate address detection attempts. |
### Configuring IPv6 Default and Static Routes

IPv6 unicast routing is always enabled. FWSM routes IPv6 traffic between interfaces as long as the interfaces are enabled for IPv6 and the IPv6 access lists allow the traffic. You can add a default route and static routes using the ipv6 route command.

To configure an IPv6 default route and static routes, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ipv6 route interface_name ::/0 next_hop_ipv6_addr`
4. `ipv6 route if_name destination next_hop_ipv6_addr [admin_distance]`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 2**

**Command**

```
configure terminal
```

**Example:**

```
Switch# configure terminal
```

**Purpose**

Enters global configuration mode.

**Step 3**

**Command**

```
ipv6 route interface_name ::/0 next_hop_ipv6_addr
```

**Example:**

```
Switch(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1
```

**Purpose**

Adds a default IPv6 route.

**Step 4**

**Command**

```
ipv6 route if_name destination next_hop_ipv6_addr [admin_distance]
```

**Example:**

```
Switch(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]
```

**Purpose**

(Optional) Adds an IPv6 static route to the IPv6 routing table.

**Step 5**

**Command**

```
end
```

**Example:**

```
Switch(config-if)# end
```

**Purpose**

Returns to privileged EXEC mode.

---

### Configuring IPv6 Access Lists

Configuring an IPv6 access list is similar configuring an IPv4 access, but with IPv6 addresses.

To create an access list, use the `ipv6 access-list` command to create entries for the access list. There are two main forms of this command to choose from, one for creating access list entries specifically for ICMP traffic, and one to create access list entries for all other types of IP traffic.

To configure an IPv6 access list, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ipv6 access-list id [line num] {permit | deny} icmp source destination [icmp_type]`
4. `ipv6 access-list id [line num] {permit | deny} protocol source [src_port] destination [dst_port]`
5. `access-group iaccess_list_name {in | out} interface if_name [icmp_type]`
6. `end`

---

Cisco ME 2600X Series Ethernet Access Switch Software Configuration Guide

OL-28850-04

415
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td>• To create an IPv6 access list entry specifically for ICMP traffic go to step 3.</td>
</tr>
<tr>
<td></td>
<td>• To create an IPv6 access list entry for IP traffic other than ICMP go to step 4.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates an IPv6 access list entry specifically for ICMP traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The following describes the arguments for the <code>ipv6 access-list</code> command:</td>
</tr>
<tr>
<td><code>Switch(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D</code></td>
<td>• <code>id</code>—The name of the access list. Use the same <code>id</code> in each command when you are entering multiple entries for an access list.</td>
</tr>
<tr>
<td></td>
<td>• <code>line num</code>—When adding an entry to an access list, you can specify the line number in the list where the entry should appear.</td>
</tr>
<tr>
<td></td>
<td>• `permit</td>
</tr>
<tr>
<td></td>
<td>• <code>icmp</code>—Indicates that the access list entry applies to ICMP traffic.</td>
</tr>
<tr>
<td></td>
<td>• <code>protocol</code>—Specifies the traffic being controlled by the access list entry. The entry could be the name (<code>ip, tcp, or udp</code>) or number (1-254) of an IP protocol. Alternatively, you can specify a protocol object group using <code>object-group grp_id</code>.</td>
</tr>
<tr>
<td></td>
<td>• <code>source and destination</code>—Specifies the source or destination of the traffic. The source or destination can be an IPv6 prefix, in the format <code>prefix/length</code>, to indicate a range of addresses, the keyword any, to specify any address, or a specific host designated by <code>host host_ipv6_addr</code>.</td>
</tr>
<tr>
<td></td>
<td>• <code>src_port and dst_port</code>—The source and destination port (or service) argument. Enter an operator (Lt for less than, <code>gt</code> for greater than, <code>eq</code> for equal to, <code>neq</code> for not equal to, or <code>range</code> for an inclusive range) followed by a space and a port number (or two port numbers separated by a space for the <code>range</code> keyword).</td>
</tr>
<tr>
<td></td>
<td>• <code>icmp_type</code>—Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 155) or one of the ICMP type literals as shown in Appendix D, &quot;Addresses, Protocols, and Ports&quot;. Alternatively, you can specify an ICMP object group using <code>object-group id</code>.</td>
</tr>
</tbody>
</table>
### Configuring the Neighbor Solicitation Message Interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, complete the following steps:

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd ns-interval value
5. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Example:**
Switch> enable | • Enter your password if prompted. |

**Step 2**

configure terminal

**Example:**
Switch# configure terminal

Enters global configuration mode.

**Step 3**

interface type slot/port

**Example:**
Switch(config)# interface GigabitEthernet 0/1

Enters interface configuration mode.

**Step 4**

ipv6 nd ns-interval value

**Example:**
Switch(config-if)# ipv6 nd ns-interval 1500

Changes the neighbor solicitation message interval. When you configure an interface to send out more than one duplicate address detection attempt, you can also use the `ipv6 nd ns-interval` command to configure the interval at which the neighbor solicitation messages are sent out. By default, they are sent out once every 1000 milliseconds. The `value` argument can be from 1000 to 3600000 milliseconds.

**Note** This setting is also sent in router advertisement messages.

**Step 5**

derend

**Example:**
Switch(config-if)# end

Returns to privileged EXEC mode.

---

**Configuring the Neighbor Reachable Time**

The neighbor reachable time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd reachable-time value
5. end
DETAILED STEPS

<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><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type slot/port</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface GigabitEthernet 0/1</td>
</tr>
<tr>
<td></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ipv6 nd reachable-time value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# ipv6 nd reachable-time 1000</td>
</tr>
<tr>
<td></td>
<td>Sets the amount of time that a remote IPv6 node is reachable.</td>
</tr>
<tr>
<td></td>
<td>The value argument can be from 0 to 3600000 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>The default is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This information is also sent in router advertisement messages.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuring the Router Advertisement Transmission Interval

To change the interval between router advertisement transmissions on an interface, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd ra-interval [msec] value
5. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | **enable** | Enables privileged EXEC mode.  
   - Enter your password if prompted. |
|   | **Example:**  
   Switch> enable | |
| Step 2 | **configure terminal** | Enters global configuration mode. |
|   | **Example:**  
   Switch# configure terminal | |
| Step 3 | **interface type slot/port** | Enters interface configuration mode. |
|   | **Example:**  
   Switch(config)# interface GigabitEthernet 0/1 | |
| Step 4 | **ipv6 nd ra-interval [msec] value** | Sets the interval between IPv6 router advertisement transmissions.  
The optional msec keyword indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is in seconds.  
The value argument can be from 3 to 1800 seconds or from 500 to 1800000 milliseconds if the msec keyword is provided. The default is 200 seconds.  
**Note** The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the FWSM is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the desired value. |
|   | **Example:**  
   Switch(config-if)# ipv6 nd ra-interval 1000 | |
| Step 5 | **end** | Returns to privileged EXEC mode. |
|   | **Example:**  
   Switch(config-if)# end | |

### Configuring the Router Lifetime Value

The router lifetime value specifies how long nodes on the local link should consider FWSM as the default router on the link.

To configure the router lifetime value in IPv6 router advertisements on an interface, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd ra-lifetime value
5. end

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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 nd ra-lifetime value</td>
<td>Sets the interval between IPv6 router advertisement transmissions.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# ipv6 nd ra-lifetime 5000</td>
<td>The value argument can be from 0 to 9000 seconds. The default is 1800 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the IPv6 Prefix

Stateless autoconfiguration uses IPv6 prefixes provided in router advertisement messages to create the global unicast address from the link-local address.

To configure which IPv6 prefixes are included in IPv6 router advertisements, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd prefix ipv6-prefix/prefix-length
5. end

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.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface GigabitEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 nd prefix ipv6-prefix/prefix-length</td>
<td>Configures which IPv6 prefixes are included in IPv6 router advertisements.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: For stateless autoconfiguration to work properly, the advertised prefix length in router advertisement messages must always be 64 bits.</td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 nd prefix 2001:200:200::/35 1000 900</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Suppressing Router Advertisement Messages

By default, Router Advertisement messages are automatically sent in response to router solicitation messages. You may want to disable these messages on any interface for which you do not want FWSM to supply the IPv6 prefix (for example, the outside interface).

To suppress IPv6 router advertisement transmissions on an interface, complete the following steps:
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 nd suppress-ra
5. end

### DETAILED STEPS

<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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type slot/port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface GigabitEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ipv6 nd suppress-ra</td>
<td>Suppresses the router lifetime value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# ipv6 nd suppress-ra</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Static IPv6 Neighbor

You can manually define a neighbor in the IPv6 neighbor cache. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

To configure a static entry in the IPv6 neighbor discovery cache, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ipv6 neighbor ipv6_address if_name mac_address
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type slot/port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 ipv6 neighbor ipv6_address if_name mac_address</td>
<td>Configures a static entry in the IPv6 neighbor discovery cache.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472</td>
<td></td>
</tr>
<tr>
<td>The ipv6_address argument is the link-local IPv6 address of the neighbor, the if_name argument is the interface through which the neighbor is available, and the mac_address argument is the MAC address of the neighbor interface.</td>
<td></td>
</tr>
<tr>
<td>Note The clear ipv6 neighbors command does not remove static entries from the IPv6 neighbor discovery cache.</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Troubleshooting Tips

Use these debug commands to troubleshoot IPv6:

• debug ipv6 pim—Helps discover whether the PIM protocol activities are working correctly.
configuration examples for IPv6

configuring IPv6 Duplicate Address Detection
the following example shows how to configure an IPv6 duplicate address detection:

```plaintext
configure terminal
interface GigabitEthernet 0/1
ipv6 address 2001:db8::/64 eui64
ipv6 nd reachable-time 10
```

configuring IPv6 Default Route
the following example shows how to configure an IPv6 default route:

```plaintext
configure terminal
interface GigabitEthernet 0/1
ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1
```

configuring IPv6 Static Route
the following example shows how to configure an IPv6 static route:

```plaintext
configure terminal
interface GigabitEthernet 0/1
ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]
```

configuring IPv6 Access Lists
the following example shows how to configure an IPv6 access lists:

```plaintext
configure terminal
interface GigabitEthernet 0/1
ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D
ip access-group noncorp in
```

configuring the Neighbor Solicitation Message Interval
the following example shows how to configure the neighbor solicitation message interval:

```plaintext
configure terminal
interface GigabitEthernet 0/1
interface GigabitEthernet 0/1 ipv6 nd ns-interval 1500
```
Configuring the Neighbor Reachable Time

The following example shows how to configure the neighbor reachable time:

```
configure terminal
interface GigabitEthernet 0/1
ipv6 nd reachable-time 1000
```

Configuring the Router Advertisement Transmission Interval

The following example shows how to configure the router advertisement transmission interval:

```
configure terminal
interface GigabitEthernet 0/1
ipv6 nd ra-interval 1000
```

Configuring the Router Lifetime Value

The following example shows how to configure the router lifetime value:

```
configure terminal
interface GigabitEthernet 0/1
ipv6 nd ra-lifetime 5000
```

Configuring the IPv6 Prefix

The following example shows how to configure the IPv6 prefix:

```
configure terminal
interface GigabitEthernet 0/1
ipv6 nd prefix 2001:200:200::/35 1000 900
```

Suppressing Router Advertisement Messages

The following example shows how to suppress router advertisement messages:

```
configure terminal
interface GigabitEthernet 0/1
ipv6 nd suppress-ra
```

Configuring a Static IPv6 Neighbor

The following example shows how to configure a static IPv6 neighbor:

```
configure terminal
interface GigabitEthernet 0/1
ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

Verifying the IPv6 Configuration

Use the `show ipv6 interface` and `show ipv6 route` commands to display the various interfaces, multicast groups, protocol, and more for IPv6. This section contains examples of these commands and sample data.

IPv6 Interface Settings

To display the IPv6 interface settings, enter the following command:

```
Switch# show ipv6 interface [if_name]
```

Including the interface name, such as "outside", displays the settings for the specified interface. Excluding the name from the command displays the setting for all interfaces that have IPv6 enabled on them. The output for the command shows the following:
• The name and status of the interface.
• The link-local and global unicast addresses.
• The multicast groups the interface belongs to.
• ICMP redirect and error message settings.
• Neighbor discovery settings.

Switch# show ipv6 interface [if_name]

ipv6interface is down, line protocol is down
IPv6 is enabled, link-local address is fe80::20d:88ff:feee:6a82 [TENTATIVE]
No global unicast address is configured
Joined group address(es):
 ff02::1
 ff02::1:ffee:6a82
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds

Note: The show interface command displays only the IPv4 settings for an interface. To see the IPv6 configuration on an interface, use the show ipv6 interface command. The show ipv6 interface command does not display any IPv4 settings for the interface (if both are configured on the interface).

IPv6 Routes
To display the routes in the IPv6 routing table, use this command:

Switch# show ipv6 route

The output from the show ipv6 route command is similar to the IPv4 show route command. It displays the following information:

• The protocol that derived the route.
• The IPv6 prefix of the remote network.
• The administrative distance and metric for the route.
• The address of the next-hop router.
• The interface through which the next hop router to the specified network is reached.

Switch# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L fe80::/10 [0/0]
via ::, inside
L fec0::a:0:0:a0a:a70/128 [0/0]
via ::, inside
C fec0:0:0:a::/64 [0/0]
Additional References for IPv6

The following sections provide references related to the IPv6 feature.

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 addressing and connectivity</td>
<td>IPv6 Configuration Guide</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>IPv6 commands</td>
<td>Cisco IOS IPv6 Command Reference</td>
</tr>
<tr>
<td>Cisco IOS IPv6 features</td>
<td>Cisco IOS IPv6 Feature Mapping</td>
</tr>
<tr>
<td>RFCs for IPv6</td>
<td>IPv6 RFCs</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFCs for IPv6</td>
<td>IPv6 RFCs</td>
</tr>
</tbody>
</table>
# MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-CONFIG-COPY-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td>• CISCO-CONFIG-MAN-MIB</td>
<td><a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
<tr>
<td>• CISCO-DATA-COLLECTION-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-FLASH-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-SNMP-TARGET-EXT-MIB</td>
<td></td>
</tr>
<tr>
<td>• ENTITY-MIB</td>
<td></td>
</tr>
<tr>
<td>• IP-FORWARD-MIB</td>
<td></td>
</tr>
<tr>
<td>• IP-MIB</td>
<td></td>
</tr>
<tr>
<td>• NOTIFICATION-LOG-MIB</td>
<td></td>
</tr>
<tr>
<td>• SNMP-TARGET-MIB</td>
<td></td>
</tr>
</tbody>
</table>

CISCO-CONFIG-COPY-MIB and CISCO-FLASH-MIB support IPv6 addressing when TFTP, remote copy protocol (rcp), or FTP is used.

# RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported, and support for existing RFCs has not been modified.</td>
</tr>
<tr>
<td>—</td>
<td>—</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
SSH

This chapter describes SSH and procedures to configure SSH.

- SSH, page 431
- Prerequisites for SSH, page 432
- Restrictions for SSH, page 432
- Information About SSH, page 432
- How to Configure SSH, page 433
- Troubleshooting Tips, page 440
- Configuration Examples for SSH, page 441
- Verifying the SSH Configuration, page 441
- Additional References for SSH, page 443

SSH

Secure Shell (SSH) is an application; a protocol that provides secure replacement for the suite of Berkeley r-tools such as rsh, rlogin and rcp. (Cisco IOS supports the rlogin tool.) The protocol secures the sessions using standard cryptographic mechanisms. The application can be used in the same way as the Berkeley reexec and rsh tools.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see the Bug Toolkit and 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 the 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.
Prerequisites for SSH

- The Cisco IOS image used must be a k9 (crypto) image in order to support SSH. For example, me2600x-universalk9-mz.152-2.SA.fc5.tar.

- Ensure that you configure the IP on a Layer 3 interface, out-of-band on the management 0 interface or in-band on an Ethernet interface.

Restrictions for SSH

- SSH supports only the execution-shell application.

- The SSH server and the SSH client are supported only on DES (56-bit) and 3DES (168-bit) data encryption software.

Information About SSH

SSH is a protocol which provides a secure remote access connection to network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. Implement SSH version 2 when possible because it uses a more enhanced security encryption algorithm.

**SSH Server**

The SSH server feature enables a SSH client to make a secure, encrypted connection to a Cisco ME 2600X device. SSH uses strong encryption for authentication. The SSH server in the Cisco ME 2600X device will interoperate with publicly and commercially available SSH clients.

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, and the use of locally stored user names and passwords.

**SSH Client**

The SSH client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco ME 2600X device to make a secure, encrypted connection to another Cisco ME 2600X device or to any other device running the SSH server. This connection provides an outbound connection that is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco ME 2600X device works with publicly and commercially available SSH servers.

**SSH Server Keys**

SSH requires server keys for secure communications to the Cisco ME 2600X device. You can use SSH keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography

- SSH version 2 using the Digital System Algorithm (DSA)
Be sure to have an SSH server key-pair with the appropriate version before enabling the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts three types of key-pairs for use by SSH version 2:

- The `dsa` option generates the DSA key-pair for the SSH version 2 protocol.
- The `rsa` option generates the RSA key-pair for the SSH version 2 protocol.

By default, the Cisco ME 2600X device generates an RSA key using 1024 bits.

**Caution**
If you delete all the SSH keys, you cannot start the SSH services.

---

### How to Configure SSH

To configure SSH on the device, complete the following steps:

**Before You Begin**
Configure user authentication for local or remote access.

**SUMMARY STEPS**

1. Set up the device to run SSH.
2. Verify that SSH is enabled.
3. Export the RSA keys to the supervisor using RCP.
4. Replace the node as necessary.
5. Import the RSA keys stored on supervisor.
6. Verify that the crypto configurations have imported successfully.
7. Configure IPv6/IPv4 address and verify SSH (use another connected node).

**DETAILED STEPS**

**Step 1**
Set up the device to run SSH.
See [Setting Up Cisco ME 2600X to Run SSH](#), on page 434.

**Step 2**
Verify that SSH is enabled.
See [Verifying the SSH Configuration](#), on page 441.

**Step 3**
Export the RSA keys to the supervisor using RCP.
See [Exporting The RSA Keys to the Supervisor Using RCP](#), on page 436.

**Step 4**
Replace the node as necessary.
Use the `show crypto key mypubkey rsa` command to verify that the startup-configuration is restored and no crypto configurations are present.

**Step 5**
Import the RSA keys stored on supervisor.
See [Importing the RSA Keys Stored on the Supervisor](#), on page 437.
Step 6 Verify that the crypto configurations have imported successfully. See Verifying the SSH Configuration, on page 441.


Setting Up Cisco ME 2600X to Run SSH

To set up your device to run SSH, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ip address ip-address
5. no shutdown
6. exit
7. ip ssh version [1 | 2]
8. crypto key generate rsa [general-keys | usage-keys | signature | encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename :] [redundancy] [on devicename :]
9. username username
10. password password
11. aaa new-model

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# ipv6 address 2012:14/64 (for IPv6)</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# ip address 192.168.1.2 255.255.255.0 (for IPv4)</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>no shutdown</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# no shutdown</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# exit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ip ssh version [1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ip ssh version 2</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>crypto key generate rsa [general-keys</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# crypto key generate rsa exportable label sshkey modulus 1024</td>
</tr>
</tbody>
</table>

Generates Rivest, Shamir, and Adelman (RSA) key pairs.

- **general-keys**—(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
- **usage-keys**—(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
- **signature**—(Optional) Specifies that the RSA public key generated will be a signature special usage key.
- **encryption**—(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
- **label key-label**—(Optional) Specifies the name that is used for an RSA key pair when they are being exported.
- **exportable**—(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
- **modulus modulus-size**—(Optional) Specifies the IP size of the key modulus.

By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits.
Purpose

Command or Action | Purpose
--- | ---
**Note** Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size is expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits.

- **storage devicename:**—(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
- **redundancy:**—(Optional) Specifies that the key should be synchronized to the standby CA.
- **on devicename:**—(Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:).

Keys created on a USB token must be 2048 bits or less.

**Step 9**

*username username*

Example:

Switch(config)# username abc

Specifies the user name on your device.

**Step 10**

*password password*

Example:

Switch(config)# password xyz

Establishes a new password or change an existing password for the privileged command level.

**Step 11**

*aaa new-model*

Example:

Switch(config)# aaa new-model

Enables AAA.

---

**Exporting The RSA Keys to the Supervisor Using RCP**

To export RSA keys in privacy-enhanced mail (PEM)-formatted files, complete the following steps:

**SUMMARY STEPS**

1. *enable*
2. *configure terminal*
3. *crypto key export rsa key-label pem {terminal | url url} {3des | des} passphrase*
### 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.</td>
</tr>
<tr>
<td><em>Example:</em> Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto key export rsa key-label pem {terminal</td>
<td>url url} {3des</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# crypto key export rsa sshkey pem url flash: 3des sshkeysave % Key name: sshkey</td>
<td>The key-label argument must match the key pair name that was specified via the crypto key generate rsa command.</td>
</tr>
<tr>
<td>• terminal—RSA key pair will be displayed in PEM format on the console terminal.</td>
<td></td>
</tr>
<tr>
<td>• url url—URL of the file system where your router should export the RSA key pair.</td>
<td></td>
</tr>
<tr>
<td>• 3des—Export the RSA key pair using the Triple Data Encryption Standard (3DES) encryption algorithm.</td>
<td></td>
</tr>
<tr>
<td>• des—Export the RSA key pair using the DES encryption algorithm.</td>
<td></td>
</tr>
<tr>
<td>• passphrase—Passphrase that is used to encrypt the PEM file for import.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.</td>
<td></td>
</tr>
</tbody>
</table>

### Importing the RSA Keys Stored on the Supervisor

To import the RSA keys stored on the supervisor, complete the following steps:

#### SUMMARY STEPS

1. enable
2. configure terminal
3. crypto key import rsa key-label pem [usage-keys | signature | encryption | general-purpose] \{storage | terminal [passphrase] | url url\} [exportable] [on devicename:]
## 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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto key import rsa <strong>key-label</strong> pem [usage-keys</td>
<td>Imports RSA keys.</td>
</tr>
<tr>
<td>Example: Switch(config)# crypto key</td>
<td>signature</td>
</tr>
<tr>
<td>import rsa sshkey exportable</td>
<td>key-label—Name of the RSA key pair that is imported to the device.</td>
</tr>
<tr>
<td>url flash1: sshkeysave</td>
<td>The key-label argument must match the key pair name that was specified through the crypto key generate rsa command.</td>
</tr>
</tbody>
</table>

- **pem**—(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request. |
- **usage-keys**—(Optional) Specifies that two RSA special usage key pairs, one encryption pair and one signature pair, are imported. |
- **signature**—(Optional) Specifies that RSA signature keys are imported. |
- **encryption**—(Optional) Specifies that RSA encryption keys are imported. |
- **general-purpose**—(Optional) Specifies a General Purpose Key. |
- **storage**—Stores the key on the specified device. |
- **terminal**—Specifies the certificates and RSA key pairs are manually imported to the console terminal. |
- **passphrase**—Passphrase that is used to encrypt the PEM file for import. |

**Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. |

- **url url**—URL of the file system where your router should export the RSA key pair. |
- **exportable**—(Optional) Specifies that the imported RSA key pair can be exported to another Cisco device such as a router. |
- **on devicename:**—(Optional) Specifies that the imported RSA key pair is created on the specified device. Devices supported include local disks, NVRAM, and USB tokens. The name of the device is followed by a colon (:). |

Keys created on a USB token have a maximum size of 1024-bits.
If RSA keys are already present, you are prompted to either replace or retain the existing RSA keys. If you replace the existing RSA keys, the new keys are imported and a message displays confirming that the RSA key pair import succeeded.

**Configuring IPv6/IPv4 Addressing and Verifying SSH**

To configure IPv6/IPv4 address and verify SSH, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `hostname name`
4. `interface type slot/port`
5. `ip address ip-address`
6. `no shutdown`
7. `exit`
8. `ssh -l userid ip-address`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; <code>enable</code></td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>hostname name</code></td>
<td>Specifies or modifies the hostname for the network server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# <code>hostname Switch2</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>interface type slot/port</code></td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch2(config)# <code>interface GigabitEthernet 0/1</code></td>
</tr>
</tbody>
</table>
### Troubleshooting Tips

- If your SSH configuration commands are rejected as illegal commands, you have not successfully generated a RSA key pair for your router. Make sure you have specified a host name and domain. Then use the crypto key generate rsa command to generate an RSA key pair and enable the SSH server.

- When you configure the RSA key pair, you might encounter these error messages:

  1. **No hostname specified**

     You must configure a host name for the router using the `hostname` global configuration command.

  2. **No domain specified**

     You must configure a host domain for the router using the `ip domain-name` global configuration command.

- The number of allowable SSH connections is limited to the maximum number of vty's configured for the router. Each SSH connection uses a vty resource.

- SSH uses either local security or the security protocol that is configured through AAA on your router for user authentication. When you configure AAA, you must ensure that the console is not running under AAA by applying a keyword in the global configuration mode to disable AAA on the console.

- No SSH server connections running.
The above output displays when the SSH server is disabled or not enabled properly. If you have already configured SSH, it is recommended that you reconfigure the SSH server in the device.

**Configuration Examples for SSH**

**Configuring IPv6 Duplicate Address Detection**

The following example shows how to configure IPv6 duplicate address detection:

```
Switch # configure terminal
Switch(config) # interface GigabitEthernet 0/1
Switch(config-if) # ipv6 address 2001:db8::/64 eui64
Switch(config-if) # ipv6 nd reachable-time 10
```

**Verifying the SSH Configuration**

Use the `show crypto key mypubkey rsa` command to display the RSA public keys and `show ip ssh` command to display the version and configuration data for Secure Shell. This section contains example of these commands and sample data.

**Keys Settings**

Step 2 of Setting Up Cisco ME 2600X to Run SSH, on page 434—To display the RSA public keys, enter the following command:

```
Switch# show crypto key mypubkey rsa
```

% Key pair was generated at: 20:07:09 UTC Feb 28 1980
Key name: sshkey
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is exportable. Redundancy enabled.
Key Data:

30819F30 0D06092A 864886F7 0D010101 05003081 8D003081 8028181 0094EF56
210F4E82 9563D238 FE082B37 4F8C0772 632C24AA E885CB23 A97FB6B0 A7903930
782F39FD 495FC5AA 049EB807 F3AB76CA 22E7D837 9B469745 89241300 E2AA8D43
3D55F3DD 5D2E4871 7606242C A27E38D2 51ABD47F 9AD57152 F26B2B68 F9FF1BB9
1D6F531D 5544BC1B 5083B53B 14C0909D 42595376 DE061CA4 30A0AD51 77020301
0001
% Key pair was generated at: 20:07:10 UTC Feb 28 1980
Key name: sshkey.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable. Redundancy enabled.
Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00CB7A48 E905EFBC
ED765788 54D51A08 88A423E3 BD1ECED5 2DD5AA2C 4CAE079C 802EABB3 0EFB2535
Verifying the SSH Configuration

Step 2 of Setting Up Cisco ME 2600X to Run SSH, on page 434—To display the version and configuration data for Secure Shell, enter the following command:

```
Switch# show ip ssh
```

SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
  ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAgQCU71YhD06ClWPSOF4IKzdPjAdyYywquiFyyOpf7aw
      p5A5M4q0f1JX8wg8J64B/Oordsoi59g3m0aXRYkkEwDigo1DFvXz3V0uSHF2BiQson4401Gr1H+a1XFS
        8msmIPn/G7kd1MvVUS8G1CDtTsUwJCDq11Tdt4GHKQwo1Rdw==

Keys Settings

Step 6 of Setting Up Cisco ME 2600X to Run SSH, on page 434—To display the RSA public keys, enter the following command:

```
Switch# show crypto key mypubkey rsa
```

% Key pair was generated at: 20:14:18 UTC Feb 28 1980
Key name: sshkey
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 0094EF56
  210F4E82 9563D238 FE082B37 4F8C0772 632C24AA E885CB23 A97FB6B0 A7903930
  782F39FD 495FC5AA 049EB807 F3AB76CA 22E7D837 9B469745 89241300 E2AAAD43
  3D55F3DD 5D2E4871 7606242C A27E38D2 51ABD47F 9AD5715F 2F6B2688 F9FF1BB9
  1D6F531D 5544BC1B 5083B53B 14C0909D 42595376 DE061CA4 30A0AD51 77020301
  0001
% Key pair was generated at: 20:14:18 UTC Feb 28 1980
Key name: sshkey.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable. Redundancy enabled.
Key Data:
  307C3C0D 06092A86 4886F70D 01010105 0036B0 30680261 00A9C084 B0979B9B
  5E0FA8A6 D7DA98B3 14EE8E55 6FCFF4A4 50678A0A 1748D1C7 23994432 E68179EE
  E76D9F4A 614474D3 3E237EE2 197C8B55 F8064927 F6421317 357FF089 6B8A81A7
  85C5A67E AEBD8ABD 5152C608 73A3E91E 5B8745B2 30364394 C7020301 0001
## Additional References for SSH

The following sections provide references related to the IPv6 feature.

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</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>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-SECURE-SHELL-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported, and support for existing RFCs has not been modified.</td>
<td>—</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
This chapter describes Point-to-point protocol over Ethernet intermediate agent (PPPoE IA) and the configuration examples.

- PPPoE Intermediate Agent, page 445
- Prerequisites for PPPoE Intermediate Agent, page 446
- Restrictions for PPPoE Intermediate Agent, page 446
- Information About PPPoE Intermediate Agent, page 447
- How to Configure PPPoE Intermediate Agent, page 447
- Verifying the PPPoE IA Configuration, page 462
- Clearing Packet Counters, page 464
- Troubleshooting Tips, page 465
- Additional References for PPPoE Intermediate Agent, page 465

**PPPoE Intermediate Agent**

Point-to-point protocol over Ethernet intermediate agent (PPPoE IA) is placed between a subscriber and broadband remote access server (BRAS). PPPoE IA helps the service provider BRAS to distinguish between
end hosts connected over Ethernet and an access device. The topology of a typical PPPoE implementation is shown in the figure below.

*Figure 26: PPP in an Ethernet Scenario*

![Diagram of PPP in an Ethernet Scenario]

**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 Toolkit 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Prerequisites for PPPoE Intermediate Agent**

- Interface and Interface-EFP based PPPoE IA configurations take effect only when the PPPoE IA feature is enabled globally. Discovery packets are dropped if PPPoE IA is disabled globally.

- For EtherChannel, you must configure PPPoE IA on the port-channel interface. If a member port is removed from the EtherChannel, PPPoE IA configuration is also removed from the member port.

- PPPoE IA feature on Cisco ME 2600X supports global/per-port/per-EFP based format configuration for generating the circuit-id and remote-id. Choose the appropriate option to meet the requirements.

- To configure a large number of intermediate agent devices for PPPoE IA, use the `pppoe intermediate-agent` command for automatically generating subscriber-line information in the VSA tag by the feature.

**Restrictions for PPPoE Intermediate Agent**

- PPPoE IA is not supported on routed interfaces.
More than 6000 PPPoE sessions are not supported through the Cisco ME 2600X device acting as an intermediate agent.

Host connected ports configured as PPPoE IA trusted are not supported. Only BRAS connecting ports can be configured as trusted interfaces.

### Information About PPPoE Intermediate Agent

On the access switch, PPPoE IA enables subscriber line identification by appropriately tagging Ethernet frames of different users. The tag contains specific information such as, which subscriber is connected to the switch and ethernet flow point (EFP).

PPPoE IA acts as mini security firewall between host and BRAS by intercepting all PPPoE Active Discovery (PAD) messages on a per-port per-EFP basis. It provides specific security feature such as, verifying the intercepted PAD message from untrusted port, performing per-port PAD message rate limiting, inserting and removing VSA Tags into and from PAD messages respectively.

### How to Configure PPPoE Intermediate Agent

The following tasks describe how to configure PPPoE IA on the Cisco ME 2600X device:

- **Enabling or Disabling PPPoE IA on a Device**, on page 447
- **Configuring the Access Node Identifier for PPPoE IA**, on page 448
- **Configuring the Generic ErrorMessage for PPPoE IA**, on page 449
- **Configuring the Identifier String, Option, and Delimiter for PPPoE IA**, on page 450
- **Enabling or Disabling PPPoE IA on an Interface**, on page 452
- **Configuring PPPoE IA Circuit-ID on an Interface**, on page 453
- **Configuring PPPoE IA Remote-ID on an Interface**, on page 454
- **Configuring PPPoE IA Rate Limiting Setting on an Interface**, on page 455
- **Configuring the PPPoE IA Trust Setting on an Interface**, on page 456
- **Configuring PPPoE IA Vendor-tag Stripping on an Interface**, on page 457
- **Enabling or Disabling PPPoE IA on an EFP**, on page 459
- **Configuring PPPoE IA Circuit-ID on an EFP**, on page 460
- **Configuring PPPoE IA Remote-ID on an EFP**, on page 461

### Enabling or Disabling PPPoE IA on a Device

To enable or disable PPPoE IA globally on the device, complete the following steps:
### SUMMARY STEPS

1. enable
2. configure terminal
3. pppoe intermediate-agent
4. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>pppoe intermediate-agent</td>
<td>Enables PPPoE IA on the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# pppoe intermediate-agent</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

#### Configuring the Access Node Identifier for PPPoE IA

**Note**

If you do not specify the access node identifier of the switch, the value is automatically set as the IP address of the management interface.

### SUMMARY STEPS

1. enable
2. configure terminal
3. pppoe intermediate-agent format-type access-node-identifier string string_value
4. end
### 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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> pppoe intermediate-agent format-type access-node-identifier string string_value</td>
<td>Specifies the ASCII string value for the access node identifier.</td>
</tr>
<tr>
<td>Example: Switch(config)# pppoe intermediate-agent</td>
<td></td>
</tr>
<tr>
<td>format-type access-node-identifier string switch123</td>
<td>Note: To disable the access node identifier string for PPPoE IA, use the no pppoe intermediate-agent format-type access-node-identifier string command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

#### Configuring the Generic Error Message for PPPoE IA

**Note** PPPoE IA sends a generic error message only on a specific error condition. If you do not specify `string {message}`, the error message is not added.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. pppoe intermediate-agent format-type generic-error-message string `message`
4. end

#### 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.</td>
</tr>
</tbody>
</table>
### Enabling or Disabling PPPoE IA on a Device

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <strong>enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>pppoe intermediate-agent format-type</code></td>
<td>Specifies the ASCII string value for the</td>
</tr>
<tr>
<td><code>generic-error-message string</code> message</td>
<td>generic error message.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>By default the generic-error-message is</td>
</tr>
<tr>
<td>Switch(config)# <code>pppoe</code></td>
<td>not set. The string value is converted</td>
</tr>
<tr>
<td>intermediate-agent format-type</td>
<td>to UTF-8 before it is added to the</td>
</tr>
<tr>
<td><code>generic-error-message string</code> message</td>
<td>response. A message similar to the</td>
</tr>
<tr>
<td>packet_length&gt;1484</td>
<td>following displays:</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>PPPoE Discover packet too large to</td>
</tr>
<tr>
<td></td>
<td>process. Try reducing the number of</td>
</tr>
<tr>
<td></td>
<td>tags added.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This TAG (0x0203 Generic-Error) indicates</td>
</tr>
<tr>
<td></td>
<td>an error. It can be added to PPPoE Active</td>
</tr>
<tr>
<td></td>
<td>Discovery Offer (PADO) or PPPoE Active</td>
</tr>
<tr>
<td></td>
<td>Discovery Session-confirmation (PADS)</td>
</tr>
<tr>
<td></td>
<td>packets generated by PPPoE IA. The tag can</td>
</tr>
<tr>
<td></td>
<td>then be sent back to the user in response</td>
</tr>
<tr>
<td></td>
<td>to PPPoE Active Discovery Initiation (PADI)</td>
</tr>
<tr>
<td></td>
<td>or PPPoE active discovery request (PADR),</td>
</tr>
<tr>
<td></td>
<td>when a PPPoE discovery packet received by</td>
</tr>
<tr>
<td></td>
<td>PPPoE IA with PPPoE payload is greater than</td>
</tr>
<tr>
<td></td>
<td>1484 bytes. Error data must be a UTF-8</td>
</tr>
<tr>
<td></td>
<td>string.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To disable the generic error message on the</td>
</tr>
<tr>
<td></td>
<td>device, use the <code>no pppoe</code></td>
</tr>
<tr>
<td></td>
<td>`intermediate-agent format-type generic-</td>
</tr>
<tr>
<td></td>
<td>error-message string` command.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Identifier String, Option, and Delimiter for PPPoE IA

- **Note**: By default, the circuit-ID is automatically generated by the device.
SUMMARY STEPS

1. enable
2. configure terminal
3. pppoe intermediate-agent format-type identifier-string string string_value option sp | sv | pv | spv delimiter type
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable           | Enables privileged EXEC mode.  
|      | Example:         | • Enter your password if prompted. |
|      | Switch> enable   |         |
| 2    | configure terminal | Enters global configuration mode. |
|      | Example:         |         |
|      | Switch# configure terminal |         |
| 3    | pppoe intermediate-agent format-type identifier-string string string_value option sp | sv | pv | spv delimiter type | Specifies the ASCII string value for the circuit-ID. |
|      | Example:         | Specify an option value: |
|      | Switch(config)# pppoe intermediate-agent format-type identifier-string string circuit1 option spv delimiter : | • sp—slot + port |
|      |                  | • sv—slot + BD-VLAN |
|      |                  | • pv—port + BD-VLAN |
|      |                  | • spv—slot + port + BD-VLAN |
|      |                  | Specify the delimiter between slot/port/BD-VLAN. |
|      |                  | Values for delimiter include: #,|,|,|,|,|,|,|,|,|,|,|,|,space.| |
|      |                  | This command does not affect the circuit-ID configured explicitly per-interface or per-interface per-EFP with the pppoe intermediate-agent format-type circuit-id or pppoe intermediate-agent vlan num format-type circuit-id commands. |
|      |                  | **Note** To revert back to default automatic generation of circuit-ID, use the *no pppoe intermediate-agent format-type identifier-string* command without WORD, options, and delimiters. |
| 4    | end              | Returns to privileged EXEC mode. |
|      | Example:         |         |
|      | Switch(config)# end |         |
Enabling or Disabling PPPoE IA on an Interface

**Note**

This setting applies to all frames passing through this interface, regardless of the EFP to which they belong. By default the PPPoE IA feature is disabled on all interfaces. You need to run this command on every interface that requires this feature.

**Before You Begin**

You must enable PPPoE IA on the device in the global configuration mode. See Enabling or Disabling PPPoE IA on a Device, on page 447.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. pppoe intermediate-agent
5. end

**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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 1/1</td>
<td>- type—Type of interface to be configured</td>
</tr>
<tr>
<td></td>
<td>- slot—Chassis slot number</td>
</tr>
<tr>
<td></td>
<td>- /port—Port or interface number</td>
</tr>
<tr>
<td><strong>Step 4</strong> pppoe intermediate-agent</td>
<td>Enables PPPoE IA on the interface.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# pppoe intermediate-agent</td>
<td><strong>Note</strong> Enabling PPPoE IA on an interface does not ensure that incoming packets are tagged. For this to happen PPPoE IA must be enabled globally, and at least one interface that connects the device to PPPoE server has a trusted PPPoE IA setting.</td>
</tr>
</tbody>
</table>
### Configuring PPPoE IA Circuit-ID on an Interface

You can configure the circuit-ID on a physical interface. The PADI, PADR, and PADT packets (belonging to PPPoE discovery stage) that are received on this physical interface are tagged with either one of these IDs. These packets are tagged regardless of their VLAN if PPPoE is not enabled for that VLAN.

Set the circuit-ID on an interface to override the automatic generation of the circuit-ID by the switch.

To configure the circuit-ID on an interface, complete the following steps:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `pppoe intermediate-agent format-type circuit-id string circuit_id_name`
5. `end`

#### 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.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 1/1</td>
<td></td>
</tr>
</tbody>
</table>

**Note**: To disable the PPPoE IA feature on the interface, use the `no pppoe intermediate-agent` command.
### Enabling or Disabling PPPoE IA on an Interface

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4** | **pppoe intermediate-agent format-type circuit-id string circuit_id_name**  
Example:  
Switch(config-if)# pppoe intermediate-agent format-type circuit-id string root  
| Configure the circuit-ID. This command overrides the automatic generation of *circuit-id* by the device.  
**Note** To disable the circuit-ID on an interface, use the **no pppoe intermediate-agent format-type circuit-id string root** command. |
| **Step 5** | **end**  
Example:  
Switch(config-if)# end  
| Returns to privileged EXEC mode. |

### Configuring PPPoE IA Remote-ID on an Interface

You can configure the remote-ID on a physical interface. The PADI, PADR, and PADT packets (belonging to PPPoE discovery stage) that are received on this physical interface are tagged with either one of these IDs. These packets are tagged regardless of their VLAN if PPPoE is not enabled for that VLAN.

Set the remote-ID for subscriber link identification. Configure the remote-ID on every interface in which you enabled PPPoE IA. Otherwise, the default value for remote-ID is the switch MAC address.

To configure the remote-ID on an interface, complete the following steps:

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. interface type slot/port  
4. pppoe intermediate-agent format-type remote-id string *remote_id_name*  
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable**  
Example:  
Switch> enable  
| Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2** | **configure terminal**  
Example:  
Switch# configure terminal  
| Enters global configuration mode. |
**Purpose**

Command or Action: `interface type slot/port`

Purpose: Specifies the interface to configure and enters interface configuration mode.

**Step 3**

Example:

```
Switch(config)# interface GigabitEthernet 1/1
```

**Step 4**

Command or Action: `pppoe intermediate-agent format-type remote-id string remote_id_name`

Purpose: Configures the remote-ID. This command overrides the automatic generation of `circuit-id` by the device.

**Note**

To disable the remote-ID on an interface, use the `no pppoe intermediate-agent format-type remote-id string` command.

Example:

```
Switch(config-if)# pppoe intermediate-agent format-type remote-id string granite
```

**Step 5**

Command or Action: `end`

Purpose: Returns to privileged EXEC mode.

Example:

```
Switch(config-if)# end
```

---

### Configuring PPPoE IA Rate Limiting Setting on an Interface

You can limit the rate (packets per second) at which PPPoE discovery packets (PADI, PADO, PADR, PADS, and PADT) are received on an interface. When the incoming packet rate achieves or exceeds the configured limit, a port enters an error-disabled state and shuts down.

**Note**

This limit applies to the physical interface to counter misbehaving hosts. Even if a single EFP misbehaves on an interface in trunk mode, the entire interface is shut down (error-disabled), bringing down other EFP traffic on the interface.

If you set the limit on the interface that connect the access switch to BRAS, use a higher value since the BRAS aggregates all the PPPoE traffic to the access switch through this interface.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `pppoe intermediate-agent limit rate packets-per-second`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Command or Action

**Example:**

Switch> enable

- **Step 2**
  - **configure terminal**
  
  **Example:**
  
  Switch# configure terminal

- **Step 3**
  - **interface type slot/port**
  
  **Example:**
  
  Switch(config)# interface GigabitEthernet 1/1

- **Step 4**
  - **pppoe intermediate-agent limit rate packets-per-second**
  
  **Example:**
  
  Switch(config-if)# pppoe intermediate-agent limit rate 30

- **Step 5**
  - **end**

**Note**

To disable rate limit on an interface, use the `no pppoe intermediate-agent limit rate` command.

### Configuring the PPPoE IA Trust Setting on an Interface

Interfaces that connect the device to the PPPoE server are configured as trusted. Interfaces that connect the device to users (PPPoE clients) are untrusted.

This setting is disabled by default.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. pppoe intermediate-agent
5. pppoe intermediate-agent trust
6. end
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
enable | Enables privileged EXEC mode.  
- Example:  
Switch> enable |
| **Step 2**  
configure terminal | Enters global configuration mode.  
- Example:  
Switch# configure terminal |
| **Step 3**  
interface type slot/port | Specifies the interface to configure and enters interface configuration mode.  
- Example:  
Switch(config)# interface GigabitEthernet 1/1  
- type—Type of interface to be configured  
- slot—Chassis slot number  
- /port—Port or interface number |
| **Step 4**  
pppoe intermediate-agent | Enables PPPoE IA for an EFP on the interface.  
- Example:  
Switch(config-if)# pppoe intermediate-agent  
- Note For pppoe intermediate-agent command to take effect, it is not required to enable PPPoE IA on the interface.  
- Note To disable the PPPoE IA feature for an EFP on the interface, use the no pppoe intermediate-agent command. |
| **Step 5**  
pppoe intermediate-agent trust | Sets the interface as trusted.  
- Example:  
Switch(config-if)# pppoe intermediate-agent trust  
- Note To disable a physical interface as trusted, use the no pppoe intermediate-agent trust command. |
| **Step 6**  
end | Returns to privileged EXEC mode.  
- Example:  
Switch(config-if)# end |

---

### Configuring PPPoE IA Vendor-tag Stripping on an Interface

Vendor-specific tags (VSAs) carry subscriber and line identification information in the packets. Vendor-tag stripping involves removing the VSAs from PADO, PADS, and PADT packets that are received on an interface before forwarding them to the user.

You can configure vendor-tag stripping on interfaces connected to the PPPoE server. This setting is disabled by default.
BRAS automatically strips the vendor-specific tag off of the PPPoE discovery packets before sending them downstream to the access switch. To operate with older BRAS which does not possess this capability, use the `pppoe intermediate-agent vendor-tag strip` command on the interface connecting the access switch to BRAS.

To enable stripping on an interface, complete the following steps:

**Before You Begin**

1. Enable PPPoE on an interface. See Enabling or Disabling PPPoE IA on an Interface, on page 452.
2. Set the PPPoE interface to trust. See Configuring the PPPoE IA Trust Setting on an Interface, on page 456.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `pppoe intermediate-agent vendor-tag strip`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt;</code> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface type slot/port</code></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# interface GigabitEthernet 1/1</code></td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>pppoe intermediate-agent vendor-tag strip</code></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config-if)# pppoe intermediate-agent vendor-tag strip</code></td>
<td>Enables vendor tag stripping on the trusted interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To disable the stripping on an interface, use the <code>no pppoe intermediate-agent vendor-tag strip</code> command.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Enabling or Disabling PPPoE IA on an EFP

To enable or disable PPPoE IA on an EFP, complete the following steps:

**Before You Begin**

You must enable PPPoE IA on the device in the global configuration mode. See Enabling or Disabling PPPoE IA on a Device, on page 447.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. service instance id ethernet
5. pppoe intermediate-agent
6. end

**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.</td>
</tr>
<tr>
<td><em>Example:</em> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# interface GigabitEthernet 1/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> pppoe intermediate-agent</td>
<td>Enables PPPoE IA for an EFP on the interface.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config-if-srv)# pppoe intermediate-agent</td>
<td><strong>Note</strong> For <code>pppoe intermediate-agent</code> command to take effect, it is not required to enable PPPoE IA on the interface.</td>
</tr>
</tbody>
</table>
To disable the PPPoE IA feature for an EFP on the interface, use the `no pppoe intermediate-agent` command.

Note

Returns to privileged EXEC mode.

Example:

Switch(config-if-srv)# end

Configuring PPPoE IA Circuit-ID on an EFP

To configure the circuit-ID on an EFP, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. service instance id ethernet
5. pppoe intermediate-agent format-type circuit-id string circuit_id_name
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface GigabitEthernet 1/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 service instance id ethernet</td>
<td>Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# service instance 1 ethernet</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring PPPoE IA Remote-ID on an EFP

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** type slot/port
4. **service instance** id ethernet
5. **pppoe intermediate-agent format-type remote-id string** remote_id_name
6. **end**

**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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** Switch(config)# interface GigabitEthernet 1/1 | • type—Type of interface to be configured  
• slot—Chassis slot number |
### Purpose

Command or Action | Purpose
--- | ---
• /port — Port or interface number

#### Step 4

**service instance id ethernet**

**Example:**

Switch(config-if)# service instance 1 ethernet

Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

#### Step 5

**pppoe intermediate-agent format-type remote-id string**

**Example:**

Switch(config-if-srv)# pppoe intermediate-agent format-type remote-id string root

Sets the remote-id for an EFP on this interface.

**Note**

The `pppoe intermediate-agent format-type remote-id string` command overrides the remote-id specified for the interface and the device uses the value of the remote-id string to tag packets received on this EFP.

**Note**

The default value of `remote-id` is the device MAC address (for all vlans). To encode subscriber specific information, it is strongly recommended that you set this parameter.

**Note**

To disable the remote-ID on an EFP, use the `no pppoe intermediate-agent format-type remote-id string` command.

#### Step 6

**end**

**Example:**

Switch(config-if-srv)# end

Returns to privileged EXEC mode.

---

**Verifying the PPPoE IA Configuration**

Use the `show pppoe intermediate-agent [info | statistics] [interface {interface}]` command to display the various configuration parameters, statistics, and counters stored for PPPoE. This section contains examples of this command and sample data.

**PPPoE IA Information for All Interfaces**

Use the following command to show the interfaces and VLANs on which PPPoE is configured:

`Switch# show pppoe intermediate-agent information`

<table>
<thead>
<tr>
<th>Interface IA</th>
<th>Trusted Vsa Strip</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/33</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
PPPoE Intermediate-Agent is configured on following bridge domains: 40,50

**PPPoE Information for an Interface**

Use the following command to show PPPoE information for a specified interface:

```
Switch# show pppoe intermediate-agent information interface GigabitEthernet 0/10
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>IA</th>
<th>Trusted</th>
<th>Vsa</th>
<th>Strip</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/33</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>unlimited</td>
<td></td>
</tr>
</tbody>
</table>

PPPoE Intermediate-Agent is configured on following bridge domains: 40,50

**Statistics-All Interfaces**

Use the following command to show the number of PADI/PADR/PADT packets received, and the time the last packet was received on all interfaces and on all VLANs pertaining to those interfaces:

```
Switch# show pppoe intermediate-agent statistics
```

PPPOE IA Per-Port Statistics

```
Interface : GigabitEthernet0/33
Packets received
All = 53
PADI = 17 PADO = 0
PADR = 17 PADS = 0
PADT = 19
Packets dropped:
Rate-limit exceeded = 0
Server responses from untrusted ports = 0
Client requests towards untrusted ports = 0
Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 8 PADO = 0 PADR = 8 PADS = 0 PADT = 9
BD 50: Packets received PADI = 9 PADO = 0 PADR = 9 PADS = 0 PADT = 10
```

**Statistics-Specific Interface**

Use the following command to show statistics for a specified interface:

```
Switch# show pppoe intermediate-agent statistics interface GigabitEthernet 0/10
```

```
Interface : Gi 0/10
Packets received
All = 3
PADI = 0 PADO = 0
PADR = 0 PADS = 0
PADT = 3
Packets dropped:
Rate-limit exceeded = 0
Server responses from untrusted ports = 0
Client requests towards untrusted ports = 0
Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 6 PADO = 0 PADR = 6 PADS = 0 PADT = 6
BD 50: Packets received PADI = 4 PADO = 0 PADR = 4 PADS = 0 PADT = 4
```
Clearing Packet Counters

Use the following command to clear packet counters for all PPPoE discovery packets (PADI, PADO, PADR, PADS, PADT) on all interfaces (per-port and per-port-per-EFP):

Switch# clear pppoe intermediate-agent statistics

Use the following command to view the statistics of all the interfaces on which PPPoEIA is enabled:

Switch# show pppoe intermediate-agent statistics

PPPoE IA Per-Port Statistics

<table>
<thead>
<tr>
<th>Interface</th>
<th>GigabitEthernet0/33</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets received</td>
<td></td>
</tr>
<tr>
<td>All = 53</td>
<td></td>
</tr>
<tr>
<td>PADI = 17</td>
<td>PADO = 0</td>
</tr>
<tr>
<td>PADR = 17</td>
<td>PADS = 0</td>
</tr>
<tr>
<td>PADT = 19</td>
<td></td>
</tr>
<tr>
<td>Packets dropped:</td>
<td></td>
</tr>
<tr>
<td>Rate-limit exceeded = 0</td>
<td></td>
</tr>
<tr>
<td>Server responses from untrusted ports = 0</td>
<td></td>
</tr>
<tr>
<td>Client requests towards untrusted ports = 0</td>
<td></td>
</tr>
<tr>
<td>Malformed PPPoE Discovery packets = 0</td>
<td></td>
</tr>
<tr>
<td>BD 40: Packets received</td>
<td>PADI = 8 PADO = 0 PADR = 8 PADS = 0 PADT = 9</td>
</tr>
<tr>
<td>BD 50: Packets received</td>
<td>PADI = 9 PADO = 0 PADR = 9 PADS = 0 PADT = 10</td>
</tr>
</tbody>
</table>

Interface : GigabitEthernet0/34

Packets received

| All = 59 |
| PADI = 0 PADO = 19 |
| PADR = 0 PADS = 26 |
| PADT = 14 |

Packets dropped:

| Rate-limit exceeded = 0 |
| Server responses from untrusted ports = 0 |
| Client requests towards untrusted ports = 0 |
| Malformed PPPoE Discovery packets = 0 |
| BD 40: Packets received | PADI = 0 PADO = 12 PADR = 0 PADS = 15 PADT = 7 |
| BD 50: Packets received | PADI = 0 PADO = 7 PADR = 0 PADS = 11 PADT = 7 |

Use the following command to clear packet counters on a selected interface:

Switch# clear pppoe intermediate-agent statistics interface type port/slot

Example:

Switch# clear pppoe intermediate-agent statistics interface gigabitEthernet 0/3

Use the following command to view the packet details on an interface:

Switch# show pppoe intermediate-agent statistics interface type port/slot

Example:

Switch# show pppoe intermediate-agent statistics interface gigabitEthernet 0/3

Interface : Gi 0/3

Packets received

| All = 0 |
| PADI = 0 PADO = 0 |
| PADR = 0 PADS = 0 |
| PADT = 0 |
Troubleshooting Tips

The following debug commands can help you troubleshoot an improper PPPoE intermediate agent configuration and its related features:

- **debug pppoe intermediate-agent packet**—Displays the contents of a packet received in the software: source and destination MAC address of Ethernet frame, code, version and type of PPPoE Discovery packet and a list of TAGs present.

- **debug pppoe intermediate-agent event**—Provides debugging information about PPPoE events.

- **debug radius**—Generates a report that includes information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

Additional References for PPPoE Intermediate Agent

The following sections provide references related to the PPPoE IA feature.

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported, and support for existing RFCs has not been modified.</td>
<td>—</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
CFM over EVC

This chapter describes CFM and procedures to configure CFM.

- CFM over EVC, page 467
- Restrictions for CFM, page 468
- Information About CFM, page 468
- How to Configure CFM, page 474
- Configuration Examples for CFM, page 490
- Verifying the CFM Configuration, page 493
- Additional References for CFM, page 499

CFM over EVC

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

Cisco ME 2600X supports the IEEE 802.1ag standard implementation of CFM. It supports CFM over the following:

- Point–to–multipoint bridge domain associated with Ethernet Flow Points (EFP)
- Port Maintenance End Point (MEP)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see the Bug Toolkit and 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 the 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.
Restrictions for CFM

- CFM over the point-to-point bridge domain is not supported.
- CFM over Virtual Private LAN Service (VPLS) is not supported.
- Depending on the Continuity Check (CC) interval, more than 16000 Maintenance End Points (MEPs) are not supported.
- More than 16000 Maintenance Intermediate Points (MIPs) are not supported.
- CFM alarms is not supported.
- CFM over VLAN based forwarding is not supported.
- CFM is not supported on a bridge domain that has the split horizon configured.
- CFM handles blocked ports only for tagged packets as REP operates only on tagged packets.

The following table specifies the number of supported remote and local MEPs depending on the configured CC interval.

<table>
<thead>
<tr>
<th>CC Interval</th>
<th>Number of Remote MEPs</th>
<th>Number of Local MEPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 milliseconds</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>1 second</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>10 seconds</td>
<td>8000</td>
<td>8000</td>
</tr>
<tr>
<td>1 minute</td>
<td>16000</td>
<td>16000</td>
</tr>
<tr>
<td>10 minutes</td>
<td>16000</td>
<td>16000</td>
</tr>
</tbody>
</table>

Information About CFM

IEEE CFM is an end-to-end per-service Ethernet layer OAM protocol that supports provider edge-to-provider edge (PE-to-PE) and customer edge-to-customer edge (CE-to-CE) services. A service is identified as an Ethernet virtual circuit (EVC) service.

Benefits of IEEE CFM

- End-to-end service-level OAM technology.
- Reduced operating expense for service provider Ethernet networks.
- Competitive advantage for service providers.
- Support for both distribution and access network environments with Down (toward the wire) MEPs.
**Maintenance Domain**

A maintenance domain is an administrative domain for managing and administering a network. The maintenance domain allows CFM to support multiple independent operators, each supporting service instances from multiple independent customers.

A unique maintenance level in the range of 0 to 7 is assigned to each maintenance domain by a network administrator. Maintenance levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallels the structure of customer, service provider, and operator. The higher the domain level, the broader the scope of the domain. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators would have the smallest domains and customers the largest domains, with service provider domains in between these domains, varying in size. All levels of the hierarchy must operate together.

Domains must not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch but when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Nesting maintenance domains is useful in the business model where a service provider contracts with one or more operators to provide Ethernet service to a customer.

Each operator would have its own maintenance domain and the service provider would define its domain that is a superset of the operator domains. Furthermore, the customer has its own end-to-end domain, which is in turn a superset of the service provider domain. Maintenance levels of various nesting domains must be communicated among the administering organizations. For example, one approach would be to have the service provider assign maintenance levels to operators.

The following characteristics of maintenance domains are supported:

- Maintenance domains are identified by a unique domain name that can be up to 154 characters.
- The domain name as null is supported; the maintenance association name is used as the identifier.
- Domain configuration is not required for devices that have only Maintenance Intermediate Points (MIPs).
- Mix of Up (toward the bridge) and Down (toward the wire) Maintenance Association End Points (MEPs) is supported.

A domain can be removed when all the maintenance points within the domain have been removed and all the remote MEPs entries in the continuity check database (CCDB) for the domain have been purged.

The following figure illustrates a hierarchy of operator, service provider, and customer domains and also illustrates touching, intersecting, and nested domains.
Maintenance Association

There can be any number of maintenance associations (MA) within a maintenance domain. A maintenance association identifies a service that can be uniquely identified within the maintenance domains. The CFM protocol runs within a specific maintenance association.

The MA direction is specified when the MA is configured. The MA name must be configured on a domain before MEPs can be configured. Configuring an MA is not required for devices that have only MIPs.

Maintenance Point

Any port of a bridge is referred to as a Maintenance Point. A maintenance point is a demarcation point on an interface or port that participates in CFM within a maintenance domain. Maintenance points must be explicitly configured on Cisco devices.

There are two classes of maintenance points:

- Maintenance End Points (MEPs)
- Maintenance Intermediate Points (MIPs)
Maintenance End Points

MEPs reside at the edge of a maintenance domain and are active elements of CFM. They confine CFM messages within the domain through the maintenance domain level. MEPs periodically transmit and receive continuity check messages (CCMs) from other MEPs within the domain. MEPs also transmit linktrace and loopback messages at the request of the administrator.

MEP ID uniquely identifies each MEP along with those configured on a single MA. The MEP IDs range from 1 to 8191.

There are two types of MEPs:

- Up (inwards, toward the bridge). This is the default.
- Down (outwards, toward the wire).

MEP supports multicast loopbacks and pings. When a multicast ping is initiated for a particular domain or service, all the related remote MEPs reply to the ping.

 MEP configurations can be removed after all pending loopback and linktrace replies are removed and the service on the interface is set to transparent mode. To set the service to transparent mode, MIP filtering must not be configured.

Up MEPs

An Up MEP is an MEP that resides in a bridge and transmits to and receives CFM messages from the direction of the bridge relay entity.

An Up MEP performs the following functions:

- Sends and receives CFM frames at its level through the bridge relay and not through the wire connected to the port on which the MEP is configured.
- Drops all CFM frames at its level (or lower level) that come from the direction of the wire.
- Processes all CFM frames at its level coming from the direction of the bridge.
- Drops all CFM frames at a lower level coming from the direction of the bridge.
- Forwards all CFM frames transparently at a higher level, independent of whether they came in from the bridge or wire.

Down MEPs

A Down MEP is an MEP that resides in a bridge and transmits to and receives CFM messages from the direction of the wire.

A Down MEP performs the following functions:

- Sends and receives CFM frames at its level through the wire connected to the port where the MEP is configured.
- Drops all CFM frames at its level (or at a lower level) that come from the direction of the bridge.
- Processes all CFM frames at its level coming from the direction of the wire.
- Drops all CFM frames at a lower level coming from the direction of the wire.
• Forwards all CFM frames transparently at a higher level, independent of whether they came in from the bridge or wire.

Port MEPs
Cisco ME 2600X also supports Port MEP at the physical port. A port MEP can be created either on the physical port or on the port of a channel group. The port MEP takes higher precedence if both the port MEP and the Down MEP on untagged EFP is created on the same port.

Maintenance Intermediate Points
Maintenance intermediate points (MIPs) are internal to the maintenance domain and are passive elements of CFM. They store information received from MEPs and other MIPs and respond only to CFM linktrace and loopback messages. An MIP has only one level associated with it. MIPs forward CFM messages within a maintenance domain.

MIPs are defined as two MIP half functions (MHFs)—an Up MHF that resides above the port filtering entities and a Down MHF that resides below the port filtering entities. The same configuration parameters and characteristics apply to both MHFs of an MIP:

• Can be created manually or dynamically (auto MIPs).
• Dynamically created depending on configured policies at managed objects (MA, maintenance domain, or the default domain level).
• Manual MIPs can be created under a service instance within an interface.
• Auto MIP commands can be issued globally or under a domain or service.
• Can be created per MA, which means that an MIP in the MA can be lower level than an MEP in another MA.
• CFM frames received from MEPs and other MIPs are cataloged and forwarded, using both the wire and the bridge relay.
• When MIP filtering is enabled, all CFM frames at a lower level are stopped and dropped, independent of whether they originate from the wire or the bridge relay.
• All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or from the bridge relay.
• Passive points respond only when triggered by CFM linktrace and loopback messages.

The following figure illustrates MEPs and MIPs at the operator, service provider, and customer levels.
CFM Messages

CFM uses standard Ethernet frames that can be distinguished by their EtherType and for multicast messages by their MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to a maintenance association. Three types of messages are supported:

- Continuity Check
- Linktrace
- Loopback

Continuity Check Messages

CFM continuity check messages (CCMs) are multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a domain.

CFM CCMs have the following characteristics:

- Transmitted at a periodic interval by MEPs. The interval can be one of the following configurable values. The default is 10 seconds.
  - 100 milliseconds
  - 1 second
  - 10 seconds
  - 1 minute
  - 10 minutes
- Cataloged by MIPs at the same maintenance level.
- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
• Indicate the status of the bridge port on which the MEP is configured.

**Loopback Messages**

CFM loopback messages (LBMs) are unicast frames that an MEP transmits, at the request of an administrator, to verify connectivity to a specific maintenance point. A loopback message reply (LBR) indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.

Since LBMs are unicast messages, they are forwarded like normal data frames except with the maintenance level restriction. If the outgoing port is known in the forwarding database of the bridge and allows CFM frames at the maintenance level of the image to pass through, the frame is sent out on that port. If the outgoing port is unknown, the message is broadcast on all the ports in that domain.

A CFM LBM can be generated on demand using the CLI. The source of a loopback message must be an MEP; the destination may be an MEP or MIP. Both CFM LBMs and LBRs are unicast. CFM LBMs specify the destination MAC address or MPID, VLAN, and maintenance domain.

**Linktrace Messages**

CFM linktrace messages (LTMs) are multicast frames that an MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They are similar to Layer 3 traceroute messages. LTMs allow the transmitting node to discover vital connectivity data about the path and allow the discovery of all MIPs along the path that belong to the same maintenance domain. LTMs are intercepted by maintenance points along the path and processed, transmitted, or dropped. At each hop where there is a maintenance point at the same level, a linktrace message reply (LTR) is transmitted back to the originating MEP. For each visible MIP, linktrace messages indicate ingress action, relay action, and egress action. LTMs are multicast and LTRs are unicast.

**How to Configure CFM**

The following tasks describe how to configure CFM on the Cisco ME 2600X device:

• [Configuring IPv6 on an Interface](#), on page 409

**Enabling or Disabling CFM Globally**

To enable or disable CFM globally, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ethernet cfm global`
4. `end`
Enabling or Disabling CFM on an Interface

To enable or disable CFM on an interface, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type
4. ethernet cfm interface
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet cfm global</td>
<td>Enables Ethernet CFM globally on the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ethernet cfm global</td>
<td></td>
</tr>
</tbody>
</table>

**Note** To disable CFM globally on the device, use the no ethernet cfm global command.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
---|---
**Step 2**  
configure terminal  
**Example:**
Switch# configure terminal | Enters global configuration mode.

**Step 3**  
interface type  
**Example:**
Switch(config)# interface GigabitEthernet 1/1 | Enters global configuration mode.

**Step 4**  
ethernet cfm interface  
**Example:**
Switch(config-if)# ethernet cfm interface | Enables the Ethernet CFM processing on the interface.  
**Note** To disable Ethernet CFM processing on the interface, use the `no ethernet cfm interface` command.

**Step 5**  
end  
**Example:**
Switch(config-if)# end | Returns to privileged EXEC mode.

---

### Enabling Caching of CFM Data

To enable caching of CFM data, complete the following steps:

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. ethernet cfm traceroute cache  
4. ethernet cfm traceroute cache size entries  
5. ethernet cfm traceroute cache hold-time minutes  
6. end

**DETAILED STEPS**

| Command or Action | Purpose |
---|---|
**Step 1**  
enable  
**Example:**
Switch> enable | Enables privileged EXEC mode.  
* Enter your password if prompted.
### Creating a Maintenance Domain

To create a maintenance domain, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ethernet cfm domain domain-name level level-id`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch&gt; enable</code></td>
</tr>
</tbody>
</table>
Creating a Maintenance Association

To create a maintenance association, complete the following steps:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ethernet cfm domain domain-name level level-id`
4. `service {ma-name | number ma-name} {evc evc-name | port} [ direction down]`
5. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>ethernet cfm domain domain-name level level-id</code></td>
<td>Creates a CFM maintenance domain at a specific maintenance level and enters Ethernet CFM configuration mode. The range of the maintenance domain level is from 0 to 7.</td>
</tr>
<tr>
<td>`service {ma-name</td>
<td>number ma-name} {evc evc-name</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
## Configuring CFM Encapsulation

To configure CFM encapsulation, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type`
4. `service instance id ethernet [evc-id]`
5. `encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]} second-dot1q {any | vlan-id [vlan-id [-vlan-id]]}
6. `bridge-domain bridge-id [split-horizon]`
7. `cfm encapsulation dot1q {dot1ad vlan-id | dot1q vlan-id} [dot1q vlan-id | second-dot1q vlan-id]`
8. `end`

**DETAILED STEPS**

<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>Example:</td>
<td><code>Switch&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Creating a Port MEP

To create a port MEP, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type
4. ethernet cfm mep domain domain-name mpid mpid {port}
5. end
DETAILED STEPS

<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><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface GigabitEthernet 1/1</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ethernet cfm mep domain domain-name mpid mpid</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# ethernet cfm mep domain Customer mpid 701 port</td>
</tr>
<tr>
<td>Sets a port as internal to a maintenance domain and creates a port MEP. A port MEP can be created only on a physical port or on a port of a channel group.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

Creating an MEP for an EFP

To create an MEP for an EFP, complete the following steps:

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type
4. service instance id ethernet [evc-id]
5. encapsulation dot1q {any | vlan-id [vlan-id [-vlan-id]]} second-dot1q {any | vlan-id [vlan-id [-vlan-id]]}
6. bridge-domain bridge-id [split-horizon]
7. cfm mep domain domain-name mpid mpid-value
8. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `enable`          | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| 2    | `configure terminal` | Enters global configuration mode. |
| 3    | `interface type`  | Enters global configuration mode. |
| 4    | `service instance id ethernet [evc-id]` | Configures an Ethernet service instance on an interface and enters service instance configuration mode. |
| 5    | `encapsulation dot1q {any \| vlan-id \[vlan-id [-vlan-id]\]}`  
`second-dot1q {any \| vlan-id \[vlan-id [-vlan-id]\]}` | Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance. |
| 6    | `bridge-domain bridge-id [split-horizon]` | Binds the Ethernet service instance to a bridge domain instance where `bridge-id` is the identifier for the bridge domain instance. |
| 7    | `cfm mep domain domain-name mpid mpid-value` | Creates an MEP under the Ethernet service instance. |
| 8    | `end`             | Returns to privileged EXEC mode. |

---

**Defining MEPs Statically within a Maintenance Association**

To define MEPs statically within a maintenance association, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. ethernet cfm domain *domain-name level level-id*
4. service {ma-name | number ma-num} {evc evc-name | port} [direction down]
5. mep mpid mpid
6. 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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ethernet cfm domain <em>domain-name level level-id</em></td>
<td>Creates a CFM maintenance domain at a specific maintenance level and enters Ethernet CFM configuration mode. The range of the maintenance domain level is from 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ethernet cfm domain customer level 7</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>service {ma-name</td>
<td>number ma-num} {evc evc-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ecfm)# service Customer1 port</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>mep mpid mpid</td>
<td>Statically defines the MEPs within a maintenance association.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ecfm-srv)# mep mpid 702</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-ecfm-srv)# end</td>
<td></td>
</tr>
</tbody>
</table>

Specifying the Number of MEPs in a Maintenance Association

To specify the number of MEPs in a maintenance association, complete the following steps:
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ethernet cfm domain domain-name level level-id`
4. `service {ma-name | number ma-num} {evc evc-name | port} [direction down]`
5. `maximum meps max-num`
6. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example: | Switch> `enable` | |
| Step 2 | `configure terminal` | Enters global configuration mode. |
| Example: | Switch# `configure terminal` | |
| Step 3 | `ethernet cfm domain domain-name level level-id` | Creates a CFM maintenance domain at a specific maintenance level and enters Ethernet CFM configuration mode. The range of the maintenance domain level is from 0 to 7. |
| Example: | Switch(config)# `ethernet cfm domain customer level 7` | |
| Step 4 | `service {ma-name | number ma-num} {evc evc-name | port} [direction down]` | Configures a maintenance association within a maintenance domain for a port MEP or MEP for an EFP and enters CFM service configuration mode. |
| Example: | Switch(config-ecfm)# `service Customer1 port` | |
| Step 5 | `maximum meps max-num` | Specifies the maximum number of MEPs in a maintenance association. The default is 100. The range is from 1 to 65535. |
| Example: | Switch(config-ecfm-srv)# `maximum meps 50` | |
| Step 6 | `end` | Returns to privileged EXEC mode. |
| Example: | Switch(config-ecfm-srv)# `end` | |
Creating an MIP Dynamically

**Note**

The `ethernet cfm mip auto-create` command has lower precedence than the `ethernet cfm mip level manual` MIP command. For example, if you manually configure an MIP for a particular maintenance association, that configuration overrides the MIP created by the global `ethernet cfm mip auto-create` command for that maintenance association.

To create an MIP dynamically, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ethernet cfm mip {auto-create level level-id [lower-mep-only] [sender-id chassis] | filter}`
4. `end`

**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>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>`ethernet cfm mip {auto-create level level-id [lower-mep-only] [sender-id chassis]</td>
<td>filter}`</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To disable CFM globally on the device, use the <code>no ethernet cfm global</code> command.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# ethernet cfm mip auto-create level 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring an MIP on a Service Instance in CFM Manually

**Note** You cannot configure an MIP at a level lower than the level of already configured maintenance endpoints (MEPs) on an interface. Configuring an MIP using this command is known as a manual MIP and has precedence over the ethernet `cfm mip auto-create` command.

To create an MIP manually, complete the following steps:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type`
4. `service instance id ethernet [evc-name]`
5. `encapsulation dot1ad vlan-id dot1q vlan-id`
6. `bridge-domain bridge-id`
7. `cfm mip level level-id`
8. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type</code></td>
<td>Specifies the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# interface GigabitEthernet 0/10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>service instance id ethernet [evc-name]</code></td>
<td>Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-if)# service instance 1 ethernet evc1</code></td>
<td></td>
</tr>
</tbody>
</table>

- `id` — Integer from 1 to 4294967295 that uniquely identifies a service instance on an interface.
- `evc-name` — (Optional) String of a maximum of 100 bytes that associates an Ethernet virtual connection (EVC) to the service instance.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> encapsulation dot1ad vlansi dot1q vlansi</td>
<td>Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# encapsulation dot1ad 430 dot1q 431</td>
<td>• <strong>dot1ad</strong>— Indicates that the IEEE 802.1ad provider bridges encapsulation type is used for the outer tag.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dot1q</strong>— Indicates that the IEEE 802.1q standard encapsulation type is used for the inner tag.</td>
</tr>
<tr>
<td></td>
<td>• <strong>vlansi</strong>— VLAN ID, integer in the range 1 to 4094. A hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) A comma must be entered to separate each VLAN ID range from the next range.</td>
</tr>
<tr>
<td><strong>Step 6</strong> bridge-domain bridge-id</td>
<td>Binds a service instance to a bridge domain instance.</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# bridge-domain 340</td>
<td>• <strong>bridge-id</strong>— Numerical ID of the bridge domain instance. The range is from 1 to 16384.</td>
</tr>
<tr>
<td><strong>Step 7</strong> cfm mip level level-id</td>
<td>Provisions a IEEE CFM MIP manually at a specified maintenance level on an EFP service.</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# cfm mip level 7</td>
<td>• <strong>level-id</strong>— Maintenance level ID. The valid values range from 0 to 7.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if-srv)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling the Transmission of Continuity Check Messages

To enable the transmission of continuity check messages, complete the following steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. ethernet cfm domain domain-name level level-id
4. service {ma-name | number ma-name} {evc evc-name | port} [ direction down]
5. continuity-check [interval time | loss-threshold threshold | static rmeP]
6. continuity-check [interval time | loss-threshold threshold | static rmeP]
7. continuity-check [interval time | loss-threshold threshold | static rmeP]
8. exit
9. mep archive-hold-time minutes
10. end

DETAILED STEPS

<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>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ethernet cfm domain domain-name level level-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ethernet cfm domain Customer level 7</td>
</tr>
<tr>
<td></td>
<td>Creates a maintenance domain at a specified level and enters Ethernet CFM configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>service {ma-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-ecfm)# service Customer1 port</td>
</tr>
<tr>
<td></td>
<td>Creates a maintenance association within a maintenance domain and enters CFM service configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>continuity-check [interval time</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-ecfm-srv)# continuity-check</td>
</tr>
<tr>
<td></td>
<td>Enables the transmission of CCMs.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>continuity-check [interval time</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-ecfm-srv)# continuity-check interval 10s</td>
</tr>
<tr>
<td></td>
<td>Configures the time period between CCM transmissions.</td>
</tr>
</tbody>
</table>
### Sending CFM Loopback and Linktrace Messages

To send CFM loopback and linktrace messages, complete the following steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ping ethernet {mpid mpid | mac-address} {domain domain-name} {port | evc evc-name} [source source-mpid] [cos cos-value]`
4. `traceroute ethernet {mpid mpid | mac-address} {domain domain-name} {port | evc evc-name} [cos cos-value] [fdb-only]`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  - Enter your password if prompted. |

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>`continuity-check [interval time</td>
<td>loss-threshold threshold</td>
</tr>
</tbody>
</table>

Example:

```
Switch(config-ecfm-srv)# continuity-check
lossthreshold 10
```

| Step 8 | `exit` | Returns to Ethernet CFM configuration mode. |

Example:

```
Switch(config-ecfm-srv)# end
```

| Step 9 | `mep archive-hold-time minutes` | Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged. The default value is 100 minutes. The range is from 1 to 65535 minutes. |

Example:

```
Switch(config-ecfm)# mep archive-hold-time 60
```

| Step 10 | `end` | Returns to privileged EXEC mode. |

Example:

```
Switch(config-ecfm)# end
```
### Configuration Examples for CFM

#### Enabling or Disabling CFM Globally

The following example shows how to enable Ethernet Connectivity Fault Management (CFM):

```
Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm global
```

The following example shows how to disable CFM:

```
Switch > enable
Switch # configure terminal
Switch(config) # no ethernet cfm global
```

#### Enabling or Disabling CFM on an Interface

The following example shows how to enable CFM on an Interface:

```
Switch > enable
Switch # configure terminal
Switch(config) # interface GigabitEthernet 1/1
Switch(config-if) # ethernet cfm interface
```
The following example shows how to disable CFM on an Interface:

Switch > enable
Switch # configure terminal
Switch(config) # interface GigabitEthernet 1/1
Switch(config-if) # no ethernet cfm interface

Enabling Caching of CFM Data
The following example shows how to set the maximum number of entries in the CFM traceroute cache table to 2500:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm traceroute cache size 2500

The following example shows how to set the retention time for entries in the CFM traceroute cache table to 5 minutes:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm traceroute cache hold-time 5

Creating a Maintenance Domain
The following example shows how to define a domain named domain1 at level 6 and enters Ethernet CFM configuration mode:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm domain domain1 level 6

Creating a Maintenance Association
The following example shows how to create a maintenance association:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm domain operator level 5
Switch(config-ecfm) # service operatorA port
Switch(config-ecfm) # exit

Creating a Port MEP
The following example shows how to set a port as internal to a maintenance domain and creates a port Maintenance End Points (MEP):

Switch > enable
Switch # configure terminal
Switch(config) # interface GigabitEthernet 4/1
Switch(config-if) # ethernet cfm mep domain CustomerB mpid 5 port

Creating an MEP for an EFP (Global)
The following example shows how to create an MEP for an Ethernet Flow Point (EFP) (global):

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm global
Switch(config) # ethernet cfm domain D7 level 7
Creating an MEP for an EFP (Interface)

The following example shows how to create an MEP for an EFP (interface):

Switch > enable
Switch # configure terminal
Switch(config) # interface GigabitEthernet 1/1
Switch(config-if) # service instance 1 ethernet evc1
Switch(config-if-srv) # service S1 evc evc1
Switch(config-if-srv) # encapsulation dot1ad 430 dot1q 431
Switch(config-if-srv) # bridge-domain 340
Switch(config-if-srv) # cfm mep domain D7 mpid 3400
Switch(config-if-srv) # exit

Defining the MEPs Statical within a Maintenance Association

The following example shows how to configure an MEP with an ID of 25:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm domain operator level 5
Switch(config-ecfm) # service operatorA port
Switch(config-ecfm-srv) # mep mpid 25
Switch(config-ecfm-srv) # exit
Switch(config-ecfm) # exit

Specifying the Number of MEPs in a Maintenance Association

The following example shows how to configure a maximum of 50 MEPs:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm domain operator level 5
Switch(config-ecfm) # service operatorA port
Switch(config-ecfm-srv) # maximum meps 50
Switch(config-ecfm-srv) # exit
Switch(config-ecfm) # exit

Creating an MIP Dynamically

The following example shows how to dynamically create a Maintenance Intermediate Point (MIP) at maintenance level 6:

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm mip auto-create level 6

Configuring MIP on a Service Instance in CFM Manually

The following example shows how to manually configure MIP on a service instance in CFM:

Switch > enable
Switch # configure terminal
Switch(config) # interface GigabitEthernet 0/10
Switch(config-if) # service instance 1 ethernet evc1
Switch(config-if-srv) # encapsulation dot1ad 430 dot1q 431
Switch(config-if-srv) # bridge-domain 340
Enabling the Transmission of Continuity Check Messages

The following example shows how to configure a loss threshold of 50 Continuity Check Messages (CCMs):

Switch > enable
Switch # configure terminal
Switch(config) # ethernet cfm domain operator level 5
Switch(config-ecfm) # service operatorA port
Switch(config-ecfm-srv) # continuity-check loss-threshold 50
Switch(config-ecfm-srv) # exit
Switch(config-ecfm) # exit

Sending CFM Loopback and Traceroute Messages

The following example shows how to send an Ethernet CFM loopback message to MAC address 1010.pcef.1010 on evc5:

Switch > enable
Switch # ping ethernet 1010.pcef.1010 domain domain1 evc evc5

The following example shows how to send an Ethernet CFM traceroute message to MAC address aabb.cc00.1010 at maintenance level 4 on evc_100:

Switch > enable
Switch # traceroute ethernet aabb.cc00.1010 domain domain1 evc evc_100

Verifying the CFM Configuration

Verifying the CFM Configuration

CFM Platform Capabilities

Use the following command to display information about the CFM platform capabilities:

Switch# show ethernet cfm capabilities

Global CFM PD Capabilities: (0x001011F3)
BD does not equal VLAN

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000001</td>
<td>INWARD MEP          Up MEPS are supported</td>
</tr>
<tr>
<td>0x00000002</td>
<td>OUTWARD MEP        Down MEPS are supported</td>
</tr>
<tr>
<td>0x00000010</td>
<td>AIS             AIS is supported</td>
</tr>
<tr>
<td>0x00000020</td>
<td>OOS              LCK is supported</td>
</tr>
<tr>
<td>0x00000040</td>
<td>EVC         EVC-based CFM config is permitted</td>
</tr>
<tr>
<td>0x00000080</td>
<td>PORTMEP          Port MEPS are supported</td>
</tr>
<tr>
<td>0x00000100</td>
<td>DE              DE bit is set in Loopback packets</td>
</tr>
<tr>
<td>0x00001000</td>
<td>XCONNECT         CFM is supported on xconnects</td>
</tr>
<tr>
<td>0x00100000</td>
<td>HYBRID MODE      The router is running in hybrid mode, with active-active RPs</td>
</tr>
</tbody>
</table>
**CFM Domain**

Use the following command to display information about maintenance domain:

```
Switch# show ethernet cfm domain
```

<table>
<thead>
<tr>
<th>Domain Name: D7</th>
<th>Level: 7</th>
<th>Total Services: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type Id</td>
<td>Dir CC</td>
<td>CC-int</td>
</tr>
<tr>
<td>BD</td>
<td>340</td>
<td>Up</td>
</tr>
</tbody>
</table>

**CFM Maintenance-Points Local**

Use the following command to display information about local CFM maintenance points that are configured on a device:

```
Switch# show ethernet cfm maintenance-points local
```

Local MEPs:

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>Lvl</th>
<th>MacAddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>3400</td>
<td>D7</td>
<td>7</td>
<td>0000.3148.3379 BD</td>
</tr>
<tr>
<td>Y</td>
<td>No</td>
<td>Up</td>
<td>Gi0/10 340</td>
</tr>
<tr>
<td></td>
<td>S1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Static</td>
<td></td>
<td>evcl</td>
</tr>
</tbody>
</table>

Total Local MEPs: 1
Local MIPs: None

**CFM Maintenance-Points Remote**

Use the following command to display information about remote CFM maintenance endpoints (RMEPs) that are configured statically in the MEP list and their status in the continuity check database (CCDB):

```
Switch# show ethernet cfm maintenance-points remote
```

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>MacAddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>IfSt</td>
<td>PtSt</td>
<td>Lvl</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Ingress</td>
<td></td>
</tr>
<tr>
<td>RDI</td>
<td>MA Name</td>
<td>Type Id</td>
</tr>
<tr>
<td>SrvcInst</td>
<td>EVC Name</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>Age</td>
<td></td>
</tr>
</tbody>
</table>
Local MEP Info

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain</th>
<th>MAC Address</th>
<th>Up/Down</th>
<th>Interface</th>
<th>MA</th>
<th>BD</th>
<th>Type</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>4300</td>
<td>D7</td>
<td>0000.3148.3377</td>
<td>Up</td>
<td>G10/20</td>
<td>S1</td>
<td></td>
<td>340</td>
<td>58s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>evc1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MPID: 3400 Domain: D7 MA: S1
Total Remote MEPS: 1

CFM MIP Database

Use the following command to display information about the contents of a MIP CCDB:

Switch# show ethernet cfm mpdb

* = Can Ping/Traceroute to MEP

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>MacAddress</th>
<th>Version</th>
<th>Lvl</th>
<th>Domain ID</th>
<th>Ingress</th>
<th>Expd</th>
<th>MA Name</th>
<th>Type</th>
<th>Id</th>
<th>SrvcInst</th>
<th>EVC Name</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>4300</td>
<td>D7</td>
<td>0000.3148.3377</td>
<td>IEEE-CFM</td>
<td>7</td>
<td>D7</td>
<td></td>
<td></td>
<td>S1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>45s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>evc1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Remote MEPS: 1

CFM Runtime

Use the following command to display available sub-options for CFM runtime:

Switch# show ethernet cfm runtime ?

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lmep</td>
<td>Local MEP specific runtime information</td>
</tr>
<tr>
<td>ma-info</td>
<td>MA queue info</td>
</tr>
<tr>
<td>mcl-info</td>
<td>MCL queue info</td>
</tr>
<tr>
<td>smep</td>
<td>Server MEP specific runtime information</td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP DB specific runtime information</td>
</tr>
</tbody>
</table>

CFM Runtime Local MEPS

Use the following command to display information about CFM runtime for local MEPS:

Switch# show ethernet cfm runtime lmep
### Local MEPs

- **MPID**: 3400
- **DomainName**: D7
- **MA Name**: S1
- **Level**: 7
- **Direction**: Up
- **EVC**: evc1
- **Bridge Domain**: 340
- **Service Instance**: 1
- **Interface**: Gi0/10
- **CC Offload**: No
- **CC Status**: Enabled
- **CC Loss Threshold**: 3
- **MAC**: 0000.3148.3379
- **LCK-Status**: Enabled
- **LCK Expiry Threshold**: 3.5
- **Level to transmit LCK**: Default
- **Defect Condition**: 0x0
- **Defect**:
  - EFD nfn: Not Sent
  - lck_mep_timer: Stopped

---

**CFM Runtime MA**

Use the following command to display information about CFM runtime for maintenance association (MA):

```
Switch# show ethernet cfm runtime ma-info
```

Display Maintenance Association info:

```
IDB = GigabitEthernet0/10
  BD=340: Up:7 7 Down:-1 -1 MCL:7 MIP:-1
```

**CFM Runtime MCL**

Use the following command to display information about maximum configured level (MCL) service for Up MEPs, Down MEPs, or a MIP. This value is kept per service, either VLAN or bridge domain.

```
Switch# show ethernet cfm runtime mcl-info
```

```
BD=340  MCL=7
```

**Server MEP Specific Runtime Information**

Use the following command to display information about server MEP specific runtime information for CFM:

```
Switch# show ethernet cfm runtime smep
```

**SMEP Settings**:

```
Interface: GigabitEthernet0/5
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
```
Defect Condition: 0x1
LCK up timer: Stopped
LCK down timer: Stopped
AIS periodic timer: Running

Interface: GigabitEthernet0/10
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: 0x0

CFM SNMP

Use the following command to display information about Simple Network Management Protocol (SNMP) for CFM:

Switch# show ethernet cfm runtime snmp

SNMP Settings:
CMF DB is in sync with CFM-SNMP DB
CMF-SNMP DB is sync with CFM DB
Stack :49154
MEP :3400

CFM SMEP

Use the following command to display the output contents of Ethernet CFM SMEP:

Switch# show ethernet cfm smep

SMEP Settings:
--------------
Interface: GigabitEthernet0/5
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS

Interface: GigabitEthernet0/10
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: No Defect

Interface: GigabitEthernet0/11
LCK-Status: Enabled
LCK Period: 60000 (ms)
CFM over EVC

Verifying the CFM Configuration

Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS

Interface: GigabitEthernet0/20
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: No Defect

CFM Statistics

Use the following command to display CFM information:

Switch# show ethernet cfm statistics

BRAIN MAC: 0000.3148.3379
DomainName: D7
MA Name: S1
MPID: 3400
Last clearing of counters: never
CCMs:
  Transmitted: 1133  Rcvd Seq Errors: 0
LTRs:
  Unexpected Rcvd: 0
LBRs:
  Transmitted: 5  Rcvd Seq Errors: 0
  Rcvd in order: 5  Rcvd Bad MSDU: 0

CFM Traceroute-Cache

Note

You must enable traceroute cache globally before using this command.

Use the following command to display information about the contents of the traceroute cache:

Switch# show ethernet cfm traceroute-cache

Current Cache-size: 5 Hops
Max Cache-size: 100 Hops
Hold-time: 100 Minutes

Traceroute to 0000.3148.3377 on Domain D7, Level 7, service S1, evc evc1
issued at *13:29:52.125 UTC Sat Mar 8 1902
path found via MPDB

B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout

Switch# show ethernet cfm traceroute-cache
### Additional References for CFM

The following sections provide references related to the CFM feature.

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standard</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>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported, and support for existing RFCs has not been modified.</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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
</tbody>
</table>
INDEX

A
attaching or removing traffic policy using IOS 78
authentication 252

egress LLQ 86
    configuring LLQ using IOS 86
egress queuing and scheduling 65
    bandwidth remaining ratio and bandwidth remaining percent 65
egress bandwidth 65
egress shaping 65
    LLQ 65
egress shaping 90
    configuring shaping using IOS 90
egress classification 85
    configuring using IOS 85
      egress LLQ 86
      configuring LLQ using IOS 86
      egress queuing and scheduling 65
      bandwidth remaining ratio and bandwidth remaining percent 65
      egress bandwidth 65
      egress shaping 65
      LLQ 65
      egress shaping 90
      configuring shaping using IOS 90
ethernet virtual private line 38
evc 37, 38, 43, 50, 410
    attributes 37
    configuring using Cisco IOS 50, 410
    encapsulation and rewrite operations for EVC 43
    features 37
    interactions with other features 38
    types 38

B
bridge domain 42, 43
    types 43

cdp 267
changing a password 254
channel group 139, 140, 141, 142, 145, 151
    adding and removing interfaces 140, 142
    configuring with lacp 139, 141
    manual and default load balancing 145
    show commands 151
classification 62, 64
    egress classification 64
    ingress classification 62
Classification Tasks 4
Configuring 5
    Device Host Name 5
    Configuring Passwords on the Device 5

e
efp 41, 42
    attributes 42
efp counters 42
egress bandwidth 88
    configuring bandwidth using IOS 88
egress BRR and BRP 92
    configuring egress BRR and BRP using IOS 92
egress classification 85
    configuring using IOS 85

cfgmr
Cisco ME 2600X Series Ethernet Access Switch Software Configuration Guide
IGMP (continued)
  report suppression 191
  statistics and counters 201
  understanding 183
ingress classification 70
  configuring using IOS 70
ingress marking 80, 82
  configuring ingress marking using IOS 80
  configuring ingress re-marking using IOS 82
ingress policing 73
  configuring using IOS 73

L
lACP 130, 131, 133, 134, 136, 144
  configuring over port channel 133
  configuring redundancy with fast switchover 136
  functions 130
  modes 131
  monitoring status 134
  priority 134
  redundancy 136
  setting maximum and minimum thresholds 144
lag 138
  restrictions 138
LAG 154
  interactions with other features 154
layer 2 protocol tunneling 52
  configuring using Cisco IOS 52
local authentication 252
  configuring 252

M
mac address limiting 160
mac learning 157
mac move 158
MAC-BD-LIMT-REACHED 208
MAC-SYS-LIMT-REACHED 209
manual load balancing 146, 149
  configuring using Cisco IOS 146, 149
Manually booting 2
  IOS software image 2
marking 63
  ingress marking 63
mode 3
MVR 171
  television application 171

P
password protection 254, 255, 256
  changing a line password 256
  enabling password and secret password 255
policing 62
  ingress policing 62
privilege level 257, 258, 259
  display current privilege levels 258
  logging in to a privilege level 259
  setting the privilege level for a command 258
  understanding 257

Q
QoS 60, 61, 63, 65, 66, 67, 70, 78
  advantages 60
  Cisco ME 2600X system QoS 61
  configuring QoS features using IOS 70
  egress functions 63
  EVCS support 66
  hierarchical-QoS 65
  ingress and egress port-channel support 66
  ingress functions 61
  statistics 67

R
rep 101, 103, 104, 106, 107, 109, 113, 114, 116, 117, 119, 121
  administrative vlan 107
  configuration guidelines 106
  configuration sequence 107
  configure LSL retries and LSL ageout 117
  configure rep over evc 121
  configuring using IOS 109
  configuring vlan load balancing using IOS 114
  edge no-neighbor 104
  fast convergence 103
  link adjacency 103
  LSL ageout timer and LSL retries 116
  ports 104
  rep with evc 119
  vlan load balancing 113
rep segments 101, 103
  characteristics 103
RMON 205, 206, 207
  configuring RMON settings 206
  displaying RMON status 207
Index

S

SNMP 271, 272, 274, 277, 279
  community names 279
  Components 272
  IETF traps and examples 277
  introduction 271

SNMP (continued)
  messages 279
  MIB 274
  MIBs Supported in Cisco ME 2600X 274
  traps 277
  static mac address 162