Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 2

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

CONTENTS

Overview of ISG 1

- Finding Feature Information 1
- Information About ISG 1
  - What Is ISG 1
  - ISG Principles 2
    - Subscriber Sessions 2
    - Subscriber Access 3
    - Subscriber Identification 3
    - Subscriber Services 3
    - Policies 4
    - Dynamic Policy Updates 4
  - Benefits of ISG 5
  - Planning for ISG Implementation 5
    - Trust Model 6
    - Subscriber Access Model 6
    - Single Sign-On Requirements 6
    - Network Forwarding 6
    - Service Packaging 6
    - Billing Model 7
- Additional References 7
- Feature Information for the Overview of ISG 7

Configuring ISG Control Policies 9

- Finding Feature Information 9
- Prerequisites for ISG Control Policies 9
- Restrictions for ISG Control Policies 9
- Information About ISG Control Policies 10
  - Control Policies 10
    - Differentiated Initial Policy Control 11
  - Uses of Control Policies 11

How to Configure an ISG Control Policy 11

Configuring a Control Class Map 11

Configuring a Control Policy Map 17

Applying the Control Policy Map 21

Applying a Control Policy Map Globally on the Router 22

Applying an ISG Control Policy Map to an Interface or Subinterface 22

Applying an ISG Control Policy Map to a Virtual Template 23

Monitoring and Maintaining ISG Control Policies 24

Configuration Examples for ISG Control Policies 25

Control Policy for Layer 2 Access and Service Provisioning Example 25

Verifying a Control Policy Examples 26

Control Policy for Restricting Access on the Basis of Interface and Access Media Example 28

Control Policies for Automatic Subscriber Login Example 29

Additional References 29

Feature Information for ISG Control Policies 31

Configuring ISG Access for PPP Sessions 35

Finding Feature Information 35

Prerequisites for ISG Access for PPP Sessions 35

Restrictions for ISG Access for PPP Sessions 35

Information About ISG Access for PPP Sessions 36

Overview of ISG Access for PPP Sessions 36

ISG Subscriber IP Address Management for PPP Sessions 36

VRF Transfer for PPP Sessions 37

Default Policy for ISG Access for PPP Sessions 37

How to Configure ISG Access for PPP Sessions Using Control Policies 37

Enabling ISG VRF Transfer for PPP Sessions 38

Verifying VRF Transfer for PPP Sessions 39

Troubleshooting ISG Access for PPP Sessions 40

Configuration Examples for ISG Access for PPP Sessions 42

Configuring ISG Access for PPP Sessions Example 42

VRF Transfer for PPP Sessions Using IPCP Renegotiation Example 44

Additional References 45

Feature Information for ISG Access for PPP Sessions 46

Configuring ISG Access for IP Subscriber Sessions 49

Finding Feature Information 49

Prerequisites for ISG Access for IP Subscriber Sessions 49

Restrictions for ISG Access for IP Subscriber Sessions 50

Information About ISG Access for IP Subscriber Sessions 51

Types of IP Subscriber Sessions 52

IP Sessions 52

IP Interface Sessions 52

IP Subnet Sessions 52

Coexistence of Multicast and IP Sessions 53

IP Subscriber Connectivity 53

Layer 2 Connected Access Networks 53

Routed Access Networks 53

IP Subscriber Session Initiation 54

IP Subscriber Addressing 54

Methods of ISG Subscriber IP Address Assignment 55

IP Interface Sessions 55

IP Sessions 55

IP Subnet Sessions 55

Public and Private IP Addresses 55

Overlapping IP Addresses 56

ISG Subscriber IP Address Assignment Using DHCP 56

IP Subscriber Identity 56

Routed IP Subscriber Identity 57

MAC Address as Secondary Identity 57

DHCP Lease Query Support 57

Layer 2 Connected IP Subscriber Identity 58

VPN Connectivity and Services for IP Subscribers 58

Subscriber VPN Membership 58

Multiservice Interface Model 58

VPN Addressing 59

VPN IP Subscriber Identity 60

Service Model for VRF Transfers 60

Benefits of Dynamic VPN Selection 60

IP Session Termination 61

IP Session Recovery for DHCP-Initiated IP Sessions 61

Default Services for IP Subscriber Sessions 61

How to Configure ISG for IP Subscriber Sessions 62
Creating ISG Sessions for IP Subscribers 62
Creating IP Subscriber Sessions for Routed ISG Subscribers 62
Creating IP Subscriber Sessions for Layer 2 Connected ISG Subscribers 64
Creating ISG IP Interface Sessions 65
Creating an ISG Static Session 66
Creating ISG IP Subnet Sessions 69
Configuring IP Session Recovery for DHCP-Initiated IP Sessions 71
Verifying ISG IP Subscriber Sessions 73
Clearing ISG IP Subscriber Sessions 74
Troubleshooting Tips 75
Assigning ISG Subscriber IP Addresses Using DHCP 75
Configuring an ISG Interface for Dynamic DHCP Class Association 76
Configuring DHCP Server User Authentication 77
Troubleshooting Tips 79
Configuring a DHCP Class in a Service Policy Map 80
What to Do Next 81
Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server 81
Prerequisites 81
What to Do Next 82
Configuring a DHCP Server IP Address 82
Configuring ISG Dynamic VPN Selection 83
Configuring a Multiservice Interface 83
Specifying a VRF in a Service Policy Map 84
Verifying VRF Transfer for IP Sessions 86
Troubleshooting VRF Transfer for IP Sessions 87
Configuration Examples for ISG Access for IP Subscriber Sessions 88
Example ISG IP Interface Subscriber 89
Example ISG Routed IP Subscriber 89
Example ISG Layer 2 Connected IP Subscriber 89
Example ISG Static Session Creation 89
Example DHCP-Initiated Session Recovery 89
Example ISG Interface with DHCP Class-Aware Capability 90
Example DHCP Address Pool Classes and Relay Actions for ISG 90
Example Dynamic VPN Selection 91

Additional References 92

Feature Information for ISG Access for IP Subscriber Sessions 93

Configuring MQC Support for IP Sessions 99

Finding Feature Information 99

Restrictions for MQC Support for IP Sessions 99

Information About MQC Support for IP Sessions 100

Supported Interfaces 100

ISG Policers 100

Precedence Order in Policy Maps 100

How to Configure MQC Support for IP Sessions 101

Configuring Local Subscriber Profile for MQC Support 101

Configuring ISG QoS for IP Sessions 102

Configuration Examples for MQC Support for IP Sessions 103

QoS Policy-Map Service Profile and Command Policy-Map Configurations Example 103

Additional References 103

Feature Information for MQC Support for IP Sessions 104

Configuring ISG Port-Bundle Host Key 107

Finding Feature Information 107

Prerequisites for the ISG Port-Bundle Host Key Feature 107

Restrictions for the ISG Port-Bundle Host Key Feature 107

Information About ISG Port-Bundle Host Key 108

Overview of ISG Port-Bundle Host Key 108

Port-Bundle Host Key Mechanism 108

Port-Bundle Length 109

Benefits of ISG Port-Bundle Host Key 110

Support for Overlapped Subscriber IP Addresses Extended to Include External Portal Usage 110

Portal Provisioning for Subscriber and ISG IP Addresses No Longer Required 110

How to Configure ISG Port-Bundle Host Key 110

Enabling the ISG Port-Bundle Host Key Feature in a Service Policy Map 111

What to Do Next 112

Enabling the ISG Port-Bundle Host Key Feature in a User Profile or Service Profile on the AAA Server 112

What to Do Next 112

Configuring Port-Bundle Host Key Parameters 113

Verifying ISG Port-Bundle Host Key Configuration 114

Configuration Examples for ISG Port-Bundle Host Key 115

ISG Port-Bundle Host Key Configuration Example 115

Additional References 116

Feature Information for ISG Port-Bundle Host Key 116

Configuring ISG as a RADIUS Proxy 119

Finding Feature Information 119

Prerequisites for ISG RADIUS Proxy 119

Restrictions for ISG RADIUS Proxy 119

Information About ISG RADIUS Proxy 120

Overview of ISG RADIUS Proxy 120

ISG RADIUS Proxy Handling of Accounting Packets 120

RADIUS Client Subnet Definition 121

ISG RADIUS Proxy Support for Mobile Wireless Environments 121

Attribute Processing and RADIUS Request Correlation 121

3GPP Attribute Support 121

Benefits of ISG RADIUS Proxy 122

How to Configure ISG as a RADIUS Proxy 122

Initiating ISG RADIUS Proxy IP Sessions 122

Configuring ISG RADIUS Proxy Global Parameters 124

Configuring ISG RADIUS Proxy Client-Specific Parameters 126

Defining an ISG Policy for RADIUS Proxy Events 128

Verifying ISG RADIUS Proxy Configuration 130

Clearing ISG RADIUS Proxy Sessions 131

Configuration Examples for ISG RADIUS Proxy 132

ISG RADIUS Proxy Configuration Example 132

ISG RADIUS Proxy and Layer 4 Redirect Example 133

Additional References 134

Feature Information for ISG RADIUS Proxy 135

Configuring RADIUS-Based Policing 139

Finding Feature Information 139

Prerequisites for RADIUS-Based Policing 139

Restrictions for RADIUS-Based Policing 139

Information About RADIUS-Based Policing 140

RADIUS Attributes 140

RADIUS Attributes 250 and 252 140

Cisco VSA 1 141

Add-Class Primitive 141

Remove-Class Primitive 142

Parameterized QoS Policy as VSA 1 143

Parameterization of QoS ACLs 143

How to Configure RADIUS-Based Policing 143

Configuring Per-Session Shaping 143

Configuring a QoS Policy with Shaping on ISG 143

Configuring Per-Session Shaping on RADIUS 145

Configuring Per-Service Shaping and Policing 145

Configuring a Hierarchical QoS Child Policy with Shaping and Policing on ISG 145

Configuring a Hierarchical QoS Parent Policy with Shaping and Policing on ISG 147

Configuring Per-Service Shaping and Policing on RADIUS 148

Verifying RADIUS-Based Policing 148

Configuration Examples for RADIUS-Based Policing 150

Example Adding Parameterization of QoS ACLs 150

Example Setting the Shaping Rate Using an Access-Accept Message 151

Example Setting the Shaping Rate Using a CoA Message 152

Example Setting the Policing Rate Using an Access-Accept Message 154

Example Setting the Policing Rate Using a CoA Message 155

Additional References 156

Feature Information for RADIUS-Based Policing 157

Configuring ISG Policies for Automatic Subscriber Logon 159

Finding Feature Information 159

Prerequisites for ISG Automatic Subscriber Logon 159

Restrictions for ISG Automatic Subscriber Logon 160

Information About ISG Automatic Subscriber Logon 160

Overview of ISG Automatic Subscriber Logon 160

Supported Identifiers for ISG Automatic Subscriber Logon 160

Authorization Based on Circuit ID and Remote ID 160

Accounting Behavior When ISG Automatic Subscriber Logon Is Configured 161

How to Configure ISG Policies for Automatic Subscriber Logon 161

Configuring an ISG Control Policy for Automatic Subscriber Logon 161

What to Do Next 163

Verifying ISG Automatic Subscriber Logon 163

Configuration Examples for ISG Automatic Subscriber Logon 164

Automatic Subscriber Logon Based on IP Address Example 164

Additional References 165

Feature Information for ISG Automatic Subscriber Logon 166

Enabling ISG to Interact with External Policy Servers 169

Finding Feature Information 169

Restrictions for ISG Interaction with External Policy Servers 169

Information About ISG Interaction with External Policy Servers 169

Initial and Dynamic Authorization 170

Triple-Key Authentication for ISG 170

How to Enable ISG to Interact with External Policy Servers 171

Configuring the ISG as a AAA Client 171

Configuring the ISG as a AAA Server 172

Enabling the Location VSA for Triple-Key Authentication 174

Configuration Examples for ISG Interaction with External Policy Servers 176

Example ISG Interaction with External Policy Servers 176

Example Triple-Key Authentication 176

Additional References 177

Feature Information for ISG Interaction with External Policy Servers 178

Configuring ISG Subscriber Services 181

Finding Feature Information 181

Restrictions for ISG Subscriber Services 181

Information About ISG Subscriber Services 182

ISG Services 182

Primary Services 182

Traffic Classes and Traffic Class Priority 182

Traffic Policies 183

ISG Features 183

Service Groups 183

Service Activation Methods 184

How to Configure ISG Services on the Router 184

Configuring an ISG Service with Per-Session Functionality 185

Configuring an ISG Service with a Traffic Policy 187

Defining an ISG Traffic Class Map 187

Configuring an ISG Service Policy Map with a Traffic Policy 189

Configuring the Default Class in an ISG Service Policy Map 191

Activating ISG Subscriber Services 192

Configuring Automatic Service Activation in a User Profile 193

Configuring ISG Control Policies to Activate Services 193

Verifying ISG Services 194

Configuration Examples for ISG Services 195

Example Service for Per-Flow Accounting 195

Example Service for Absolute Timeout and Idle Timeout 196

Example Service for ISG Policing 196

Example Service for Per-Subscriber Firewall 197

Example Service for Redirecting Layer 4 Subscriber Traffic 197

Example Deactivating a Layer 4 Redirection Service Following Authorization 198

Additional References 198

Feature Information for ISG Subscriber Services 199

Configuring ISG Network Forwarding Policies 201

Finding Feature Information 201

Restrictions for ISG Network Forwarding Policies 201

Information About ISG Network Policies 201

Network Policies 202

Configuration Sources for Network Policies 202

How to Configure ISG Network Policies 202

Configuring Network Policies for PPP Sessions in Service Policy Maps 202

What to Do Next 204

Configuring Network Policies for IP Sessions in Service Policy Maps 204

What to Do Next 206

Configuration Examples for ISG Network Policies 206

Network Forwarding Policy for PPP Sessions Example 206

Network Forwarding Policy for IP Sessions Example 206

Additional References 206

Feature Information for ISG Network Policies 207

Configuring ISG Accounting 209

Finding Feature Information 209

Restrictions for ISG Accounting 209

Information About ISG Accounting 209

Overview of ISG Accounting 210

ISG Accounting Messages on ANCP Ports 210

ISG Accounting Records 210

Interim ISG Accounting Updates 211

Broadcast Accounting 211

ISG Postpaid Tariff Switching 211

How to Configure ISG Accounting 212

Enabling ISG Per-Session Accounting 212

Prerequisites 212

Enabling Per-Session Accounting in a User Profile on a AAA Server 212

What to Do Next 213

Troubleshooting Tips 213

Enabling ISG Per-Flow Accounting 213

Prerequisites 213

Enabling Per-Flow Accounting in a Service Profile on the AAA Server 214

Enabling Per-Flow Accounting in a Service Policy Map on the Router 214

Troubleshooting Tips 215

What to Do Next 216

Enabling ISG Per-Service Accounting 216

Prerequisites 216

Enabling Per-Service Accounting on the ISG 216

Configuring RADIUS for Service Activation and Deactivation 217

Enabling Per-Service Accounting in a Service Profile on a AAA Server 217

Enabling Per-Service Accounting in a Service Policy Map on the Router 218

What to Do Next 220

Troubleshooting Tips 220

Configuring ISG Postpaid Tariff Switching 220

What to Do Next 221

Verifying ISG Accounting and Postpaid Tariff Switching 221

Display Information About a Subscriber Session 221

Examples 222

Display AAA Subscriber Sessions 223

Examples 224

Display AAA Information for Subscribers 224

Examples 224

Display Information About ISG Postpaid Tariff Switching 227

Configuration Examples for ISG Accounting 227
Per-Flow Accounting Examples 227
Per-Service Accounting Example 228
Per-Service Accounting on ISG Example 228
ISG Postpaid Tariff Switching Examples 228
Additional References 229
Feature Information for ISG Accounting 230
Configuring ISG Support for Prepaid Billing 233
Finding Feature Information 233
Prerequisites for ISG Prepaid Billing Support 233
Restrictions for ISG Prepaid Billing Support 233
Information About ISG Prepaid Billing Support 234
Overview of ISG Support for Prepaid Billing 234
ISG Prepaid Volume Monitor Polling Timer and QV Values 234
ISG Prepaid Threshold 235
ISG Prepaid Idle Timeout 235
Benefits of ISG Prepaid Billing 235
How to Configure ISG Support for Prepaid Billing 236
Configuring RADIUS Attribute Support for ISG Prepaid Billing 236
Creating an ISG Prepaid Billing Configuration 237
Enabling ISG Prepaid Billing 240
Enabling ISG Prepaid Billing in a Service Policy Map 240
What to Do Next 241
Enabling ISG Prepaid Billing in Service Profile on the AAA Server 242
What to Do Next 243
Redirecting Subscriber Traffic upon Exhaustion of Credit 243
Credit-Exhausted Event 243
Configuring L4 Redirection in a Service Policy Map 243
Applying a Service Policy Map to Subscriber Traffic upon Exhaustion of Credit 245
What to Do Next 246
Forwarding Subscriber Traffic upon Depletion of Quota 247
Quota-Depleted Event 247
What to Do Next 248
Troubleshooting ISG Prepaid Billing Support 249
Configuration Examples for ISG Prepaid Billing Support 249

ISG Prepaid Billing Support Example 249

ISG Policies for Handling Credit-Exhausted and Quota-Depleted Prepaid Billing Events Example 250

Additional References 251

Feature Information for ISG Support for Prepaid Billing 252

Configuring ISG Policies for Session Maintenance 255

Finding Feature Information 255

Prerequisites for ISG Policies for Session Maintenance 255

Restrictions for ISG Policies for Session Maintenance 256

Information About ISG Policies for Session Maintenance 256

Session Maintenance Timers 256

Benefits of Session Maintenance Timers 256

Monitoring Sessions 256

ARP for Keepalive Messages 257

ICMP for Keepalive Messages 257

How to Configure ISG Policies for Session Maintenance 257

Configuring the Session Timer in a Service Policy Map 258

What to Do Next 259

Configuring the Session Timer on a AAA Server 259

Configuring the Connection Timer in a Service Policy Map 259

What to Do Next 261

Configuring the Connection Timer on a AAA Server 261

Verifying the Session and Connection Timer Settings 261

Troubleshooting the Session and Connection Timer Settings 262

Prerequisites for Troubleshooting the Session Maintenance Timers 262

Restrictions for Troubleshooting the Session Maintenance Timers 262

Debug Commands Available for the Session Maintenance Timers 263

Enabling the Session Maintenance Timer Debug Commands 263

Configuring a Session Keepalive on the Router 264

Configuring a Session Keepalive on a RADIUS Server 266

Configuring the ISG to Interact with the RADIUS Server 266

Configuration Examples for ISG Policies for Session Maintenance 268

Example Session Timer Configuration in a Service Policy Map 268

Example Connection Idle Timer Configuration in a Service Policy Map 269

Example Session Timer Show Command Output 269

Example Connection Idle Timer Show Command Output 269

Example Session Timer Debug Output 270

Example Connection Idle Timer Debug Output 270

Additional References 270

Feature Information for ISG Policies for Session Maintenance 272

Redirecting Subscriber Traffic Using ISG Layer 4 Redirect 275

Finding Feature Information 275

Restrictions for Redirecting ISG Subscriber Traffic 275

Information About Redirecting ISG Subscriber Traffic 276

Overview of ISG Layer 4 Redirect 276

Layer 4 Redirect Applications 276

How to Configure ISG Layer 4 Redirect 277

Defining a Redirect Server Group 277

Configuring Layer 4 Redirection in a Service Policy Map 278

What to Do Next 280

Configuring Layer 4 Redirection in a Service Profile or User Profile on the AAA Server 280

What to Do Next 280

Verifying ISG Traffic Redirection 281

Configuration Examples for ISG Layer 4 Redirect 282

Redirecting Unauthenticated Subscriber Traffic Example 283

Redirecting Unauthorized Subscriber Traffic Example 283

Initial ISG Redirection Example 284

Periodic ISG Redirection Example 284

Redirecting DNS Traffic Example 284

Additional References 284

Feature Information for Redirecting ISG Subscriber Traffic 285

Configuring ISG Policies for Regulating Network Access 287

Finding Feature Information 287

Information About ISG Policies for Regulating Network Access 287

Methods of Regulating Network Access 287

Overview of ISG Policing 288

How to Configure ISG Policies for Regulating Network Access 289

Configuring ISG Policing 289

Configuring Policing in a Service Policy Map on the Router 289

What to Do Next 290

Configuring Policing in a Service Profile or User Profile on the AAA Server 290

What to Do Next 291

Verifying ISG Policing 291

Configuration Examples for ISG Policies for Regulating Network Access 292

ISG Policing Examples 293

Additional References 293

Feature Information for ISG Policies for Regulating Network Access 294

Configuring ISG Integration with SCE 297

Finding Feature Information 297

Prerequisites for Configuring ISG Integration with SCE 297

Hardware Requirements 297

Software Requirements 298

Restrictions for Configuring ISG Integration with SCE 298

Information About Configuring ISG Integration with SCE 298

Overview of ISG-SCE Integration 299

ISG and SCE Roles in Subscriber Management 299

How to Configure ISG Integration with SCE 299

Configuring Communication Between SCE and ISG 300

Configuring SCE Connection Parameter on ISG 301

Configuring Control Policy on the Policy Manager 303

Configuring Control Policy on the ISG 303

Configuring Auto Service on the AAA Server 304

Configuring Services 304

Configuring Services on ISG 305

Configuring Services on the AAA Server 306

Troubleshooting Tips 307

Examples 307

Configuration Examples for ISG Integration with SCE 308

ISG Control Bus Configuration Example 308

ISG Integration with SCE Example 308

SCE Control Bus Configuration Examples 309

Additional References 309

Feature Information for Configuring ISG Integration with SCE 310

Service Gateway Interface 313

Finding Feature Information 313

Information About Service Gateway Interface 313
ISG 313
BEEP 314
Benefits of SGI 314
How to Enable Service Gateway Interface 314
Configuring BEEP Listener Connection 314
Troubleshooting SGI 315
Configuration Examples for Service Gateway Interface 316
Configuring BEEP Listener Connection Example 316
Additional References 317
Feature Information for Service Gateway Interface 318
Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging 321
Finding Feature Information 321
Prerequisites for ISG Session Monitoring and Distributed Conditional Debugging 321
Restrictions for Distributed Conditional Debugging 322
Information About ISG Session Monitoring and Distributed Conditional Debugging 322
ISG Session and Flow Monitoring 322
ISG Distributed Conditional Debugging 322
Benefits of Enhanced Conditional Debugging for the ISG Platforms 322
Cisco IOS Software Components Supported by Distributed Conditional Debugging 322
How to Enable ISG Session Monitoring and Distributed Conditional Debugging 323
Monitoring ISG Sessions and Flows 323
Configuring Distributed Conditional Debugging 324
ISG Debug Condition Commands 324
Debug Commands That Are Supported by ISG Conditional Debug 325
Restrictions 327
Enabling Distributed Conditional Debugging 328
Displaying Debugging Conditions 328
Troubleshooting Tips 329
Configuration Examples for ISG Distributed Conditional Debugging 330
Monitoring Interface Statistics Example 330
Monitoring CPU Statistics Example 330
Enabling ISG Distributed Conditional Debugging Example 331
Displaying Debugging Conditions Example 331
Filtering Debug Output Example 331

Additional References 331

Feature Information for Distributed Conditional Debugging 332

Last Updated: August 21, 2011

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

© 2011 Cisco Systems, Inc. All rights reserved.

Overview of ISG

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document provides information about what ISG is, the benefits of ISG, and how to begin implementing it.

- Finding Feature Information, page 1
- Information About ISG, page 1
- Additional References, page 7
- Feature Information for the Overview of ISG, page 7

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 the Feature Information Table at the end of this document.

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

Information About ISG

- What Is ISG, page 1
- ISG Principles, page 2
- Benefits of ISG, page 5
- Planning for ISG Implementation, page 5

What Is ISG

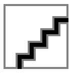
ISG is a structured framework in which edge access devices can deliver flexible and scalable services to subscribers. ISG handles the following key aspects of subscriber management:

- Subscriber identification
- Service and policy determination
- Session policy enforcement
- Session life-cycle management
- Accounting for access and service usage
- Session state monitoring

In addition, ISG introduces a dynamic element to the provisioning and activation of services through control policies and Change of Authorization (CoA) extensions to the RADIUS protocol.

An ISG-enabled device may be deployed at the access edge and service edge of a network and is applicable to a range of subscriber network environments, such as digital subscriber line (DSL), public wireless LAN (PWLAN), and mobile wireless. Moreover, ISG has been designed to accommodate a flexible distribution of subscriber and service information within a given solution. The figure below illustrates a typical DSL deployment for which service profile data may be stored in an authentication, authorization, and accounting (AAA) database and retrieved and cached on demand.

Figure 1



It is also possible to define services directly on an ISG. In all cases, service activation may be triggered as a result of a locally defined control policy, user profile associations, or CoA commands from an external policy server or portal application.

ISG Principles

Fundamental to the ISG architecture is the provisioning of a common session layer at which the management of generic subscriber sessions is decoupled from the technology that is used to provide access to the edge device.

Within this session management layer, common methods are provided for the extraction of subscriber identity information and the determination and activation of services. These methods are described in the following sections:

- Subscriber Sessions, page 2
- Subscriber Access, page 3
- Subscriber Identification, page 3
- Subscriber Services, page 3
- Policies, page 4
- Dynamic Policy Updates, page 4

Subscriber Sessions

An ISG subscriber session is a generic system context that is created for every subscriber who interacts with the edge device. A subscriber session is created on first interaction so that policies may be applied as early as possible. Such policies may facilitate the retrieval of subscriber identity information. All subscriber sessions are assigned a locally unique identifier that may subsequently be used to reference the session.

The session context is the basis for common handling at the session management layer, but the type of traffic that is encompassed in a session context may vary. Broadly, session types may be categorized as Layer 2 or Layer 3, depending on the packet types that are being handled by the session. For instance, a PPP session is a Layer 2 session in that it includes all packets transferred over a link that was established using PPP negotiation. An IP session is Layer 3 because it includes all IP packets exchanged with a subscriber device at a single IP address. Whether a session is Layer 2 or Layer 3 will, to some extent, determine the type of polices that may be activated for the session.

ISG also provides flexibility in terms of how an IP session is defined for an interface. For example, on a particular interface, ISG can be provisioned to classify IP sessions on the basis of a single address (an IP session), a subnet (an IP subnet session), or the interface itself (an IP interface session), wherein all IP packets transferred over the interface are encompassed by the same session.

In a network deployment, ISG session types should be provisioned to represent individual subscriber entities. For example, a particular ISG interface may be directly connected to a subscriber household in which several subscriber devices with individual IP addresses are attached to a household LAN. If the plan is to model each LAN-attached device as a separate subscriber and apply different policies and services to each, the interface should be provisioned to expect IP sessions. However, if the household represents a single subscriber account, and common handling is required for all packets exchanged, the interface should be provisioned as an IP interface or subnet session.

Subscriber Access

Under ISG, the provisioning and handling of specific access media and protocols is decoupled as far as possible from the functionality that is applicable to all session types. This model has the following benefits:

- A common set of subscriber services may be used on an ISG at which heterogeneous subscriber networks are aggregated.
- A common set of subscriber services may be used for multiple ISGs, even when the access technology differs.
- For a given subscriber, the access method may be altered (through provisioning or roaming) without any need to change the service provisioning.
- As new access protocols become available, they can be leveraged by existing edge deployments without requiring changes to the service content; new access protocols plug into the ISG framework.

Subscriber Identification

A subscriber session is created when the first control protocol packet is received from the subscriber device. The control protocol will vary depending on the session type. If there is no control protocol, the session is signaled by the first data packet from the subscriber.

At session start, certain identity information is available, although typically not enough to completely identify the subscriber. Through the use of control policies, the identity information available at session start can be used to drive the extraction of further identity from the subscriber and determine new policy for the session. The following example illustrates how ISG might handle subscriber identity:

- For an IP session, where session start is signaled by a DHCP protocol event, a TCP redirection policy could be activated. This policy would facilitate the collection of a username and credential at an external web portal.

Subscriber Services

An ISG service is a collection of policies applicable to a subscriber session. When a service is activated on a session, all policies contained within that service are activated on the session. Likewise, when a service is deactivated, all policies that are contained within the service are deactivated or removed from the session.

Services are useful for handling fixed policy combinations that are applicable to a number of subscribers. This application reduces duplication of persistent data and allows a group of policies to be activated with a single action and a single reference.

A service may be defined on the edge device directly, through the command-line interface (CLI), or in an external repository and downloaded as required. A downloaded service definition is cached on the device for as long as it is active on one or more sessions.

A service may be activated in one of the following ways:

- As a result of control policy execution
- By receipt of a CoA service-logon command
- By reference in a user profile, where the service is flagged for automatic activation

Services primarily contain traffic policies. There are some restrictions regarding the policies that may be combined in a given service; for example, a service may not contain two traffic policies that specify a different nondefault traffic class unless they apply to different traffic directions (inbound versus outbound).

Where a service contains a network-forwarding policy, it is known as a *primary service* . Only one primary service may be active for a given session at any point in time; that is, primary services are mutually exclusive.

Policies

ISG introduces support for two basic policy types:

- Traffic policies
- Control policies

Traffic policies define the handling of data packets and consist of a traffic class, which defines the packet-based criteria for which the policy is applicable, and one or more traffic actions, which are functional instances that perform specific operations on a data stream and are often referred to as *features* . The traffic actions configured within a traffic policy are invoked for data packets that meet the criteria defined by the traffic class.

Network-forwarding policies are a specific type of traffic policy, for which the action is a network-forwarding action, such as to route packets using a specific virtual routing and forwarding instance (VRF) or to forward packets over a Layer 2 connection. Network-forwarding policies are “classless” in that it is not possible to refine the criteria for which the forwarding action is applicable.

Control policies define the handling of system events and consist of one or more control policy rules and a decision strategy that governs how the constituent policy rules are evaluated. A control policy rule consists of a control class (a flexible condition clause), an event for which the condition is evaluated, and one or more control actions. Control actions are general system functions, such as “authenticate” or “activate a service.”

Control policies may be activated on various targets, such as interfaces or ATM virtual circuits (VCs), and typically control the extraction and authentication of subscriber identity and the activation of services on sessions. Traffic policies may be activated only on sessions and are typically (though not always) applied through service activation.

Control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies represent an intuitive and extensible framework for specifying system behavior. As additional functionality is added to the system, an administrator just has to learn what new events and actions can be included in a control policy, not a completely new set of configuration commands.

Dynamic Policy Updates

Traditionally, subscriber policy has been determined at one point only, at session establishment time, once the principal identity of a subscriber has been authenticated. ISG introduces a dynamic policy model in which session policy may be altered at any time.

Session policy is evaluated at session start and may be reassessed whenever additional identity or service selection information is gleaned from the subscriber via the access protocol. In addition, policy may be updated for a session through the activation of control policies or by means of CoA commands from an external application. In the latter case, the external application may update policy as a result of administrator activity, back-end processing, or subscriber activity (such as service selection at a web portal).

Benefits of ISG

ISG provides the following benefits:

- A common system for session management across Cisco products and access technologies. New access protocols, forwarding protocols, and features may be plugged in with minimal impact and maximum potential for reuse.
- Separation of the concerns of subscriber identification, service application, and subscriber access and session type.
- Flexible session definitions.
- Flexible session detection.
- Flexible, iterative approach to identification, service activation, and policy activation.
- Different trust levels. Session authorization is not contingent on authentication.
- Control policies. Control policies facilitate distributed policy decision-making, reducing round-trip latency between the edge device and policy server, and allow system event handling to be described in a consistent and intuitive manner.
- Common policy model and language for control and traffic policy.
- Provision for dynamic policy updates via CoA (through service activation or “policy push”).
- Use of existing Cisco IOS infrastructure to provide session functionality.
- Use of existing Cisco IOS infrastructure to track session state and life cycle.
- Creation of a session context at first instance of subscriber interaction, thereby facilitating the immediate application of policy to subscriber traffic.
- Flexible distribution of service data.
- Range of accounting options, including prepaid accounting, postpaid accounting, tariff switching for prepaid and postpaid accounting, interim accounting, event-based accounting, and flow-based accounting.
- Single sign-on services to an external application.
- Flexible infrastructure in support of “equal-access” deployments, such as service-based Dynamic Host Configuration Protocol (DHCP) pool and DHCP server determination, dynamic readdressing through DHCP, and VRF transfer.
- Support for standard external interfaces, such as RADIUS and CoA.

Planning for ISG Implementation

ISG is very flexible and supports a wide variety of functionality. Before you begin to configure ISG, you should plan your system carefully. The following sections describe some of the important aspects of your system that you should consider:

- Trust Model, page 6
- Subscriber Access Model, page 6
- Single Sign-On Requirements, page 6
- Network Forwarding, page 6
- Service Packaging, page 6
- Billing Model, page 7

Trust Model

Trust levels are determined by the security needs of a particular application domain and the inherent security afforded by the subscriber network. In the following situations, it may not be necessary to authenticate subscriber identity:

- When security is not considered paramount
- When end-to-end security is provided in-band
- When the subscriber network is intrinsically secure

Whether or not subscribers must be authenticated will influence the choice of access protocol. When authentication is not required, control policies may be used to determine authorization and other session policy on the basis of subscriber identity.

Where authentication is considered necessary, the authenticated identity may be trusted:

- For the duration of the session
- Until a periodic reauthentication is instigated
- Beyond the duration of a session; for example, for the lifetime of a subscription

For complete security, cryptographic methods may be used to secure the session (to the edge) following authentication, obviating the need for reauthentication. However, there are administrative and performance overheads associated with this practice.

Subscriber Access Model

The trust model will, to a large extent, determine the choice of access protocol. However, the access model will also depend on other factors such as the underlying media (for example, ATM versus Ethernet), type of endpoint (for example, PC, cell phone, PDA), mobility requirements, the system's ability to influence the software installed on a subscriber device, and scalability requirements.

Single Sign-On Requirements

Where a subscriber will have access to services provided by other devices in the administrative domain of the access or service provider, is an additional authentication required, or should the identity of the subscriber be trusted? It may be necessary for the latter device to query the access device to collect additional subscriber identity information and ascertain whether the subscriber has already been authenticated by the access device. The single sign-on facility is provided through the "session query" capability of CoA.

Network Forwarding

How should subscribers be given access to network services? Network forwarding options include the following:

- Layer 2 connections; for example, a Layer 2 Tunneling Protocol (L2TP) tunnel to an L2TP network server (LNS)
- Layer 3 connections, by associating all session packets with a particular VRF or routing domain

Service Packaging

How should subscriber policies be organized into services, if at all? Some considerations for service packaging include the following:

- Are certain policy combinations common to multiple subscribers?
- Are shared policy combinations dependent on a particular forwarding domain?
- Is it necessary for a subscriber to move between service domains?
- Should services be defined on the device or in a remote repository? Externally defined services will be cached locally for as long as they are activated for one or more sessions.

Billing Model

How should subscribers be billed for service usage? Billing options include the following:

- Billing by usage of time or volume
- Billing in advance (prepaid) or at regular intervals (traditional postpaid)
- Billing according to policies provisioned for the session
- Billing according to the time of day (tariff switching)

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Overview of ISG

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

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

Table 1 Feature Information for the Overview of ISG

Feature Name	Releases	Feature Configuration Information
ISG:Session: Auth: Single Sign-on	Cisco IOS XE Release 2.2.	Single sign-on eliminates the need to authenticate a session more than once when a subscriber has access to services provided by other devices in the administrative domain of the access or service provider.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Control Policies

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG control policies are a means of defining the actions the system will take in response to specified conditions and events. A wide variety of system actions, conditions, and events can be combined using a consistent policy language, providing a flexible and precise way of configuring ISG. This module provides information about how to configure ISG control policies.

- Finding Feature Information, page 9
- Prerequisites for ISG Control Policies, page 9
- Restrictions for ISG Control Policies, page 9
- Information About ISG Control Policies, page 10
- How to Configure an ISG Control Policy, page 11
- Configuration Examples for ISG Control Policies, page 25
- Additional References, page 29
- Feature Information for ISG Control Policies, page 31

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Control Policies

Authentication, authorization, and accounting (AAA) method lists must be configured prior to defining authentication and authorization actions.

Restrictions for ISG Control Policies

Control policies are activated for specific contexts, not directly on sessions. Control policies apply to all sessions hosted on the context.

Only one control policy map may be applied to a given context.

Control policies can be defined only through the router’s command-line interface (CLI).

Not all actions may be associated with all events.

A new control class may not be inserted between existing control classes once a control policy map has been defined.

Information About ISG Control Policies

- Control Policies, page 10
- Uses of Control Policies, page 11

Control Policies

Control policies define the actions that the system will take in response to specified events and conditions. For example, a control policy can be configured to authenticate specific subscribers and then provide them with access to specific services.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed.

Three steps are involved in defining a control policy:

1 Create one or more control class maps.

A control class map specifies the conditions that must be met for a policy to be activated, and, optionally, the event that causes the class to be evaluated. A control class map may contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the individual conditions must evaluate true in order for the class to evaluate true.

1 Create a control policy map.

A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

1 Apply the control policy map.

A control policy map is activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts. In the following list, the context types are listed in order of precedence. For example, a control policy map that is applied to a PVC takes precedence over a control policy map that is applied to an interface.

- ◦ Permanent virtual circuit (PVC)
  - Virtual circuit (VC) class
  - Virtual template
  - Subinterface
  - Interface
  - Global

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts.

Note Traffic policies are another type of policy used by ISG. Traffic policies define the handling of data packets and are configured in service policy maps or service profiles. For more information about traffic policies, see the "Configuring ISG Subscriber Services" module.

- Differentiated Initial Policy Control, page 11

Differentiated Initial Policy Control

Authentication failure for a subscriber may happen for an access-reject (which means a RADIUS server responded with a Reject) or due to an access request timeout (RADIUS server is unreachable).

Using ISG control policies, and actions configured for the 'radius-timeout' and 'access-reject' events, the system can distinguish between the different reasons for an authentication failure. Different events are thrown by the system (for example, a received authentication reject or an unavailable RADIUS server event). This allows the control policy to specify different actions for each type of authentication failure. For example, if the RADIUS server is down or unreachable, temporary access can be given to subscribers.

This feature is available only for IP-based sessions for subscriber authentication. This feature does not support the Point-to-Point Protocol over Ethernet (PPPoE) sessions.

Uses of Control Policies

Use control policies to configure an ISG to perform specific actions in response to specific events and conditions. For example, control policies could be used for the following purposes:

- To activate a default service when a subscriber session is first detected
- To sequence the gathering of subscriber identity, where a control protocol exists on the access side
- To determine how the system responds to an idle timeout or to a subscriber who has run out of credit
- To enable transparent automatic login, which enables authorization on the basis of an IP address or MAC address
- To configure the maximum amount of time a session can remain unauthenticated
- To send periodic session state information to other devices

How to Configure an ISG Control Policy

- Configuring a Control Class Map, page 11
- Configuring a Control Policy Map, page 17
- Applying the Control Policy Map, page 21
- Monitoring and Maintaining ISG Control Policies, page 24

Configuring a Control Class Map

A control class map contains conditions that must be met for a control policy to be executed. A control class map can contain one or more conditions. Perform this task to configure a control class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control** [**match-all**|**match-any**|**match-none**] *class-map-name*
4. **available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
5. **greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
6. **greater-than-or-equal** [**not**]**nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
7. **less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
8. **less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
9. **match authen-status** {**authenticated** | **unauthenticated**}
10. **match authenticated-domain** {*domain-name* | **regexp** *regular-expression*}
11. **match authenticated-username** {*username* | **regexp** *regular-expression*}
12. **match dnis** {*dnis* | **regexp** *regular-expression*}
13. **match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}
14. **match mlp-negotiated** {**no** | **yes**}
15. **match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate**| **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
16. **match no-username** {**no** | **yes**}
17. **match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}
18. **match service-name** {*service-name* | **regexp** *regular-expression*}
19. **match source-ip-address** *ip-address subnet-mask*
20. **match timer** {*timer-name* | **regexp** *regular-expression*}
21. **match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*}
22. **match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*}
23. **match unauthenticated-username** {*username* | **regexp** *regular-expression*}
24. **match vrf** {*vrf-name* | **regexp** *regular-expression}*

DETAILED STEPS

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

Step 3	**class-map type control** [**match-all**|**match-any**|**match-none**] *class-map-name*
	Example:
	`Router(config)# class-map type control match-all class1`
		Creates or modifies a control class map, which defines the conditions under which the actions of a control policy map will be executed, and enters control class map mode.

Step 4	**available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
	Example:
	`Router(config-control-classmap)# available nas-port`
		(Optional) Creates a condition that evaluates true if the specified subscriber identifier is locally available.

Step 5	**greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# greater-than nas-port type atm vpi 200 vci 100`
		(Optional) Creates a condition that evaluates true if the subscriber network access server (NAS) port identifier is greater than the specified value.

	Command or Action	Purpose

Step 6	**greater-than-or-equal** [**not**]**nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# greater-than-or-equal nas-port vlan 10`
		(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is greater than or equal to the specified value.

Step 7	**less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# less-than nas-port type atm vpi 200 vci 105`
		(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than the specified value.

Step 8	**less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# less-than-or-equal nas-port ipaddr 10.10.10.10`
		(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than or equal to the specified value.

Step 9	**match authen-status** {**authenticated** | **unauthenticated**}
	Example:
	`Router(config-control-classmap)# match authen-status authenticated`
		(Optional) Creates a condition that evaluates true if a subscriber’s authentication status matches the specified authentication status.

Step 10	**match authenticated-domain** {*domain-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match authenticated-domain cisco.com`
		(Optional) Creates a condition that evaluates true if a subscriber’s authenticated domain matches the specified domain.

	Command or Action	Purpose

Step 11	**match authenticated-username** {*username* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match authenticated-username regexp "admin@.*com"`
		(Optional) Creates a condition that evaluates true if a subscriber's authenticated username matches the specified username.

Step 12	**match dnis** {*dnis* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match dnis reg-exp 5551212`
		(Optional) Creates a condition that evaluates true if a subscriber's Dialed Number Identification Service number (DNIS number, also referred to as *called-party number*) matches the specified DNIS number.

Step 13	**match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}
	Example:
	`Router(config-control-classmap)# match media atm`
		(Optional) Creates a condition that evaluates true if a subscriber's access media type matches the specified media type.

Step 14	**match mlp-negotiated** {**no** | **yes**}
	Example:
	`Router(config-control-classmap)# match mlp-negotiated yes`
		(Optional) Creates a condition that evaluates true or false depending on whether the subscriber's session was established using multilink PPP negotiation.
		• If the **yes** keyword is used, the condition evaluates true if the subscriber's session was established using multilink PPP negotiation.

Step 15	**match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate**| **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# match nas-port type ether slot 3`
		(Optional) Creates a condition that evaluates true if a subscriber's NAS port identifier matches the specified value.

	Command or Action	Purpose

Step 16	**match no-username** {**no** | **yes**}
	Example:
	`Router(config-control-classmap)# match no-username yes`
		(Optional) Creates a condition that evaluates true or false depending on whether or not a subscriber's username is available.
		• If the **yes** keyword is used, the condition evaluates true if the subscriber's username is not available.

Step 17	**match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}
	Example:
	`Router(config-control-classmap)# match protocol ip`
		(Optional) Creates a condition that evaluates true if a subscriber's access protocol type matches the specified protocol type.

Step 18	**match service-name** {*service-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match service-name service1`
		(Optional) Creates a condition that evaluates true if the service name associated with a subscriber matches the specified service name.

Step 19	**match source-ip-address** *ip-address subnet-mask* **Example:** `Router(config-control-classmap)# match source-ip-address 10.10.10.10 255.255.255.255`	(Optional) Creates a condition that evaluates true if a subscriber's source IP address matches the specified IP address.

Step 20	**match timer** {*timer-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match timer TIMERA`
		(Optional) Creates a condition that evaluates true upon expiry of a specified policy timer.

Step 21	**match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match tunnel-name regexp L.*`
		(Optional) Creates a condition that evaluates true if a subscriber's virtual private dialup network (VPDN) tunnel name matches the specified tunnel name.

Step 22	**match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match unauthenticated-domain example.com`
		(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated domain name matches the specified domain name.

	Command or Action	Purpose

Step 23	**match unauthenticated-username** {*username* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match unauthenticated-username regexp examplename1`
		(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated username matches the specified username.

Step 24	**match vrf** {*vrf-name* | **regexp** *regular-expression}*
	Example:
	`Router(config-control-classmap)# match vrf regexp examplename2`
		(Optional) Creates a condition that evaluates true if a subscriber's VPN routing and forwarding (VRF) matches the specified VRF.

Configuring a Control Policy Map

A control policy map contains one or more control policy rules that associate a control class with one or more actions. Perform this task to configure a control policy map.

Note The actions that can be configured in a policy rule depend on the type of event that is specified by the **class type control** command. For example, if the **account-logoff** event is specified, the only action that can be configured in that policy rule is **service**. The procedure in this section shows all actions that can be configured in a policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} [**event** {**access-reject**| **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed**| **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]
5. *action-number* **authenticate aaa list** *list-name*
6. *action-number* **authorize use method** {**aaa**|**legacy**|**rm**|**sgf**|**ssg**|**xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect**| **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id**| **source-ip-address** | **tunnel-name**| **unauthenticated-domain** | **unauthenticated-username**|**vendor-class-id**}
7. *action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username** | **vrf**}
8. *action-number* **if upon network-service-found** {**continue** | **stop**}
9. *action-number* **proxy accounting aaa list** {*list-name*| **default**}
10. *action-number* **service** [**disconnect** | **local** | **vpdn**]
11. *action-number* **service-policy type control** *policy-map-name*
12. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
13. *action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address**| **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**| **vrf**}
14. *action-number* **set-timer** *name-of-timer minutes*
15. *action-number* **substitute** *name matching-pattern pattern-string*
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control MY-POLICY`	Creates or modifies a control policy map, which is used to define a control policy.

Step 4	**class type control** {*control-class-name* | **always**} [**event** {**access-reject**| **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed**| **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]
	Example:
	`Router(config-control-policymap)# class type control always event session-start`
		Specifies a control class for which actions may be configured.
		• A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.

Step 5	*action-number* **authenticate aaa list** *list-name* **Example:** `Router(config-control-policymap-class-control)# 1 authenticate aaa list LIST1`	(Optional) Initiates an authentication request.

Step 6	*action-number* **authorize use method** {**aaa**|**legacy**|**rm**|**sgf**|**ssg**|**xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect**| **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id**| **source-ip-address** | **tunnel-name**| **unauthenticated-domain** | **unauthenticated-username**|**vendor-class-id**}
	Example:
	`Router(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`
		(Optional) Initiates a request for authorization on the basis of the specified identifier.

	Command or Action	Purpose

Step 7	*action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username** | **vrf**}
	Example:
	`Router(config-control-policymap-class-control)# 1 collect identifier authen-status`
		(Optional) Collects the specified subscriber identifier from the access protocol.

Step 8	*action-number* **if upon network-service-found** {**continue** | **stop**}
	Example:
	`Router(config-control-policymap-class-control)# 2 if upon network-service-found stop`
		(Optional) Specifies whether the system should continue processing policy rules once the subscriber's network service has been identified.

Step 9	*action-number* **proxy accounting aaa list** {*list-name*| **default**} **Example:** `Router(config-control-policymap-class-control)# 1 proxy accounting aaa list default`	(Optional) Specifies the list that the request should be proxied to.
Step 10	*action-number* **service** [**disconnect** | **local** | **vpdn**] **Example:** `Router(config-control-policymap-class-control)# 3 service disconnect`	(Optional) Specifies a network service type for PPP sessions.
Step 11	*action-number* **service-policy type control** *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# service-policy type control domain based access`	(Optional) Nests the specified control policy map within a parent control policy map.

	Command or Action	Purpose

Step 12	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** |**unauthenticated-domain** | **unauthenticated-username**}}
	Example:
	`Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`
		(Optional) Activates an ISG service.
		• Specifying an identifier instead of a service name will activate a service that has the same name as the specified identifier.

Step 13	*action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address**| **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**|**vrf**}
	Example:
	`Router(config-control-policymap-class-control)# 1 set APJ identifier authen-status`
		(Optional) Sets a variable name.

Step 14	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Router(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	(Optional) Starts a named policy timer. • Expiration of the timer generates the event timed-policy-expiry.
Step 15	*action-number* **substitute** *name matching-pattern pattern-string* **Example:** `Router(config-control-policymap-class-control)# 1 substitute TPK SUBA SUBB`	(Optional) Substitutes a matching pattern in variable content by a rewrite pattern.

Step 16	**end**
	Example:
	`Router(config-control-policymap-class-control)# end`
		(Optional) Ends the current configuration session and returns to privileged EXEC mode.

Applying the Control Policy Map

A control policy map must be activated by applying it to a context. Perform one or more of the following tasks to apply a control policy to a context:

- Applying a Control Policy Map Globally on the Router, page 22
- Applying an ISG Control Policy Map to an Interface or Subinterface, page 22

- Applying an ISG Control Policy Map to a Virtual Template, page 23

Applying a Control Policy Map Globally on the Router

Perform this task to apply a control policy globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-policy type control** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service-policy type control** *policy-map-name* **Example:** `Router(config)# service-policy type control policy1`	Applies a control policy.

Applying an ISG Control Policy Map to an Interface or Subinterface

Perform this task to apply an ISG control policy to an interface or subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**.** *subinterface-number*]
4. **service-policy type control** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [**.** *subinterface-number*] **Example:** `Router(config)# interface gigabitethernet 0/0/1.1`	Specifies an interface and enters interface configuration mode.
Step 4	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control policy1`	Applies a control policy.

Applying an ISG Control Policy Map to a Virtual Template

Perform this task to apply an ISG control policy map to a virtual template.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **service-policy type control** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template0`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control policy1`	Applies a control policy.

Monitoring and Maintaining ISG Control Policies

Optionally, you can perform this task to monitor and maintain ISG control policy operation. Steps can be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show class-map type control**
3. **show policy-map type control**
4. **clear class-map control**
5. **clear policy-map control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show class-map type control** **Example:** `Router# show class-map type control`	Displays information about ISG control class maps. - The display includes statistics on the number of times a particular class has been evaluated and what the results were.
Step 3	**show policy-map type control** **Example:** `Router# show policy-map type control`	Displays information about ISG control policy maps. - The display includes statistics on the number of times each policy rule within the policy map has been executed.
Step 4	**clear class-map control** **Example:** `Router# clear class-map control`	Clears the control class map counters.
Step 5	**clear policy-map control** **Example:** `Router# clear policy-map control`	Clears the control policy map counters.

Configuration Examples for ISG Control Policies

- Control Policy for Layer 2 Access and Service Provisioning Example, page 25
- Verifying a Control Policy Examples, page 26
- Control Policy for Restricting Access on the Basis of Interface and Access Media Example, page 28
- Control Policies for Automatic Subscriber Login Example, page 29

Control Policy for Layer 2 Access and Service Provisioning Example

The following example shows how to configure a control policy that produces the following results:

- VPDN forwarding is applied to anyone dialing in from “example1.com”.
- Access to locally terminated Layer 3 network resources is provided to anyone dialing in from “example2.com”.
- Anyone else is barred.

```
! Configure the control class maps.
class-map type control match-all MY-FORWARDED-USERS
```

```
 match unauthenticated-domain "example1.com"
!

class-map type control match-all MY-LOCAL-USERS
 match unauthenticated-domain "example2.com"
!
! Configure the control policy map.
policy-map type control MY-POLICY
 class type control MY-FORWARDED-USERS event session-start
  1 service-policy type service identifier nas-port
  2 service local
!
 class type control MY-LOCAL-USERS event session-start
  1 service local
!
 class type control always event session-start
  2 service disconnect
!
! Apply the control policy to dialer interface 1.
interface Dialer1
 service-policy type control MY-POLICY
```

Verifying a Control Policy Examples

The following examples show sample output generated from the configuration in the Control Policy for Layer 2 Access and Service Provisioning Example:

```
Router# show users

Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
Interface User Mode Idle Peer Address
Vi1.1 user1@xyz.com PPPoE - 10.1.126.14
Vi1.2 user2@abc.com PPPoE - 10.1.126.15

Router# show subscriber session

Current Subscriber Information: Total sessions 2
Uniq ID Interface State Service Identifier Up-time
2022 Vi1.1 authen Local Term user1@xyz.com 00:08:41
2023 Vi1.2 authen Local Term user2@abc.com 00:08:40
MCP_BBA_8#show subscriber session
MCP_BBA_8#show subscriber session uid 2022 detailed
Unique Session ID: 2022
Identifier: user1@xyz.com
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:08:57, Last Changed: 00:08:57
Interface: Virtual-Access1.1
Policy information:
Context 2C655DF0: Handle A2070D8D
AAA_id 00007DE8: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Downloaded User profile, including services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Config history for session (recent to oldest):
Access-type: PPP Client: SM
Policy event: Process Config Connecting
Profile name: apply-config-only, 3 references
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
```

```
ssg-account-info ''QU;10000;D;20000''
Rules, actions and conditions executed:
subscriber rule-map ppp-users
condition always event session-start
1 collect identifier unauthenticated-domain
2 service-policy type control MY-POLICY
subscriber condition-map match-all MY-FORWARDING-USERS
match identifier unauthenticated-domain xyz.com [TRUE]
subscriber rule-map MY-POLICY
condition MY-FORWARDING-USERS event session-start
1 service local
subscriber rule-map ppp-users
condition always event session-start
2 service-policy type control MY-POLICY
Session inbound features:
Feature: Policing
Upstream Params:
Average rate = 10000, Normal burst = 1875, Excess burst = 3750
Config level = Per-user
Session outbound features:
Feature: Policing
Dnstream Params:
Average rate = 20000, Normal burst = 3750, Excess burst = 7500
Config level = Per-user
Non-datapath features:
Feature: Session Timeout
Timeout value is 720 seconds
Time remaining is 00:02:56
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:09:03
Router# show subscriber session uid 2023 detailed
Unique Session ID: 2023
Identifier: user2@abc.com
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:09:17, Last Changed: 00:09:17
Interface: Virtual-Access1.2
Policy information:
Context 2C656120: Handle F4070D8E
AAA_id 00007DE9: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Downloaded User profile, including services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Config history for session (recent to oldest):
Access-type: PPP Client: SM
Policy event: Process Config Connecting
Profile name: apply-config-only, 3 references
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Rules, actions and conditions executed:
subscriber rule-map ppp-users
condition always event session-start
1 collect identifier unauthenticated-domain
2 service-policy type control MY-POLICY
subscriber condition-map match-all MY-FORWARDING-USERS
match identifier unauthenticated-domain xyz.com [FALSE]
subscriber rule-map MY-POLICY
condition MY-FORWARDING-USERS event session-start
subscriber condition-map match-all MY-LOCAL-USERS
match identifier unauthenticated-domain abc.com [TRUE]
subscriber rule-map MY-POLICY
condition MY-LOCAL-USERS event session-start
1 service local
```

```
subscriber rule-map ppp-users
condition always event session-start
2 service-policy type control MY-POLICY
Session inbound features:
Feature: Policing
Upstream Params:
Average rate = 10000, Normal burst = 1875, Excess burst = 3750
Config level = Per-user
Session outbound features:
Feature: Policing
Dnstream Params:
Average rate = 20000, Normal burst = 3750, Excess burst = 7500
Config level = Per-user
Non-datapath features:
Feature: Session Timeout
Timeout value is 720 seconds
Time remaining is 00:02:40
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:09:19
```

Control Policy for Restricting Access on the Basis of Interface and Access Media Example

This example shows how to configure a control policy to allow access only to users who enter the router from a particular interface and access type. In this case, only PPPoE users will be allowed; everyone else is barred.

The first condition class map “MATCHING-USERS” evaluates true only if all of the lines within it also evaluate true; however, within “MATCHING-USERS” is a nested class map (second condition), “NOT-ATM”. This nested class map represents a subcondition that must also evaluate to true. Note that the class map “NOT-ATM” specifies “match-none”. This means that “NOT-ATM” evaluates to true only if every condition line within it evaluates to false.

The third condition specifies matching on the NAS port associated with this subscriber. Specifically, only subscribers that arrive on a Gigabit Ethernet interface and on slot 3 will evaluate to true.

```
! Configure the control class maps.
class-map type control match-all MATCHING-USERS
 class type control NOT-ATM
 match media ether
 match nas-port type ether slot 3
!
class-map type control match-none NOT-ATM
 match media atm
!
```

If the conditions in the class map “MATCHING-USERS” evaluate to true, the first action to be executed is to authenticate the user. If authentication is successful, the service named “service1” will be downloaded and applied. Finally, a Layer 3 service is provided.

If “MATCHING-USERS” is not evaluated as true, the “always” class will apply, which results in barring anyone who does not match “MATCHING-USERS”.

```
! Configure the control policy map.
policy-map type control my-pppoe-rule
 class type control MATCHING-USERS event session-start
  1 authenticate aaa list XYZ
  2 service-policy type service service1
  3 service local
!
```

class type control always

```
  1 service disconnect
```

```
!
! Apply the control policy to an interface.
interface gigabitethernet3/0/0
 service-policy type control my-pppoe-rule
```

Finally, the policy is associated with an interface.

Default Method Lists

If you specify the default method list for any of the control policy actions, the default list will not display in the output from the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

The following will display in the output from the **show running-config** command:

```
1 authenticate
```

Control Policies for Automatic Subscriber Login Example

In the following example, if the client is from the a subnet, automatic subscriber login is applied and an authorization request is sent to the list TALLIST with the subscriber’s source IP address as the username. If the authorization request is successful, any automatic activation services specified in the returned user profile are activated for the session and the execution of rules within the control policy stops. If the authorization is not successful, the rule execution proceeds, and the subscriber is redirected to the policy server to log in. If the subscriber does not log in within five minutes, the session is disconnected.

```
interface GigabitEthernet0/0/0
 service-policy type control RULEA
aaa authentication login TALLIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any
class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100
```

policy-map type service redirectprofile

```
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080
class-map type control match-all CONDA
 match source-ip-address 209.165.201.1 255.255.255.0
!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 apply aaa list LOCAL service redirectprofile
  3 set-timer TIMERB 5 minutes
 class type control CONDF event timed-policy-expiry
```

1 service disconnect

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
Traffic Policies	"Configuring ISG Subscriber Services" module in this guide

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Control Policies

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

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

Table 2 Feature Information for ISG Control Policies

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Policy: Domain Based (Autodomain, Proxy)	Cisco IOS XE Release 2.2	ISG control policies manage the primary services and rules used to enforce particular contracts. These policies include programmable interfaces to dynamic triggers and conditional logic to be applied to flows within a session, or other characteristics of a session, upon meeting the policy criteria. Policies can be configured to interpret the domain as a request to activate the service associated with that domain name, allowing users to automatically receive services in accordance with the domain to which they are attempting to connect.
ISG: Policy Control: Policy: Triggers	Cisco IOS XE Release 2.2	ISG control policies can be configured with time-based, volume-based, and duration-based policy triggers. Time-based triggers use an internal clock, allowing policies to be applied at specific times. Volume-based triggers are based on packet count; when the packet count reaches a specified value, the specified policy is applied. Duration-based triggers are based on an internal timer. Upon expiration of the timer, the specified policy is applied.

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Multidimensional Identity per Session	Cisco IOS XE Release 2.2	ISG control policies provide a flexible way to collect pieces of subscriber identity information during session establishment. Control policies also allow session policy to be applied iteratively as more elements of identity information become available to the system.
ISG: Policy Control: Cisco Policy Language	Cisco IOS XE Release 2.2	ISG control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies provide an intuitive and extensible framework, with a consistent set of CLI commands, for specifying system behavior.
ISG: Policy Control: Differentiated Initial Policy Control	Cisco IOS XE Release 2.5.0	This features provides the ability to distinguish RADIUS authentication rejects from RADIUS server unavailability. It allows minimal or temporary network access to the subscribers when the RADIUS servers are down or cannot be accessed because of network problems or when an authentication reject is received for a subscriber. In Cisco IOS Release 12.2(33)XNE, support was added for the Cisco 10000 Series Routers. The following command was introduced or modified:**class type control**.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Access for PPP Sessions

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document provides information about how to configure ISG access for Point-to-Point Protocol (PPP) subscribers.

- Finding Feature Information, page 35
- Prerequisites for ISG Access for PPP Sessions, page 35
- Restrictions for ISG Access for PPP Sessions, page 35
- Information About ISG Access for PPP Sessions, page 36
- How to Configure ISG Access for PPP Sessions Using Control Policies, page 37
- Configuration Examples for ISG Access for PPP Sessions, page 42
- Additional References, page 45
- Feature Information for ISG Access for PPP Sessions, page 46

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Access for PPP Sessions

The specific access protocol that is being used must be provisioned on the interface.

If local PPP authentication is required, the **ppp authentication** command must be configured on the interface or virtual template.

The tasks and examples in this document assume that you know how to configure and use ISG control policies. See the module “Configuring ISG Control Policies” for information about how to configure control policies.

Restrictions for ISG Access for PPP Sessions

In Cisco IOS XE, SSO and ISSU are not supported for the following features on ISG PPP sessions:

- Port-Bundle Host Key
- Layer 4 Redirect
- Traffic Class
- Accounting

The idle timeout value configured with the **ppp timeout idle** command in a virtual template applies to a PPP session even when the session is forwarded.

Information About ISG Access for PPP Sessions

- Overview of ISG Access for PPP Sessions, page 36
- ISG Subscriber IP Address Management for PPP Sessions, page 36
- VRF Transfer for PPP Sessions, page 37
- Default Policy for ISG Access for PPP Sessions, page 37

Overview of ISG Access for PPP Sessions

Layer 2 sessions are established by means of control protocols that operate between the peer entities and the ISG device. Typically, Layer 2 sessions are encapsulated to isolate them from other sessions on the same physical media.

Although the system provides default handling for Layer 2 sessions, you may want to configure policies to forward or locally terminate the protocol or to locally authenticate subscribers on the basis of identity data that is collected from the access protocol. ISG control policies can be configured to extract identity and credentials of peer entities from access protocols. This mechanism allows services to be provisioned for Layer 2 sessions on the basis of any identity pertaining to the session, whether explicitly provided via the protocol or native to the underlying media or access port.

ISG supports the following Layer 2 access protocols:

- PPP
- PPP over Ethernet (PPPoE)
- Layer 2 Tunnel Protocol (L2TP)

ISG Subscriber IP Address Management for PPP Sessions

ISG subscriber IP address management applies to IP sessions or Layer 2 (PPP) sessions that are terminated locally.

For a subscriber to be routable within a given IP service domain, the subscriber must present a domain-specific IP address to the network. If a subscriber transfers between IP service domains (which includes any private domain managed by the access provider), the IP address presented to the network must change to reflect the new domain. For locally terminated PPP sessions, ISG supports the following methods of IP address assignment:

- IP address in a user profile
- IP subnet in a user profile
- Named address pool in a user profile
- Local address pools
- Standard methods of IP address management for PPP

When a locally terminated PPP session is transferred from one virtual routing and forwarding (VRF) instance to another VRF, the peer IP address is renegotiated using IPCP.

VRF Transfer for PPP Sessions

VRF transfer enables an ISG subscriber session to move from one VRF to another following selection of a new primary service. Once a PPP session comes up with the IP address from the network access point (NAP), the subscriber can access a web portal and choose a service provider. On VRF transfers in PPP sessions, ISG must reassign the IP address from the new domain to the PPP session. In PPP sessions, the IP address is reassigned by IP Control Protocol (IPCP) renegotiation.

Without PPP renegotiation, VRF transfer is not supported for PPP sessions.

Default Policy for ISG Access for PPP Sessions

ISG provides default handling of Layer 2 sessions in the absence of a configured control policy. If the **vpdn enable** command is configured and a domain name is specified in the username (for example, user@domain) or a Dialed Number Identification Service (DNIS) number has been provided, the system will perform authorization on the basis of this information. If virtual private dialup network (VPDN) tunnel information is found, the session will be forwarded for handling at an L2TP network server (LNS). If authentication is required by the remote LNS, the **ppp authentication** command must be configured at the PPP interface or virtual template. If the **vpdn authen-before-forward** command is configured, the system will attempt to authenticate the PPP session locally before forwarding it on to the LNS.

If tunnel information is not found for the domain name or DNIS or the **vpdn enable** command is not configured, Stack Group Bidding Protocol (SGBP) authorization will be attempted (if SGBP is configured). If no authorization information is located using SGBP, the PPP session will be terminated locally. Local termination means that the PPP session will be established between the peer and the ISG device, and the IP payload will be routed. In the latter case, authentication will occur only if the **ppp authentication** command is configured on the PPP interface or virtual template.

If an ISG control policy is defined for the session-start event, that policy will override the default handling.

How to Configure ISG Access for PPP Sessions Using Control Policies

To configure ISG Layer 2 access, perform the following steps:

1. Decide how you want Layer 2 session handling to be influenced by subscriber identity. Do you want to forward the protocol or terminate it locally? Do you want to authenticate subscribers locally?
2. Configure control policies to provide Layer 2 session handling. See the module "Configuring ISG Control Policies" for information about how to configure control policies. See the "Configuration Examples for ISG Access for PPP Sessions" section for an example of a control policy for Layer 2 access.
3. Enable ISG VRF transfer for PPP sessions.
4. Verify and troubleshoot the configuration as needed.

This section contains the following tasks:

- Enabling ISG VRF Transfer for PPP Sessions, page 38
- Verifying VRF Transfer for PPP Sessions, page 39
- Troubleshooting ISG Access for PPP Sessions, page 40

Enabling ISG VRF Transfer for PPP Sessions

VRF transfer enables an ISG subscriber session to move from one VRF to another when a new primary service is activated for a session. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

This procedure assumes that you have configured support for PPP sessions by configuring a virtual template and method of IP address allocation. Note that the original VRF, loopback interface, and IP address pool must be specified in a virtual template rather than in a user profile in order for VRF transfer to work. For information about how to configure virtual templates and support for PPP sessions, see the *Cisco IOS XEDial Technologies Configuration Guide.*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.

	Command or Action	Purpose
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF.
Step 5	**sg-service-type primary** **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service is a service that contains a network-forwarding policy. A primary service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.
Step 6	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	(Optional) Associates an ISG service with a service group. • A service group is a grouping of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.

Verifying VRF Transfer for PPP Sessions

Perform this task to verify VRF transfer for PPP sessions. All of the **show** steps are optional and may be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session all**
3. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
4. **show ip route** [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show subscriber session all** **Example:** `Router# show subscriber session all`	Displays information pertaining to the service chosen by the subscriber.

Step 3	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
	Example:
	`Router# show idmgr session key session-handle 48000002`
		Displays information related to ISG session and service identity.

Step 4	**show ip route** [**vrf** *vrf-name*] **Example:** `Router# show ip route`	Displays the current state of the routing table.

Troubleshooting ISG Access for PPP Sessions

The commands in this task can be used to monitor and troubleshoot Layer 2 sessions. All of these commands are optional and do not need to be entered in a particular order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session detailed**
3. **debug condition** *condition*
4. **debug subscriber packet** [**event**| **full**| **detail**]
5. **debug subscriber error**
6. **debug subscriber event**
7. **debug subscriber fsm**
8. **debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session detailed** **Example:** `Router# show subscriber session detailed`	Displays information about ISG subscriber sessions.
Step 3	**debug condition** *condition* **Example:** `Router# debug condition username user5@isp.com`	Filters debug output on the basis of the specified condition. **Note** See the module "Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging" for information about conditional debugging.
Step 4	**debug subscriber packet** [**event**| **full**| **detail**] **Example:** `Router# debug subscriber packet event`	Displays diagnostic information about packets during Subscriber Service Switch (SSS) call setup.
Step 5	**debug subscriber error** **Example:** `Router# debug subscriber error`	Displays diagnostic information about errors that can occur during SSS call setup.
Step 6	**debug subscriber event** **Example:** `Router# debug subscriber event`	Displays diagnostic information about SSS call setup events.
Step 7	**debug subscriber fsm** **Example:** `Router# debug subscriber fsm`	Displays diagnostic information about the SSS call setup state.

	Command or Action	Purpose

Step 8	**debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**}
	Example:
	`Router# debug ppp packet`
		Displays information on traffic and exchanges in an internetwork that is implementing the PPP.

Example

In the following example, the output of the **debug subscriber packet detail** command is filtered on the basis of the username "cpe6_1@isp.com":

```
Router# debug condition username cpe6_1@isp.com
Condition 1 set
Router# show debug

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on
Router# show debug
SSS:
  SSS packet detail debugging is on

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router#
```

Configuration Examples for ISG Access for PPP Sessions

- Configuring ISG Access for PPP Sessions Example, page 42
- VRF Transfer for PPP Sessions Using IPCP Renegotiation Example, page 44

Configuring ISG Access for PPP Sessions Example

The following example shows the configuration of an ISG policy that provides services to PPP subscribers. This example configures ISG to perform the following actions:

- PPP local termination

ISG will provide local termination by activating the service "ispa" for subscribers matching the domain "ispa". The system will authenticate the subscriber using method-list "list1". For local termination services, the global VRF is applied by default unless another VRF is specified in the service profile, on the interface, or in the virtual template.

- PPP authentication before forwarding

ISG will locally authenticate subscribers matching domain "ispb" before forwarding the sessions to an LNS. (Sessions are forwarded to an LNS because service policy map "ispb" specifies a VPDN group). The system will authenticate the subscribers using method-list "list2".

- PPP forwarding without local authentication

ISG will forward sessions to an LNS without local authentication for subscribers matching domain “ispc”.

- PPP domain exclusion

ISG will deny service to and disconnect the session for subscribers matching domain “ispd”.

- PPP domain-based service activation

For subscribers matching all other domains, ISG will activate a service that has the same name as the specified domain.

Configure control class maps, which define the conditions that must be met before a control policy rule will be executed.

```
class-map type control match-all PPP_SESSION
  match protocol ppp

class-map type control match-all NAS_PORT_CONDITION
  class type control match identifier name PPP_SESSION
  less-than identifier nas-port type atm vpi 200 vci 100
class-map type control match-all ISPA
  match unauthenticated-domain ispa

class-map type control match-all ISPB
  match unauthenticated-domain ispb

class-map type control match-all ISPC
  match unauthenticated-domain ispc

class-map type control match-all ISPD
  match unauthenticated-domain ispd
```

Define the top-level control policy map.

```
policy-map type control L2_ACCESS
```

Define a control policy rule that activates a forwarding service on the basis of the ATM VPI/VCI on which the call came in.

```
 class type control NAS_PORT_CONDITION event session-start
  1 service-policy type service xconnect
```

Define a control policy rule that collects the domain name from the protocol. The domain name is available from a structured user name (e.g., user@domain).

```
 class type control PPP_SESSION event session-start
  1 collect identifier unauthenticated-domain
  2 service-policy type control DOMAIN_BASED_ACCESS
```

Define the nested control policy.

```
policy-map type control DOMAIN_BASED_ACCESS
```

Define a control policy rule that provides local termination by activating the service “ispa”.

```
 class type control ISPA event session-start
  1 authenticate aaa list list1
  2 service-policy type service ispa
```

Define a control policy rule that configures the system to authenticate the subscriber locally before activating service “ispb”. The service “ispb” specifies forwarding the session to an LNS.

```
 class type control ISPB event session-start
  1 authenticate aaa list list2
  2 service-policy type service ispb
```

Define a control policy rule that activates service “ispc”, which specifies forwarding.

```
 class type control ISPC event session-start
  1 service-policy type service ispc
```

Define a control policy rule that results in session disconnection for subscribers that match service “ispd”.

```
 class type control ISPD event session-start
  service disconnect
```

Define a control policy rule that defines the default for all other domains, which is to activate a service having the same name as the specified domain.

```
 class type control always event session-start
    service-policy type service identifier unauthenticated-domain
```

Configure the service policy maps.

```
policy-map type service xconnect
  service vpdn group 1

policy-map type service ispa
  service local
  ip vrf forwarding red

policy-map type service ispb
  service vpdn group 2

policy-map type service ispc
  service vpdn group 3
```

Apply the control policy map globally.

```
service-policy type control L2_ACCESS
```

VRF Transfer for PPP Sessions Using IPCP Renegotiation Example

The following example shows a configuration that uses PPPoE to establish a session, and the RADIUS service profile that is created to associate the VRF. In this example, when a PPP session initially comes up, it belongs to the default routing table, and the IP address is assigned from the default IP address pool “DEF-POOL”. When the subscriber selects the “ISP-RED” service, ISG downloads the “ISP-RED” service profile and applies it to the session. The PPP session is then transferred to VRF “RED”. IPCP renegotiation occurs between the client device and the ISG device, and the subscriber is assigned a new IP address from the pool “POOL-RED”.

```
ip vrf RED
 rd 1:1
interface Loopback0
 ip address 10.0.0.1 255.255.255.0
interface Loopback1
 ip address 10.0.1.0 255.255.255.0
 ip vrf forwarding RED
!
```

```
interface Ethernet0/0
  pppoe enable
interface Virtual-Template1
 ip unnumbered Loopback0
 service-policy control RULE2
 peer default ip address pool DEF-POOL
 ppp authentication chap
ip local pool DEF-POOL 172.16.5.1 172.16.5.250
ip local pool POOL-RED 172.20.5.1 172.20.5.250
```

Service Profile for ISP RED

```
Cisco-AVpair = ip:vrf-id=RED
Cisco-AVpair = "ip:ip-unnumbered=loopback 1"
Cisco-AVpair = ip:addr-pool=POOL-RED
Cisco-AVpair = subscriber:sg-service-type=primary
Cisco-AVpair = subscriber:sg-service-group=RED-GROUP
Cisco-SSG-Service-Info = IPPPOE-RED
Cisco-SSG-Service-Info = R10.1.1.0;255.255.255.0
Framed-Protocol = PPP
Service-Type = Framed
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
AAA configuration tasks	The "Authentication" section in the *Cisco IOS XE Security Configuration Guide*
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" section in the *Cisco IOS XE Security Command Reference*
PPP configuration tasks	The “PPP Configuration” section in the *Cisco IOS XE Dial Services Configuration Guide*
PPP commands	*Cisco IOS XE Dial Services Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for ISG Access for PPP Sessions

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

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

Table 3 Feature Information for ISG Layer 2 Access

Feature Name	Releases	Feature Configuration Information
ISG:Session: Creation: P2P Session (PPPoE, PPPoXoX)	Cisco IOS XE Release 2.2	The ISG session is the primary context to which services and policies are associated across specific data flows. Point-to-point (P2P) sessions are established through a signaling protocol. ISG handles many variants of P2P encapsulation, such as PPP, PPPoE and PPPoA.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Access for IP Subscriber Sessions

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports IP sessions for subscribers who connect to ISG from Layer 2 or routed Layer 3 access networks. This module describes how to configure ISG to bring up IP subscriber sessions, manage subscriber IP addressing, and configure dynamic Virtual Private Network (VPN) selection.

Note This document assume that network address translation (NAT) is performed on a Layer 3 gateway other than the ISG.

- Finding Feature Information, page 49
- Prerequisites for ISG Access for IP Subscriber Sessions, page 49
- Restrictions for ISG Access for IP Subscriber Sessions, page 50
- Information About ISG Access for IP Subscriber Sessions, page 51
- How to Configure ISG for IP Subscriber Sessions, page 62
- Configuration Examples for ISG Access for IP Subscriber Sessions, page 88
- Additional References, page 92
- Feature Information for ISG Access for IP Subscriber Sessions, page 93

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Access for IP Subscriber Sessions

The Dynamic Host Configuration Protocol (DHCP) server must support the DHCP lease protocol.

For ISG to use DHCP to assign IP addresses:

- The subscriber must be Layer 2 connected.

- ISG must be in the path of DHCP requests, serving as a DHCP server or relay.
- The appropriate IP subnets must be configured on the subscriber interface.

Restrictions for ISG Access for IP Subscriber Sessions

Overlapping IP Address Restrictions

Overlapping IP addresses in the same virtual routing and forwarding (VRF) instance are not supported.

Overlapping IP subscribers in different VRFs are not supported on the same interface for static IP subscriber sessions and routed IP subscriber sessions. Overlapping IP subscribers in different VRFs are supported on the same interface for Layer 2 connected DHCP subscriber sessions.

IP Subnet Session Restrictions

IP subnet sessions are not supported on an interface configured with the **ip subscriber l2-connected** command. IP subnet sessions are supported only when the **ip subscriber routed** command is configured on the interface.

ISG DHCP Restrictions

ISG cannot relay DHCP requests when a Layer 3 DHCP relay agent is between the ISG device and subscriber devices.

Dynamic VPN Selection Restrictions

Dynamic VPN selection is not supported for IP interface sessions, IP subnet sessions, and subscribers coming in on nonglobal VRF interfaces.

Dynamic VPN selection is not supported for subscribers with a static VPN configuration on the access interface.

Dynamic VPN selection with address reassignment is not supported for routed IP subscriber sessions that are initiated by DHCP. IP addresses of routed IP subscribers must be routable in the access network. Because Internet service provider (ISP)- or VRF-owned private addresses could overlap or be unroutable in the network between subscribers and the ISG device, it is not possible to assign IP addresses to those subscribers.

IP interface sessions do not support dynamic VRF; only static VRF is supported. If an interface is configured with the **ip subscriber interface** command, dynamic VRF through a RADIUS VSA is not supported, only static VRF is supported.

General IP Session Restrictions

Network Address Translation (NAT) configuration is not supported on the access side of ISG.

IP subscriber sessions are not supported on ambiguous IEEE 802.1QinQ (QinQ) or IEEE 802.1Q (Dot1Q) subinterfaces.

IP subscriber sessions are not supported on interfaces that receive Multiprotocol Label Switching (MPLS) packets.

Modular quality of service (QoS) CLI (MQC) shaping and queuing is supported in the egress direction in the default class for IP subscriber sessions.

Configuring features on static IP sessions is not supported.

ISG IP subscriber functionality is not supported on the following types of access interfaces:

- Gigabit EtherChannel (Port Channel)
- Generic routing encapsulation (GRE)
- PPP (virtual-template)
- Layer 2 Tunnel Protocol (L2TP)

Interface statistics are not generated for ISG multiservice interfaces.

Stateful switchover (SSO) and In Service Software Upgrade (ISSU) are not supported for any features on ISG IP subscriber sessions or traffic class sessions. Upon switchover, an IP session must be re-created or restarted (for DHCP sessions) when the session becomes active again.

The following subscriber features are not supported on IPoE sessions:

- Per-session firewall
- Per-session NAT
- Per-session PBR
- Per-session NBAR
- Per-session netflow
- Per-session multicast

The following PPP session features are not supported on IP sessions:

- Session limit per system, VLAN, or MAC
- Dual stack session (single PPP session carrying both IPv4 and IPv6 traffic)
- Packet of Disconnect (PoD)

Multiservice Interface Restrictions

IP interface features (such as QoS and access lists) are not supported on multiservice interfaces.

Only one multiservice interface can belong to a single VRF. For example, the following configuration will not work:

```
interface multiservice 1
 ip vrf forwarding VRF_A
!
interface multiservice 2
 ip vrf forwarding VRF_A
```

Information About ISG Access for IP Subscriber Sessions

- Types of IP Subscriber Sessions, page 52
- Coexistence of Multicast and IP Sessions, page 53
- IP Subscriber Connectivity, page 53
- IP Subscriber Session Initiation, page 54
- IP Subscriber Addressing, page 54
- IP Subscriber Identity, page 56
- VPN Connectivity and Services for IP Subscribers, page 58
- IP Session Termination, page 61
- IP Session Recovery for DHCP-Initiated IP Sessions, page 61
- Default Services for IP Subscriber Sessions, page 61

Types of IP Subscriber Sessions

ISG supports the following types of IP subscriber sessions:

- IP Sessions, page 52
- IP Interface Sessions, page 52
- IP Subnet Sessions, page 52

IP Sessions

An IP session includes all the traffic that is associated with a single subscriber IP address. If the IP address is not unique to the system, other distinguishing characteristics such as a VRF or MAC address form part of the identity of the session. ISG can be configured to create IP sessions upon receipt of DHCP packets, packets with unclassified IP or MAC addresses, or RADIUS packets. See the "IP Subscriber Session Initiation" section for more information.

IP sessions may be hosted for a connected subscriber device (one routing hop from the ISG) or one that is more than one hop from the gateway.

IP Interface Sessions

An IP interface session includes all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered, and the session is continuous, even when the interface is shut down. By default, IP interface sessions come up in the state “unauthenticated” with full network access.

IP interface sessions might be used in situations in which a subscriber is represented by an interface (with the exception of PPP) and communicates using more than one IP address. For example, a subscriber using routed bridge encapsulation (RBE) access might have a dedicated ATM virtual circuit (VC) to home customer premises equipment (CPE) that is hosting a number of PCs.

IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet session is configured, ISG treats the subnet as a single subscriber, which means that ISG features and functionality are applied to the subnet traffic as an aggregate.

IP subnet sessions are supported for routed IP subscriber traffic.

IP subnet sessions are created the same way as IP sessions, except that when a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Note Where an ingress interface maps to a single subnet, the subnet might be accommodated with an IP interface session. However, if the ISG is more than one hop away from a subscriber, and there is the possibility that multiple subnets are accessible through the same interface, IP subnet sessions may be defined to distinguish the traffic and apply appropriate edge functionality to each subnet.

Coexistence of Multicast and IP Sessions

The ISG Session Multicast Coexistence feature introduces the ability to host all the subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco ASR 10000 Series Aggregation Routers. ISG IP sessions are supported on nonaccess-type subinterfaces. In the case of an existing session or even when no session exists, this support helps the multicast traffic to pass through the interfaces configured for the IP sessions in both upstream and downstream directions without creating a session.

IP Subscriber Connectivity

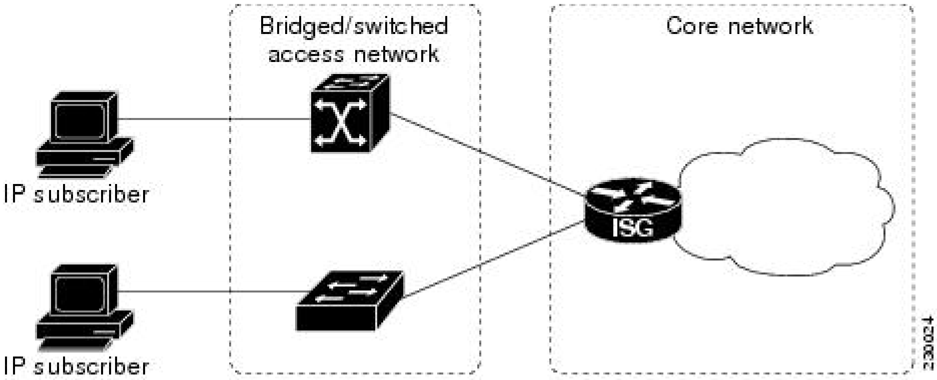
IP subscribers connect to ISG through either Layer 2 connected access networks or routed access networks. The following sections describe these types of IP subscriber connectivity:

- Layer 2 Connected Access Networks, page 53
- Routed Access Networks, page 53

Layer 2 Connected Access Networks

Layer 2 connected subscribers are either directly attached to the physical interfaces of an ISG or connected to an ISG through a Layer 2 access network, such as a bridged or a switched network. Layer 3 forwarding is either absent or not used to direct subscriber traffic in the Layer 2 access network. IP addresses of the subscribers may or may not be on the same subnet as the Layer 2 connected physical interfaces. The figure below shows an example of a Layer 2 connected access network.

Figure 2

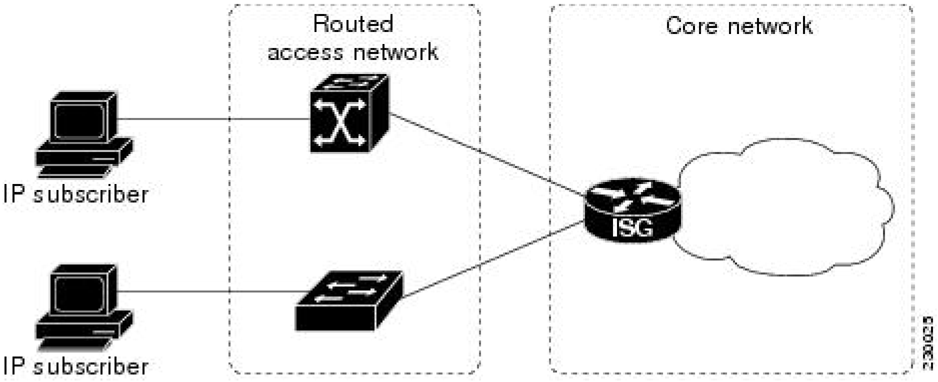


Routed Access Networks

Routed subscriber traffic is routed through a Layer 3 access network with at least one transit router before reaching the ISG. IP addresses of the subscribers are at least routable in the Layer 3 access network. Layer

3 access networks contain a single routing domain and therefore do not support overlapping IP addresses. The figure below shows an example of a routed access network.

Figure 3



IP Subscriber Session Initiation

ISG can be configured to allow one or more of the following events to signal the start of an IP session or IP subnet session on an interface:

- DHCP DISCOVER packet

If the following conditions are met, receipt of a DHCP DISCOVER packet will trigger the creation of an IP session:

-
  - The ISG serves as a DHCP relay or server for new IP address assignments.
  - Subscribers are configured for DHCP.
  - The DHCP DISCOVER packet is the first DHCP request received from the subscriber.
- Unclassified source IP address

For routed IP subscribers, a new IP session is triggered by the appearance of an IP packet with an unclassified source IP address (which means that an IP session does not yet exist for that IP address).

- Unclassified source MAC address

For Layer 2 connected IP subscribers, a new IP session is triggered by the appearance of an IP packet with an unclassified source MAC address (which means that an IP session does not yet exist for that MAC address).

- RADIUS Access-Request packet

For routed or Layer 2 connected access, a new IP session is triggered by the appearance of a RADIUS Access-Request packet when ISG is serving as a RADIUS proxy.

IP Subscriber Addressing

The following sections provide information about how ISG handles IP addressing for IP subscribers:

- Methods of ISG Subscriber IP Address Assignment, page 55
- Public and Private IP Addresses, page 55
- Overlapping IP Addresses, page 56

- ISG Subscriber IP Address Assignment Using DHCP, page 56

Methods of ISG Subscriber IP Address Assignment

IP subscribers either have IP addresses configured statically or obtain IP addresses dynamically through some network protocol that has the ability to assign IP addresses. For a subscriber to be routable within a given IP service domain, the subscriber must present a domain-specific IP address to the network. If a subscriber transfers between IP service domains (which include any private domain managed by the access provider), the IP address presented to the network must change to reflect the new domain.

The following sections describe the methods of IP address assignment that ISG supports for each type of Layer 3 session:

- IP Interface Sessions, page 55
- IP Sessions, page 55
- IP Subnet Sessions, page 55

IP Interface Sessions

For IP interface sessions, ISG is not involved in (or aware of) the assignment of subscriber IP addresses.

IP Sessions

For IP sessions, ISG supports the following methods of IP address assignment:

- Static IP addresses

If a subscriber’s static IP address is configured correctly for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber.

- DHCP

If DHCP is being used to assign IP addresses, and the IP address that is assigned by DHCP is correct for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber.

If the IP address that is assigned by DHCP is not correct for the service domain, or if the domain changes because of a VRF transfer, ISG can be configured to influence the DHCP IP address assignment.

The following conditions must be met in order for ISG to influence DHCP IP address assignment:

-
    - The subscriber must be Layer 2 connected.
    - The ISG device must be in the path of DHCP requests by serving as a DHCP server or relay.
    - Subscribers must not have statically configured IP addresses.

For deployments that support it, DHCP is the recommended method of IP address assignment.

IP Subnet Sessions

For IP subnet sessions, the IP subnet is specified in the user profile.

Public and Private IP Addresses

No matter how an IP subscriber is assigned an IP address, the IP address falls in either the public or the private IP address category. If an IP subscriber is assigned with a private IP address and the subscriber has to reach the Internet, a Layer 3 gateway, such as ISG or a firewall, between the subscriber and the Internet must perform Network Address Translation (NAT) for the subscriber’s private IP address.

When the access network is a Layer 2 connected network, a subscriber IP address can be either native or foreign to an access interface. A native subscriber IP address is one that belongs to the subnet provisioned on the access interface. A foreign subscriber IP address is one that does not belong to the subnet provisioned on the access interface. A foreign subscriber IP address could result when a retail ISP assigns an IP address to the IP subscriber from its own IP address allotment, which is different from the wholesale ISPs, or when an IP subscriber with a static IP address that is native in the home access network roams to a foreign access network. To support IP subscribers with foreign IP addresses, ISG must be able to respond to Address Resolution Protocol (ARP) requests that originate from foreign IP addresses with a MAC address of the ISG itself. Because the access network is Layer 2 connected, ISG maintains an adjacency to every subscriber.

When the access network is a routed network, a subscriber IP address must be routable in the access network; otherwise, subscriber traffic will never be able to reach ISG. ISG may not have an adjacency for each subscriber in this case, but rather an adjacency of the next hop toward a subscriber. The next hop is determined by the routing process on ISG.

Overlapping IP Addresses

When an access network is deployed without VPN capability, the IP address space in the access network is shared among all IP subscribers. When the IP addresses are assigned dynamically, care must be taken to ensure that these addresses do not overlap. In cases where overlapping IP addresses are assigned to IP subscribers intentionally, the access network should use a Layer 2 separation mechanism to differentiate the IP address spaces. For example, the access network may put each IP address space in a different VLAN.

In cases in which the access network serves both local IP subscribers and roaming users, the static private IP address of a roaming subscriber may overlap the native private IP address of another subscriber. For example, a public wireless hot spot that generally assigns dynamic IP addresses might want to provide access to occasional roaming users with statically configured IP addresses. To support this special overlapping condition, all IP subscribers must be in a Layer 2 connected access network in which overlapping MAC addresses do not exist. In this case, IP subscribers can be distinguished using MAC addresses.

ISG Subscriber IP Address Assignment Using DHCP

When ISG is in the path of DHCP requests (as either a DHCP server or a DHCP relay), ISG can influence the IP address pool and DHCP server that are used to assign subscriber IP addresses. To enable ISG to influence the IP addresses assigned to subscribers, associate a DHCP address pool class with an address domain. The DHCP address pool class must also be configured in a service policy map, service profile, or user profile that is associated with a subscriber. When a DHCP request is received from a subscriber, DHCP uses the address pool class that is associated with the subscriber to determine which DHCP address pool should be used to service the request. As a result, on a per-request basis, an IP address is provided by the local DHCP server or relayed to a remote DHCP server that is defined in the selected pool.

IP Subscriber Identity

IP subscriber identity is closely related to IP session initiation because ISG must uniquely identify an IP subscriber at the moment that it creates the IP session. However, the need to identify an IP subscriber goes beyond the session initiation phase. The following sections describe how ISG uniquely identifies IP subscribers:

- Routed IP Subscriber Identity, page 57
- MAC Address as Secondary Identity, page 57
- DHCP Lease Query Support, page 57

- Layer 2 Connected IP Subscriber Identity, page 58

Routed IP Subscriber Identity

If the access network is a routed network, subscriber IP addresses can be used to uniquely identify IP subscribers because by definition subscriber IP addresses are at least routable in the access network.

When using a subscriber IP address as the identifier, ISG assumes that the subscriber IP address is unique. If the access network is deployed with Layer 3 load balancing, redundancy, or asymmetric routing, ISG also assumes that IP traffic from the same IP subscriber may arrive at different access interfaces. To support this type of deployment, ISG assumes a single IP address space for all the access interfaces connecting to the same access network.

If there is a requirement to support several IP address spaces over a single physical access network, the access network must use some Layer 2 encapsulation to create a separate logical access network for each IP address space. In this case, ISG can still have a single IP address space for all the logical access interfaces that connect to a logical access network.

When subscriber IP addresses are private IP addresses, the access network must be able to route such subscriber traffic. If the subscriber traffic is destined to the Internet, NAT must be performed.

For routed IP subscribers, the subscriber IP address serves as the key for an IP session. ISG associates IP traffic with an IP session as follows:

- In the upstream direction, the source IP address of an IP packet is used to identify the IP session. The source IP address is the subscriber IP address.
- In the downstream direction, the destination IP address of an IP packet is used to identify the IP session. The destination IP address is the subscriber IP address.

If the IP subscriber is a VPN user, the subscriber IP address must be routable in both the global routing table and the VPN routing table on the ISG.

In the case of an IP subnet subscriber, a subscriber IP address is defined as an IP prefix address instead of a /32 IP host address. This IP prefix covers a range of IP addresses used by end users but represents a single logical IP subscriber from the ISG point of view. In this deployment, all end users share the same connectivity and services provided by the ISG.

To normalize the classification of IP subscribers that have different network masks, ISG uses the network mask in conjunction with the subscriber IP address for routed IP subscribers.

MAC Address as Secondary Identity

You must configure the **collect identifier mac-address** command at the start of a session. This instructs the ISG devices to store the MAC address as part of the session identifiers. For routed IP subscriber sessions, the MAC address is collected from the DHCP server using the DHCP Lease Query Protocol. For information about configuring the command, see the "Configuring ISG Control Policies" module.

DHCP Lease Query Support

The DHCP Lease Query message is a DHCP message type transmitted from a DHCP relay agent to a DHCP server. A DHCP Lease Query-aware relay agent sends the location of an IP endpoint to the DHCP Lease Query message.

The DHCP Lease Query transaction is a DHCP transaction with special message types that enable clients to query DHCP servers regarding the owner and the lease expiration time of an IP address. For information about configuring DHCP server for Lease Query, see the Configuring a DHCP Server IP Address, page 82.

Layer 2 Connected IP Subscriber Identity

A Layer 2 connected access network is capable of providing IP connectivity to IP subscribers with foreign and overlapping IP addresses, in addition to IP subscribers with native IP addresses. Because subscriber IP addresses might not be unique in such an access network, ISG uses the subscriber MAC address to identify Layer 2 connected IP subscribers, regardless of what kind of IP address a subscriber has.

Traffic that comes from IP subscribers with private or overlapping IP addresses and that is destined to the Internet is subject to NAT.

For Layer 2 connected IP subscribers, both the subscriber MAC address (unique within a VLAN) and the IP address serve as the keys for the IP session, but they are used in different directions:

- In the upstream direction, the VLAN ID and source MAC address of an IP packet are used to identify the IP session.
- In the downstream direction, both the destination IP address and the VLAN ID of an IP packet are used to identify the IP subscriber context.

VPN Connectivity and Services for IP Subscribers

- Subscriber VPN Membership, page 58
- Multiservice Interface Model, page 58
- VPN Addressing, page 59
- VPN IP Subscriber Identity, page 60
- Service Model for VRF Transfers, page 60
- Benefits of Dynamic VPN Selection, page 60

Subscriber VPN Membership

Depending on deployment requirements, an IP subscriber may or may not have VPN service. If an IP subscriber does have VPN service, the subscriber may belong to only one VPN domain at any time. An IP subscriber is associated with a VPN domain in one of the following ways:

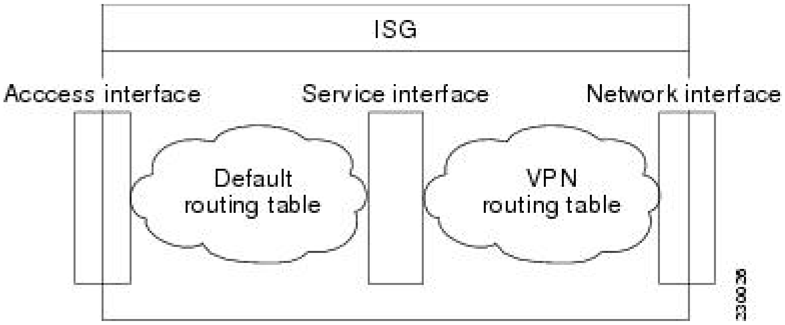
- Static VPN assignment--The VPN IP subscriber belongs to a static VPN domain. Whenever the IP subscriber connects to ISG, the IP subscriber is placed in the preassigned VPN domain.
- Dynamic VPN selection--The VPN IP subscriber can choose and switch among different VPN domains through dynamic service logon. Whenever a new VPN domain is selected, VPN services of the current VPN domain must be removed before VPN services of the new VPN domain can be applied to the IP subscriber.

Dynamic VPN selection can be initiated through automatic service logon, where the VRF is downloaded and applied to the subscriber session at session start, or through subscriber service selection at a web portal, in which case the subscriber is transferred to the VRF that corresponds to the selected service.

Multiservice Interface Model

For a subscriber without a static VPN configuration, a multiservice interface must be configured on the ISG device to map the IP session to a VRF. The multiservice interface represents a boundary between a VPN routing domain and the default routing domain. In cases where an IP subscriber may be associated with several routing domains throughout the duration of a connection, multiservice interfaces serve as demarcation points for the IP subscriber to switch from one VPN domain to another. One multiservice interface must be configured for each VPN routing domain. The figure below illustrates the multiservice interface model.

Figure 4



VPN Addressing

When a subscriber session is transferred from one VPN domain to another, it is effectively entering a new addressing domain that may or may not overlap the subscriber's previous domain. The subscriber's network-facing address must be altered accordingly so that packets can be correctly routed back from within the service domain.

A VRF transfer is necessary when a subscriber's identity and subscribed services cannot be determined without interaction with a web portal. A local routing context is required, at least initially, so that IP packets may be routed to and from the portal server. Following portal-based service selection, the subscriber would typically have to be transferred into the VRF associated with the selected service domain. Following a VRF transfer, the subscriber must also receive an address that is routable in this new domain.

If ISG is adjacent to the subscriber device and serves as a DHCP relay or server, DHCP can be used to assign domain-specific addresses to subscribers.

In order for VRF transfers to be supported, it is strongly recommended that DHCP be configured with short initial leases (this is because existing subscriber addresses can only be altered once the current lease has expired). Subscribers will not have access to the selected domain before the next DHCP renew request is received. Using short initial lease times minimizes the interval between a VRF change and a DHCP renewal. If long lease times are used, an out-of-band method of initiating IP address change should be implemented.

When DHCP can be used to assign a new address at the subscriber device, subnet-based VRF selection can be used to bring about the transfer. Subnet-based VRF selection (also known as *VRF autoclassify*) is a feature that selects the VRF at the ingress port on the basis of the source IP subnet address.

Service providers and organizations have allocated public IP address blocks that are not overlapping by nature. Therefore, when they are assigned public IP addresses, VPN IP subscribers have no overlapping IP addresses. When VPN IP subscribers of different VPN domains have private IP addresses assigned, they are likely to have overlapping addresses in the access network.

An access network is a single IP address space when there is no Layer 2 encapsulation separating VPN IP subscribers of different VPN domains. Therefore, ISG must be able to handle overlapping IP addresses when deploying VPN IP subscribers. IP connectivity for VPN IP subscribers with overlapping IP addresses is possible only when they are connected to ISG through a Layer 2 connected access network.

VPN IP Subscriber Identity

ISG identifies VPN IP subscribers in the same way that it identifies non-VPN IP subscribers. Upstream IP traffic is defined as the subscriber IP traffic traveling from the access network to the VPN (overlaid on top of the service provider core network). Downstream IP traffic is defined as the subscriber IP traffic traveling from the VPN to the access network.

Service Model for VRF Transfers

A *primary* service is a service that contains a network-forwarding policy (such as a VRF) in its service definition. Only one primary service at a time can be activated for a session. A *secondary* service is any service that does not contain a network-forwarding policy.

When a subscriber for whom a primary service has already been activated tries to select another primary service, ISG will deactivate all current services (including the current primary service) and activate the new primary service, and hence switch the VRF.

When a subscriber for whom a primary service has already been activated tries to select a secondary service, the action taken by ISG depends on whether the secondary service is part of a service group. A *service group* is a grouping of services that may be simultaneously active for a given session. Typically, a service group includes one primary service and one or more secondary services. The table below describes the action that ISG will take when a subscriber selects a secondary service.

Table 4 ISG Activation Policy for Secondary Services

Primary Service Characteristics	Secondary Service Characteristics	Resulting Behavior at ISG
Primary service with no service group attribute	Secondary service with service group	Do not bring up the secondary service.
	Secondary service with no service group	Bring up the secondary service.
Primary service with service group attribute	Secondary service with different service group	Do not bring up the secondary service.
	Secondary service with same service group	Bring up the secondary service.
	Secondary service with no service group	Bring up the secondary service.

Benefits of Dynamic VPN Selection

The need for switching of a subscriber session between routing and forwarding domains (also called *network services*) occurs frequently in markets where so-called *equal access networking* must be supported. Equal access networking is often mandated by regulatory rules stating that an access provider should allow service providers equal access to a retail subscriber network. ISG dynamic VPN selection facilitates equal access networking by allowing subscribers to transfer between network services.

IP Session Termination

An IP session may be terminated in one of the following ways:

- DHCP Lease Expiry or DHCP Release from client

If DHCP is used to detect a new session, its departure may also be signaled by a DHCP event.

- Application stop

An application command that is used to terminate a session. The **application stop** command is typically used to terminate a session when a subscriber initiates an account logoff from a web portal. An application stop may also result from the actions of an administrator, such as action taken in response to rogue behavior from a subscriber.

- Idle timeout and session timeout

Idle timeouts and session timeouts can be used to detect or impose termination of an IP session.

- Control policy

A control policy containing the “service disconnect” action can be used to terminate a session.

IP Session Recovery for DHCP-Initiated IP Sessions

When an IP session is terminated (for example, by account logoff or session timeout) or lost (for example, by router reload), the client may continue to hold an unexpired DHCP lease. When this happens, ISG performs a session restart to prevent the client’s IP connection from being stuck until the DHCP lease expires. A control policy can be configured to define the actions that ISG will take when the session restart event occurs. If a policy is not defined, a default policy will take effect. The default policy causes ISG to disconnect the session after 60 seconds following a session restart and is the equivalent of the following configuration:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

This default policy appears in the output for the **show subscriber policy rules** command as follows:

```
Rule: internal-rule-session-restart
 Class-map: always event session-restart
  Action: 1 service disconnect delay 60
  Executed: 0
```

Default Services for IP Subscriber Sessions

Newly created IP sessions may require a default service to allow subsequent subscriber packets to be processed appropriately; for example, to permit or force TCP packets to a captive portal where menu-driven authentication and service selection can be performed. A default service policy map or service profile may be configured for IP sessions to redirect traffic, enable port-bundle host-key functionality for session identification, or enable transparent autologon. A default service would also likely include a network service, which allows subscribers to access a web portal for authentication and service selection.

How to Configure ISG for IP Subscriber Sessions

- Creating ISG Sessions for IP Subscribers, page 62
- Assigning ISG Subscriber IP Addresses Using DHCP, page 75
- Configuring ISG Dynamic VPN Selection, page 83

Creating ISG Sessions for IP Subscribers

An ISG device creates IP sessions for IP traffic on subscriber-side interfaces. The following tasks enable IP sessions and indicate how sessions will be identified:

- Creating IP Subscriber Sessions for Routed ISG Subscribers, page 62
- Creating IP Subscriber Sessions for Layer 2 Connected ISG Subscribers, page 64
- Creating ISG IP Interface Sessions, page 65
- Creating an ISG Static Session, page 66
- Creating ISG IP Subnet Sessions, page 69
- Configuring IP Session Recovery for DHCP-Initiated IP Sessions, page 71
- Verifying ISG IP Subscriber Sessions, page 73
- Clearing ISG IP Subscriber Sessions, page 74
- Troubleshooting Tips, page 75

Creating IP Subscriber Sessions for Routed ISG Subscribers

Routed IP subscribers are subscribers that are routed through a Layer 3 access network with at least one transit router before reaching the ISG. Perform this task to configure ISG to create IP sessions for routed IP subscribers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber routed**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber routed** **Example:** `Router(config-if)# ip subscriber routed`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.

Step 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**}
	Example:
	`Router(config-subscriber)# initiator dhcp`
		Configures ISG to create an IP subscriber session upon receipt of the specified packet type.
		• **dhcp** --ISG will initiate an IP session upon receipt of a DHCP DISCOVER packet. The **class-aware** keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
		• **radius-proxy** --ISG will initiate an IP session upon receipt of a RADIUS Access-Request packet.
		• **unclassified ip-address** --ISG will initiate an IP session upon receipt of the first IP packet with an unclassified IP source address.
		• This command can be entered more than once to specify more than one method of IP session initiation.
		Note If the ISG device serves as either a DHCP relay or DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions upon receipt of DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of the **initiator unclassified ip** or **initiator unclassified mac** command.

Step 6	**end**
	Example:
	`Router(config-subscriber)# end`
		(Optional) Returns to privileged EXEC mode.

Creating IP Subscriber Sessions for Layer 2 Connected ISG Subscribers

Layer 2 connected subscribers are either directly attached to the physical interfaces of an ISG or connected to an ISG through a Layer 2 access network, such as a bridged network or a switched network. Perform this task to configure ISG to create IP sessions for Layer 2 connected IP subscribers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber l2-connected**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber l2-connected** **Example:** `Router(config-if)# ip subscriber l2-connected`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode. **Note** It is recommended that IP sessions for Layer 2 connected subscribers be configured using the **ip subscriber l2-connected** command. However, the **ip subscriber routed** command could also be used if subscriber IP addresses are routable in the access domain.

	Command or Action	Purpose

Step 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**}
	Example:
	`Router(config-subscriber)# initiator unclassified mac-address`
		Configures ISG to create an IP subscriber session upon receipt of the specified packet type.
		• **dhcp** --ISG initiates an IP session upon receipt of a DHCP DISCOVER packet. The **class-aware** keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
		• **radius-proxy** --ISG initiates an IP session upon receipt of a RADIUS packet.
		• **unclassified mac-address** --ISG will initiate an IP session upon receipt of the first IP packet with an unclassified MAC source address.
		• This command can be entered more than once to specify more than one method of IP session initiation.
		Note If the ISG device serves as either a DHCP relay or DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions upon receipt of DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of the **initiator unclassified ip** or **initiator unclassified mac** command.

Step 6	**end**
	Example:
	`Router(config-subscriber)# end`
		(Optional) Returns to privileged EXEC mode.

Creating ISG IP Interface Sessions

An ISG IP interface session encompasses all IP packets that cross the specified interface or subinterface. Perform this task to create an ISG IP interface session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**.** *subinterface-number*]
4. **ip subscriber interface**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [**.** *subinterface-number*] **Example:** `Router(config)# interface GigabitEthernet 0//0/0.1`	Specifies an interface or subinterface and enters interface configuration mode.
Step 4	**ip subscriber interface** **Example:** `Router(config-subif)# ip subscriber interface`	Specifies the type of IP subscriber to be hosted on the interface.

Step 5	**end**
	Example:
	`Router(config-subif)# exit`
		(Optional) Returns to privileged EXEC mode.

Creating an ISG Static Session

The ISG Static Session Creation feature enables administrator initiated static IP sessions. An ISG static session enables you to configure static IP sessions from the CLI. You can create static IP sessions by configuring a group of server addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. Do one of the following:
   - **ip source** *ipaddress* **mac** *macaddress*
   -
   - **ip source** *ipaddress* **mask** *subnetmask*
5. **exit**
6. **interface** *type number*
7. Do one of the following:
   - **ip subscriber l2-connected**
   - **ip subscriber routed**
8. **initiator static ip subscriber list** *list-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip subscriber list** *list-name* **Example:** `Router(config)# ip subscriber list mylist`	Specifies the IP subscriber list name and enters server list configuration mode.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **ip source** *ipaddress* **mac** *macaddress*
	•
	• **ip source** *ipaddress* **mask** *subnetmask*
	Example:
	`Router(config-server-list)# ip source 209.165.200.225 mac 0.7.f`
	Example:
	Example:
	`Router(config-server-list)# ip source 209.165.200.225 mask 255.255.255.224`
		Specifies the static server IP address and MAC address (in the case of Layer 2-connected) or subnet mask (in the case of routed).

Step 5	**exit** **Example:** `Router(config-server-list)# exit`	Returns to global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 2/0/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose

Step 7	Do one of the following:
	• **ip subscriber l2-connected**
	• **ip subscriber routed**
	Example:
	`Router(config-if)# ip subscriber l2-connected`
	Example:
	Example:
	`Router(config-if)# ip subscriber routed`
		Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode.
		Note It is recommended that IP sessions for Layer 2 connected subscribers be configured using the **ip subscriber l2-connected** command. However, the **ip subscriber routed** command could also be used if subscriber IP addresses are routable in the access domain.

Step 8	**initiator static ip subscriber list** *list-name* **Example:** `Router(config-subscriber)# initiator static ip subscriber list mylist`	Creates an IP subscriber session with the packet type as static and attaches the session to the list.

Step 9	**end**
	Example:
	`Router(config-subscriber)# end`
		Returns to privileged EXEC mode.

Creating ISG IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet session is configured, ISG treats the subnet as a single subscriber, which means that ISG features and functionality are applied to the subnet traffic as an aggregate. Perform this task to configure an IP subnet session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber routed**
5. **initiator unclassified ip-address**
6. **end**
7. Add the Framed-IP-Netmask attribute to the service or user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber routed** **Example:** `Router(config-if)# ip subscriber routed`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.
Step 5	**initiator unclassified ip-address** **Example:** `Router(config-subscriber)# initiator unclassified ip-address`	Configures ISG to create an IP subscriber session upon receipt of an IP packet with an unclassified IP source address.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-subscriber)# end`
		(Optional) Returns to privileged EXEC mode.

Step 7	Add the Framed-IP-Netmask attribute to the service or user profile.	Enables an IP subnet session for the subscriber. • When a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Configuring IP Session Recovery for DHCP-Initiated IP Sessions

Perform this task to configure ISG to perform specific actions upon recovery of an IP session after ISG has terminated the session or reloaded. This task applies to DHCP-initiated IP sessions only.

If a policy for session recovery is not configured, ISG will apply the following default policy:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event session-restart**
5. *action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
7. *action-number* **set-timer** *name-of-timer minutes*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control MY-POLICY`	Creates or modifies a control policy map, which is used to define a control policy, and enters control policy map configuration mode.

Step 4	**class type control** {*control-class-name* | **always**} **event session-restart**
	Example:
	`Router(config-control-policymap)# class type control always event session-restart`
		Specifies a control class that will be evaluated when the session-restart event occurs, and enters policy map class control configuration mode.
		- A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.

Step 5	*action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
	Example:
	`Router(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`
		(Optional) Initiates a request for authorization on the basis of the specified identifier.

	Command or Action	Purpose

Step 6	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
	Example:
	`Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`
		(Optional) Activates an ISG service.
		- Specifying an identifier instead of a service name will activate a service that has the same name as the specified identifier.

Step 7	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Router(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	(Optional) Starts a named policy timer. - Expiration of the timer generates the event timed-policy-expiry.

Step 8	**end**
	Example:
	`Router(config-control-policymap-class-control)# end`
		(Optional) Returns to privileged EXEC mode.

Verifying ISG IP Subscriber Sessions

Perform this task to verify IP subscriber session configuration and creation. The commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]
3. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
4. **show platform isg session-count** {**all** | *slot*}
5. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays information about ISG policies and features for subscriber sessions.
Step 3	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **Example:** `Router# show ip subscriber ip 10.10.10.10`	Displays information about ISG IP subscriber sessions.
Step 4	**show platform isg session-count** {**all** | *slot*} **Example:** `Router# show platform isg session-count all`	Displays the number of active ISG subscriber sessions by line card.
Step 5	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Clearing ISG IP Subscriber Sessions

Perform this task to clear IP subscriber sessions.

SUMMARY STEPS

1. **enable**
2. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
3. **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **Example:** `Router# show ip subscriber ip 10.10.10.10`	(Optional) Displays information about ISG subscriber IP sessions.
Step 3	**clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]] **Example:** `Router# clear ip subscriber ip 10.10.10.10`	Clears ISG IP subscriber sessions.
Step 4	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Troubleshooting Tips

Use the following commands to troubleshoot ISG IP subscriber sessions:

- **debug ip subscriber**
- **debug condition**

Assigning ISG Subscriber IP Addresses Using DHCP

The tasks in this section assume that you have configured DHCP support in your network.

- Configuring an ISG Interface for Dynamic DHCP Class Association, page 76
- Configuring DHCP Server User Authentication, page 77
- Configuring a DHCP Class in a Service Policy Map, page 80
- Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server, page 81
- Configuring a DHCP Server IP Address, page 82

Configuring an ISG Interface for Dynamic DHCP Class Association

Perform this task to enable ISG to influence the assignment of IP addresses to subscribers on the interface by providing the local DHCP component with a class name. The class name refers to a class configured using the **ip dhcp pool** command and can reference a pool of addresses or a relay destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **ip subscriber** [**l2-connected** | **routed**]
6. **initiator dhcp class-aware**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface for configuration, and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.1.0.1 255.255.0.0`	Sets a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 5	**ip subscriber** [**l2-connected** | **routed**] **Example:** `Router(config-if)# ip subscriber`	Enables ISG IP subscriber configuration mode.
Step 6	**initiator dhcp class-aware** **Example:** `Router(config-if) initiator dhcp class-aware`	Configures ISG to create IP sessions upon receipt of DHCP DISCOVER packets. • The **class-aware** keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.

Step 7	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Returns to privileged EXEC mode.

Configuring DHCP Server User Authentication

Perform this task to authenticate the DHCP clients on the server.

You need to use the ISG framework to enable DHCP server user authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **local**
5. **ip dhcp pool** *pool-name*
6. **network** *network-number mask*
7. **exit**
8. **interface** *type number*
9. **ip subscriber l2-connected**
10. **initiator dhcp class-aware**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new model`	Enables authentication, authorization, and accounting (AAA).
Step 4	**aaa authentication login** *list-name* **local** **Example:** `Router(config)# aaa authentication login mylist local`	Sets the AAA authentication at login.
Step 5	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool testpool`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 6	**network** *network-number mask* **Example:** `Router(dhcp-config)# network 172.16.0.0 255.240.0.0`	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server.
Step 7	**exit** **Example:** `Router(dhcp-config)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 8	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/0`	Enters interface configuration mode.
Step 9	**ip subscriber l2-connected** **Example:** `Router(config-if)# ip subscriber l2-connected`	Configures a Layer 2 connected IP session on the interface and enters IP subscriber configuration mode.
Step 10	**initiator dhcp class-aware** **Example:** `Router(config-subscriber)# initiator dhcp class-aware`	Initiates a class for DHCP for an IP session initiated by DHCP.

Step 11	**end**
	Example:
	`Router(config-subscriber)# end`
		Returns to privileged EXEC mode.

- Troubleshooting Tips, page 79

Troubleshooting Tips

You can determine the DHCP authentication by using the **debug ip dhcp server events**, **debug ip dhcp server packet**,and **debug subscriber policy dpm event** commands. The following is sample output from the **debug subscriber policy dpm event** command:

```
*Apr 20 20:20:03.510: SG-DPM: DHCP Discover notification from client, mac_address = 001a.
7014.c03e
*Apr 20 20:20:03.510: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Could not find a dhcp_context for 001a.7014.c03e:
*Apr 20 20:20:03.510: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.510: SG-DPM: Session Initiation notification on Active
*Apr 20 20:20:03.510: SG-DPM: Allocated SHDB Handle (0xB6000252) for Mac address 001a.
7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Client is able to perform DHCP Authentication.Setting the
SSS_INFOTYPE_DHCP_AUTH_KEY
*Apr 20 20:20:03.510: SG-DPM: Sending Session start to PM, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Request for Classname from client, mac_address = 001a.
7014.c03e
*Apr 20 20:20:03.514: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.514: SG-DPM: No session found in ID manager
*Apr 20 20:20:03.514: SG-DPM: Processing sg_dpm_get_more_keys from SSS hdl 56000E52
*Apr 20 20:20:03.514: SG-DPM: DPM is providing Auth-User
```

You can also use the **show subscriber session detailed** and **show ip dhcp binding**commands to display subscriber information and DHCP pool information. The following is sample output from the **show ip dhcp binding** command:

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.1            0100.1a70.1530.38       Nov 18 2008 03:43 PM    Automatic
```

Configuring a DHCP Class in a Service Policy Map

Perform this task to assign a DHCP class to a service policy map. Subscribers for which this service policy map is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

A DHCP pool must be configured. Classes configured within the DHCP pool must match the DHCP classes configured in the service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **classname** *class-name*
5. **end**
6. **show policy-map type service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-name* **Example:** `Router(config)# policy-map type service service1`	Creates a service policy map or specifies an existing service policy map for configuration, and enters service policy-map configuration mode.

	Command or Action	Purpose
Step 4	**classname** *class-name* **Example:** `Router(config-service-policymap)# classname class1`	Associates a DHCP pool with a service policy map.

Step 5	**end**
	Example:
	`Router(config-service-policymap)# end`
		(Optional) Returns to privileged EXEC mode.

Step 6	**show policy-map type service** **Example:** `Router# show policy-map type service`	(Optional) Displays the contents of all service policy maps. • Use this command to verify that the DHCP class is associated with the service policy map.

- What to Do Next, page 81

What to Do Next

Once you have configured the DHCP address pool class in a service policy map, you may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server

Perform this task to add the vendor-specific attribute (VSA) for a DHCP class to a user profile or service profile on the AAA server. Subscribers for whom the user or service profile is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

- Prerequisites, page 81
- What to Do Next, page 82

Prerequisites

A DHCP address pool must be configured. Classes configured within the DHCP address pool must match the DHCP address pool classes configured in the service or user profile.

SUMMARY STEPS

1. Add the DHCP Class attribute to the user or service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the DHCP Class attribute to the user or service profile. **Example:** `26,9,1 = ”subscriber:classname=`*`class-name`*`”`	Associates a DHCP address pool with a service or specific subscriber.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring a DHCP Server IP Address

Perform this task to specify which DHCP servers to use on your network, or to configure the IP address of one or more DHCP servers available on the network, and to specify the DHCP Lease Query for routed IP sessions.

Note The DHCP server IP address needs to be configured for routed IP sessions, if the DHCP Lease Query is performed.

- The DHCP server must support the DHCP lease protocol.
- The IP address of the phone must be assigned by DHCP address assignments.
- The traffic must be classified as Layer 3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}}
	Example:
	`Router(config)# ip dhcp-server query lease retries 3`
		Configures the IP address of one or more DHCP servers available on the network, and specifies the DHCP Lease Query for routed IP sessions.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode.

Configuring ISG Dynamic VPN Selection

- Configuring a Multiservice Interface, page 83
- Specifying a VRF in a Service Policy Map, page 84
- Verifying VRF Transfer for IP Sessions, page 86
- Troubleshooting VRF Transfer for IP Sessions, page 87

Configuring a Multiservice Interface

Perform the steps in this procedure to configure a multiservice interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multiservice** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multiservice** *interface-number* **Example:** `Router(config)# interface multiservice 1`	Creates a multiservice interface, which enables dynamic VPN selection, and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding vrf1`	Associates a VPN VRF with an interface or subinterface.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.16.0.0 255.255.255.0`	Sets the primary IP address for an interface. • Specify the IP address of the VPN.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Returns to privileged EXEC mode.

Specifying a VRF in a Service Policy Map

VRF transfer occurs when a new primary service is activated for a session, causing the session to transfer from one VRF to another. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding vrf1`	Associates the service with a VRF.
Step 5	**sg-service-type primary** **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service is a service that contains a network-forwarding policy. A primary service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

	Command or Action	Purpose
Step 6	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	(Optional) Associates an ISG service with a service group. • A service group is a grouping of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.

Step 7	**end**
	Example:
	`Router(config-service-policymap)# end`
		(Optional) Returns to privileged EXEC mode.

Verifying VRF Transfer for IP Sessions

Perform the steps in the following task as needed to verify VRF transfer for IP sessions.

SUMMARY STEPS

1. **enable**
2. **show subscriber session uid** *session-identifier* **detail**
3. **show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds*| **detail** | **ip** *ip-address*]]
4. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
5. **show ip route** [**vrf** *vrf-name*]
6. **show ip dhcp binding** [**ip-address**]
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show subscriber session uid** *session-identifier* **detail** **Example:** `Router# show subscriber session uid 4 detail`	Displays information about ISG subscriber sessions with a specific session identifier.
Step 3	**show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds*| **detail** | **ip** *ip-address*]] **Example:** `Router# show ip subscriber vrf vrf1`	Displays information about ISG IP subscriber sessions.

Step 4	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
	Example:
	`Router# show idmgr session key nativeip-vrf ip-address 209.165.200.225`
		Displays information related to ISG session and service identity.

Step 5	**show ip route** [**vrf** *vrf-name*] **Example:** `Router# show ip route`	Displays the current state of the routing table.
Step 6	**show ip dhcp binding** [**ip-address**] **Example:** `Router# show ip dhcp binding`	Displays address bindings on the Cisco IOS DHCP server.
Step 7	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Troubleshooting VRF Transfer for IP Sessions

The commands in this procedure can be used to troubleshoot VRF transfer for IP sessions. These commands can be entered in any order.

SUMMARY STEPS

1. **debug subscriber** {**event** | **error** | **packet**| **policy** | **service**}
2. **debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
3. **debug subscriber policy dpm** {**error** | **event**}
4. **debug ip dhcp server** {**events** | **packets** | **linkage** | **class**}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**debug subscriber** {**event** | **error** | **packet**| **policy** | **service**}
	Example:
	`Router# debug subscriber service`
		Displays debugging messages pertaining to subscriber policies, policy server events, and changes to service.

Step 2	**debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
	Example:
	`Router# debug ip subscriber error`
		Displays debugging messages pertaining to an IP session created on the service gateway.

Step 3	**debug subscriber policy dpm** {**error** | **event**} **Example:** `Router# debug subscriber policy dpm event`	Displays diagnostic information about policy execution that is related to DHCP events.
Step 4	**debug ip dhcp server** {**events** | **packets** | **linkage** | **class**} **Example:** `Router# debug dhcp ip dhcp server events`	Enables Cisco IOS DHCP server debugging.

Configuration Examples for ISG Access for IP Subscriber Sessions

- Example ISG IP Interface Subscriber, page 89
- Example ISG Routed IP Subscriber, page 89
- Example ISG Layer 2 Connected IP Subscriber, page 89
- Example ISG Static Session Creation, page 89
- Example DHCP-Initiated Session Recovery, page 89

- Example ISG Interface with DHCP Class-Aware Capability, page 90
- Example DHCP Address Pool Classes and Relay Actions for ISG, page 90
- Example Dynamic VPN Selection, page 91

Example ISG IP Interface Subscriber

The following example shows how to configure an IP interface session on GigabitEthernet interface 0/0/1.401:

```
interface GigabitEthernet 0/0/1.401
 ip subscriber interface
```

Example ISG Routed IP Subscriber

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface 0/0/1.401 through a routed access network. ISG will create IP sessions upon receipt of DHCP DISCOVER packets, incoming valid IP packets, and RADIUS Access-Request packets.

```
interface GigabitEthernet0/0/1.401
 ip subscriber routed
  initiator dhcp class-aware
  initiator unclassified ip-address
  initiator radius-proxy
```

Example ISG Layer 2 Connected IP Subscriber

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface0/0/1.401 through a Layer 2 connected access network. ISG will create IP sessions upon receipt of any frame with a valid source MAC address.

```
interface GigabitEthernet0/0/1.401
 ip subscriber l2-connected
  initiator unclassified mac-address
```

Example ISG Static Session Creation

The following example shows how to create an ISG static session for server 209.165.200.225 for subscribers who connect to ISG on GigabitEthernet interface 0/4 through a Layer 2 connected access network. ISG will create a static session upon receipt of valid source IP address.

```
ip subscriber list mylist
 ip source 209.165.200.225 mac 0.7.f
interface GigabitEthernet 2/0/0
 ip subscriber l2-connected
  initiator static ip subscriber list mylist
```

Example DHCP-Initiated Session Recovery

The following example shows how to configure an ISG policy that applies a service called “FIRST-SERVICE” upon session restart for subscribers belonging to the VRF “FIRST”:

```
class-map type control TEST
 match vrf FIRST
```

```
policy-map type control GLOBAL
 class type control TEST event session-restart
  1 service-policy type service name FIRST-SERVICE
```

Example ISG Interface with DHCP Class-Aware Capability

In the following example, GigabitEthernet interface 1/0/0.400 is configured with DHCP class-aware functionality, which enables ISG to influence DHCP IP address assignment. If the service “SERVICE_DHCP” is activated, the DHCP pool “DHCP_POOL2” is used for address assignment. Otherwise, the default pool “DHCP_POOL1” is used.

```
interface GigabitEthernet1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.15.1 255.255.255.0 secondary
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP_POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp class default
!
ip dhcp pool DHCP_POOL2
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
   lease 0 0 30
   class DHCP_CLASS2
!
ip dhcp class DHCP_CLASS2
!
policy-map type service SERVICE_DHCP
 classname DHCP_CLASS2
!
```

Example DHCP Address Pool Classes and Relay Actions for ISG

This section contains examples of DHCP address pool configuration and relay actions for ISG.

DHCP Server Coresident with ISG Configuration

In the following configuration example, the ISPs are ISP1 and ISP2 companies. The ISP1 company has its addresses assigned from an address pool that is dynamically allocated using on-demand address pools (ODAP). The ISP2 company has its customer addresses assigned from the address pool 10.100.0.0/16. Customers not associated with any ISP will have an address allocated from the address pool 10.1.0.0/16, and the lease time is set to 10 minutes.

```
!Address pool for ISP1 customers
ip dhcp pool isp1-pool
 origin dhcp
 class isp1
!
!Address pool for ISP2 customers
!
ip dhcp pool isp2-pool
 network 10.100.0.0 255.255.0.0
 class isp2
```

```
!
!Address pool for customers without an ISP
!
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

DHCP Relay Agent Coresident with ISG Configuration

In the following configuration example, there are two ISPs, “poolA” and “poolB”. The “poolA” ISP and its customers are allowed to have addresses in the ranges 10.1.0.0/16 and 10.3.0.0/16, and are relayed to the DHCP server at 10.55.10.1. The “poolB” ISP and its customers are allowed to have addresses in the range 10.2.0.0/16 and 10.4.0.0/16, and are relayed to the DHCP server at 10.10.2.1.

```
!Address ranges:
interface gigabitethernet1/0/0
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary
interface gigabitethernet2/0/0
 ip address 10.3.0.0 255.255.0.0
 ip address 10.4.0.0 255.255.0.0
!Address pools for poolA1 and poolB2:
 ip dhcp pool poolA1
 relay source 10.1.0.0 255.255.0.0
 class poolA1
 relay target 10.55.10.1
!Address pool for poolA2:
ip dhcp pool poolA2
 relay source 10.3.0.0 255.255.0.0
 class poolA2
 relay target 10.55.10.1
!Address pools for poolB1 and poolB2:
ip dhcp pool poolB1
 relay source 10.2.0.0 255.255.0.0
 class poolB1
 relay target 10.10.2.1
ip dhcp pool poolB2
 relay source 10.4.0.0 255.255.0.0
 class poolB2
  relay target 10.10.2.1
```

Configuration of secure ARP for the relay will use the same configuration command as secure ARP already uses on a DHCP server by using the **update arp** command in address-pool configuration mode. If the system is allocating an address from this address pool, it will add secure ARP. If the system is relaying a packet using this address pool, it will also add secure ARP.

Example Dynamic VPN Selection

The following example shows a configuration in which subscribers are initially assigned an IP address from the DHCP global pool “DHCP_POOL1”. After a subscriber accesses the web portal and selects the service “CorporateVPN”, ISG performs a VRF transfer and the subscriber is assigned a new IP address from the DHCP pool “VPN_POOL1.” In this case, a single multiservice interface is required.

```
!
ip vrf VPN_406_1001
rd 406:1001
route-target export 406:1001
route-target import 406:1001
!
interface GigabitEthernet 1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
```

```
  initiator dhcp class-aware
!
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
!!!! Default Global DHCP Pool
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP_POOL1
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 lease 0 0 30
 class default
!
ip dhcp class default
!
!
!!! DHCP Pool for CorporateVPN
!
ip dhcp excluded-address 10.1.11.1
!
ip dhcp pool VPN_POOL1
 vrf VPN_406_1001
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.1
 lease 0 0 30
class DHCP_CLASS_VPN_406_1001
!
interface multiservice 1
 ip vrf forwarding VPN_406_1001
 ip address 10.1.11.1 255.255.255.0
 no keepalive
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
DHCP configuration	The "DHCP" module of the *Cisco IOS XEIP Addressing Configuration Guide*
Configuring ISG control policies	"Configuring ISG Control Policies" module in this guide

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Access for IP Subscriber Sessions

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

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

Table 5 Feature Information for ISG Access for IP Subscriber Sessions

Feature Name	Releases	Feature Configuration Information
DHCP--Server User Authentication	Cisco IOS XE Release 3.1S	The DHCP Server User Authentication feature is used to authenticate the DHCP clients. The following commands were introduced or modified by this feature: **aaa authentication login**, **network** (DHCP).
IP Session Recovery for DHCP-Initiated IP Sessions	Cisco IOS XE Release 2.2	ISG provides a default policy and the ability to configure a policy that determines the actions ISG will take upon session restart following the recovery of a DHCP-initiated IP session. The following commands were introduced or modified by this feature: **class type control**, **match vrf**.
IP Subscriber Session CLI Updates	Cisco IOS XE Release 2.2	Some of the commands that are used to configure ISG IP subscriber sessions were modified or replaced. The following commands were introduced or modified by this feature: **clear ip subscriber**, **debug ip subscriber**, **identifier interface**, **identifier ip src-addr**, **initiator**, **interface multiservice**, **ip subscriber interface, ip subscriber**, **show ip subscriber**.
ISG: Instrumentation: DHCP Lease Query Support	Cisco IOS XE Release 2.5.0	The DHCP Lease Query transaction is a DHCP transaction with special message types that enable, among other things, clients to query DHCP servers regarding the owner and the lease expiration time of an IP address. The following commands were introduced or modified: **ip dhcp-server**, **collect identifier**.

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: DHCP Proxy	Cisco IOS XE Release 2.2	This feature enables ISG to dynamically interact with DHCP and apply policies that influence the IP addresses that DHCP assigns subscribers.
ISG: Session: Creation: Interface IP Session: L2	Cisco IOS XE Release 2.5.0	ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.
ISG: Session: Creation: Interface IP Session: L3	Cisco IOS XE Release 2.5.0	ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.
ISG: Session: Creation: IP Session: Protocol Event (DHCP)	Cisco IOS XE Release 2.2	Most ISG sessions are created upon detection of a data flow that cannot be affiliated with an already active session. An ISG can be configured to create an IP session upon receipt of the first DHCP DISCOVER packet received from a subscriber.
ISG: Session: Creation: IP Session: Subnet and Source IP: L2	Cisco IOS XE Release 2.2	The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address.

Feature Name	Releases	Feature Configuration Information
ISG: Session: Creation: IP Session: Subnet and Source IP: L3	Cisco IOS XE Release 2.2	The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address.
ISG: Session: Multicast: Coexistence	Cisco IOS XE Release 2.5.0	The ISG Session Multicast Coexistence feature introduces the ability to host all the subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco ASR 10000 Series Aggregation Routers.
ISG: Session: VRF Transfer:	Cisco IOS XE Release 2.2	The ISG session is the primary component used for associating services and policies with specific data flows. ISG sessions are associated with virtual routing and forwarding instances when routing is required for the network service. ISG VRF transfer provides a means to dynamically switch an active session between virtual routing domains.
ISG: Static Session Creation	Cisco IOS XE Release 2.5.0	The ISG Static Session Creation feature enables administrator initiated static IP sessions. The following commands were introduced or modified by this feature: **initiator static subscriber list**, **ip source**, **ip subscriber list**, **show ip subscriber list**.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring MQC Support for IP Sessions

The MQC Support for IP Sessions feature provides modular quality of service (QoS) command-line interface (CLI) provisioning on Cisco Intelligent Services Gateway (ISG) IP sessions. It makes the full set of modular QoS CLI (MQC) syntax available for the sessions, whether they are configured locally or downloaded from a remote authentication, authorization, and accounting (AAA) server.

- Finding Feature Information, page 99
- Restrictions for MQC Support for IP Sessions, page 99
- Information About MQC Support for IP Sessions, page 100
- How to Configure MQC Support for IP Sessions, page 101
- Configuration Examples for MQC Support for IP Sessions, page 103
- Additional References, page 103
- Feature Information for MQC Support for IP Sessions, page 104

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 the Feature Information Table at the end of this document.

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

Restrictions for MQC Support for IP Sessions

General Restrictions

Creation of IP sessions over PPP sessions is not supported.

Note This document uses the generic term PPP to cover all protocol types. Examples of protocols include PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA).

Only the marking and policing features work in upstream traffic. All queuing, policing, and marking MQC features work in downstream traffic.

Class-level queues are allowed only at the child level in session policy maps. All other levels must have a single-level policy and use the default queues.

IP sessions over Gigabit EtherChannel (GEC) are not supported.

Because IP sessions cannot be load-balanced, load balancing is not supported on any system.

Information About MQC Support for IP Sessions

- Supported Interfaces, page 100
- ISG Policers, page 100
- Precedence Order in Policy Maps, page 100

Supported Interfaces

MQC is not supported on the following interfaces:

- Bridge-Group Virtual Interface (BVI)
- GEC
- Interfaces configured for Layer 2 Tunnel Protocol (L2TP) sessions (on L2TP Network Servers (LNS))

ISG Policers

You can create configurations to work on an IP session with multiple traffic classes, and with one or more of the traffic classes acting as a policer. ISG policer is retained for backward compatibility and is fully supported if you do not want to migrate to MQC now. Note that ISG policing is supported on traffic classes, but MQC is not supported for traffic classes.

An ISG session can be configured with the ISG policer (also called dynamic rate limiting) or MQC, but not both. You should either use the ISG policer or migrate fully to MQC. If you do not migrate fully from ISG policer to MQC, a misconfiguration will occur.

Precedence Order in Policy Maps

A policy map can be attached to one or more interfaces to specify a service policy. Configuration sources combined with context determines which QoS policy map is applied. The three configuration sources and their general order of precedence are as follows:

1. Per-user (per-subscriber) configuration
2. Service profile
3. Interface configuration

This order of precedence shows the general condition, that is, service profiles and per-user configurations have higher priority than interface configurations.

However, a change of authorization (CoA) per-user push replaces the current per-user configuration for any overlapping or common feature. Similarly, when a new service logs in, its configuration replaces any overlapping feature, from previously configured service profiles, that is not already in effect from a per-user configuration source

If the new service then logs off, the previously existing configuration is reapplied if no higher-precedence configuration source is in effect.

Given those precedence qualifications, the policy map is determined as follows:

- If there is no policy map on the session, the incoming policy map is not applied.

- If an existing policy map is configured from a higher priority source than an incoming one, the incoming policy map is not applied.
- If an existing policy map is configured from a lower priority source than an incoming one, the incoming policy map replaces it.

How to Configure MQC Support for IP Sessions

- Configuring Local Subscriber Profile for MQC Support, page 101
- Configuring ISG QoS for IP Sessions, page 102

Configuring Local Subscriber Profile for MQC Support

To configure a QoS policy map to define a service policy, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-name*
4. **service-policy** *policy-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *service-name* **Example:** `Router# (config)# policy-map type service service1`	Enters policy-map configuration mode. Specifies the policy-map name and its service configuration.

	Command or Action	Purpose
Step 4	**service-policy** *policy-name* **Example:** `Router# (config-service-policymap)# service-policy service-policy1`	Configures the service policy.

For information about configuring a local service profile, see the section “Configuring Per-Session QoS Using the ISG Framework” in the "Configuring ISG Control Policies" chapter in the *Cisco IOS XE Intelligent Services Gateway Configuration Guide*.

Configuring ISG QoS for IP Sessions

To associate a previously configured traffic class with a policy map, perform these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-name*
4. **class type traffic** *class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *service-name* **Example:** `Router# (config)# policy-map type service`	Enters policy-map configuration mode. Specifies the policy-map name and its service configuration.

	Command or Action	Purpose

Step 4	**class type traffic** *class-name*
	Example:
	`Router# (config-service-policymap)# class type traffic`
		Associates a previously configured traffic class with the policy map.

Configuration Examples for MQC Support for IP Sessions

- QoS Policy-Map Service Profile and Command Policy-Map Configurations Example, page 103

QoS Policy-Map Service Profile and Command Policy-Map Configurations Example

The following example shows how to configure a QoS policy map, a service profile, and a command policy map. The command policy map is then configured onto interface GigabitEthernet 0/0/0 with the **service-policy** keyword.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map match-any EF-customer
Router(config-cmap)# match access-group name CUSTOMER-EF
Router(config-cmap)# class-map match-any EF-WAN
Router(config-cmap)# match qos-group 6
Router(config-cmap)# policy-map PREMIUM_MARK_IN
Router(config-pmap)# class EF-customer
Router(config-pmap-c)# set cos 6
Router(config-pmap-c)# set dscp ef
Router(config-pmap-c)# set qos-group 6
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# set dscp af11
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# policy-map PREMIUM_UB_OUT
Router(config-pmap)# class EF-WAN
Router(config-pmap-c)# police cir 200000000
Router(config-pmap-c-police)# priority
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# policy-map type service PREMIUM_SERVICE
Router(config-service-policymap)# service-policy input PREMIUM_MARK_IN
Router(config-service-policymap)# service-policy output PREMIUM_UB_OUT
Router(config-service-policymap)# policy-map type control INT
Router(config-control-policymap)# class type control always event account-logon
Router(config-control-policymap-class-control)# 1 service-policy type service name
PREMIUM_SERVICE
Router(config-control-policymap-class-control)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# pppoe enable group global
Router(config-if)# service-policy type control INT
```

Additional References

Related Documents

Related Topic	Document Title
How to configure ISG control policies	“Configuring ISG Control Policies” module in this guide
How to configure QoS policies using the MQC	*Cisco IOS XEQuality of Service Solutions Configuration Guide*
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/techsupport

Feature Information for MQC Support for IP Sessions

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

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

Table 6 Feature Information for MQC Support for IP Sessions

Feature Name	Releases	Feature Information
MQC Support for IP Sessions	Cisco IOS XE Release 2.2	Provides MQC provisioning on Cisco ISG IP sessions. The following commands were introduced or modified: **policy-map** and **service-policy**.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Port-Bundle Host Key

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module contains information on how to configure ISG port-bundle host key functionality, which maps TCP packets from subscribers to a local IP address for the ISG gateway and a range of ports. This mapping allows an external portal to identify the ISG gateway from which a session originated.

- Finding Feature Information, page 107
- Prerequisites for the ISG Port-Bundle Host Key Feature, page 107
- Restrictions for the ISG Port-Bundle Host Key Feature, page 107
- Information About ISG Port-Bundle Host Key, page 108
- How to Configure ISG Port-Bundle Host Key, page 110
- Configuration Examples for ISG Port-Bundle Host Key, page 115
- Additional References, page 116
- Feature Information for ISG Port-Bundle Host Key, page 116

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 the Feature Information Table at the end of this document.

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

Prerequisites for the ISG Port-Bundle Host Key Feature

The external portal must support port-bundle host keys and must be configured with the same port-bundle host key parameters.

Restrictions for the ISG Port-Bundle Host Key Feature

The ISG Port-Bundle Host Key feature must be separately enabled at the portal and at all connected ISGs.

All ISG source IP addresses configured with the**source**command must be routable in the management network where the portal resides.

For each portal server, all connected ISGs must have the same port-bundle length.

The ISG Port-Bundle Host Key feature uses TCP. Packets will not be mapped for a subscriber who is not sending TCP traffic.

Specifying the Port-Bundle Host Key feature in a user profile will work only when the user profile is available prior to the arrival of IP packets; for example, for PPP sessions or for Dynamic Host Configuration Protocol (DHCP)-initiated IP sessions with transparent autologon.

Information About ISG Port-Bundle Host Key

- Overview of ISG Port-Bundle Host Key, page 108
- Port-Bundle Host Key Mechanism, page 108
- Port-Bundle Length, page 109
- Benefits of ISG Port-Bundle Host Key, page 110

Overview of ISG Port-Bundle Host Key

The ISG Port-Bundle Host Key feature serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISG gateway and a range of ports. This mapping allows the portal to identify the ISG gateway from which the session originated. The mapping also identifies sessions uniquely even when subscribers have overlapping IP addresses. The ISG Port-Bundle Host Key feature enables a single portal to be deployed for multiple Virtual Routing and Forwardings (VRFs) even when there are subscribers with overlapping IP addresses.

Port-Bundle Host Key Mechanism

With the ISG Port-Bundle Host Key feature, an ISG performs Port-Address Translation (PAT) and Network Address Translation (NAT) on the TCP traffic between the subscriber and the portal. When a subscriber TCP connection is set up, the ISG creates a port mapping that changes the source IP address to a configured ISG IP address and changes the source TCP port to a port allocated by the ISG. The ISG assigns a bundle of ports to each subscriber because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned port-bundle host key, or combination of the port bundle and ISG source IP address, uniquely identifies each subscriber. The host key is carried in RADIUS packets sent between the portal server and the ISG in the Subscriber IP vendor-specific attribute (VSA). The table below describes the Subscriber IP VSA. When the portal server sends a reply to the subscriber, the ISG uses the translation tables to identify the destination IP address and destination TCP port.

Table 7 Subscriber IP VSA Description

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Attribute Data
26	9	250 Account-Info	Subscriber IP	S *subscriber-ip-address* [:*port-bundle-number*] • S--Account-Info code for subscriber IP. • *subscriber-ip-address* [:*port-bundle-number*]--The port-bundle number is used only if the ISG Port-Bundle Host Key feature is configured.

For each TCP session between a subscriber and the portal, the ISG uses one port from the port bundle as the port map. Individual port mappings are flagged as eligible for reuse on the basis of inactivity timers, but are not explicitly removed once assigned. The number of port bundles is limited per ISG address, but there is no limit to the number of ISG IP addresses that can be configured for port bundle usage.

Port-Bundle Length

The port-bundle length is used to determine the number of ports in one bundle. By default, the port-bundle length is four bits. The maximum port-bundle length is ten bits. See the table below for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. You may want to increase the port-bundle length when you see frequent error messages about running out of ports in a port bundle.

Table 8 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per ISG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per ISG Source IP Address)
7	128	504
8	256	252
9	512	126
10	1024	63

Note For each portal server, all connected ISGs must have the same port-bundle length, which must correspond to the configured value given in the portal server's BUNDLE_LENGTH argument. If you change the port-bundle length on an ISG, be sure to make the corresponding change in the configuration on the portal.

Benefits of ISG Port-Bundle Host Key

- Support for Overlapped Subscriber IP Addresses Extended to Include External Portal Usage, page 110
- Portal Provisioning for Subscriber and ISG IP Addresses No Longer Required, page 110

Support for Overlapped Subscriber IP Addresses Extended to Include External Portal Usage

The ISG Port-Bundle Host Key feature enables external portal access regardless of subscriber IP address or VRF membership. Without the use of port-bundle host keys, all subscribers accessing a single external portal must have unique IP addresses. Furthermore, because port-bundle host keys isolate VRF-specific addresses from the domain in which the portal resides, routing considerations are simplified.

Portal Provisioning for Subscriber and ISG IP Addresses No Longer Required

Without the ISG Port-Bundle Host Key feature, a portal must be provisioned for subscriber and ISG IP addresses before the portal is able to send RADIUS packets to the ISG or send HTTP packets to subscribers. The ISG Port-Bundle Host Key feature eliminates the need to provision a portal in order to allow one portal server to serve multiple ISGs and to allow one ISG to be served by multiple portal servers.

How to Configure ISG Port-Bundle Host Key

- Enabling the ISG Port-Bundle Host Key Feature in a Service Policy Map, page 111
- Enabling the ISG Port-Bundle Host Key Feature in a User Profile or Service Profile on the AAA Server, page 112
- Configuring Port-Bundle Host Key Parameters, page 113
- Verifying ISG Port-Bundle Host Key Configuration, page 114

Enabling the ISG Port-Bundle Host Key Feature in a Service Policy Map

Perform this task to enable the ISG Port-Bundle Host Key feature in a service policy map. The ISG Port-Bundle Host Key feature will be applied to any subscriber who uses this service policy map.

Note We recommend that you use a dedicated service policy for the feature. Do not share a policy with other ISG features.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **ip portbundle**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-name* **Example:** `Router(config)# policy-map type service service1`	Creates or defines a service policy map, which is used to define an ISG service.
Step 4	**ip portbundle** **Example:** `Router(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key feature for the service.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Router(config-service-policymap)# end`
		(Optional) Returns to privileged EXEC mode.

- What to Do Next, page 112

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Enabling the ISG Port-Bundle Host Key Feature in a User Profile or Service Profile on the AAA Server

Perform this task to enable the ISG Port-Bundle Host Key feature in a user profile or service profile on the Authentication, Authorization, and Accounting (AAA) server.

SUMMARY STEPS

1. Add the Port-Bundle Host Key attribute to the user or service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Port-Bundle Host Key attribute to the user or service profile. **Example:** `26,9,1 = "ip:portbundle=enable"`	Enables the ISG Port-Bundle Host Key feature in the user or service profile.

- What to Do Next, page 112

What to Do Next

If you enabled the ISG Port Bundle Host Key feature in a service profile, you may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the "Configuring ISG Subscriber Services" module.

Configuring Port-Bundle Host Key Parameters

Perform this task to configure ISG Port-Bundle Host Key parameters and specify the interface for which ISG will use translation tables to derive the IP address and port number for downstream traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip portbundle**
4. **match access-list** *access-list-number*
5. **length** *bits*
6. **source** *interface-type interface-number*
7. **exit**
8. **interface** *type number*
9. **ip portbundle outside**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip portbundle** **Example:** `Router(config)# ip portbundle`	Enters IP portbundle configuration mode.
Step 4	**match access-list** *access-list-number* **Example:** `Router(config-portbundle)# match access-list 101`	Specifies packets for port mapping by specifying an access list to compare against the subscriber traffic.

	Command or Action	Purpose
Step 5	**length** *bits* **Example:** `Router(config-portbundle)# length 5`	Specifies the ISG port-bundle length, which determines the number of ports per bundle and bundles per group. • The default number of bits is 4. • The Cisco ASR 1000 series router supports a maximum port-bundle length of 7. • See the section "Port-Bundle Length" for more information.
Step 6	**source** *interface-type interface-number* **Example:** `Router(config-portbundle)# source loopback 0`	Specifies the interface for which the main IP address will be mapped by ISG to the destination IP addresses in subscriber traffic. • We recommend that you use a loopback interface as the source interface.
Step 7	**exit** **Example:** `Router(config-portbundle)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface for configuration. Enters interface configuration mode.
Step 9	**ip portbundle outside** **Example:** `Router(config-if)# ip portbundle outside`	Configures ISG to reverse translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber for the interface being configured.

Verifying ISG Port-Bundle Host Key Configuration

Perform this task to display information about ISG port-bundle host key configuration.

SUMMARY STEPS

1. **enable**
2. **show ip portbundle status** [**free** | **inuse**]
3. **show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number*
4. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip portbundle status** [**free** | **inuse**] **Example:** `Router# show ip portbundle status free`	Displays information about ISG port-bundle groups.
Step 3	**show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number* **Example:** `Router# show ip portbundle ip 10.10.10.10 bundle 65`	Displays information about a specific ISG port bundle.
Step 4	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Configuration Examples for ISG Port-Bundle Host Key

- ISG Port-Bundle Host Key Configuration Example, page 115

ISG Port-Bundle Host Key Configuration Example

The following example shows how to configure the ISG Port-Bundle Host Key feature to apply to all sessions:

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule
interface gigabitethernet0/0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
```

```
ip portbundle
 match access-list 101
 length 5
 source loopback 0
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Port-Bundle Host Key

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

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

Table 9 Feature Information for ISG Port-Bundle Host Key

Feature Name	Releases	Feature Configuration Information
ISG: Session: Auth: PBHK	Cisco IOS XE Release 2.2	The ISG Port-Bundle Host Key feature serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISG gateway and a range of ports. This mapping allows the portal to identify the ISG gateway from which the session originated. This module provides information about how to configure the ISG Port-Bundle Host Key feature.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG as a RADIUS Proxy

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. The ISG RADIUS proxy feature enables ISG to serve as a proxy between a client device that uses RADIUS authentication and an authentication, authorization, and accounting (AAA) server. When configured as a RADIUS proxy, ISG is able to “sniff” (look at) the RADIUS packet flows and, on successful authentication, it can transparently create a corresponding ISG session. This document describes how to configure ISG as a RADIUS proxy.

- Finding Feature Information, page 119
- Prerequisites for ISG RADIUS Proxy, page 119
- Restrictions for ISG RADIUS Proxy, page 119
- Information About ISG RADIUS Proxy, page 120
- How to Configure ISG as a RADIUS Proxy, page 122
- Configuration Examples for ISG RADIUS Proxy, page 132
- Additional References, page 134
- Feature Information for ISG RADIUS Proxy, page 135

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG RADIUS Proxy

The Cisco IOS image must support AAA and ISG.

Restrictions for ISG RADIUS Proxy

Wireless Internet service provider roaming (WISPr) attributes are not supported.

Information About ISG RADIUS Proxy

- Overview of ISG RADIUS Proxy, page 120
- ISG RADIUS Proxy Handling of Accounting Packets, page 120
- RADIUS Client Subnet Definition, page 121
- ISG RADIUS Proxy Support for Mobile Wireless Environments, page 121
- Benefits of ISG RADIUS Proxy, page 122

Overview of ISG RADIUS Proxy

Public wireless LANs (PWLANs) and wireless mesh networks can contain hundreds of access points, each of which must send RADIUS authentication requests to a AAA server. The ISG RADIUS proxy functionality allows the access points to send authentication requests to ISG, rather than directly to the AAA server. ISG relays the requests to the AAA server. The AAA server sends a response to ISG, which then relays the response to the appropriate access point.

When serving as a RADIUS proxy, ISG can pull user-specific data from the RADIUS flows that occur during subscriber authentication and authorization, and transparently create a corresponding IP session upon successful authentication. This functionality provides an automatic login facility with respect to ISG for subscribers that are authenticated by devices that are closer to the network edge.

When configured as a RADIUS proxy, ISG proxies all RADIUS requests generated by a client device and all RADIUS responses generated by the corresponding AAA server, as described in RFC 2865, RFC 2866, and RFC 2869.

ISG RADIUS proxy functionality is independent of the type of client device and supports standard authentication (that is, a single Access-Request/Response exchange) using both Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), Access-Challenge packets, and Extensible Authentication Protocol (EAP) mechanisms.

In cases where authentication and accounting requests originate from separate RADIUS client devices, ISG associates all requests with the appropriate session through the use of correlation rules. For example, in a centralized PWLAN deployment, authentication requests originate from the wireless LAN (WLAN) access point, and accounting requests are generated by the Access Zone Router (AZR). The association of the disparate RADIUS flows with the underlying session is performed automatically when the Calling-Station-ID (Attribute 31) is sufficient to make the association reliable.

Following a successful authentication, authorization data collected from the RADIUS response is applied to the corresponding ISG session.

Sessions that were created using ISG RADIUS proxy operation are generally terminated by receipt of an Accounting-Stop packet.

ISG RADIUS Proxy Handling of Accounting Packets

By default, ISG RADIUS proxy responds locally to accounting packets it receives. The **accounting method-list** command can be used to configure ISG to forward RADIUS proxy client accounting packets to a specified server. Forwarding of accounting packets can be configured globally for all RADIUS proxy clients or on a per-client basis.

RADIUS Client Subnet Definition

If ISG is acting as a proxy for more than one client device, all of which reside on the same subnet, the clients may be configured using a subnet definition rather than a discrete IP address for each device. This configuration method results in the sharing of a single configuration by all the client devices.

ISG RADIUS Proxy Support for Mobile Wireless Environments

ISG RADIUS proxy uses mobile wireless-specific processes to provide support for Gateway General Packet Radio Service (GPRS) Support Node (GGSN) environments. The following sections describe ISG RADIUS proxy attribute support and processing:

- Attribute Processing and RADIUS Request Correlation, page 121
- 3GPP Attribute Support, page 121

Attribute Processing and RADIUS Request Correlation

When authentication and accounting requests originate from separate RADIUS client devices, ISG uses correlation rules to associate all the requests with the appropriate session. The association of the disparate RADIUS flows with the underlying session is performed automatically when the Calling-Station-ID (Attribute 31) is sufficient to make the association reliable.

In mobile wireless environments attribute processing and the correlation of RADIUS requests with a session are implemented differently than in a PWLAN environment. For example, in a PWLAN environment the Attribute 31 is a MAC address, and in a GGSN environment Attribute 31 is a Mobile Station Integrated Services Digital Network (MSISDN), which is a plain number or alphanumeric string. In addition, in a GGSN environment the correlation of RADIUS requests can be performed using attributes other than Attribute 31.

ISG RADIUS proxy supports mobile wireless environments by allowing you to specify whether the RADIUS-proxy client uses a MAC or MSISDN format for Attribute 31. The format is specified using the**calling-station-id format** command. In addition, you can use the **session-identifier** command to configure ISG RADIUS proxy to use other attributes (apart from Attribute 31) to perform RADIUS request correlation.

3GPP Attribute Support

In GGSN environments ISG RADIUS proxy must understand and parse the Third Generation Partnership Project (3GPP) attributes described in the table below. These attributes form part of the accounting requests.

Table 10 3GPP Attributes Supported by ISG RADIUS Proxy

Attribute	Description	Vendor ID/type
3GPP-IMSI	The International Mobile Subscriber Identity (IMSI) for the user.	10415/1

Attribute	Description	Vendor ID/type
3GPP-Charging-Id	The charging ID for this Packet Data Protocol (PDP) context (this together with the GGSN address constitutes a unique identifier for PDP context).	10415/2
3GPP-SGSN-Address	The Serving GPRS Support Node (SGSN) address that is used by the GPRS Tunneling Protocol (GTP) control plane for handling of control messages. It may be used to identify the Public Line Mobile Network (PLMN) to which the user is attached.	10415/6

Benefits of ISG RADIUS Proxy

Use of ISG RADIUS proxy has the following benefits:

- Allows the complete set of ISG functionality to be applied to EAP subscriber sessions.
- Allows an ISG device to be introduced into a network with minimum disruption to the existing network access server (NAS) and AAA servers.
- Simplifies RADIUS server configuration because only the ISG, not every access point, must be configured as a client.

How to Configure ISG as a RADIUS Proxy

- Initiating ISG RADIUS Proxy IP Sessions, page 122
- Configuring ISG RADIUS Proxy Global Parameters, page 124
- Configuring ISG RADIUS Proxy Client-Specific Parameters, page 126
- Defining an ISG Policy for RADIUS Proxy Events, page 128
- Verifying ISG RADIUS Proxy Configuration, page 130
- Clearing ISG RADIUS Proxy Sessions, page 131

Initiating ISG RADIUS Proxy IP Sessions

Perform this task to configure ISG to initiate an IP session upon receipt of a RADIUS proxy message from a RADIUS client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber** {**interface** | **l2-connected**| **routed**}
5. **initiator radius-proxy**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Specifies an interface for configuration and enters interface configuration mode.

Step 4	**ip subscriber** {**interface** | **l2-connected**| **routed**}
	Example:
	`Router(config-if)# ip subscriber routed`
		Enables ISG IP subscriber support on an interface, specifies the access method that IP subscribers will use to connect to ISG on an interface and enters subscriber configuration mode.

Step 5	**initiator radius-proxy** **Example:** `Router(config-subscriber)# initiator radius-proxy`	Configures ISG to initiate IP sessions upon receipt of any RADIUS packet.

	Command or Action	Purpose

Step 6	**end**
	
	Example:
	`Router(config-subscriber)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Configuring ISG RADIUS Proxy Global Parameters

Perform this task to configure ISG RADIUS proxy parameters that are applied by default to all RADIUS proxy clients. Client-specific parameters can also be configured and take precedence over this global configuration. To specify a client-specific configuration, see the Configuring ISG RADIUS Proxy Client-Specific Parameters, page 126.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. aaa new-model
4. **aaa server radius proxy**
5. **session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
6. **calling-station-id format** {**mac-address** | **msisdn**}
7. **accounting method-list** {*method-list-name*| **default**}
8. **accounting port** *port-number*
9. **authentication port** *port-number*
10. **key** [**0** | 7] *word*
11. **timer** {**ip-address** | **request**} *seconds*
12. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	aaa new-model **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa server radius proxy** **Example:** `Router(config)# aaa server radius proxy`	Enters ISG RADIUS proxy server configuration mode.

Step 5	**session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
	Example:
	`Router(config-locsvr-proxy-radius)# session-identifier attribute 1`
		(Optional) Correlates the RADIUS server requests of a session and identifies the session in the RADIUS proxy module.

Step 6	**calling-station-id format** {**mac-address** | **msisdn**}
	Example:
	`Router(config-locsvr-proxy-radius)# calling-station-id format msisdn`
		Specifies the calling-station-id format.

Step 7	**accounting method-list** {*method-list-name*| **default**}
	Example:
	`Router(config-locsvr-proxy-radius)# accounting method-list fwdacct`
		Specifies the server to which accounting packets from RADIUS clients are forwarded.
		Note By default, ISG RADIUS proxy handles accounting packets locally.

Step 8	**accounting port** *port-number* **Example:** `Router(config-locsvr-proxy-radius)# accounting port 2222`	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. • The default port is 1646.
Step 9	**authentication port** *port-number* **Example:** `Router(config-locsvr-proxy-radius)# authentication port 1111`	Specifies the port on which the ISG listens for authentication packets from RADIUS clients. • The default port is 1645.

	Command or Action	Purpose
Step 10	**key** [**0** | **7**] *word* **Example:** `Router(config-locsvr-proxy-radius)# key radpro`	Configures the encryption key to be shared between ISG and RADIUS clients. • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 11	**timer** {**ip-address** | **request**} *seconds* **Example:** `Router(config-locsvr-proxy-radius)# timer ip-address 5`	Specifies the amount of time ISG waits for the specified event before terminating the session. • **ip-address** --Specifies the amount of time ISG waits for an IP address to be assigned to the session. • **request** --Specifies the amount of time ISG waits to receive an Access-Request from a client device.

Step 12	**end**
	Example:
	`Router(config-locsvr-proxy-radius)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Configuring ISG RADIUS Proxy Client-Specific Parameters

Perform this task to configure client-specific parameters for the ISG RADIUS proxy. This configuration applies to the specified client or subnet only. The client-specific configuration takes precedence over the global ISG RADIUS proxy configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. aaa new-model
4. **aaa server radius proxy**
5. **client** {**name** | *ip-address*} [*subnet-mask* [**vrf** *vrf-id*]]
6. **session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
7. **calling-station-id format** {**mac-address** | **msisdn**}
8. **accounting method-list** {*method-list-name*| **default**}
9. **accounting port** *port-number*
10. **authentication port** *port-number*
11. **key** [**0** | **7**] *word*
12. **timer** {**ip-address** | **request**} *seconds*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	aaa new-model **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa server radius proxy** **Example:** `Router(config)# aaa server radius proxy`	Enters ISG RADIUS proxy server configuration mode.
Step 5	**client** {**name** | *ip-address*} [*subnet-mask* [**vrf** *vrf-id*]] **Example:** `Router(config-locsvr-proxy-radius)# client 172.16.54.45 vrf myvrftable`	Specifies a RADIUS proxy client for which client-specific parameters can be configured, and enters RADIUS client configuration mode.

Step 6	**session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
	Example:
	`Router(config-locsvr-radius-client)# session-identifier vsa vendor 5335 type 123`
		(Optional) Correlates the RADIUS requests of a session and identifies the session in the RADIUS proxy module.

Step 7	**calling-station-id format** {**mac-address** | **msisdn**}
	Example:
	`Router(config-locsvr-radius-client)# calling-station-id format msisdn`
		Specifies the calling-station-id format.

	Command or Action	Purpose

Step 8	**accounting method-list** {*method-list-name*| **default**}
	Example:
	`Router(config-locsvr-radius-client)# accounting method-list fwdacct`
		Specifies the server to which accounting packets from RADIUS clients are forwarded.

Step 9	**accounting port** *port-number* **Example:** `Router(config-locsvr-radius-client)# accounting port 2222`	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. • The default port is 1646.
Step 10	**authentication port** *port-number* **Example:** `Router(config-locsvr-radius-client)# authentication port 1111`	Specifies the port on which the ISG listens for authentication packets from RADIUS clients. • The default port is 1645.
Step 11	**key** [**0** | **7**] *word* **Example:** `Router(config-locsvr-radius-client)# key radpro`	Configures the encryption key to be shared between ISG and RADIUS clients. • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 12	**timer** {**ip-address** | **request**} *seconds* **Example:** `Router(config-locsvr-radius-client)# timer ip-address 5`	Specifies the amount of time ISG waits for the specified event before terminating the session. • **ip-address** --Specifies the amount of time ISG waits for an IP address to be assigned to the session. • **request** --Specifies the amount of time ISG waits to receive an Access-Request from a client device.

Step 13	**end**
	Example:
	`Router(config-locsvr-radius-client)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Defining an ISG Policy for RADIUS Proxy Events

Perform this task to configure a policy that is applied at session start and causes ISG to proxy RADIUS packets to a specified server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. aaa new-model
4. **aaa authorization radius-proxy** {**default**| *list-name*} *method1* [*method2* [*method3*...]]
5. **policy-map type control** *policy-map-name*
6. **class type control** {*control-class-name* | **always**} **event session-start**
7. *action-number* **proxy** [**aaa list** {**default** | *list-name*}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	aaa new-model **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa authorization radius-proxy** {**default**| *list-name*} *method1* [*method2* [*method3*...]] **Example:** `Router(config)# aaa authorization radius-proxy RP group radius`	Configures AAA authorization methods for ISG RADIUS proxy subscribers. • A method may be either of the following: ◦ **group** *group-name*--Uses a subset of RADIUS servers for authorization as defined by the **server group** *group-name* command. ◦ **group radius** --Uses the list of all RADIUS servers for authorization as defined by the **aaa group server radius** command.

	Command or Action	Purpose
Step 5	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control proxyrule`	Creates or modifies a control policy map, which defines an ISG control policy and enters control policy-map configuration mode.

Step 6	**class type control** {*control-class-name* | **always**} **event session-start**
	Example:
	`Router(config-control-policymap)# class type control always event session-start`
		Specifies a control class for which actions may be configured and enters control policy-map class configuration mode.

Step 7	*action-number* **proxy** [**aaa list** {**default** | *list-name*}
	Example:
	`Router(config-control-policymap-class-control)# 1 proxy aaa list RP`
		Sends RADIUS packets to the specified server.
		• Use this command to configure ISG to forward RADIUS proxy packets to the server specified by the **aaa authorization radius-proxy** command in Step 4.

Step 8	**end**
	Example:
	`Router(config)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Verifying ISG RADIUS Proxy Configuration

Use one or more of the following commands to verify ISG RADIUS proxy configuration. The commands may be entered in any order.

SUMMARY STEPS

1. **show radius-proxy client** *ip-address* [**vrf** *vrf-id*]
2. **show radius-proxy session** {**id** *id-number* | **ip** *ip-address*}
3. **show subscriber session** [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask*| **timer** *timer-name*| **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier*| **username** *username*] [**detailed**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show radius-proxy client** *ip-address* [**vrf** *vrf-id*] **Example:** `Router# show radius-proxy client 10.10.10.10`	Displays RADIUS proxy configuration information and a summary of sessions for an ISG RADIUS proxy client.

Step 2	**show radius-proxy session** {**id** *id-number* | **ip** *ip-address*}
	Example:
	`Router# show radius-proxy session ip 10.10.10.10`
		Displays information about an ISG RADIUS proxy session.
		Note The ID can be found in the output of the show radius-proxy client command.

Step 3	**show subscriber session** [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask*| **timer** *timer-name*| **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier*| **username** *username*] [**detailed**] **Example:** `Router# show subscriber session detailed`	Displays information about subscriber sessions on an ISG device.

Clearing ISG RADIUS Proxy Sessions

Perform this task to clear ISG RADIUS proxy sessions.

SUMMARY STEPS

1. **enable**
2. **clear radius-proxy client** *ip-address*
3. **clear radius-proxy session** {**id** *id-number* | **ip** *ip-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**clear radius-proxy client** *ip-address* **Example:** `Router# clear radius-proxy client 10.10.10.10`	Clears all ISG RADIUS proxy sessions that are associated with the specified client device.

Step 3	**clear radius-proxy session** {**id** *id-number* | **ip** *ip-address*}
	Example:
	`Router# clear radius-proxy session ip 10.10.10.10`
		Clears a specific ISG RADIUS proxy session.
		Note The ID can be found in the output of the **show radius-proxy client** command.

Configuration Examples for ISG RADIUS Proxy

- ISG RADIUS Proxy Configuration Example, page 132
- ISG RADIUS Proxy and Layer 4 Redirect Example, page 133

ISG RADIUS Proxy Configuration Example

The following example configures ISG to serve as a RADIUS proxy and to send RADIUS packets to the method list called RP. FastEthernet interface 0/0 is configured to initiate IP sessions upon receipt of RADIUS packets.

```
!
aaa new-model
!
aaa group server radius EAP
server 10.2.36.253 auth-port 1812 acct-port 1813
!
aaa authorization radius-proxy RP group EAP
aaa accounting network FWDACCT start-stop group EAP
aaa accounting network FLOWACCT start-stop group EAP
!
aaa server radius proxy
session-identifier attribute 1
calling-station-id format msisdn
authentication port 1111
accounting port 2222
key radpro
message-authenticator ignore
! The method list "FWDACCT" was configured by the aaa accounting network FWDACCT
! start-stop group EAP command above.
accounting method-list FWDACCT
client 10.45.45.2
timer request 5
!
client 10.45.45.3
key aashica#@!$%&/
timer ip-address 120
!
!
! This control policy references the method list called "RP" that was configured using
the aaa authorization radius-proxy command above.
policy-map type control PROXYRULE
```

```
class type control always event session-start
1 proxy aaa list RP
!
!
!
bba-group pppoe global
!
!
interface GigabitEthernet 2/1/0
ip address 10.45.45.1 255.255.255.0
ip subscriber routed
initiator radius-proxy
no ip route-cache cef
no ip route-cache
no cdp enable
!
! The control policy "PROXYRULE" is applied to the interface.
service-policy type control PROXYRULE
!
!
radius-server host 10.2.36.253 auth-port 1812 acct-port 1813 key cisco
radius-server host 10.76.86.83 auth-port 1665 acct-port 1666 key rad123
radius-server vsa send accounting
radius-server vsa send authentication
aaa new-model
!
!
aaa group server radius EAP
server 10.2.36.253 auth-port 1812 acct-port 1813
!
```

ISG RADIUS Proxy and Layer 4 Redirect Example

The following example shows an ISG policy configured for both ISG RADIUS proxy and Layer 4 redirection:

```
aaa authorization network default local
!
redirect server-group REDIRECT
 server ip 10.255.255.28 port 23
 !
class-map type traffic match-any traffic1
match access-group input 101
!
policy-map type service service1
 class type traffic traffic1
  redirect list 101 to group REDIRECT
!
policy-map type control PROXYRULE
 class type control always event session-start
  1 proxy aaa list RP
  2 service-policy type service name service1
!
access-list 101 permit tcp host 10.45.45.2 any
```

The following example shows corresponding sample output from the **show subscriber session** command:

```
Router# show subscriber session username 12345675@cisco
Unique Session ID: 66
Identifier: aash
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:40, Last Changed: 00:00:00
Policy information:
  Authentication status: authen
  Active services associated with session:
    name "service1", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map PROXYRULE
```

```
      condition always event session-start
        1 proxy aaa list RP
        2 service-policy type service name service1
Session inbound features:
Feature: Layer 4 Redirect ------>>> L4 redirect is applied to the session at session start
  Rule table is empty
Traffic classes:
  Traffic class session ID: 67
   ACL Name: 101, Packets = 0, Bytes = 0
Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0
Configuration sources associated with this session:
Service: service1, Active Time = 00:00:40
Interface: FastEthernet0/1, Active Time = 00:00:40
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2869	RADIUS Extensions

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/techsupport

Feature Information for ISG RADIUS Proxy

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

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

Table 11 Feature Information for ISG RADIUS Proxy

Feature Name	Releases	Feature Information
ISG: AAA Wireless Enhancements	Cisco IOS XE Release 2.5.0	This feature enhances ISG RADIUS proxy to provide additional support for mobile wireless environments. It includes changes to RADIUS attribute 31 processing. The following commands were introduced by this feature: **session-identifier**, **calling-station-id format**.
ISG: Authentication:RADIUS Proxy WiMax Enhancements	Cisco IOS XE Release 2.5.0	This feature enhances ISG RADIUS proxy to provide additional support for WiMax broadband environments.

Feature Name	Releases	Feature Information
RADIUS Proxy Enhancements for ISG	Cisco IOS XE Release 2.2	This feature enables ISG to serve as a proxy between a client device that uses RADIUS authentication and an AAA server. This functionality enables ISG to be deployed in PWLAN and wireless mesh networks where authentication requests for mobile subscribers must be sent to specific RADIUS servers. The following commands were introduced or modified by this feature: **aaa authorization radius-proxy**, **aaa server radius proxy**, **accounting method-list**, **accounting port**, **authentication port**, **clear radius-proxy client**, **clear radius-proxy session**, **client** (ISG RADIUS proxy), **debug radius-proxy**, **initiator radius-proxy**, **key** (ISG RADIUS proxy), **message-authenticator ignore**, **proxy** (ISG RADIUS proxy), **show radius-proxy client**, **show radius-proxy session**, **timer** (ISG RADIUS proxy).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring RADIUS-Based Policing

The RADIUS-Based Policing feature enables Intelligent Services Gateway (ISG) to make automatic changes to the policing rate of specific sessions and services.

- Finding Feature Information, page 139
- Prerequisites for RADIUS-Based Policing, page 139
- Restrictions for RADIUS-Based Policing, page 139
- Information About RADIUS-Based Policing, page 140
- How to Configure RADIUS-Based Policing, page 143
- Configuration Examples for RADIUS-Based Policing, page 150
- Additional References, page 156
- Feature Information for RADIUS-Based Policing, page 157

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 the Feature Information Table at the end of this document.

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

Prerequisites for RADIUS-Based Policing

You must configure all traffic classes on the ISG before referencing the classes in policy maps.

You must configure and apply QoS policy maps on the ISG before the ISG can construct and apply an ANCP-based dynamic service policy.

Restrictions for RADIUS-Based Policing

Per-service policing cannot be configured on the class-default class at the parent level of a hierarchical policy. You can configure per-service policing on class-default classes at the child or grandchild level.

Transient policies are not visible in the running-configuration file. Only the original policy configuration is visible.

Parameterized QoS is not supported for IP sessions.

The parameterized Access Control List (pACL) name is limited to 80 characters. The pACL name is formed by concatenating the ACL entries in the RADIUS CoA or Access-Accept message to the ACL name configured on the ISG. If the pACL name exceeds 80 characters the parameterization operation fails and an error message displays. For a CoA message, the ISG also sends a negative Ack (Nack) response to the RADIUS server.

The RADIUS-Based Policing feature is supported only on PPP Termination and Aggregation (PTA) sessions in Cisco IOS Release XE 3.1 and earlier releases; it is supported on L2TP access concentrator (LAC) or L2TP network server (LNS) sessions in Cisco IOS Release XE 3.2 and later releases.

If there is a concatenated service-activation push, QoS policies are applied first and then service activation occurs. If a concatenated service activation fails, any QoS policies applied are not rolled back.

Information About RADIUS-Based Policing

- RADIUS Attributes, page 140
- Parameterized QoS Policy as VSA 1, page 143
- Parameterization of QoS ACLs, page 143

RADIUS Attributes

RADIUS communicates with ISG by embedding specific attributes in Access-Accept and change of authentication (CoA) messages. RADIUS-based shaping and policing employs this exchange of attributes to activate and deactivate services and to modify the active quality of service (QoS) policy applied to a session. The RADIUS server determines the new shaping or policing rate based on vendor-specific attributes (VSAs) configured in a subscriber’s user profile on RADIUS and on the Advanced Node Control Protocol (ANCP)-signaled rate received from ISG.

After receiving the Access-Accept or CoA message, ISG copies the original policy map applied to the session and changes the shaping or policing rate of the copied, transient policy as indicated by RADIUS. ISG does not change the shaping rate of the original policy. After changing the transient policy, ISG applies the transient policy to the subscriber service.

The following sections describe the RADIUS attributes used in RADIUS-based policing:

- RADIUS Attributes 250 and 252, page 140
- Cisco VSA 1, page 141

RADIUS Attributes 250 and 252

RADIUS uses attribute 250 in Access-Accept messages and attribute 252 in CoA messages to activate and deactivate parameterized services. ISG services are configured locally on the ISG device; RADIUS sends only the service name.

Attributes 250 and 252 have the following syntax for service activation:

Access-Accept Messages

```
250 "Aservice(parameter1=value,parameter2=value,...)"
```

CoA Messages

```
252 0b "service(parameter1=value,parameter2=value,...)"
```

RADIUS uses only Attribute 252 in a CoA message when deactivating a service. RADIUS sends the same information in Attribute 252 that was used for service activation, except that service deactivation uses 0c in the syntax instead of the 0b parameter used for service activation.

```
252 0xC "service(parameter1=value,parameter2=value,...)"
```

VSA 252 has the above syntax for service deactivation.

Cisco VSA 1

RADIUS uses a vendor-specific attribute (VSA) 1 command to modify the active QoS policy on a session. This VSA has the following format:

```
av-pair = "policy-type=command 9 parameter1 ,...,parametern"
```

Use the following Cisco VSA 1 format to add and remove classes and QoS actions to and from the QoS policy that is currently active on a session:

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

Before the ISG can construct a policy using the policing parameters specified in the RADIUS message, a QoS policy must be active on the session. If a QoS policy is not active in the specified direction, the ISG does not create the policy.

When implementing the changes specified in the Cisco VSA, the ISG does not make the changes to the originally configured QoS policy on the ISG device. Instead, the ISG copies the active QoS policy for the session and then makes the required changes to the policy copy, which is referred to as a *transient policy* . The originally configured QoS policy on the ISG device is not changed.

The following sections describe the Cisco VSA 1 commands used to automatically modify policing parameters of active policies:

- Add-Class Primitive, page 141
- Remove-Class Primitive, page 142

Add-Class Primitive

To add or modify QoS actions to a traffic class, use the add-class primitive. This attribute has the following format:

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list
```

- *target* field-- Indicates the QoS policy to be modified. The only valid value for this field is sub, which indicates the active QoS policy attached to the subscriber session. The Access-Accept or CoA message that includes this attribute must be targeting a subscriber session.
- *class-list* field--A list of class names enclosed in parentheses that identifies the traffic class to which the specified QoS action applies. The class names you specify must be either user-configured class maps or the system-generated class-default class. The order in which you specify the class names indicates the hierarchical level of the class within the QoS policy.

For example, the following class list identifies the class named “voip”, which gets added to a nested policy. The VoIP class is configured in a nested child policy that is applied to the parent class-default class.

```
(class-default, voip)
```

ISG Configuration

```
policy-map child
 class voip
 police 8000
policy-map parent
 class class-default
 service-policy child
```

The following class list specifies the voip-2 class, which is configured in a nested policy that is applied to the voip-aggregate class of another nested child policy. The policy containing the voip-aggregate class is in turn nested under the class-default class of the QoS policy attached to the target session.

```
(class-default, voip-aggregate, voip-2)
```

MSQ Configuration

```
policy-map child2
 class voip-2
 police 8000
policy-map child1
 class voip-aggregate
 police 20000
 service-policy child2
policy-map parent
 class class-default
 shape 512000
 service-policy child1
```

The *qos-actions-list* field indicates a QoS action such as police, followed by the action parameters enclosed in parentheses and separated by commas. For example, the following sample configuration specifies the police action and defines the parameters *bps* , *burst-normal* , *burst-max* , *conform-action* , *exceed-action* , and *violate-action* . Parentheses enclose the action parameters.

```
(voip-aggregate police(200000,9216,0,transmit,drop,drop))
```

Note The example shows a double-parenthesis at the end, because the syntax of the VSA specifies enclosure of the target, class-list, and qos-actions-list in parentheses.

Remove-Class Primitive

To remove traffic classes and QoS actions defined in the active QoS policy on a session, use the remove-class primitive. This attribute has the following format:

```
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

- target field--Indicates the QoS policy to be modified. Currently, the only valid value for this field is sub, which indicates the active QoS policy attached to the subscriber session. The Access-Accept or CoA message that includes this attribute must be targeting a subscriber session.
- class-list field--A list of class names enclosed in parentheses that identifies the class or classes to be removed. The class names you specify must be either user-configured class maps or the system-generated class-default class. The order in which you specify the class names indicates the hierarchical level of the class within the QoS policy.

For example, the following VSA1 attribute removes the Bronze class and all associated QoS policy actions from the nested child policy that is applied to the parent class-default class:

```
qos-policy-out=remove-class(sub,(class-default,Bronze))
```

When you remove a traffic class from a QoS policy, all of the attributes for the class are also removed. To re-add the class with the same attributes, you must reissue the add-class RADIUS attribute and provide the required parameters and values.

Parameterized QoS Policy as VSA 1

Multiple complex strings in a CoA message are not supported because they do not display the correct behavior of VSA 1, as shown in the following example:

```
vsa cisco 250 S152.1.1.2
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct1(1)((c-d,tv)1(10000))"
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct(1)((c-d,voip)1(10000))"
```

In the example:

- All services are enabled on target.
- Parameterized QoS policy in the second command syntax is not echoed in the ISG service.
- Parameterized QoS policy in the first command syntax is echoed.

Parameterization of QoS ACLs

The Parameterization of QoS Access Control Lists (ACLs) feature supports multiple ISG and QoS parameterized services in a single Access-Accept or CoA message. This feature allows the authentication, authorization, and accounting (AAA) device to change parameters dynamically.

How to Configure RADIUS-Based Policing

- Configuring Per-Session Shaping, page 143
- Configuring Per-Service Shaping and Policing, page 145
- Verifying RADIUS-Based Policing, page 148

Configuring Per-Session Shaping

- Configuring a QoS Policy with Shaping on ISG, page 143
- Configuring Per-Session Shaping on RADIUS, page 145

Configuring a QoS Policy with Shaping on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset* } **aal5** *subscriber-encap*]
6. **service-policy** *policy-map-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map child`	Creates or modifies a policy-map and enters policy-map configuration mode.

Step 4	**class class-default**
	Example:
	`Router(config-pmap)# class class-default`
		Modifies the class-default traffic class.

Step 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset* } **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate.

	Command or Action	Purpose
Step 6	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy child`	Applies the child policy map to the parent class-default class. • *policy-map-name* —Name of the child policy map.

Step 7	**end**
	Example:
	`Router(config-pmap-c)# end`
		Exits policy-map class configuration mode and returns to Privileged EXEC mode.

Configuring Per-Session Shaping on RADIUS

To use RADIUS to set the shaping rate for a subscriber session, configure the following Cisco VSA in the user profile on RADIUS:

```
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default), shape(rate))"
```

When the ISG receives a RADIUS Access-Accept or change of authentication (CoA) message with this VSA included, the ISG copies the currently configured policy map applied on the session and changes the shaping rate of the transient parent class-default class to the shaping rate specified in the VSA. The ISG makes changes only to the transient policy; no changes are made to the original policy map. After changing the transient policy, the ISG applies the transient policy to the subscriber session.

Configuring Per-Service Shaping and Policing

- Configuring a Hierarchical QoS Child Policy with Shaping and Policing on ISG, page 145
- Configuring a Hierarchical QoS Parent Policy with Shaping and Policing on ISG, page 147
- Configuring Per-Service Shaping and Policing on RADIUS, page 148

Configuring a Hierarchical QoS Child Policy with Shaping and Policing on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*]
6. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map child`	Creates or modifies a policy map and enters policy-map configuration mode.

Step 4	**class** *class-name*
	Example:
	`Router(config-pmap)# class voip`
		Configures QoS parameters for the traffic class you specify and enters policy-map class configuration mode.
		• *class-name* —Name of a traffic class you previously configured using the **class-map** command.

Step 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate.
Step 6	**police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] **Example:** `Router(config-pmap-c)# police 10000`	Configures traffic policing. **Note** Specify either the **shape** command or the **police** command for a traffic class, but not both commands for the same class.

Step 7	**end**
	Example:
	`Router(config-pmap-c)# end`
		Exits policy-map class configuration mode and returns to Privileged EXEC mode.
		Note Repeat steps 3 through 7 for each child policy map you want to create, or repeat steps 4 through 7 for each traffic class you want to define in each policy map.

Configuring a Hierarchical QoS Parent Policy with Shaping and Policing on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset* } **aal5** *subscriber-encap*]
6. **service-policy** *policy-map-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map parent`	Creates or modifies a policy map.

Step 4	**class class-default**
	Example:
	`Router(config-pmap)# class class-default`
		Modifies the class-default traffic class and enters policy-map class configuration mode.

Step 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset* } **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate.

	Command or Action	Purpose
Step 6	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy child`	Applies the child policy map to the parent class-default class. • *policy-map-name* —Name of the child policy map.
Step 7	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.

Configuring Per-Service Shaping and Policing on RADIUS

To use RADIUS to set the shaping and policing rate for a subscriber service, configure the following Cisco VSAs in the service profile on RADIUS:

```
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), shape(rate))"
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), police(rate))"
```

When the ISG receives a RADIUS Access-Accept or CoA message with these VSAs included, the ISG copies the originally configured policy map that is active on the session and changes the shaping or policing rate of the traffic class specified in the class-list field. The ISG makes changes only to the transient policy and applies the transient policy to the subscriber service; no changes are made to the original policy map.

Note Per-service shaping and policing do not apply to the parent class-default class.

For more information, see the "RADIUS Attributes" section.

Verifying RADIUS-Based Policing

To verify the configuration of RADIUS-based policing on the ISG, use any of the following commands in privileged EXEC mode.

Command or Action	Purpose
`Router#`**show policy-map interface**	Displays the configuration of all classes configured for all policy maps attached to all interfaces.

Command or Action	Purpose
`Router#` **show policy-map interface** *interface [input* | *output]*	Displays the configuration of all classes configured for all inbound or outbound policy maps attached to the specified interface. • *interface* is the name of the interface or subinterface. • **input** indicates the statistics for the attached inbound policy. • **output** indicates the statistics for the attached outbound policy. If you do not specify **input** or **output**, the router shows information about all classes that are configured for all inbound and outbound policies attached to the interface you specify.
`Router#` **show policy-map** *policy-map-name*	Displays the configuration of all of the traffic classes contained in the policy map you specify. • *policy-map-name* is the name of the policy map for the configuration information you want to appear. • If you do not specify a value for the *policy-map-name*argument, the command shows the configuration of all policy maps configured on the router.
`Router#` **show policy-map** *policy-map-name* **class** *class-name*	Displays the configuration of the class you specify. The policy map you specify includes this class. • *policy-map-name* is the name of the policy map that contains the class configuration you want to appear. • *class-name* is the name of the class whose configuration you want to. If you do not specify a value for the *class-name*argument, the command shows the configuration of all of the classes configured in the policy map.
`Router#` **show policy-map session** [**output** | **output** |*uid*]	Displays the inbound or outbound policy maps configured per session. Also displays the dynamic policy map that is applied to the subscriber session. If you do not specify any arguments, the command shows all sessions with configured policy maps, which might impact performance. • **input** indicates inbound policy maps. • **output** indicates outbound policy maps. • *uid* is the session ID.

Command or Action	Purpose
`Router#` **show running-config**	Displays the running-configuration file, which contains the current configuration of the router, including the default QoS policy.
`Router#` **show running-config interface** *interface*	Displays the configuration of the interface you specify that is currently configured in the running-config file, including any service policies attached to the interface.

Configuration Examples for RADIUS-Based Policing

- Example Adding Parameterization of QoS ACLs, page 150
- Example Setting the Shaping Rate Using an Access-Accept Message, page 151
- Example Setting the Shaping Rate Using a CoA Message, page 152
- Example Setting the Policing Rate Using an Access-Accept Message, page 154
- Example Setting the Policing Rate Using a CoA Message, page 155

Example Adding Parameterization of QoS ACLs

The following example shows how to parameterize the set source IP address and destination IP address parameter, set-src-dst-ip-in-acl, through CoA or Access-Accept messages. The QoS parameterized service is added in the parameterized QoS service RADIUS form:

```
VSA252 0b q-p-out=IPOne(1)((c-d,voip)13(10.10.1.0/28,10.3.20/29))
! The above command activates the service in a CoA message.
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default,voip),set-src-dst-
ip-in-acl(10.10.1.0/28,10.3.20/29))"
! The above command activates the service in a Access-Accept message.
```

The router is configured as follows:

```
ip access-list extended IPOne-acl
 remark Voice-GW
 permit ip host 10.0.1.40 any
!
class-map match-any voip
  match access-group name IPOne-acl
!
class-map type traffic match-any IPOne
 match access-group output name IPOne-acl
 match access-group input name IPOne-acl
 !
!
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
!
policy-map output_parent
  class class-default
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action
drop
  service-policy output_child
  !
!
```

```
policy-map output_child
  class voip
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action
drop
    !
  !
!
! RADIUS relays the string for service activation. After the VSA is received, a new ACL
is created.
ip access-list extended IPOne-acl-10.10.1.0/28,10.3.20/29
 remark Voice-GW
 permit ip host 10.0.1.40 any
 permit ip 10.10.1.0 0.0.0.15 any
 permit ip any 10.10.1.0 0.0.0.15
 permit ip 10.3.2.0 0.0.0.7 any
 permit ip any 10.3.2.0 0.0.0.7
!
! A new class map is created.
class-map match-any voip-10.10.1.0/28,10.3.20/29
  match access-group name IPOne-acl-10.10.1.0/28,10.3.20/29
!
! The old class is replaced with the new class in the output QoS policy of the
subscriber, along with any other attributes.
```

Adding Parameterization of QoS ACLs with ISG Service Accounting

The following example shows how to add QoS accounting by configuring the ISG accounting service:

```
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
 class type traffic default in-out
 !
!
! After the VSA is received, a new traffic class map is created on the service.
class-map type traffic match-any IPOne-10.10.1.0/28,10.3.2.0/29
 match access-group output name IPOne-acl-10.10.1.0/28$10.3.2.0/29
 match access-group input name IPOne-acl-10.10.1.0/28$10.3.2.0/29
!
! A new ISG service is created.
policy-map type service IPOne(tc_in=IPOne-acl-10.10.1.0/28$10.3.2.0/29)
 10 class type traffic IPOne-10.10.1.0/28,10.3.2.0/29
  accounting aaa list default
 !
 class type traffic default in-out
!
```

Example Setting the Shaping Rate Using an Access-Accept Message

The examples in this section illustrate how to set the shaping rate of a session using an access-accept message.

ISG Original Policy

This configuration example uses a RADIUS Access-Accept message to change the shaping rate of a session:

```
class-map match-any Premium
  match access-group name Premium_Dest
!
policy-map Child
  class Premium
    shape average 5000
!
policy-map Parent
  class class-default
```

```
    shape average 10000
    service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA adds the class-default class to the QoS policy attached to the subscriber session for outbound traffic and shapes the class-default class to 120,000 bps.

```
radius subscriber 6
  framed protocol ppp
  service framed
  vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default),
shape(120000))"  [New shaping rate]
```

RADIUS Access-Accept Message

The ISG receives the following RADIUS Access-Accept message. Notice that the above Cisco VSA configured in the user’s profile is present in the Access-Accept message and that the parent shaping rate has changed to 120,000.

```
1d21h: RADIUS: Received from id 1645/3 192.168.1.6:1812, Access-Accept, len 100
1d21h: RADIUS: authenticator 4A 2C F7 05 4B 88 38 64 - DE 60 69 5A 4B EE 43 E1
1d21h: RADIUS: Framed-Protocol [7] 6 PPP [1]
1d21h: RADIUS: Service-Type [6] 6 Framed [2]
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default),
shape(120000))"
1d21h: RADIUS(0000000D): Received from id 1645/3
1d21h: SSS PM [uid:4][65ADE2E8]: SERVICE: Adding Service attachment to event
1d21h: RADIUS/ENCODE(0000000D):Orig. component type = PPoE
1d21h: RADIUS(0000000D): Config NAS IP: 0.0.0.0
1d21h: RADIUS(0000000D): sending
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent. While the parent shaping rate, as previously shown, changes to 120,000, the shaping rate displayed in the transient New_Parent policy is the old rate of 10,000, as seen in the following example. The child policy remains unchanged.

```
policy-map New_Parent    [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy Child
```

Example Setting the Shaping Rate Using a CoA Message

The examples in this section illustrate how to set the shaping rate of a session using a CoA message.

ISG Original Policy

This configuration example uses a RADIUS CoA message to change the shaping rate of a session:

```
class-map match-any Premium
  match access-group name Premium_Dest
!
policy-map Child
```

```
  class Premium
    shape average 5000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA adds the class-default class to the QoS policy attached to the subscriber session for outbound traffic and shapes the class-default class to 120,000 bps.

```
radius subscriber 1047
  vsa cisco 250 S192.168.1.2
  vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default),
shape(120000))"  [New shaping rate]
```

RADIUS CoA Message

The ISG receives the following RADIUS CoA message. Notice that the above Cisco VSA configured in the user's profile is present in the CoA message.

```
1d21h: RADIUS: COA received from id 0 192.168.1.6:1700, CoA Request, len 106
1d21h: COA: 192.168.1.6 request queued
1d21h: RADIUS: authenticator FF A2 6B 63 06 F0 E6 A3 - 0D 04 6C DC 01 0A BE F1
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.2"
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default),
shape(120000))"
1d21h: ++++++ CoA Attribute List ++++++
1d21h: 63C829B0 0 00000009 ssg-account-info(427) 10 S192.168.1.2
1d21h: 63C82A18 0 00000009 qos-policy-out(378) 45 add-class(sub,(class-default),
shape(120000))
1d21h:
ISG#
1d21h: RADIUS(00000000): sending
1d21h: RADIUS(00000000): Send CoA Ack Response to 192.168.1.6:1700 id 0, len 65
1d21h: RADIUS: authenticator 62 B4 B0 1A 90 10 01 01 - F6 C8 CD 17 79 15 C7 A7
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.2"
1d21h: RADIUS: Vendor, Cisco [26] 27
1d21h: RADIUS: ssg-account-info [250] 21 "$IVirtual-Access2.2"
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the CoA message, the ISG changes the shaping rate of the parent class-default class to 120,000 bps. However, the shaping rate displayed in the transient New_Parent policy is the old rate of 10,000, as seen in the following example. The child policy remains unchanged.

```
policy-map Child
  class Premium
    shape average 5000

policy-map New_Parent    [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy Child
```

Example Setting the Policing Rate Using an Access-Accept Message

The examples in this section illustrate how to set the policing rate of a traffic class using an access-accept message.

ISG Original Policy

This configuration example uses a RADIUS Access-Accept message to change the policing rate of a traffic class at the child level of a hierarchical policy:

```
class-map match-any Premium
match access-group name Premium_Dest
!
policy-map Child
  class Premium
    shape average 5000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA changes the policing rate of the Premium class in the Child policy. The Child policy is applied to the class-default class of the Parent policy.

```
radius subscriber 6
  framed protocol ppp
  service framed
  vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
```

RADIUS Access-Accept Message

The ISG receives the following RADIUS Access-Accept message. Notice that the above Cisco VSA configured in the user's profile is present in the Access-Accept message.

```
1d21h: RADIUS: Received from id 1645/3 192.168.1.6:1812, Access-Accept, len 100
1d21h: RADIUS: authenticator 4A 2C F7 05 4B 88 38 64 - DE 60 69 5A 4B EE 43 E1
1d21h: RADIUS: Framed-Protocol [7] 6 PPP [1]
1d21h: RADIUS: Service-Type [6] 6 Framed [2]
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default,
Premium), police(200000))"
1d21h: RADIUS(0000000D): Received from id 1645/3
1d21h: SSS PM [uid:4][65ADE2E8]: SERVICE: Adding Service attachment to event
1d21h: RADIUS/ENCODE(0000000D):Orig. component type = PPoE
1d21h: RADIUS(0000000D): Config NAS IP: 0.0.0.0
1d21h: RADIUS(0000000D): sending
```

ISG Transient Policy

The ISG copies the service policy that is currently applied to the session and creates a transient policy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the

Access-Accept message, the ISG adds the policing rate to the Premium traffic class. The Premium class is configured in the transient New_Child policy, which is applied to the New_Parent class-default class.

```
policy-map New_Child    [New cloned child policy]
  class Premium
    police 200000    [New policing rate]
    shape average 5000
!
policy-map New_Parent    [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy New_Child    [New cloned child policy attached to the new
    cloned parent policy]
```

Example Setting the Policing Rate Using a CoA Message

The examples in this section illustrate how to set the policing rate of a service using a CoA message.

ISG Original Policy

This configuration example uses a RADIUS CoA message to change the policing rate of a service and is based on the following ISG configuration:

```
policy-map Child
  class Premium
    police 12000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
```

RADIUS Configuration

The following Cisco VSA is configured in a user’s profile on RADIUS. This VSA modifies the Premium class of the Child policy, which is applied to the class-default class of the Parent policy.

```
radius subscriber 1048
vsa cisco 250 S192.168.1.10
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
```

RADIUS CoA Message

The ISG receives the following RADIUS CoA message. Notice that the above Cisco VSA configured in the user profile is present in the CoA message.

```
1d21h: RADIUS: COA received from id 0 192.168.1.6:1700, CoA Request, len 106
1d21h: COA: 192.168.1.6 request queued
1d21h: RADIUS: authenticator FF A2 6B 63 06 F0 E6 A3 - 0D 04 6C DC 01 0A BE F1
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default,
Premium), police(200000))"
1d21h: ++++++ CoA Attribute List ++++++
1d21h: 63C829B0 0 00000009 ssg-account-info(427) 10 S192.168.1.10
1d21h: 63C82A18 0 00000009 qos-policy-out(378) 45 add-class(sub,(class-default, Premium),
police(200000))
1d21h:
ISG#
1d21h: RADIUS(00000000): sending
1d21h: RADIUS(00000000): Send CoA Ack Response to 192.168.1.6:1700 id 0, len 65
1d21h: RADIUS: authenticator 62 B4 B0 1A 90 10 01 01 - F6 C8 CD 17 79 15 C7 A7
```

```
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 27
1d21h: RADIUS: ssg-account-info [250] 21 "$IVirtual-Access2.2"
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the Access-Accept message, the ISG changes the policing rate of the Premium traffic class from 5000 bps to 200,000 bps. The Premium class is configured in the New_Child policy, which is applied to the New_Parent class-default class.

```
policy-map New_Child    [New cloned child policy]
  class Premium
    police 200000    [New policing rate]
!
policy-map New_Parent    [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy New_Child    [New cloned child policy attached to the new
    cloned parent policy]
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RADIUS-Based Policing

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

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

Table 12 Feature Information for RADIUS-Based Policing

Feature Name	Releases	Feature Information
ISG: Policy Control: Policy Server: RADIUS-Based Policing	Cisco IOS XE Release 2.4	The RADIUS-Based Policing feature extends ISG functionality to allow the use of a RADIUS server to provide subscriber policy information. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router.
RADIUS-Based Policing Attribute Modifications	Cisco IOS XE Release 2.4	The RADIUS-Based Policing Attribute Modifications feature allows the RADIUS server to communicate with the ISG by embedding specific attributes in Access-Accept and CoA messages. RADIUS-based shaping and policing employs this exchange of attributes to activate and deactivate services, and to modify the active QoS policy applied to a session. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router.
Parameterization of QoS ACLs	Cisco IOS XE Release 2.4	The Parameterization of QoS ACLs feature provides enhancements for QoS ACLs. This feature allows the AAA device to change parameters dynamically. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Policies for Automatic Subscriber Logon

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module contains information on how to configure ISG to use specified identifiers in place of the username in authorization requests, enabling a user profile to be downloaded from an authentication, authorization, and accounting (AAA) server as soon as packets are received from a subscriber.

- Finding Feature Information, page 159
- Prerequisites for ISG Automatic Subscriber Logon, page 159
- Restrictions for ISG Automatic Subscriber Logon, page 160
- Information About ISG Automatic Subscriber Logon, page 160
- How to Configure ISG Policies for Automatic Subscriber Logon, page 161
- Configuration Examples for ISG Automatic Subscriber Logon, page 164
- Additional References, page 165
- Feature Information for ISG Automatic Subscriber Logon, page 166

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Automatic Subscriber Logon

Depending on your AAA implementation, you may need to configure one of the following identifiers in the password field of the user profile: source IP address, MAC address, remote ID, circuit ID. You may also need to configure a global address in the password field.

To use circuit ID and remote ID for authorization for IP sessions, the DSLAM must insert the circuit ID and remote ID in the DHCP Option 82 information.

To use remote ID for authorization of PPPoE sessions, the PPPoE client must provide the remote ID information in the PPPoE Tag ID or line ID.

Restrictions for ISG Automatic Subscriber Logon

The username field in an authorization request has a limit of 253 characters.

Information About ISG Automatic Subscriber Logon

- Overview of ISG Automatic Subscriber Logon, page 160
- Supported Identifiers for ISG Automatic Subscriber Logon, page 160
- Authorization Based on Circuit ID and Remote ID, page 160
- Accounting Behavior When ISG Automatic Subscriber Logon Is Configured, page 161

Overview of ISG Automatic Subscriber Logon

Service providers commonly implement a policy at the start of IP sessions that redirects all subscriber packets to a logon portal for authentication. Following successful authentication, per-subscriber authorization data is typically returned from a AAA server. For some deployments, usually in subscriber networks that are well protected against spoofing and denial-of-service (DoS) attacks, service providers are willing to forgo authentication and trust subscriber identity. ISG automatic subscriber logon allows service providers to grant certain subscribers access to services without requiring the subscribers to log on.

ISG automatic subscriber logon enables a specified identifier to be used in place of the username in authorization requests. Enabling the AAA server to authorize subscribers on the basis of a specified identifier allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

The event that triggers automatic subscriber logon is session-start. For IP sessions, session-start occurs when a DHCP DISCOVER request is received or when an unrecognized source IP address is detected. For PPPoE sessions, session-start occurs when a client attempts to initiate a session by sending a PPPoE Active Discovery Initiation (PADI) packet.

Supported Identifiers for ISG Automatic Subscriber Logon

For IP sessions, an ISG device can be configured to use the following identifiers in place of the username in authorization requests: IP address, MAC address, circuit ID, remote ID, or a combination of the circuit ID and remote ID.

For PPPoE sessions, an ISG device can be configured to use the remote ID in place of the username in authorization requests.

Authorization Based on Circuit ID and Remote ID

The circuit ID and remote ID fields are part of the DHCP relay agent information option (also referred to as Option 82) and the PPPoE Tag VSA. These fields are inserted into DHCP and PPPoE messages by a DSLAM. An ISG device can be configured to use the circuit ID, remote ID, or a combination of circuit ID and remote ID as the username in authorization requests.

By default, the ISG device will use the circuit ID and remote ID that are provided by the Layer 2 edge access device for authorization. If the **ip dhcp relay information option** command is configured, the ISG device will use the circuit ID and remote ID that are received in a DHCP message.

Accounting Behavior When ISG Automatic Subscriber Logon Is Configured

Accounting Behavior for MAC-Address-Based Authorization

If the MAC address is sent as the username in authorization requests, the MAC address will also be sent as the Calling Station ID in accounting records.

Accounting Behavior for Remote-ID- and Circuit-ID-Based Authorization

For IP sessions that use DHCP Option 82 authorization, accounting messages are sent to the AAA server with the Circuit ID and Remote ID Cisco VSAs. Although you can configure a combination of circuit ID and remote ID as the username for authorization, the attributes are sent individually in accounting records. You can also configure the circuit ID and remote ID to be sent together in accounting records as the NAS Port ID.

For PPPoE sessions, the Remote ID VSA is sent in accounting records, and the remote ID is also sent as the NAS Port ID.

If the **radius-server attribute 31 remote-id** command is configured, the remote ID is sent in accounting records as the Calling Station ID.

How to Configure ISG Policies for Automatic Subscriber Logon

- Configuring an ISG Control Policy for Automatic Subscriber Logon, page 161
- Verifying ISG Automatic Subscriber Logon, page 163

Configuring an ISG Control Policy for Automatic Subscriber Logon

Perform this task to configure an ISG control policy that initiates subscriber authorization and inserts a specified identifier into the username field of the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Creates or modifies a control policy map, which is used to define a control policy.

Step 4	**class type control** {*class-map-name* | **always**} **event session-start**
	Example:
	`Router(config-control-policymap)# class type control TAL-subscribers event session-start`
		Specifies a control class, which defines the conditions that must be met in order for an associated set of actions to be executed.
		- Specify the control class-map that was configured in the task “Identifying Traffic for Automatic Logon in a Control Policy Class Map”.

Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address`	Inserts the specified identifier into the username field of authorization requests.

Step 6	**end**
	Example:
	`Router(config-control-policymap-class-control)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

- What to Do Next, page 163

What to Do Next

You must apply the control policy to a context by using the **service-policy type control** command. For information about applying control policies, see the module "Configuring ISG Control Policies".

You may want to configure policies to determine what should happen for autologon subscribers whose IP address or MAC address authorization fails; for example, you may want to redirect the subscriber to the policy server for authentication.

Verifying ISG Automatic Subscriber Logon

Perform this task to determine whether or not automatic subscriber logon was successful.

SUMMARY STEPS

1. **enable**
2. **show subscriber session**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Step 2 **show subscriber session**

Use the **show subscriber session** command to display information about ISG subscriber sessions. If the output shows that a session was brought up in the state “authen”, automatic subscriber authorization was successful. If automatic subscriber authorization was not successful, the session will still be brought up, but in the state “unauthen”.

The following sample output shows information for a session for which automatic subscriber authorization was successful:

Example:

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 1
--------------------------------------------------
Unique Session ID: 3
Identifier: aabb.cc01.3000
```

SIP subscriber access type(s): IP

Example:

```
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:24, Last Changed: 00:00:21

Policy information:
  Authentication status: authen
  Rules, actions and conditions executed:
    subscriber rule-map DEFAULT
      condition always event session-start
        1 authorize identifier mac-address

Session inbound features:
 Feature: IP Idle Timeout
  Timeout value is 600
  Idle time is 00:00:21
Configuration sources associated with this session:
Interface: GigabtiEthernet0/0/0, Active Time = 00:00:24
```

Configuration Examples for ISG Automatic Subscriber Logon

- Automatic Subscriber Logon Based on IP Address Example, page 164

Automatic Subscriber Logon Based on IP Address Example

In the following example, if the client is from the 1.1.1.0 subnet, the ISG sends an authorization request to the list “TAL_LIST” with the subscriber’s source IP address as the username. If the authorization request is successful, any automatic-activation services specified in the returned user profile are activated for the session, and the execution of rules within the control policy stops. If the authorization is not successful, the rule execution proceeds, and the subscriber is redirected to the policy server to log in. If the subscriber does not log in within five minutes, the session is disconnected.

ISG Configuration

```
subscriber service password cisco
interface GigabitEthernet0/0/0
 service-policy type control RULEA
aaa authorization network TAL_LIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any
class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100
policy-map type service redirectprofile
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080
class-map type control match-all CONDA
 match source-ip-address 10.1.1.0 255.255.255.0
!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 service-policy type service aaa list LOCAL name redirectprofile
  3 set-timer TIMERB 5 minutes
!
 class type control CONDF event timed-policy-expiry
  1 service disconnect
```

User Profile Configuration

```
1.1.1.1 Password = "cisco"
 Service-Type = Outbound,
 Cisco:Account-Info = "AAuto-Internet;proxy-user;cisco"
```

Service Profile Configuration

```
Auto-Internet Password = "cisco"
 Cisco:Service-Info = "IAuto-Internet",
 Cisco-Avpair = "traffic-class=input access-group 100"
proxy-user Password = "cisco"
```

Idle-Timeout = 5

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Automatic Subscriber Logon

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

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

Table 13 Feature Information for ISG Automatic Subscriber Logon

Feature Name	Releases	Feature Configuration Information
ISG: Session: Authentication (MAC, IP)	Cisco IOS XE Release 2.2	ISG automatic subscriber logon enables an IP address or MAC address to be used in place of the username in authorization requests. This functionality allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.
ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support	Cisco IOS XE Release 2.2	This feature enhances ISG automatic subscriber logon by providing support for authorization on the basis of the circuit-id and remote-id.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Enabling ISG to Interact with External Policy Servers

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document describes how to enable ISG to retrieve session policies or accept dynamic updates to session policies from external policy servers.

- Finding Feature Information, page 169
- Restrictions for ISG Interaction with External Policy Servers, page 169
- Information About ISG Interaction with External Policy Servers, page 169
- How to Enable ISG to Interact with External Policy Servers, page 171
- Configuration Examples for ISG Interaction with External Policy Servers, page 176
- Additional References, page 177
- Feature Information for ISG Interaction with External Policy Servers, page 178

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 the Feature Information Table at the end of this document.

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

Restrictions for ISG Interaction with External Policy Servers

The ISG and external policy servers should be available in the same virtual routing and forwarding (VRF) instance.

Information About ISG Interaction with External Policy Servers

- Initial and Dynamic Authorization, page 170
- Triple-Key Authentication for ISG, page 170

Initial and Dynamic Authorization

ISG works with external devices, referred to as *policy servers* , that store per-subscriber and per-service information. ISG supports two models of interaction between ISG and external policy servers: initial authorization and dynamic authorization.

In the initial authorization model, ISG must retrieve policies from the external policy server at specific points in a session. In this model, the external policy server is typically an authentication, authorization, and accounting (AAA) server that uses RADIUS. ISG is the RADIUS client. Instead of a AAA server, some systems use a RADIUS proxy component that converts to other database protocols such as Lightweight Directory Access Protocol (LDAP).

The dynamic authorization model allows the external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of some algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Triple-Key Authentication for ISG

Triple-key authentication is a method of authenticating users based on their username, password, and location after ISG redirects them to the Cisco Service Management Engine (SME) portal. The SME server provides the location based on the source IP address of the subscriber being authenticated. Before the Triple Key Authentication Support feature was introduced, users were authenticated on the basis of the username and password only (two-key authentication). The triple-key authentication feature also eases migration from Service Selection Gateway (SSG) to an ISG platform because SSG uses triple-key authentication.

For SSG, the Cisco Subscriber Edge Services Manager (SESM) server populates RADIUS attribute 31 (calling-station ID) in the user-login request that it sends to SSG with a string containing the subscriber’s location. SSG then includes this value in the access-request message that it sends to the RADIUS server where the login is authenticated based on the username, password, and location string.

With ISG triple-key authentication, the location string that SME sends to ISG in attribute 31 in the CoA account-logon request is repeated in the access-request packet that ISG sends to the RADIUS server to authenticate the subscriber. ISG sends the location string within a Cisco vendor-specific attribute (VSA) included in the access-request message to the RADIUS server.

If the account-logon request from SME contains location information in both attribute 31 and the Cisco VSA, the value of the Cisco VSA location string takes precedence. The location information is received from SME as either attribute 31 or Cisco VSA 250. The location information is included in session authentication requests, session accounting requests from ISG, and prepaid authorization requests.

The table below shows the Cisco vendor-specific non-AVPair attribute used for triple-key authentication.

Table 14 Cisco Vendor-Specific Non-AVPair Attribute

Sub-AttrID	Attribute Type	Value	Function	Example	Used in
250	account-info	L<location-string>	Third key in triple-key authentication	LWiFiHotSpot 001	Acc-Req CoA Req Accounting

How to Enable ISG to Interact with External Policy Servers

- Configuring the ISG as a AAA Client, page 171
- Configuring the ISG as a AAA Server, page 172
- Enabling the Location VSA for Triple-Key Authentication, page 174

Configuring the ISG as a AAA Client

Perform this task to configure AAA method lists and enable ISG to retrieve policies from a AAA server. This task must be performed for both initial and dynamic authorization models.

The servers and server groups referenced by the AAA methods must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
6. **aaa authorization subscriber-service** {**default**| *list-name*} *method1* [*method2...*]
7. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login PPP1 group radius`	Specifies one or more AAA authentication methods to be used at login.

	Command or Action	Purpose
Step 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default group radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	**aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization network NET1 radius`	Specifies one or more AAA authorization methods to be used for restricting subscriber access to a network.
Step 6	**aaa authorization subscriber-service** {**default**| *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization subscriber-service default radius`	Specifies one or more AAA authorization methods for ISG to use in providing a service.
Step 7	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name* **Example:** `Router(config)# aaa accounting network default start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes.

Step 8	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode.

Configuring the ISG as a AAA Server

Dynamic authorization allows a policy server to dynamically send policies to ISG. Perform this task to configure the ISG as a AAA server and enable dynamic authorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client** {**name** | *ip-address*} [**key** [**0**|**7**] *word*] [**vrf** *vrf-id*]
5. **port** *port-number*
6. **server-key** [**0**|**7**] *word*
7. **auth-type** {**all** | **any** | **session-key**}
8. **ignore** {**server-key** | **session-key**}
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures the ISG as a AAA server. - Enters dynamic authorization local server configuration mode.
Step 4	**client** {**name** | *ip-address*} [**key** [**0**|**7**] *word*] [**vrf** *vrf-id*] **Example:** `Router(config-locsvr-da-radius)# client 10.76.86.90 key cisco`	Specifies a client with which ISG will be communicating.
Step 5	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1600`	Specifies the RADIUS server port. - Default is 1700.

	Command or Action	Purpose
Step 6	**server-key** [**0**|**7**] *word* **Example:** `Router(config-locsvr-da-radius)# server-key cisco`	Specifies the encryption key shared with the RADIUS client.

Step 7	**auth-type** {**all** | **any** | **session-key**}
	Example:
	`Router(config-locsvr-da-radius)# auth-type all`
		Specifies the attributes to be used for session authorization.

Step 8	**ignore** {**server-key** | **session-key**}
	Example:
	`Router(config-locsvr-da-radius)# ignore session-key`
		Configures ISG to ignore the shared encryption key or attribute 151.

Step 9	**end**
	Example:
	`Router(config-locsvr-da-radius)# end`
		Exits global configuration mode.

Enabling the Location VSA for Triple-Key Authentication

To enable ISG to include the location VSA in authentication and accounting requests, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server vsa send accounting**
5. **radius-server vsa send authentication**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**radius-server vsa send accounting** **Example:** `Router(config)# radius-server vsa send accounting`	Enables ISG to recognize and use accounting VSAs as defined by RADIUS attribute 26.
Step 5	**radius-server vsa send authentication** **Example:** `Router(config)# radius-server vsa send authentication`	Enables ISG to recognize and use authentication VSAs as defined by RADIUS attribute 26.

Step 6	**end**
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

Examples

The following example shows how to configure ISG to use VSAs for accounting and authentication:

```
aaa new-model
!
!
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuration Examples for ISG Interaction with External Policy Servers

- Example ISG Interaction with External Policy Servers, page 176
- Example Triple-Key Authentication, page 176

Example ISG Interaction with External Policy Servers

The following example configures ISG to interact with external policy servers:

```
!
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
!
aaa server radius dynamic-author
 client 10.76.86.90 key cisco
 client 172.19.192.25 vrf VRF1 key cisco
 client 172.19.192.25 vrf VRF2 key cisco
 client 172.19.192.25 key cisco
```

message-authenticator ignore

Example Triple-Key Authentication

The following example shows an authentication record with the session information including the location attribute. You can display this output by using the **debug radius accounting** command or the **gw-accounting syslog** command.

```
*Feb  5 01:20:50.413: RADIUS/ENCODE: Best Local IP-Address 10.0.1.1 for Radius-Server
10.0.1.2
*Feb  5 01:20:50.425: RADIUS(0000000F): Send Access-Request to 10.0.1.2:1645 id 1645/5,
len 107
*Feb  5 01:20:50.425: RADIUS:  authenticator 4D 86 12 BC BD E9 B4 9B - CB FC B8 7E 4C 8F
B6 CA
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  19
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 13  "LWiFiHotSpot001"
*Feb  5 01:20:50.425: RADIUS:  Calling-Station-Id  [31]  16  "AAAA.BBBB.CCCC"
*Feb  5 01:20:50.425: RADIUS:  User-Name           [1]   7   "george"
*Feb  5 01:20:50.425: RADIUS:  User-Password       [2]   18  *
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
*Feb  5 01:20:50.425: RADIUS:  NAS-Port            [5]   6   0
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Feb  5 01:20:50.425: RADIUS:  NAS-IP-Address      [4]   6   10.0.1.1
*Feb  5 01:20:50.425: RADIUS(0000000F): Started 5 sec timeout
*Feb  5 01:20:50.425: RADIUS: Received from id 1645/5 10.0.1.2:1645, Access-Accept, len 68
*Feb  5 01:20:50.425: RADIUS:  authenticator 49 A1 2C 7F C5 E7 9D 1A - 97 B3 E3 72 F3 EA
56 56
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  17
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 11  "S10.0.0.2"
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  31
*Feb  5 01:20:50.425: RADIUS:   Cisco AVpair       [1]   25  "accounting-list=default"
*Feb  5 01:20:50.433: RADIUS(0000000F): Received from id 1645/5
*Feb  5 01:20:50.437: RADIUS/ENCODE(0000000F):Orig. component type = Iedge IP SIP
```

```
*Feb  5 01:20:50.437: RADIUS(0000000F): Config NAS IP: 0.0.0.0
*Feb  5 01:20:50.437: RADIUS(0000000F): sending
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
AAA configuration tasks	Part 1, “Authentication, Authorization, and Accounting (AAA),” *Cisco IOS XESecurity Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Interaction with External Policy Servers

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

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

Table 15 Feature Information for ISG Interaction with External Policy Servers

Feature Name	Releases	Feature Information
ISG: Policy Control: Policy Server: CoA	Cisco IOS XE Release 2.2 Cisco IOS XE Release 2.4	This feature provides ISG support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization. This feature was integrated into Cisco IOS XE Release 2.4.
ISG: Session: Lifecycle: Packet of Disconnect (POD)	Cisco IOS XE Release 2.2	This feature enables an external policy server to terminate an ISG session when it receives a RADIUS Packet of Disconnect (POD).

Feature Name	Releases	Feature Information
ISG: Triple Key Authentication Support	Cisco IOS XE Release 3.1S	This feature enables triple-key authentication by passing the location information from SESM to the RADIUS server in the access-request message.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Subscriber Services

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG defines a *service* as a collection of policies that can be applied to any subscriber session. This module describes how ISG subscriber services work, how to configure services and traffic classes that may be used to qualify policies defined within a service, and how to activate services.

- Finding Feature Information, page 181
- Restrictions for ISG Subscriber Services, page 181
- Information About ISG Subscriber Services, page 182
- How to Configure ISG Services on the Router, page 184
- Configuration Examples for ISG Services, page 195
- Additional References, page 198
- Feature Information for ISG Subscriber Services, page 199

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 the Feature Information Table at the end of this document.

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

Restrictions for ISG Subscriber Services

Only one nondefault traffic class may be configured in each service.

When multiple services are active on a given session, class-based actions are executed on a first-match basis only; in other words, once a class is matched, the actions associated with that class will be executed, and no other class will be matched.

Services that are defined on the ISG device cannot be selected externally because they will not be advertised to a portal.

Removing or modifying a feature in the configuration, for example an access control list (ACL), is not supported by active sessions that reference that feature.

Information About ISG Subscriber Services

- ISG Services, page 182
- Primary Services, page 182
- Traffic Classes and Traffic Class Priority, page 182
- Traffic Policies, page 183
- ISG Features, page 183
- Service Groups, page 183
- Service Activation Methods, page 184

ISG Services

An ISG service is a collection of policies that may be applied to a subscriber session. ISG services can be applied to any session, regardless of subscriber access media or protocol, and a single service may be applied to multiple sessions. An ISG service is not necessarily associated with a destination zone or a particular uplink interface.

Services can be defined in two ways: in a service policy map that is configured on the ISG device by using the CLI, and in a service profile that is configured on an external device, such as an authentication, authorization, and accounting (AAA) server. Although they are configured differently, service policy maps and service profiles serve the same purpose: they contain a collection of traffic policies and other functionality that can be applied to a subscriber session. Traffic policies determine which functionality will be applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Primary Services

When a network-forwarding policy is included in a service profile or service policy map, the service is known as a *primary service* . Primary services are mutually exclusive and may not be simultaneously active. Upon activation of a new primary service, ISG will deactivate the existing primary service and any other services dependent on the existing primary service through association with a service group.

If a primary service is deactivated, sessions may be left without a network-forwarding policy, that is, with no means to route or forward packets. A policy may be applied to defend against this condition such that a specific service is activated upon deactivation of all others (or all other primary services). This backup service would return network-forwarding policy to the session and allow the subscriber to reach a web portal. However, it should be noted that an IP session will not be automatically terminated when all services are deactivated unless such a policy has been defined and applied.

Traffic Classes and Traffic Class Priority

ISG traffic classes allow for differentiated behavior for different traffic streams to and from a particular subscriber. For traffic to be classified into streams, you must specify an access control list (ACL) that classifies the traffic and specify the direction of the traffic to which the ACL applies (inbound or outbound). Optionally, the priority of the traffic class can also be specified.

Traffic that meets the specifications of a traffic class is said to *match* the traffic class. Once a match is made, features defined in the traffic policy are executed for that traffic class.

The priority of a traffic class determines which class is used first for a specified match if more than one traffic policy has been activated for a single session. In other words, if a packet matches more than one traffic class, it is classified to the class with the higher priority.

Packets that do not match any of the ACLs are considered to be part of the default traffic class and are processed as if a traffic policy was not applied to the session. A default class exists for every service, and the default action of the default class is to pass traffic. The default class can be configured to drop traffic. Default traffic is accounted for in the main session accounting.

A service can contain one traffic class and one default class.

Traffic classes are assigned unique identifiers that can be tracked with Cisco IOS **show** commands.

Traffic Policies

Traffic policies define the handling of data packets. A traffic policy contains a traffic class and one or more features. Whereas you can specify the event that will trigger an ISG control policy, the trigger for a traffic policy is implicit--the arrival of a data packet.

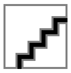
The features configured within a traffic policy apply only to the traffic defined by the traffic class. Multiple traffic policies with various features can be applied to a session.

ISG Features

An ISG feature is a functional component that performs a specific operation on a session’s data stream. A feature may or may not be associated with a traffic class. However, once associated with a traffic class, a feature can be applied only to the packets that match that traffic class. Otherwise, the feature is applied to all packets for that session.

The figure below shows how features apply to a subscriber session and to traffic flows within the session.

Figure 5



Note Two or more services that specify the same feature and apply to the entire session rather than to a specified traffic flow should not be activated for a session simultaneously. If two or more of these services are activated for a session, deactivation of one of the services will remove the feature from the session. If you need to offer to a subscriber multiple services that specify the same feature and apply to the session rather than a specific flow, configure the services so that they are mutually exclusive. That is, the subscriber should not be able to activate more than one such service at the same time. Similarly, control policies should not activate more than one such service at the same time.

Service Groups

A *service group* is a grouping of services that may be simultaneously active for a given session. Typically, a service group includes one primary service and one or more secondary services.

Secondary services in a service group are dependent on the primary service and should not be activated unless the primary service is already active. Once a primary service has been activated, any other services that reference the same group may also be activated. Services that belong to other groups, however, may be activated only if they are primary. If a primary service from another service group is activated, all services in the current service group will also be deactivated because they have a dependency on the previous primary service.

Service Activation Methods

There are three methods by which services can be activated:

- Automatic service activation
- Control policy service activation
- Subscriber-initiated service activation

Automatic Service Activation

The Auto Service attribute, which can be configured in user profiles, enables subscribers to be automatically logged in to specified services when the user profile is downloaded, usually following authentication. Features that are specified by the Auto Service attribute in a user profile are referred to as *auto services* . A user profile can specify more than one service as auto services.

Control Policy Service Activation

ISG control policies can be configured to activate services in response to specific conditions and events.

Subscriber-Initiated Service Activation

Subscriber-initiated service activation takes place when a subscriber manually selects a service at a portal.

When the system receives a subscriber request to activate a service, the ISG policy engine searches for a policy matching the event “service-start”. If no such policy is found, the policy engine will by default download the service via the default AAA network authorization method list. This default behavior is identical to the behavior generated by the following policy configuration:

```
class-map type control match-all SERVICE1_CHECK
   match service-name SERVICE1
policy-map type control SERVICE1_CHECK event service-start
   1 service-policy type service name SERVICE1
```

The same default behavior applies to subscriber logoffs, with the ISG policy engine searching for a policy that matches the event “service-stop”.

If a policy is configured, it is the responsibility of the policy to specify how the service should be applied.

How to Configure ISG Services on the Router

There are two ways to configure an ISG service. One way is to configure a service policy map on the local device by using the CLI. The second way is to configure a service profile on a remote AAA server. To configure a service policy map directly on the ISG, perform the tasks in the following sections:

- Configuring an ISG Service with Per-Session Functionality, page 185
- Configuring an ISG Service with a Traffic Policy, page 187
- Configuring the Default Class in an ISG Service Policy Map, page 191
- Activating ISG Subscriber Services, page 192
- Verifying ISG Services, page 194

Configuring an ISG Service with Per-Session Functionality

Certain types of functionality that are configured in a service must be applied to the entire subscriber session rather than to a specific traffic flow. Services that are configured with this type of per-session functionality must not contain a traffic class. Perform this task to configure a service policy map without a traffic class on the ISG.

Note Some of the commands that can be configured in a service policy map require other configuration in order to work properly. Details on how to configure specific ISG features and functionality are provided in other modules.

Note A service that is configured with per-session functionality and a traffic policy will not work correctly.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **authenticate aaa list** *name-of-list*
5. **classname** *dhcp-pool-name*
6. **ip portbundle**
7. **ip unnumbered** *interface-type interface-number*
8. **ip vrf forwarding** *name-of-vrf*
9. **service deny**
10. **service relay pppoe vpdn group** *VPDN-group-name*
11. **service vpdn group** *VPDN-group-name*
12. **sg-service-group** *service-group-name*
13. **sg-service-type** {**primary** | **secondary**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**authenticate aaa list** *name-of-list* **Example:** `Router(config-service-policymap)# authenticate aaa list mlist`	Indicates that the service requires authentication as a condition of activation and initiates an authentication request.
Step 5	**classname** *dhcp-pool-name* **Example:** `Router(config-service-policymap)# classname green`	Associates a Dynamic Host Configuration Protocol (DHCP) address pool with a service or specific subscriber.
Step 6	**ip portbundle** **Example:** `Router(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key feature in the service policy map.
Step 7	**ip unnumbered** *interface-type interface-number* **Example:** `Router(config-service-policymap)# ip unnumbered ethernet 0`	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 8	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF. • Configuring this command will make the service a primary service.

	Command or Action	Purpose
Step 9	**service deny** **Example:** `Router(config-service-policymap)# service deny`	Denies network service to the subscriber session.
Step 10	**service relay pppoe vpdn group** *VPDN-group-name* **Example:** `Router(config-service-policymap)# service relay pppoe vpdn group group1`	Enables relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel for a subscriber session.
Step 11	**service vpdn group** *VPDN-group-name* **Example:** `Router(config-service-policymap)# service vpdn group vpdn1`	Provides virtual private dialup network (VPDN) service for ISG subscriber sessions. • Configuring this command will make the service a primary service.
Step 12	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	Associates the service with a specified service group.

Step 13	**sg-service-type** {**primary** | **secondary**}
	Example:
	`Router(config-service-policymap)# sg-service-type primary`
		Defines the service as a primary or secondary service.
		• A primary service is a service that contains a network-forwarding policy. A service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

Configuring an ISG Service with a Traffic Policy

An ISG traffic policy contains a traffic class and one or more ISG features. The traffic class defines the traffic to which the features will be applied. Perform the following tasks to configure an ISG service with a traffic policy on the router:

- Defining an ISG Traffic Class Map, page 187
- Configuring an ISG Service Policy Map with a Traffic Policy, page 189

Defining an ISG Traffic Class Map

Perform this task to configure a traffic class map. A traffic class map usually specifies an access control list (ACL) that classifies the flow and the direction of traffic to which the ACL applies (inbound or outbound).

Note You can also configure an empty traffic class map, that is, a traffic class map that does not specify an access list, in order to configure a service with a traffic policy that applies to all session traffic.

This task assumes that access control lists (ACLs) have been configured for classifying traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **match access-group input** {*access-list-number* | **name** *access-list-name*}
5. **match access-group output** {*access-list-number* | **name** *access-list-name*}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type traffic match-any** *class-map-name* **Example:** `Router(config)# class-map type traffic match-any class1`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class.

Step 4	**match access-group input** {*access-list-number* | **name** *access-list-name*}
	Example:
	`Router(config-traffic-classmap)# match access-group input 101`
		(Optional) Configures the match criteria for an input class map on the basis of the specified ACL.
		• Skip this step if you want to define a traffic policy that applies to all session traffic rather than to a specific traffic flow.

	Command or Action	Purpose

Step 5	**match access-group output** {*access-list-number* | **name** *access-list-name*}
	Example:
	`Router(config-traffic-classmap)# match access-group output 102`
		(Optional) Configures the match criteria for an output class map on the basis of the specified ACL.
		• Skip this step if you want to define a traffic policy that applies to all session traffic rather than to a specific traffic flow.

Step 6	**exit** **Example:** `Router(config-traffic-classmap)# exit`	Returns to global configuration mode.

Configuring an ISG Service Policy Map with a Traffic Policy

ISG services are configured by creating service policy maps on the ISG or service profiles on an external AAA server. Perform this task to configure a traffic policy in a service policy map on the ISG.

Note Some of the commands that can be configured in a service policy map require other configuration in order to work properly. Details on how to configure specific ISG features and functionality are provided in other modules in the *Cisco IOS Intelligent Services Gateway Configuration Guide* .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **accounting aaa list** *AAA-method-list*
6. **police** {**input** | **output**} *committed-rate normal-burst excess-burst*
7. **prepaid config** *name-of-configuratio* n
8. **redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]
9. **timeout absolute** *duration-in-seconds*
10. **timeout idle** *duration-in-seconds*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic classb`	Specifies a named traffic class whose policy you want to create or change. • The *priority* argument determines which class will be used first for a specified match. When a packet matches more than one traffic class, it will be classified to the class with higher priority
Step 5	**accounting aaa list** *AAA-method-list* **Example:** `Router(config-service-policymap-class-traffic)# accounting aaa list mlist1`	Enables accounting and specifies the AAA method list to which accounting updates will be sent.
Step 6	**police** {**input** | **output**} *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	Enables ISG policing for upstream or downstream traffic. • This command can be entered twice to configure upstream and downstream policing.

	Command or Action	Purpose
Step 7	**prepaid config** *name-of-configuratio* n **Example:** `Router(config-service-policymap-class-traffic)# prepaid config conf-prepaid`	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters.
Step 8	**redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	Redirects traffic to a specified server or server group.
Step 9	**timeout absolute** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout absolute 30`	Specifies the session lifetime, in a range from 30 to 4294967 seconds.
Step 10	**timeout idle** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout idle 3000`	Specifies how long a connection can be idle before it is terminated. The range is platform and release-specific. For more information, use the question mark (?) online help function.

Step 11	**end**
	Example:
	`Router(config-service-policymap-class-traffic)#end`
		(Optional) Returns to privileged EXEC mode.

Configuring the Default Class in an ISG Service Policy Map

Packets that do not match any traffic classes are considered to be part of default traffic and are processed as if a traffic policy were not applied to the session. A default class exists by default for every service, and the default action of the default class is to pass traffic. Perform this task to configure the default class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic default** {**in-out** | **input** | **output**}
5. **drop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**class type traffic default** {**in-out** | **input** | **output**} **Example:** `Router(config-service-policymap)# class type traffic default in-out`	Associates a default traffic class with a service policy map. • The default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.
Step 5	**drop** **Example:** `Router(config-service-policymap-class-traffic)# drop`	Configures the default traffic class to discard packets matching that class.

Activating ISG Subscriber Services

There are three ways that ISG subscriber services can be activated: by specifying the service as an automatic activation service in a subscriber’s user profile, by configuring control policies to activate the service, and by a subscriber-initiated service logon. No special configuration is necessary to enable a subscriber to log on to a service.

To configure a service for automatic activation and to configure control policies to activate services, perform the following tasks:

- Configuring Automatic Service Activation in a User Profile, page 193
- Configuring ISG Control Policies to Activate Services, page 193

Configuring Automatic Service Activation in a User Profile

Perform this task to configure automatic service activation for a service in a subscriber's user profile.

SUMMARY STEPS

1. Add the Auto Service attribute to the user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Auto Service attribute to the user profile. **Example:** `26,9,251="`**A** *service-name*`[`**;** *username* **;** *password*`]"`	Automatically logs the subscriber in to the specified service when the user profile is downloaded.

Configuring ISG Control Policies to Activate Services

Perform this task to configure a control policy to activate a service.

A control class map must be configured if you specify a named control class map in the control policy map. See the module "Configuring ISG Control Policies" for information about configuring control policies.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found**| **session-start** | **timed-policy-expiry**]
5. *action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policy1`	Creates or modifies a policy map to specify an ISG control policy.

Step 4	**class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found**| **session-start** | **timed-policy-expiry**]
	Example:
	`Router(config-control-policymap)# class type control always event session-start`
		Specifies a class and, optionally, an event for which actions may be configured.

Step 5	*action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service service1`	Applies the specified service policy map. • To remove the service policy map, use the **unapply** keyword.

Verifying ISG Services

Perform this task to verify ISG service configuration.

SUMMARY STEPS

1. **enable**
2. **show class-map type traffic**
3. **show policy-map type service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map type traffic** **Example:** `Router# show class-map type traffic`	Displays all traffic class maps and their matching criteria.
Step 3	**show policy-map type service** **Example:** `Router# show policy-map type service`	Displays the contents of all service policy maps.

Configuration Examples for ISG Services

- Example Service for Per-Flow Accounting, page 195
- Example Service for Absolute Timeout and Idle Timeout, page 196
- Example Service for ISG Policing, page 196
- Example Service for Per-Subscriber Firewall, page 197
- Example Service for Redirecting Layer 4 Subscriber Traffic, page 197
- Example Deactivating a Layer 4 Redirection Service Following Authorization, page 198

Example Service for Per-Flow Accounting

In the following examples, the service “SERVICE1” is configured with per-flow accounting. The access lists “SERVICE1_ACL_IN” and “SERVICE1_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two alternative methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
```

Example Service for Absolute Timeout and Idle Timeout

In the following examples, the service “SERVICE1” is configured with per-flow accounting, an absolute timeout, and an idle timeout. The access lists “SERVICE1_ACL_IN” and “SERVICE1_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  timeout idle 600
  timeout absolute 1800
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
  session-timeout = 1800
  idle-timeout = 600
```

Example Service for ISG Policing

In the following examples, the service “BOD1M” is configured with per-flow accounting and ISG policing. The access lists “BOD1M_IN_ACL_IN” and “BOD1M_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any BOD1M_TC
 match access-group input name BOD1M_IN_ACL_IN
 match access-group output name BOD1M_ACL_OUT
```

```
!
policy-map type service BOD1M
 10 class type traffic BOD1M_TC
  accounting aaa list CAR_ACCNT_LIST
  police input 512000 256000 5000
  police output 1024000 512000 5000
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name BOD1M_IN_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name BOD1M _OUT_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = IBOD1M
 Cisco-SSG-Service-Info = QU;512000;256000;5000;D;1024000;512000;5000
```

Example Service for Per-Subscriber Firewall

In the following examples, the service “SERVICE2” is configured with a per-subscriber firewall. The service does not include a traffic class, so it will apply to the entire session. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
policy-map type service SERVICE2
 ip access-group INTERNET_IN_ACL in
 ip access-group INTERNET_OUT_ACL out
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = ip:inacl=INTERNET_IN_ACL
 Cisco-AVPair = ip:outacl=INTERNET_OUT_ACL
```

Example Service for Redirecting Layer 4 Subscriber Traffic

The following example shows the configuration of a service called “UNAUTHORIZED_REDIRECT_SVC”. The control policy “UNAUTHEN_REDIRECT” is configured to apply the service upon session start.

```
class-map type traffic match-any UNAUTHORIZED_TRAFFIC
 match access-group input 100

policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class type traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080

policy-map type control UNAUTHEN_REDIRECT
 class type control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
```

Example Deactivating a Layer 4 Redirection Service Following Authorization

In the following example, a service configured with Layer 4 redirection is deactivated when traffic becomes authorized; that is, following activation of the appropriate service.

```
class-map traffic UNAUTHORIZED_TRAFFIC
match access-group input 100
policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080
class-map control match-all CHECK_ISP1
 match service ISP1
policy-map control UNAUTHEN_REDIRECT
 class control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
 class control CHECK_ISP1 event service-start
  1 service-policy type service unapply UNAUTHORIZED_REDIRECT_SVC
  1 service-policy type service name ISP1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Subscriber Services

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

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

Table 16 Feature Information for ISG Subscriber Services

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Service Profiles	Cisco IOS XE Release 2.2	ISG defines a service as a collection of policies that can be applied to any subscriber session. Services can be configured on the router or on an external AAA server.

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: User Profiles	Cisco IOS XE Release 2.2	ISG user profiles specify services and functionality that can be applied to ISG sessions for the specified subscriber. User profiles are defined on an external AAA server.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Network Forwarding Policies

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. An ISG network forwarding policy is a type of traffic policy that allows packets to be routed or forwarded to and from an upstream network. This module provides information about how to configure network forwarding policies.

- Finding Feature Information, page 201
- Restrictions for ISG Network Forwarding Policies, page 201
- Information About ISG Network Policies, page 201
- How to Configure ISG Network Policies, page 202
- Configuration Examples for ISG Network Policies, page 206
- Additional References, page 206
- Feature Information for ISG Network Policies, page 207

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 the Feature Information Table at the end of this document.

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

Restrictions for ISG Network Forwarding Policies

A service can contain only one network forwarding policy.

For each subscriber session, only one instance of a network forwarding policy can be in effect at any one time.

Information About ISG Network Policies

- Network Policies, page 202
- Configuration Sources for Network Policies, page 202

Network Policies

For subscriber packets to reach a network, some form of forwarding must be specified for a subscriber session. A traffic policy that allows packets to be routed or forwarded to and from an upstream network is known as a *network forwarding policy* .

Where the network forwarding policy type is routing, forwarding decisions are made at Layer 3, and a VRF (Virtual Routing and Forwarding) identifier must be specified to indicate which routing table should be used to make the routing decision (each VRF represents an independent routing context within a single router). Where the network policy type is forwarding, forwarding decisions are made at Layer 2, which means that all subscriber packets are forwarded to and from a single virtual endpoint within the system. This virtual endpoint represents a Layer 2 tunnel, and a tunnel identifier determines which tunnel should be used. If a network forwarding policy is not specified, the global routing table will be used to route traffic.

An ISG service that includes a network forwarding policy is known as a *primary service* . Primary services are mutually exclusive and may not be active simultaneously. Upon activation of a new primary service, ISG will deactivate the existing primary service and any other services dependent on the existing primary service through association with a service group.

Configuration Sources for Network Policies

Network policies can be configured in user profiles and service profiles on an external authentication, authorization, and accounting (AAA) server or in service policy maps on the ISG-enabled device. A network forwarding policy configured in a user profile takes precedence over a network forwarding policy specified in a service.

If a network forwarding policy is not specified in a user profile or service, the ISG session will inherit the network service from another source. ISG can inherit a network service from the following sources:

- Global
- Interface
- Subinterface
- Virtual template

These configuration sources are listed in order of precedence. For example, a network forwarding policy that is configured for a virtual template takes precedence over a network forwarding policy that is configured on an interface.

For each subscriber session, only one instance of a network forwarding policy can be in effect at any point in time.

How to Configure ISG Network Policies

- Configuring Network Policies for PPP Sessions in Service Policy Maps, page 202
- Configuring Network Policies for IP Sessions in Service Policy Maps, page 204

Configuring Network Policies for PPP Sessions in Service Policy Maps

Network policies can be configured in user profiles or service profiles on an external AAA server or in a service policy map on the ISG device. Perform this task to configure a network forwarding policy for PPP sessions in a service policy map on the ISG device.

Note If a network forwarding policy is not specified in a user profile, service profile, or service policy map, a subscriber session will inherit the network forwarding policy from another source. See the "Configuration Sources for Network Policies" section for more information.

This task assumes that virtual private dial up network (VPDN) groups have been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. Do one of the following:
    - **service vpdn group** *vpdn-group-name*
    - **service local**
    - **service relay pppoe vpdn group** *vpdn-group-name*
5. **ip vrf forwarding** *name-of-vrf*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **service vpdn group** *vpdn-group-name*
	• **service local**
	• **service relay pppoe vpdn group** *vpdn-group-name*
	Example:
	`Router(config-service-policymap)# service vpdn group vpdn1`
	Example:
	`Router(config-service-policymap)# service local`
	Example:
	`Router(config-service-policymap)# service relay pppoe vpdn group vpdn1`
		Provides virtual private dialup network (VPDN) service.
		or
		Provides local termination service.
		or
		Provides VPDN service by relaying PPPoE over VPDN L2TP tunnels.
		• If you terminate the service locally by configuring the **service local** command, you can also specify the routing domain in which to terminate the session by configuring the **ip vrf forwarding** command.

Step 5	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF. • Perform this step only if you configured the **service local** command in Step 4. If you configured the **service local** command, you can use the**ip vrf forwarding** command to specify the routing domain in which to terminate session. If you do not specify the routing domain, the global VRF will be used.

- What to Do Next, page 204

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Network Policies for IP Sessions in Service Policy Maps

Network policies can be configured in user profiles or service profiles on an external AAA server or in a service policy map on the ISG device. Perform this task to configure a network forwarding policy for IP sessions in a service policy map on the device.

Note If a network forwarding policy is not specified in a user profile, service profile, or service policy map, a subscriber session will inherit the network forwarding policy from another source. See the "Configuration Sources for Network Policies" section for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF.

	Command or Action	Purpose
Step 5	**sg-service-type primary** **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service is a service that contains a network forwarding policy. A primary service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

- What to Do Next, page 206

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Configuration Examples for ISG Network Policies

- Network Forwarding Policy for PPP Sessions Example, page 206
- Network Forwarding Policy for IP Sessions Example, page 206

Network Forwarding Policy for PPP Sessions Example

The following example shows a service policy map configured with a network forwarding policy for PPP sessions:

```
policy-map type service my_service
 service vpdn group vpdn1
```

Network Forwarding Policy for IP Sessions Example

The following example shows a service policy map configured with a network forwarding policy for IP sessions:

```
policy-map type service my_service
 ip vrf forwarding vrf1
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
VPDN configuration tasks	*Cisco IOS XE VPDN Technologies Configuration Guide*
PPP and VPDN commands	*Cisco IOS XE VPDN Technologies Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Network Policies

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

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

Table 17 Feature Information for ISG Network Forwarding Policies

Feature Name	Releases	Feature Configuration Information
ISG: Network Interface: IP Routed, VRF-Aware MPLS	Cisco IOS XE Release 2.2	ISG supports multiple forwarding types to connect sessions to networks. These connections can be to the Internet, corporate intranets, ISPs, or walled gardens for content delivery. ISG supports both routed and MPLS-enabled interfaces for network access.
ISG: Network Interface: Tunneled (L2TP)	Cisco IOS XE Release 2.2	ISG is flexible to support multiple interface types to connect sessions to networks. These connections can be to the Internet, corporate intranets, ISPs or walled gardens for content delivery. ISG supports tunneled interfaces to networks.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Accounting

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure ISG accounting, including per-session accounting or per-flow accounting, broadcast accounting, and postpaid tariff switching.

- Finding Feature Information, page 209
- Restrictions for ISG Accounting, page 209
- Information About ISG Accounting, page 209
- How to Configure ISG Accounting, page 212
- Configuration Examples for ISG Accounting, page 227
- Additional References, page 229
- Feature Information for ISG Accounting, page 230

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 the Feature Information Table at the end of this document.

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

Restrictions for ISG Accounting

ISG accounting supports only the RADIUS protocol.

If authentication, authorization, and accounting (AAA) broadcast accounting is used in conjunction with periodic accounting, you cannot configure different accounting periods for different accounting groups.

Information About ISG Accounting

- Overview of ISG Accounting, page 210
- ISG Accounting Records, page 210
- Interim ISG Accounting Updates, page 211
- Broadcast Accounting, page 211

- ISG Postpaid Tariff Switching, page 211

Overview of ISG Accounting

ISG supports per-session, per-service, and per-flow accounting. Per-session accounting is the aggregate of all the flow traffic for a session. Per-session accounting can be enabled in a user profile. Per-service accounting can be enabled in a service profile or service policy map.

Per-flow accounting, which accounts for a subset of session traffic as defined by a traffic class, is enabled in a service profile or service policy map. When per-flow accounting is configured, the Parent-Session-ID vendor-specific attribute (VSA) is included in accounting records so that per-session and per-flow accounting records can be correlated in the RADIUS server.

When accounting is configured in a user profile, the service name attribute is not included in accounting records.

Session accounting is enabled if the **aaa accounting network default** command is configured and a AAA method list is specified. (It is recommended that you use a named method list rather than the default method list.) Flow accounting is disabled by default and will take place only if a AAA method list is specified in the service profile or service policy map. ISG accounting sends Accounting-Start, interim, and Accounting-Stop records to the specified AAA method list.

Per-service accounting allows RADIUS to track when services become active and stop within a subscriber session. Per-service accounting is the aggregate of all flow traffic for the duration of the service. Using this feature, the router includes all activated services for the session in a single accounting start message. When per-service accounting is configured, the service name and Parent-Session-ID attributes are included in accounting records.

- ISG Accounting Messages on ANCP Ports, page 210

ISG Accounting Messages on ANCP Ports

Accounting messages sent by ISG for sessions on an Access Node Control Protocol (ANCP) port contain the following AAA attributes: nas-tx-speed, nas-tx-speed-bps, nas-rx-speed, and nas-rx-speed-bps. ISG retrieves the values for these attributes from the Digital Subscriber Line Access Multiplexer (DSLAM) ANCP notification sent to ISG or from the Quality of Service (QoS) policy configured on the interface.

When an ANCP port is in an UP state, the attribute values are taken from the DSLAM ANCP notification sent to ISG. If the ANCP port state changes to a DOWN state, the ANCP accounting messages will continue to contain the AAA attributes sent in the DSLAM notification.

If the ANCP-port state has never been set to the UP state, ISG can retrieve the nas-tx-speed, nas-tx-speed-bps, nas-rx-speed, and nas-rx-speed-bps AAA attributes from the QoS policy on that interface.

In order to retrieve the AAA attributes from the QoS policy, the policy must be configured prior to the configuration of the ANCP neighbor, otherwise ISG uses the previous values (if any) for the AAA attributes when a session is established.

If the QoS policy values are changed, ISG continue to use the previous values until the ANCP neighbor is removed and reconfigured.

ISG Accounting Records

ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server. ISG sends accounting records with the associated attributes to the AAA accounting method list when the following events occur: account logon, account logoff, service logon, and service logoff. The accounting server can be configured to interpret the records to generate bills for postpaid sessions.

Account Logon and Logoff

ISG sends a RADIUS Accounting-Request record to the specified AAA method list when a subscriber logs onto or off of ISG. The Acct-Status-Type attribute included in the Accounting-Request record indicates if the record marks the start (commencement) of the subscriber session or the stop (termination) of the session.

When the **aaa accounting** command is enabled with the **system**, **default**, **start-stop**, and **group**keywords, accounting records are sent to the AAA server. When a subscriber logs on, ISG sends an Accounting-Start record to the AAA server. When a subscriber logs off, ISG sends an Accounting-Stop record.

Service Logon and Logoff

ISG sends a RADIUS Accounting-Start record to the AAA server when a service is activated for a subscriber, and it sends an Accounting-Stop record when a service is deactivated. The record contains a different accounting session ID from the accounting session ID of the parent session.

The Acct-Status-Type attribute included in the Accounting-Request record indicates whether the record marks the start or the end of the service. The name of the service is included in accounting records for service logon and logoff.

Accounting records may be sent for events other than account and service logon and logoff. See the "Configuring Accounting" chapter of the *Cisco IOS Security Configuration Guide,* Release 12.2, for more information.

Interim ISG Accounting Updates

ISG supports interim (intermittent) RADIUS accounting updates, which work the same way as “watchdog” RADIUS accounting. Accounting updates are sent between the times that ISG sends Accounting-Start and Accounting-Stop records.

ISG supports two types of interim accounting: accounting updates for new information (such as a new IP address) and periodic accounting, in which accounting records are sent at a configurable interval.

Interim accounting for new information can be enabled or disabled globally. Periodic accounting can be enabled for specific contexts, such as globally, in user profiles, and in services.

Broadcast Accounting

ISG supports AAA broadcast accounting, which is the ability to send user accounting records to multiple RADIUS servers. AAA broadcast accounting provides service providers with geographical redundancy for RADIUS servers, and provides accounting records to partners in wholesale models. For information about configuring AAA broadcast accounting, see the “Configuring Accounting ” chapter in the “Authentication, Authorization, and Accounting” part of the *Cisco IOS XE Security Configuration Guide* .

ISG Postpaid Tariff Switching

ISG postpaid tariff switching allows changes in tariffs during the lifetime of a connection. This feature applies to time-based or volume-based postpaid sessions in which the tariff changes at certain times of the day.

Typically, a service provider would use postpaid tariff switching to offer different tariffs to a subscriber while the subscriber is still connected; for example, changing a subscriber to a less expensive tariff during off-peak hours.

To handle tariff switches for postpaid connections, the accounting packets log the usage information during the various tariff-switch intervals. The service profile contains a weekly tariff-switch plan detailing the times of day at which tariff changes occur. ISG monitors the usage at every tariff-switch point and records this information in interim accounting records. The billing server monitors all interim accounting updates and obtains the information about the traffic sent at each tariff rate.

Note Tariff switching is not required for time-based billing services. Because the billing server knows the service logon time stamp and logoff time stamp, it can calculate the various tariffs that apply during that time.

How to Configure ISG Accounting

- Enabling ISG Per-Session Accounting, page 212
- Enabling ISG Per-Flow Accounting, page 213
- Enabling ISG Per-Service Accounting, page 216
- Configuring ISG Postpaid Tariff Switching, page 220
- Verifying ISG Accounting and Postpaid Tariff Switching, page 221

Enabling ISG Per-Session Accounting

Per-session accounting can be configured in the following configuration sources:

- User profile on a AAA server

This procedure contains the following sections:

- Prerequisites, page 212
- Enabling Per-Session Accounting in a User Profile on a AAA Server, page 212
- What to Do Next, page 213
- Troubleshooting Tips, page 213

Prerequisites

ISG sends accounting records to the authentication, authorization, and accounting (AAA) method list specified in the user profile, service profile, or service policy map. The tasks in this section assume that you have configured a AAA method list by using the **aaa accounting** command. See the Cisco IOS Security Command Reference for more information.

AAA servers must be configured to support ISG accounting.

Enabling Per-Session Accounting in a User Profile on a AAA Server

Use the attributes in this procedure to enable per-session accounting in a user profile on a AAA server. When accounting is configured in the user profile instead of the service profile, the Service Name attribute does not appear in the accounting.

SUMMARY STEPS

1. Cisco-Avpair="accounting-list=*accounting-mlist-name* "
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-Avpair="accounting-list=*accounting-mlist-name* "
Add the Accounting attribute to the user profile. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent.

Step 2 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)
(Optional) Add the Acct-Interim-Interval (attribute 85) to the user profile. This attribute specifies the number of seconds between interim updates.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Troubleshooting Tips

The following commands can be used to troubleshoot ISG accounting:

- **debug aaa accounting**
- **debug radius** [**brief**]
- **debug subscriber feature name accounting** {**event** | **error** | **detail**}

Enabling ISG Per-Flow Accounting

ISG per-flow accounting can be configured in the following configuration sources:

- Service profile on a AAA server
- Service policy map on the ISG device

This procedure contains the following sections:

- Prerequisites, page 212
- Enabling Per-Flow Accounting in a Service Profile on the AAA Server, page 214
- Enabling Per-Flow Accounting in a Service Policy Map on the Router, page 214
- Troubleshooting Tips, page 213
- What to Do Next, page 216

Prerequisites

ISG sends accounting records to the authentication, authorization, and accounting (AAA) method list specified in the user profile, service profile, or service policy map. The tasks in this section assume that you have configured a AAA method list by using the **aaa accounting** command. See the Cisco IOS Security Command Reference for more information.

AAA servers must be configured to support ISG accounting.

Enabling Per-Flow Accounting in a Service Profile on the AAA Server

Perform this task to configure per-flow accounting in a service profile on the AAA server.

This task assumes that you have defined IP access lists for specifying traffic.

SUMMARY STEPS

1. Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"
2. Cisco-Avpair="accounting-list=*accounting-mlist-name* "
3. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"
Add the ISG Traffic Class attribute to the service profile. This attribute specifies input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

Step 2 Cisco-Avpair="accounting-list=*accounting-mlist-name* "
Add the Accounting attribute to the service profile on the AAA server. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent. The AAA method list must be configured.

Note If this attribute is configured in a service profile that does not include a traffic class, accounting is performed on the session rather than on the flow.

Step 3 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)
(Optional) Add the IETF RADIUS attribute Acct-Interim-Interval (attribute 85) to the service profile on the AAA server. This attribute specifies the number of seconds between interim updates.

Enabling Per-Flow Accounting in a Service Policy Map on the Router

Perform this task to enable accounting in a local service policy map for a specific flow.

This task assumes that you have defined a traffic class map and associated IP access lists. See the module "Configuring ISG Subscriber Services" for more information about configuring traffic classes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic** *class-map-name*
5. **accounting aaa list** *AAA-method-list*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or defines a service policy map, which is used to define an ISG service and enters service policy-map configuration mode.

Step 4	**class type traffic** *class-map-name*
	Example:
	`Router(config-service-policymap)# class type traffic firstclass`
		Associates a previously configured traffic class with the policy map and enters

Step 5	**accounting aaa list** *AAA-method-list* **Example:** `Router(config-control-policymap-class-traffic)# accounting aaa list list1`	Enables accounting and specifies the AAA method list to which accounting updates will be sent. • The AAA method list must be configured.
Step 6	**exit** **Example:** `Router(config-control-policymap-class-traffic)# exit`	Returns to service policy-map configuration mode.

Troubleshooting Tips

The following commands can be used to troubleshoot ISG accounting:

- **debug aaa accounting**
- **debug radius** [**brief**]
- **debug subscriber feature name accounting** {**event** | **error** | **detail**}

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Enabling ISG Per-Service Accounting

Per-service accounting can be configured in the following configuration sources:

- Service profile on a AAA server
- Service policy map on the ISG device

This procedure contains the following sections:

- Prerequisites, page 212
- Enabling Per-Service Accounting on the ISG, page 216
- Configuring RADIUS for Service Activation and Deactivation, page 217
- Enabling Per-Service Accounting in a Service Profile on a AAA Server, page 217
- Enabling Per-Service Accounting in a Service Policy Map on the Router, page 218
- What to Do Next, page 213
- Troubleshooting Tips, page 213

Prerequisites

ISG sends accounting records to the authentication, authorization, and accounting (AAA) method list specified in the user profile, service profile, or service policy map. The tasks in this section assume that you have configured a AAA method list by using the **aaa accounting** command. See the Cisco IOS Security Command Reference for more information.

AAA servers must be configured to support ISG accounting.

Enabling Per-Service Accounting on the ISG

Use the following procedure to enable per-service accounting on the ISG.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. subscriber service session-accounting
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	subscriber service session-accounting **Example:** `Router(config)# subscriber service session-accounting`	Enables subscriber services accounting. • All started services are included in the session accounting start message.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring RADIUS for Service Activation and Deactivation

Configure Cisco VSA 250 and VSA 252 in the service profile on RADIUS to dynamically activate and deactivate services. RADIUS uses VSA 250 in Access-Accept and VSA 252 in CoA messages. These VSAs have the following syntax:

```
252 0b "service(parameter1=value,parameter2=value,...)"
250 "service(parameter1=value,parameter1=value,...)"
```

When deactivating a service, RADIUS sends the same information in VSA 252 that was used for service activation, except that service deactivation uses 0c in the VSA instead of the 0b parameter used for service activation. VSA 252 has the following syntax for service deactivation:

252 0xC "service(parameter1=value,parameter2=value,...)"

Enabling Per-Service Accounting in a Service Profile on a AAA Server

Use the attributes in this procedure to enable per-service accounting in a service profile on a AAA server. Note that for per-service accounting, the traffic class attribute should not be included in the service profile.

SUMMARY STEPS

1. Cisco-Avpair="accounting-list=*accounting_mlist_name* "
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-Avpair="accounting-list=*accounting_mlist_name* "
Add the Accounting attribute to the service profile. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent.

Step 2 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)
(Optional) Add the Acct-Interim-Interval (attribute 85) to the service profile. This attribute specifies the number of seconds between interim updates.

Enabling Per-Service Accounting in a Service Policy Map on the Router

To configure per-service accounting in a service policy map on the router, you must configure an empty traffic class map (a traffic class map that does not specify an access list) and enable accounting within the empty traffic class in a service policy map. Perform this task to enable per-service accounting in a service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** class-map-name
4. **exit**
5. **policy-map type service** *policy-map-name*
6. **class type traffic** *class-map-name*
7. **accounting aaa list** *AAA-method-list*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type traffic match-any** class-map-name **Example:** `Router(config)# class-map type traffic match-any empty_class`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class, and enters traffic class map configuration mode. • For per-session accounting, create an empty traffic class map, that is, a traffic class map that does not specify an access list for matching traffic.
Step 4	**exit** **Example:** `Router(config-traffic-classmap)# exit`	Exit traffic class map configuration mode.
Step 5	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service polmap1`	Creates or defines a service policy map, which is used to define an ISG service and enters service policy-map configuration mode.

Step 6	**class type traffic** *class-map-name*
	Example:
	`Router(config-service-policymap)# class type traffic empty_class`
		Specifies a named traffic class whose policy you want to create or change and enters service policy traffic class configuration mode.
		• In this step, reference the empty traffic class map that you created in Step 3.

Step 7	**accounting aaa list** *AAA-method-list* **Example:** `Router(config-service-policymap-class-traffic)# accounting aaa list list1`	Enables accounting and specifies the AAA method list to which accounting updates will be sent.
Step 8	**exit** **Example:** `Router(config-service-policymap-class-traffic)# exit`	Returns to service policy-map configuration mode.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Troubleshooting Tips

The following commands can be used to troubleshoot ISG accounting:

- **debug aaa accounting**
- **debug radius** [**brief**]
- **debug subscriber feature name accounting** {**event** | **error** | **detail**}

Configuring ISG Postpaid Tariff Switching

ISG postpaid tariff switching can be configured in the service profile on a AAA server.

If you include a traffic class in the service profile, postpaid tariff switching will apply to the specified flow. If you do not configure a traffic class, postpaid tariff switching will apply to the session. Perform this task to configure per-session or per-flow postpaid tariff switching.

ISG per-session or per-flow accounting must be configured in order for postpaid tariff switching to work.

SUMMARY STEPS

1. Cisco-AVpair = “PPW*hh*:*mm*:*ss*:*d*”
2. Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

DETAILED STEPS

Step 1 Cisco-AVpair = “PPW*hh*:*mm*:*ss*:*d*”
Add the Post Paid VSA to the service profile. This attribute specifies the weekly tariff-switch points for postpaid tariff switching. The syntax description follows:

hh :*mm*:*ss*:*d*--Weekly tariff-switch time.

- hh = hour of day <0-23>
- mm = minutes <0-59>
- ss = seconds <0-59>
- d = bitmap format for the days of week. Each weekday is represented by one bit, as follows:

00000001 = Monday

00000010 = Tuesday

00000100 = Wednesday

00001000 = Thursday

00010000 = Friday

00100000 = Saturday

01000000 = Sunday

Step 2 Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"
Add the ISG Traffic Class attribute to the service profile. This attribute specifies input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

- What to Do Next, page 213

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Verifying ISG Accounting and Postpaid Tariff Switching

Perform the following tasks to verify ISG accounting and postpaid tariff switching configuration:

- Display Information About a Subscriber Session, page 221
- Examples, page 222
- Display AAA Subscriber Sessions, page 223
- Examples, page 224
- Display AAA Information for Subscribers, page 224
- Examples, page 224
- Display Information About ISG Postpaid Tariff Switching, page 227

Display Information About a Subscriber Session

Use the **show subscriber session** command to display information about an ISG subscriber session.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session`	Displays ISG subscriber session information.

Examples

This section contains examples of output for the **show subscriber session** command.

show subscriber session Output When ISG Accounting Is Applied to a Flow

In the following example, ISG accounting is configured in a service profile that specifies a traffic class, which means that accounting will be performed on the flow and not the parent session. In this example, 157 is the unique ID of the traffic class.

```
Router# show subscriber session uid 157 detailed
Subscriber session handle: E5000092, state: connected, service: Ltm Internal
Unique Session ID: 157
Identifier:
SIP subscriber access type(s): Traffic-Class
Root SIP Handle: 2B000011, PID: 76
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 45 seconds, Last Changed: 3 minutes, 45 seconds
AAA unique ID: 0
Switch handle: F300015F
Session inbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
```

Packets = 84, Bytes = 33600

```
Feature: Policing
 Upstream Params:
Average rate = 8000, Normal burst = 1500, Excess burst = 3000
Config level = Service
Session outbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
        Packets = 84, Bytes = 33600
Feature: Policing
 Dnstream Params:
Average rate = 64000, Normal burst = 12000, Excess burst = 24000
Config level = Service
Configuration sources associated with this session:
```

Service: video1, Active Time = 3 minutes, 46 seconds

show subscriber session Output When ISG Accounting Is Applied to a Session

The following example shows sample output for the **show subscriber session** command for a session rather than a flow.

```
Router# show subscriber session uid 730 detailed
```

```
Subscriber session handle: 3800009A, state: connected, service: Local Term
Unique Session ID: 730
Identifier: igq2acct
SIP subscriber access type(s): IP-Interface/Account-Logon-CH
Root SIP Handle: A600000E, PID: 75
Child SIP Handle: F9000018, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 57 seconds, Last Changed: 2 minutes, 59 seconds
AAA unique ID: 81
Switch handle: 890003A0
Interface: ATM6/0.1
Policy information:
  Authentication status: authen
  Config downloaded for session policy:
  From Access-Type: Account-Logon-CH, Client: SM, Event: Got More Keys
    Profile name: apply-config-only, 2 references
      ssg-account-info     "SAfoo"
  Rules, actions and conditions executed:
    subscriber rule-map rule1
      condition always event any-event
        action 1 authenticate
Session inbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000
Session outbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000
Configuration sources associated with this session:
```

Interface: ATM6/0.1, Active Time = 3 minutes, 58 seconds

Display AAA Subscriber Sessions

Use the **show aaa sessions** command to display information about AAA subscriber sessions.

SUMMARY STEPS

1. **enable**
2. **show aaa sessions**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show aaa sessions** **Example:** `Router# show aaa sessions`	Displays AAA subscriber session information.

Examples

This example shows sample output for the **show aaa sessions** command:

```
Router# show aaa sessions
Total sessions since last reload: 141
Session Id: 167
   Unique Id: 151
   User Name: *not available*
   IP Address: 192.168.0.1
   Idle Time: 0
   CT Call Handle: 0
```

Display AAA Information for Subscribers

Use the **show aaa user** command to display information about AAA subscribers.

SUMMARY STEPS

1. **enable**
2. **show aaa user** {**all**| *unique id*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show aaa user** {**all**| *unique id*}
	Example:
	`Router# show aaa users all`
		Displays AAA subscriber information for all users or a specified user.
		• Valid values for the user ID keyword are 1- 4294967295.

Examples

This section contains examples of output for the **show aaa user** command:

Output for a Specific User

```
Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
```

Dynamic attribute list:

```
1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  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 = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

Output for All Users

```
Router# show aaa user all
--------------------------------------------------
Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
  Dynamic attribute list:
    1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  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 = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

Display Information About ISG Postpaid Tariff Switching

Use the **show sss session**command to display information about ISG postpaid tariff switching.

SUMMARY STEPS

1. **enable**
2. **show sss session** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show sss session** [**all**] **Example:** `Router# show sss session`	Displays Subscriber Service Switch session status.

Configuration Examples for ISG Accounting

- Per-Flow Accounting Examples, page 227
- Per-Service Accounting Example, page 228
- Per-Service Accounting on ISG Example, page 228
- ISG Postpaid Tariff Switching Examples, page 228

Per-Flow Accounting Examples

Per-Flow Accounting Configured in a Local Service Policy Map

The following example shows per-flow accounting configured in a service policy map for a service called “video1”:

```
class-map type traffic match-any video1
 match access-group output 101
 match access-group input 100
policy-map type service video1
 class type traffic video1
```

accounting aaa list mlist1

Per-Flow Accounting Configured in a Service Profile on the AAA Server

The following example shows per-flow accounting configured in a remote service profile for a service called “video1”:

```
video1        Password = "cisco"
   Cisco-AVpair = "traffic-class=input access-group 101 priority 20",
   Cisco-AVpair = "traffic-class=output access-group 112 priority 20",
   Cisco-Avpair = "accounting-list=remote-local",
   Service-Info = "QU;8000",
```

Service-Info = "QD;64000"

Per-Service Accounting Example

The following configuration example allows multiple services in a single Access-Accept message and enables session accounting for the services. The example also enables RADIUS to authorize the subscriber to access the services.

```
subscriber service multiple-accept
subscriber service session-accounting
subscriber authorization enable
```

vpdn enable

Per-Service Accounting on ISG Example

The following example shows how to configure per-service accounting in a service policy map on the ISG device:

```
class-map type traffic match-any classmap1
policy-map type service polmap1
class type traffic classmap1
accounting aaa list mlist1
```

ISG Postpaid Tariff Switching Examples

The following example shows the configuration of a postpaid tariff switch each day of the week at midnight:

```
Cisco-AVpair = "PPW00:00:00:127"
```

The following example shows the configuration of a postpaid tariff switch Monday through Friday at 8:00 p.m.:

```
Cisco-AVpair = "PPW20:00:00:31"
```

The following example shows the configuration of a postpaid tariff switch Monday through Friday at 6:00 a.m.:

```
Cisco-AVpair = "PPW06:00:00:31"
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
AAA configuration tasks	"Authentication, Authorization, and Accounting (AAA)” section in the *Cisco IOS XE Security Configuration Guide*
AAA commands	"Authentication, Authorization, and Accounting (AAA)" section in the *Cisco IOS XE Security Command Reference*
Configuring ISG Subscriber Services	"Configuring ISG Subscriber Services" section in the *Cisco IOS XE Intelligent Services Gateway Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Accounting

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

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

Table 18 Feature Information for ISG Accounting

Feature Name	Releases	Feature Configuration Information
ISG: Accounting: Per Session, Service, and Flow	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server.
ISG: Accounting: Postpaid	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG sends accounting start and stop records for sessions and services to an accounting server for postpaid billing. The accounting server interprets the records to generate bills.

Feature Name	Releases	Feature Configuration Information
ISG: Accounting: Tariff Switching	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. Where billing rates change at fixed times and sessions are active across the boundary at which the rates change, ISG will provide accounting data to the billing server indicating the boundary.
ISG: Accounting: Per-Service Accounting	Cisco IOS XE Release 2.4	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Support for Prepaid Billing

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG prepaid billing support allows an ISG to check a subscriber's available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG prepaid billing works on a repeated reauthorization model in which fragments of credit, called *quotas* , are allotted by a prepaid billing server. This model allows a subscriber to be connected to multiple simultaneous prepaid services, each with a different billing rate. ISG supports time- and volume-based prepaid billing.

This module provides information about how to configure ISG support for prepaid billing.

- Finding Feature Information, page 233
- Prerequisites for ISG Prepaid Billing Support, page 233
- Restrictions for ISG Prepaid Billing Support, page 233
- Information About ISG Prepaid Billing Support, page 234
- How to Configure ISG Support for Prepaid Billing, page 236
- Configuration Examples for ISG Prepaid Billing Support, page 249
- Additional References, page 251
- Feature Information for ISG Support for Prepaid Billing, page 252

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Prepaid Billing Support

The tasks in this document assume that a subscriber session has been created and a method of service activation is in place.

Restrictions for ISG Prepaid Billing Support

- ISG prepaid billing support can only be applied to traffic flows that have been defined by an ISG traffic class.
- Quotas are measured in seconds for time and in bytes for volume. There is no way to change the unit of measure.
- The volume quota is for combined upstream and downstream traffic.
- The volume quota supports a maximum value of 4 GB.

Information About ISG Prepaid Billing Support

- Overview of ISG Support for Prepaid Billing, page 234
- ISG Prepaid Volume Monitor Polling Timer and QV Values, page 234
- ISG Prepaid Threshold, page 235
- ISG Prepaid Idle Timeout, page 235
- Benefits of ISG Prepaid Billing, page 235

Overview of ISG Support for Prepaid Billing

ISG prepaid billing support allows ISG to check the available credit for a subscriber to determine whether to activate the service for the subscriber and how long the session can last. The subscriber’s credit is administered by a prepaid billing server as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). A *quota* is an allotment, or fragment, of available credit. Allocating quotas in fragments rather than providing all the credit at once enables ISG to support the use of credit for multiple simultaneous prepaid sessions.

ISG uses the RADIUS protocol to facilitate interaction between ISG and external authentication, authorization, and accounting (AAA) servers and prepaid billing servers. A single device can serve as the AAA server and the billing server.

To obtain the first quota for a session, ISG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to ISG. ISG then monitors the session to track the quota usage. When the quota runs out or a specified limit is reached, ISG performs reauthorization. During reauthorization, the prepaid billing server may provide ISG with an additional quota if there is available credit. If no further quota is provided, ISG will log the user off from the service or perform some other specified action.

When a service is deactivated, the cumulative usage is provided to the prepaid billing server in an Accounting-Stop message.

ISG Prepaid Volume Monitor Polling Timer and QV Values

The Cisco IOS prepaid volume monitor polling timer determines when ISG will initiate a prepaid reauthorization. The polling timer value is (15 seconds < polling-monitor-time < 300 seconds). This value is calculated dynamically based on the QV value (which defines the volume-based quota), the actual rate, and the configured volume threshold. The prepaid volume monitor polling timer is not directly configurable.

To avoid allocating more volume quota than the subscriber is entitled to during the first authorization (when usage rate is unknown), the QV value should be a minimum of (15 x access rate). In cases in which the usage rate is known, the QV value should be at least (15 x usage rate).

In cases in which the input access rate is much higher than the QV value, it is recommended that the correct QV value be calculated using the following formula: access rate x 15 > QV < access rate x 300. For example, an ADSL2 or VDSL user access-rate can be up to 20 Mbps. That is approximately 2.5 megabytes (MB) of data in one second. Calculate the QV value by using the following formula: 2.5 MB x 15 seconds > QV < 2.5 MB x 300 seconds. This calculation results in a QV value between 37.5 MB and 750 MB, however we recommend you do not choose either the highest or lowest value in this range. For example, you might pick a value of QV = 100 MB.

ISG Prepaid Threshold

By default, ISG sends reauthorization requests to the billing server when a subscriber's quota is exhausted. ISG prepaid thresholds allow ISG to send reauthorization requests before a quota is used up. When a prepaid threshold is configured, ISG sends a reauthorization request to the billing server when the amount of remaining quota is equal to the value of the threshold. Prepaid thresholds can be configured for both time and volume.

For example, if the prepaid threshold is configured for 10 seconds, and the prepaid billing server sends ISG a quota of 30 seconds, ISG will send a reauthorization request to the prepaid billing server when the subscriber has used up 20 seconds of the quota and has 10 seconds remaining.

ISG Prepaid Idle Timeout

The ISG prepaid idle timeout can be used to suspend a prepaid service session if no traffic is received for a specified period of time. ISG keeps the session up during the suspension but releases all quota previously received for the prepaid session. Subsequent traffic on the session will cause ISG to send a reauthorization request and download a new quota for the session.

Benefits of ISG Prepaid Billing

Concurrent Prepaid Service Access

The ISG Support for Prepaid Billing feature is capable of supporting concurrent prepaid service access while maintaining the same pool of quota at the prepaid billing server. ISG services can be configured for concurrent or sequential access. Concurrent access allows users to log on to a service while simultaneously connected to other services.

Real-Time Billing

The ISG Support for Prepaid Billing feature allows for real-time billing with maximum flexibility, regardless of the type of service and billing scheme. Users can be billed on a flat rate, air-time, or volume basis.

Redirection Upon Exhaustion of Quota

When a user runs out of quota, ISG can redirect the user to a portal where the user can replenish the quota without being disconnected from the service.

Returning Residual Quota

ISG can return residual quota to the billing server from services that a user is logged into but not actively using. The quota that is returned to the billing server can be applied to other services that the user is actively using.

Threshold Values

ISG enables you to configure threshold values that cause prepaid sessions to be reauthorized before the subscriber completely consumes the allotted quota for a service.

Traffic Status During Reauthorization

You can prevent revenue leaks by configuring ISG to drop connected traffic during reauthorization of a service. The user remains connected to the service and does not need to log in to the service again, but no traffic is forwarded during the reauthorization process. This prevents a user from continuing to use a service for which the user has run out of quota while ISG sends a reauthorization request to the billing server.

Simultaneous Volume-Based and Time-Based Prepaid Billing

ISG supports rating on both time and volume simultaneously for prepaid services. The prepaid billing server may allocate quotas in both time and volume, and ISG monitors the session on both these parameters. ISG performs a reauthorization whenever either of these quota types is exhausted.

How to Configure ISG Support for Prepaid Billing

- Configuring RADIUS Attribute Support for ISG Prepaid Billing, page 236
- Creating an ISG Prepaid Billing Configuration, page 237
- Enabling ISG Prepaid Billing, page 240
- Redirecting Subscriber Traffic upon Exhaustion of Credit, page 243
- Forwarding Subscriber Traffic upon Depletion of Quota, page 247
- Troubleshooting ISG Prepaid Billing Support, page 249

Configuring RADIUS Attribute Support for ISG Prepaid Billing

Perform this task to enable ISG to include RADIUS attribute 44 in Access-Request packets and attribute 55 in Accounting-Request packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]
4. **radius-server attribute 55 include-in-acct-req**
5. **end**
6. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] **Example:** `Router(config)# radius-server attribute 44 include-in-access-req`	Sends RADIUS attribute 44 (Accounting Session ID) in Access-Request packets before user authentication.
Step 4	**radius-server attribute 55 include-in-acct-req** **Example:** `Router(config)# radius-server attribute 55 include-in-acct-req`	Sends the RADIUS attribute 55 (Event-Timestamp) in Accounting-Request packets.

Step 5	**end**
	Example:
	`Router(config)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Step 6	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

Creating an ISG Prepaid Billing Configuration

Perform this task to create or modify an ISG prepaid billing configuration. This configuration can be referenced in service profiles or service policy maps in which ISG prepaid support is enabled.

A default prepaid configuration exists with the following parameters:

```
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list authorization default
 method-list accounting default
 password cisco
```

The default configuration will not show up in the output of the **show running-config** command unless you change any one of the parameters.

The parameters of named prepaid configurations are inherited from the default configuration, so if you create a named prepaid configuration and want only one parameter to be different from the default configuration, you have to configure only that parameter.

This task assumes that AAA method lists, server groups, and servers have been configured. See the Cisco IOS Security Configuration Guide: Securing User Services for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber feature prepaid** {*name-of-config* | **default**}
4. **interim-interval** *number-of-minutes*
5. **method-list** {**accounting** | **authorization**} *name-of-method-list*
6. **password** *password*
7. **threshold** {**time** *seconds* | **volume** {*kilobytes* **Kbytes** | *megabytes* **Mbytes** | *bytes* **bytes**}}
8. **end**
9. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

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

	Command or Action	Purpose

Step 3	**subscriber feature prepaid** {*name-of-config* | **default**}
	Example:
	`Router(config)# subscriber feature prepaid conf-prepaid`
		Creates a new ISG prepaid configuration or specifies an existing configuration so it can be modified, and enters prepaid configuration mode.

Step 4	**interim-interval** *number-of-minutes* **Example:** `Router(config-prepaid)# interim-interval 5`	Enables interim prepaid accounting and specifies the interval at which ISG will send interim prepaid accounting records.
Step 5	**method-list** {**accounting** | **authorization**} *name-of-method-list* **Example:** `Router(config-prepaid)# method-list accounting list1`	Specifies the AAA method list to be used for ISG prepaid accounting or authorization.
Step 6	**password** *password* **Example:** `Router(config-prepaid)# password cisco`	Configures the password to be used for ISG prepaid authorization and reauthorization requests.

Step 7	**threshold** {**time** *seconds* | **volume** {*kilobytes* **Kbytes** | *megabytes* **Mbytes** | *bytes* **bytes**}}
	Example:
	`Router(config-prepaid)# threshold time 20`
		Configures the threshold at which ISG will send a reauthorization request to the prepaid billing server.
		• The quota provided by the billing server minus the configured threshold equals the value at which ISG will send a reauthorization request
		• This command can be entered twice to configure thresholds in both time and volume.

Step 8	**end**
	Example:
	`Router(config-prepaid)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 9	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

Enabling ISG Prepaid Billing

Perform one of the following tasks to enable prepaid billing in a service policy map or a remote service profile:

- Enabling ISG Prepaid Billing in a Service Policy Map, page 240
- Enabling ISG Prepaid Billing in Service Profile on the AAA Server, page 242

Enabling ISG Prepaid Billing in a Service Policy Map

Perform this task to enable ISG prepaid billing support in a service policy map.

ISG prepaid billing is enabled in a traffic class within a service policy map. This task assumes that you have defined the traffic class map and associated IP access lists. See the module "Configuring ISG Subscriber Services" for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **prepaid config** *name-of-configuration*
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service mp3`	Creates or defines a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic class-acl-101`	Associates a previously configured traffic class with the policy map, and enters control policy-map traffic class configuration mode.
Step 5	**prepaid config** *name-of-configuration* **Example:** `Router(config-control-policymap-class-traffic)# prepaid config conf-prepaid`	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters. **Note** The presence of this command does not guarantee that prepaid billing will be applied to the flow. This command causes the first prepaid authorization request. Whether prepaid billing will be applied to the flow is determined by the billing server.

Step 6	**end**
	Example:
	`Router(config-control-policymap-class-traffic)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

- What to Do Next, page 241

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Enabling ISG Prepaid Billing in Service Profile on the AAA Server

Perform this task to enable ISG support for prepaid billing in a service profile that is configured on a remote AAA server.

SUMMARY STEPS

1. Do one of the following:
   - Add the ISG Traffic Class attribute to the service profile.
   -
   - Cisco-AVpair = "ip:traffic-class=in access-group [<acl_number> | name <acl_name>] [priority <n>]"
   -
   -
   - Cisco-AVpair = "ip:traffic-class=out access-group [<acl_number> | name <acl_name>] [priority <n>]"
2. Add the ISG Prepaid Billing VSA to the service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Add the ISG Traffic Class attribute to the service profile. • • Cisco-AVpair = "ip:traffic-class=in access-group [<acl_number> | name <acl_name>] [priority <n>]" • • • Cisco-AVpair = "ip:traffic-class=out access-group [<acl_number> | name <acl_name>] [priority <n>]"	Specifies input and output traffic to which the service will apply. • Both an input and output traffic classifier can be added to a service profile.

Step 2	Add the ISG Prepaid Billing VSA to the service profile.
	Example:
	Example:
	`26,9,1 = "prepaid-config={<name-of-config>`
	`|`
	`default"`
		Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters.

- What to Do Next, page 243

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Redirecting Subscriber Traffic upon Exhaustion of Credit

Service providers often want to offer subscribers an opportunity to recharge their accounts when they have run out of credit for their prepaid services. The tasks in this section enable you to redirect a subscriber’s Layer 4 traffic to a specified server when the subscriber has run out of credit.

Before you configure ISG Layer 4 Redirect for exhaustion of credit, you should understand the following concept:

Perform the following tasks to redirect a subscriber’s Layer 4 traffic upon exhaustion of credit:

- Credit-Exhausted Event, page 243
- Configuring L4 Redirection in a Service Policy Map, page 243
- Applying a Service Policy Map to Subscriber Traffic upon Exhaustion of Credit, page 245
- What to Do Next, page 246

Credit-Exhausted Event

The ISG credit-exhausted event occurs when the prepaid server responds with an Access-Accept packet with a quota value of zero (time or volume) and an idle timeout greater than zero. In this case, the prepaid server has determined for certain that the subscriber does not have enough credit, but the idle timeout provides a grace period in which the subscriber could recharge the account. Typically, a service provider would want to redirect the subscriber’s traffic to a web portal where the subscriber could recharge the account. At the end of the idle-timeout interval, ISG will send a reauthorization request.

The default ISG behavior is to drop subscriber packets when the credit-exhausted event occurs.

Note Layer 4 redirection is one action that a service provider could take when a subscriber has run out of credit. Other actions can be configured instead of or in addition to Layer 4 redirection.

Configuring L4 Redirection in a Service Policy Map

Perform this task to configure ISG Layer 4 redirection in a service policy map.

The ISG Layer 4 Redirect feature can also be configured in a service profile on a AAA server. For more information about redirecting Layer 4 subscriber traffic, see the "Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module.

The ISG Layer 4 Redirect feature is configured under a traffic class within the service policy map. This task assumes that you have defined the traffic class map. See the "Configuring ISG Subscriber Services" module for more information.

Traffic can be redirected to a server or server group. If you are redirecting traffic to a server group, this task assumes that the server group has been configured. See the "Configuring ISG Subscriber Services" module for more information about configuring server groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-name*
5. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*]
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service redirect-service`	Creates or defines a service policy map, which is used to define an ISG service and enters service policy-map configuration mode.
Step 4	[*priority*] **class type traffic** *class-name* **Example:** `Router(config-service-policymap)# class type traffic class-all`	(Optional) Associates a previously configured traffic class with the policy map, and enters service policy-map traffic class configuration mode.
Step 5	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to group redirect-sg`	Redirects traffic to a specified server or server group.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-control-policymap-class-traffic)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

Applying a Service Policy Map to Subscriber Traffic upon Exhaustion of Credit

Perform this task to configure a control policy and apply a service policy map to subscriber traffic upon exhaustion of credit.

If you specify a named control class map, this task assumes that the class map has been configured. See the "Configuring ISG Control Policies" module for information about configuring control class maps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event credit-exhausted**
5. *action-number* **service-policy type service name** *policy-map-name*
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policyA`	Creates or modifies a policy map that defines a control policy.

Step 4	**class type control** {*control-class-name* | **always**} **event credit-exhausted**
	Example:
	`Router(config-control-policymap)# class type control always event credit-exhausted`
		Specifies a control class and event for which actions may be configured.

Step 5	*action-number* **service-policy type service name** *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service name redirect-profile`	Applies the specified service policy map or service profile in which the ISG Layer 4 Redirect feature has been configured.

Step 6	**end**
	Example:
	`Router(config-control-policymap-class-control)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

What to Do Next

Control policies must be applied to a context by using the **service-policy type control** command.

Forwarding Subscriber Traffic upon Depletion of Quota

By default, ISG drops subscriber packets when a subscriber’s quota has been depleted. This task enables you to override the default and forward subscriber traffic when the quota-depleted event occurs.

Before you perform this task you should understand the concept described in the Quota-Depleted Event, page 247 section.

- Quota-Depleted Event, page 247
- What to Do Next, page 246

Quota-Depleted Event

A quota-depleted event occurs when a subscriber’s quota is exhausted and ISG has not yet received a reauthorization response from the billing server. This event can occur in two situations:

- When a prepaid threshold is not configured and the subscriber’s quota is used up.
- When a prepaid threshold is configured but the quota is exhausted before the prepaid server responds to the reauthorization request that ISG sent when the threshold was met.

The quota-depleted event is not necessarily an indication that a subscriber does not have any more credit. ISG does not know for certain whether the subscriber has any more credit until a reauthorization response is returned from the billing server. For this reason, some service providers may choose to forward subscriber packets upon quota depletion until a reauthorization response is returned.

The default ISG behavior is to drop subscriber packets when a quota-depleted event occurs.

If you specify a named control class map, this task assumes that the class map has been configured. See the module "Configuring ISG Control Policies" for information about configuring control class maps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event quota-depleted**
5. *action-number* **set-param drop-traffic false**
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policyB`	Creates or modifies a policy map that can be applied globally, to an interface, or to an ATM VC to specify a control policy, and enters control policy-map configuration mode.

Step 4	**class type control** {*control-class-name* | **always**} **event quota-depleted**
	Example:
	`Router(config-control-policymap)# class type control always event quota-depleted`
		Specifies a control class and event for which actions may be configured, and enters control policy-map class control configuration mode.

Step 5	*action-number* **set-param drop-traffic false** **Example:** `Router(config-control-policymap-class-control)# 1 set-param drop-traffic false`	Configures ISG to continue to allow traffic to pass when the quota has been depleted.

Step 6	**end**
	Example:
	`Router(config-control-policymap-class-control)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

What to Do Next

Control policies must be applied to a context by using the **service-policy type control** command.

Troubleshooting ISG Prepaid Billing Support

Perform these steps to troubleshoot ISG prepaid billing support.

SUMMARY STEPS

1. Use the **show subscriber session** command to make sure the service in which prepaid billing support is configured has been activated.
2. If the service requires service authentication, make sure the authentication succeeded.
3. Make sure the AAA method list referred to in the prepaid billing configuration is valid and has been configured with the **aaa accounting network** command.
4. Use the **test aaa** command to make sure the AAA server is reachable from ISG.
5. Use the **debug subscriber policy prepaid** command to display debug messages about prepaid operation.

DETAILED STEPS

Step 1 Use the **show subscriber session** command to make sure the service in which prepaid billing support is configured has been activated.

Step 2 If the service requires service authentication, make sure the authentication succeeded.

Step 3 Make sure the AAA method list referred to in the prepaid billing configuration is valid and has been configured with the **aaa accounting network** command.

Step 4 Use the **test aaa** command to make sure the AAA server is reachable from ISG.

Step 5 Use the **debug subscriber policy prepaid** command to display debug messages about prepaid operation.

Configuration Examples for ISG Prepaid Billing Support

- ISG Prepaid Billing Support Example, page 249
- ISG Policies for Handling Credit-Exhausted and Quota-Depleted Prepaid Billing Events Example, page 250

ISG Prepaid Billing Support Example

The following example shows ISG prepaid billing support configured with the following parameters:

- The time threshold is 20 seconds.
- The volume threshold is 1000 bytes.
- When the quota-depleted event occurs, ISG will drop subscriber packets until the billing server sends another quota.
- When the credit-exhausted event occurs, subscriber packets will be redirected to the server group “redirect-sg”.
- The prepaid service is called “mp3” and is configured directly on the router in a service policy map.

- The AAA method list that will be used for this service to authenticate subscribers is called “cp-mlist”. That is the same method list to which the service accounting records will be sent.
- Prepaid authorization, reauthorization and accounting messages will be sent to the AAA method list called “ap-mlist”.

```
!
aaa authorization network default local
aaa authorization network ap-mlist group sg2
aaa authentication login cp-mlist group sg1
aaa accounting network cp-mlist start-stop group sg1
aaa accounting network ap-mlist start-stop group sg2
service-policy type control RULEA
!
class-map type traffic match-any CLASS-ALL
!
class-map type traffic match-any CLASS-ACL-101
    match access-group input 101
!
policy-map type control RULEA
 class type control always event credit-exhausted
  1 service-policy type service name redirectprofile
!
policy-map type service redirectprofile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
policy-map type service mp3
 class type traffic CLASS-ACL-101
  accounting aaa list cp-mlist
 !
 authenticate aaa list cp-mlist
!
subscriber feature prepaid conf-prepaid
 method-list accounting ap-mlist
 method-list authorization default
 password cisco
 threshold time 20
 threshold volume 1000 bytes
```

ISG Policies for Handling Credit-Exhausted and Quota-Depleted Prepaid Billing Events Example

In the following example, a single control policy called “RULEA” has been defined to override the ISG prepaid default behavior by forwarding subscriber packets after a quota-depleted event and redirecting subscriber packets after a credit-exhausted event:

```
!class-map type traffic match-any CLASS-ALL
!
policy-map type control RULEA
 class type control always event quota-depleted
  1 set-param drop-traffic false
 class type control always event credit-exhausted
  1 service-policy type service name l4redirect
!
policy-map type service l4redirect
 class type traffic CLASS-ALL
  redirect to group SESM
!
subscriber feature prepaid conf-prepaid
 threshold time 100
 threshold volume 1000 bytes
 method-list author prepaidlist
 method-list accounting default
 password cisco
```

Additional References

Related Documents

Related Topic	Document Title
AAA configuration tasks	The "Authentication, Authorization, and Accounting (AAA)" section in the*Cisco IOS XE Security Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Support for Prepaid Billing

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

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

Table 19 Feature Information for ISG Support for Prepaid Billing

Feature Name	Releases	Feature Configuration Information
ISG: Accounting: Prepaid	Cisco IOS XE Release 2.5.0	ISG prepaid billing support allows ISG to check a subscriber’s available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG supports volume-based and time-based prepaid billing.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Policies for Session Maintenance

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure a session timer and connection timer through a service policy map. Additionally, the Internet Engineering Task Force (IETF) RADIUS attributes Session-Timeout (attribute 27) and Idle-Timeout (attribute 28) can be used in service profiles on an authentication, authorization, and accounting (AAA) server to configure the same session maintenance control.

IP subscriber session keepalive support is configured for monitoring session data traffic in the upstream direction for idleness. Address Resolution Protocol (ARP) is used for Layer 2 connected subscribers. For routed host (Layer 3 connected) subscribers, the protocol defaults to Internet Control Message Protocol (ICMP). ICMP is also used in configurations where the access interface does not support ARP.

- Finding Feature Information, page 255
- Prerequisites for ISG Policies for Session Maintenance, page 255
- Restrictions for ISG Policies for Session Maintenance, page 256
- Information About ISG Policies for Session Maintenance, page 256
- How to Configure ISG Policies for Session Maintenance, page 257
- Configuration Examples for ISG Policies for Session Maintenance, page 268
- Additional References, page 270
- Feature Information for ISG Policies for Session Maintenance, page 272

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Policies for Session Maintenance

A traffic class is required only if an idle timer or session timer is being installed on a service that has a traffic class definition in it. If the timer is installed on a session or service that has no traffic class, a traffic class is not required. See the "Configuring ISG Subscriber Services" module for information about how to configure a traffic class.

Restrictions for ISG Policies for Session Maintenance

For an idle timeout that is applied on an IP session (rather than on a PPP session), there is currently no way to specify the direction. By default, the direction in which the idle timer is applied is always outbound.

Information About ISG Policies for Session Maintenance

- Session Maintenance Timers, page 256
- Benefits of Session Maintenance Timers, page 256
- Monitoring Sessions, page 256
- ARP for Keepalive Messages, page 257
- ICMP for Keepalive Messages, page 257

Session Maintenance Timers

ISG provides two commands (each of which can be set independently) to maintain control over a session and its connection. The **timeout absolute** command controls how long a session can be connected before it is terminated. The **timeout idle** command controls how long a connection can be idle before it is terminated. Both commands detect both PPP and IP sessions and can be applied in a non-traffic-class-based service, on a per-session basis, or in a flow (traffic-class-based service). All subscriber traffic will reset the timers; however, non-network traffic such as PPP control packets will not reset the timers.

The scope of the session timers and connection timers is determined by the type of service within which the timer is specified. If specified in a service profile for which no traffic class is defined, the timer action will be to terminate the session or connection. If a traffic class specifier resides in the service profile, the timer action will be to deactivate the service.

Benefits of Session Maintenance Timers

The PPP idle timeout functionality has been replaced by the ISG idle timeout feature. The idle timer is a generic feature that can be set to detect idle traffic in both PPP and IP sessions.

You set the idle timer in a service profile that is installed on a session to control how long that service stays installed before it is removed from the session because no traffic is flowing through that service. If the service has traffic class parameters associated with it, that traffic class is terminated when this timer expires, or when the session itself is terminated.

The same is true for the session timer, except that this timer determines how long the session or service stays up, regardless of traffic flowing through it.

Monitoring Sessions

The IP subscriber session’s data traffic in the upstream direction can be monitored for idleness using a keepalive feature configured for the subscriber. If a session is idle for a configured period of time, keepalive requests are sent to the subscriber. This action verifies that the connection is still active. The protocol to use for the keepalive request and response can be configured based on the IP subscriber session type. If it is a directly connected host (Layer #2 connection), ARP is used. For routed host (Layer 3 connected) subscribers, ICMP is used. If the access interface does not support ARP, the keepalive protocol defaults to ICMP.

ARP for Keepalive Messages

When a session is established and the keepalive feature is configured to use ARP, the keepalive feature saves the ARP entry as a valid original entry for verifying future ARP responses.

Note In cases where the access interface does not support ARP, the protocol for keepalives defaults to ICMP.

When ARP is configured, the ARP unicast request is sent to the subscriber. After a configured interval of time, the ARP response (if received) is verified. If the response is correct and matches the original entry that was saved when the subscriber was initially established, the keepalive feature continues monitoring the data plane for the configured interval of time. If the response is not correct, the keepalive feature resends the ARP request until a correct response is received or the configured maximum number of attempts is exceeded.

ICMP for Keepalive Messages

If ICMP is configured, the ICMP “hello” request is sent to the subscriber and checked for a response, until the configured maximum number of attempts is exceeded.

For IP subnet sessions, the peer (destination) IP address to be used for ICMP “hello” requests will be all the IP addresses within the subnet. This means “hello” requests will be sent sequentially (not simultaneously) to all the possible hosts within that subnet. If there is no response from any host in that subnet, the session will be disconnected.

Another option is to configure ICMP directed broadcast for keepalive requests. If the subscriber hosts recognize the IP subnet broadcast address, the ISG can send the ICMP “hello” request to the subnet broadcast address. The subscribers need not be on the same subnet as the ISG for this configuration to work. A directed broadcast keepalive request can work multiple hops away as long as these conditions are satisfied:

- The group of subscribers identified by the subnet must have the same subnet mask provisioned locally as the subnet provisioned on the subnet subscriber session on the ISG. Otherwise, the subscriber hosts will not recognize the subnet broadcast address.
- The router directly connected to the hosts must enable directed-broadcast forwarding, so that the IP subnet broadcast gets translated into a Layer 2 broadcast.

When these two conditions are satisfied, you can optimize the ICMP keepalive configuration to minimize the number of ICMP packets.

Note Because enabling directed broadcasts increases the risk of denial of service attacks, the use of subnet directed broadcasts is not turned on by default.

How to Configure ISG Policies for Session Maintenance

Configuring the session maintenance timers requires two separate tasks, one to set the idle timer and one to set the session timer. Either one or both of these tasks can be performed in order to set session maintenance control. The following tasks show how to set these timers in a service policy map and in a RADIUS AAA server profile:

- Configuring the Session Timer in a Service Policy Map, page 258
- Configuring the Session Timer on a AAA Server, page 259
- Configuring the Connection Timer in a Service Policy Map, page 259
- Configuring the Connection Timer on a AAA Server, page 261
- Verifying the Session and Connection Timer Settings, page 261
- Troubleshooting the Session and Connection Timer Settings, page 262
- Configuring a Session Keepalive on the Router, page 264
- Configuring a Session Keepalive on a RADIUS Server, page 266
- Configuring the ISG to Interact with the RADIUS Server, page 266

Configuring the Session Timer in a Service Policy Map

Perform this task to set the session timer in a service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*]**class type traffic***class-map-name*
5. **timeout absolute** *duration-in-seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service policy1`	Enters policy map configuration mode so you can begin configuring the service policy.

	Command or Action	Purpose
Step 4	[*priority*]**class type traffic***class-map-name* **Example:** `Router(config-control-policymap)# class type traffic class1`	Associates a previously configured traffic class with the policy map.
Step 5	**timeout absolute** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-control)# timeout absolute 30`	Specifies the session lifetime, in a range from 30 to 4294967 seconds.

Step 6	**end**
	Example:
	`Router(conf-subscriber-profile)# end`
		Returns to privileged EXEC mode.

- What to Do Next, page 259

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring the Session Timer on a AAA Server

Perform this task to set the session timer on a AAA server profile.

SUMMARY STEPS

1. **Session-Timeout=** *duration-in-seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Session-Timeout=** *duration-in-seconds*	Sets the IETF RADIUS session timer (attribute 27) in a user or service profile, in a range from 0 to 4294967 seconds.

Configuring the Connection Timer in a Service Policy Map

Perform this task to set the connection timer in a service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic***class-map-name*
5. **timeout idle** *duration-in-seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service policy1`	Enters policy map configuration mode so you can begin configuring the service policy.
Step 4	[*priority*] **class type traffic***class-map-name* **Example:** `Router(config-service-policymap)# class type traffic class1`	Associates a previously configured traffic class to the policy map.
Step 5	**timeout idle** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout idle 3000`	Specifies how long a connection can be idle before it is terminated. The range is platform and release-specific. For more information, use the question mark (?) online help function.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-control-policymap-class-traffic)# end`
		Returns to privileged EXEC mode.

- What to Do Next, page 259

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring the Connection Timer on a AAA Server

Perform this task to set the connection timer on a AAA server profile.

SUMMARY STEPS

1. **Idle-Timeout=** *duration-in-seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Idle-Timeout=** *duration-in-seconds*	Sets IETF RADIUS (attribute 28) in a user or service profile, in a range from 1 to 4294967 seconds.

Verifying the Session and Connection Timer Settings

Perform this task to verify that the timers have been installed correctly.

SUMMARY STEPS

1. **enable**
2. **show subscriber session all**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session all** **Example:** `Router# show subscriber session all`	Displays current subscriber information, including reports about the timers that are enabled.
Step 3	**end** **Example:** `Router#` **end**	Returns to privileged EXEC mode.

Troubleshooting the Session and Connection Timer Settings

The following sections list the **debug** commands that can be used to troubleshoot the session maintenance timers and describe the tasks you perform to enable them:

- Prerequisites for Troubleshooting the Session Maintenance Timers, page 262
- Restrictions for Troubleshooting the Session Maintenance Timers, page 262
- Debug Commands Available for the Session Maintenance Timers, page 263
- Enabling the Session Maintenance Timer Debug Commands, page 263

Prerequisites for Troubleshooting the Session Maintenance Timers

Before performing the task in this section, it is recommended that you be familiar with the use of Cisco IOS **debug** commands described in the introductory chapters of the *Cisco IOS Debug Command Reference* . Also see the module "Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging".

Restrictions for Troubleshooting the Session Maintenance Timers

Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the Cisco IOS **debug**commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users, or on a debug chassis with a single active session. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Debug Commands Available for the Session Maintenance Timers

The table below lists the **debug** commands that can be used to diagnose problems with the session maintenance timers.

Table 20 Debug Commands for Troubleshooting Session Maintenance Timers

Command	Purpose
debug subscriber feature error	Displays general Feature Manager errors.
debug subscriber feature event	Displays general Feature Manager events.
debug subscriber feature name idle-timer error	Displays idle timer errors.
debug subscriber feature name idle-timer event	Displays idle timer events.
debug subscriber feature name session-timer error	Displays session timer errors.
debug subscriber feature name session-timer event	Displays session timer events.

Enabling the Session Maintenance Timer Debug Commands

Perform this task to enable the session maintenance timer **debug** commands.

SUMMARY STEPS

1. **enable**
2. **debug** *command*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug** *command* **Example:** `Router# debug subscriber feature name session-timer error`	Enter one or more of the **debug** commands listed in Enabling the Session Maintenance Timer Debug Commands, page 263. • Enter the specific **no debug**command when you are finished.
Step 3	**end** **Example:** `Router#` **end**	Exits privileged EXEC mode.

Configuring a Session Keepalive on the Router

This task describes how to configure the keepalive feature on the router, using either ARP or ICMP.

Because the session keepalive feature is checking for the subscriber's health and presence, this feature is applied only to the session as a whole and not per-flow.

Note

- If a service profile includes an ISG traffic class configuration, the keepalive feature will be ignored.
- If this feature is applied to a non-IP session, for example, a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session, this feature application will fail and the following applies:
    - If the feature is applied at a session-start event, both the feature application and the session will fail.
    - If this feature is pushed onto a session after the session-start event, the push will fail.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol**{**ARP** | **ICMP** [**broadcast**]}]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service policymap1`	Enters service policy map configuration mode.
Step 4	**keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol**{**ARP** | **ICMP** [**broadcast**]}] **Example:** `Router(config-service-policymap)# keepalive idle 7 attempts 3 interval 1 protocol arp`	Enables keepalive messages and sets the maximum idle period, number of requests, interval between requests, and protocol for keepalive messages. • The ranges and default values for the **idle**, **attempts**, and **interval** keywords are platform and release-specific. For more information, use the question mark (**?**) online help function. • **protocol** --For Layer 2 connections, the default is ARP; for routed connections, the default is ICMP. • **broadcast** --This option is disabled by default. **Note** If this command is applied to a non-IP session, the command will fail. If the command is applied to a non-IP session at the session-start event, the session will also fail.
Step 5	**exit** **Example:** `Router(config-service-policymap)# exit`	Returns to global configuration mode.

Example

The following example configures the keepalive feature on a router using ARP:

```
policy-map type service accting_service
 class type traffic ALL
 !
```

```
  keepalive interval 3 protocol ARP
!
```

Configuring a Session Keepalive on a RADIUS Server

This task describes how to configure the session keepalive parameters on a RADIUS server.

SUMMARY STEPS

1. Service-Name password = “cisco”
2. Cisco-Avpair = "subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP* }"

DETAILED STEPS

Step 1 Service-Name password = “cisco”

Step 2 Cisco-Avpair = "subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP* }"
Configures the allowable idle period, maximum number of attempts to connect, the interval between attempts, and the communication protocol to be used.

The ranges and defaults are as follows:

- Idle period: range is 5 to10 seconds; default is 10 seconds.
- Attempts: range is 3 to 10; default is 5.
- Interval: default is 1 to 10 seconds.
- Protocol: for Layer 2 connections, the default is ARP; for routed connections, the default is ICMP.
- Broadcast option: by default this option is disabled.

Note If a service profile includes an ISG traffic class configuration, the keepalive feature will be ignored.

Configuring the ISG to Interact with the RADIUS Server

The ISG device interacts with the RADIUS server to listen for the Packet of Disconnect (POD) message from the RADIUS server. On receipt, the POD and associated attributes are handed to the appropriate client to disconnect the session. Perform this task to configure the ISG to interact with the RADIUS server to listen for the POD message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** *ip-address*
6. **port** *port-number*
7. **server-key** *word*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures a device as a AAA server to facilitate interaction with an external policy server and enters dynamic authorization local server configuration mode.
Step 5	**client** *ip-address* **Example:** `Router(config-locsvr-da-radius)# client 10.10.10.11`	Specifies a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests. • The example specifies 10.10.10.11 as the IP address of the RADIUS client.

	Command or Action	Purpose
Step 6	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1650`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. • The example specifies port 1650.
Step 7	**server-key** *word* **Example:** `Router(config-locsvr-da-radius)# server-key abc`	Configures the RADIUS key to be shared between a device and RADIUS clients. • The example specifies “abc” as the encryption key shared with the RADIUS client.
Step 8	**exit** **Example:** `Router(config-locsvr-da-radius)# exit`	Returns to global configuration mode.

Configuration Examples for ISG Policies for Session Maintenance

- Example Session Timer Configuration in a Service Policy Map, page 268
- Example Connection Idle Timer Configuration in a Service Policy Map, page 269
- Example Session Timer Show Command Output, page 269
- Example Connection Idle Timer Show Command Output, page 269
- Example Session Timer Debug Output, page 270
- Example Connection Idle Timer Debug Output, page 270

Example Session Timer Configuration in a Service Policy Map

The following example limits session time in a service policy map to 4800 seconds (80 minutes):

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout absolute 4800
 class type traffic default
 drop
```

Example Connection Idle Timer Configuration in a Service Policy Map

The following example limits idle connection time in a service policy map to 30 seconds:

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class type traffic traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout idle 30
 class type traffic default
 drop
```

Example Session Timer Show Command Output

The following example shows the settings for the session timer displayed by the **show subscriber session all** privileged EXEC command.

```
Current Subscriber Information: Total sessions 1
--------------------------------------------------
Unique Session ID: 3
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:50, Last Changed: 00:02:53
AAA unique ID: 4
Interface: Virtual-Access2.1
Policy information:
  Context 02DE7380: Handle 1B000009
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present
Non-datapath features:
 Feature: Session Timeout
  Timeout value is 180000 seconds
  Time remaining is 2d01h
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:02:52
```

Example Connection Idle Timer Show Command Output

The following example shows the settings for the idle timer as displayed by the **show subscriber session all** privileged EXEC command.

```
Current Subscriber Information: Total sessions 1
--------------------------------------------------
Unique Session ID: 4
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:44, Last Changed: 00:01:46
AAA unique ID: 5
Interface: Virtual-Access2.1

Policy information:
  Context 02DE7380: Handle AD00000C
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present
Session outbound features:
 Feature: PPP Idle Timeout
  Timeout value is 2000
  Idle time is 00:01:44

Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:01:47
```

Example Session Timer Debug Output

The following example shows output when the session timer debug commands (**debug subscriber feature error**, **debug subscriber feature event**, **debug subscriber feature name session-timer error**, and **debug subscriber feature name session-timer event**)are enabled.

```
*Jan 12 18:38:51.947: SSF[Vi2.1/Abs Timeout]: Vaccess interface config
update; not per-user, ignore
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Install interface configured
features
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Associate segment element handle
0x95000002 for session 1191182344, 1 entries
*Jan 12 18:38:53.195: SSF[Vt1/uid:3/Abs Timeout]: Group feature install
*Jan 12 18:38:53.195: SSF[uid:3/Abs Timeout]: Adding feature to none segment(s)
```

Example Connection Idle Timer Debug Output

The following example shows output when the idle timer debug commands (**debug subscriber feature error**, **debug subscriber feature event**, **debug subscriber feature name idle-timer error**, and **debug subscriber feature name idle-timer event**)are enabled.

```
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Install interface configured
features
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Associate segment element handle
0xF4000003 for session 67108875, 1 entries
*Jan 12 18:43:15.167: SSF[Vt1/uid:4/Idle Timeout]: Group feature install
*Jan 12 18:43:15.167: SSF[uid:4/Idle Timeout]: Adding feature to outbound
segment(s)
*Jan 12 18:43:15.167: Idle Timeout[uid:4]: Idle timer start, duration 2000
seconds, direction: outbound
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] created
02DFFDD8
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] added
02DFFDD8 [outbound]
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:19.147: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] bound
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
ppp timeout idle and **timeout absolute** PPP timer commands	*Cisco IOS Dial Technologies Command Reference*

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Policies for Session Maintenance

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

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

Table 21 Feature Information for ISG Session Maintenance

Feature Name	Releases	Feature Configuration Information
ISG: Session: Lifecycle: Idle Timeout	Cisco IOS XE Release 2.2	The ISG idle timeout controls how long a connection can be idle before it is terminated.

Feature Name	Releases	Feature Configuration Information
ISG: Session Protection & Resiliency: Keepalive-ARP, ICMP	Cisco IOS XE Release 2.2	IP subscriber session keepalive support is configured for monitoring session data traffic in the upstream direction for idleness. Address Resolution Protocol (ARP) is used for Layer 2 connected subscribers. For routed hosts (Layer 3 connected) subscribers, the protocol defaults to Internet Control Message Protocol (ICMP). ICMP is also used in configurations where the access interface does not support ARP. The following command was introduced: **keepalive** [**idle** *period1*] [**attempts** *max-retries*] [**interval** period2] [**protocol** *ICMP* [**broadcast**] | *ARP*] .
ISG: Session: Lifecycle: Packet of Disconnect (POD)	Cisco IOS XE Release 2.2	An ISG can be configured to interact with external policy servers. A policy server can use RADIUS Packet of Disconnect (POD) to manage the life cycle of any ISG session. The primary role of the POD message is to terminate an ISG session.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Redirecting Subscriber Traffic Using ISG Layer 4 Redirect

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure ISG to redirect subscriber traffic by using the ISG Layer 4 Redirect feature. The ISG Layer 4 Redirect feature enables service providers to better control the user experience by allowing subscriber TCP or User Datagram Protocol (UDP) packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be used to facilitate subscriber authentication, initial and periodic advertising captivation, redirection of application traffic, and Domain Name System (DNS) redirection.

- Finding Feature Information, page 275
- Restrictions for Redirecting ISG Subscriber Traffic, page 275
- Information About Redirecting ISG Subscriber Traffic, page 276
- How to Configure ISG Layer 4 Redirect, page 277
- Configuration Examples for ISG Layer 4 Redirect, page 282
- Additional References, page 284
- Feature Information for Redirecting ISG Subscriber Traffic, page 285

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 the Feature Information Table at the end of this document.

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

Restrictions for Redirecting ISG Subscriber Traffic

The ISG Layer 4 Redirect feature applies only to TCP or UDP traffic.

A Layer 4 Redirect feature and a Traffic-Class (TC) service containing a Layer 4 Redirect feature cannot be applied on the same session. A Layer 4 Redirect feature can be applied either on a session or on a TC on the session.

In Cisco IOS XE software, access lists cannot be configured as match criteria in an ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.

Information About Redirecting ISG Subscriber Traffic

- Overview of ISG Layer 4 Redirect, page 276
- Layer 4 Redirect Applications, page 276

Overview of ISG Layer 4 Redirect

The ISG Layer 4 Redirect feature redirects specified packets to servers that handle the packets in a specified manner. For example, packets sent upstream by unauthorized users can be forwarded to a server that redirects the users to a login page. Similarly, if users try to access a service to which they have not logged in, the packets can be redirected to a server that provides a service login screen.

The Layer 4 Redirect feature supports three types of redirection, which can be applied to subscriber sessions or to flows:

- Initial redirection--Specified traffic is redirected for a specific duration of the time only, starting from when the feature is applied.
- Periodic redirection--Specified traffic is periodically redirected. The traffic is redirected for a specified duration of time. The redirection is then suspended for another specified duration. This cycle is repeated. During periodic redirect, all new TCP connections are redirected until the duration of the redirect is over. After that time any new incoming TCP connections will not be redirected. However, all existing TCP connections that were initiated during this redirection will still be redirected so as not to break the connections.
- Permanent redirection--Specified traffic is redirected to the specified server all the time.

A redirect server can be any server that is programmed to respond to the redirected packets. If ISG is used with a web portal, unauthenticated subscribers can be sent automatically to a login page when they start a browser session. Web portal applications can also redirect to service login pages, advertising pages, and message pages.

Redirected packets are sent to an individual redirect server or redirect server group that consists of one or more servers. ISG selects one server from the group on a rotating basis to receive the redirected packets.

When traffic is redirected, ISG modifies the destination IP address and TCP port of upstream packets to reflect the destination server. For downstream packets, ISG changes the destination IP address and port to the original packet’s source.

When traffic is selected by a policy map that includes a **redirection** command, packets are fed back into the policy map classification scheme for a second service selection. The modified IP headers can be subject to different classification criteria. For example, if two class maps exist, each with different **redirection** commands, packets could be redirected, selected by the first class map, and redirected a second time. To avoid this situation, configure traffic class maps so that two consecutive redirections cannot be applied to the same packet.

Layer 4 Redirect Applications

The Layer 4 Redirect feature supports the following applications:

- TCP redirection for unauthenticated users and unauthorized services

HTTP traffic from subscribers can be redirected to a web dashboard where the subscribers can log in so that authentication and authorization can be performed.

- Initial and periodic redirection for advertising captivation

Subscriber traffic can be redirected to a sponsor's web page for a brief period of time at the start of the session or periodically throughout the session.

- Redirection of application traffic

Application traffic from a subscriber can be redirected so as to provide value-added services. For example, a subscriber's Simple Mail Transfer Protocol (SMTP) traffic can be redirected to a local mail server that can function as a forwarding agent for the mail.

- DNS redirection

DNS queries may be redirected to a local DNS server. In some deployments, such as public wireless LAN (PWLAN) hot spots, subscribers may have a static DNS server addresses, which may not be reachable at certain locations. Redirecting DNS queries to a local DNS server allows applications to work properly without requiring reconfiguration.

How to Configure ISG Layer 4 Redirect

There are three ways to apply Layer 4 redirection to sessions. One way is to configure redirection directly on a physical main interface or logical subinterface. A second way is to configure a service profile or service policy map with the Layer 4 redirect attribute in it, and apply that service to the session. A third way is to configure the Layer 4 redirect attribute in the user profile.

The following tasks describe how to configure Layer 4 redirection. The first task is optional. One or more of the next three tasks is required. The last task is optional.

For examples of Layer 4 redirection configuration for specific applications (such as unauthenticated user redirect), see the "Configuration Examples for ISG Layer 4 Redirect" section.

- Defining a Redirect Server Group, page 277
- Configuring Layer 4 Redirection in a Service Policy Map, page 278
- Configuring Layer 4 Redirection in a Service Profile or User Profile on the AAA Server, page 280
- Verifying ISG Traffic Redirection, page 281

Defining a Redirect Server Group

Perform this task to define a group of one or more servers to which traffic will be redirected. Traffic will be forwarded to servers on a rotating basis.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redirect server-group** *group-name*
4. **server ip** *ip-address* **port** *port-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redirect server-group** *group-name* **Example:** `Router(config)# redirect server-group ADVT-SERVER`	Enters redirect server-group configuration mode to define a group of servers in a named redirection server group.
Step 4	**server ip** *ip-address* **port** *port-number* **Example:** `Router(config-sg-l4redirect-group)# server ip 10.0.0.1 port 8080`	Adds a server to a redirect server group. - You can enter this command more than one time to add multiple servers to the server group.

Configuring Layer 4 Redirection in a Service Policy Map

Perform this task to configure Layer 4 redirection in a service policy map.

The ISG Layer 4 Redirect feature is configured under a traffic class within a service policy map. This task assumes that you have defined the traffic class map. See the "Configuring ISG Subscriber Services" module for more information.

Note Only ISG policing and accounting features can be enabled in conjunction with redirection on the same service policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redirect session-limit** *maximum-number*
4. **policy-map type service** *policy-map-name*
5. **class type traffic** *class-name*
6. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redirect session-limit** *maximum-number* **Example:** `Router(config)# redirect session-limit 5`	(Optional) Sets the maximum number of Layer 4 redirects allowed for each subscriber session.
Step 4	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Enters service policy-map configuration mode to create or modify a service policy map, which is used to define an ISG service.

Step 5	**class type traffic** *class-name*
	Example:
	`Router(config-service-policymap)# class type traffic class1`
		(Optional) Enters traffic class map configuration mode to specify a traffic class map that identifies the traffic to which this service applies.

	Command or Action	Purpose
Step 6	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	Redirects traffic to a specified server or server group.

- What to Do Next, page 280

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Layer 4 Redirection in a Service Profile or User Profile on the AAA Server

The Layer 4 Redirect feature can be configured as a Cisco vendor-specific attribute (VSA) in a user or service profile on an authentication, authorization, and accounting (AAA) server. This attribute can appear more than once in a profile to define different types of redirections for a session and can be used in both user and non-TC service profiles simultaneously.

SUMMARY STEPS

1. Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server. **Example:** `Cisco-AVPair = “ip:l4redirect=redirect to {group` *server-group-name* `| ip` *ip-address* `[port` *port-number*`]} [duration` *seconds*`] [frequency` *seconds*`]”`	Redirects traffic to a specified server or server group.

- What to Do Next, page 280

What to Do Next

If you configure ISG Layer 4 redirection in a service profile, you may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the "Configuring ISG Subscriber Services" module.

Verifying ISG Traffic Redirection

Perform this task to verify the configuration and operation of ISG Layer 4 traffic redirection. The commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show redirect translations** [**ip** *ip-address*]
3. **show redirect group** [*group-name*]
4. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show redirect translations** [**ip** *ip-address*] **Example:** `Router# show redirect translations ip 10.0.0.0`	Displays ISG Layer 4 redirect translations for sessions.
Step 3	**show redirect group** [*group-name*] **Example:** `Router# show redirect group redirect1`	Displays information about ISG redirect server groups.
Step 4	**show subscriber session** [**detailed**] [**identifier** *identifier*	**uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Examples

The following is sample output from the **show redirect translations** command:

```
Router# show redirect translations ip 10.53.0.2
Destination IP/port    Server IP/port        Prot  In Flags  Out Flags  Timestamp
172.20.0.2       23     10.2.36.253      23     TCP   none      none       May 08 2003
12:37:10
```

The following is sample output from the **show subscriber session** command. This output shows that Layer 4 redirect is being applied from the service profile.

```
Router# show subscriber session uid 135
Subscriber session handle: 7C000114, state: connected, service: Local Term
Unique Session ID: 135
Identifier: blind-rdt
SIP subscriber access type(s): IP-Interface
Root SIP Handle: CF000020, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 40 minutes, 30 seconds, Last Changed: 40 minutes, 30 seconds
AAA unique ID: 135
Switch handle: F000086
Interface: ATM2/0.53
Policy information:
  Authentication status: unauthen
  Config downloaded for session policy:
  From Access-Type: IP-Interface, Client: SM, Event: Service Selection Request, Service
    Profile name: blind-rdt, 2 references
      username             "blind-rdt"
      l4redirect           "redirect to group sesm-grp"
  Rules, actions and conditions executed:
    subscriber rule-map blind-rdt
      condition always event session-start
        action 1 service-policy type service name blind-rdt
Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    SVC  Redirect to group sesm-grp  !! applied redirect
Configuration sources associated with this session:
Service: blind-rdt, Active Time = 40 minutes, 32 seconds
Interface: ATM2/0.53, Active Time = 40 minutes, 32 seconds
```

The following is sample output from the **show subscriber session**command for a session in which the Layer 4 redirection is applied on the interface:

```
Router# show subscriber session uid 133
Subscriber session handle: D7000110, state: connected, service: Local Term
Unique Session ID: 133
Identifier:
SIP subscriber access type(s): IP-Interface
Root SIP Handle: 1E, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 42 minutes, 54 seconds, Last Changed: 42 minutes, 54 seconds
AAA unique ID: 133
Switch handle: 17000084
Interface: FastEthernet0/0.505
Policy information:
  Authentication status: unauthen
Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    INT  Redirect to group sesm-grp
Configuration sources associated with this session:
Interface: FastEthernet0/0.505, Active Time = 42 minutes, 54 seconds
```

Configuration Examples for ISG Layer 4 Redirect

- Redirecting Unauthenticated Subscriber Traffic Example, page 283
- Redirecting Unauthorized Subscriber Traffic Example, page 283
- Initial ISG Redirection Example, page 284
- Periodic ISG Redirection Example, page 284
- Redirecting DNS Traffic Example, page 284

Redirecting Unauthenticated Subscriber Traffic Example

In the following example, Layer 4 redirection is configured in the service policy map “BLIND-RDT.” This policy is applied to all sessions at session start and redirects subscriber TCP traffic to the server group called “PORTAL.” At account login the subscriber is authenticated and the redirection is not applied.

```
Service-policy type control DEFAULT-IP-POLICY
policy-map type control DEFAULT-IP-POLICY
 class type control always event session-start
  1 service-policy type service BLIND-RDT
!
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply BLIND-RDT
policy-map type service BLIND-RDT
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

Redirecting Unauthorized Subscriber Traffic Example

The following example shows the configuration of redirection for unauthorized subscribers. If the subscriber is not logged into the service called “svc,” traffic that matches “svc” is redirected to the server group “PORTAL.” Once the subscriber logs on to the service, the traffic is no longer redirected. When the subscriber logs off the service, redirection is applied again.

```
service-policy type control THE_RULE
!
class-map type traffic match-any CLASS-ALL
!
class-map type traffic match-any CLASS-100_110
 match access-group input 100
 match access-group output 110
!
policy-map type service blind-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc
 class type traffic CLASS-100_110
 class type traffic default in-out
  drop

!


policy-map type control THE_RULE
 class type control alwyas event account-logon
  1 authenticate
  2 service-policy type service name svc-rdt
 class type control cond-svc-logon event service-start
  1 service-policy type service unapply name svc-rdt
  2 service-policy type service identifier service-name
 class type control cond-svc-logon event service-stop
  1 service-policy type service unapply name svc
  2 service-policy type service name svc-rdt
 !
class-map type control match-all cond-svc-logon
 match identifier service-name svc
!
```

```
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

Initial ISG Redirection Example

The following example shows ISG configured to redirect the Layer 4 traffic of all subscribers to a server group called “ADVT” for the initial 60 seconds of the session. After the initial 60 seconds, ISG will stop redirecting the traffic for the rest of the lifetime of the session.

```
service-policy type control initial-rdt
policy-map type control intial-rdt
 class type control always event session-start
  1 service-policy type service name initial-rdt-profile
 !
policy-map type service initial-rdt-profile
 class type traffic CLASS-ALL
  redirect to group ADVT duration 60
```

Periodic ISG Redirection Example

The following example shows how to redirect all subscriber traffic for a period of 60 seconds every 3600 seconds:

```
service-policy control periodic-rdt session-start
!
policy-map type control periodic-rdt
 class type control always event session-start
  1 service-policy service periodic-rdt-profile
 !
policy-map type service periodic-rdt-profile
```

redirect to group ADVT duration 60 frequency 3600

Redirecting DNS Traffic Example

The following example shows how to redirect all subscriber DNS packets to the server group “DNS-server”:

service-policy type control DNS-rdt

```
policy-map type control DNS-rdt
 class type control event session-start
  1 service-policy type service name DNS-rdt-profile
  !
policy-map type service DNS-rdt-profile
 class type traffic CLASS-ALL
  redirect to group DNS-server
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
Configuring ISG subscriber services	"Configuring ISG Subscriber Services" module in this guide

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Redirecting ISG Subscriber Traffic

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

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

Table 22 Feature Information for Redirecting ISG Subscriber Traffic

Feature Name	Releases	Feature Information
ISG: Flow Control: Flow Redirect	Cisco IOS XE Release 2.2	The ISG Layer 4 Redirect feature enables service providers to better control the user experience by allowing subscriber TCP or UDP packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be applied to individual subscriber sessions or flows.
Parameterization for ACL and Layer 4 Redirect	Cisco IOS XE Release 2.4	The Parameterization for ACL and Layer 4 Redirect feature provides parameterization enhancements for access control lists and Layer 4 redirect.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Policies for Regulating Network Access

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports the use of policies for governing subscriber session bandwidth and network accessibility. This module provides information about the following methods of regulating session bandwidth and network access: Modular Quality of Service (QoS) command-line interface (CLI) policies and ISG policing.

- Finding Feature Information, page 287
- Information About ISG Policies for Regulating Network Access, page 287
- How to Configure ISG Policies for Regulating Network Access, page 289
- Configuration Examples for ISG Policies for Regulating Network Access, page 292
- Additional References, page 293
- Feature Information for ISG Policies for Regulating Network Access, page 294

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 the Feature Information Table at the end of this document.

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

Information About ISG Policies for Regulating Network Access

- Methods of Regulating Network Access, page 287
- Overview of ISG Policing, page 288

Methods of Regulating Network Access

ISG supports the following methods of regulating network access. Each of these methods can be applied to an ISG session and can be dynamically updated.

Modular QoS CLI (MQC) Policies

QoS policies configured using the MQC are supported for subscriber sessions only. MQC policies cannot be applied to ISG services.

ISG Policing

ISG policing supports policing of upstream and downstream traffic. ISG policing differs from policing configured using the MQC in that ISG policing can be configured in service profiles to support policing of traffic flows. MQC policies cannot be configured in service profiles. ISG policing can also be configured in user profiles and service profiles to support session policing.

Overview of ISG Policing

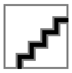
Traffic policing allows you to control the maximum rate of traffic sent or received on an interface. Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds the parameters is dropped or sent with a different priority.

ISG policing supports policing of upstream and downstream traffic and can be applied to a session or a flow. The following sections describe session-based policing and flow-based policing.

Session-Based Policing

Session-based policing applies to the aggregate of subscriber traffic for a session. In the figure below, session policing would be applied to all traffic moving from the PPPoE client to ISG and from ISG to the PPPoE client.

Figure 6

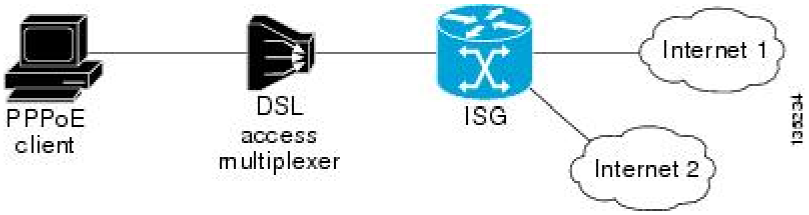


Session-based policing parameters can be configured on a AAA server in either a user profile or a service profile that does not specify a traffic class. It can also be configured on the router in a service policy map. Session-based policing parameters that are configured in a user profile take precedence over session-based policing parameters configured in a service profile or service policy map.

Flow-Based Policing

Flow-based policing applies only to the destination-based traffic flows that are specified by a traffic class. In the figure below, flow-based policing would allow you to police the traffic between the PPPoE client and Internet 1 or Internet 2.

Figure 7



Flow-based policing can be configured on a AAA server in a service profile that specifies a traffic class. It can also be configured on the router under a traffic class in a service policy map. Flow-based policing and session-based policing can coexist and operate simultaneously on subscriber traffic.

How to Configure ISG Policies for Regulating Network Access

- Configuring ISG Policing, page 289

Configuring ISG Policing

- Configuring Policing in a Service Policy Map on the Router, page 289
- Configuring Policing in a Service Profile or User Profile on the AAA Server, page 290
- Verifying ISG Policing, page 291

Configuring Policing in a Service Policy Map on the Router

Perform this task to configure ISG policing on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*]**class type traffic** *class-map-name*
5. **police input** *committed-rate normal-burst excess-burst*
6. **police output** *committed-rate normal-burst excess-burst*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	[*priority*]**class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic silver`	Associates a previously configured traffic class with the policy map.
Step 5	**police input** *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	Configures ISG policing of upstream traffic. • These parameters will be used to limit traffic flowing from the subscriber toward the network.
Step 6	**police output** *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police output 21000 31500 63000`	Configures ISG policing of downstream traffic. • These parameters will be used to limit the traffic flowing from the network toward the subscriber.

- What to Do Next, page 290

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Policing in a Service Profile or User Profile on the AAA Server

SUMMARY STEPS

1. Do one of the following:
   - Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server.
   - 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*"
   -
   - Add the following Policing VSA to the service profile on the AAA server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server. • 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*" • • Add the following Policing VSA to the service profile on the AAA server. **Example:** `26,9,251 "QU;`*committed-rate*`;`*normal-burst*`;`*excess-burst*`;D;`*committed-rate*`;`*normal-burst*`;`*excess-burst*`"`	Enables ISG policing of upstream and downstream traffic. • If you specify the committed rate and normal burst, excess burst will be calculated automatically. • You can specify upstream or downstream parameters first.

- What to Do Next, page 291

What to Do Next

You may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Verifying ISG Policing

Perform this task to verify ISG policing configuration.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Examples

The following example shows output for the **show subscriber session** command when policing parameters have been configured in the service profile. The “Config level” field indicates where the policing parameters are configured; in this case, in the service profile.

```
Router# show subscriber session detailed
Current Subscriber Information: Total sessions 2
Unique Session ID: 1
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Service
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service
.....
```

The following example shows output for the **show subscriber session** command where upstream policing parameters are specified in a user profile and downstream policing parameters are specified in a service profile.

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 2
Unique Session ID: 2
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Per-user  ===========> Upstream parameters are specified in
the user profile.
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service ============> No downstream parameters in the user
profile, hence the parameters in the service profile are applied.
.....
```

Configuration Examples for ISG Policies for Regulating Network Access

- ISG Policing Examples, page 293

ISG Policing Examples

Flow-Based Policing Configured in a Service Policy Map Using the CLI

The following example shows the configuration of ISG flow-based policing in a service policy map:

```
class-map type traffic match-any C3
 match access-group in 103
 match access-group out 203
policy-map type service P3
 class type traffic C3
  police input 20000 30000 60000
  police output 21000 31500 63000
```

Session-Based Policing Configured in a User Profile on a AAA Server

The following example shows policing configured in a user profile:

```
Cisco:Account-Info = "QU;23465;8000;12000;D;64000"
```

Session-Based Policing Configured in a Service Profile on a AAA Server

The following example shows policing configured in a service profile:

```
Cisco:Service-Info = "QU;16000;D;31000"
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
How to configure QoS policies using the MQC	"Applying QoS Features Using MQC" module in the *Cisco IOS XEQuality of Service Configuration Guide*
How to configure DBS	"Controlling Subscriber Bandwidth" module in the *Cisco IOS XEBroadband Access Aggregation and DSL Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/techsupport

Feature Information for ISG Policies for Regulating Network Access

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

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

Table 23 Feature Information for Policies for Regulating Network Access

Feature Name	Releases	Feature Configuration Information
ISG: Flow Control: QoS Control: Dynamic Rate Limiting	Cisco IOS XE Release 2.2	ISG can change the allowed bandwidth of a session or flow by dynamically applying rate-limiting policies.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Configuring ISG Integration with SCE

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure ISG and Cisco Service Control Engine (SCE) to function as a single policy enforcement point for subscriber sessions.

- Finding Feature Information, page 297
- Prerequisites for Configuring ISG Integration with SCE, page 297
- Restrictions for Configuring ISG Integration with SCE, page 298
- Information About Configuring ISG Integration with SCE, page 298
- How to Configure ISG Integration with SCE, page 299
- Configuration Examples for ISG Integration with SCE, page 308
- Additional References, page 309
- Feature Information for Configuring ISG Integration with SCE, page 310

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 the Feature Information Table at the end of this document.

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

Prerequisites for Configuring ISG Integration with SCE

- Hardware Requirements, page 297
- Software Requirements, page 298

Hardware Requirements

- An ISG platform, which can be a Cisco ASR 1000 series router
- An SCE platform
- Two connections between the ISG device and the SCE:
    - A control path, through which the ISG device and SCE can exchange policy information

  - A data path that carries the subscriber traffic
- A policy server configured to communicate with the ISG platform. The ISG-SCE integration removes any need for a communication layer between the policy server and the SCE.

Software Requirements

- Configure control and access policies, accounting, session maintenance, and network access regulation for ISG. For details on these configurations, see the *Cisco IOS XEIntelligent Services Gateway Configuration Guide.*
- Cisco Software Release 3.1.0 or later on the SCE
- Configure SCE appropriately. For instructions on configuring SCE, see the *Cisco Service Control Engine (SCE) Software Configuration Guide,* Release 3.1.

Restrictions for Configuring ISG Integration with SCE

The following restrictions apply to the integration of the ISG and an SCE:

- When an SCE policy is deactivated, the policy is removed from the session on the SCE, and the session policy reverts to the default SCE policy.
- Only one SCE policy at a time may be applied to a session. Applying additional policies will override the policy previously applied on the SCE.

This feature requires a control bus communication protocol, which runs over RADIUS and RADIUS extensions (as specified in RFC 3576), operating in two modes; PUSH and PULL.

- In PULL mode the ISG device waits for a query from the SCE.
- In PUSH mode the download of an external feature is initiated by the ISG device as soon as an external service is activated on the subscriber session.

To work with the SCE for subscriber management, the control bus protocol must do the following:

- Support pushing a session and make relevant changes to a session to the SCE.
- Allow a session, its relevant identity, and the SCE policy profile to be pulled from the ISG device by using an identity-based query.
- Support accounting events, including the following:
  - Accepting SCE initiated accounting events asynchronously.
  - Correlating SCE accounting data to the appropriate ISG session.
  - Parsing the SCE accounting data to perform protocol translation.

The per-user IP subnet assigned to Point-to-Point Protocol (PPP) users during login is not communicated to SCE. A per-user static route is downloaded to PPP users through the framed-route RADIUS attribute during login. ISG does not send the per-user subnet address for a PPP session to SCE in the CoA provision session (ProvSess) attribute.

Information About Configuring ISG Integration with SCE

- Overview of ISG-SCE Integration, page 299
- ISG and SCE Roles in Subscriber Management, page 299

Overview of ISG-SCE Integration

The ISG Integration with SCE feature integrates ISG and SCE at the policy plane level so that for purposes of subscriber provisioning, ISG and SCE function as a single logical entity. The ISG device and SCE communicate to manage subscriber sessions jointly, minimizing the requirements for coordination with additional external components. ISG handles subscriber management at Layer 4 and below. SCE is primarily focused at Layer 4 and above. When ISG and SCE are configured to work together, they provide tools for these functions:

- Subscriber mapping--Subscriber awareness is distributed between ISG and the SCE. The shared subscriber session is referenced by both devices using a unique session identifier allocated by the ISG. Identity keys such as IP Address, IP Subnet, network access server (NAS) identifier, and NAS port are also associated to the session. SCE policies that should be enabled on the session are identified by their policy names.
- Subscriber policy updates--Change subscriber policies in real time.

ISG and SCE Roles in Subscriber Management

The table below shows the specific roles of ISG and SCE in subscriber management.

Table 24 ISG and SCE Roles in Subscriber Management

Provided by ISG	Provided by SCE
Subscriber aggregation (broadband remote access service--BRAS) Subscriber authorization or authentication Policy management Policy enforcement for • Quality of service (QoS) • Multiprotocol label switching (MPLS) virtual private network (VPN) • Redirection • Session termination • Postpaid billing	Policy enforcement for • Application-aware services • Redirection and application-based policy management • Service security • Behavioral classification • URL caching and filtering • Value-added services • Parental controls • Usage and content billing

ISG pushes policies (or external services) to the SCE for a given subscriber session, in the form of RADIUS change of authorization (CoA) messages. External service activation can be triggered by the policy manager component inside the ISG or by an external authentication, authorization, and accounting (AAA) server. The SCE sees the ISG as the policy manager. ISG serves as a proxy for service activation requests from the external AAA server to the SCE. The SCE sends accounting records to the ISG. The ISG, if configured to do so, serves as a proxy that sends the accounting records to an external AAA server. SCE can also query the ISG about session information for unprovisioned sessions. ISG informs SCE when a session terminates by means of a RADIUS Packet of Disconnect (PoD).

How to Configure ISG Integration with SCE

- Configuring Communication Between SCE and ISG, page 300
- Configuring SCE Connection Parameter on ISG, page 301
- Configuring Control Policy on the Policy Manager, page 303
- Configuring Services, page 304

Configuring Communication Between SCE and ISG

Communication between the SCE and the ISG device is managed by an external policy delegation (EPD) handler module in Cisco IOS software. The EPD implements the control bus on the ISG and handles all messaging between the ISG device and SCE. This task is necessary to establish the parameters for the communication between the ISG device and the SCE, including the following:

- Port to which CoA messages are sent from the ISG device and SCE
- Port on which ISG should receive access, accounting, and connection management requests from SCE
- Shared secret between the ISG device and SCE

To configure communication between SCE and the ISG device, enter the following commands on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius** {**sesm** | **proxy** | **policy-device**}
4. **client** *ipaddress* [**port** *coa destination port*] [**key** *shared secret]*
5. **authentication port** *port-number*
6. **accounting port** *port-number*
7. **key** *shared-secret*
8. **exit**

DETAILED STEPS

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

	Command or Action	Purpose

Step 3	**aaa server radius** {**sesm** | **proxy** | **policy-device**}
	Example:
	`Router(config)# aaa server radius policy-device`
		Enters RADIUS server configuration mode and configures the RADIUS profile.

Step 4	**client** *ipaddress* [**port** *coa destination port*] [**key** *shared secret]* **Example:** `Router(config-locsvr-radius)# client 10.10.10.1 key cisco port 1431`	Configures client-specific details. • The IP address identifies the destination for CoA messages. If no port is configured, the default port (3799) is used. ISG sends CoA messages to the SCE to provision, update, or deactivate a session and activate or deactivate policies. • A shared secret configured for a specific client overrides the key configured using the **key shared-secret**command.
Step 5	**authentication port** *port-number* **Example:** `Router(config-locsvr-radius)# authentication port 1433`	Specifies the port on which the EPD handler listens for session and identity query requests from SCE. • If no port is specified, the default port (1645) is used.
Step 6	**accounting port** *port-number* **Example:** `Router(config-locsvr-radius)# accounting port 1435`	Specifies the port on which the EPD handler listens for accounting and peering requests and maintenance packets from SCE. • If no port is specified, the default port (1646) is used.
Step 7	**key** *shared-secret* **Example:** `Router(config-locsvr-radius)# key xxxxxxxxxx`	Configures the secret shared between the EPD handler and SCE. • This key is used if no per-client shared secret is configured.
Step 8	**exit** **Example:** `Router(config-locsvr-rasius)# exit`	Exits RADIUS server configuration mode.

Configuring SCE Connection Parameter on ISG

To configure the server connection management on either a per-server or a global basis, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-peer address** *ip-address* **keepalive** *seconds*
4. **policy-peer keepalive** *seconds*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-peer address** *ip-address* **keepalive** *seconds* **Example:** `Router(config)# policy-peer address 10.10.10.1 keepalive 6`	Configures the keepalive value, in seconds, for a specific policy defined by the given IP address. • Valid values are from 5 to 3600. • The default value is zero (0). • If the default value is in effect on the ISG device, the keepalive value proposed by the external policy device is used.
Step 4	**policy-peer keepalive** *seconds* **Example:** `Router(config)# policy-peer keepalive 10`	Configures the keepalive value, in seconds, globally. • The range of valid values is from 5 to 3600. • The default value is zero (0). • If no per-server keepalive value is configured, the global value is used. • If different values are configured on the ISG device and the SCE, the lower value is used as the keepalive interval. • If neither a per-server nor a global value is configured, the default value of zero is used.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Control Policy on the Policy Manager

To configure the policy manager to download a service, through rules configured by Cisco IOS commands, follow the steps in this section.

- Configuring Control Policy on the ISG, page 303
- Configuring Auto Service on the AAA Server, page 304

Configuring Control Policy on the ISG

To configure the control policy on the ISG device, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **service-policy type service name** *service-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control GOLD_POLICY`	Configures the specified policy-map on the ISG and enters policy map configuration mode.

	Command or Action	Purpose

Step 4	**class type control** {*class-map-name* | **always**} **event session-start**
	Example:
	`Router(config-control-policymap)# class type control always event acct-notification`
		Specifies to apply actions matching conditions defined by the class-map-name or always for an event type.
		• Event types include the following: account-logoff, account-logon, acct-notification, credit-exhausted, quota-depleted, service-failed, service-start, service-stop, session-default-service, session-restart, session-service-found, session-start, and timed-policy-expiry.

Step 5	*action-number* **service-policy type service name** *service-name* **Example:** `Router(config-control-policymap)# 1 service-policy type service name sce-service`	Defines the list of actions to be performed when the control policy is matched.
Step 6	**exit** **Example:** `Router(config-control-policymap)# exit`	Exits policy map configuration mode.

Configuring Auto Service on the AAA Server

To download a service to the ISG by means of auto service, perform the steps in this section.

SUMMARY STEPS

1. Cisco-Avpair="subscriber: auto-logon-service=sce-service"

DETAILED STEPS

Cisco-Avpair="subscriber: auto-logon-service=sce-service"
Downloads a service name from the SCE to the ISG device.

Configuring Services

To configure services, perform the steps in this section. You can configure this feature either on the ISG device, using the Cisco IOS command line interface (CLI) commands, or on the AAA server.

- Configuring Services on ISG, page 305
- Configuring Services on the AAA Server, page 306
- Troubleshooting Tips, page 307
- Examples, page 307

Configuring Services on ISG

To configure a service containing accounting features and to activate an external policy on the SCE device, follow the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-map-name*
4. **class-map type traffic** *class-map-name*
5. **accounting aaa list** *listname*
6. **sg-service-type external-policy**
7. **policy-name** *name*
8. **service-monitor enable**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *service-map-name* **Example:** `Router(config-traffic-classmap)# policy-map type service SVC`	Creates a service and enters traffic class map configuration mode.

Step 4	**class-map type traffic** *class-map-name*
	Example:
	`Router(config-control-policymap-class-control)# class-map type traffic bar`
		Defines a traffic class and enters control policy-map class configuration mode.

	Command or Action	Purpose
Step 5	**accounting aaa list** *listname* **Example:** `Router(config-service-policymap)# accounting aaa list list1`	Configures accounting for ISG and enters service policy map configuration mode.
Step 6	**sg-service-type external-policy** **Example:** `Router(config-control-policymap)# sg-service-type external-policy`	Defines the service as an external policy and enters policy map configuration mode.
Step 7	**policy-name** *name* **Example:** `Router(config-control-policymap)# policy-name gold` **Example:**	Defines a corresponding external policy name on the SCE.
Step 8	**service-monitor enable** **Example:** `Router(config-control-policymap)# service-monitor enable` **Example:**	Enables service monitoring for the external policy device.
Step 9	**exit** **Example:** `Router(config-pol-map)# exit`	Exits policy map configuration mode.

Configuring Services on the AAA Server

To configure a service on the external AAA server, perform the steps in this section.

SUMMARY STEPS

1. Cisco:Avpair="subscriber:sg-service-type=external-policy"
2. Cisco:Avpair="subscriber:policy-name=gold"
3. Cisco:Avpair="subscriber:service-monitor=1"
4. Cisco:Avpair="accounting-list=list1"

DETAILED STEPS

Step 1 Cisco:Avpair="subscriber:sg-service-type=external-policy"
Defines the service as an external policy.

Step 2 Cisco:Avpair="subscriber:policy-name=gold"
Defines a corresponding external policy name on the ISG.

Step 3 Cisco:Avpair="subscriber:service-monitor=1"
Enables service monitoring for the external policy device.

Step 4 Cisco:Avpair="accounting-list=list1"
Configures accounting for ISG.

Troubleshooting Tips

The following command can be used to troubleshoot the integration of ISG with SCE:

- **show subscriber policy peer { address** *ip-address* **| handle** *connection-handle* **|** *id* **| all }**

Examples

This section contains sample output of the **show subscriber policy peer**command.

show subscriber policy peer all

The following example shows sample output of the command when the **all** keyword is used.

```
Router# show subscriber policy peer all
Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:00:14
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:00:14
Remove owner on pull: TRUE
```

show subscriber policy peer all detail

The following example shows sample output for the **show subscriber policy peer**command when the **detail** keyword is added.

```
Router# show subscriber policy peer all detail
```

```
Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:04:00
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:04:00
Remove owner on pull: TRUE
Associated session details:
12.134.4.5session_guid_str
12.34.4.5session_guid_str
```

Configuration Examples for ISG Integration with SCE

- ISG Control Bus Configuration Example, page 308
- ISG Integration with SCE Example, page 308
- SCE Control Bus Configuration Examples, page 309

ISG Control Bus Configuration Example

The following example shows how to configure the ISG control bus with the SCE management IP address and shared authentication key:

```
aaa server radius policy-device
 client 10.10.10.10
 key cisco
 message-authenticator ignore
!
policy-peer address 10.10.10.10 keepalive 60
!
interface GigabitEthernet5/1/1
 ip address 10.10.10.1 255.255.255.0
!
```

ISG Integration with SCE Example

The following example shows how to configure two SCEs, each with the same authentication and accounting ports. ISG handles CoA messages on port 1700 for one SCE and on default port 3799 for the other SCE. Peering is maintained for each SCE with the ISG via different keepalive intervals.

When a user session starts, POLICY-LOCAL is applied. If the user's profile at the AAA server has auto-logon, the session will begin using the SCE-SERVICE-LOCAL service. This service has the SCE service-monitor facility enabled. If the user profile does not specify auto-logon to the SCE-SERVICE-LOCAL service, SCE will use its default values for the *policy-name* argument and the **service-monitor**command, which are configured at the SCE.

```
aaa accounting network service_acct start-stop group radius
aaa accounting network session_acct start-stop group radius
aaa server radius policy-device
 authentication port 1343
 accounting port 1345
 message-authenticator ignore
 client 10.10.10.1 port 1341 key cisco
class-map type traffic match-any bar
 match access-group input 102
access-list 102 permit ip any any
policy-map type service sce_service
```

```
 class type traffic bar
  accounting aaa list service_acct
 sg-service-type external-policy
 policy-name gold
 service-monitor enable
policy-map type control sce_policy
 class type control always event session-start
   1 service-policy type service sce_service
 class type control always event acct-notification
  1 proxy aaa list session_acct
```

SCE Control Bus Configuration Examples

SCE Control Bus Setup Configured in PUSH Mode

The following example shows how to configure the SCE control bus in PUSH mode:

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
scmp subscriber send-session-start
interface LineCard 0
 subscriber anonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

SCE Control Bus Setup Configured in PULL Mode

The following example shows how to configure the SCE control bus in PULL mode:

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
interface LineCard 0
 subscriber anaonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Intelligent Services Gateway Command Reference*
AAA configuration tasks	The "Authentication, Authorization, and Accounting (AAA)" module in the*Cisco IOS XESecurity Configuration Guide*
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" module in the *Cisco IOS Security Command Reference*
SCE configuration	Cisco Service Control Engine (SCE) Software Configuration Guide, Release 3.1

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/techsupport

Feature Information for Configuring ISG Integration with SCE

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

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

Table 25 Feature Information for ISG Integration with SCE

Feature Name	Releases	Feature Information
ISG: Policy Control: ISG-SCE Control Bus	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server. The following commands were introduced or modified: **aaa server radius policy-device**, **class type control**, **clear subscriber policy peer**, **clear subscriber policy peer session, policy-name**, **policy peer**, **proxy (ISG RADIUS proxy)**, **service-monitor**, **sg-service-type external policy**, **show subscriber policy peer**.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Service Gateway Interface

The Service Gateway Interface (SGI) feature implements a web services interface to access the policy, subscriber, and session management functionality of the Intelligent Services Gateway (ISG). It allows application developers to author subscriber management applications using commonly available commercial and open source protocols, encoding, and toolkits.

ISG is a framework of components for the policy-based control of sessions and services on network devices. The SGI feature comprises the data model for policy and associated elements and the operational interface to provision, update, delete, and control activation of those policies.

- Finding Feature Information, page 313
- Information About Service Gateway Interface, page 313
- How to Enable Service Gateway Interface, page 314
- Configuration Examples for Service Gateway Interface, page 316
- Additional References, page 317
- Feature Information for Service Gateway Interface, page 318

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 the Feature Information Table at the end of this document.

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

Information About Service Gateway Interface

- ISG, page 313
- BEEP, page 314
- Benefits of SGI, page 314

ISG

ISG is a Cisco IOS and Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. See "Overview of ISG" for further information.

BEEP

Block Extensible Exchange Protocol (BEEP) is a protocol standard that is scalable, efficient, simple, extensible, and robust. BEEP is a framework for designing application protocols.

Benefits of SGI

SGI is a protocol that allows Cisco IOS XE software to be controlled using third-party applications, toolkits, and development platforms for web services.

The SGI feature is a common model that can express ISG provisioning in many languages, and it is easy to use.

How to Enable Service Gateway Interface

- Configuring BEEP Listener Connection, page 314
- Troubleshooting SGI, page 315

Configuring BEEP Listener Connection

Perform this task to enable SGI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sgi beep listener [** *port][* **acl** *access-list][* **sasl** *sasl-profile][* **encrypt** *trustpoint]*
4. end

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**sgi beep listener [** *port][* **acl** *access-list][* **sasl** *sasl-profile][* **encrypt** *trustpoint]* **Example:** `Router(config)# sgi beep listener 2089`	Enables the SGI feature.

Step 4	end
	Example:
	`Router(config)# end`
		Exits global configuration mode.

Troubleshooting SGI

Perform this task to troubleshoot the SGI.

SUMMARY STEPS

1. **enable**
2. **show sgi** [**session**| **statistics**]
3. **debug sgi** [**error**| **info**| **xml**| **gsi**| **isg-api**| **all**]
4. **test sgi xml** *filename*

DETAILED STEPS

Step 1 **enable**

Enables privilege EXEC mode. Enter your password if prompted.

Step 2 **show sgi** [**session**| **statistics**]

Displays information about current SGI session. This command shows information about SGI sessions that have been started and are currently running, including the running state. It also shows statistical information about SGI sessions that have been started and are currently running. The following is sample output from this command:

Example:

```
Router# show sgi session
sgi sessions: open 1(max 10, started 15
session id:1;started at 9:08:05; state OPEN

Router# show sgi statistics
sgi statistics
total messages received 45
current active messages 5; maximum active messages 7
total isg service requests 4
current active services 2; maximum active services 2
sgi process statistics
process sgi handler 1
pid 95, cpu percent (last minute) 1, cpu runtime 10(msec), memory accocated 4200 (bytes)
```

Step 3 **debug sgi** [**error**| **info**| **xml**| **gsi**| **isg-api**| **all**]

Enables debugging of SGI sessions. The following is sample output from this command when all debugging has been enabled:

Example:

```
Router# debug sgi all
Router# show debug

SGI:
SGI All debugging is on
SGI Errors debugging is on
SGI XML debugging is on
SGI Informational debugging is on
SGI Generic Service Interface debugging is on
SGI ISG_API Events debugging is on
SGI ISG_API Errors debugging is on
Router#
Router#
*Jul 1 20:55:11.364: SGI: Session created, session Id 7
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M number=1
answer=-1 more=* size=1400
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: Content-Type: application/xml
<?xml version="1.0" encoding="UTF-8"?>
...
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M number=1
answer=-1 more=. size=111
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: gitypes:policyGroup>
</objects>
</sgiops:insertPolicyObjectsRequest>
...
*Jul 1 20:55:11.372: SGI: GSI message received, msgid 1, session 7
*Jul 1 20:55:11.376: SGI: XML parsed successfully, request insertPolicyObjectsRequest, msgid 1
*Jul 1 20:55:11.376: SGI: authentication request sent to AAA
*Jul 1 20:55:11.376: SGI: req = [0x67454088] authentication succeeded
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsRequest
*Jul 1 20:55:11.376: SGI: insertPolicyObjectsRequest processing policyGroup:VPDN1, type 1, result:
0
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsResponse
*Jul 1 20:55:11.376: SGI: GSI message sent, msgid 1, session 7
*Jul 1 20:55:12.088: sgi beep listen app beep[0x66245188]: close confirmation: status=+ no error
origin=L scope=C
*Jul 1 20:55:12.088: SGI: Session terminating, session Id 7
```

Step 4 **test sgi xml** *filename*

Verifies the format ofan SGI XML request. The XML file must be copied to the router before it can be used.

Configuration Examples for Service Gateway Interface

- Configuring BEEP Listener Connection Example, page 316

Configuring BEEP Listener Connection Example

The following example shows how to configure the BEEP listener connection. The port number is set to 2089.

```
enable
```

```
configure terminal
sgi beep listener 2089
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
Overview of ISG	*Cisco IOS XE Intelligent Services Gateway Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/techsupport

Feature Information for Service Gateway Interface

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

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

Table 26 Feature Information for Service Gateway Interface

Feature Name	Releases	Feature Information
Service Gateway Interface	Cisco IOS XE Release 2.2	The SGI implements a web services interface to access the policy, subscriber, and session management functionality of ISG. The following commands were introduced or modified: **debug sgi**, **sgi beep listener**, **show sgi, test sgi xml**.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers.This document describes ISG session monitoring and distributed conditional debugging. Conditional debugging facilitates debug filtering for ISG and is available as distributed conditional debugging.

- Finding Feature Information, page 321
- Prerequisites for ISG Session Monitoring and Distributed Conditional Debugging, page 321
- Restrictions for Distributed Conditional Debugging, page 322
- Information About ISG Session Monitoring and Distributed Conditional Debugging, page 322
- How to Enable ISG Session Monitoring and Distributed Conditional Debugging, page 323
- Configuration Examples for ISG Distributed Conditional Debugging, page 330
- Additional References, page 331
- Feature Information for Distributed Conditional Debugging, page 332

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 the Feature Information Table at the end of this document.

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

Prerequisites for ISG Session Monitoring and Distributed Conditional Debugging

Before using the information in this module, it is recommended that you be familiar with the use of Cisco IOS **debug** commands and conditional debugging. See the "Additional References" section to find information about these topics.

Restrictions for Distributed Conditional Debugging

Conditions that are set for an active session take effect only when the session is terminated and reestablished.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the Cisco IOS **debug**commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users, or on a debug chassis with a single active session. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Information About ISG Session Monitoring and Distributed Conditional Debugging

- ISG Session and Flow Monitoring, page 322
- ISG Distributed Conditional Debugging, page 322

ISG Session and Flow Monitoring

ISG introduces a mechanism that allows an administrator to monitor ISG sessions and flows continuously. The **show interface monitor** command, which displays interface statistics, and the **show process cpu monitor** command, which displays information about CPU usage, both update the information in their displays at specified intervals. These commands also provide the ability to freeze or clear the information in the display.

ISG Distributed Conditional Debugging

- Benefits of Enhanced Conditional Debugging for the ISG Platforms, page 322
- Cisco IOS Software Components Supported by Distributed Conditional Debugging, page 322

Benefits of Enhanced Conditional Debugging for the ISG Platforms

Because thousands of user sessions run on the ISG platforms, it is not practical to troubleshoot a problem with a session by enabling the various component **debug** commands that are available and trace through the messages for a single session or user. Instead, it is more practical to filter debugging messages for a single session or call across the various Cisco IOS XE components that a session traverses. For this reason, the conditional debugging previously offered in the Cisco IOS XE software has been enhanced to facilitate debug filtering for ISG and is available as distributed conditional debugging.

Cisco IOS Software Components Supported by Distributed Conditional Debugging

The following components are supported for ISG distributed conditional debugging:

- Authentication, authorization, and accounting (AAA) and RADIUS
- ATM components
- Feature Manager
- Policy Manager
- PPP
- PPP over Ethernet (PPPoE)
- Session Manager
- Virtual Private Dialup Network (VPDN)

See Table 1 and Table 2 for specific commands that are supported for distributed conditional debugging.

How to Enable ISG Session Monitoring and Distributed Conditional Debugging

- Monitoring ISG Sessions and Flows, page 323
- Configuring Distributed Conditional Debugging, page 324

Monitoring ISG Sessions and Flows

Perform this task to monitor interface and CPU statistics. The **show** commands are not required and may be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show interface** *type number* **monitor** [**interval** *seconds*]
3. **show processes cpu monitor** [**interval** *seconds*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**show interface** *type number* **monitor** [**interval** *seconds*] **Example:** `Router# show interface ethernet 3/0 monitor interval 10`	Displays interface statistics that are updated at specified intervals.

	Command or Action	Purpose
Step 3	**show processes cpu monitor** [**interval** *seconds*] **Example:** `Router# show processes cpu monitor`	Displays detailed CPU utilization statistics that are updated at specified intervals.

Configuring Distributed Conditional Debugging

Two main tasks are required for configuring distributed conditional debugging: enabling conditional debugging, and issuing one or more supported **debug** commands. These required tasks are described in the following sections:

- ISG Debug Condition Commands, page 324
- Debug Commands That Are Supported by ISG Conditional Debug, page 325
- Restrictions, page 327
- Enabling Distributed Conditional Debugging, page 328
- Displaying Debugging Conditions, page 328
- Troubleshooting Tips, page 329

ISG Debug Condition Commands

The table below lists the **debug condition** commands that you can issue at the EXEC prompt to enable distributed conditional debugging. You can set more than one condition.

Table 27 Supported Conditional Debug Commands

Command	Purpose
debug condition domain *domain-name*	Filters messages on the specified domain name.
debug condition interface atm *ATM-interface* **vc** {*vci* / *vpi*| *vci*}	Filters messages on the specified virtual circuit.
debug condition interface {**atm** *ATM-interface* **vc** {*vci* / *vpi* | *vci*} | **Ethernet** | **Fast Ethernet** | **Gigabit Ethernet**} **vlan-id** *ID*	Filters messages on the specified VLAN identifier.
debug condition mac-address *hexadecimal-MAC-address*	Filters messages on the specified MAC address.
debug condition portbundle ip *IP-address* **bundle** *bundle-number*	Filters messages on the specified Port-Bundle Host Key (PBHK).
debug condition session-id *session-ID*	Filters messages on the specified session identifier. **Note** The session identifier can be obtained by entering the **show subscriber session** command.
debug condition username *email-address*	Filters messages on the specified Internet username.

Debug Commands That Are Supported by ISG Conditional Debug

The table below lists the Cisco IOS debugging commands that are supported for distributed conditional debugging. The commands are listed by component. One or more of these commands can be issued after enabling one of the **debug condition** commands listed in the table above.

Table 28 Debug Commands Supported by ISG Distributed Conditional Debugging

AAA Debug Commands
debug aaa accounting
debug aaa authentication
debug aaa authorization
debug aaa id
ATM Debug Commands
debug atm arp
debug atm error
debug atm event
debug atm oam
debug atm packet
debug atm state
PPP Debug Commands
debug ppp authentication
debug ppp bap error
debug ppp bap events
debug ppp bap negotiation
debug ppp cbcp
debug ppp error
debug ppp mppe detailed
debug ppp mppe events
debug ppp mppe pack
debug ppp multi data
debug ppp multi events

AAA Debug Commands
debug ppp multi frag
debug ppp negotiation
debug ppp pack
debug ppp subscriber
PPPoE Debug Commands
debug pppoe data
debug pppoe error
debug pppoe event
debug pppoe packet
Session Manager Debug Commands
debug subscriber aaa authorization event
debug subscriber aaa authorization fsm
debug subscriber error
debug subscriber event
Feature Manager Debug Commands
debug subscriber feature access-list error
debug subscriber feature access-list event
debug subscriber feature compression detail
debug subscriber feature compression error
debug subscriber feature compression event
debug subscriber feature detail
debug subscriber feature error
debug subscriber feature event
debug subscriber feature interface-config error
debug subscriber feature interface-config event
debug subscriber feature modem-on-hold detail
debug subscriber feature modem-on-hold error
debug subscriber feature modem-on-hold event

AAA Debug Commands
debug subscriber feature portbundle error
debug subscriber feature portbundle event
debug subscriber feature portbundle packet
debug subscriber feature qos-policy error
debug subscriber feature qos-policy event
debug subscriber feature static-routes error
debug subscriber feature static-routes event
debug subscriber feature traffic-classification detail
debug subscriber feature traffic-classification error
debug subscriber feature traffic-classification event
Policy Manager Debug Commands
debug subscriber fsm
debug subscriber policy condition
debug subscriber policy detail
debug subscriber policy error
debug subscriber policy event
debug subscriber policy fsm
debug subscriber policy rule
debug subscriber session error
debug subscriber session event
VPDN Debug Commands
debug vpdn call event
debug vpdn call fsm
debug vpdn error
debug vpdn event
debug vpdn event disconnect

Restrictions

The **debug condition session-id** command filters a session only after the session has been established. The session identifier is a unique dynamic number generated internally by the Cisco IOS software and assigned to each session when the session is established.

In VPDN, the **debug** commands and messages associated with tunnels cannot be filtered because they are not associated with a session, but are displayed during the tunnel-establishment phase. The debugging messages will be displayed even if filtering is enabled by one of the conditions.

If multiple conditions are set, the debugging messages corresponding to all the sessions that meet any of the conditions will be displayed. Some conditions, such as domain name, will trigger debugging messages for all the sessions that belong to the particular domain.

Enabling Distributed Conditional Debugging

Perform this task to enable distributed conditional debugging for ISG.

SUMMARY STEPS

1. **enable**
2. **debug condition** *command*
3. **debug** *command*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug condition** *command* **Example:** `Router# debug condition username user@cisco.com`	Enter one or more of the **debug condition** commands listed in Table 1 to enable distributed conditional debugging.
Step 3	**debug** *command* **Example:** `Router# debug subscriber aaa authorization fsm`	Enter one or more of the supported **debug** commands from Table 2.

Displaying Debugging Conditions

To display the debugging conditions that have been set, perform the following task:

SUMMARY STEPS

1. **enable**
2. **show debug condition**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show debug condition** **Example:** `Router# show debug condition`	Displays conditions that have been set for debugging.

Troubleshooting Tips

The Cisco IOS software displays messages as you set the conditions for filtering the debugging.

When a condition is set, it is assigned a number, as follows:

```
Condition 1 set
```

If a condition has already been set, the following message is displayed:

```
% Condition already set
```

The following messages and prompt are displayed when you attempt to disable the last condition using the **no** form of a **debug condition** command:

```
This condition is the last interface condition set.
Removing all conditions may cause a flood of debugging messages
to result, unless specific debugging flags are first removed.

Proceed with removal? [yes/no]: yes
Condition 1 has been removed
```

Tip Use the **no** form of the commands to disable all **debug** commands before disabling all of the debugging conditions that have been set.

Configuration Examples for ISG Distributed Conditional Debugging

- Monitoring Interface Statistics Example, page 330
- Monitoring CPU Statistics Example, page 330
- Enabling ISG Distributed Conditional Debugging Example, page 331
- Displaying Debugging Conditions Example, page 331
- Filtering Debug Output Example, page 331

Monitoring Interface Statistics Example

The following example shows sample output for the **show interface monitor** command. The display will be updated every 10 seconds.

```
Router> show interface ethernet 0/0 monitor interval 10

Router Name:  Scale3-Router8       Update Secs: 10
Interface Name:   Ethernet 0/0          Interface Status: UP, line is up

Line Statistics:          Total:        Rate(/s)    Delta
Input Bytes:              123456        123         7890
Input Packets:              3456         56          560
Broadcast:                  1333          6           60
OutputBytes:               75717        123         1230
Output Packets:              733         44          440

Error Statistics:         Total:        Delta:
Input Errors:              0               0
CRC  Errors:               0               0
Frame Errors:              0               0
Ignored:                   0               0
Output Errors:             0               0
Collisions:                0               0

No. Interface Resets:  2
End = e       Clear = c      Freeze = f
Enter Command:
```

Monitoring CPU Statistics Example

The following example shows sample output for the **show processes cpu monitor** command:

```
Router> show processes cpu monitor

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs    5Sec   1Min     5Min    TTY Process
   3      772          712       1084    0.08%  0.04%    0.02%    0    Exec
  67      276         4151         66    0.08%  0.03%    0.01%    0 L2TP mgmt daemon
 116      604         2263        266    0.16%  0.05%    0.01%    0 IDMGR CORE

End = e    Freeze = f
```

Enter Command:

Enabling ISG Distributed Conditional Debugging Example

The following example shows how to filter PPP, PPPoE, and Session Manager debugs for a PPPoE session with username “user@cisco.com”. Only debugging messages for the defined user are displayed on the console. Any other debugging messages associated with other users will not be displayed.

```
Router# debug condition username user@cisco.com
Condition 1 set

Router# debug ppp negotiation
Router# debug pppoe event
Router# debug subscriber session event
```

Displaying Debugging Conditions Example

The following example shows how to display debugging conditions that have been set.

```
Router# show debug condition

Condition 1: domain cisco.com (0 flags triggered)
Condition 2: username user@cisco.com (0 flags triggered)
Condition 3: ip 172.19.200.10 (0 flags triggered)
```

Filtering Debug Output Example

In the following example, the output of the **debug subscriber packet detail** command is filtered on the basis of the username “cpe6_1@isp.com”:

```
Router# debug condition username cpe6_1@isp.com
Condition 1 set
Router# show debug

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on

Router# show debug
SSS:
  SSS packet detail debugging is on

Condition 1: username cpe6_1@isp.com (0 flags triggered)
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
Debug commands	*Cisco IOS Debug Command Reference*

Related Topic	Document Title
Conditional debugging	"Conditionally Triggered Debugging" chapter in the *Cisco IOS Debug Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Distributed Conditional Debugging

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

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

Table 29 Feature Information for ISG Session Monitoring and Distributed Conditional Debugging

Feature Name	Releases	Feature Configuration Information
ISG: Instrumentation: Session and Flow Monitoring	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG provides a mechanism for continuously monitoring interface and CPU statistics. This feature introduces the **show interface monitor** and **show processes cpu monitor**commands, which display statistics that are updated at specified intervals. In Cisco IOS Release 12.2(28)SB, this feature was introduced. This feature was integrated into Cisco IOS Release 12.2(33)SRC.
ISG: Instrumentation: Advanced Conditional Debugging	12.2(28)SB 12.2(33)SRC	ISG provides the ability to define various conditions for filtering debug output. Conditional debugging generates very specific and relevant information that can be used for session, flow, subscriber, and service diagnostics. In Cisco IOS Release 12.2(28)SB, this feature was introduced. This feature was integrated into Cisco IOS Release 12.2(33)SRC.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.