



Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 3S

First Published: 2006-03-20

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

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 NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview of ISG 1

Finding Feature Information	1
Information About ISG	1
ISG Overview	1
ISG Principles	2
Subscriber Sessions	2
Subscriber Access	3
Subscriber Identification	3
Subscriber Services	4
Policies	4
Dynamic Policy Updates	5
Benefits of ISG	5
Planning for ISG Implementation	6
Trust Model	6
Subscriber Access Model	6
Single Sign-On Requirements	6
Network Forwarding	7
Service Packaging	7
Billing Model	7
Additional References	7
Feature Information for the Overview of ISG	8

CHAPTER 2

Configuring ISG Control Policies 9

Finding Feature Information	9
Prerequisites for ISG Control Policies	9
Restrictions for ISG Control Policies	10

Information About ISG Control Policies	10
Control Policies	10
Differentiated Initial Policy Control	11
Uses of Control Policies	11
HA Support for ISG Control Policies	11
How to Configure an ISG Control Policy	12
Configuring a Control Class Map	12
Configuring a Control Policy Map	16
Applying the Control Policy Map	20
Applying a Control Policy Map Globally on the Router	20
Applying an ISG Control Policy Map to an Interface or Subinterface	21
Applying an ISG Control Policy Map to a Virtual Template	22
Monitoring and Maintaining ISG Control Policies	22
Configuration Examples for ISG Control Policies	23
Control Policy for Layer 2 Access and Service Provisioning Example	23
Verifying a Control Policy Examples	24
Control Policy for Restricting Access on the Basis of Interface and Access Media Example	26
Control Policies for Automatic Subscriber Login Example	27
Additional References	28
Feature Information for ISG Control Policies	28

CHAPTER 3

Configuring ISG Access for PPP Sessions	31
Finding Feature Information	31
Prerequisites for ISG Access for PPP Sessions	31
Restrictions for ISG Access for PPP Sessions	32
Information About ISG Access for PPP Sessions	32
Overview of ISG Access for PPP Sessions	32
ISG Subscriber IP Address Management for PPP Sessions	32
VRF Transfer for PPP Sessions	33
Default Policy for ISG Access for PPP Sessions	33
How to Configure ISG Access for PPP Sessions Using Control Policies	33
Enabling ISG VRF Transfer for PPP Sessions	34
Verifying VRF Transfer for PPP Sessions	35
Troubleshooting ISG Access for PPP Sessions	36

Configuration Examples for ISG Access for PPP Sessions	38
Configuring ISG Access for PPP Sessions Example	38
VRF Transfer for PPP Sessions Using IPCP Renegotiation Example	40
Additional References	41
Feature Information for ISG Access for PPP Sessions	41

CHAPTER 4
Configuring ISG Access for IP Subscriber Sessions 43

Finding Feature Information	43
Prerequisites for ISG Access for IP Subscriber Sessions	43
Restrictions for ISG Access for IP Subscriber Sessions	44
Information About ISG Access for IP Subscriber Sessions	46
Types of IP Subscriber Sessions	46
IP Sessions	46
IP Interface Sessions	46
IP Subnet Sessions	47
Coexistence of Multicast and IP Sessions	47
IP Subscriber Connectivity	47
Layer 2-Connected Access Networks	47
Routed Access Networks	48
IP Subscriber Session Initiation	48
IP Subscriber Addressing	49
Methods of ISG Subscriber IP Address Assignment	49
Public and Private IP Addresses	50
Overlapping IP Addresses	50
ISG Subscriber IP Address Assignment Using DHCP	50
IP Subscriber Identity	51
Routed IP Subscriber Identity	51
MAC Address as Secondary Identity	51
DHCP Lease Query Support	52
Layer 2-Connected IP Subscriber Identity	52
VPN Connectivity and Services for IP Subscribers	52
Subscriber VPN Membership	52
Multiservice Interface Model	52
VPN Addressing	53

VPN IP Subscriber Identity	54
Service Model for VRF Transfers	54
Benefits of Dynamic VPN Selection	54
IP Session Termination	54
IP Session Recovery for DHCP-Initiated IP Sessions	55
Default Services for IP Subscriber Sessions	55
How to Configure ISG for IP Subscriber Sessions	55
Creating ISG Sessions for IP Subscribers	55
Creating IP Subscriber Sessions for Routed ISG Subscribers	56
Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers	57
Creating ISG IP Interface Sessions	58
Creating ISG Static Sessions	59
Creating ISG IP Subnet Sessions	60
Configuring IP Session Recovery for DHCP-Initiated IP Sessions	62
Verifying ISG IP Subscriber Sessions	63
Clearing ISG IP Subscriber Sessions	64
Troubleshooting ISG IP Subscriber Sessions	65
Assigning ISG Subscriber IP Addresses by Using DHCP	66
Configuring an ISG Interface for Dynamic DHCP Class Association	66
Configuring DHCP Server User Authentication	67
Configuring a DHCP Class in a Service Policy Map	69
Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server	70
Configuring a DHCP Server IP Address	70
Configuring ISG Dynamic VPN Selection	71
Configuring a Multiservice Interface	71
Specifying a VRF in a Service Policy Map	72
Verifying VRF Transfer for IP Sessions	73
Troubleshooting VRF Transfer for IP Sessions	75
Configuration Examples for ISG Access for IP Subscriber Sessions	76
Example: Configuring ISG Routed IP Subscriber	76
Example: Creating ISG IP Interface Sessions	76
Example: Creating ISG Static Sessions	76
Example: Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers	76
Example: Configuring IP Session Recovery for DHCP-Initiated IP Session	77

Example: Configuring an ISG Interface for Dynamic DHCP Class Association	77
Example: Configuring DHCP Address Pool Classes and Relay Actions for ISG	77
Example: Configuring ISG Dynamic VPN Selection	79
Example: Troubleshooting DHCP Server User Authentication	79
Additional References	80
Feature Information for ISG Access for IP Subscriber Sessions	81

CHAPTER 5

Configuring ISG IPv6 Support	85
Finding Feature Information	85
Restrictions for ISG IPv6 Support	85
Information About ISG IPv6 Support	86
ISG IPv6 Session Support	86
Session Coexistence on ISG Interfaces	86
ISG Dual-Stack Features	86
ISG Protocol-Dependent Features	87
IPv6 Support for ISG Features	87
Time-Based Billing Service	88
How to Configure ISG IPv6 Support	89
Defining an IPv6 Prefix for ISG Subscriber Sessions	89
Configuring Time-Based Billing Service	90
Configuration Examples for ISG IPv6 Support	91
Example: IPv6 Prefix for ISG Subscriber Sessions	91
Example: Time-Based Billing Service	92
Additional References	94
Feature Information for ISG IPv6 Support	95

CHAPTER 6

Configuring MQC Support for IP Sessions	97
Finding Feature Information	97
Restrictions for MQC Support for IP Sessions	97
Information About MQC Support for IP Sessions	98
ISG Policers	98
Precedence Order in Policy Maps	98
How to Configure MQC Support for IP Sessions	99
Configuring Local Subscriber Profile for MQC Support	99

- Configuring ISG QoS for IP Sessions 100
- Configuration Examples for MQC Support for IP Sessions 101
 - QoS Policy-Map Service Profile and Command Policy-Map Configurations Example 101
- Additional References 101
- Feature Information for MQC Support for IP Sessions 102

CHAPTER 7

Configuring ISG Port-Bundle Host Key 103

- Finding Feature Information 103
- Prerequisites for the ISG Port-Bundle Host Key Feature 103
- Restrictions for the ISG Port-Bundle Host Key Feature 104
- Information About ISG Port-Bundle Host Key 104
 - Overview of ISG Port-Bundle Host Key 104
 - Port-Bundle Host Key Mechanism 104
 - Port-Bundle Length 105
 - Benefits of ISG Port-Bundle Host Key 106
 - Support for Overlapped Subscriber IP Addresses Extended to Include External Portal Usage 106
 - Portal Provisioning for Subscriber and ISG IP Addresses No Longer Required 106
- How to Configure ISG Port-Bundle Host Key 106
 - Enabling the ISG Port-Bundle Host Key Feature in a Service Policy Map 106
 - What to Do Next 107
 - Enabling the ISG Port-Bundle Host Key Feature in a User Profile or Service Profile on the AAA Server 107
 - What to Do Next 107
 - Configuring Port-Bundle Host Key Parameters 108
 - Verifying the ISG Port-Bundle Host Key Configuration 109
- Configuration Examples for ISG Port-Bundle Host Key 110
 - Example: Configuring ISG Port-Bundle Host Key 110
- Additional References 110
- Feature Information for ISG Port-Bundle Host Key 111

CHAPTER 8

Configuring ISG as a RADIUS Proxy 113

- Finding Feature Information 113
- Prerequisites for ISG RADIUS Proxy 113
- Restrictions for ISG RADIUS Proxy 114

Information About ISG RADIUS Proxy	114
Overview of ISG RADIUS Proxy	114
ISG RADIUS Proxy Handling of Accounting Packets	115
RADIUS Client Subnet Definition	115
ISG RADIUS Proxy Support for Mobile Wireless Environments	115
Attribute Processing and RADIUS Request Correlation	115
3GPP Attribute Support	115
Benefits of ISG RADIUS Proxy	116
How to Configure ISG as a RADIUS Proxy	116
Initiating ISG RADIUS Proxy IP Sessions	116
Configuring ISG RADIUS Proxy Global Parameters	117
Configuring ISG RADIUS Proxy Client-Specific Parameters	119
Defining an ISG Policy for RADIUS Proxy Events	121
Verifying ISG RADIUS Proxy Configuration	123
Clearing ISG RADIUS Proxy Sessions	124
Examples for Configuring ISG as a RADIUS Proxy	124
ISG RADIUS Proxy Configuration Example	124
Example: ISG RADIUS Proxy and Layer 4 Redirect	125
Additional References for Configuring ISG as a RADIUS Proxy	126
Feature Information for Configuring ISG as a RADIUS Proxy	127
<hr/>	
CHAPTER 9	Configuring ISG as a RADIUS Proxy in Passthrough Mode
	129
Finding Feature Information	129
Prerequisites for Configuring ISG as a RADIUS Proxy in Passthrough Mode	129
Restrictions for Configuring ISG as a RADIUS Proxy in Passthrough Mode	130
Information About Configuring ISG as a RADIUS Proxy in Passthrough Mode	130
ISG Acting as a RADIUS Proxy Passthrough	130
Benefits of Using ISG in RADIUS Proxy Passthrough Mode	130
How to Configure ISG as a RADIUS Proxy in Passthrough Mode	131
Enabling RADIUS Proxy Passthrough mode at Global Level	131
Enabling RADIUS Proxy Passthrough mode at Client Level	132
Verifying ISG RADIUS Proxy Passthrough Sessions	134
Clearing ISG RADIUS Proxy Statistics	135
Configuration Examples for Configuring ISG as RADIUS Proxy in Passthrough Mode	136

Example: Configuring Radius Proxy Passthrough Mode	136
Example: Verifying Radius Proxy Passthrough Mode	136
Additional References for ISG as RADIUS Proxy in Passthrough Mode	137
Feature Information for Configuring ISG as a RADIUS Proxy in Passthrough Mode	138

CHAPTER 10**ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering**
139

Finding Feature Information	139
Restrictions for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering	140
Restrictions for RADIUS Proxy Support for Hotspot Roaming	140
Restrictions for RADIUS Proxy Support for Accounting Start Filtering	140
Information About ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering	140
Hotspot Roaming Timer	140
RADIUS Packet Filter Creation	141
How to Configure ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering	141
Configuring a Roaming Timer for the ISG RADIUS Proxy Session	141
Configuring RADIUS Proxy Support for Accounting Start Filtering	142
Configuring a RADIUS Packet Filter	143
Applying RADIUS Filters to RADIUS Proxy Server or Client	144
Configuration Examples for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering	145
Example: Configuring a Roaming Timer for an ISG RADIUS Proxy Session	145
Example: Configuring a RADIUS Packet Filter	145
Example: Applying RADIUS Packet Filters to RADIUS Proxy Server	146
Additional References	146
Feature Information for ISG RADIUS Proxy Support for Mobile Users: Hotspot Roaming and Accounting Start Filtering	147

CHAPTER 11**Walk-By User Support in ISG** 149

Finding Feature Information	149
Prerequisites for Walk-By User Support for PWLANs in ISG	149
Restrictions for Walk-By User Support for PWLANs in ISG	150

Information About Walk-By User Support for PWLANs in ISG	150
Default Sessions	150
Lite Sessions or Walk-By Sessions	150
Dedicated Sessions	150
Supported Triggers	151
Session Limit	151
How to Configure Walk-By User Support for PWLANs in ISG	151
Creating and Enabling a Default Policy for a Default Session	151
Configuration Examples for Walk-By User Support for PWLANs in ISG	155
Example: Creating and Enabling a Default Policy for a Default Session	155
Additional References	156
Feature Information for Walk-By User Support for PWLANs in ISG	156

CHAPTER 12
ISG L2 Subscriber Roaming 159

Restrictions for ISG L2 Subscriber Roaming	159
Information About ISG L2 Subscriber Roaming	159
ISG Subscriber Roaming	159
ISG L2 Roaming Events	160
ISG L2 Roaming Deployments	160
Unclassified MAC (External DHCP server)	161
DHCP subscribers (DHCP relay)	161
DHCP subscribers (DHCP server)	162
Hybrid (DHCP with unclassified MAC)	163
ISG L2 Roaming Behavior	164
How to Configure ISG L2 Subscriber Roaming	166
Enabling Roaming for Simple IP Subscribers	166
Configuration Examples for ISG L2 Subscriber Roaming	166
Example: Verifying L2 Roaming on ISG	166
Additional References for ISG L2 Subscriber Roaming	167
Feature Information for ISG L2 Subscriber Roaming	168

CHAPTER 13
Configuring RADIUS-Based Policing 169

Finding Feature Information	169
Prerequisites for RADIUS-Based Policing	169

Restrictions for RADIUS-Based Policing	169
Information About RADIUS-Based Policing	170
RADIUS Attributes	170
RADIUS Attributes 250 and 252	170
Cisco VSA 1	171
Parameterized QoS Policy as VSA 1	173
Parameterization of QoS ACLs	173
HA Support for RADIUS-Based Policing	173
How to Configure RADIUS-Based Policing	174
Configuring per-Session Shaping	174
Configuring a QoS Policy with Shaping on ISG	174
Configuring per-Session Shaping on RADIUS	175
Configuring per-Service Shaping and Policing	175
Configuring a Hierarchical QoS Child Policy with Shaping and Policing on ISG	175
Configuring a Hierarchical QoS Parent Policy with Shaping and Policing on ISG	176
Configuring per-Service Shaping and Policing on RADIUS	177
Verifying RADIUS-Based Policing	178
Configuration Examples for RADIUS-Based Policing	179
Example: Adding Parameterization of QoS ACLs	179
Example: Setting the Shaping Rate Using an Access-Accept Message	181
Example: Setting the Shaping Rate Using a CoA Message	182
Example: Setting the Policing Rate Using an Access-Accept Message	183
Example: Setting the Policing Rate Using a CoA Message	184
Additional References	186
Feature Information for RADIUS-Based Policing	186

CHAPTER 14
ISG Dynamic VLAN Interface Provisioning 189

Finding Feature Information	189
Prerequisites for ISG Dynamic VLAN Interface Provisioning	189
Restrictions for ISG Dynamic VLAN Interface Provisioning	190
Information About ISG Dynamic VLAN Interface Provisioning	190
Overview of ISG Dynamic VLAN Interface Provisioning	190
Benefits of ISG Dynamic VLAN Provisioning	191
IOS Shell Maps and Usage	191

Configuration Examples for ISG Dynamic VLAN Interface Provisioning	192
Example: Configuring ISG Dynamic VLAN Interface Provisioning	192
Example: Configuring RSIM	195
Additional References for ISG Dynamic VLAN Interface Provisioning	196
Feature Information for ISG Dynamic VLAN Interface Provisioning	196

CHAPTER 15**Ambiguous VLAN Support for IP sessions over ISG 197**

Finding Feature Information	197
Restrictions for Ambiguous VLAN Support for IP Sessions over ISG	197
Information About Configuring Ambiguous VLAN Support for IP Sessions over ISG	198
Benefits of Ambiguous VLAN Support for IP Sessions over ISG	198
Configuring Ambiguous VLAN Support for IP Sessions over ISG	198
Verifying Ambiguous VLAN Support for IP Sessions over ISG Configuration	199
Additional References for Ambiguous VLAN Support for IP Sessions over ISG	199
Feature Information for Ambiguous VLAN Support for IP Sessions over ISG	200

CHAPTER 16**Configuring ISG Policies for Automatic Subscriber Logon 201**

Finding Feature Information	201
Prerequisites for ISG Automatic Subscriber Logon	201
Restrictions for ISG Automatic Subscriber Logon	202
Information About ISG Automatic Subscriber Logon	202
Overview of ISG Automatic Subscriber Logon	202
Supported Identifiers for ISG Automatic Subscriber Logon	202
Authorization Based on Circuit ID and Remote ID	202
Accounting Behavior When ISG Automatic Subscriber Logon Is Configured	203
How to Configure ISG Policies for Automatic Subscriber Logon	203
Identifying Traffic for Automatic Logon in a Control Policy Class Map	203
Configuring an ISG Control Policy for Automatic Subscriber Logon	204
What to Do Next	206
Enabling the Remote-ID to Be Sent as the Calling-Station-ID	206
Verifying ISG Automatic Subscriber Logon	206
Configuration Examples for ISG Automatic Subscriber Logon	208
Automatic Subscriber Logon Based on IP Address Example	208
Additional References	209

Feature Information for ISG Automatic Subscriber Logon 210

CHAPTER 17

Configuring DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 211

Finding Feature Information 211

Prerequisites for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 212

Restrictions for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 212

Information About DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 212

ISA Automatic Subscriber Logon 212

Authorization Based on Option 60 and Option 82 212

DHCP Option 82 with VPN-ID Suboption 213

How to Configure DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 213

Configuring an ISG Control Policy Using Option 60 and Option 82 213

Configuring an ISG Control Policy Using NAS-Port-ID 214

Configuring NAS-Port-ID to Include Option 60 and Option 82 215

Configuration Examples for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 216

Example Option 60 and Option 82 in NAS-Port-ID 216

Additional References 217

Feature Information for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 218

CHAPTER 18

Enabling ISG to Interact with External Policy Servers 219

Finding Feature Information 219

Restrictions for ISG Interaction with External Policy Servers 219

Information About ISG Interaction with External Policy Servers 220

Initial and Dynamic Authorization 220

Triple Key Authentication for ISG 220

How to Enable ISG to Interact with External Policy Servers 221

Configuring ISG as a AAA Client 221

Configuring ISG as a AAA Server 222

Enabling the Location VSA for Triple Key Authentication	224
Configuration Examples for ISG Interaction with External Policy Servers	225
Example: Enabling ISG to Interact with External Policy Servers	225
Example: Enabling the Location VSA for Triple Key Authentication	225
Additional References	226
Feature Information for ISG Interaction with External Policy Servers	227

CHAPTER 19

Configuring ISG Subscriber Services	229
Finding Feature Information	229
Restrictions for ISG Subscriber Services	229
Information About ISG Subscriber Services	230
ISG Services	230
Primary Services	230
Traffic Classes and Traffic Class Priority	231
Flow Classifiers	231
Traffic Policies	232
ISG Features	232
Service Groups	232
Service Activation Methods	233
How to Configure ISG Services on the Router	233
Configuring an ISG Service with Per-Session Functionality	234
Configuring an ISG Service with a Traffic Policy	236
Defining an ISG Traffic Class Map	236
Configuring an ISG Service Policy Map with a Traffic Policy	237
Configuring the Default Class in an ISG Service Policy Map	239
Activating ISG Subscriber Services	240
Configuring Automatic Service Activation in a User Profile	240
Configuring ISG Control Policies to Activate Services	241
Verifying ISG Services	242
Configuration Examples for ISG Services	243
Example Service for Per-Flow Accounting	243
Example Service for Absolute Timeout and Idle Timeout	243
Example Service for ISG Policing	244
Example Service for Per-Subscriber Firewall	244

Example Service for Redirecting Layer 4 Subscriber Traffic 245

Example Deactivating a Layer 4 Redirection Service Following Authorization 245

Additional References 245

Feature Information for ISG Subscriber Services 246

CHAPTER 20

Configuring ISG Network Forwarding Policies 249

Finding Feature Information 249

Restrictions for ISG Network Forwarding Policies 249

Information About ISG Network Policies 250

 Network Policies 250

 Configuration Sources for Network Policies 250

How to Configure ISG Network Policies 251

 Configuring Network Policies for PPP Sessions in Service Policy Maps 251

 What to Do Next 252

 Configuring Network Policies for IP Sessions in Service Policy Maps 252

 What to Do Next 253

Configuration Examples for ISG Network Policies 254

 Network Forwarding Policy for PPP Sessions Example 254

 Network Forwarding Policy for IP Sessions Example 254

Additional References 254

Feature Information for ISG Network Policies 255

CHAPTER 21

Configuring ISG Accounting 257

Finding Feature Information 257

Prerequisites for ISG Accounting 257

Restrictions for ISG Accounting 258

Information About ISG Accounting 258

 Overview of ISG Accounting 258

 ISG Accounting Messages on ANCP Ports 258

 Service Activation and Deactivation Configuration on RADIUS 259

ISG Accounting Records 259

Interim ISG Accounting Updates 260

Broadcast Accounting 260

ISG Postpaid Tariff Switching 260

Subscriber Accounting Accuracy	261
HA Support for ISG Accounting	261
How to Configure ISG Accounting	262
Enabling ISG per-Session Accounting	262
Enabling ISG per-Session Accounting in a User Profile on a AAA Server	262
Enabling a per-User Accounting List	262
Enabling ISG per-Flow Accounting	263
Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server	263
Enabling ISG per-Flow Accounting in a Service Policy Map	264
Enabling ISG per-Service Accounting	265
Enabling per-Service Accounting on ISG	265
Enabling per-Service Accounting in a Service Profile on a AAA Server	266
Enabling per-Service Accounting in a Service Policy Map	267
Configuring ISG Postpaid Tariff Switching	268
What to Do Next	269
Verifying ISG Accounting and Postpaid Tariff Switching	269
Enabling Periodic Session Update	270
Verifying Periodic Session Update	271
Troubleshooting ISG Accounting	271
Configuration Examples for ISG Accounting	272
Example: Enabling ISG per-Flow Accounting	272
Example: Enabling ISG per-Service Accounting	273
Example: Enabling a per-User Accounting List	273
Example: Enabling ISG per-Service Accounting in a Service Policy Map	273
Example: Configuring Postpaid Tariff Switching	273
Example: Enabling Periodic Session Update	274
Examples: Verifying ISG Accounting and Postpaid Tariff Switching	274
Example: Troubleshooting ISG Accounting	278
Additional References	279
Feature Information for ISG Accounting	279
CHAPTER 22	Configuring ISG Support for Prepaid Billing
	281
Finding Feature Information	281
Prerequisites for ISG Prepaid Billing Support	281

- Restrictions for ISG Prepaid Billing Support 282
- Information About ISG Prepaid Billing Support 282
 - Overview of ISG Support for Prepaid Billing 282
 - ISG Prepaid Volume Monitor Polling Timer and QV Values 282
 - ISG Prepaid Threshold 283
 - ISG Prepaid Idle Timeout 283
 - Benefits of ISG Prepaid Billing 283
- How to Configure ISG Support for Prepaid Billing 284
 - Configuring RADIUS Attribute Support for ISG Prepaid Billing 284
 - Creating an ISG Prepaid Billing Configuration 285
 - Enabling ISG Prepaid Billing 287
 - Enabling ISG Prepaid Billing in a Service Policy Map 287
 - Enabling ISG Prepaid Billing in Service Profile on the AAA Server 289
 - Redirecting Subscriber Traffic upon Exhaustion of Credit 289
 - Credit-Exhausted Event 290
 - Configuring L4 Redirection in a Service Policy Map 290
 - Applying a Service Policy Map to Subscriber Traffic upon Exhaustion of Credit 291
 - What to Do Next 293
 - Forwarding Subscriber Traffic upon Depletion of Quota 293
 - Quota-Depleted Event 293
 - What to Do Next 294
 - Troubleshooting ISG Prepaid Billing Support 295
- Configuration Examples for ISG Prepaid Billing Support 295
 - ISG Prepaid Billing Support Example 295
 - ISG Policies for Handling Credit-Exhausted and Quota-Depleted Prepaid Billing Events Example 296
 - Example: Configuring Prepaid Support for Simple IP Dual Stack Sessions 297
- Additional References 299
- Feature Information for ISG Support for Prepaid Billing 300

CHAPTER 23

- Configuring ISG Policies for Session Maintenance 303**
 - Finding Feature Information 303
 - Prerequisites for ISG Policies for Session Maintenance 304
 - Information About ISG Policies for Session Maintenance 304

Session Maintenance Timers	304
Benefits of Session Maintenance Timers	304
Monitoring Sessions	304
ARP for Keepalive Messages	305
ICMP for Keepalive Messages	305
HA Support for Session Maintenance Timers	305
How to Configure ISG Policies for Session Maintenance	306
Configuring the Session Timer in a Service Policy Map	306
What to Do Next	307
Configuring the Session Timer on a AAA Server	307
Configuring the Connection Timer in a Service Policy Map	307
What to Do Next	308
Configuring the Connection Timer on a AAA Server	308
Verifying the Session and Connection Timer Settings	309
Troubleshooting the Session and Connection Timer Settings	310
Prerequisites for Troubleshooting the Session Maintenance Timers	310
Restrictions for Troubleshooting the Session Maintenance Timers	310
Debug Commands Available for the Session Maintenance Timers	310
Configuring a Session Keepalive on the Router	310
Configuring a Session Keepalive on a RADIUS Server	312
Configuring the ISG to Interact with the RADIUS Server	313
Configuration Examples for ISG Policies for Session Maintenance	314
Example: Session Timer Configuration in a Service Policy Map	314
Example: Connection Idle Timer Configuration in a Service Policy Map	314
Example: Session Timer Show Command Output	315
Example: Connection Idle Timer Show Command Output	315
Example: Session Timer Debug Output	316
Example: Connection Idle Timer Debug Output	316
Additional References	317
Feature Information for ISG Policies for Session Maintenance	317
<hr/>	
CHAPTER 24	Redirecting Subscriber Traffic Using ISG Layer 4 Redirect 319
	Finding Feature Information 319
	Restrictions for Redirecting ISG Subscriber Traffic 319

Information About Redirecting ISG Subscriber Traffic	320
Overview of ISG Layer 4 Redirect	320
Layer 4 Redirect Applications	320
HA Support for Layer 4 Redirect	321
How to Configure ISG Layer 4 Redirect	321
Defining a Redirect Server Group	321
Configuring Layer 4 Redirection in a Service Policy Map	322
What to Do Next	323
Configuring Layer 4 Redirection in a Service Profile or User Profile on the AAA Server	323
What to Do Next	324
Verifying ISG Traffic Redirection	324
Configuration Examples for ISG Layer 4 Redirect	326
Example: Redirecting Unauthenticated Subscriber Traffic	326
Example: Redirecting Unauthorized Subscriber Traffic	327
Example: Initial ISG Redirection	327
Example: Periodic ISG Redirection	328
Example: Redirecting DNS Traffic	328
Additional References	328
Feature Information for Redirecting ISG Subscriber Traffic	329

CHAPTER 25

Configuring Layer 4 Redirect Logging	331
Finding Feature Information	331
Prerequisites for Layer 4 Redirect Logging	331
Information About Layer 4 Redirect Logging	332
ISG Layer 4 Redirect Logging	332
Template Formats for Layer 4 Redirect Logging	332
How to Configure Layer 4 Redirect Logging	334
Enabling ISG Layer 4 Redirect Logging	334
Configuration Examples for Layer 4 Redirect Logging	336
Example: Enabling Layer 4 Redirect Logging	336
Example: Layer 4 Redirect Logging Events	336
Additional References	336
Feature Information for Layer 4 Redirect Logging	337

CHAPTER 26	Configuring ISG Policies for Regulating Network Access	339
	Finding Feature Information	339
	Information About ISG Policies for Regulating Network Access	339
	Methods of Regulating Network Access	339
	Overview of ISG Policing	340
	How to Configure ISG Policies for Regulating Network Access	341
	Configuring ISG Policing	341
	Configuring Policing in a Service Policy Map on the Router	341
	Configuring Policing in a Service Profile or User Profile on the AAA Server	342
	Verifying ISG Policing	343
	Configuration Examples for ISG Policies for Regulating Network Access	344
	ISG Policing Examples	344
	Additional References	345
	Feature Information for ISG Policies for Regulating Network Access	345

CHAPTER 27	Configuring ISG Integration with SCE	347
	Finding Feature Information	347
	Prerequisites for Configuring ISG Integration with SCE	347
	Hardware Requirements	347
	Software Requirements	348
	Restrictions for Configuring ISG Integration with SCE	348
	Information About Configuring ISG Integration with SCE	349
	Overview of ISG-SCE Integration	349
	ISG and SCE Roles in Subscriber Management	349
	How to Configure ISG Integration with SCE	350
	Configuring Communication Between SCE and ISG	350
	Configuring SCE Connection Parameter on ISG	351
	Configuring Control Policy on the Policy Manager	352
	Configuring Control Policy on the ISG	353
	Configuring Auto Service on the AAA Server	354
	Configuring Services	354
	Configuring Services on ISG	354
	Configuring Services on the AAA Server	356

- Troubleshooting Tips 356
- Examples 356
- Configuration Examples for ISG Integration with SCE 357
 - ISG Control Bus Configuration Example 357
 - ISG Integration with SCE Example 358
 - SCE Control Bus Configuration Examples 358
- Additional References 359
- Feature Information for Configuring ISG Integration with SCE 359

CHAPTER 28

- Service Gateway Interface 361**
 - Finding Feature Information 361
 - Information About Service Gateway Interface 361
 - ISG 361
 - BEEP 362
 - Benefits of SGI 362
 - How to Enable Service Gateway Interface 362
 - Configuring BEEP Listener Connection 362
 - Troubleshooting SGI 363
 - Configuration Examples for Service Gateway Interface 364
 - Configuring BEEP Listener Connection Example 364
 - Additional References 365
 - Feature Information for Service Gateway Interface 366

CHAPTER 29

- ISG MIB 367**
 - Information About ISG MIB 367
 - ISG MIB Overview 367
 - Subscriber Session MIB 367
 - Dynamic Template MIB 368
 - Additional References 368
 - Feature Information for ISG MIB 369

CHAPTER 30

- ISG SSO and ISSU 371**
 - Finding Feature Information 371
 - Prerequisites for ISG SSO and ISSU 371

Information About ISG SSO and ISSU	371
High Availability for ISG Features	371
Additional References	372
Feature Information for ISG SSO and ISSU	373

CHAPTER 31**ISG Debuggability 375**

Restrictions for ISG Debuggability	375
Information About ISG Debuggability	375
ISG Debugging Behavior	375
Additional References for ISG Debuggability	376
Feature Information for ISG Debuggability	376

CHAPTER 32**Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging 377**

Finding Feature Information	377
Prerequisites for ISG Session Monitoring and Distributed Conditional Debugging	377
Restrictions for Distributed Conditional Debugging	378
Information About ISG Session Monitoring and Distributed Conditional Debugging	378
ISG Session and Flow Monitoring	378
ISG Distributed Conditional Debugging	378
Benefits of Enhanced Conditional Debugging for the ISG Platforms	378
Cisco IOS XE Software Components Supported by Distributed Conditional Debugging	378
How to Enable ISG Session Monitoring and Distributed Conditional Debugging	379
Monitoring ISG Sessions and Flows	379
Configuring Distributed Conditional Debugging	379
ISG Debug Condition Commands	380
Debug Commands That Are Supported by ISG Conditional Debug	380
Restrictions	383
Enabling Distributed Conditional Debugging	383
Displaying Debugging Conditions	384
Troubleshooting Tips	384
Configuration Examples for ISG Distributed Conditional Debugging	385
Monitoring Interface Statistics Example	385
Monitoring CPU Statistics Example	385
Enabling ISG Distributed Conditional Debugging Example	385

Displaying Debugging Conditions Example	386
Filtering Debug Output Example	386
Additional References	386
Feature Information for Distributed Conditional Debugging	387

CHAPTER 33

Configuring ISG Troubleshooting Enhancements	389
Information About ISG Troubleshooting Enhancements	389
Event Tracing for Subscriber Sessions	389
Dumping Event Traces	390
How to Enable ISG Troubleshooting Enhancements	390
Enabling Event Tracing for ISG Sessions	390
Displaying Event Traces for ISG Sessions	391
Additional References	392
Feature Information for ISG Troubleshooting Enhancements	393



CHAPTER 1

Overview of ISG

Intelligent Services Gateway (ISG) is a Cisco 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, on page 1](#)
- [Information About ISG, on page 1](#)
- [Additional References, on page 7](#)
- [Feature Information for the Overview of ISG, on page 8](#)

Finding Feature Information

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

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

ISG Overview

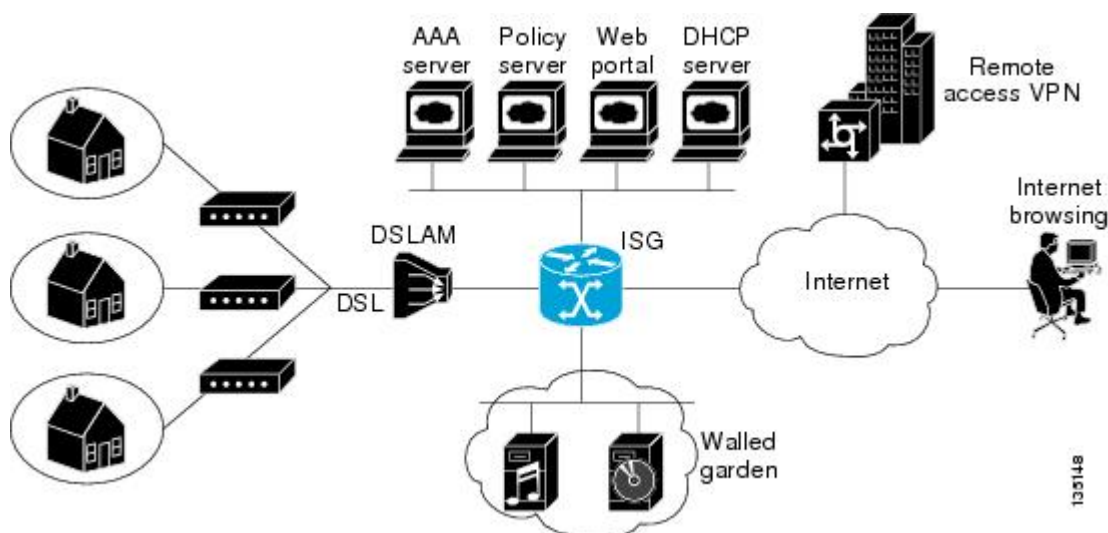
Intelligent Services Gateway (ISG) is a structured framework in which edge access devices deliver flexible and scalable services to subscribers. ISG handles the following key aspects of subscriber management:

- 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 network. 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: Sample Topology for a DSL Deployment



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.



Note The IP Base license does not support ISG/PPP/VPDN subscriber features. The minimum feature set for Subscriber support is ADV IP Services or ADV Enterprise Services.

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

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 policies 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

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

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.



CHAPTER 2

Configuring ISG Control Policies

Intelligent Services Gateway (ISG) is a Cisco 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, on page 9](#)
- [Prerequisites for ISG Control Policies, on page 9](#)
- [Restrictions for ISG Control Policies, on page 10](#)
- [Information About ISG Control Policies, on page 10](#)
- [How to Configure an ISG Control Policy, on page 12](#)
- [Configuration Examples for ISG Control Policies, on page 23](#)
- [Additional References, on page 28](#)
- [Feature Information for ISG Control Policies, on page 28](#)

Finding Feature Information

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

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

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.
2. 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.
3. 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

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

HA Support for ISG Control Policies

The ISG Policy HA and RADIUS-Based Policing HA feature adds stateful switchover (SSO) and In Service Software Upgrade (ISSU) support to ISG control policies.

For information about configuring high availability (HA) on the ISG router, see the [High Availability Configuration Guide, Cisco IOS XE Release 3S](#).

How to Configure an ISG Control Policy

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map type control [match-all match-any match-none] class-map-name Example: <pre>Router(config)# class-map type control match-all class1</pre>	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: <pre>Router(config-control-classmap)# available nas-port</pre>	(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: <pre>Router(config-control-classmap)# greater-than nas-port type atm vpi 200 vci 100</pre>	(Optional) Creates a condition that evaluates true if the subscriber network access server (NAS) port identifier is greater than the specified value.
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:	(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is greater than or equal to the specified value.

	Command or Action	Purpose
	Router(config-control-classmap)# greater-than-or-equal nas-port vlan 10	
Step 7	<p>less-than [not] nas-port {adapter <i>adapter-number</i> channel <i>channel-number</i> ipaddr <i>ip-address</i> port <i>port-number</i> shelf <i>shelf-number</i> slot <i>slot-number</i> sub-interface <i>sub-interface-number</i> type <i>interface-type</i> vci <i>vci-number</i> vlan <i>vlan-id</i> vpi <i>vpi-number</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# less-than nas-port type atm vpi 200 vci 105</pre>	(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than the specified value.
Step 8	<p>less-than-or-equal [not] nas-port {adapter <i>adapter-number</i> channel <i>channel-number</i> ipaddr <i>ip-address</i> port <i>port-number</i> shelf <i>shelf-number</i> slot <i>slot-number</i> sub-interface <i>sub-interface-number</i> type <i>interface-type</i> vci <i>vci-number</i> vlan <i>vlan-id</i> vpi <i>vpi-number</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# less-than-or-equal nas-port ipaddr 10.10.10.10</pre>	(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	<p>match authen-status {authenticated unauthenticated}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match authen-status authenticated</pre>	(Optional) Creates a condition that evaluates true if a subscriber's authentication status matches the specified authentication status.
Step 10	<p>match authenticated-domain {<i>domain-name</i> regex <i>regular-expression</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match authenticated-domain cisco.com</pre>	(Optional) Creates a condition that evaluates true if a subscriber's authenticated domain matches the specified domain.
Step 11	<p>match authenticated-username {<i>username</i> regex <i>regular-expression</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match authenticated-username regex "admin@.*com"</pre>	(Optional) Creates a condition that evaluates true if a subscriber's authenticated username matches the specified username.
Step 12	<p>match dnis {<i>dnis</i> regex <i>regular-expression</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match dnis reg-exp 5551212</pre>	(Optional) Creates a condition that evaluates true if a subscriber's Dialed Number Identification Service number (DNIS number, also referred to as <i>called-party number</i>) matches the specified DNIS number.

	Command or Action	Purpose
Step 13	<p>match media {<i>async</i> <i>atm</i> <i>ether</i> <i>ip</i> <i>isdn</i> <i>mpls</i> <i>serial</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match media atm</pre>	(Optional) Creates a condition that evaluates true if a subscriber's access media type matches the specified media type.
Step 14	<p>match mlp-negotiated {<i>no</i> <i>yes</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match mlp-negotiated yes</pre>	<p>(Optional) Creates a condition that evaluates true or false depending on whether the subscriber's session was established using multilink PPP negotiation.</p> <ul style="list-style-type: none"> If the yes keyword is used, the condition evaluates true if the subscriber's session was established using multilink PPP negotiation.
Step 15	<p>match nas-port {<i>adapter adapter-number</i> <i>channel channel-number</i> <i>circuit-id name</i> <i>ipaddr ip-address</i> <i>port port-number</i> <i>remote-id name</i> <i>shelf shelf-number</i> <i>slot slot-number</i> <i>sub-interface sub-interface-number</i> type {<i>async</i> <i>atm</i> <i>basic-rate</i> <i>enm</i> <i>ether</i> <i>fxo</i> <i>fxs</i> <i>none</i> <i>primary-rate</i> <i>synch</i> <i>vlan</i> <i>vty</i>} <i>vci vci-number</i> <i>vlan vlan-id</i> <i>vpi vpi-number</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match nas-port type ether slot 3</pre>	(Optional) Creates a condition that evaluates true if a subscriber's NAS port identifier matches the specified value.
Step 16	<p>match no-username {<i>no</i> <i>yes</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match no-username yes</pre>	<p>(Optional) Creates a condition that evaluates true or false depending on whether or not a subscriber's username is available.</p> <ul style="list-style-type: none"> If the yes keyword is used, the condition evaluates true if the subscriber's username is not available.
Step 17	<p>match protocol {<i>atom</i> <i>ip</i> <i>pdsn</i> <i>ppp</i> <i>vpdn</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match protocol ip</pre>	(Optional) Creates a condition that evaluates true if a subscriber's access protocol type matches the specified protocol type.
Step 18	<p>match service-name {<i>service-name</i> regex <i>regular-expression</i>}</p> <p>Example:</p> <pre>Router(config-control-classmap)# match service-name service1</pre>	(Optional) Creates a condition that evaluates true if the service name associated with a subscriber matches the specified service name.

	Command or Action	Purpose
Step 19	match source-ip-address <i>ip-address subnet-mask</i> Example: <pre>Router(config-control-classmap)# match source-ip-address 10.10.10.10 255.255.255.255</pre>	(Optional) Creates a condition that evaluates true if a subscriber's source IP address matches the specified IP address.
Step 20	match timer <i>{timer-name regexp regular-expression}</i> Example: <pre>Router(config-control-classmap)# match timer TIMER_A</pre>	(Optional) Creates a condition that evaluates true upon expiry of a specified policy timer.
Step 21	match tunnel-name <i>{tunnel-name regexp regular-expression}</i> Example: <pre>Router(config-control-classmap)# match tunnel-name regexp L.*</pre>	(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 <i>{domain-name regexp regular-expression}</i> Example: <pre>Router(config-control-classmap)# match unauthenticated-domain example.com</pre>	(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated domain name matches the specified domain name.
Step 23	match unauthenticated-username <i>{username regexp regular-expression}</i> Example: <pre>Router(config-control-classmap)# match unauthenticated-username regexp examplename1</pre>	(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated username matches the specified username.
Step 24	match vrf <i>{vrf-name regexp regular-expression}</i> Example: <pre>Router(config-control-classmap)# match vrf regexp examplename2</pre>	(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** | **flow-timeout** | **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**|**srg**|**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:	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> 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 { <i>control-class-name</i> always } [event { access-reject account-logoff account-logon acct-notification credit-exhausted dummy-event flow-timeout 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. <ul style="list-style-type: none"> 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	<i>action-number</i> authenticate aaa list <i>list-name</i> Example: Router(config-control-policymap-class-control)# 1 authenticate aaa list LIST1	(Optional) Initiates an authentication request.
Step 6	<i>action-number</i> authorize use method { aaa legacy rm sgf ssg xconnect } [aaa parameter-name] [password <i>password</i>] [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.
Step 7	<i>action-number</i> collect [aaa list <i>list-name</i>] 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	(Optional) Collects the specified subscriber identifier from the access protocol.

	Command or Action	Purpose
	<p>Command: <code>unauthenticated-domain unauthenticated-username vrf}</code></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# 1 collect identifier authen-status</pre>	
Step 8	<p>Command: <code>action-number if upon network-service-found {continue stop}</code></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# 2 if upon network-service-found stop</pre>	(Optional) Specifies whether the system should continue processing policy rules once the subscriber's network service has been identified.
Step 9	<p>Command: <code>action-number proxy accounting aaa list {list-name default}</code></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# 1 proxy accounting aaa list default</pre>	(Optional) Specifies the list that the request should be proxied to.
Step 10	<p>Command: <code>action-number service [disconnect local vpdn]</code></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# 3 service disconnect</pre>	(Optional) Specifies a network service type for PPP sessions.
Step 11	<p>Command: <code>action-number service-policy type control policy-map-name</code></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# service-policy type control domain based access</pre>	(Optional) Nests the specified control policy map within a parent control policy map.
Step 12	<p>Command: <code>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}}</code></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT</pre>	<p>(Optional) Activates an ISG service.</p> <ul style="list-style-type: none"> Specifying an identifier instead of a service name will activate a service that has the same name as the specified identifier.
Step 13	<p>Command: <code>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 </code></p>	(Optional) Sets a variable name.

	Command or Action	Purpose
	unauthenticated-domain unauthenticated-username vrf} Example: <pre>Router(config-control-policy-map-class-control)# 1 set APJ identifier authen-status</pre>	
Step 14	<i>action-number</i> set-timer <i>name-of-timer</i> <i>minutes</i> Example: <pre>Router(config-control-policy-map-class-control)# 1 set-timer TIMERA 5</pre>	(Optional) Starts a named policy timer. <ul style="list-style-type: none"> Expiration of the timer generates the event <code>timed-policy-expiry</code>.
Step 15	<i>action-number</i> substitute <i>name</i> <i>matching-pattern</i> <i>pattern-string</i> Example: <pre>Router(config-control-policy-map-class-control)# 1 substitute TPK SUBA SUBB</pre>	(Optional) Substitutes a matching pattern in variable content by a rewrite pattern.
Step 16	end Example: <pre>Router(config-control-policy-map-class-control)# end</pre>	(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

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:	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	service-policy type control <i>policy-map-name</i> 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. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>.subinterface-number</i>] Example: Router(config)# interface gigabitethernet 0/0/1.1	Specifies an interface and enters interface configuration mode.
Step 4	service-policy type control <i>policy-map-name</i> 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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface virtual-template <i>number</i> Example: <pre>Router(config)# interface virtual-template0</pre>	Creates a virtual template interface and enters interface configuration mode.
Step 4	service-policy type control <i>policy-map-name</i> Example: <pre>Router(config-if)# service-policy type control policy1</pre>	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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show class-map type control Example: <pre>Router# show class-map type control</pre>	Displays information about ISG control class maps. <ul style="list-style-type: none"> • 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: <pre>Router# show policy-map type control</pre>	Displays information about ISG control policy maps. <ul style="list-style-type: none"> • 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: <pre>Router# clear class-map control</pre>	Clears the control class map counters.
Step 5	clear policy-map control Example: <pre>Router# clear policy-map control</pre>	Clears the control policy map counters.

Configuration Examples for ISG Control Policies

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-Templatel, 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-Templatel, 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
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
HA commands	Cisco IOS High Availability Command Reference
HA configuration	<i>High Availability Configuration Guide</i>
Traffic Policies	"Configuring ISG Subscriber Services" module in this guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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.
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 feature 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 .

Feature Name	Releases	Feature Configuration Information
ISG Policy HA and RADIUS-Based Policing HA	Cisco IOS XE Release 3.5S	Adds SSO and ISSU support to the ISG policy manager.



CHAPTER 3

Configuring ISG Access for PPP Sessions

Intelligent Services Gateway (ISG) is a 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, on page 31](#)
- [Prerequisites for ISG Access for PPP Sessions, on page 31](#)
- [Restrictions for ISG Access for PPP Sessions, on page 32](#)
- [Information About ISG Access for PPP Sessions, on page 32](#)
- [How to Configure ISG Access for PPP Sessions Using Control Policies, on page 33](#)
- [Configuration Examples for ISG Access for PPP Sessions, on page 38](#)
- [Additional References, on page 41](#)
- [Feature Information for ISG Access for PPP Sessions, on page 41](#)

Finding Feature Information

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

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

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

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

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.

Before you begin

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 *Dial 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> 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 <i>name-of-vrf</i> Example: Router(config-service-policymap)# ip vrf forwarding blue	Associates the service with a VRF.
Step 5	sg-service-type primary	Defines the service as a primary service.

	Command or Action	Purpose
	Example: <pre>Router(config-service-policy) # sg-service-type primary</pre>	<ul style="list-style-type: none"> 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 <i>service-group-name</i> Example: <pre>Router(config-service-policy) # sg-service-group group1</pre>	(Optional) Associates an ISG service with a service group. <ul style="list-style-type: none"> 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

- enable**
- show subscriber session all**
- 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**}
- show ip route** [*vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show subscriber session all Example: <pre>Router# show subscriber session all</pre>	Displays information pertaining to the service chosen by the subscriber.
Step 3	show idmgr { memory [detailed [component [<i>substring</i>]]] service key session-handle <i>session-handle-string</i> service-key <i>key-value</i> session key { aaa-unique-id <i>aaa-unique-id-string</i> domainip-vrf <i>ip-address ip-address</i>	Displays information related to ISG session and service identity.

	Command or Action	Purpose
	vrf-id <i>vrf-id</i> nativeip-vrf ip-address <i>ip-address</i> vrf-id <i>vrf-id</i> portbundle ip <i>ip-address</i> bundle <i>bundle-number</i> session-guid <i>session-guid</i> session-handle <i>session-handle-string</i> session-id <i>session-id-string</i> } statistics } Example: <pre>Router# show idmgr session key session-handle 48000002</pre>	
Step 4	show ip route [<i>vrf vrf-name</i>] Example: <pre>Router# show ip route</pre>	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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show subscriber session detailed Example: <pre>Router# show subscriber session detailed</pre>	Displays information about ISG subscriber sessions.
Step 3	debug condition <i>condition</i> Example:	Filters debug output on the basis of the specified condition.

	Command or Action	Purpose
	Router# debug condition username user5@isp.com	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.
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)
```

Configuration Examples for ISG Access for PPP Sessions

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 <i>Security Configuration Guide</i>
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" section in the <i>Security Command Reference</i>
PPP configuration tasks	The "PPP Configuration" section in the <i>Dial Services Configuration Guide</i>
PPP commands	<i>Dial Services Command Reference</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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.



CHAPTER 4

Configuring ISG Access for IP Subscriber Sessions

Intelligent Services Gateway (ISG) 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 VPN selection.



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

- [Finding Feature Information, on page 43](#)
- [Prerequisites for ISG Access for IP Subscriber Sessions, on page 43](#)
- [Restrictions for ISG Access for IP Subscriber Sessions, on page 44](#)
- [Information About ISG Access for IP Subscriber Sessions, on page 46](#)
- [How to Configure ISG for IP Subscriber Sessions, on page 55](#)
- [Configuration Examples for ISG Access for IP Subscriber Sessions, on page 76](#)
- [Additional References, on page 80](#)
- [Feature Information for ISG Access for IP Subscriber Sessions, on page 81](#)

Finding Feature Information

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

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 DHCP server must support the DHCP lease protocol.

- For ISG to use DHCP to assign IP addresses, the following conditions must be met:
 - The subscriber must be Layer 2-connected.
 - ISG must be in the path of DHCP requests, serving as a DHCP server or relay.
 - Appropriate IP subnets must be configured on the subscriber interface.

Restrictions for ISG Access for IP Subscriber Sessions

IPv6 Session Restrictions

- Layer 2 connected interfaces are not supported. Only Layer 3-routed inband IPv6 sessions are supported.
- Out-of-band IPv6 sessions are not supported.
- DHCP-initiated or RADIUS proxy-initiated sessions are not supported for IPv6 sessions.
- Dual-stack sessions are not supported. A native IP session can have either an IPv4 or IPv6 address, not both.

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 on the same interface are not supported for static and routed IP subscriber sessions. In contrast, overlapping IP subscribers in different VRFs on the same interface are supported 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 an ISG device and subscriber devices.

Dynamic VPN Selection Restrictions

- Dynamic VPN selection is not supported for IP interface sessions, IP subnet sessions, and subscribers connecting 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. The IP addresses of routed IP subscribers must be routable in the access network. Because ISP- or VRF-owned private addresses could overlap or be unroutable in the network between subscribers and an ISG device, IP addresses cannot be addressed to subscribers in such networks.

- 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 vendor-specific attributes (VSA) is not supported; only static VRF is supported.
- Traffic from locally imported VRF routes is not supported for subscribers. From subscriber side, VRF transfer works fine.

General IP Session Restrictions

- Virtual Fragment Reassembly (VFR) configuration is not supported on the virtual-template interface.
- IP subscriber sessions are not supported on ambiguous IEEE 802.1QinQ 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 queueing 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:
 - Layer 2 Tunnel Protocol (L2TP)
 - PPP (virtual template)
- Interface statistics are not generated for ISG multiservice interfaces.
- Stateful switchover (SSO) and In Service Software Upgrade (ISSU) are not supported for DHCP IP sessions (where ISG serves as a relay or server). Upon switchover, a DHCP IP session must be restarted when the session becomes active again.
- The following subscriber features are not supported for Internet Protocol over Ethernet (IPoE) sessions:
 - Per-session firewall
 - Per-session NAT
 - Per-session netflow
 - Per-session network-based application recognition (NBAR)
 - Per-session multicast
 - Per-session policy-based routing (PBR)
- The following PPP session features are not supported for IP sessions:
 - Packet of Disconnect (PoD)
 - Session limit per system, VLAN, or MAC



Note IP Sessions over Gigabit EtherChannel (IPoGEC) and IP Sessions over EoGRE tunnels are supported starting from Cisco IOS XE Release 3.9S. For more information, see [IP Sessions Over Gigabit EtherChannel](#) Chapter of the *Intelligent Wireless Access Gateway Configuration Guide*.



Note Network Address Translation (NAT) configuration is supported on the access side of ISG starting from Cisco IOS XE Release 3.12S. For more information, see [IP Sessions Over Gigabit EtherChannel](#) Chapter of the *Intelligent Wireless Access Gateway Configuration Guide*.

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

ISG supports the types of IP subscriber sessions described in the following sections:

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 a MAC address form part of the identity of the session. ISG can be configured to create IP sessions when it receives 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 a subscriber device that is more than one hop from the gateway.

IP Interface Sessions

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

IP interface sessions can be used in situations where 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 a 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, that is 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 in 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 an ISG device is more than one hop away from a subscriber, and multiple subnets could be 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 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 1000 Series Aggregation routers. ISG IP sessions are supported on nonaccess-type subinterfaces. For an existing session or even when no session exists, this support helps multicast traffic to pass through the interfaces that are configured for IP sessions in both upstream and downstream directions without creating a session.

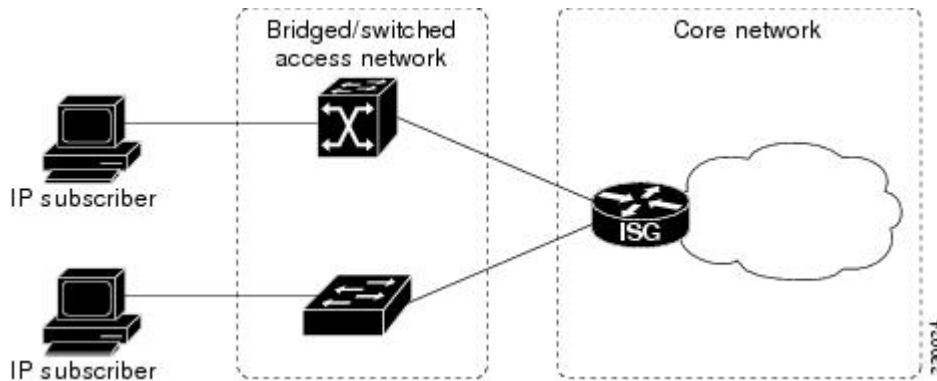
IP Subscriber Connectivity

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

Layer 2-connected subscribers are either directly attached to the physical interfaces of ISG or connected to 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: Layer 2-Connected Access Network

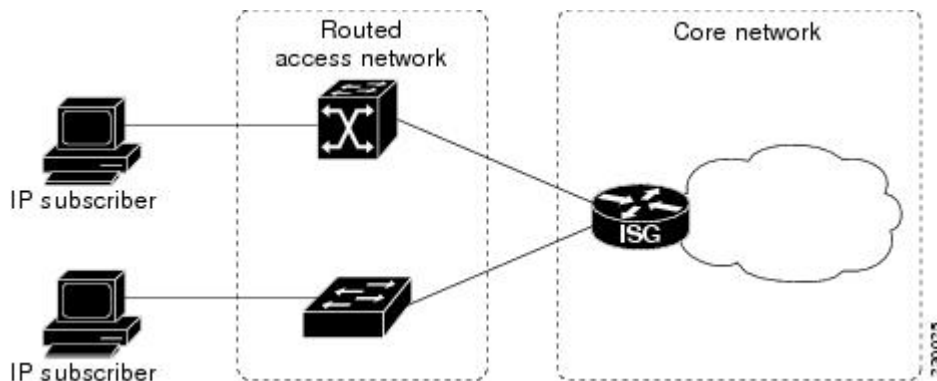


Roaming can be configured on Layer 2-connected IP subscriber sessions by using the **ip subscriber l2-roaming** command. When a Layer 2-connected IP subscriber tries to establish a session with an existing MAC address and a new IP address on an interface that is different from the one that is running the current session, ISG terminates the existing session and creates a new session with a new MAC address-IP address pair. When the subscriber tries to establish a session with an existing MAC address and a new IP address on the same interface that is running the current session, ISG blocks the new session.

Routed Access Networks

For routed access networks, 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: Routed Access Network



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, an IP session is created after ISG receives a DHCP DISCOVER packet:
 - ISG serves as a DHCP relay or a server for new IP address assignments.

- Subscribers are configured for DHCP.
- The DHCP DISCOVER packet is the first DHCP request received from the subscriber.
- Source IP address is unclassified— For routed IP subscribers, a new IP session is triggered when an IP packet with an unclassified source IP address (an IP session does not yet exist for that IP address) is received.
- Unclassified source MAC address— For Layer 2-connected IP subscribers, a new IP session is triggered when an IP packet with an unclassified source MAC address (which means that an IP session does not yet exist for that MAC address) is received.
- 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

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 (including 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

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 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

An IP address falls in either the public or the private IP address category, irrespective of the method used to assign the IP address to the IP subscriber. If an IP subscriber is assigned a private IP address and the subscriber has to reach the Internet, a Layer 3 gateway, such as an ISG or a firewall, that is present 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 belongs to the subnet provisioned on the access interface. A foreign subscriber IP address 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 has an adjacency of the next hop towards 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. When 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.

When 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 hotspot that generally assigns dynamic IP addresses may 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 the 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 either 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 time that it creates an 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

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

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 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 for 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 ISG.

For 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 for ISG. In this deployment, all end users share the same connectivity and services provided by 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.

Layer 2-Connected IP Subscriber Identity

A Layer 2-connected access network can provide IP connectivity to IP subscribers with native IP addresses and foreign and overlapping 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.

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 keys for the IP session and are used in the following 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, 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

Based on the deployment requirements, an IP subscriber may or may not have the VPN service. If an IP subscriber does have the 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 login. 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.

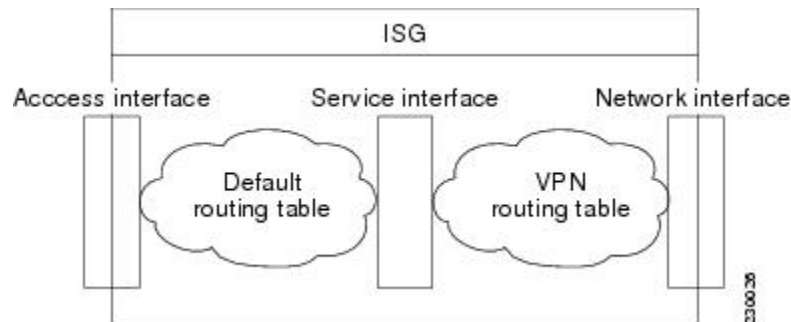
Dynamic VPN selection can be initiated through automatic service login, where the virtual routing and forwarding (VRF) instance is downloaded and applied to the subscriber session at the start of a session. Dynamic VPN selection can also be initiated through subscriber service selection at a web portal, where 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 instance. The multiservice interface represents a boundary between a VPN routing domain and the default routing domain. When an IP subscriber is 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 VPN domain. One multiservice interface must be configured for each VPN routing domain. The figure below illustrates the multiservice interface model.

Figure 4: Multiservice Interface Model



VPN Addressing

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

A VRF transfer is necessary when a identity of the subscriber 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. After the portal-based service selection, the subscriber has to be transferred into the VRF that is associated with the selected service domain. After the 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.

To support VRF transfers, DHCP should be configured with short initial leases. This is because existing subscriber addresses can be altered only after 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 public IP address blocks allocated to them 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 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 deactivates all current services (including the current primary service) and activates the new primary service, and hence, switches 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 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—The **application stop** command is typically used to terminate a session when a subscriber initiates an account logout 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 the client continues to hold an unexpired DHCP lease, ISG performs a session restart to prevent the client's IP connection from being nonfunctional until the DHCP lease expires. A control policy can be configured to define the actions that ISG performs when the session restart event occurs. If a policy is not defined, a default policy takes effect. The default policy causes ISG to disconnect the session after 60 seconds after 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 of 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

New 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 autologin. A default service might also 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

An Intelligent Services Gateway (ISG) device creates IP sessions for IP traffic on subscriber-side interfaces. The tasks in the following sections enable IP sessions and indicate how sessions are identified:

Creating IP Subscriber Sessions for Routed ISG Subscribers

IP subscribers that are routed through a Layer 3 access network with at least one transit router before reaching ISG are known as routed IP subscribers. 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** [**ipv4** | [**ipv6**] [**list list-name**]]}
6. **passthru downstream ipv6**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Specifies an interface and enters interface configuration mode.
Step 4	ip subscriber routed Example: Device(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 [ipv4 [ipv6] [list list-name]]} Example: Device(config-subscriber)# initiator unclassified ip-address	Enables ISG to create an IP subscriber session upon receipt of the specified packet type. <ul style="list-style-type: none">• Enter this command 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 a DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions on receiving DHCP DISCOVER packets. In other words, the initiator dhcp command must be configured instead of the initiator unclassified ip-address or initiator unclassified mac-address command.

	Command or Action	Purpose
Step 6	passthru downstream ipv6 Example: Device(config-subscriber)# passthru downstream ipv6	(Optional) Allows IPv6 downstream traffic from the ISG interface to pass through without a subscriber session.
Step 7	end Example: Device(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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Specifies an interface and enters interface configuration mode.
Step 4	ip subscriber l2-connected Example:	Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode.

	Command or Action	Purpose
	Device(config-if)# ip subscriber l2-connected	Note We recommend that you configure IP sessions for Layer 2-connected subscribers using the ip subscriber l2-connected command. However, you could also use the ip subscriber routed command if subscriber IP addresses are routable in the access domain.
Step 5	initiator {dhcp [class-aware] radius-proxy unclassified mac-address} Example: Device(config-subscriber)# initiator unclassified mac-address	Configures ISG to create an IP subscriber session upon receipt of the specified packet type. <ul style="list-style-type: none"> • Enter this command 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 a 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-address or initiator unclassified mac-address command.
Step 6	end Example: Device(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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>. subinterface-number</i>] Example: <pre>Device(config)# interface GigabitEthernet 0/0/0.1</pre>	Specifies an interface or subinterface and enters interface or subinterface configuration mode.
Step 4	ip subscriber interface Example: <pre>Device(config-subif)# ip subscriber interface</pre>	Specifies the type of IP subscriber to be hosted on the interface. Note The ip subscriber interface command cannot be configured if the service-policy input or service-policy output command is already configured on the interface; these commands are mutually exclusive.
Step 5	end Example: <pre>Device(config-subif)# end</pre>	(Optional) Returns to privileged EXEC mode.

Creating ISG Static Sessions

An Intelligent Services Gateway (ISG) static session enables you to configure static IP sessions by configuring a group of server addresses. Perform the following task to create ISG static sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ip source** *ip-address* {**mac** *mac-address* | **mask** *subnet-mask*}
5. **exit**
6. **interface** *type number*
7. **ip subscriber** {**l2-connected** | **routed**}
8. **initiator static ip subscriber list** *list-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip subscriber list list-name Example: Device(config)# ip subscriber list mylist	Specifies the IP subscriber list name and enters server list configuration mode.
Step 4	ip source ip-address {mac mac-address mask subnet-mask} Example: Device(config-server-list)# ip source 209.165.200.225 mac 0.7.f	Specifies the static server IP address and MAC address (in case of Layer 2-connected subscribers) or subnet mask (in the case of routed interfaces).
Step 5	exit Example: Device(config-server-list)# exit	Exits server list configuration mode and returns to global configuration mode.
Step 6	interface type number Example: Device(config)# interface GigabitEthernet 2/0/0	Specifies an interface and enters interface configuration mode.
Step 7	ip subscriber {l2-connected routed} Example: Device(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 IP sessions for Layer 2-connected subscribers should be configured using the ip subscriber l2-connected command. However, the ip subscriber routed command can also be used if subscriber IP addresses are routable in the access domain.
Step 8	initiator static ip subscriber list list-name Example: Device(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: Device(config-subscriber)# end	(Optional) 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 create an IP subnet session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber routed**
5. **initiator unclassified ip-address** [ipv4 | [ipv6] [list *list-name*]]
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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Specifies an interface and enters interface configuration mode.
Step 4	ip subscriber routed Example: Device(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 [ipv4 [ipv6] [list <i>list-name</i>]] Example: Device(config-subscriber)# initiator unclassified ip-address	Configures ISG to create an IP subscriber session when an IP packet with an unclassified IP source address is received.
Step 6	end Example: Device(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. <ul style="list-style-type: none">• 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

	Command or Action	Purpose
		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 Intelligent Services Gateway (ISG) to take specific actions after the recovery of an IP session when ISG has terminated or reloaded the session. This task applies to DHCP-initiated IP sessions only.

If a policy for session recovery is not configured, ISG applies 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: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: Device(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.

	Command or Action	Purpose
Step 4	<p>class type control {<i>control-class-name</i> always} event session-restart</p> <p>Example:</p> <pre>Device(config-control-policymap)# class type control always event session-restart</pre>	<p>Specifies a control class that is evaluated when the session-restart event occurs and enters policy-map class control configuration mode.</p> <ul style="list-style-type: none"> 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	<p><i>action-number</i> authorize [aaa list <i>list-name</i>] [password <i>password</i>] [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}</p> <p>Example:</p> <pre>Device(config-control-policymap-class-control)# 1 authorize identifier source-ip-address</pre>	<p>(Optional) Initiates a request for authorization on the basis of the specified identifier.</p>
Step 6	<p><i>action-number</i> service-policy type service [unapply] [aaa list <i>list-name</i>] {name <i>service-name</i> identifier {authenticated-domain authenticated-username dnis nas-port tunnel-name unauthenticated-domain unauthenticated-username}}</p> <p>Example:</p> <pre>Device(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT</pre>	<p>(Optional) Activates an ISG service.</p> <ul style="list-style-type: none"> Specifying an identifier instead of a service name activates a service that has the same name as the specified identifier.
Step 7	<p><i>action-number</i> set-timer <i>name-of-timer</i> <i>minutes</i></p> <p>Example:</p> <pre>Device(config-control-policymap-class-control)# 1 set-timer TIMERA 5</pre>	<p>(Optional) Starts a named policy timer.</p> <ul style="list-style-type: none"> Expiration of the timer generates the event timed-policy expiry.
Step 8	<p>end</p> <p>Example:</p> <pre>Device(config-control-policymap-class-control)# end</pre>	<p>(Optional) Returns to privileged EXEC mode.</p>

Verifying ISG IP Subscriber Sessions

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

SUMMARY STEPS

- enable**
- 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*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show subscriber session [detailed] [identifier <i>identifier</i> uid <i>session-id</i> username <i>name</i>] Example: Device# show subscriber session detailed	Displays information about ISG policies and features for subscriber sessions.
Step 3	show ip subscriber [mac <i>mac-address</i> [vrf <i>vrf-name</i>] [[dangling <i>seconds</i>] [detail] interface <i>interface-name</i> [detail statistics] ip <i>ip-address</i> static list <i>listname</i> statistics { arp dangling }]] Example: Device# show ip subscriber ip 10.10.10.10	Displays information about ISG IP subscriber sessions.
Step 4	show platform isg session-count { all <i>slot</i> } Example: Device# show platform isg session-count all	Displays the number of active ISG subscriber sessions by line card.

Clearing ISG 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**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	show ip subscriber [mac <i>mac-address</i> [vrf <i>vrf-name</i>] [[dangling <i>seconds</i>] [detail] interface <i>interface-name</i> [detail statistics] ip <i>ip-address</i> static list <i>listname</i> statistics { arp dangling }]] Example: Device# show ip subscriber ip 10.10.10.10	(Optional) Displays information about ISG IP subscriber sessions.
Step 3	clear ip subscriber [interface <i>interface-name</i> mac <i>mac-address</i> slot <i>slot-number</i> no-hardware [vrf <i>vrf-name</i>] [dangling <i>seconds</i> ip <i>ip-address</i> statistics]] Example: Device# clear ip subscriber ip 10.10.10.10	Clears ISG IP subscriber sessions.

Troubleshooting ISG IP Subscriber Sessions

Use the following commands to troubleshoot ISG IP subscriber sessions. You can use the **debug** commands in any order.

SUMMARY STEPS

1. **enable**
2. **debug ip subscriber packet**
3. **debug condition username** *username*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug ip subscriber packet Example: Device# debug ip subscriber packet	Enables ISG IP subscriber session debugging.
Step 3	debug condition username <i>username</i> Example: Device# debug condition username user1	Filters debugging output for certain debug commands on the basis of specified conditions.

Assigning ISG Subscriber IP Addresses by Using DHCP

Configure DHCP support in your network before performing the tasks in this section.

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Device(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: Device(config-if)# ip address 10.1.0.1 255.255.0.0	Sets a primary or secondary IP address for an interface.
Step 5	ip subscriber [l2-connected routed] Example: Device(config-if)# ip subscriber	Enables ISG IP subscriber configuration mode.

	Command or Action	Purpose
Step 6	initiator dhcp class-aware Example: <pre>Device(config-subscriber) initiator dhcp class-aware</pre>	Configures ISG to create IP sessions upon receipt of DHCP DISCOVER packets. <ul style="list-style-type: none"> 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: <pre>Device(config-if) # end</pre>	(Optional) Returns to privileged EXEC mode.

Configuring DHCP Server User Authentication

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

Before you begin

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: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	aaa new-model Example: Device(config)# aaa new model	Enables authentication, authorization, and accounting (AAA).
Step 4	aaa authentication login list-name local Example: Device(config)# aaa authentication login mylist local	Sets the AAA authentication at login.
Step 5	ip dhcp pool pool-name Example: Device(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: Device(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 DHCP server.
Step 7	exit Example: Device(dhcp-config)# exit	Exits DHCP pool configuration mode and returns to global configuration mode.
Step 8	interface type number Example: Device(config)# interface GigabitEthernet 0/0	Enters interface configuration mode.
Step 9	ip subscriber l2-connected Example: Device(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: Device(config-subscriber)# initiator dhcp class-aware	Initiates a class for DHCP for an IP session initiated by DHCP.
Step 11	end Example: Device(config-subscriber)# end	Returns to privileged EXEC mode.

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.

Before you begin

Before configuring a DHCP class in a service policy map, you must configure a DHCP pool and the 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: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-name</i> Example: Device(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.
Step 4	classname <i>class-name</i> Example: Device(config-service-policymap)# classname class1	Associates a DHCP pool with a service policy map.
Step 5	end Example: Device(config-service-policymap)# end	(Optional) Returns to privileged EXEC mode.
Step 6	show policy-map type service	(Optional) Displays the contents of all service policy maps.

	Command or Action	Purpose
	Example: Device# show policy-map type service	<ul style="list-style-type: none"> Use this command to verify that the DHCP class is associated with the service policy map.

What to Do Next

After 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.

Before configuring a DHCP class in a service profile or user profile on the AAA Server, 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. To associate a DHCP address pool with a service or specific subscriber, add the DHCP class attribute to the user or service profile. For example:

```
26,9,1 = "subscriber:classname=class-name "
```

After associating a DHCP address pool with a service or specific subscriber, 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 either 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.

Before you begin

The following prerequisites apply for this task:

- 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

- 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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip dhcp-server {ip-address query lease {retries max-retransmissions timeout timeout-query-seconds}} Example: Device(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: Device(config)# end	Exits global configuration mode.

Configuring ISG Dynamic VPN Selection

Configuring 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	Enables privileged EXEC mode.

Specifying a VRF in a Service Policy Map

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface multiservice interface-number Example: Device(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: Device(config-if)# ip vrf forwarding vrf1	Associates a VPN VRF with an interface or subinterface.
Step 5	ip address ip-address mask Example: Device(config-if)# ip address 172.16.0.0 255.255.255.0	Sets the primary IP address for an interface. <ul style="list-style-type: none"> Specifies the IP address of the VPN.
Step 6	end Example: Device(config-if)# end	(Optional) Returns to privileged EXEC mode.

Specifying a VRF in a Service Policy Map

VPN routing and forwarding (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

- enable
- configure terminal
- policy-map type service *policy-map-name*
- ip vrf forwarding *name-of-vrf*
- sg-service-type primary
- sg-service-group *service-group-name*
- end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: Device(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 <i>name-of-vrf</i> Example: Device(config-service-policymap)# ip vrf forwarding vrf1	Associates the service with a VRF.
Step 5	sg-service-type primary Example: Device(config-service-policymap)# sg-service-type primary	Defines the service as a primary service. <ul style="list-style-type: none"> • A primary service 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.
Step 6	sg-service-group <i>service-group-name</i> Example: Device(config-service-policymap)# sg-service-group group1	(Optional) Associates an ISG service with a service group. <ul style="list-style-type: none"> • A service group is a group 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: Device(config-service-policymap)# end	(Optional) Returns to privileged EXEC mode.

Verifying VRF Transfer for IP Sessions

Perform the following task as needed to verify VRF transfer for IP sessions. You can use the **show** commands in this task in any order.

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]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show subscriber session uid <i>session-identifier</i> detail Example: Device# show subscriber session uid 4 detail	Displays information about ISG subscriber sessions with a specific session identifier.
Step 3	show ip subscriber [dangling <i>seconds</i> detail ip <i>ip-address</i> mac <i>mac-address</i> vrf <i>vrf-name</i> [dangling <i>seconds</i> detail ip <i>ip-address</i>]] Example: Device# show ip subscriber vrf vrf1	Displays information about ISG IP subscriber sessions.
Step 4	show idmgr {memory [detailed [component [<i>substring</i>]]] service key session-handle <i>session-handle-string</i> service-key <i>key-value</i> session key {aaa-unique-id <i>aaa-unique-id-string</i> domainip-vrf ip-address <i>ip-address</i> vrf-id <i>vrf-id</i> nativeip-vrf ip-address <i>ip-address</i> vrf-id <i>vrf-id</i> portbundle ip <i>ip-address</i> bundle <i>bundle-number</i> session-guid <i>session-guid</i> session-handle <i>session-handle-string</i> session-id <i>session-id-string</i>} statistics} Example: Device# 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 <i>vrf-name</i>] Example: Device# show ip route	Displays the current state of the routing table.

	Command or Action	Purpose
Step 6	show ip dhcp binding [ip-address] Example: Device# show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

Troubleshooting VRF Transfer for IP Sessions

The commands in this task can be used to troubleshoot VRF transfer of IP sessions. The **debug** commands can be entered in any order.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug subscriber {event error packet policy service} Example: Device# debug subscriber service	Displays debugging messages pertaining to subscriber policies, policy server events, and changes to service.
Step 3	debug ip subscriber {event error packet fsm all} Example: Device# debug ip subscriber error	Displays debugging messages pertaining to an IP session created on the service gateway.
Step 4	debug subscriber policy dpm {error event} Example: Device# debug subscriber policy dpm event	Displays diagnostic information about policy execution that is related to DHCP events.
Step 5	debug ip dhcp server {events packets linkage class} Example: Device# debug dhcp ip dhcp server events	Enables Cisco IOS DHCP server debugging.

Configuration Examples for ISG Access for IP Subscriber Sessions

Example: Configuring 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 GigabitEthernet 0/0/1.401
 ip subscriber routed
   initiator dhcp class-aware
   initiator unclassified ip-address
   initiator radius-proxy
```

Example: Creating ISG IP Interface Sessions

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: Creating ISG Static Sessions

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 0/4
 ip subscriber l2-connected
   initiator static ip subscriber list mylist
```

Example: Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers

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 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: Configuring IP Session Recovery for DHCP-Initiated IP Session

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: Configuring an ISG Interface for Dynamic DHCP Class Association

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: Configuring 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).

Example: Configuring DHCP Address Pool Classes and Relay Actions for ISG

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 10.3.0.2 255.255.0.0
  ip address 10.4.0.2 255.255.0.0
!Address pools for poolA1 and poolB2:
ip dhcp pool poolA1
  relay source 10.1.0.2 255.255.0.0
  class poolA1
  relay target 10.55.10.1
!Address pool for poolA2:
ip dhcp pool poolA2
  relay source 10.3.0.2 255.255.0.0
  class poolA2
  relay target 10.55.10.1
!Address pools for poolB1 and poolB2:
ip dhcp pool poolB1
  relay source 10.2.0.2 255.255.0.0
  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 uses the same configuration command as secure ARP uses on a DHCP server. It uses the **update arp** command in address-pool configuration mode. If the system allocates an address from this address pool, secure ARP is added to it. If the system relays a packet using this address pool, secure ARP is also added to it.

Example: Configuring ISG 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 Corporate VPN service, 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

```

Example: Troubleshooting DHCP Server User Authentication

You can determine the DHCP authentication by using the **debug ip dhcp server events**, **debug ip dhcp server packets**, 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:

```

Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   Hardware address/
                   User name
10.0.0.1            0100.1a70.1530.38   Nov 18 2008 03:43 PM   Automatic

```

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	<i>IP Addressing: DHCP Configuration Guide</i>
Configuring ISG control policies	“Configuring ISG Control Policies” module in the <i>Intelligent Services Gateway Configuration Guide</i> .

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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 and 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 and 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 , and show ip subscriber .
ISG—Downstream Pass-Through and Idle Timer	Cisco IOS XE Release 3.6S	Enables IPv6 downstream traffic from an ISG interface to pass through to a subscriber without a subscriber session present. The following command was introduced by this feature: passthru downstream ipv6 .

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. 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.
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 , and show ip subscriber list .

Feature Name	Releases	Feature Configuration Information
L3 Routed Dual Stack	Cisco IOS XE Gibraltar 16.10.x	The L3 Routed Dual Stack feature allows both IPv4 and IPv6 L3 routed sessions to exist together as a part of the same session. To enable the functionality, you must configure the 'collect identifier mac-address' command at the beginning of the session.



CHAPTER 5

Configuring ISG IPv6 Support

Intelligent Services Gateway (ISG) is a software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes the IPv6 support available for ISG IP subscriber sessions including information about the Time-Based Billing feature.

- [Finding Feature Information, on page 85](#)
- [Restrictions for ISG IPv6 Support, on page 85](#)
- [Information About ISG IPv6 Support, on page 86](#)
- [How to Configure ISG IPv6 Support, on page 89](#)
- [Configuration Examples for ISG IPv6 Support, on page 91](#)
- [Additional References, on page 94](#)
- [Feature Information for ISG IPv6 Support, on page 95](#)

Finding Feature Information

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

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 IPv6 Support

- Layer 2 connected interfaces are not supported. Only Layer 3 routed in-band IPv6 sessions are supported.
- Out-of-band IPv6 sessions are not supported, which means DHCP initiated or RADIUS proxy initiated sessions are not supported for IPv6 sessions.
- Time-based billing is not supported on PPP sessions directly; it is supported through services and flows installed on the PPP session.

Information About ISG IPv6 Support

ISG IPv6 Session Support

ISG creates an IPv6 subscriber session based on the first IPv6 packet received from an unclassified IPv6 address or IPv6 prefix, similar to the way subscriber sessions are created for IPv4 packets. The subscriber session is identified by the IPv6 address. Native IP sessions have either an IPv4 or IPv6 address, but not both. A native IPv6 session has an IPv6 address only and all traffic generated from the subscriber uses IPv6.

IPv6 single-stack sessions are supported for ISG subscriber sessions. If a native IP subscriber's host sends traffic for both an IPv4 and IPv6 address, ISG creates a separate IP session for each of these IP addresses. This subscriber will have an IPv4 session and an IPv6 session with no interaction between them. A dual-stack session is a single subscriber session with two distinct IP addresses, one for IPv4 and one for IPv6. Dual-stack native IP sessions are not supported.

Layer 3 unclassified IPv6 sessions for routed subscribers are supported. These sessions are identified by their unique IPv6 IP address or an IPv6 subnet session (IPv6 address and prefix). IPv6 is not supported for Layer 2 connected and DHCP-initiated subscriber sessions.

Session Coexistence on ISG Interfaces

The following session combinations can exist on the same ISG interface in Cisco IOS XE Release 3.5S and later releases:

- Native IPv6 and native IPv4 sessions
- Native IPv6 and PPP IPv4 sessions
- Native IPv6 and PPP IPv6 sessions
- Native IPv6 and PPP dual-stack sessions

ISG Dual-Stack Features

Dual-stack features are protocol independent and work at the session level. These features cannot be configured based on the stack. A single generic configuration is applied to the session regardless of whether it is a single-stack or dual-stack session. The configuration of these features is the same for IPv4 and IPv6.

Because these features are applied at the session level, the same instance of the feature handles both the IPv4 and IPv6 stacks for a dual-stack session, and the behavior is aggregated. For example, the same instance of the accounting feature counts both IPv4 and IPv6 packets. Similarly, the same instance of the idle timeout feature monitors both IPv4 and IPv6 traffic and considers a session to be idle when there is neither type of traffic.

The following features are examples of dual-stack features:

- Absolute Timeout (Session Timer)
- Idle Timeout (Connection Timer)
- ISG Accounting
- ISG Policer (Dynamic Rate Limiting)

- Quality of Service

ISG Protocol-Dependent Features

Protocol-dependent features rely on the underlying protocol. An instance of the feature works only for one of the protocols, either IPv6 or IPv4. For example, the Layer 4 Redirect feature has translation rules that are protocol dependent. An IPv6 packet can be redirected only to an IPv6 destination; an IPv4 packet can be redirected only to an IPv4 destination.

The configuration of protocol-dependent features applies only to the corresponding stack of the session. If a feature must run on both protocols for a dual-stack session, separate configurations must be created and applied on both stacks respectively. These features cannot be configured for an entire session unless it is a single-stack session.

The behavior of protocol-dependent features is limited to a single stack. An instance of the feature runs only on a particular stack and has no functional impact on the other stack, if applicable. If the feature is applied on both stacks of a dual-stack session, two separate instances are created and run independently. There is no aggregated behavior for these features.

The following features are examples of ISG protocol-dependent features:

- Access Control Lists (ACLs)
- Layer 4 Redirect
- Port-Bundle Host Key
- Traffic Classes

IPv6 Support for ISG Features

The following ISG features are supported for native IPv6 sessions and PPP dual-stack sessions:

Feature	Description	Session Support
Absolute Timeout (Session Timer)	IPv6 functionality and configuration are the same as for IPv4 subscriber sessions. For configuration information, see the “Configuring ISG Policies for Session Maintenance” module in this guide.	<ul style="list-style-type: none"> • Native IPv4/IPv6 • PPP dual stack
Idle Timeout (Connection Timer)	IPv6 functionality and configuration are the same as for IPv4 subscriber sessions. For configuration information, see the “Configuring ISG Policies for Session Maintenance” module in this guide.	<ul style="list-style-type: none"> • Native IPv4/IPv6 • PPP dual stack
ISG Accounting	Per-session and per-service accounting can be configured on either an IPv4-only or IPv6-only IP session. Per-flow accounting can be configured on either an IPv4 or IPv6 traffic class. For configuration information, see the “Configuring ISG Accounting” module in this guide.	<ul style="list-style-type: none"> • Native IPv4/IPv6 • PPP dual stack

Feature	Description	Session Support
ISG Policer (Dynamic Rate Limiting)	IPv6 functionality and configuration are the same as for IPv4 subscriber sessions. For information, see the “Configuring MQC Support for IP Sessions” module in this guide.	<ul style="list-style-type: none"> • Native IPv4/IPv6 • PPP dual stack
Layer 4 Redirect	IPv6 packets can be redirected only to an IPv6 destination; IPv4 packets can be redirected only to an IPv4 destination. For configuration information, see the “Redirecting Subscriber Traffic Using ISG Layer 4 Redirect” module in this guide.	<ul style="list-style-type: none"> • Native IPv4/IPv6 • PPP dual stack • Protocol dependent
Modular QoS CLI (MQC)	The following operations are supported for an MQC policy applied to PPP IPv6 sessions and PPP dual-stack sessions: <ul style="list-style-type: none"> • Add or remove a class • Add, remove, or modify an action under a class • Modify an ACL For configuration information, see the “Configuring MQC Support for IP Sessions” module in this guide.	<ul style="list-style-type: none"> • Native IPv4 • PPP IPv6 • PPP dual stack
Traffic Classes	The protocol version of a traffic class is determined by the protocol version of the access control list (ACL) that was used to configure the traffic class. IPv6 traffic classes are supported using named IPv6 ACLs. Traffic classes are also supported on PPP sessions. For configuration information, see the “Configuring ISG Subscriber Services” module in this guide.	<ul style="list-style-type: none"> • Native IPv4/IPv6 • PPP dual stack • Protocol dependent

Time-Based Billing Service

The Time-Based Billing feature calculates the 24-hour volume usage for all subscriber sessions that are active on an L2TP network server (LNS) at a specified time each day. It reports the volume used by a session since the last specified time, in 24-hour intervals. You can configure the router to collect the volume statistics of all active sessions at the same time every day, for example, everyday at midnight. The system would report the volume usage of a session from midnight of the previous day to midnight of the current day.

Time-based billing will also report input and output traffic statistics for IPv6 and IPv4 traffic separately and as an aggregate using new AAA attributes in AAA accounting records.

Changes in local time based on Day Light Savings Time (DST), Network Time Protocol (NTP), or clock changes configured on the router are taken into account when reporting volume statistics at the specified time.

Time-based billing is supported for IPv4, IPv6, and PPP sessions.

How to Configure ISG IPv6 Support

For information on creating IPv6 subscriber sessions for routed ISG subscribers, see the module “Configuring ISG Access for IP Subscriber Sessions.”



Note IPv6 sessions for Layer 2 connected subscribers are not supported.

Defining an IPv6 Prefix for ISG Subscriber Sessions

To enable ISG to create an IPv6 subscriber session after receiving the first packet with a particular IPv6 prefix, you define the IPv6 prefix in an IP subscriber list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ipv6 prefix default** *length*
5. **exit**
6. **interface** *type number*
7. **ip subscriber routed**
8. **initiator unclassified ip-address** [**ipv6**] [**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 <i>list-name</i> Example: Router(config)# ip subscriber list mylist	Specifies the IP subscriber list name and enters server list configuration mode.
Step 4	ipv6 prefix default <i>length</i> Example: Router(config-server-list)# ipv6 prefix default 64	Defines the IPv6 prefix for which ISG initiates IPv6 subscriber sessions.

	Command or Action	Purpose
Step 5	exit Example: Router(config-server-list)# exit	Returns to global configuration mode.
Step 6	interface <i>type number</i> Example: Router(config)# interface GigabitEthernet 2/0/0	Specifies an interface and enters interface configuration mode.
Step 7	ip subscriber routed Example: Router(config-if)# ip subscriber routed	Specifies that routed IP subscribers are to be hosted on the interface and enters ISG IP subscriber configuration mode.
Step 8	initiator unclassified ip-address [ipv6] [list list-name] Example: Router(config-subscriber)# initiator unclassified ip-address ipv6 list mylist	Enables ISG to create an IPv6 subscriber session after receiving a packet with the IPv6 prefix.
Step 9	end Example: Router(config-subscriber)# end	Returns to privileged EXEC mode.

Configuring Time-Based Billing Service

ISG time-based billing is configured in the service profile on a AAA server. If you include a traffic class in the service profile, time-based billing will apply to the specified flow. If you do not configure a traffic class, time-based billing will apply to the session.

Before you begin

ISG per-session or per-flow accounting must be configured.

SUMMARY STEPS

1. Cisco-AVpair = "PPWhh:mm:ss:d"
2. Cisco-AVpair = "ip:traffic-class={in | out} access-group [acl-number | name acl-name] [priority n]"
3. **show subscriber session feature time-based-billing detailed**

DETAILED STEPS

Step 1 Cisco-AVpair = "PPWhh:mm:ss:d"

Add the Post Paid VSA to the service profile. This attribute specifies the weekly tariff-billing points as follows:

hh:mm:ss:d—Weekly billing 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 the 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 3 **show subscriber session feature time-based-billing detailed**

Enter this command on the ISG router to display information about time-based billing. The following example shows output from this command:

```
Router# show subscriber session feature time-based-billing detailed

-----
Type: IP, UID: 7, State: authen, Identity: aabb.cc00.6400
Session Up-time: 00:00:08, Last Changed: 00:00:08
Switch-ID: 4102

Time-based-billing:
Class-id  Dir  Last-Tariff  Packets-v4  Bytes-v4  Packets-v6  Bytes-v6  Source
0         In   1291415061  4           400       2           200      Peruser
1         Out  1291415061  3           200       1           100      Peruser
```

Configuration Examples for ISG IPv6 Support

Example: IPv6 Prefix for ISG Subscriber Sessions

The following example shows an IPv6 prefix defined in the IP subscriber list named mylist, which has been assigned to Gigabit Ethernet port 0/0/0. ISG will create an IPv6 subscriber session when it receives the first packet with the default IPv6 prefix.

```
ip subscriber list mylist
  ipv6 prefix default 64

interface GigabitEthernet0/0/0
 ip vrf forwarding vrf-1
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 out
 ip virtual-reassembly
```

```

zone-member security private
media-type sfp
negotiation auto
ipv6 address 2001:DB8:1:1::26/64
ip subscriber routed
initiator unclassified ip-address ipv6 list mylist

```

Example: Time-Based Billing Service

The following example shows an IPv6 session configured for doing billing daily at midnight:

```
PPW00:00:00:127
```

Day 1—A native IPv6 session starts at 10 a.m.

Day 1 at tariff-switch point (12 a.m.)—A snapshot of the current volume used from 10 a.m. is recorded, for example:

```

IPv6-input-bytes = 10000
IPv6-input-packets = 100
IPv6-output-bytes = 20000
IPv6-output-packets= 200

```

Day 2 say at 12:10 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```

Tariff-Input-Packets = 100           Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 10000        Aggregate Input IPv4 and IPv6 Bytes
Tariff-Input-Packets-IPv6 = 100
Tariff-Input-Octets-IPv6 = 10000
Tariff-Output-Packets = 200        Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000       Aggregate Output IPv4 and IPv6 Bytes
Tariff-Output-Packets-IPv6 = 200
Tariff-Output-Octets-IPv6 = 200

```

Day 2—All Interim records sent thereafter until the next tariff-switch point will carry the above values.

Day 2 at tariff-switch point (12 a.m.)—A snapshot of the volume used from Day 1 at 12 a.m. to Day 2 at 12 a.m. is recorded, for example:

```

IPv6-input-bytes = 600000
IPv6-input-packets = 6000
IPv6-output-bytes = 20000
IPv6-output-packets= 200

```

Day 3 say at 12:20 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```

Tariff-Input-Packets = 6000        Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 600000       Aggregate Input IPv4 and IPv6 Bytes
Tariff-Input-Packets-IPv6 = 6000
Tariff-Input-Octets-IPv6 = 600000
Tariff-Output-Packets = 200        Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000       Aggregate Output IPv4 and IPv6 Bytes
Tariff-Output-Packets-IPv6 = 200
Tariff-Output-Octets-IPv6 = 200

```

Day 3—All Interim records sent thereafter until the next tariff-switch point will carry the above same values.

Day 4—The session is disconnected at 8 a.m. A snapshot of the volume used from last tariff to the session disconnect time is taken, for example:

```
IPv6-input-bytes = 500
IPv6-input-packets = 1
IPv6-output-bytes = 400
IPv6-output-packets= 1
```

A stop record is sent with the following values in the VSAs:

```
Tariff-Input-Packets = 1           Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 500         Aggregate Input IPv4 and IPv6 Bytes
Tariff-Input-Packets-IPv6 = 1
Tariff-Input-Octets-IPv6 = 500
Tariff-Output-Packets = 1        Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 400       Aggregate Output IPv4 and IPv6 Bytes
Tariff-Output-Packets-IPv6 = 1
Tariff-Output-Octets-IPv6 = 400
```

The following example shows an IPv4 session configured for doing billing daily at midnight:

```
PPW00:00:00:127
```

Day 1—A native IPv4 session starts at 10 a.m.

Day 1 at tariff-switch point (12 a.m.)—A snapshot of the current volume used from 10 a.m. is recorded, for example:

```
IPv4-input-bytes = 10000
IPv4-input-packets = 100
IPv4-output-bytes = 20000
IPv4-output-packets= 200
```

Day 2 say at 12:10 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```
Tariff-Input-Packets = 100        Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 10000       Aggregate Input IPv4 and IPv6 Bytes
Tariff-Output-Packets = 200       Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000     Aggregate Output IPv4 and IPv6 Bytes
```

Day 2—All Interim records sent thereafter until the next tariff-switch point will carry the same above values.

Day 2 at tariff-switch point (12 a.m.)—A snapshot of the volume used from Day 1 at 12 a.m. to Day 2 at 12 a.m. is recorded, for example:

```
IPv4-input-bytes = 60000
IPv4-input-packets = 6000
IPv4-output-bytes = 20000
IPv4-output-packets= 200
```

Day 3 say at 12:20 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```
Tariff-Input-Packets = 6000       Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 600000      Aggregate Input IPv4 and IPv6 Bytes
Tariff-Output-Packets = 200       Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000     Aggregate Output IPv4 and IPv6 Bytes
```

Day 3—All Interim records sent thereafter until the next tariff-switch point will carry the same above values.

Day 4—The session is disconnected at 8 a.m. A snapshot of the volume used from the last tariff-switch point to session disconnect time is taken, for example:

```
IPv4-input-bytes = 500
IPv4-input-packets = 1
IPv4-output-bytes = 400
IPv4-output-packets= 1
```

A stop record is sent with the following values in the VSAs:

```
Tariff-Input-Packets = 1           Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 500         Aggregate Input IPv4 and IPv6 Bytes
Tariff-Output-Packets = 1        Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 400       Aggregate Output IPv4 and IPv6 Bytes
```

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
IPv6 Configuration	IPv6 Configuration Guide, Cisco IOS XE Release 3S
Configuring ISG accounting	“Configuring ISG Accounting” module in this guide
Configuring ISG timers	“Configuring ISG Policies for Session Maintenance” module in this guide
Configuring Layer 4 redirect	“Redirecting Subscriber Traffic Using ISG Layer 4 Redirect” module in this guide
Configuring traffic classes	“Configuring ISG Subscriber Services” module in this guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG IPv6 Support

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 ISG IPv6 Support

Feature Name	Releases	Feature Information
ISG IPv6 Support	Cisco IOS XE Release 3.4S	<p>Adds IPv6 support for routed IP subscriber sessions and for the following ISG features:</p> <ul style="list-style-type: none"> • Absolute Timeout • Idle Timeout • ISG Accounting • Traffic Classes <p>Adds the Time-Based Billing feature and traffic class support for services and flows on PPP sessions.</p> <p>Note Only single-stack sessions are supported for ISG subscriber sessions; dual-stack sessions are not supported.</p> <p>The following commands were introduced or modified: initiator, ipv6 prefix, show ip subscriber, show subscriber session.</p>

Feature Name	Releases	Feature Information
ISG: IPv6 Support phase II	Cisco IOS XE Release 3.5S	<p>Adds support for IPv6 PPP sessions and PPP dual-stack sessions for the following features:</p> <ul style="list-style-type: none"> • HA-supported ISG features • ISG Policer • Layer 4 Redirect • MQC <p>Adds support for PPP dual-stack sessions for the following features:</p> <ul style="list-style-type: none"> • Absolute Timeout • Idle Timeout • ISG Accounting • Traffic Classes <p>The following commands were introduced or modified: redirect session-limit, redirect to, show redirect group, show redirect translations, server ip.</p>



CHAPTER 6

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, on page 97](#)
- [Restrictions for MQC Support for IP Sessions, on page 97](#)
- [Information About MQC Support for IP Sessions, on page 98](#)
- [How to Configure MQC Support for IP Sessions, on page 99](#)
- [Configuration Examples for MQC Support for IP Sessions, on page 101](#)
- [Additional References, on page 101](#)
- [Feature Information for MQC Support for IP Sessions, on page 102](#)

Finding Feature Information

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

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



Note Restrictions that are applicable to PPPoGEC with per-session QoS are also applicable to IPoGEC with per-session QoS. For more information, see [PPPoGEC: Per Session QoS](#) chapter of the *QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)*.

Information About MQC Support for IP Sessions

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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>service-name</i> Example: Router# (config)# policy-map type service service1	Enters policy-map configuration mode. Specifies the policy-map name and its service configuration.
Step 4	service-policy <i>policy-name</i> Example: Router# (config-service-policymap)# service-policy service-policy1	Configures the service policy.

What to do next

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 *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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>service-name</i> Example: Router# (config)# policy-map type service	Enters policy-map configuration mode. Specifies the policy-map name and its service configuration.
Step 4	class type traffic <i>class-name</i> 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

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	<i>Quality of Service Solutions Configuration Guide</i>
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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 7: 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 .



CHAPTER 7

Configuring ISG Port-Bundle Host Key

The Intelligent Services Gateway (ISG) provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure the ISG Port-Bundle Host Key feature, which maps TCP packets from subscribers to a local IP address for the ISG and a range of ports. This mapping allows an external portal to identify the ISG from which a session originated.

- [Finding Feature Information, on page 103](#)
- [Prerequisites for the ISG Port-Bundle Host Key Feature, on page 103](#)
- [Restrictions for the ISG Port-Bundle Host Key Feature, on page 104](#)
- [Information About ISG Port-Bundle Host Key, on page 104](#)
- [How to Configure ISG Port-Bundle Host Key, on page 106](#)
- [Configuration Examples for ISG Port-Bundle Host Key, on page 110](#)
- [Additional References, on page 110](#)
- [Feature Information for ISG Port-Bundle Host Key, on page 111](#)

Finding Feature Information

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

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 ISG Port-Bundle Host Key feature must be enabled separately 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 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 uses TCP. Packets will not be mapped for a subscriber who does not send TCP traffic.
- Specifying the ISG Port-Bundle Host Key feature in a user profile works only when the user profile is available prior to the arrival of IP packets; for example, for PPP sessions or for DHCP-initiated IP sessions with transparent autologon.

Information About ISG Port-Bundle Host Key

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 and a range of ports. This mapping allows the portal to identify the ISG 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 forwarding (VRF) instances 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 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 a combination of the port bundle and the 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 translation tables to identify the destination IP address and destination TCP port.

Table 8: Subscriber IP VSA Description

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Attribute Data
26	9	250 Account-Info	Subscriber IP	<p>S <i>subscriber-ip-address</i> [:<i>port-bundle-number</i>]</p> <ul style="list-style-type: none"> • S—Account-Info code for subscriber IP. • <i>subscriber-ip-address</i> [:<i>port-bundle-number</i>]<i>—</i>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.



Note The ISG Port-Bundle Host Key feature assigns ISG IP addresses to the source IP in a round-robin fashion based on the available IP addresses and ports.

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 4 bits. The maximum port-bundle length is 10 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 9: 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
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

The ISG Port-Bundle Host Key feature enables external portal access regardless of the 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 HTTP packets to subscribers. The ISG Port-Bundle Host Key feature eliminates the need to provision a portal to allow one portal server to serve multiple ISGs and 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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	<code>Router# configure terminal</code>	
Step 3	<p>policy-map type service <i>policy-name</i></p> <p>Example:</p> <pre>Router(config)# policy-map type service service1</pre>	Creates or defines a service policy map, which is used to define an ISG service.
Step 4	<p>ip portbundle</p> <p>Example:</p> <pre>Router(config-service-policymap)# ip portbundle</pre>	Enables the ISG Port-Bundle Host Key feature for the service.
Step 5	<p>end</p> <p>Example:</p> <pre>Router(config-service-policymap)# end</pre>	(Optional) Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method for 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

SUMMARY STEPS

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

DETAILED STEPS

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

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**
10. **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 portbundle Example: Router(config)# ip portbundle	Enters IP portbundle configuration mode.
Step 4	match access-list <i>access-list-number</i> Example: Router(config-portbundle)# match access-list 101	Specifies packets for port mapping by specifying an access list to compare against the subscriber traffic.
Step 5	length <i>bits</i> 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. • See the section “Port-Bundle Length” for more information.

	Command or Action	Purpose
Step 6	source <i>interface-type interface-number</i> Example: <pre>Router(config-portbundle)# source loopback 0</pre>	Specifies the interface for which the main IP address is mapped by ISG to the destination IP addresses in subscriber traffic. <ul style="list-style-type: none"> • We recommend that you use a loopback interface as the source interface.
Step 7	exit Example: <pre>Router(config-portbundle)# exit</pre>	Returns to global configuration mode.
Step 8	interface <i>type number</i> Example: <pre>Router(config)# interface gigabitethernet 0/0/0</pre>	Specifies an interface for configuration and enters the interface configuration mode.
Step 9	ip portbundle outside Example: <pre>Router(config-if)# ip portbundle outside</pre>	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.
Step 10	end Example: <pre>Router(config-if)# end</pre>	Exits interface configuration mode.

Verifying the 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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ip portbundle status [free inuse] Example:	Displays information about ISG port-bundle groups.

	Command or Action	Purpose
	Router# show ip portbundle status free	
Step 3	show ip portbundle ip <i>portbundle-ip-address</i> bundle <i>port-bundle-number</i> 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 <i>identifier</i> uid <i>session-id</i> username <i>name</i>] Example: Router# show subscriber session detailed	Displays ISG subscriber session information.

Configuration Examples for ISG Port-Bundle Host Key

Example: Configuring ISG Port-Bundle Host Key

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

```

policy-map type service ISGPBKService
  ip portbundle
  !
policy-map type control PBHKRule
  class type control always event session-start
    1 service-policy type service ISGPBKService
  !
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
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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 10: Feature Information for ISG Port-Bundle Host Key

Feature Name	Releases	Feature Configuration Information
ISG Port-Bundle Host Key	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 and a range of ports. This mapping allows the portal to identify the ISG from which the session originated.



CHAPTER 8

Configuring ISG as a RADIUS Proxy

Intelligent Services Gateway (ISG) is a Cisco 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 module describes how to configure ISG as a RADIUS proxy.

In public wireless LAN (PWLAN) deployments, service providers must absolutely ensure the billing accuracy of a user’s session. The billing accuracy must also be met in case of a network component failure. The RADIUS proxy billing accuracy feature ensures that the start and stop session events are accurate and the events are the main references for session management.

- [Finding Feature Information, on page 113](#)
- [Prerequisites for ISG RADIUS Proxy, on page 113](#)
- [Restrictions for ISG RADIUS Proxy, on page 114](#)
- [Information About ISG RADIUS Proxy, on page 114](#)
- [How to Configure ISG as a RADIUS Proxy, on page 116](#)
- [Examples for Configuring ISG as a RADIUS Proxy, on page 124](#)
- [Additional References for Configuring ISG as a RADIUS Proxy, on page 126](#)
- [Feature Information for Configuring ISG as a RADIUS Proxy, on page 127](#)

Finding Feature Information

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

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 software image must support authentication, accountability and authorization (AAA) and Intelligent Services Gateway (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

Public wireless LANs (PWLANS) and wireless mesh networks can contain hundreds of access points, each of which must send RADIUS authentication requests to an authentication, addressing and authorization (AAA) server. The Intelligent Services Gateway (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.

To configure RADIUS proxy billing, you can use the **timer reconnect** command and **show radius-proxy session** command in the appropriate configuration modes.

To enable session reconnection for ISG RADIUS proxy servers and clients, use **pwan-session reconnect** command in the appropriate configuration mode.

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 Intelligent Services Gateway (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.

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 11: 3GPP Attributes Supported by ISG RADIUS Proxy

Attribute	Description	Vendor ID/type
3GPP-IMSI	International Mobile Subscriber Identity (IMSI) for the user.	10415/1
3GPP-Charging-ID	Charging ID for this Packet Data Protocol (PDP) context (this together with the GGSN address constitutes a unique identifier for PDP context).	10415/2

Attribute	Description	Vendor ID/type
3GPP-SGSN-Address	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 Intelligent Services Gateway (ISG) RADIUS proxy has the following benefits:

- Allows the complete set of ISG functionality to be applied to extensible authentication protocol (EAP) subscriber sessions.
- Allows an ISG device to be introduced into a network with minimum disruption to the existing network access server (NAS) and authentication, authorization and accounting (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

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/subslot/port`
4. `ip subscriber {interface | l2-connected | routed}`
5. `initiator radius-proxy`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>type slot/subslot/port</i> Example: Device(config)# interface GigabitEthernet 2/1/0	Specifies an interface for configuration and enters interface configuration mode.
Step 4	ip subscriber { interface I2-connected routed } Example: Device(config-if)# ip subscriber routed	Enables Intelligent Services Gateway (ISG) IP subscriber support on an interface, specifies the access method used by IP subscribers to connect to ISG on an interface, and enters subscriber configuration mode.
Step 5	initiator radius-proxy Example: Device(config-subscriber)# initiator radius-proxy	Configures ISG to initiate IP sessions upon receipt of any RADIUS packet.
Step 6	end Example: Device(config-subscriber)# end	Exits the subscriber configuration mode and returns to privileged EXEC mode.

Configuring ISG RADIUS Proxy Global Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **pvlan-session reconnect**
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:	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the authentication, authorization and accounting (AAA) access control model.
Step 4	aaa server radius proxy Example: Device(config)# aaa server radius proxy	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	pwan-session reconnect Example: Device(config-locsvr-proxy-radius)# pwan-session reconnect	Enables the Public Wireless LAN (PWLAN) session reconnect feature.
Step 6	session-identifier {attribute <i>number</i> vsa vendor id type <i>number</i> } Example: Device(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 7	calling-station-id format {mac-address msisdn} Example: Device(config-locsvr-proxy-radius)# Calling-Station-ID format msisdn	Specifies the Calling-Station-ID format.
Step 8	accounting method-list {method-list-name default} Example: Device(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 9	accounting port <i>port-number</i> Example: Device(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.

	Command or Action	Purpose
Step 10	authentication port <i>port-number</i> Example: <pre>Device(config-locsvr-proxy-radius)# authentication port 1111</pre>	Specifies the port for which the ISG listens for authentication packets from RADIUS clients. <ul style="list-style-type: none"> • The default port is 1645.
Step 11	key [0 7] <i>word</i> Example: <pre>Device(config-locsvr-proxy-radius)# key radpro</pre>	Configures the encryption key to be shared between ISG and RADIUS clients. <ul style="list-style-type: none"> • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 12	timer { <i>ip-address</i> request } <i>seconds</i> Example: <pre>Device(config-locsvr-proxy-radius)# timer ip-address 5</pre>	Specifies the amount of time for which ISG waits for the specified event before terminating the session.
Step 13	end Example: <pre>Device(config-locsvr-proxy-radius)# end</pre>	Exits the ISG RADIUS proxy server configuration mode and returns to privileged EXEC mode.

Configuring ISG RADIUS Proxy Client-Specific Parameters

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. **pvlan-session reconnect**
7. **session-identifier** {*attribute number* | **vsa vendor id type number**}
8. **calling-station-id format** {*mac-address* | *msisdn*}
9. **accounting method-list** {*method-list-name* | **default**}
10. **accounting port** *port-number*
11. **authentication port** *port-number*
12. **key** [0 | 7] *word*
13. **timer** {*ip-address* | **reconnect** | **request**} *seconds*
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# new-model	Enables the authentication, authorization and accounting(AAA) access control model.
Step 4	aaa server radius proxy Example: Device(config)# aaa server radius proxy	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	client {name ip-address} [subnet-mask [vrf vrf-id]] Example: Device(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	pwan-session reconnect Example: Device(config-locsvr-radius-client)# pwan-session reconnect	Enables the Public Wireless LAN (PWLAN) session reconnect feature.
Step 7	session-identifier {attribute number vsa vendor id type number} Example: Device(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 8	calling-station-id format {mac-address msisdn} Example: Device(config-locsvr-radius-client)# calling-station-id format msisdn	Specifies the Calling-Station-ID format.

	Command or Action	Purpose
Step 9	accounting method-list <i>{method-list-name default}</i> Example: <pre>Device(config-locsvr-radius-client)# accounting method-list fwdacct</pre>	Specifies the server to which accounting packets from RADIUS clients are forwarded.
Step 10	accounting port <i>port-number</i> Example: <pre>Device(config-locsvr-radius-client)# accounting port 2222</pre>	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. <ul style="list-style-type: none"> • The default port is 1646.
Step 11	authentication port <i>port-number</i> Example: <pre>Device(config-locsvr-radius-client)# authentication port 1111</pre>	Specifies the port on which the ISG listens for authentication packets from RADIUS clients. <ul style="list-style-type: none"> • The default port is 1645.
Step 12	key <i>[0 7] word</i> Example: <pre>Device(config-locsvr-radius-client)# key radpro</pre>	Configures the encryption key to be shared between ISG and RADIUS clients. <ul style="list-style-type: none"> • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 13	timer <i>{ip-address reconnect request} seconds</i> Example: <pre>Device(config-locsvr-radius-client)# timer ip-address 5</pre>	Specifies the amount of time ISG waits for the specified event before terminating the session.
Step 14	end Example: <pre>Device(config-locsvr-radius-client)# end</pre>	Exits the ISG RADIUS client configuration mode and returns to privileged EXEC mode.

Defining an ISG Policy for RADIUS Proxy Events

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the AAA access control model.
Step 4	aaa authorization radius-proxy {default list-name} method1 [method2 [method3...]] Example: Device(config)# aaa authorization radius-proxy RP group radius	Configures AAA authorization methods for ISG RADIUS proxy subscribers.
Step 5	policy-map type control policy-map-name Example: Device(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: Device(config-control-policymap-class-control)# 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: Device(config-control-policymap-class-control)# 1 proxy aaa list RP	Sends RADIUS packets to the specified server. <ul style="list-style-type: none"> 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:	Exits the config-control policymap-class-control mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Device (config-control-policy-map-class-control) # end	

Verifying ISG RADIUS Proxy Configuration

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 <i>ip-address</i> [vrf <i>vrf-id</i>] Example: Device# 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 <i>id-number</i> ip <i>ip-address</i> }	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 <i>domain-name</i> authenticated-username <i>username</i> dnis <i>dnis</i> media <i>type</i> nas-port <i>identifier</i> protocol <i>type</i> source-ip-address <i>ip-address subnet-mask</i> timer <i>timer-name</i> tunnel-name <i>name</i> unauthenticated-domain <i>domain-name</i> unauthenticated-username <i>username</i> } uid <i>session-identifier</i> username <i>username</i>] [detailed] Example: Device# show subscriber session detailed	Displays information about subscriber sessions on an ISG device.

Clearing 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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear radius-proxy client ip-address Example: Device# 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: Device# 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.

Examples for Configuring ISG as a RADIUS Proxy

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
!

```

Example: ISG RADIUS Proxy and Layer 4 Redirect

```

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 servicel
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 servicel
!
access-list 101 permit tcp host 10.45.45.2 any

```

The following is sample output from the containing RADIUS proxy details using the **show subscriber session** command, which displays RADIUS proxy details:

```

Device# show subscriber session username 12345675@example

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 "servicel", 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 servicel
Session inbound features:
Feature: Layer 4 Redirect
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: servicel, Active Time = 00:00:40
Interface: FastEthernet0/1, Active Time = 00:00:40

```

Additional References for Configuring ISG as a RADIUS Proxy

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Overview of ISG RADIUS proxy	<i>Configuring Intelligent Service Gateway Configuration Guide</i>

Standards and RFCs

Standard/RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting

Standard/RFC	Title
RFC 2869	RADIUS Extensions

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring ISG as a 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 12: Feature Information for Configuring ISG as a RADIUS Proxy

Feature Name	Releases	Feature Information
RADIUS Proxy Enhancements for ISG	Cisco IOS XE Release 2.2	<p>RADIUS proxy enhancements enable 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.</p> <p>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).</p>

Feature Name	Releases	Feature Information
ISG—AAA Wireless Enhancements	Cisco IOS XE Release 2.5.0	<p>AAA Wireless Enhancements enable ISG RADIUS proxy to provide additional support for mobile wireless environments. It includes changes to RADIUS attribute 31 processing.</p> <p>The following commands were introduced by this feature: session-identifier, calling-station-id format.</p>
ISG—Authentication:RADIUS Proxy WiMax Enhancements	Cisco IOS XE Release 2.5.0	<p>This feature enhances ISG RADIUS proxy to provide additional support for WiMax broadband environments.</p>
ISG—PWLAN Reconnect	Cisco IOS XE Release 3.8S	<p>PWLAN Reconnect enhances user authentication and security while authenticating over PWLAN networks.</p> <p>The following command was introduced by this feature: pwlan-session reconnect.</p>



CHAPTER 9

Configuring ISG as a RADIUS Proxy in Passthrough Mode

Configuring ISG as a RADIUS Proxy in Passthrough Mode allows the Cisco Intelligent Services Gateway (ISG) acting as a RADIUS Proxy to direct all the RADIUS traffic from the client to the RADIUS server, without creating an ISG session.

This module describes how to configure ISG in RADIUS Proxy passthrough mode.

- [Finding Feature Information, on page 129](#)
- [Prerequisites for Configuring ISG as a RADIUS Proxy in Passthrough Mode, on page 129](#)
- [Restrictions for Configuring ISG as a RADIUS Proxy in Passthrough Mode, on page 130](#)
- [Information About Configuring ISG as a RADIUS Proxy in Passthrough Mode, on page 130](#)
- [How to Configure ISG as a RADIUS Proxy in Passthrough Mode, on page 131](#)
- [Configuration Examples for Configuring ISG as RADIUS Proxy in Passthrough Mode, on page 136](#)
- [Additional References for ISG as RADIUS Proxy in Passthrough Mode, on page 137](#)
- [Feature Information for Configuring ISG as a RADIUS Proxy in Passthrough Mode, on page 138](#)

Finding Feature Information

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

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 as a RADIUS Proxy in Passthrough Mode

- You need to configure the authentication and accounting methods.
- You need to configure the AAA server.

Restrictions for Configuring ISG as a RADIUS Proxy in Passthrough Mode

- High availability for RADIUS proxy passthrough is not supported. However, once, the switchover is completed, new sessions are entertained.

Information About Configuring ISG as a RADIUS Proxy in Passthrough Mode

ISG Acting as a RADIUS Proxy Passthrough

The RADIUS proxy module of the Cisco ISG can be run in the passthrough mode to proxy the client's RADIUS traffic. This improves manageability. The RADIUS Proxy passthrough mode can be configured in two ways:

- Global level: You can enable RADIUS proxy passthrough globally by configuring the **mode pass-through** command in the ISG RADIUS proxy server configuration mode. This causes all the clients configured after this command to be in RADIUS Proxy passthrough mode.
- Client level: You can enable RADIUS proxy passthrough at the client level by configuring the **mode pass-through** command for a specific client in the RADIUS proxy client configuration mode.



Note

The ISG interface can also be configured for dual initiators where one initiator can be RADIUS proxy and the other non-RADIUS proxy. When a specified ISG interface having dual initiators receives the non-RADIUS proxy trigger, ISG creates a session for the client. However, if this interface has a client configured to be in RADIUS proxy pass-through mode, it does not create a session when the RADIUS proxy trigger is received. Both these scenarios can co-exist on the same ISG interface.

The RADIUS proxy configuration allows you to configure the accounting method list which specifies the AAA server to which the accounting start, interim and stop records are forwarded. This can be done at both the client level and the global level.

Benefits of Using ISG in RADIUS Proxy Passthrough Mode

- RADIUS proxy passthrough mode offers more security as the AAA server's IP address is hidden from the ultimate host.
- Performance is improved as ISG sessions are not created for RADIUS clients.
- The same ISG can serve in two different modes as listed below:
 - ISG acting as a RADIUS proxy where a session is created and the client's RADIUS messages are sent to an external AAA server.

- ISG acting as a RADIUS proxy passthrough where a session is not created and the client's RADIUS messages are sent to an external AAA server.

How to Configure ISG as a RADIUS Proxy in Passthrough Mode

Enabling RADIUS Proxy Passthrough mode at Global Level

Perform this task to enable the RADIUS proxy passthrough mode globally.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa server radius proxy
5. mode pass-through
6. key [0 | 7] word
7. accounting method-list {method-list-name | default}
8. authentication method-list {method-list-name | default}
9. authentication port port-number
10. accounting port port-number
11. client {name | ip-address} [subnet-mask [vrfvrf-id]]
12. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the authentication, authorization and accounting(AAA) access control model.
Step 4	aaa server radius proxy Example: Device(config)# aaa server radius proxy	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.

	Command or Action	Purpose
Step 5	mode pass-through Example: Device(config-locsvr-proxy-radius)# mode pass-through	Enables ISG RADIUS proxy pass-through mode.
Step 6	key [0 7] word Example: Device(config-locsvr-proxy-radius)# key radprxykey	Configures the encryption key to be shared between ISG and RADIUS clients. <ul style="list-style-type: none"> • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 7	accounting method-list {method-list-name default} Example: Device(config-locsvr-proxy-radius)# accounting method-list SVC_ACCT	Specifies the server to which accounting packets from RADIUS clients are forwarded.
Step 8	authentication method-list {method-list-name default} Example: Device(config-locsvr-proxy-radius)# authentication method-list SVC_ACCT	Specifies the server to which authentication packets from RADIUS clients are forwarded.
Step 9	authentication port port-number Example: Device(config-locsvr-proxy-radius)# authentication port 1645	Specifies the port on which the ISG listens for authentication packets from RADIUS clients. <ul style="list-style-type: none"> • The default port is 1645.
Step 10	accounting port port-number Example: Device(config-locsvr-proxy-radius)# accounting port 1646	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. <ul style="list-style-type: none"> • The default port is 1646.
Step 11	client {name ip-address} [subnet-mask [vrfvrf-id]] Example: Device(config-locsvr-proxy-radius)# client 1.1.1.1	Specifies a RADIUS proxy client for which client-specific parameters can be configured, and enters RADIUS proxy client configuration mode.
Step 12	end Example: Device(config-locsvr-radius-client)# end	Exits the ISG RADIUS proxy client configuration mode and returns to privileged EXEC mode.

Enabling RADIUS Proxy Passthrough mode at Client Level

Perform this task to enable the RADIUS proxy passthrough mode for an individual client.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa server radius proxy
5. client {name | ip-address} [subnet-mask [vrfvrf-id]]
6. mode pass-through
7. key [0 | 7] word
8. accounting method-list {method-list-name | default}
9. authentication method-list {method-list-name | default}
10. authentication port port-number
11. accounting port port-number
12. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the authentication, authorization and accounting(AAA) access control model.
Step 4	aaa server radius proxy Example: Device(config)# aaa server radius proxy	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	client {name ip-address} [subnet-mask [vrfvrf-id]] Example: Device(config-locsvr-proxy-radius)# client 1.1.1.1	Specifies a RADIUS proxy client for which client-specific parameters can be configured, and enters RADIUS proxy client configuration mode.
Step 6	mode pass-through Example: Device(config-locsvr-radius-client)# mode pass-through	Enables ISG RADIUS proxy pass-through mode.
Step 7	key [0 7] word Example:	Configures the encryption key to be shared between ISG and RADIUS clients. <ul style="list-style-type: none">• 0 specifies that an unencrypted key will follow.

	Command or Action	Purpose
	Device(config-locsvr-radius-client)# key radprxykey	<ul style="list-style-type: none"> 7 specifies a hidden key will follow.
Step 8	accounting method-list {method-list-name default} Example: Device(config-locsvr-radius-client)# accounting method-list SVC_ACCT	Specifies the server to which accounting packets from RADIUS clients are forwarded.
Step 9	authentication method-list {method-list-name default} Example: Device(config-locsvr-radius-client)# authentication method-list SVC_ACCT	Specifies the server to which authentication packets from RADIUS clients are forwarded.
Step 10	authentication port port-number Example: Device(config-locsvr-radius-client)# authentication port 1645	Specifies the port for which the ISG listens for authentication packets from RADIUS clients. <ul style="list-style-type: none"> The default port is 1645.
Step 11	accounting port port-number Example: Device(config-locsvr-radius-client)# accounting port 1646	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. <ul style="list-style-type: none"> The default port is 1646.
Step 12	end Example: Device(config-locsvr-radius-client)# end	Exits the ISG RADIUS proxy client configuration mode and returns to privileged EXEC mode.

Verifying ISG RADIUS Proxy Passthrough Sessions

SUMMARY STEPS

1. enable
2. show radius-proxy statistics
3. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	show radius-proxy statistics Example: <pre>Device> show radius-proxy statistics Device> show radius-proxy statistics include access request</pre>	Displays statistics of all RADIUS proxy sessions on the ISG. Note You can also use appropriate output modifiers to display a section of the statistics for all the ISG RADIUS proxy sessions based on the specification.
Step 3	end Example: <pre>Device> end</pre>	Returns to user EXEC mode.

Clearing ISG RADIUS Proxy Statistics

SUMMARY STEPS

1. enable
2. clear radius-proxy statistics
3. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear radius-proxy statistics Example: <pre>Device> clear radius-proxy statistics</pre>	Clears all ISG RADIUS proxy statistics.
Step 3	end Example: <pre>Device> exit</pre>	Returns to user EXEC mode.

Configuration Examples for Configuring ISG as RADIUS Proxy in Passthrough Mode

Example: Configuring Radius Proxy Passthrough Mode

The following example shows how to configure ISG as a RADIUS Proxy passthrough where the interface is configured with dual initiators. Here, an ISG session is not created for the client 10.0.0.2 as it is in passthrough mode whereas a session is created for the client 12.0.0.2 as session creation is triggered by the RADIUS proxy initiator.

```

aaa server radius proxy
message-authenticator ignore
!
client 10.0.0.2
mode pass-through
key radprxykey
accounting method-list SVC_ACCT
authentication port 1645
accounting port 1646

client 12.0.0.2
key radprxykey
accounting method-list SVC_ACCT
authentication method-list SVC_ACCT
authentication port 1647
accounting port 1648

```

Example: Verifying Radius Proxy Passthrough Mode

Use the **show radius-proxy statistics** command to verify that ISG is functioning in RADIUS proxy passthrough mode.

The following is a sample output from the **show radius-proxy statistics** command, showing information for both passthrough and non-passthrough clients.

```

Device#show radius-proxy statistics

NON-PASSTHROUGH CLIENTS
FROM: Client      ISG      AAA
Access Requests: 0         0         0
Access Accepts:  0         0         0
Access Rejects:  0         0         0
Access Challenges 0         0         0
Accounting Requests 0         0         0
Accounting Starts  0         0         0
Accounting Stops   0         0         0
Accounting Updates 0         0         0
Accounting Responses 0         0         0
Accounting ON/OFFS 0         0         0

PASSTHROUGH CLIENTS
FROM: Client      ISG      AAA

```



```

Access Requests:      48000      48000      0
Access Accepts:      0          48000     48000
Access Rejects:      0          0          0
Access Challenges    0          0          0
Accounting Requests  80000     80000     0
Accounting Starts    80000     0          0
Accounting Stops     0          0          0
Accounting Updates   0          0          0
Accounting Responses 0          0          80000
Accounting ON/OFFS   0          0          0

```

Additional References for ISG as RADIUS Proxy in Passthrough Mode

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference
ISG as RADIUS Proxy	"Configuring ISG as a RADIUS Proxy" module in the <i>Intelligent Services Gateway Configuration Guide</i>
RADIUS configurations	"Configuring RADIUS" module in the <i>RADIUS Configuration Guide</i>
ISG Subscriber Service configurations	"Configuring ISG Subscriber Services" module in the <i>Intelligent Services Gateway Configuration Guide</i>
Command Lookup Tool	Command Lookup Tool

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for Configuring ISG as a RADIUS Proxy in Passthrough Mode

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 Configuring ISG as a RADIUS Proxy in Passthrough Mode

Feature Name	Releases	Feature Information
Configuring ISG as a RADIUS Proxy in Passthrough Mode		<p>Configuring the ISG as a RADIUS Proxy in Passthrough Mode allows the Cisco Intelligent Services Gateway (ISG) acting as a RADIUS Proxy to direct all the RADIUS traffic from the client to the RADIUS server, without creating an ISG session.</p> <p>The following commands were introduced: mode pass-thru and authentication method-list list-authen.</p>



CHAPTER 10

ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

The ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering feature allows the Intelligent Services Gateway (ISG) to perform the following:

- Allow the hotspot roaming subscriber to continue accessing the ISG services seamlessly.
- Filter RADIUS packets that are received by the RADIUS proxy server based on the attributes present in the packets.
- [Finding Feature Information, on page 139](#)
- [Restrictions for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering, on page 140](#)
- [Information About ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering, on page 140](#)
- [How to Configure ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering, on page 141](#)
- [Configuration Examples for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering, on page 145](#)
- [Additional References, on page 146](#)
- [Feature Information for ISG RADIUS Proxy Support for Mobile Users: Hotspot Roaming and Accounting Start Filtering, on page 147](#)

Finding Feature Information

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

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 RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Restrictions for RADIUS Proxy Support for Hotspot Roaming

A subscriber is connected to an access point (AP1) that is connected to an Access Zone Router (AZR) (AZR1). The subscriber moves to a different AZR and moves back to a different access point (AP2) within AZR1. When the subscriber tries to reauthenticate with the same IP address that it had for AP1, ISG cannot determine that it is a new session with AP2 and terminates the session when the roaming timer expires.

Restrictions for RADIUS Proxy Support for Accounting Start Filtering

- Configuring RADIUS packet filtering in RADIUS proxy client configuration mode can cause negative impact on the number of RADIUS packets that ISG can process in a second and can bring down calls per second.
- A maximum of four filters can be applied to a single configuration.

Information About ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Hotspot Roaming Timer

When an Extensible Authentication Protocol (EAP)-authenticated subscriber moves from one hotspot to another (hotspot roaming), the subscriber authenticates against a new access point. ISG checks the following conditions to validate if the user has roamed from one hotspot to another:

- The IP address of the access point has changed.
- The user is authenticated.

If the reauthentication on hotspot roaming is successful, the ISG RADIUS proxy server saves the following data in the RADIUS proxy session context:

- The time of reauthentication.
- Authorization data that comes as part of the reauthentication.

If the reauthentication fails, ISG clears the session.

If reauthentication is successful, ISG receives an accounting-start request on the existing session from the new access point, with a different IP address. ISG creates a new RADIUS proxy session for the subscriber with a new IP address and provides seamless roaming by applying the services saved during reauthentication if the following conditions are satisfied:

- The time difference between the arrival of the accounting start request and the reauthentication request is less than the configured IP timer. For more information on IP timers, see the “Configuring ISG RADIUS Proxy Global Parameters” and the “Configuring ISG RADIUS Proxy Client-Specific Parameters” sections in the “Configuring ISG as a RADIUS Proxy” chapter.
- The subscriber is EAP-authenticated.

If the new session is created successfully, a roaming timer is started for the first session. Use the **timer roaming** command in RADIUS proxy server configuration and RADIUS proxy client configuration modes to configure the roaming timer. Once the cleanup timer expires, ISG clears the first session, and the second session remains as the only session for the subscriber.

If the subscriber moves back to the first hotspot before the roaming timer expires on the first session and reauthentication is successful, the roaming timer is stopped for the first session. A new roaming timer is initiated for the second session. If the reauthentication fails, the first session is cleared.

If ISG receives an accounting-stop request for the first session from the AZR to which the session belongs, before the roaming timer expires, the timer is stopped and the first session is cleared. The accounting-stop request is forwarded to the RADIUS server. The response from the RADIUS server is forwarded to the AZR.

If the subscriber roams between multiple hotspots, ISG creates multiple parallel sessions. All these sessions are maintained on ISG until the roaming timer associated with them expires. Only the session that is authenticated last is not associated with a roaming timer.

RADIUS Packet Filter Creation

The RADIUS filter consists of a filter structure and a CLI through which subscribers can configure the filter on RADIUS packets. When a packet is received by ISG, ISG reads the attributes in the packet and matches them with the attributes defined in the filter. Depending on the match criteria that are specified in the filter, ISG takes the defined action on the RADIUS packet.

To create a RADIUS packet filter, follow three steps:

1. Create the RADIUS filter with match criteria.
2. Get the list of standard IETF attributes or vendor-specific attributes from the RADIUS packet that is received.
3. Accept, reject, or ignore the RADIUS packets by applying the filter criteria.

How to Configure ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Configuring a Roaming Timer for the ISG RADIUS Proxy Session

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`

4. `aaa server radius proxy`
5. `timer roaming timer-value`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	aaa server radius proxy Example: Device(config)# aaa server radius proxy	Enters ISG RADIUS proxy server configuration mode.
Step 5	timer roaming timer-value Example: Device(config-locsvr-proxy-radius)# timer roaming 60	Configures a roaming timer for 60 seconds.
Step 6	end Example: Device(config-locsvr-proxy-radius)# end	Returns to privileged EXEC mode.

Configuring RADIUS Proxy Support for Accounting Start Filtering

The Accounting Start Filtering feature allows the creation of RADIUS packet filtering to filter packets that reach ISG. Based on the defined filter criteria, ISG performs certain actions on the RADIUS packet.

The RADIUS packet filter is created on ISG by defining the filter name and the match criteria in the **radius filter** command. The match criteria are applied to the attributes of the RADIUS packet. When you configure the **radius filter match-all** command, the filter is applied to the RADIUS packet only if all the attributes configured in the command match the attributes in the RADIUS packet. When you configure the **radius filter match-any** command, the filter is applied to the RADIUS packet if at least one attribute configured in the

command matches the attributes in the RADIUS packet. The attributes to match are defined in RADIUS filter configuration mode.

In RADIUS filter configuration mode, you can specify a standard IETF RADIUS attribute or a vendor-specific RADIUS attribute. These attributes must match the attributes in the RADIUS packet so that the filter can be applied accordingly. The **match** command checks if the attribute is present in the packet, and the **matchnot** command checks if the attribute is not present in the packet.

Apply RADIUS filters to the RADIUS proxy server in order for the configuration to take effect. Apply RADIUS filters in RADIUS proxy server configuration mode and RADIUS proxy client configuration mode. If filters are applied in both modes, only the client mode configuration will take effect.

You can specify the type of RADIUS packets to which the filter should be applied using the **filter access** and **filter accounting** commands.

You can configure any one of the following three actions that the RADIUS proxy server should apply to the incoming RADIUS packets to complete the filtering process:

- **drop**—Drops the RADIUS packet.
- **ignore**—Forwards the packet to the RADIUS server, but does not apply any ISG-related features to the RADIUS packet.
- **ack**—Returns the access-accept response for the access packet and the accounting response for the accounting packet.

Perform the following tasks to configure a RADIUS packet filter and apply the filter criteria to RADIUS proxy.

Configuring a RADIUS Packet Filter

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius filter match-all** *name*
4. **match attribute** *att-type-number*
5. **matchnot vendor-type** *9*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	radius filter match-all <i>name</i> Example: Device(config)# radius filter match-all filter1	Configures a RADIUS packet filter, defines the condition to filter RADIUS packets if all attributes match, and enters RADIUS filter configuration mode. <ul style="list-style-type: none"> The filter condition is applied only after the attributes are defined in RADIUS filter configuration mode.
Step 4	match attribute <i>att-type-number</i> Example: Device(config-radius-filter)# match attribute 25	Configures a match condition.
Step 5	matchnot vendor-type <i>9</i> Example: Device(config-radius-filter)# matchnot vendor-type 9	Configures a vendor-type match condition.
Step 6	end Example: Device(config-radius-filter)# end	Returns to privileged EXEC mode.

Applying RADIUS Filters to RADIUS Proxy Server or Client

Use the **filter** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode to apply a RADIUS filter. If the RADIUS filter is configured in both these modes, only the filter configured in the client mode will be applied.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **filter access ack** *name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Device(config)# aaa new-model	Enables the AAA access control model.
Step 4	aaa server radius proxy Example: Device(config)# aaa server radius proxy	Enters RADIUS proxy server configuration mode.
Step 5	filter access ack name Example: Device(config-locsvr-proxy-radius)# filter access ack filter1	Acknowledges the RADIUS packet for access requests.
Step 6	end Example: Device(config-locsvr-proxy-radius)# end	Returns to privileged EXEC mode.

Configuration Examples for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Example: Configuring a Roaming Timer for an ISG RADIUS Proxy Session

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# timer roaming 60
```

Example: Configuring a RADIUS Packet Filter

Use the following example along with the example given in the “[Example: Applying RADIUS Packet Filters to RADIUS Proxy Server](#)” section to configure a RADIUS packet filter for the RADIUS proxy server.

The following example shows how to create the RADIUS packet filter, filter1, and define the matching conditions:

```
Device> enable
Device# configure terminal
Device(config)# radius filter match-all filter1
Device(config)# match attribute 25
Device(config)# match attribute 100
Device(config)# matchnot vendor-type 100
```

Example: Applying RADIUS Packet Filters to RADIUS Proxy Server

Use the following example along with the example given in “[Example: Configuring a RADIUS Packet Filter](#)” section to configure a RADIUS packet filter for the RADIUS proxy server.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# filter access ack filter1
```

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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG RADIUS Proxy Support for Mobile Users: Hotspot Roaming and Accounting Start Filtering

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 14: Feature Information for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Feature Name	Releases	Feature Information
ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering	Cisco IOS XE Release 3.5S	<p>The ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering feature allows you to configure hotspot roaming and RADIUS packet filtering for RADIUS proxy sessions.</p> <p>The following commands were introduced or modified: filter (radius-proxy), match (radius-filter), matchnot (radius-filter), radius filter, and timer (ISG RADIUS proxy).</p>



CHAPTER 11

Walk-By User Support in ISG

The Walk-By User Support in ISG feature enables the Cisco Intelligent Services Gateway (ISG) to handle unauthenticated sessions from neighboring devices that do not intend to use the ISG service. These sessions, called walk-by sessions or lite sessions, may be triggered by various initiators.

With the implementation of this feature, unauthenticated users are assigned lite sessions based on the default session. These lite sessions optimize resource usage because they enable the walk-by user to use only session start services mentioned in the default policy configured for the default session.

This module describes how to create and apply a default policy for default sessions to enable the Walk-By User Support in ISG feature.

- [Finding Feature Information, on page 149](#)
- [Prerequisites for Walk-By User Support for PWLANs in ISG, on page 149](#)
- [Restrictions for Walk-By User Support for PWLANs in ISG, on page 150](#)
- [Information About Walk-By User Support for PWLANs in ISG, on page 150](#)
- [How to Configure Walk-By User Support for PWLANs in ISG, on page 151](#)
- [Configuration Examples for Walk-By User Support for PWLANs in ISG, on page 155](#)
- [Additional References, on page 156](#)
- [Feature Information for Walk-By User Support for PWLANs in ISG, on page 156](#)

Finding Feature Information

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

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 Walk-By User Support for PWLANs in ISG

Your implementation of the Cisco software image must support authentication, authorization, and accounting (AAA) and Intelligent Services Gateway (ISG).

Restrictions for Walk-By User Support for PWLANs in ISG

- IPv6 sessions are not supported.
- Only Layer 4 Redirect (L4R), Port-Bundle Host Key (PBHK), and service virtual routing and forwarding (VRF) features are supported. The L4R feature for walk-by session supports only 16 translation entries.
- Lite sessions do not support prepaid, accounting, quality of service (QoS), timers, or RADIUS-timeout features.

Information About Walk-By User Support for PWLANs in ISG

Default Sessions

A default session is a template session that is used as a reference by lite sessions created for walk-by subscribers on a given interface. When an edge device connects to an open service set ID (SSID) in a public wireless LAN (PWLAN) environment a lite session is created on the Intelligent Services Gateway (ISG). Each lite session applies the session start services defined in the default policy configured for the default session. Only one default session can be configured on each device interface. The default policy defines the default session start services and features to be used as a template for the lite session.

Lite Sessions or Walk-By Sessions

In most public wireless LAN (PWLAN) setups, a high percentage of Intelligent Services Gateway (ISG) sessions are unauthenticated sessions from wireless devices that do not use the PWLAN service. These sessions are called walk-by sessions or lite sessions, and users that use these sessions are called walk-by users. Walk-by sessions consume a significant amount of CPU, memory and other physical resources of the ISG router. This resource utilization may lead to an increase in the number of ISG devices that are required for a given PWLAN deployment.

A lite session inherits the session start services applied for the default session. Lite sessions are created on ISG to support walk-by users and optimize resource usage. Each lite session is associated with an individual timer that specifies the duration for which the session can utilize PWLAN services while remaining unauthenticated. If these lite sessions remain unauthenticated even after the timer expires, these sessions are deleted from ISG.

Lite sessions are also created when dedicated sessions fail authentication.

Dedicated Sessions

A dedicated or regular session is a full-fledged Intelligent Services Gateway (ISG) subscriber session. All subscriber sessions that are authenticated cause the creation of dedicated sessions on ISG. The policy manager of ISG decides whether to create a complete session context (a dedicated session) or a minimal session context (a lite session).



Note ISG provides high availability support for converted (lite to dedicated) unclassified and DHCPv4 sessions.

Supported Triggers

Walk-by sessions can be created through any of the following session initiators:

- **Packet trigger:** Here the session creation is triggered by a subscriber's IP packet having an unclassified IP address or MAC address.
- **RADIUS proxy:** This trigger is commonly used in PWLAN deployments where ISG acts as a RADIUS proxy. Here, the session creation is triggered by the subscriber's RADIUS packets.
- **DHCP:** This trigger is another SIP used in a few PWLAN deployments. Here, the session creation is triggered by the subscriber's DHCP control packets.
- **EoGRE walkby:** When ISG is configured for EoGRE, DHCP control packets and unclassified MAC packets on the EoGRE interface trigger session creation on ISG.

Session Limit

The total number of sessions supported on ISG is 128,000. Currently, ISG can support 128,000 lite sessions and 64,000 converted sessions. ISG can also now support 64,000 tunnel endpoints.

How to Configure Walk-By User Support for PWLANs in ISG

Creating and Enabling a Default Policy for a Default Session

Perform this task to create and enable a default policy for a default session on an interface. Each interface can have only one default policy.

A default session is set up to optimize the creation of Intelligent Services Gateway (ISG) sessions for walk-by users. The default session serves as a template that is used by lite sessions for walk-by users. The default policy contains session start services only to which all lite sessions refer. A default policy has the following two functions:

- Identify users who qualify for lite session optimization.
- Identify services or features that need to be applied on default sessions.

SUMMARY STEPS

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

6. **exit**
7. **class-map type traffic match-any** *class-map-name*
8. **match access-group** {*input* | *output*} {*access-list-number* | **name** *access-list-name*}
9. **exit**
10. **policy-map type service** *policy-map-name*
11. [*priority*] **class type traffic** {*class-map-name* | **default** {*in-out* | *input* | *output*}}
12. **redirect to group** {*server-group-name* | **ip** *server-ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]
13. **exit**
14. **exit**
15. **policy-map type control** *policy-map-name*
16. **class type control** {*control-class-name* | **always**} [**event** *session-start*]
17. *action-number* **service-policy type service name** *policy-map-name*
18. *action-number* **service-policy type service name** *policy-map-name*
19. *action-number* **set-timer** *name-of-timer* *minutes*
20. **exit**
21. **exit**
22. **interface** *type number*
23. **service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]}
24. **service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]}
25. **end**
26. **show running-config interface** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: Device(config)# policy-map type service PBHK	Configures a service policy map, and enters service policy-map configuration mode.
Step 4	service local Example: Device(config-service-policymap)# service local	Specifies the local termination service in the ISG service policy map.
Step 5	ip portbundle Example: Device(config-service-policymap)# ip portbundle	Enables the ISG Port-Bundle Host Key (PBHK) feature for the service.

	Command or Action	Purpose
Step 6	exit Example: Device(config-service-policymap)# exit	Returns to global configuration mode.
Step 7	class-map type traffic match-any class-map-name Example: Device(config)# class-map type traffic match-any ALLTRAFFIC	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.
Step 8	match access-group {input output} {access-list-number name access-list-name} Example: Device(config-traffic-classmap)# match access-group input 100	Configures the match criteria for an ISG traffic class map on the basis of the specified access control list (ACL).
Step 9	exit Example: Device(config-traffic-classmap)# exit	Exits traffic class-map configuration mode.
Step 10	policy-map type service policy-map-name Example: Device(config)# policy-map type service L4R	Configures another service policy map, and enters service policy-map configuration mode.
Step 11	[priority] class type traffic {class-map-name default {in-out input output}} Example: Device(config-service-policymap)# class type traffic ALLTRAFFIC	Associates a previously configured ISG traffic class map with a service policy map, and enters service policy-map traffic class configuration mode.
Step 12	redirect to group {server-group-name ip server-ip-address [port port-number]} [duration seconds [frequency seconds]] Example: Device(config-service-policymap-class-traffic)# redirect to group PORTAL	Redirects ISG Layer 4 traffic to a specified server or server group.
Step 13	exit Example: Device(config-service-policymap-class-traffic)# exit	Returns to service policy-map configuration mode.
Step 14	exit Example: Device(config-service-policymap)# exit	Returns to global configuration mode.

	Command or Action	Purpose
Step 15	policy-map type control <i>policy-map-name</i> Example: Device(config)# policy-map type control DefRULE	Creates or modifies a default control policy map, which is used to define a control policy, and enters control policy-map configuration mode.
Step 16	class type control { <i>control-class-name</i> always } [event session-start] Example: Device(config-control-policymap)# class type control always event session-start	Specifies a control class for which actions are configured and enters control policy-map class configuration mode.
Step 17	action-number service-policy type service name <i>policy-map-name</i> Example: Device(config-control-policymap-class-control)# 10 service-policy type service name PBHK	Activates the specified ISG service.
Step 18	action-number service-policy type service name <i>policy-map-name</i> Example: Device(config-control-policymap-class-control)# 20 service-policy type service name L4R	(Optional) Activates another specified ISG service.
Step 19	action-number set-timer <i>name-of-timer minutes</i> Example: Device(config-control-policymap-class-control)# 30 set-timer UNAUTH 1	Starts a named policy timer. <ul style="list-style-type: none">Expiration of the timer initiates the timed-policy-expiry event.
Step 20	exit Example: Device(config-control-policymap-class-control)# exit	Returns to control policy-map configuration mode.
Step 21	exit Example: Device(config-control-policymap)# exit	Returns to global configuration mode.
Step 22	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/4	Specifies an interface and enters interface configuration mode.
Step 23	service-policy type control { <i>policy-map-name</i> default [<i>def-policy-map-name</i>]} Example: Device(config-if)# service-policy type control default DefRULE	Applies a default control policy on the interface.

	Command or Action	Purpose
Step 24	service-policy type control { <i>policy-map-name</i> default [<i>def-policy-map-name</i>]} Example: Device(config-if)# service-policy type control RegRULE	Applies a regular control policy on the interface.
Step 25	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 26	show running-config interface <i>type number</i> Example: Device# show running-config interface GigabitEthernet 0/0/4	(Optional) Displays the running configuration for a specific interface.

Configuration Examples for Walk-By User Support for PWLANs in ISG

Example: Creating and Enabling a Default Policy for a Default Session

The following example shows how to create and enable a default policy named DefRULE on the Gigabit Ethernet interface:

```

Device> enable
Device# configure terminal
Device(config)# policy-map type service PBHK
Device(config-service-policymap)# service local
Device(config-service-policymap)# ip portbundle
Device(config-service-policymap)# exit
Device(config)# class-map type traffic match-any ALLTRAFFIC
Device(config-traffic-classmap)# match access-group input 100
Device(config-traffic-classmap)# exit
Device(config)# policy-map type service L4R
Device(config-service-policymap)# class type traffic ALLTRAFFIC
Device(config-service-policymap-class-traffic)# redirect to group PORTAL
Device(config-service-policymap-class-traffic)# exit
Device(config-service-policymap)# exit
Device(config)# policy-map type control DefRULE
Device(config-control-policymap)# class type control always event session-start
Device(config-control-policymap-class-control)# 10 service-policy type service name PBHK
Device(config-control-policymap-class-control)# 20 service-policy type service name L4R
Device(config-control-policymap-class-control)# 30 set-timer UNAUTH 1
Device(config-control-policymap-class-control)# exit
Device(config-control-policymap)# exit
Device(config)# interface GigabitEthernet 0/0/4
Device(config-if)# service-policy type control default DefRULE
Device(config-if)# service-policy type control RegRULE
Device(config-if)# end

```

The following sample output from the **show running-config interface** command displays the policies configured on the Gigabit Ethernet interface. The default policy configured for default sessions on the Gigabit Ethernet interface is DefRULE, and the regular policy configured for dedicated sessions on the Gigabit Ethernet interface is RegRULE.

```
Device# show running-config interface GigabitEthernet 0/0/4

Building configuration...

Current configuration : 318 bytes
!
interface GigabitEthernet0/0/4
ip address 192.0.2.1 255.255.255.0
negotiation auto
service-policy type control default DefRULE
service-policy type control RegRULE
ip subscriber routed
    initiator unclassified ip-address
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Walk-By User Support for PWLANs in 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 15: Feature Information for Walk-By User Support for PWLANs in ISG

Feature Name	Releases	Feature Information
Walk-By User Support for PWLANs in ISG	Cisco IOS XE Release 3.7S	<p>The Walk-By User Support for PWLANs in ISG feature enables the Intelligent Services Gateway (ISG) that is configured as a RADIUS proxy to handle unauthenticated sessions from wireless devices that do not use the public wireless LAN (PWLAN) service. These sessions are called walk-by sessions.</p> <p>With the implementation of this feature, unauthenticated users are assigned lite sessions based on the default session. These lite sessions optimize resource usage because they enable the walk-by user to use only session start services mentioned in the default policy configured for the default session.</p> <p>The following commands were introduced or modified: clear subscriber lite-session, clear subscriber session, debug subscriber lite-session errors, debug subscriber lite-session events, service-policy type control, show subscriber default-session, and show subscriber statistics.</p>
Walkby session support on EoGRE interface	Cisco IOS XE Release 3.13.1S	This feature enables the Intelligent Services Gateway (ISG) to support walk-by sessions over EoGRE interfaces
HA support for converted (lite to dedicated) sessions	Cisco IOS XE Release 3.13.1S	This feature enables the Intelligent Services Gateway (ISG) to support high availability for converted (lite to dedicated) sessions.



CHAPTER 12

ISG L2 Subscriber Roaming

Subscriber roaming is common in wireless deployments. The ISG L2 Subscriber Roaming feature supports simple IP subscribers connecting to the Cisco Intelligent Services Gateway (ISG) when the subscriber device roams between interfaces, VLANs, or VRFs. This module describes how to configure Layer 2 roaming for simple IPv4 ISG subscribers.

- [Restrictions for ISG L2 Subscriber Roaming, on page 159](#)
- [Information About ISG L2 Subscriber Roaming, on page 159](#)
- [How to Configure ISG L2 Subscriber Roaming, on page 166](#)
- [Configuration Examples for ISG L2 Subscriber Roaming, on page 166](#)
- [Additional References for ISG L2 Subscriber Roaming, on page 167](#)
- [Feature Information for ISG L2 Subscriber Roaming, on page 168](#)

Restrictions for ISG L2 Subscriber Roaming

- Roaming is not supported for dual-stack sessions.
- Roaming is not supported for walk-by subscribers.
- Roaming between interfaces configured with different initiators are not supported.

Information About ISG L2 Subscriber Roaming

ISG Subscriber Roaming

Most devices used in wireless deployments are handheld ones like mobile phones and tablets. It is possible that the same subscriber connects to the Cisco ISG via different access points of the service provider. However, these access points may not always be connected to the ISG over the same VLAN or VRF.

Sometimes, a subscriber with an existing ISG session through a VLAN or VRF, reconnects to the ISG through another VLAN or VRF via a different access point. It is also possible that the VLAN or VRF does not change after the subscriber connects to the access point through the ISG via different physical interfaces or sub-interfaces. This behavior where there is a change in the SSID or access point for a given subscriber is called roaming.

Hence, a roaming subscriber is one who after moving between access points resumes the existing ISG session when it reappears on a new ISG interface.

However, a reconnect subscriber is one who gets a new ISG session when it reappears on the same or different interface. Sometimes, a subscriber who sends a DHCP Discover Packet may also be termed as a reconnect subscriber irrespective of whether it has an existing ISG session or not.

ISG L2 Roaming Events

L2 roaming is now automatically enabled on ISG. When an L2-connected subscriber roams, there may be a change in the session's key parameters. These parameters called session keys are listed below:

- IP Address
- VRF
- Subnet



Note This is applicable to DHCP deployments mostly.

- Initiator
- Control policy

When ISG receives a roaming trigger, it performs one of the following actions on the existing subscriber session:

- **Update:** When the session keys do not change, ISG updates the subscriber to a new access interface. The accounting interim records are sent to the RADIUS server with the updated interface details. Re-authentication may not happen.
- **Reconnect:** When the session keys change, ISG removes the existing session and re-creates a new subscriber session. The control policy is re-applied and the subscriber may be subjected to re-authorization.
- **No change:** When ISG receives DHCP control packets where ISG is neither a DHCP server nor a relay, ISG does not modify the existing session. A session update or reconnect occurs only if the subscriber sends data packets.

ISG L2 Roaming Deployments

Some of the deployments that L2 roaming is currently supported on are listed below:

- Unclassified MAC (External DHCP server)
- DHCP subscribers (DHCP relay)
- DHCP subscribers (DHCP server)
- Hybrid (DHCP with unclassified MAC)

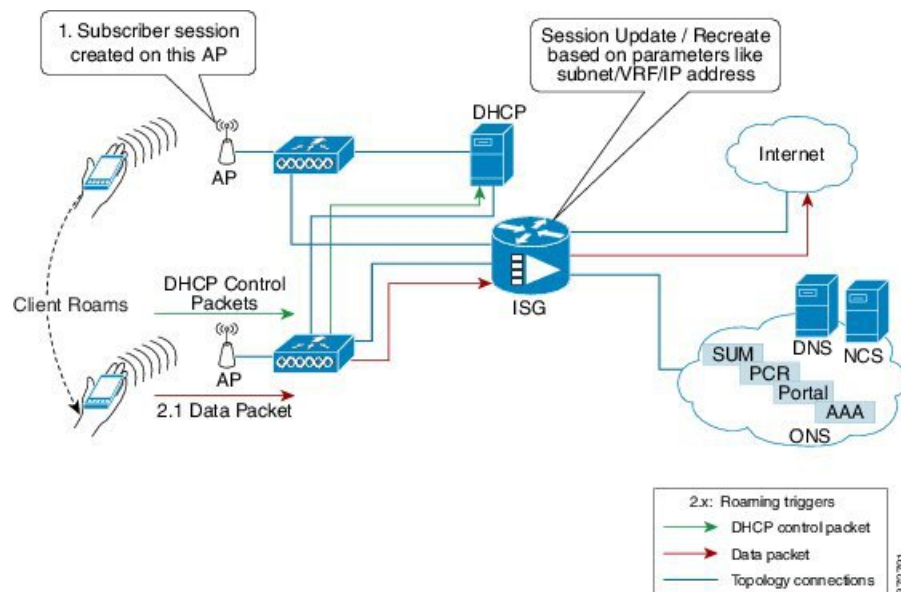
Unclassified MAC (External DHCP server)

For the external DHCP server model, ISG sessions are mainly created by unclassified packets, where the session identifiers will be the MAC address and IP address. The roaming triggers for this model are listed below:

Table 16: Simple IP L2-Connected Unclassified MAC Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP control packets (DHCP Discover, DHCP Request, Init Bootp)	No
Data packets	Yes

Figure 5: Simple IP L2-Connected Unclassified MAC Roaming



DHCP subscribers (DHCP relay)

For the DHCP relay model, the ISG sessions are mainly created by DHCP control packets. Here, the ISG relays these packets to the DHCP server and forwards the response received from the server back to the client. In this scenario, the subscriber that has roamed to a new interface may trigger one of the following session initiator packets:

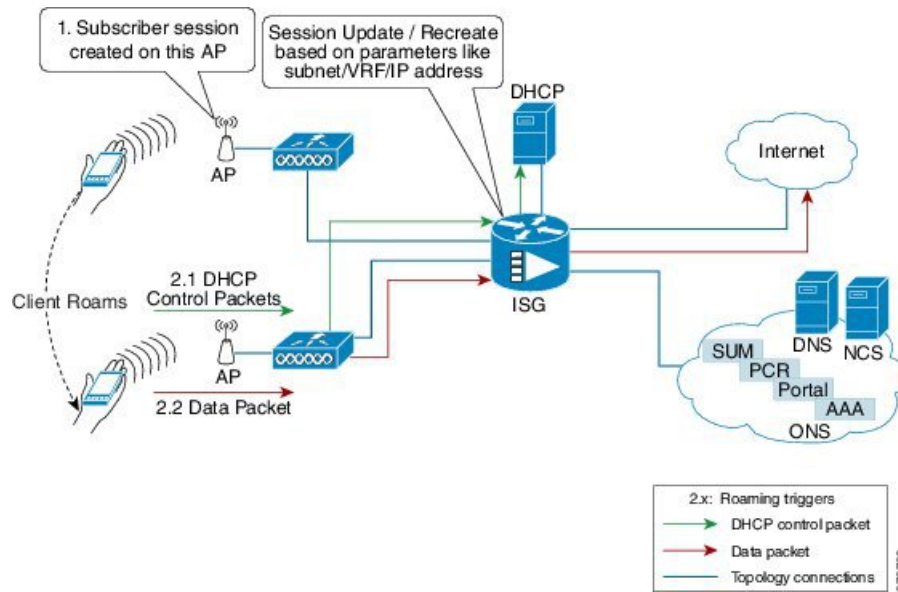
- Data packet if the subscriber has an existing IP address
- DHCP Renew control packet if the IP address needs to be renewed
- DHCP Discover control packet

The roaming triggers for the DHCP relay deployment are listed below:

Table 17: Simple IP L2-Connected (Dual Initiator) DHCP Relay with Unclassified MAC Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP Control Packets (DHCP Discover, DHCP Request, Init Bootp)	Yes
Data Packets	Yes

Figure 6: Simple IP L2-Connected (Dual Initiator) DHCP Relay with Unclassified MAC Roaming



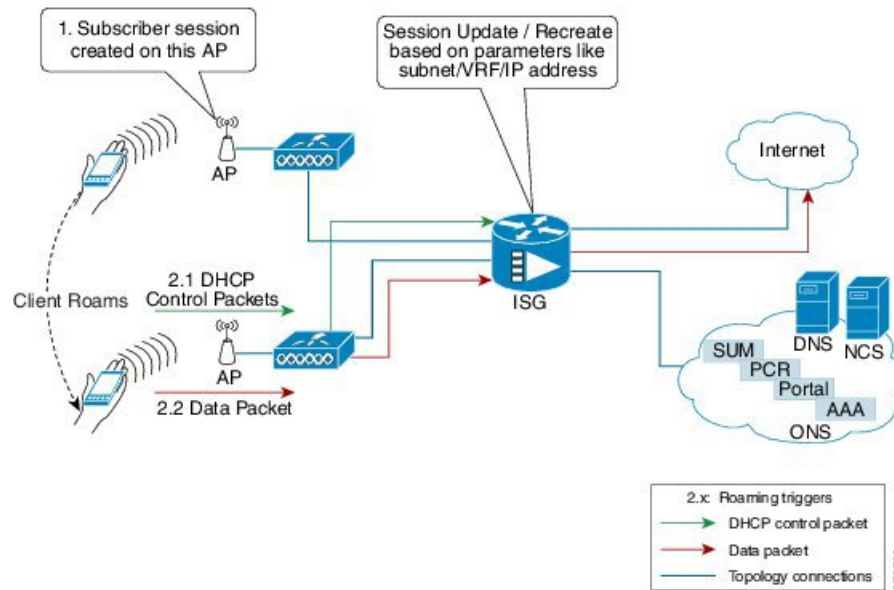
DHCP subscribers (DHCP server)

For the DHCP server deployment, ISG acts as a DHCP server. The roaming triggers for this model are listed below:

Table 18: Simple IP L2-Connected (Dual Initiator) DHCP Server with Unclassified MAC Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP Control Packets (DHCP Discover, DHCP Request, Init Bootp)	Yes
Data Packets	Yes

Figure 7: Simple IP L2-Connected (Dual Initiator) DHCP Server with Unclassified MAC Roaming



Hybrid (DHCP with unclassified MAC)

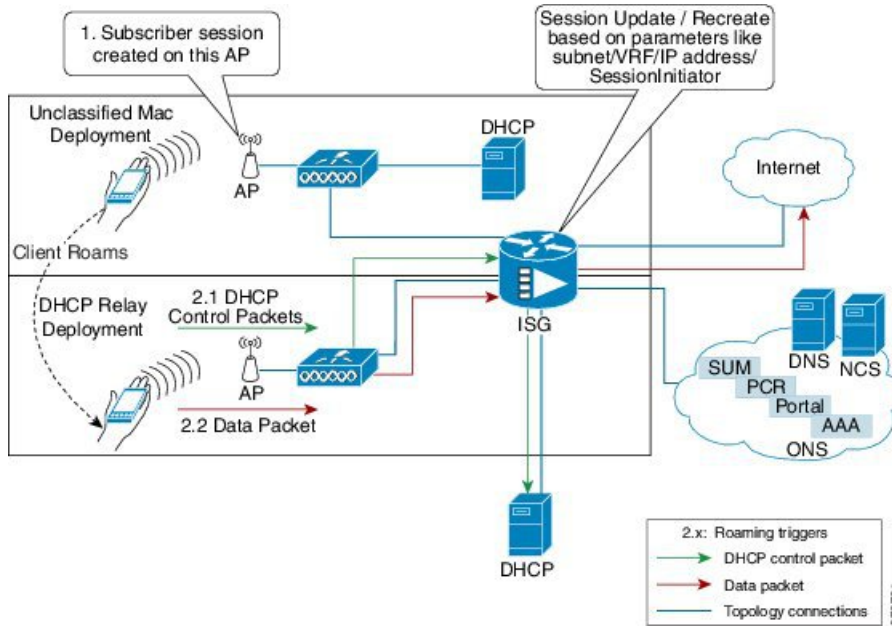
For the L2-connected hybrid model, the roaming triggers are listed below:

Table 19: Simple IP L2-Connected Hybrid (DHCP with unclassified MAC) Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP control packets (DHCP Discover, DHCP Request, Init Bootp)	Yes ¹
Data packets	Yes

¹ DHCP control packets are considered as roaming triggers when the subscriber moves from unclassified MAC to DHCP deployments.

Figure 8: Simple IP L2-Connected Hybrid (DHCP with unclassified MAC) Roaming



ISG L2 Roaming Behavior

Table 20: Roaming behavior in ISG

Deployment Type	Client roams with different roaming triggers		Client roams and with changed network conditions	ISG Roaming Behavior	Client/System Behavior
	Packet	Roaming Trigger			
L2-connected unclassified MAC	GARP/ ARP	No	<ol style="list-style-type: none"> 1. IP Address 2. Subnet 3. VRF 4. Control Policy 	<ol style="list-style-type: none"> 1. Session recreate 2. Session update 3. Session recreate 4. Session recreate 	<ol style="list-style-type: none"> 1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized.
	DHCP control packets	No			
	Data packet	Yes			

Deployment Type	Client roams with different roaming triggers		Client roams and with changed network conditions	ISG Roaming Behavior	Client/System Behavior
	Packet	Roaming Trigger			
L2-connected (Dual Initiator) DHCP Relay with Unclassified MAC	GARP/ARP	No	<ol style="list-style-type: none"> 1. IP Address 2. Subnet 3. VRF 4. Control Policy 	<ol style="list-style-type: none"> 1. Session recreate. 2. Session update/recreate² 3. Session recreate. 4. Session recreate. 	<ol style="list-style-type: none"> 1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized.
	DHCP control packets	Yes			
	Data packet	Yes			
L2-Connected (Dual Initiator) DHCP Server with Unclassified MAC	GARP/ARP	No	<ol style="list-style-type: none"> 1. IP Address 2. Subnet 3. VRF 4. Control Policy 	<ol style="list-style-type: none"> 1. Session recreate. 2. Session update/recreate.³ 3. Session recreate 4. Session recreate 	<ol style="list-style-type: none"> 1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized.
	DHCP control packets	Yes			
	Data packet	Yes			
L2-Connected (Hybrid) DHCP Relay or Server with Unclassified MAC	GARP/ARP	No	<ol style="list-style-type: none"> 1. IP Address 2. Subnet 3. VRF 4. Control Policy 5. Initiator 	<ol style="list-style-type: none"> 1. Session recreate 2. Session update/recreate⁴ 3. Session recreate 4. Session recreate 5. Session recreate 	<ol style="list-style-type: none"> 1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized. 5. Client will be re-authorized.
	DHCP control packets	Yes (based on network conditions)			
	Data packet	Yes			

² DHCP control packets may trigger session recreate.

³ DHCP control packets may trigger session recreate.

⁴ Based on initiator, the session may be updated or recreated.

How to Configure ISG L2 Subscriber Roaming

Enabling Roaming for Simple IP Subscribers

Depending upon network design, subscribers may roam between interfaces, VLANs or VRFs.



Note Simple IP subscriber roaming is enabled by default. Hence, the `ip subscriber l2-roaming` command need not be configured to support roaming.

Configuration Examples for ISG L2 Subscriber Roaming

Example: Verifying L2 Roaming on ISG

Use the `show ip subscriber mac mac_address` command to verify that the ISG subscriber has successfully roamed to a new interface.

The following are sample outputs from the `show ip subscriber mac mac_address` command where the subscriber's session is updated due to roaming. On comparing the access interface parameter in both the outputs, you can see that it has changed indicating that the subscriber has roamed.

Before Roaming

```
Device# show ip subscriber mac aabb.cc01.9000

IP subscriber: aabb.cc01.9000, type connected, status up
display uid: 1, aaa uid: 12
segment id: 4098, session hdl: 0xF4000001, shdb: 0x3E000001
session initiator: unclassified traffic
access interface: Ethernet0/0.10 # Note access interface
access address: 1.1.1.2
service address: 1.1.1.2
status: IPv4 - Up IPv6 - Down
conditional debug flag: 0x0
control plane state: connected, start time: 00:00:04
data plane state: connected, start time: 00:00:04
arp entry: 1.1.1.2, Ethernet0/0.10
forwarding statistics:
  packets total: received 8, sent 7
  bytes total: received 944, sent 798
  packets dropped: 0, bytes dropped: 0
hardware forwarding statistics:
  packets total: received 0, sent 0
  bytes total: received 0, sent 0
```

After Roaming

```
Device# show ip subscriber mac aabb.cc01.9000
```

```

IP subscriber: aabb.cc01.9000, type connected, status up
  display uid: 1, aaa uid: 12
  segment id: 4098, session hdl: 0xF4000001, shdb: 0x3E000001
  session initiator: unclassified traffic
  access interface: Ethernet0/0.20 # Change in access interface
  access address: ::
  service address: ::
  access address: 1.1.1.2
  service address: 1.1.1.2
  status: IPv4 - Up IPv6 - Down
  conditional debug flag: 0x0
  control plane state: connected, start time: 00:00:52
  data plane state: connected, start time: 00:00:52
  arp entry: 1.1.1.2, Ethernet0/0.20
  route: 1.1.1.2 -> Ethernet0/0.20
  forwarding statistics:
    packets total: received 18, sent 17
    bytes total: received 2124, sent 1938
    packets dropped: 0, bytes dropped: 0
  hardware forwarding statistics:
    packets total: received 0, sent 0
    bytes total: received 0, sent 0

```

Additional References for ISG L2 Subscriber Roaming

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for ISG L2 Subscriber Roaming

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 L2 Subscriber Roaming

Feature Name	Releases	Feature Information
ISG L2 Subscriber Roaming	Cisco IOS XE Release 3.12S	Subscriber roaming is common in wireless deployments. The ISG L2 Subscriber Roaming feature supports simple IP subscribers connecting to the Cisco Intelligent Services Gateway (ISG) when the device roams between interfaces, VLANs or VRFs. The following command was deprecated: ip subscriber l2-roaming .



CHAPTER 13

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, on page 169](#)
- [Prerequisites for RADIUS-Based Policing, on page 169](#)
- [Restrictions for RADIUS-Based Policing, on page 169](#)
- [Information About RADIUS-Based Policing, on page 170](#)
- [How to Configure RADIUS-Based Policing, on page 174](#)
- [Configuration Examples for RADIUS-Based Policing, on page 179](#)
- [Additional References, on page 186](#)
- [Feature Information for RADIUS-Based Policing, on page 186](#)

Finding Feature Information

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

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.
- 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.
- Ensure that the classmap name specified for a policy-map configuration used to create pACL and class-map does not contain an hyphen (-) character.

Information About RADIUS-Based Policing

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

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

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. 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.

HA Support for RADIUS-Based Policing

The ISG Policy HA and RADIUS-Based Policing HA feature adds stateful switchover (SSO) and In Service Software Upgrade (ISSU) support to ISG RADIUS-Based Policing for QoS parameterization that is configured through template services.

For information about modifying QoS policy maps by using template services, see the “QoS Policy Accounting” module in the [QoS: Policing and Shaping Configuration Guide, Cisco IOS XE Release 3S](#).

For information about configuring High Availability (HA) on the ISG router, see the [High Availability Configuration Guide, Cisco IOS XE Release 3S](#).

How to Configure RADIUS-Based Policing

Configuring per-Session Shaping

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. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: Router(config)# policy-map child	Creates or modifies a policy-map and enters QoS policy-map configuration mode.
Step 4	class <i>class-default</i> Example: Router(config-pmap)# class class-default	Modifies the class-default traffic class and enters QoS policy-map class configuration mode.
Step 5	shape average <i>mean-rate</i> [<i>burst-size</i>] [<i>excess-burst-size</i>] [account { <i>qinq</i> <i>dot1q</i> user-defined <i>offset</i> } <i>aal5</i> <i>subscriber-encap</i>] Example: Router(config-pmap-c)# shape average 10000	Shapes traffic to the indicated bit rate.
Step 6	service-policy <i>policy-map-name</i> Example:	Applies the child policy map to the parent class-default class.

	Command or Action	Purpose
	<code>Router(config-pmap-c)# service-policy child</code>	<ul style="list-style-type: none"> <i>policy-map-name</i>—Name of the child policy map.
Step 7	end Example: <code>Router(config-pmap-c)# end</code>	Exits QoS policy-map class configuration mode and returns to privileged EXEC mode.

Configuring per-Session Shaping on RADIUS

Example

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

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: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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 <i>policy-map-name</i> Example: Router(config)# policy-map child	Creates or modifies a policy map and enters policy-map configuration mode.
Step 4	class <i>class-name</i> Example: Router(config-pmap)# class voip	Configures QoS parameters for the traffic class you specify and enters policy-map class configuration mode. <ul style="list-style-type: none"> <i>class-name</i> —Name of a traffic class you previously configured using the class-map command.
Step 5	shape average <i>mean-rate</i> [<i>burst-size</i>] [<i>excess-burst-size</i>] [account {qinq dot1q user-defined <i>offset</i>} aal5 <i>subscriber-encap</i>] Example: Router(config-pmap-c)# shape average 10000	Shapes traffic to the indicated bit rate.
Step 6	police <i>bps</i> [<i>burst-normal</i>] [<i>burst-max</i>] conform-action <i>action</i> exceed-action <i>action</i> [violate-action <i>action</i>] 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. <ul style="list-style-type: none"> • 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.
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. <ul style="list-style-type: none"> • <i>policy-map-name</i> —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	Purpose
show policy-map interface	Displays the configuration of all classes configured for all policy maps attached to all interfaces.
show policy-map interface <i>interface [input output]</i>	Displays the configuration of all classes configured for all inbound or outbound policy maps attached to the specified interface. <ul style="list-style-type: none"> • <i>interface</i> 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.
show policy-map <i>policy-map-name</i>	Displays the configuration of all of the traffic classes contained in the policy map you specify. <ul style="list-style-type: none"> • <i>policy-map-name</i> is the name of the policy map for the configuration information you want to appear. • If you do not specify a value for the <i>policy-map-name</i> argument, the command shows the configuration of all policy maps configured on the router.

Command	Purpose
show policy-map <i>policy-map-name class</i> <i>class-name</i>	Displays the configuration of the class you specify. The policy map you specify includes this class. <ul style="list-style-type: none"> • <i>policy-map-name</i> is the name of the policy map that contains the class configuration you want to appear. • <i>class-name</i> is the name of the class whose configuration you want to. If you do not specify a value for the <i>class-name</i> argument, the command shows the configuration of all of the classes configured in the policy map.
show policy-map session [output output <i>uid</i>]	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. <ul style="list-style-type: none"> • input indicates inbound policy maps. • output indicates outbound policy maps. • <i>uid</i> is the session ID.
show running-config	Displays the running-configuration file, which contains the current configuration of the router, including the default QoS policy.
show running-config interface <i>interface</i>	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

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
```

Example: Adding Parameterization of QoS ACLs

```

!
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 Cisco VSA configured in the user's profile above 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

```

Example: Setting the Policing Rate Using a CoA Message

```
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 Cisco VSA configured in the user profile above 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
HA commands	Cisco IOS High Availability Command Reference
HA configuration	High Availability Configuration Guide
QoS Policy Configuration	QoS: Policing and Shaping Configuration Guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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 22: 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.
ISG Policy HA and RaBaPol HA	Cisco IOS XE Release 3.5S	Adds SSO and ISSU support to ISG RADIUS-based policing.



CHAPTER 14

ISG Dynamic VLAN Interface Provisioning

The ISG Dynamic VLAN Interface Provisioning feature enables the automatic creation of VLAN interfaces based on the VLAN packet trigger. The VLAN interface configuration is downloaded from the RADIUS server. This module describes how to enable ISG to dynamically configure VLAN interfaces for simple IP sessions.

- [Finding Feature Information, on page 189](#)
- [Prerequisites for ISG Dynamic VLAN Interface Provisioning, on page 189](#)
- [Restrictions for ISG Dynamic VLAN Interface Provisioning, on page 190](#)
- [Information About ISG Dynamic VLAN Interface Provisioning, on page 190](#)
- [Configuration Examples for ISG Dynamic VLAN Interface Provisioning, on page 192](#)
- [Additional References for ISG Dynamic VLAN Interface Provisioning, on page 196](#)
- [Feature Information for ISG Dynamic VLAN Interface Provisioning, on page 196](#)

Finding Feature Information

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

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 Dynamic VLAN Interface Provisioning

- Disable VLAN filtering on the corresponding SPAs by using the **hw-module subslot [m/n] ethernet vlan unlimited** command.



Note Although disabling this command avoids dropping of unknown VLAN tags, it affects other features that use VLAN filtering. For example, some QoS features like dot1p do not work when this command is disabled.

Restrictions for ISG Dynamic VLAN Interface Provisioning

- After provisioning a DVLAN interface, it is not advised to write memory as this will disable removal of the DVLAN interface.
- It is not advised to manually delete a dynamically provisioned interface. This should be done only with CoA or by using the **clear vlan-autoconfig interface** command.



Note You can delete up to a maximum of 200 interfaces using the **clear vlan-autoconfig interface** command.

- Semantic errors encountered during shell-map execution are not handled.
- You can only configure up to 64000 VLANs per system in the Cisco ASR 1000 Series Aggregation Services Routers. The following table lists the VLAN scale restrictions for the Cisco ASR 1000 Series Aggregation Services Routers RP2 and ESP40 platform with 8GB memory.

Platform Scalability	ASR 1000 RP2+ESP40
	8GB RP2
Number of VLANs per port	4000
Number of VLANs per SPA	8000 32000 with VLAN unlimited
Number of VLANs per system	64000
Number of QinQ VLANs per port	4000
Number of QinQ VLANs per SPA	8000 32000 with VLAN unlimited
Number of QinQ VLANs per system	64000

Information About ISG Dynamic VLAN Interface Provisioning

Overview of ISG Dynamic VLAN Interface Provisioning

This feature simplifies the VLAN sub-interface configuration by downloading the configuration details from a RADIUS-based server. These details are based on the VLAN tag of the first packet coming on the access interface. Any FSOL with a VLAN tag can bring up the dynamic VLAN interface. The configuration that is downloaded is defined in the shell map and the shell map parameters are passed through RADIUS during *Access Accept*. To de-provision the interface, you need to do it manually through CoA only.

Benefits of ISG Dynamic VLAN Provisioning

Some benefits of automatically dynamic VLAN provisioning on the Cisco ISG interface are listed below:

- You need not manually configure the VLAN sub-Interfaces on the device.
- Dynamic VLAN provisioning reduces maintenance time due to simplified operations.
- Performance is improved as the VLAN interface configurations are not included in the startup configuration.

IOS Shell Maps and Usage

The VLAN interface configuration for different VLANs is similar except that for the set of interface-specific parameters that need to be configured. These interface-specific parameters are downloaded from the RADIUS server.

The interface configuration commands are merged together in the IOS shell map to serve as a template. This template contains IOS CLI commands where the interface-specific parameters are replaced by shell variables. To configure a specific VLAN interface, the shell map is invoked with the appropriate parameters that replace these shell map variables.

The following steps describe how to use shell maps:

- Define the IOS shell map on the router through CLI.
- Configure this shell map name along with the VLAN interface configuration parameters on the RADIUS server for a specific VLAN ID.
- The VLAN interface configuration module downloads the specified IOS shell map along with the appropriate VLAN interface configuration parameters from the RADIUS server.
- The VLAN interface configuration module triggers the corresponding shell map with the appropriate number of parameters.
- Ensure that the number of configuration parameters for a specific VLAN matches the number of variables expected by the corresponding shell map.

The various scenarios of parameter mismatch are listed below:

- If the number of parameters are more, the extra parameters shall be ignored.
 - If the RADIUS server does not provide all the required parameters, a configuration error occurs.
 - If the RADIUS message carries a shell function name that does not exist on the device, a configuration error occurs.
- Configure separate IOS shell maps for each VLAN.
 - Use the RADIUS CoA to change the VLAN interface configuration. Here, the CoA contains the IOS shell map name to be used along with the desired parameters.
 - The IOS shell infrastructure synchronizes the active and standby IOS shell maps.

Configuration Examples for ISG Dynamic VLAN Interface Provisioning

Example: Configuring ISG Dynamic VLAN Interface Provisioning

```

sh running-config
Building configuration...

Current configuration : 5262 bytes
!
! Last configuration change at 19:15:51 IST Mon Jun 30 2014
!
version 15.5
service timestamps debug uptime
service timestamps log datetime msec localtime show-timezone
no platform punt-keepalive disable-kernel-core
!
hostname UUT
!
boot-start-marker
boot system harddisk:asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20140618_050043_2.bin
boot-end-marker
!
shell map PROFILE20 {
  conf t
  interface GigabitEthernet0/0/4.$sub_if
  encapsulation dot1q $outer_vlan second-dot1q $in_vlan
  ip address $ip 255.255.255.0
  pppoe enable group global
  end
}
shell map PROFILE33 {
  conf t
  interface Port-channel30.$sub_if
  encap dot1q $outer_vlan second-dot1q $cvlan
  ip address $ip 255.255.255.0
  pppoe enable group global
  end
}
shell trigger PROFILE20 PROFILE20
shell trigger PROFILE33 PROFILE33
shell trigger rate rate
aqm-register-fnf
!
aaa new-model
!
!
aaa authentication enable default none
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
!
!
!
aaa server radius dynamic-author
  client 9.0.0.134 server-key coa

```



```
!  
aaa session-id common  
clock timezone IST 5 30  
!  
!  
!  
!  
!  
!  
!  
!  
!  
no ip domain lookup  
  
!  
!  
!  
!  
!  
!  
!  
!  
!  
vlan-autoconfig authorize list default password cisco  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
hw-module subslot 0/0 ethernet vlan unlimited  
spanning-tree extend system-id  
!  
username lab password 0 lab  
username CPE password 0 lab  
!  
redundancy  
  mode sso  
!  
!  
!  
!  
!  
ip tftp source-interface GigabitEthernet0/0/0  
ip tftp blocksize 8192  
!  
!  
!  
!  
!  
bba-group pppoe global  
  virtual-template 1  
!  
!  
interface Loopback1
```

Example: Configuring ISG Dynamic VLAN Interface Provisioning

```

ip address 2.2.2.1 255.255.255.0
!
interface Port-channel30
no ip address
no negotiation auto
!
interface GigabitEthernet0/0/4
ip address 5.5.5.1 255.255.0.0
negotiation auto
vlan-autoconfig
!
interface Virtual-Template1
ip unnumbered Loopback1
peer default ip address pool pool1
ppp authentication chap
!
ip local pool pool1 2.2.2.2 2.2.2.100
ip default-gateway 9.27.0.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 9.0.0.134 255.255.255.255 9.27.0.1
ip route 10.64.67.0 255.255.255.0 9.27.0.1
ip route 10.105.37.142 255.255.255.255 10.64.67.1
ip route 202.153.144.25 255.255.255.255 9.27.0.1
!
ip access-list extended A
permit ip any any
!
access-list 10 permit any
!
!
!
radius-server host 9.0.0.134 key cisco
no radius-server vsa send accounting
no radius-server vsa send authentication
!
!
control-plane
!
!
!
!
!
!
!
alias exec svcs show vlan-autoconfig summary
alias exec svv show vlan-autoconfig vlan
alias exec sva show vlan-autoconfig access
alias exec stat show vlan-autoconfig statistics
alias exec punt_pol show platform software punt-policer | i Auto
alias exec punt_infra show platform software infrastructure punt | i Auto
alias exec punt_qfp show platform hardware qfp a infrastructure punt policer
alias exec cvs clear vlan-autoconfig stat
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4

```

```

transport input all
!
!
!
end

```

Example: Configuring RSIM

VLAN Sub-Interface Creation from Radius

```

simulator radius server 10.0.1.2
Subscriber profiles for creating sub interfaces
user-name prefix Ethernet0/0:12 subscriber 26
user-name prefix Ethernet0/0:11 subscriber 25
user-name prefix Ethernet0/0:10 subscriber 24
Subscriber profile 24 25 26 are defined for creating virtual interface
simulator radius subscriber 24
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-service-info=PROFILE1(vlan=10; ip=1.1.1.1)"
!
simulator radius subscriber 25
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-service-info=PROFILE1(vlan=11; ip=2.2.2.2)"
!
simulator radius subscriber 26
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-service-info=PROFILE1(vlan=12; ip=3.3.3.3)"
!

```

VLAN Sub-Interface Deletion from Radius

```

Simulator radius subscriber 101
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-subinterface-id=10"
vsa cisco generic 1 string "subscriber:command=vlan-autoconfig-delete"
attribute 87 string "Ethernet0/0"
!
simulator radius subscriber 102
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-subinterface-id=11"
vsa cisco generic 1 string "subscriber:command=vlan-autoconfig-delete"
attribute 87 string "Ethernet0/0"
!
simulator radius subscriber 103
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-subinterface-id=12"
vsa cisco generic 1 string "subscriber:command=vlan-autoconfig-delete"
attribute 87 string "Ethernet0/0"
Push the following subscriber profile from rsim as given below to delete a Sub interface
simulator radius request 1 coa 101
simulator radius request 1 coa 102
simulator radius request 1 coa 103

```

Additional References for ISG Dynamic VLAN Interface Provisioning

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for ISG Dynamic VLAN Interface Provisioning

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 ISG Dynamic VLAN Provisioning

Feature Name	Releases	Feature Information
ISG Dynamic VLAN Provisioning		<p>The ISG Dynamic VLAN Interface Provisioning feature enables the automatic creation of VLAN interfaces based on the VLAN packet trigger. The VLAN interface configuration is downloaded from the RADIUS server.</p> <p>The following command was introduced: vlan-autoconfig.</p>



CHAPTER 15

Ambiguous VLAN Support for IP sessions over ISG

The Ambiguous VLAN Support for IP Sessions over ISG feature allows network service providers to define a range or ranges of inner VLANs and create queue-in-queue (QinQ) VLANs on demand. This is done by specifying a range for the inner VLAN tag in the IEEE 802.1Q-in-Q while maintaining a single outer VLAN tag for each subinterface. This module explains the Ambiguous VLAN Support for IP Sessions over ISG feature and how to configure it.

- [Finding Feature Information, on page 197](#)
- [Restrictions for Ambiguous VLAN Support for IP Sessions over ISG, on page 197](#)
- [Information About Configuring Ambiguous VLAN Support for IP Sessions over ISG, on page 198](#)
- [Configuring Ambiguous VLAN Support for IP Sessions over ISG, on page 198](#)
- [Verifying Ambiguous VLAN Support for IP Sessions over ISG Configuration, on page 199](#)
- [Additional References for Ambiguous VLAN Support for IP Sessions over ISG, on page 199](#)
- [Feature Information for Ambiguous VLAN Support for IP Sessions over ISG, on page 200](#)

Finding Feature Information

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

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 Ambiguous VLAN Support for IP Sessions over ISG

- Ambiguous VLANs are currently supported only for Intelligent Services Gateway (ISG) sessions.
- IP sessions and PPP sessions are not supported on the same ambiguous subinterfaces. Hence, different ranges need to be specified for the outer VLAN tags for both IP sessions and PPP sessions.

- Only a limited feature set will be applied to each queue-in-queue (QinQ) pair as no subinterfaces are created for each QinQ pair. The available features include those applicable to the ISG session and those applicable to the ambiguous VLAN interface.
- This feature is restricted to Layer 2 unclassified MAC and DHCP-initiated ISG sessions.
- IPv6 sessions are not supported.
- This feature supports only Ethertype 0x8100. Other Ethertypes such as 0x88A8, 0x9100 and 0x9200 are not supported.
- This feature does not support Virtual Routing and Forwarding (VRF).

Information About Configuring Ambiguous VLAN Support for IP Sessions over ISG

Benefits of Ambiguous VLAN Support for IP Sessions over ISG

Ambiguous VLAN implementation for IP sessions in Intelligent Services Gateway (ISG) has the following benefits:

- The service provider only needs to know the end-user VLAN ranges instead of the individual end-user VLAN IDs.
- The ambiguous VLAN feature allows the configuration of multiple VLANs under one subinterface which leads to better Interface Descriptor Block (IDB) utilization.

Configuring Ambiguous VLAN Support for IP Sessions over ISG

You can define a range of inner VLANs and create QinQ VLANs, or you can use the keyword **any** for the system to assign any inner VLAN ID that has not been used elsewhere.

To configure a range of inner VLANs:

```
configure terminal
interface GigabitEthernet1/0.200
 encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000
```

or

```
configure terminal
interface GigabitEthernet1/0.200
 encapsulation dot1q 200 second-dot1q 1000-2000
```

To configure the sub-interface for ambiguous VLAN:

```
configure terminal
interface GigabitEthernet1/0.200
 encapsulation dot1q 200 second-dot1q any
```

Verifying Ambiguous VLAN Support for IP Sessions over ISG Configuration

Use **show subscriber session** command to verify the configuration of Ambiguous VLAN Support for IP Sessions over ISG feature.

```
Device# show subscriber session uid 6

Type: IP, UID: 6, State: unauthen, Identity: 12.12.12.2
IPv4 Address: 12.12.12.2
Session Up-time: 00:00:34, Last Changed: 00:00:34
Switch-ID: 8221

Policy information:
  Authentication status: unauthen

Classifiers:
Class-id   Dir   Packets   Bytes           Pri.  Definition
0          In    4         488             0    Match Any
1          Out   4         488             0    Match Any

Configuration Sources:
Type  Active Time  AAA Service ID  Name
INT  00:00:34    -              GigabitEthernet0/1/3.1
```

Additional References for Ambiguous VLAN Support for IP Sessions over ISG

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 to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/c/en/us/support/index.html

Feature Information for Ambiguous VLAN Support for IP Sessions over 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 24: Feature Information for Ambiguous VLAN Support for IP Sessions over ISG

Feature Name	Releases	Feature Information
Ambiguous VLAN Support for IP Sessions over ISG	Cisco IOS XE Release 3.8S	<p>The Ambiguous VLAN Support for IP Sessions over ISG feature allows network service providers to define a range or ranges of inner VLANs and create queue-in-queue (QinQ) VLANs on demand. This is done by specifying a range for the inner VLAN tag in the IEEE 802.1Q-in-Q while maintaining a single outer VLAN tag for each subinterface. This module explains the Ambiguous VLAN Support for IP Sessions over ISG feature and how to configure it.</p> <p>The following commands were introduced or modified by this feature: encapsulation dot1q.</p>



CHAPTER 16

Configuring ISG Policies for Automatic Subscriber Logon

Intelligent Services Gateway (ISG) is a 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, on page 201](#)
- [Prerequisites for ISG Automatic Subscriber Logon, on page 201](#)
- [Restrictions for ISG Automatic Subscriber Logon, on page 202](#)
- [Information About ISG Automatic Subscriber Logon, on page 202](#)
- [How to Configure ISG Policies for Automatic Subscriber Logon, on page 203](#)
- [Configuration Examples for ISG Automatic Subscriber Logon, on page 208](#)
- [Additional References, on page 209](#)
- [Feature Information for ISG Automatic Subscriber Logon, on page 210](#)

Finding Feature Information

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

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

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

Identifying Traffic for Automatic Logon in a Control Policy Class Map

Perform this task to configure a control policy class map that specifies the traffic to which ISG automatic subscriber logon will apply.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control match-all class-map-name**
4. Do one of the following:
 - **match source-ip-address ip-address subnet-mask**
 -
 - **match nas-port circuit-id name**
 -
 - **match nas-port remote-id name**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map type control match-all class-map-name Example: <pre>Router(config)# class-map type control match-all TAL-subscribers</pre>	Creates a control class map, which defines the conditions under which the actions of a control policy map will be executed.
Step 4	Do one of the following: <ul style="list-style-type: none"> • match source-ip-address ip-address subnet-mask • • match nas-port circuit-id name • • match nas-port remote-id name Example: <pre>Router(config-control-classmap)# match source-ip-address 10.1.1.0 255.255.255.0</pre> Example: <pre>Router(config-control-classmap)# match nas-port circuit-id circuit1</pre> Example: <pre>Router(config-control-classmap)# match nas-port remote-id remotel</pre>	Creates a condition that will evaluate true if a subscriber's source IP address matches the specified IP address. or Creates a condition that will evaluate true if a subscriber's circuit ID matches the specified value. or Creates a condition that will evaluate true if a subscriber's remote ID matches the specified value.
Step 5	end Example: <pre>Router(config-control-classmap)# end</pre>	(Optional) Returns to privileged EXEC mode.

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type control TAL</pre>	Creates or modifies a control policy map, which is used to define a control policy.
Step 4	class type control { <i>class-map-name</i> always } event session-start Example: <pre>Router(config-control-policymap)# class type control TAL-subscribers event session-start</pre>	Specifies a control class, which defines the conditions that must be met in order for an associated set of actions to be executed. <ul style="list-style-type: none"> • Specify the control class-map that was configured in the task “Identifying Traffic for Automatic Logon in a Control Policy Class Map, on page 203”.
Step 5	<i>action-number</i> authorize [aaa { <i>list-name</i> list { <i>list-name</i> default } } [password <i>password</i>]] [upon network-service-found { continue stop }] [use method <i>authorization-type</i>] identifier <i>identifier-type</i> [plus <i>identifier-type</i>] Example: <pre>Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address</pre>	Inserts the specified identifier into the username field of authorization requests.
Step 6	end Example:	Exits the current configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-control-policy-map-class-control)# end	

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.

Enabling the Remote-ID to Be Sent as the Calling-Station-ID

Perform this task to enable the ISG device to send the remote ID in the Calling-Station-ID (attribute 31) field of accounting records and access requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 31 remote-id**

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 31 remote-id Example: Router#(config) radius-server attribute 31 remote-id	Enables the ISG device to send the remote ID in the Calling Station ID (attribute 31) field of accounting records and access requests.

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

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 25: 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.



CHAPTER 17

Configuring DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. The DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon feature enables service providers to provision triple-play services to households by supporting transparent automatic logon (TAL) through Dynamic Host Configuration Protocol (DHCP) option 60 and option 82, and wholesale IP sessions through the virtual private network (VPN) ID extension to option 82.

- [Finding Feature Information, on page 211](#)
- [Prerequisites for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon, on page 212](#)
- [Restrictions for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon, on page 212](#)
- [Information About DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon, on page 212](#)
- [How to Configure DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon, on page 213](#)
- [Configuration Examples for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon, on page 216](#)
- [Additional References, on page 217](#)
- [Feature Information for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon, on page 218](#)

Finding Feature Information

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

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 DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

For vendor-class ID (option 60) to be used for authorization, the vendor-class ID must be inserted by the customer appliance (that is, the PC, phone, or set-top box) in the DHCP option 60 information.

For provisioning of wholesale IP sessions, the VPN-ID must be inserted in the DHCP option 82 information along with the circuit ID and the remote ID.

Restrictions for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

RADIUS proxy users are not supported by this feature.

Information About DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

ISA Automatic Subscriber Logon

TAL enables a specified identifier to be used in place of the username in authorization requests. Enabling the Authentication, Authorization, and Accounting (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.

Session start is the event that triggers TAL. For DHCP-initiated IP sessions, session start occurs when a DHCP DISCOVER request is received.

Authorization Based on Option 60 and Option 82

The circuit ID and remote ID fields (option 82) are part of the DHCP relay agent information option. A digital subscriber line access multiplexer (DSLAM) inserts the option 82 fields into DHCP messages; the customer appliance inserts the option 60 fields.

You can configure an ISG policy to use the circuit ID, remote ID, or vendor class ID, or a combination of the three, as the username in authorization requests. Alternatively, you can configure an ISG policy to use the NAS-Port-ID as the identifier for authorization. When you use the NAS-Port-ID as the identifier, you can configure it to include a combination of circuit ID, remote ID, and vendor-class ID.

By default, the ISG uses the circuit ID and remote ID that are provided by the Layer 2 edge-access device for authorization. The configuration of the **ip dhcp relay information option** command determines whether the ISG uses the option 82 information received, generates its own, or (when the **encapsulate** keyword is specified) encapsulates a prior option 82 along with its own option 82. For more information, see the "Configuring the Cisco IOS DHCP Relay Agent" section of the *Cisco IOS IP Addressing Services Configuration Guide*.

If the NAS-Port-ID is not configured to include option 60 and option 82, the NAS-Port-ID is populated with the ISG interface that received the DHCP relay agent information packet; for example, Ethernet1/0.

DHCP Option 82 with VPN-ID Suboption

To support wholesale services for IP sessions, the VPN-ID, together with the circuit ID and remote ID, must be specified in authorization requests. The DHCP option 60 and option 82 with VPN-ID Support for Transparent Automatic Logon feature enables you to include two sets of option 82 information in a single message so that devices within a household can be differentiated:

- The first set of option 82 information carries household information and option 60 to associate the device within the household.
- The second set of option 82 information, if VPN-ID is configured, carries the VPN information for the household.

The DHCP server processes the option 82 information, forwarded by the relay, with the VPN-ID, remote ID, circuit ID, and option 60 information to allocate an address.

How to Configure DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

You can configure an ISG policy for TAL using either a username or the NAS-Port-ID for authorization.

Configuring an ISG Control Policy Using Option 60 and Option 82

Perform this task to configure an ISG control policy that 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. <ul style="list-style-type: none"> • 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 <i>policy-map-name</i> Example: Router(config)# policy-map type control TAL	Enters control policy-map configuration mode to define a control policy.
Step 4	class type control {<i>class-map-name</i> always} event session-start Example: Router(config-control-policymap)# class type control TAL-subscribers event session-start	Enters control policy-map class configuration mode to define the conditions that must be met in order for an associated set of actions to be executed. <ul style="list-style-type: none"> Specify the control class-map that was configured in the section "Identifying Traffic for Automatic Logon in a Control Policy Class Map".
Step 5	<i>action-number</i> authorize [aaa {<i>list-name</i> list {<i>list-name</i> default}}] [password <i>password</i>]] [upon network-service-found {continue stop}] [use method <i>authorization-type</i>] identifier <i>identifier-type</i> [plus <i>identifier-type</i>] Example: Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address vendor-class-id plus circuit-id plus remote-id	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.

Configuring an ISG Control Policy Using NAS-Port-ID

Perform this task to configure an ISG control policy that uses NAS-Port-ID in the authorization request.

SUMMARY STEPS

- enable
- configure terminal
- policy-map type control *policy-map-name*
- class type control {*class-map-name* | always} event session-start
- action-number* authorize [aaa {*list-name* | list {*list-name* | default}}] [password *password*]] [upon network-service-found {continue | stop}] [use method *authorization-type*] identifier nas-port

6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: Router(config)# policy-map type control TAL	Enters control policy-map configuration mode to define a control policy.
Step 4	class type control {<i>class-map-name</i> always} event session-start Example: Router(config-control-policymap)# class type control TAL-subscribers event session-start	Enters control policy-map class configuration mode to define the conditions that must be met in order for an associated set of actions to be executed. <ul style="list-style-type: none"> • Specify the control class-map that was configured in the section "Identifying Traffic for Automatic Logon in a Control Policy Class Map".
Step 5	<i>action-number</i> authorize [aaa {<i>list-name</i> list {<i>list-name</i> default}}] [password <i>password</i>] [upon network-service-found {continue stop}] [use method <i>authorization-type</i>] identifier nas-port Example: Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier nas-port	Inserts the NAS port 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.

Configuring NAS-Port-ID to Include Option 60 and Option 82

Perform this task to include option 60 and option 82 in the NAS-Port-ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port-id include** *{identifier1 [plus identifier2] [plus identifier3]}* [**separator separator**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server attribute nas-port-id include <i>{identifier1 [plus identifier2] [plus identifier3]}</i> [separator separator] Example: Router(config)# radius-server attribute nas-port-id include circuit-id plus vendor-class-id	Includes DHCP relay agent information option 60 and option 82 in the NAS-Port-ID.

Configuration Examples for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

Example Option 60 and Option 82 in NAS-Port-ID

The following example uses the **radius-server attribute nas-port-id include** command to configure option 60 and option 82 authorization using circuit ID, remote ID, and vendor-class ID:

```
interface Ethernet0/0
  service-policy type control RULEA
  !
interface Ethernet1/0
  service-policy type control RULEB
  !
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 CONDB
  match vendor-class-id vendor1
  !
policy-map type control RULEA
```



```

class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier vendor-class-id
!
policy-map type control RULEB
  class type control CONDB event session-start
    1 authorize aaa list TAL_LIST password cisco identifier nas-port
  !
radius-server attribute nas-port-id include circuit-id plus remote-id plus vendor-class-id
separator #

```

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
Configuring ISG policies for automatic subscriber logon	"Configuring ISG Policies for Automatic Subscriber Logon" module in the <i>Intelligent Services Gateway Configuration Guide</i>
Configuring a DHCP relay agent	"Configuring the Cisco IOS DHCP Relay Agent" module in the <i>IP Addressing Services Configuration Guide</i>

Standards

Standard	Title
None	-

MIBs

MIB	MIBs Link
	<ul style="list-style-type: none"> 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
None	-

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic 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 26: Feature Information for DHCP Option 60 and Option 82 Support and VPN-ID Support

Feature Name	Releases	Feature Information
ISG: Authentication: DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon	Cisco IOS XE Release 3.1S	<p>Enables service providers to support TAL through DHCP option 60 and option 82 and wholesale IP sessions through the VPN-ID extension to option 82.</p> <p>The following commands were introduced or modified:</p> <p>radius-server attribute nas-port-id include</p>



CHAPTER 18

Enabling ISG to Interact with External Policy Servers

Intelligent Services Gateway (ISG) is a 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 the ISG to retrieve session policies or accept dynamic updates to session policies from external policy servers.

- [Finding Feature Information, on page 219](#)
- [Restrictions for ISG Interaction with External Policy Servers, on page 219](#)
- [Information About ISG Interaction with External Policy Servers, on page 220](#)
- [How to Enable ISG to Interact with External Policy Servers, on page 221](#)
- [Configuration Examples for ISG Interaction with External Policy Servers, on page 225](#)
- [Additional References, on page 226](#)
- [Feature Information for ISG Interaction with External Policy Servers, on page 227](#)

Finding Feature Information

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

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

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 the 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 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 introduces peer-to-peer capability to RADIUS that enables ISG and the external policy server to act as the RADIUS client and server respectively.

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 only on the basis of the username and password (two-key authentication). The Triple Key Authentication Support 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 the SSG with a string containing the subscriber's location. The SSG then includes this location string 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 ISG sends the location string within a Cisco vendor-specific attribute (VSA) that is included in the access-request message to the RADIUS server.

The location information is received from SME as Cisco VSA 250. This location information is included in session authentication requests, session accounting requests from the ISG, and prepaid authorization requests.

The table below shows the Cisco vendor-specific non-AVPair attribute used for triple key authentication.

Table 27: 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	LWiFiHotSpot001	Acc-Req CoA Req Accounting

How to Enable ISG to Interact with External Policy Servers

Configuring 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.

Before you begin

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	aaa authentication login {default <i>list-name</i> } <i>method1</i> [<i>method2...</i>] Example: <pre>Router(config)# aaa authentication login PPP1 group radius</pre>	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: <pre>Router(config)# aaa authentication ppp default group radius</pre>	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: <pre>Router(config)# aaa authorization network NET1 radius</pre>	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: <pre>Router(config)# aaa authorization subscriber-service default radius</pre>	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: <pre>Router(config)# aaa accounting network default start-stop group radius</pre>	Enables AAA accounting of requested services for billing or security purposes.
Step 8	end Example: <pre>Router(config)# end</pre>	Exits global configuration mode.

Configuring ISG as a AAA Server

Dynamic authorization allows a policy server to dynamically send policies to ISG. Perform this task to configure 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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	aaa server radius dynamic-author Example: <pre>Router(config)# aaa server radius dynamic-author</pre>	Configures ISG as a AAA server and enters dynamic authorization local server configuration mode.
Step 4	client {name ip-address} [key [0 7] word] [vrf vrf-id] Example: <pre>Router(config-locsvr-da-radius)# client 10.76.86.90 key cisco</pre>	Specifies a client with which ISG will be communicating.
Step 5	port port-number Example: <pre>Router(config-locsvr-da-radius)# port 1600</pre>	Specifies the RADIUS server port. <ul style="list-style-type: none"> • Default is 1700.
Step 6	server-key [0 7] word Example: <pre>Router(config-locsvr-da-radius)# server-key cisco</pre>	Specifies the encryption key shared with the RADIUS client.
Step 7	auth-type {all any session-key} Example: <pre>Router(config-locsvr-da-radius)# auth-type all</pre>	Specifies the attributes to be used for session authorization.
Step 8	ignore {server-key session-key} Example:	Configures ISG to ignore the shared encryption key or attribute 151.

	Command or Action	Purpose
	<code>Router(config-locsvr-da-radius)# ignore session-key</code>	
Step 9	end Example: <code>Router(config-locsvr-da-radius)# end</code>	Exits dynamic authorization local server configuration mode.

Enabling the Location VSA for Triple Key Authentication

Perform this task to enable ISG to include the location VSA in authentication and accounting requests.

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: <code>Router> enable</code>	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	aaa new-model Example: <code>Router(config)# aaa new-model</code>	Enables AAA.
Step 4	radius-server vsa send accounting Example: <code>Router(config)# radius-server vsa send accounting</code>	Enables ISG to recognize and use accounting VSAs as defined by RADIUS attribute 26.
Step 5	radius-server vsa send authentication Example:	Enables ISG to recognize and use authentication VSAs as defined by RADIUS attribute 26.

	Command or Action	Purpose
	Router(config)# radius-server vsa send authentication	
Step 6	end Example: Router(config)# end	Exits to privileged EXEC mode.

Configuration Examples for ISG Interaction with External Policy Servers

Example: Enabling ISG to Interact with External Policy Servers

The following example shows how to configure ISG as a AAA client.

```
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
```

The following example shows how to configure ISG as a AAA server.

```
aaa server radius dynamic-author
  client 10.76.86.90 server-key cisco
  port 1600
  server-key cisco
  auth-type all
  ignore session-key
```

Example: Enabling the Location VSA for Triple Key Authentication

The following example shows how to enable ISG to use VSAs for accounting and authentication.

```
aaa new-model
radius-server vsa send accounting
radius-server vsa send 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.

```
Device# debug radius accounting
```

```

*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)," <i>Cisco IOS XE Security Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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 28: Feature Information for ISG Interaction with External Policy Servers

Feature Name	Releases	Feature Information
ISG—Policy Control Policy Server CoA	Cisco IOS XE Release 3.3SG	<p>This feature provides ISG support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization.</p> <p>This feature was integrated into Cisco IOS XE Release 3.3SG.</p>
ISG—Session Lifecycle Packet of Disconnect (POD)	Cisco IOS XE Release 3.3SG	This feature enables an external policy server to terminate an ISG session when it receives a RADIUS Packet of Disconnect (POD).



CHAPTER 19

Configuring ISG Subscriber Services

Intelligent Services Gateway (ISG) is a 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, on page 229](#)
- [Restrictions for ISG Subscriber Services, on page 229](#)
- [Information About ISG Subscriber Services, on page 230](#)
- [How to Configure ISG Services on the Router, on page 233](#)
- [Configuration Examples for ISG Services, on page 243](#)
- [Additional References, on page 245](#)
- [Feature Information for ISG Subscriber Services, on page 246](#)

Finding Feature Information

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

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 can 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.
- 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.

- If the input ACL or output ACL that is configured in a traffic class map is not defined, or if the protocol of these ACLs is not the same (IPv4 versus IPv6), the traffic class installation fails and the service is not applied. If this failure occurs at session start, the session is not established. IPv4 ACLs are defined with the **ip access-list** command; IPv6 ACLs are defined with the **ipv6 access-list** command.
- ISG supports only single-stack traffic classes; a particular traffic class can classify either IPv4 or IPv6 traffic but not both.
- If any new service needs to be defined when the sessions are active, follow the order to update the configuration:
 1. ACL definition
 2. Class-map definition
 3. Policy-map service definition
 4. Service name in Policy rule or update dynamically through CoA.

Information About ISG Subscriber Services

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 provide differentiated behavior for different traffic streams to and from a particular subscriber. Each traffic stream is represented by a classification and a set of applied features. A traffic class, also known as a flow, is a kind of service.

For traffic to be classified into streams, you must specify an access control list (ACL) that classifies the traffic and 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 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. The default action of the default class is to pass traffic, or 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.

ISG traffic classes are created dynamically, either at session start or later during the life of the session, when a service with a classification (the class definition of the service contains at least one named or numbered ACL) is applied to a session. A service with a classification is called a flow service. A service without a classification is called a classless service.

Traffic classes are assigned unique identifiers that can be tracked with Cisco IOS **show** commands.

Flow Classifiers

In Cisco IOS XE Release 3.3S and later releases, separate sessions are no longer created for each traffic class; the traffic class is handled as a flow within the parent subscriber session.

A flow, or traffic class, represents a subset of subscriber traffic identified by a pair of class identifiers. Each class identifier, or classifier, represents a single class or a directional flow. Traffic can have a classifier in either or both directions. If there is no classifier in a particular direction, traffic in that direction is not subjected to the flow.

The ISG classifier is responsible for managing and enforcing classifiers and the corresponding policies associated with ISG subscriber sessions, also called targets. Each ISG subscriber session can have one or more classifiers associated with it. The different classifiers that can be associated with a subscriber session are:

- **Match-Always Classifier**—Identifies the entire traffic of a target in a particular direction. A target may have only one match-always classifier in each direction.
- **Flow Classifier**—Identifies a subset of traffic of a target in a particular direction. A target may have any number of flow classifiers in each direction.
- **Default Classifier**—Identifies the traffic of a target that does not match any of the flow classifiers in a particular direction. A target may have only one default classifier in each direction.

A set of features represent a policy attached to a classifier. Two classifiers on a target may have the same policy or different policies attached to it. ISG, however, considers the policy of each classifier to be independent of the other classifiers on a target.

The priority defines the order in which a packet should be subjected to classifiers when multiple classifiers are associated with a target. If no priority is defined, the default priority is assumed, which is a lower priority than any of the defined priorities in other classes but higher than the default class.

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.

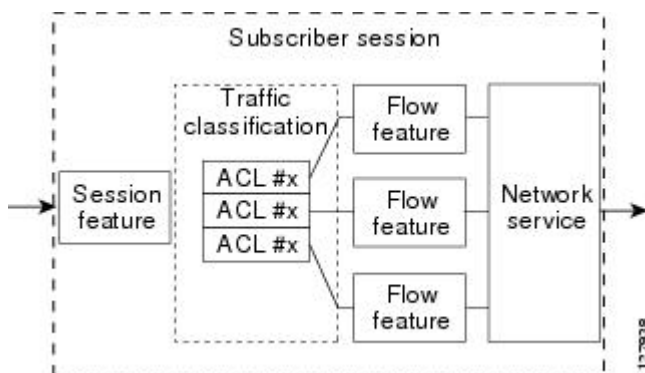
The features configured within a traffic policy apply only to the traffic defined by the traffic class. Multiple traffic policies with various features can be applied to a session.

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 9: ISG Feature Application on a Session and Flows



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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>policy-map type service <i>policy-map-name</i></p> <p>Example:</p> <pre>Router(config)# policy-map type service service1</pre>	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	<p>authenticate aaa list <i>name-of-list</i></p> <p>Example:</p> <pre>Router(config-service-policymap)# authenticate aaa list mlist</pre>	Indicates that the service requires authentication as a condition of activation and initiates an authentication request.
Step 5	<p>classname <i>dhcp-pool-name</i></p> <p>Example:</p> <pre>Router(config-service-policymap)# classname green</pre>	Associates a Dynamic Host Configuration Protocol (DHCP) address pool with a service or specific subscriber.
Step 6	<p>ip portbundle</p> <p>Example:</p> <pre>Router(config-service-policymap)# ip portbundle</pre>	Enables the ISG Port-Bundle Host Key feature in the service policy map.
Step 7	<p>ip unnumbered <i>interface-type interface-number</i></p> <p>Example:</p> <pre>Router(config-service-policymap)# ip unnumbered ethernet 0</pre>	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 8	<p>ip vrf forwarding <i>name-of-vrf</i></p> <p>Example:</p> <pre>Router(config-service-policymap)# ip vrf forwarding blue</pre>	<p>Associates the service with a VRF.</p> <ul style="list-style-type: none"> Configuring this command will make the service a primary service.
Step 9	<p>service deny</p> <p>Example:</p> <pre>Router(config-service-policymap)# service deny</pre>	Denies network service to the subscriber session.
Step 10	<p>service relay pppoe vpdn group <i>VPDN-group-name</i></p> <p>Example:</p> <pre>Router(config-service-policymap)# service relay pppoe vpdn group group1</pre>	Enables relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel for a subscriber session.
Step 11	<p>service vpdn group <i>VPDN-group-name</i></p> <p>Example:</p>	<p>Provides virtual private dialup network (VPDN) service for ISG subscriber sessions.</p> <ul style="list-style-type: none"> Configuring this command will make the service a primary service.

	Command or Action	Purpose
	Router(config-service-policy) # service vpdn group vpdn1	
Step 12	sg-service-group <i>service-group-name</i> Example: Router(config-service-policy) # sg-service-group group1	Associates the service with a specified service group.
Step 13	sg-service-type {primary secondary} Example: Router(config-service-policy) # sg-service-type primary	Defines the service as a primary or secondary service. <ul style="list-style-type: none"> • 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

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.

Before you begin

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map type traffic match-any <i>class-map-name</i> Example: <pre>Router(config)# class-map type traffic match-any class1</pre>	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 {<i>access-list-number</i> name <i>access-list-name</i>} Example: <pre>Router(config-traffic-classmap)# match access-group input 101</pre>	(Optional) Configures the match criteria for an input class map on the basis of the specified ACL. <ul style="list-style-type: none"> • 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 5	match access-group output {<i>access-list-number</i> name <i>access-list-name</i>} Example: <pre>Router(config-traffic-classmap)# match access-group output 102</pre>	(Optional) Configures the match criteria for an output class map on the basis of the specified ACL. <ul style="list-style-type: none"> • 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: <pre>Router(config-traffic-classmap)# exit</pre>	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-configuration*
8. **redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}
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 <i>policy-map-name</i> 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	[<i>priority</i>] class type traffic <i>class-map-name</i> Example: Router(config-service-policymap)# class type traffic classb	Associates a traffic class map with the service policy map. • The <i>priority</i> argument determines which traffic class will be used first for a specified match. When a packet matches more than one traffic class, it is classified to the class with the higher priority.
Step 5	accounting aaa list <i>AAA-method-list</i> 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 } <i>committed-rate normal-burst excess-burst</i> Example:	Enables ISG policing for upstream or downstream traffic. • This command can be entered twice to configure upstream and downstream policing.

	Command or Action	Purpose
	Router(config-service-policy-map-class-traffic)# police input 20000 30000 60000	
Step 7	prepaid config <i>name-of-configuration</i> Example: Router(config-service-policy-map-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 [<i>list access-list-number</i>] to { group <i>server-group-name</i> ip <i>ip-address</i> [port <i>port-number</i>]} [<i>duration seconds</i>] [<i>frequency seconds</i>] Example: Router(config-service-policy-map-class-traffic)# redirect to ip 10.10.10.10	Redirects traffic to a specified server or server group.
Step 9	timeout absolute <i>duration-in-seconds</i> Example: Router(config-control-policy-map-class-traffic)# timeout absolute 30	Specifies the session lifetime, in a range from 30 to 4294967 seconds.
Step 10	timeout idle <i>duration-in-seconds</i> Example: Router(config-control-policy-map-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-policy-map-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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type service service1</pre>	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: <pre>Router(config-service-policymap)# class type traffic default in-out</pre>	Associates a default traffic class with a service policy map. <ul style="list-style-type: none"> • 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: <pre>Router(config-service-policymap-class-traffic)# drop</pre>	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

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: <code>26,9,251="A service-name[; username ; password]"</code>	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.

Before you begin

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: <code>Router> enable</code>	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: <code>Router(config)# policy-map type control policy1</code>	Creates or modifies a policy map to specify an ISG control policy.

	Command or Action	Purpose
Step 4	<p>class type control {always <i>map-class-name</i>} [event account-logon credit-exhausted quota-depleted service-start service-stop session-default-service session-service-found session-start timed-policy-expiry]</p> <p>Example:</p> <pre>Router(config-control-policymap)# class type control always event session-start</pre>	Specifies a class and, optionally, an event for which actions may be configured.
Step 5	<p><i>action-number</i> service-policy type service {name unapply} <i>policy-map-name</i></p> <p>Example:</p> <pre>Router(config-control-policymap-class-control)# 1 service-policy type service service1</pre>	<p>Applies the specified service policy map.</p> <ul style="list-style-type: none"> 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	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>show class-map type traffic</p> <p>Example:</p> <pre>Router# show class-map type traffic</pre>	Displays all traffic class maps and their matching criteria.
Step 3	<p>show policy-map type service</p> <p>Example:</p> <pre>Router# show policy-map type service</pre>	Displays the contents of all service policy maps.

Configuration Examples for ISG Services

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 29: 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.
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.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.3S	ISG no longer creates separate sessions for each traffic class; the traffic class is handled as a flow within the parent subscriber session. The following commands were introduced or modified: debug subscriber classifier , debug subscriber feature , show subscriber service , show subscriber statistics .



CHAPTER 20

Configuring ISG Network Forwarding Policies

Intelligent Services Gateway (ISG) is a 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, on page 249](#)
- [Restrictions for ISG Network Forwarding Policies, on page 249](#)
- [Information About ISG Network Policies, on page 250](#)
- [How to Configure ISG Network Policies, on page 251](#)
- [Configuration Examples for ISG Network Policies, on page 254](#)
- [Additional References, on page 254](#)
- [Feature Information for ISG Network Policies, on page 255](#)

Finding Feature Information

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

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

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

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.

Before you begin

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example:	Creates or modifies a service policy map, which is used to define an ISG service.

	Command or Action	Purpose
	Router(config)# policy-map type service service1	
Step 4	<p>Do one of the following:</p> <ul style="list-style-type: none"> • service vpdn group <i>vpdn-group-name</i> • service local • service relay pppoe vpdn group <i>vpdn-group-name</i> <p>Example:</p> <pre>Router(config-service-policymap)# service vpdn group vpdn1</pre> <p>Example:</p> <pre>Router(config-service-policymap)# service local</pre> <p>Example:</p> <pre>Router(config-service-policymap)# service relay pppoe vpdn group vpdn1</pre>	<p>Provides virtual private dialup network (VPDN) service.</p> <p>or</p> <p>Provides local termination service.</p> <p>or</p> <p>Provides VPDN service by relaying PPPoE over VPDN L2TP tunnels.</p> <ul style="list-style-type: none"> • 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	<p>ip vrf forwarding <i>name-of-vrf</i></p> <p>Example:</p> <pre>Router(config-service-policymap)# ip vrf forwarding blue</pre>	<p>Associates the service with a VRF.</p> <ul style="list-style-type: none"> • 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

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	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>policy-map type service <i>policy-map-name</i></code></p> <p>Example:</p> <pre>Router(config)# policy-map type service service1</pre>	<p>Creates or modifies a service policy map, which is used to define an ISG service.</p>
Step 4	<p><code>ip vrf forwarding <i>name-of-vrf</i></code></p> <p>Example:</p> <pre>Router(config-service-policymap)# ip vrf forwarding blue</pre>	<p>Associates the service with a VRF.</p>
Step 5	<p><code>sg-service-type primary</code></p> <p>Example:</p> <pre>Router(config-service-policymap)# sg-service-type primary</pre>	<p>Defines the service as a primary service.</p> <ul style="list-style-type: none"> • 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

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".

Configuration Examples for ISG Network Policies

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	<i>VPDN Technologies Configuration Guide</i>
PPP and VPDN commands	<i>VPDN Technologies Command Reference</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 30: 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.



CHAPTER 21

Configuring ISG Accounting

The Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework to edge devices that 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, on page 257](#)
- [Prerequisites for ISG Accounting, on page 257](#)
- [Restrictions for ISG Accounting, on page 258](#)
- [Information About ISG Accounting, on page 258](#)
- [How to Configure ISG Accounting, on page 262](#)
- [Configuration Examples for ISG Accounting, on page 272](#)
- [Additional References, on page 279](#)
- [Feature Information for ISG Accounting, on page 279](#)

Finding Feature Information

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

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 Accounting

- Configure the authentication, authorization, and accounting (AAA) method list using the **aaa accounting** command before configuring Intelligent Services Gateway (ISG) accounting. ISG sends accounting records to the AAA method list specified in the user profile, service profile, or service policy map. For more information about the AAA commands, see the *Cisco IOS Security Command Reference: Commands A to C*.
- AAA servers must be configured to support ISG accounting.

Restrictions for ISG Accounting

- Intelligent Services Gateway (ISG) accounting supports only the RADIUS protocol.
- If authentication, authorization, and accounting (AAA) broadcast accounting is used with periodic accounting, you cannot configure different accounting periods for different accounting groups.

Information About ISG Accounting

Overview of ISG Accounting

Intelligent Services Gateway (ISG) supports per-session, per-service, or per-flow accounting. Per-session accounting is the aggregate of all the flow traffic for a session and it can be enabled in a user profile.

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.

Within a subscriber session, per-service accounting enables RADIUS to track services when they become active and when they stop. Per-service accounting is the aggregate of all flow traffic for the duration of the service. Using this feature, the device includes all activated services for the session in a single accounting start message. Per-service accounting can be enabled in a service profile or service policy map. When per-service accounting is configured, the service name and Parent-Session-ID attributes are included in accounting records.



Note 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 authentication, authorization, and accounting (AAA) method list is specified. We recommend 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 a service policy map. ISG accounting sends Accounting-Start, interim, and Accounting-Stop records to the specified AAA method list.

ISG Accounting Messages on ANCP Ports

Accounting messages sent by Intelligent Services Gateway (ISG) for sessions on an Access Node Control Protocol (ANCP) port contain the following authentication, authorization, and accounting (AAA) attributes:

- nas-rx-speed
- nas-rx-speed-bps
- nas-tx-speed
- nas-tx-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 up, 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.

To retrieve the AAA attributes from the QoS policy, the policy must be configured before 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 continues to use the previous values until the ANCP neighbor is removed and reconfigured.

Service Activation and Deactivation Configuration on RADIUS

You can 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 Change of Authorization (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 parameters 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,...)"
```

ISG Accounting Records

Intelligent Services Gateway (ISG) accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based authentication, authorization, and accounting (AAA) server or a 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 accounting 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 on to or out off 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 to the AAA server.

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 an accounting session ID that is different 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 *Securing User Services Configuration Guide Library* for more information.

Interim ISG Accounting Updates

Intelligent Services Gateway (ISG) supports interim (intermittent) RADIUS accounting updates that work the same way as “watchdog” RADIUS accounting. Accounting updates are sent between the time 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 can be enabled or disabled globally for new information. Periodic accounting can be enabled for specific contexts, such as globally, in user profiles, and in services.

Broadcast Accounting

Intelligent Services Gateway (ISG) supports authentication, authorization, and accounting (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 *Cisco Authentication, Authorization, and Accounting Configuration Guide*.

ISG Postpaid Tariff Switching

The Intelligent Services Gateway (ISG) Postpaid Tariff Switching feature 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, 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 during 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 the 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 and logoff time stamps, it can calculate the various tariffs that apply during that time.

Subscriber Accounting Accuracy

The Subscriber Accounting Accuracy feature guarantees that the I/O packet/byte statistics in the Accounting-Stop record are accurate to within one second.

Subscriber accounting data is sent to authentication, authorization, and accounting (AAA) servers during the following events:

- Configured intervals during the lifetime of the session or service
- Service logoff
- Session tear down

Use the **subscriber accounting accuracy** *milliseconds* command to set the value for the Subscriber Accounting Accuracy feature.

HA Support for ISG Accounting

The accounting start and stop records that Intelligent Services Gateway (ISG) sends to an external RADIUS accounting server contains cumulative counters associated with subscriber sessions. ISG can also send interim accounting records containing the latest time and volume statistics at periodic intervals during a session's lifetime. This information is correlated by a third-party billing software to generate billing records for the subscriber.

The ISG stateful switchover (SSO) and In Service Software Upgrade (ISSU) feature adds high availability (HA) support to the ISG session, service, and flow accounting. This HA support includes a periodic session update feature that enables ISG to retain cumulative accounting counters associated with the subscriber sessions after an SSO or ISSU event. Configuring this feature prevents the new active processor from restarting the accounting counters from zero after an SSO event. You can also specify that the first record sent after an SSO event is an interim accounting record for sessions, services, and flows that survive the switchover.

The following are some of the counters and their associated counters that retain their value after Route Processor (RP) SSO:

- Session counters:
 - Acct-Input-Octets
 - Acct-Input-Packets
 - Acct-Output-Octets
 - Acct-Output-Packets
 - Acct-Session-Time
- Service counters:
 - Acct-Input-Octets
 - Acct-Input-Packets
 - Acct-Output-Octets

- Acct-Output-Packets

For information about configuring HA on the ISG device, see the *High Availability Configuration Guide*.

How to Configure ISG Accounting

Enabling ISG per-Session Accounting

Per-session accounting can be configured in the user profile of a authentication, authorization, and accounting (AAA) server.

This task contains the following sections:

Enabling ISG per-Session Accounting in a User Profile on a AAA Server

Use the attributes given in this procedure to enable per-session accounting in a user profile on an authentication, authorization, and accounting (AAA) server.



Note You must configure a service for an accounting list before enabling a per-session accounting in a user profile. A per-session accounting list cannot be applied on a session in Intelligent Services Gateway (ISG) if a service is not configured; that is, you must have a dummy service configured under the accounting list when there is no service configured.

SUMMARY STEPS

1. Cisco-Attribute-Value pair (AVpair)="accounting-list=*accounting-mlist-name*"
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-Attribute-Value pair (AVpair)="accounting-list=*accounting-mlist-name*"

Adds 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) Adds the Acct-Interim-Interval (attribute 85) to the user profile. This attribute specifies the number of seconds between interim updates.

Enabling a per-User Accounting List

Perform this task to enable a dummy service on an accounting list. A dummy service is a string that is used to get an authorization from a server for a user profile when no service is configured.

SUMMARY STEPS

1. `userxxx2@cisco.com Cleartext-Password := "cisco111"`
2. `Cisco-Account-Info += "ADUMMYSERVICE",`

DETAILED STEPS

-
- Step 1** `userxxx2@cisco.com Cleartext-Password := "cisco111"`
Adds the username and password account information for a RADIUS user profile.
- Step 2** `Cisco-Account-Info += "ADUMMYSERVICE",`
Adds a dummy service to a RADIUS user profile for an accounting list on an authentication, authorization, and accounting (AAA) server.
-

Enabling ISG per-Flow Accounting

Intelligent Services Gateway (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:

Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server

Perform this task to configure a per-flow accounting in a service profile on the authentication, authorization, and accounting (AAA) server.

Before you begin

This task assumes that you have defined IP access lists for specifying the 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]"`
Adds the Intelligent Services Gateway (ISG) traffic class attribute to the service profile. This attribute specifies the 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*"

Adds 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) Adds 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 ISG per-Flow Accounting in a Service Policy Map

Perform this task to enable accounting in a local service policy map for the device for a specific flow.

Before you begin

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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: Device(config)# policy-map type service service1	Creates or defines a service policy map, which is used to define an Intelligent Services Gateway (ISG) service and enters service policy-map configuration mode.

	Command or Action	Purpose
Step 4	class type traffic <i>class-map-name</i> Example: <pre>Device(config-service-policymap)# class type traffic firstclass</pre>	Associates a previously configured traffic class with the policy map and enters control policy-map traffic class configuration.
Step 5	accounting aaa list <i>AAA-method-list</i> Example: <pre>Device(config-control-policymap-class-traffic)# accounting aaa list list1</pre>	Enables accounting and specifies the authentication, authorization, and accounting (AAA) method list to which accounting updates will be sent. <ul style="list-style-type: none"> • The AAA method list must be configured.
Step 6	end Example: <pre>Device(config-control-policymap-class-traffic)# end</pre>	Returns to privileged EXEC mode.

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:

Enabling per-Service Accounting on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber service multiple-accept**
4. **subscriber service session-accounting**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	subscriber service multiple-accept Example: Device(config)# subscriber service multiple-accept	Enables multiple services in a single Access-Accept message.
Step 4	subscriber service session-accounting Example: Device(config)# subscriber service session-accounting	Enables subscriber services accounting. <ul style="list-style-type: none"> • All started services are included in the session accounting start message.
Step 5	end Example: Device(config)# end	Returns to privileged EXEC mode.

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 authentication, authorization, and accounting (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*"
- Adds 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) Adds 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

To configure a per-service accounting in a service policy map on the device, 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 the 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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	class-map type traffic match-any <i>class-map-name</i> Example: Device(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. <ul style="list-style-type: none"> • 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: Device(config-traffic-classmap)# exit	Exits traffic class-map configuration mode.
Step 5	policy-map type service <i>policy-map-name</i> Example: Device(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.

	Command or Action	Purpose
Step 6	class type traffic <i>class-map-name</i> Example: <pre>Device(config-service-policymap)# class type traffic empty_class</pre>	Associates a traffic class map with the service policy map and enters service policy-map traffic class configuration mode. <ul style="list-style-type: none"> In this step, reference the empty traffic class map that you created in Step 3.
Step 7	accounting aaa list <i>AAA-method-list</i> Example: <pre>Device(config-service-policymap-class-traffic)# accounting aaa list list1</pre>	Enables accounting and specifies the authentication, authorization, and accounting (AAA) method list to which accounting updates will be sent.
Step 8	end Example: <pre>Device(config-service-policymap-class-traffic)# end</pre>	Returns to privileged EXEC mode.

Configuring ISG Postpaid Tariff Switching

ISG postpaid tariff switching can be configured in the service profile on a authentication, authorization, and accounting (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.

Before you begin

Intelligent Services Gateway (ISG) per-session or per-flow accounting must be configured for postpaid tariff switching to work.

SUMMARY STEPS

1. Cisco-AVpair = “PPWhh: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 = “PPWhh:mm:ss:d”

Adds the postpaid VSA to the service profile. This attribute specifies the weekly tariff-switch points for postpaid tariff switching. The syntax description is as 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*]”

Adds 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

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 “Configuring ISG Subscriber Services” module.

Verifying ISG Accounting and Postpaid Tariff Switching

To verify and troubleshoot Intelligent Services Gateway (ISG) accounting and postpaid tariff switching, use any of the following commands in privileged EXEC mode. You can use these commands in any order.

SUMMARY STEPS

1. **show subscriber session**
2. **show aaa sessions**
3. **show aaa user {all | *unique id*}**
4. **show sss session [all]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show subscriber session Example: Device# show subscriber session	Displays ISG subscriber session information.
Step 2	show aaa sessions Example: Device# show aaa sessions	Displays authentication, authorization, and accounting (AAA) subscriber session information.

	Command or Action	Purpose
Step 3	show aaa user {all <i>unique id</i> } Example: Device# show aaa user all	Displays AAA subscriber information for all users or a specified user.
Step 4	show sss session [all] Example: Device# show sss session	Displays Subscriber Service Switch (SSS) session status.

Enabling Periodic Session Update

Perform this task to enable Intelligent Services Gateway (ISG) to periodically synchronize the dynamic accounting statistics (counters) for subscriber sessions on the standby processor, to suppress accounting on and accounting off messages during a switchover, or to send the interim accounting record first after a switchover.

SUMMARY STEPS

1. enable
2. configure terminal
3. subscriber redundancy dynamic periodic-update interval *minutes*
4. aaa accounting redundancy suppress system-records
5. aaa accounting redundancy best-effort-reuse send-interim
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	subscriber redundancy dynamic periodic-update interval <i>minutes</i> Example: Device(config)# subscriber redundancy dynamic periodic-update interval 30	Enables periodic update of accounting statistics for subscriber sessions.

	Command or Action	Purpose
Step 4	aaa accounting redundancy suppress system-records Example: <pre>Device(config)# aaa accounting redundancy suppress system-records</pre>	Suppresses accounting on and accounting off messages during a switchover.
Step 5	aaa accounting redundancy best-effort-reuse send-interim Example: <pre>Device(config)# aaa accounting redundancy best-effort-reuse send-interim</pre>	Sends the interim accounting record first after a switchover for session and service accounting.
Step 6	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.

Verifying Periodic Session Update

To verify and troubleshoot the configuration of the periodic session update on the ISG device, use any of the following commands in privileged EXEC mode. You can use these commands in any order.

Command	Purpose
show ccm clients	Displays information about cluster control manager (CCM) clients in HA dual RP systems.
show ccm queues	Displays CCM queue statistics for HA dual RP systems.
show ccm sessions	Displays information about CCM sessions in HA dual RP systems.

Troubleshooting ISG Accounting

Use the commands in this task to monitor and troubleshoot Intelligent Services Gateway (ISG) accounting. All these commands are optional and can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **debug aaa accounting**
3. **debug radius brief**
4. **debug subscriber feature name accounting event**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug aaa accounting Example: Device# debug aaa accounting	Displays information about authentication, authorization, and accounting (AAA) TACACS+ authentication.
Step 3	debug radius brief Example: Device# debug radius brief	Enables debugging of the RADIUS configuration.
Step 4	debug subscriber feature name accounting event Example: Device# debug subscriber feature name accounting event	Displays diagnostic information about the installation and removal of ISG features on ISG subscriber sessions.

Configuration Examples for ISG Accounting

Example: Enabling ISG per-Flow Accounting

Example: Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server

The following example shows Intelligent Services Gateway (ISG) per-flow accounting configured in a remote service profile for a service called “videol”:

```
videol      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"
```

Example: Enabling ISG per-Flow Accounting in a Service Policy Map

The following example shows ISG per-flow accounting configured in a service policy map for a service called “videol”:

```
class-map type traffic match-any videol
  match access-group output 101
  match access-group input 100
!
```



```
policy-map type service videol
  class type traffic videol
    accounting aaa list mlist1
```

Example: Enabling ISG per-Service Accounting

The following configuration example allows multiple services in a single Access-Accept message and enables session accounting for services. The example also shows how to enable RADIUS to authorize the subscriber to access services.

```
subscriber service multiple-accept
subscriber service session-accounting
subscriber authorization enable
```

Example: Enabling a per-User Accounting List

The following example shows a dummy service configured for an Intelligent Services Gateway (ISG) per-session accounting list configured on an authentication, authorization, and accounting (AAA) server:

```
userxxx2@cisco.com Cleartext-Password := "cisco111"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 192.168.17.17,
  Cisco-Account-Info += "ADUMMYSERVICE",

DUMMYSERVICE Cleartext-Password := "cisco"
  Cisco-AVPair+= "accounting-list=testacct",
```

Example: Enabling ISG per-Service Accounting in a Service Policy Map

The following example shows how to configure per-service accounting in a service policy map on the Intelligent Services Gateway (ISG) device:

```
class-map type traffic match-any classmap1
!
policy-map type service polmap1
  class type traffic classmap1
    accounting aaa list mlist1
```

Example: Configuring Postpaid Tariff Switching

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"
```

Example: Enabling Periodic Session Update

The following example shows that the Intelligent Services Gateway (ISG) device is configured to suppress accounting on and accounting off messages during a switchover and to send the interim accounting record first after a switchover. The ISG device also synchronizes the accounting counters for subscriber sessions on the standby processor every 30 minutes.

```
subscriber redundancy dynamic periodic-update interval 30
!
aaa accounting redundancy suppress system-records
aaa accounting redundancy best-effort-reuse send-interim
```

Examples: Verifying ISG Accounting and Postpaid Tariff Switching

This section contains examples of output for the “Verifying ISG Accounting and Postpaid Tariff Switching” task.

show subscriber session Output When ISG Accounting Is Applied to a Flow

In the following example, Intelligent Services Gateway (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.

```
Device# 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: videol
  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: videol
  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: videol, Active Time = 3 minutes, 46 seconds
```

show subscriber session Output When ISG Accounting Is Applied to a Session

The following is sample output from the **show subscriber session** command for a session rather than a flow:

```
Device# 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
```

The following is sample output from the **show aaa sessions** command:

```
Device# 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
```

Output for a Specific User

The following is sample output from the **show aaa user** command:

```

Device# show aaa 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

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
Dbg: 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

```
Device# 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

```

Example: Troubleshooting ISG Accounting

The following is sample output from the **debug aaa accounting** command:

```

Device# debug aaa accounting

16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop:
task_id=70 service=exec port=10 protocol=telnet address=209.165.201.1 cmd=glare bytes_in=308
bytes_out=76 paks_in=45

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
AAA configuration tasks	<i>Authentication, Authorization, and Accounting Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference: Commands A to C</i>
Configuring ISG subscriber services	“Configuring ISG Subscriber Services” section in the <i>Intelligent Services Gateway Configuration Guide</i>
HA commands	Cisco IOS High Availability Command Reference
HA configuration	<i>Cisco IOS XE High Availability Configuration Guide</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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 31: Feature Information for ISG Accounting

Feature Name	Releases	Feature Information
1 second accuracy—IPv6 session counters and ISGv6 services	Cisco IOS XE Release 3.5S	Support for PPP IPv6 and dual-stack sessions was added to the Subscriber Accounting Accuracy feature.

Feature Name	Releases	Feature Information
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 accounting stop records for sessions and services to an accounting server for postpaid billing. The accounting server interprets the records to generate bills.
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.
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 Flow Control—SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for ISG features including ISG accounting.



CHAPTER 22

Configuring ISG Support for Prepaid Billing

Intelligent Services Gateway (ISG) is a 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 re-authorization 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-based and volume-based prepaid billing.

This module describes how to configure ISG support for prepaid billing for IPv4, IPv6 and dual-stack sessions.

- [Finding Feature Information, on page 281](#)
- [Prerequisites for ISG Prepaid Billing Support, on page 281](#)
- [Restrictions for ISG Prepaid Billing Support, on page 282](#)
- [Information About ISG Prepaid Billing Support, on page 282](#)
- [How to Configure ISG Support for Prepaid Billing, on page 284](#)
- [Configuration Examples for ISG Prepaid Billing Support, on page 295](#)
- [Additional References, on page 299](#)
- [Feature Information for ISG Support for Prepaid Billing, on page 300](#)

Finding Feature Information

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

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

- A subscriber session is created and a method of service activation is in place.
- Traffic classes for IPv4, IPv6, and dual-stack sessions are configured.

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.
- ISG prepaid billing support can not be applied to per-user ACL on IPv6 traffic.
- 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

ISG prepaid billing is supported for IPv4, IPv6, and dual-stack subscribers. This feature allows ISG to check the subscriber's available credit to determine whether to activate a specified service 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 re-authorization. During re-authorization, 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: $\text{access rate} \times 15 > \text{QV} < \text{access rate} \times 300$. 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: $2.5 \text{ MB} \times 15 \text{ seconds} > \text{QV} < 2.5 \text{ MB} \times 300 \text{ seconds}$. 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 $\text{QV} = 100 \text{ MB}$.

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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>radius-server attribute 44 include-in-access-req [<i>vrf vrf-name</i>]</p> <p>Example:</p> <pre>Router(config)# radius-server attribute 44 include-in-access-req</pre>	Sends RADIUS attribute 44 (Accounting Session ID) in Access-Request packets before user authentication.
Step 4	<p>radius-server attribute 55 include-in-acct-req</p> <p>Example:</p> <pre>Router(config)# radius-server attribute 55 include-in-acct-req</pre>	Sends the RADIUS attribute 55 (Event-Timestamp) in Accounting-Request packets.
Step 5	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	Exits the current configuration mode and returns to privileged EXEC mode.
Step 6	<p>show subscriber session [<i>detailed</i>] [<i>identifier identifier</i> <i>uid session-id</i>] <i>username name</i>]</p> <p>Example:</p> <pre>Router# show subscriber session detailed</pre>	(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.

Before you begin

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.
Step 3	subscriber feature prepaid { <i>name-of-config</i> default }	Creates a new ISG prepaid configuration or specifies an existing configuration so it can be modified, and enters prepaid configuration mode.
	Example: Router(config)# subscriber feature prepaid conf-prepaid	
Step 4	interim-interval <i>number-of-minutes</i> 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 } <i>name-of-method-list</i> 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 <i>password</i> Example: Router(config-prepaid)# password cisco	Configures the password to be used for ISG prepaid authorization and reauthorization requests.

	Command or Action	Purpose
Step 7	<p>threshold {<i>time seconds</i> volume {<i>kilobytes Kbytes</i> <i>megabytes Mbytes</i> <i>bytes bytes</i>}}</p> <p>Example:</p> <pre>Router(config-prepaid)# threshold time 20</pre>	<p>Configures the threshold at which ISG will send a reauthorization request to the prepaid billing server.</p> <ul style="list-style-type: none"> • 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	<p>end</p> <p>Example:</p> <pre>Router(config-prepaid)# end</pre>	<p>Exits the current configuration mode and returns to privileged EXEC mode.</p>
Step 9	<p>show subscriber session [detailed] [identifier <i>identifier</i> uid <i>session-id</i> username <i>name</i>]</p> <p>Example:</p> <pre>Router# show subscriber session detailed</pre>	<p>(Optional) Displays ISG subscriber session information.</p>

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

Perform this task to enable ISG prepaid billing support in a service policy map.

Before you begin

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type service mp3</pre>	Creates or defines a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	[<i>priority</i>] class type traffic <i>class-map-name</i> Example: <pre>Router(config-service-policymap)# class type traffic class-acl-101</pre>	Associates a previously configured traffic class with the policy map, and enters control policy-map traffic class configuration mode.
Step 5	prepaid config <i>name-of-configuration</i> Example: <pre>Router(config-control-policymap-class-traffic)# prepaid config conf-prepaid</pre>	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters. <p>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.</p>
Step 6	end Example: <pre>Router(config-control-policymap-class-traffic)# end</pre>	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	show subscriber session [detailed] [identifier <i>identifier</i> uid <i>session-id</i>] username <i>name</i>] Example: <pre>Router# show subscriber session detailed</pre>	(Optional) Displays ISG subscriber session information.

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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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: <pre>26,9,1 = "prepaid-config={<name-of-config> default"</pre>	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters.

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

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. However, in case of dual-stack subscriber, the ISG redirects the subscriber to the portal in case of credit exhaustion.



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.

Before you begin

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type service redirect-service</pre>	Creates or defines a service policy map, which is used to define an ISG service and enters service policy-map configuration mode.
Step 4	[<i>priority</i>] class type traffic <i>class-name</i> Example: <pre>Router(config-service-policymap)# class type traffic class-all</pre>	(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 <i>server-group-name</i> ip <i>ip-address</i> [port <i>port-number</i>]} [duration <i>seconds</i>] [frequency <i>seconds</i>] Example: <pre>Router(config-service-policymap-class-traffic)# redirect to group redirect-sg</pre>	Redirects traffic to a specified server or server group.
Step 6	end Example: <pre>Router(config-control-policymap-class-traffic)# end</pre>	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	show subscriber session [detailed] [identifier <i>identifier</i> uid <i>session-id</i> username <i>name</i>] Example: <pre>Router# show subscriber session detailed</pre>	(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.

Before you begin

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.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: Router(config)# policy-map type control policyA	Creates or modifies a policy map that defines a control policy.
Step 4	class type control { <i>control-class-name</i> 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	<i>action-number</i> service-policy type service name <i>policy-map-name</i> 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:	Exits the current configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router (config-control-policy-map-class-control) # end	
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, on page 293](#) section.

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.

Before you begin

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type control policyB</pre>	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 {<i>control-class-name</i> always} event quota-depleted Example: <pre>Router(config-control-policymap)# class type control always event quota-depleted</pre>	Specifies a control class and event for which actions may be configured, and enters control policy-map class control configuration mode.
Step 5	<i>action-number</i> set-param drop-traffic false Example: <pre>Router(config-control-policymap-class-control)# 1 set-param drop-traffic false</pre>	Configures ISG to continue to allow traffic to pass when the quota has been depleted.
Step 6	end Example: <pre>Router(config-control-policymap-class-control)# end</pre>	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	show subscriber session [detailed] [identifier <i>identifier</i> uid <i>session-id</i> username <i>name</i>] Example: <pre>Router# show subscriber session detailed</pre>	(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

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

```


Example: Configuring Prepaid Support for Simple IP Dual Stack Sessions

```

#-----
# AAA Configuration
#-----
aaa group server radius PREPAID_V4
server-private 6.6.6.1
!
aaa group server radius PREPAID_V6
server-private 8.8.8.1
!
aaa group server radius SERVER_GROUP1
server name RAD1
!
aaa authorization network PREPAID_V4 group PREPAID_V4
aaa authorization network PREPAID_V6 group PREPAID_V6
aaa authorization subscriber-service default local group SERVER_GROUP1
#-----
# Prepaid Service Definition
#-----
subscriber feature prepaid V4_PREPAID
threshold time 100 seconds
threshold volume 1000 bytes
interim-interval 2 minutes
method-list author PREPAID
method-list accounting List3
password cisco
!
subscriber feature prepaid V6_PREPAID
threshold time 0 seconds
threshold volume 0 bytes
interim-interval 2 minutes
method-list author PREPAID_V6
method-list accounting List1
password cisco
#-----
# Redirect Portal Configuration
#-----
redirect server-group IPv6_PORTAL
server ip 3001::2 port 23
!
redirect server-group IPv4_PORTAL
server ip 4.4.4.1 port 23
#-----
# Traffic Class Configuration
#-----
class-map type traffic match-any IPv4_L4R
match access-group input name ipv4_l4r_in
match access-group output name ipv4_l4r_out
!
class-map type traffic match-any IPv6_L4R
match access-group input name ipv6_l4r_in
match access-group output name ipv6_l4r_out

class-map type traffic match-any IPv4_PRE
match access-group input name ipv4_in
match access-group output name ipv4_out
!
class-map type traffic match-any IPv6_PRE
match access-group input name ipv6_in
match access-group output name ipv6_out

```

Example: Configuring Prepaid Support for Simple IP Dual Stack Sessions

```

class-map type control match-all PRE_V4
match service-name PREPAID_V4_SERVICE
!
class-map type control match-all PRE_V6
match service-name PREPAID_V6_SERVICE
#-----
# IPv4 and IPv6 Prepaid Service Configuration
#-----
policy-map type service PREPAID_V4_SERVICE
10 class type traffic IPv4_PRE
    prepaid config V4_PREPAID
!
class type traffic default in-out
    drop
!
policy-map type service PREPAID_V6_SERVICE
10 class type traffic IPv6_PRE
    prepaid config V6_PREPAID
!
class type traffic default in-out
    drop
!
#-----
# IPv4 and IPv6 L4R Service Definition
#-----
policy-map type service L4REDIRECT_SERVICE_V4
5 class type traffic IPv4_L4R
    redirect to group DASHBOARD
!
class type traffic default in-out
    drop
!
policy-map type service L4REDIRECT_SERVICE_V6
5 class type traffic IPv6_L4R
    redirect to group IPv6_PORTAL
!
class type traffic default in-out
    drop
#-----
# Service Policy Configuration
#-----
policy-map type control TAL
class type control PRE_V4 event credit-exhausted
    1 service-policy type service name L4REDIRECT_SERVICE_V4
!
class type control PRE_V6 event credit-exhausted
    1 service-policy type service name L4REDIRECT_SERVICE_V6
!
class type control always event session-start
    9 authorize identifier mac-address
!
class type control always event quota-depleted
    1 set-param drop-traffic TRUE
!
#-----
# IPv4 and IPv6 Access Lists Configuration
#-----
ip access-list extended ipv4_in
permit ip any 4.4.4.0 0.0.0.255
!
ip access-list extended ipv4_out
permit ip 4.4.4.0 0.0.0.255 any
!
ip access-list extended ipv4_l4r_in

```

```

permit tcp any any
permit udp any any
!
ip access-list extended ipv4_l4r_out
permit tcp any any
permit udp any any
!
ipv6 access-list ipv6_in
permit ipv6 any 3001::/64
!
ipv6 access-list ipv6_out
permit ipv6 3001::/64 any
!
ipv6 access-list ipv6_l4r_in
permit tcp any any
permit udp any any
!
ipv6 access-list ipv6_l4r_out
permit udp any any
permit tcp any any
!
#-----
# RADIUS Server Configuration
#-----
radius-server host 6.6.6.1
radius-server host 8.8.8.1
!
radius server RAD1
address ipv4 4.4.4.1 auth-port 1645 acct-port 1646

```

Additional References

Related Documents

Related Topic	Document Title
AAA configuration tasks	The “Authentication, Authorization, and Accounting (AAA)”? section in the <i>Security Configuration Guide</i>
AAA commands	<i>Cisco IOS Security Command Reference</i>
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 32: 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.
Prepaid Support for Dual-Stack Sessions	Cisco IOS XE Release 3.13S	ISG prepaid billing support is extended to dual-stack sessions.



CHAPTER 23

Configuring ISG Policies for Session Maintenance

Intelligent Services Gateway (ISG) is a 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, on page 303](#)
- [Prerequisites for ISG Policies for Session Maintenance, on page 304](#)
- [Information About ISG Policies for Session Maintenance, on page 304](#)
- [How to Configure ISG Policies for Session Maintenance, on page 306](#)
- [Configuration Examples for ISG Policies for Session Maintenance, on page 314](#)
- [Additional References, on page 317](#)
- [Feature Information for ISG Policies for Session Maintenance, on page 317](#)

Finding Feature Information

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

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.

Information About ISG Policies for Session Maintenance

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.

HA Support for Session Maintenance Timers

The SSO and ISSU feature provides high availability (HA) support for ISG timers including the connection timer, session timer, and the session keepalive. The timers and keepalive are restarted on the new standby Route Processor (RP) after a stateful switchover (SSO) or In Service Software Upgrade (ISSU) event.

For information about configuring HA on the ISG router, see the [High Availability Configuration Guide, Cisco IOS XE Release 3S](#).

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type trafficclass-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 <i>policy-map-name</i> Example: Router(config)# policy-map type service policy1	Enters policy map configuration mode so you can begin configuring the service policy.
Step 4	[<i>priority</i>] class type trafficclass-map-name Example: Router(config-control-policymap)# class type traffic class1	Associates a previously configured traffic class with the policy map.

	Command or Action	Purpose
Step 5	timeout absolute <i>duration-in-seconds</i> Example: <pre>Router(config-control-policy-map-class-control)# timeout absolute 30</pre>	Specifies the session lifetime, in seconds.
Step 6	end Example: <pre>Router(conf-subscriber-profile)# end</pre>	Returns to privileged EXEC 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".

Configuring the Session Timer on a AAA Server

Perform this task to configure the session timer in a service profile on a AAA server.

SUMMARY STEPS

1. **Session-Timeout**=*duration-in-seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Session-Timeout = <i>duration-in-seconds</i>	Sets the IETF RADIUS session timer (attribute 27) in a user or service profile, in a range from 0 to 31104000 seconds.

Configuring 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* [**both** | **inbound**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type service policy1</pre>	Enters policy map configuration mode so you can begin configuring the service policy.
Step 4	[<i>priority</i>] class type traffic <i>class-map-name</i> Example: <pre>Router(config-service-policymap)# class type traffic class1</pre>	Associates a previously configured traffic class to the policy map.
Step 5	timeout idle <i>duration-in-seconds</i> [both inbound] Example: <pre>Router(config-control-policymap-class-traffic)# timeout idle 3000 inbound</pre>	Specifies how long a connection can be idle before it is terminated and in which direction to apply the timer. The range is platform and release-specific. For more information, use the question mark (?) online help function.
Step 6	end Example: <pre>Router(config-control-policymap-class-traffic)# end</pre>	Returns to privileged EXEC 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".

Configuring the Connection Timer on a AAA Server

Perform this task to set the connection timer (idle timeout) in a AAA service profile.

SUMMARY STEPS

1. **idle-timeout= *duration-in-seconds***

2. `idle-timeout-direction= direction`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>idle-timeout= duration-in-seconds</code>	Sets IETF RADIUS attribute 28 in a user or service profile, in a range from 1 to 15552000 seconds.
Step 2	<code>idle-timeout-direction= direction</code>	Sets the direction of subscriber traffic on which to apply the idle timeout. Values are inbound or both . If the timer is configured without specifying a direction, it is applied by default to the outbound direction.

Example

```
simulator radius subscriber 999
attribute 28 numeric 100
vsa cisco generic 1 string "subscriber:idle-timeout-direction=inbound"
attribute 44 string "00000008"
```

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	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	<code>show subscriber session all</code> Example: Router# <code>show subscriber session all</code>	Displays current subscriber information, including reports about the timers that are enabled.
Step 3	<code>end</code> Example: Router# <code>end</code>	Returns to privileged EXEC mode.

Troubleshooting the Session and Connection Timer Settings

The following sections describe the **debug** commands that can be used to troubleshoot the session maintenance timers:

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, we recommend that you 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 33: 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.

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type service <i>policy-map-name</i> Example: Router(config)# policy-map type service policymap1	Enters service policy map configuration mode.
Step 4	keepalive [idle <i>idle-seconds</i>] [attempts <i>max-retries</i>] [interval <i>retry-seconds</i>] [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. <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
		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 idle 7 attempts 3 interval 1 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 to 10 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.

	Command or Action	Purpose
Step 5	client <i>ip-address</i> 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. <ul style="list-style-type: none"> The example specifies 10.10.10.11 as the IP address of the RADIUS client.
Step 6	port <i>port-number</i> Example: Router(config-locsvr-da-radius)# port 1650	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. <ul style="list-style-type: none"> The example specifies port 1650.
Step 7	server-key <i>word</i> Example: Router(config-locsvr-da-radius)# server-key abc	Configures the RADIUS key to be shared between a device and RADIUS clients. <ul style="list-style-type: none"> 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

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-Templat1, 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]

```

Example: Session Timer Debug Output

```

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-Templat1, 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
02DFD8
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] added
02DFD8 [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
HA commands	Cisco IOS High Availability Command Reference
HA configuration	<i>High Availability Configuration Guide</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	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 34: Feature Information for ISG Policies for Session Maintenance

Feature Name	Releases	Feature 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 Information
ISG: Session Protection and 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 (ISG).
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.
Downstream Idle Timeout Support	Cisco IOS XE Release 3.4.1S	The connection timer (idle timeout) can be applied to subscriber traffic in a specific direction, through an ISG service policy map or a AAA service profile. The following command was modified: timeout idle.
Session Timeout Ext to 360 Days	Cisco IOS XE Release 3.5S	Maximum value of the session timer was increased to 31,104,000 seconds. Maximum value of the connection timer was increased to 15,552,000 seconds. The following commands were modified: timeout absolute, timeout idle.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for the session maintenance timers and keepalive.



CHAPTER 24

Redirecting Subscriber Traffic Using ISG Layer 4 Redirect

Intelligent Services Gateway (ISG) is a 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 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, on page 319](#)
- [Restrictions for Redirecting ISG Subscriber Traffic, on page 319](#)
- [Information About Redirecting ISG Subscriber Traffic, on page 320](#)
- [How to Configure ISG Layer 4 Redirect, on page 321](#)
- [Configuration Examples for ISG Layer 4 Redirect, on page 326](#)
- [Additional References, on page 328](#)
- [Feature Information for Redirecting ISG Subscriber Traffic, on page 329](#)

Finding Feature Information

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

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 on a TC in a service, but not directly on a session.

Information About Redirecting ISG Subscriber Traffic

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 source IP address and port to the original packet's destination.

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.

HA Support for Layer 4 Redirect

The SSO and In ISSU feature provides high availability (HA) support for the ISG Layer 4 Redirect feature. Layer 4 redirect includes the selected service group in its checkpointed data during the initial session and bulk synchronization. The standby processor uses the service group instead of selecting a new one.

Because Layer 4 redirect translations are maintained on the forwarding processor, the translation entries and associated timers are preserved after a route processor stateful switchover (SSO) or In Service Software Upgrade (ISSU) event. The entries are re-created, however, on the new active processor after a forwarding processor switchover.

For information about configuring HA on the ISG router, see the [High Availability Configuration Guide, Cisco IOS XE Release 3S](#).

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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	redirect server-group <i>group-name</i> 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 <i>ip-address</i> port <i>port-number</i> Example: Router(config-sg-l4redirect-group)# server ip 10.0.0.1 port 8080	Adds a server to a redirect server group. <ul style="list-style-type: none"> • 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.

Before you begin

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	redirect session-limit <i>maximum-number</i> 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 <i>policy-map-name</i> 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 <i>class-name</i> 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.
Step 6	redirect to {group <i>server-group-name</i> ip <i>ip-address</i> [port <i>port-number</i>]}[duration <i>seconds</i>] [frequency <i>seconds</i>] 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

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 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	<p>Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server.</p> <p>Example:</p> <pre>Cisco-AVPair = "ip:l4redirect=redirect to {group server-group-name ip server-ip-address [port port-number]} [duration seconds] [frequency seconds]"</pre>	Redirects traffic to a specified server or server group.

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 **show** commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show redirect translations** [**ip** *ip-address* | **ipv4** | **ipv6**] [**verbose**]
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	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show redirect translations [ip <i>ip-address</i> ipv4 ipv6] [verbose]</p> <p>Example:</p>	Displays ISG Layer 4 redirect translations for sessions.

	Command or Action	Purpose
	Router# show redirect translations ip 10.0.0.0	
Step 3	<p>show redirect group <i>[group-name]</i></p> <p>Example:</p> <p>Router# show redirect group redirect1</p>	Displays information about ISG redirect server groups.
Step 4	<p>show subscriber session <i>[detailed]</i> <i>[identifier identifier uid session-id username name]</i></p> <p>Example:</p> <p>Router# show subscriber session detailed</p>	Displays ISG subscriber session information.

Examples

The following is sample output from the **show redirect translations** command showing the number of active redirect translations:

```
Router# show redirect translations

Maximum allowed number of L4 Redirect translations per session: 5
Destination IP/port   Server IP/port   Prot  In Flags  Out Flags  Timestamp
10.0.1.2             23              10.0.2.2 23      TCP                Oct 21 2009 11:48:01
10.0.1.2             23              10.0.2.2 23      TCP                Oct 21 2009 11:48:01
10.0.1.2             23              10.0.2.2 23      TCP                Oct 21 2009 11:48:01
Total Number of Translations: 3
Highest number of L4 Redirect: 3 by session with source IP 10.0.0.2
```

The following sample output from the **show subscriber session** command 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: FastEthernet0/0/0.505
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: FastEthernet0/0/0.505, Active Time = 42 minutes, 54 seconds

```

Configuration Examples for ISG Layer 4 Redirect

Example: Redirecting Unauthenticated Subscriber Traffic

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 name BLIND-RDT
!
class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply name BLIND-RDT
policy-map type service BLIND-RDT
class type traffic CLASS-ALL
  redirect to group PORTAL
!
redirect server-group PORTAL
server ip 2001:ABCD:14::6, Port 8000

```

Example: Redirecting Unauthorized Subscriber Traffic

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 always 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

```

Example: Initial ISG Redirection

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 initial-rdt
  class type control always event session-start
    1 service-policy type service name initial-rdt-profile
  !
policy-map type service initial-rdt-profile

```

Example: Periodic ISG Redirection

```
class type traffic CLASS-ALL
  redirect to group ADVT duration 60
```

Example: Periodic ISG Redirection

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
```

Example: Redirecting DNS Traffic

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
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Configuring ISG subscriber services	“Configuring ISG Subscriber Services” module in this guide
HA commands	Cisco IOS High Availability Command Reference
HA configuration	<i>High Availability Configuration Guide</i>

Technical Assistance

Description	Link
<p>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

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 35: Feature Information for Redirecting ISG Subscriber Traffic

Feature Name	Releases	Feature Information
<p>ISG: Flow Control: Flow Redirect</p>	<p>Cisco IOS XE Release 2.2</p>	<p>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.</p>
<p>Parameterization for ACL and Layer 4 Redirect</p>	<p>Cisco IOS XE Release 2.4</p>	<p>The Parameterization for ACL and Layer 4 Redirect feature provides parameterization enhancements for access control lists and Layer 4 redirect.</p>
<p>ISG: IPv6 Support phase II</p>	<p>Cisco IOS XE Release 3.5S</p>	<p>IPv6 support was added for the Layer 4 Redirect feature. The following commands were introduced or modified: redirect session-limit, redirect to, server ip, show redirect group, show redirect translations.</p>
<p>ISG: Flow Control: SSO/ISSU</p>	<p>Cisco IOS XE Release 3.5S</p>	<p>HA support was added for ISG features including the Layer 4 Redirect feature.</p>



CHAPTER 25

Configuring Layer 4 Redirect Logging

Intelligent Services Gateway (ISG) is a software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes the Layer 4 Redirect Logging feature.

- [Finding Feature Information, on page 331](#)
- [Prerequisites for Layer 4 Redirect Logging, on page 331](#)
- [Information About Layer 4 Redirect Logging, on page 332](#)
- [How to Configure Layer 4 Redirect Logging, on page 334](#)
- [Configuration Examples for Layer 4 Redirect Logging, on page 336](#)
- [Additional References, on page 336](#)
- [Feature Information for Layer 4 Redirect Logging, on page 337](#)

Finding Feature Information

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

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 Layer 4 Redirect Logging

The Layer 4 Redirect feature must be enabled. For configuration information, see the module “Redirecting Subscriber Traffic Using ISG Layer 4 Redirect” in the *Intelligent Services Gateway Configuration Guide, Cisco IOS XE*.

Information About Layer 4 Redirect Logging

ISG Layer 4 Redirect Logging

The Layer 4 Redirect Logging feature allows ISG to capture records of the creation and deletion events for Layer 4 redirect translation entries. These records can identify users who have applications that do not react to HTTP redirect.

The ISG router acts as an exporter of the Layer 4 redirect logging information, sending a UDP packet periodically to the configured external collector. The packet contains all of the Layer 4 redirect logging records, in the NetFlow version 9 export format, for IPv4, IPv6, and dual-stack sessions. The ISG router tracks every creation and deletion event for Layer 4 redirect translation entries on the router. A packet containing the logging records is generated and sent to the external collector after the first of one of the following events occurs:

- A predefined amount of Layer 4 redirect logging data has accumulated in the local buffer.
- A predefined amount of time has passed without the router sending any data records to the collector, and there are data records in the local buffer to be sent.

If more than one type of logging feature is configured on the same router (for example, network address translation (NAT) or Firewall), the number of events that can be generated at one time is shared among all of the logging features. Logging requests are served on a first-come first-serve basis.

Any external collector that supports the NetFlow version 9 or IP information export (IPFIX) protocol can be used to process Layer 4 redirect logging data exported by the ISG router.

Template Formats for Layer 4 Redirect Logging

The Layer 4 Redirect Logging records that the ISG router sends to the collector use a preconfigured template format. The NetFlow version 9 export packets include a NetFlow packet header followed by the data records and template records that define the structure of the data records, in a format corresponding to the configured template.

The following tables list the fields that are included in records sent to the external collector, in the basic and extended IPv4 and IPv6 templates. The fields are listed in the order in which they appear in the templates. All of the fields in the basic template are also included in the extended template. The last four fields listed in the tables below are the additional fields that are included only in the extended template.

Table 36: IPv4 Translation Entries Record in the Layer 4 Redirect Logging Template

Field Name	Field Type	Field Length (bytes)	Description
sourceIPv4Address	8	4	Source IPv4 address.
sourceTransportPort	7	2	Source port number in the transport header.
destinationIPv4Address	12	4	Destination IPv4 address.

Field Name	Field Type	Field Length (bytes)	Description
destinationTransportPort	11	2	Destination port number in the transport header.
l4rServerIPv4Address	44000	4	Layer 4 redirect server IPv4 address.
l4rServerTransportPort	44001	2	Layer 4 redirect server port number.
protocolIdentifier	4	1	Protocol number in the IP header.
l4rEvent	44003	1	1—Translation Entry Create event 2—Translation Entry Delete event
l4rEventTimestamp	44004	4	Time stamp for this Layer 4 Redirect event.
inPackets	2	4	Incoming packet counter.
outPackets	24	4	Outgoing packet counter.
flowId	148	4	ASR internal identifier (EVSI#) of the session or traffic class on which the Layer 4 Redirect feature is configured.

Table 37: IPv6 Translation Entries Record in the Layer 4 Redirect Logging Template

Field Name	Field Type	Field Length (bytes)	Description
sourceIPv6Address	27	16	Source IPv6 address.
sourceTransportPort	7	2	Source port number in the transport header.
destinationIPv6Address	28	16	Destination IPv6 address.
destinationTransportPort	11	2	Destination port number in the transport header.
l4rServerIPv6Address	44002	16	Layer 4 redirect server IPv6 address.
l4rServerTransportPort	44001	2	Layer 4 redirect server port number.
protocolIdentifier	4	1	Protocol number in the IP header.
l4rEvent	44003	1	1—Translation Entry Create event 2—Translation Entry Delete event
l4rEventTimestamp	44004	4	Time stamp for this Layer 4 redirect event.
inPackets	2	4	Incoming packet counter.
outPackets	24	4	Outgoing packet counter.

Field Name	Field Type	Field Length (bytes)	Description
flowId	148	4	ASR internal identifier (EVSI#) of the session or traffic class on which the L4R feature is configured.

How to Configure Layer 4 Redirect Logging

Enabling ISG Layer 4 Redirect Logging

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **source** *interface-type interface-number*
6. **transport udp** *udp-port*
7. **export-protocol netflow-v9**
8. **template data timeout** *seconds*
9. **exit**
10. **redirect log translations** {**basic** | **extended**} **exporter** *exporter-name*
11. **exit**
12. **show flow exporter** *exporter-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow exporter <i>exporter-name</i> Example: Router(config)# flow exporter L4R-EXPORTER	Creates the flow exporter and enters flow exporter configuration mode. <ul style="list-style-type: none">• This command also allows you to modify an existing flow exporter.

	Command or Action	Purpose
Step 4	destination <i>{ip-address hostname} [vrf vrf-name]</i> Example: <pre>Router(config-flow-exporter)# destination 172.16.10.2</pre>	Specifies the IP address or hostname of the destination system for the exporter.
Step 5	source <i>interface-type interface-number</i> Example: <pre>Router(config-flow-exporter)# source gigabitethernet 0/0/0</pre>	Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams.
Step 6	transport udp <i>udp-port</i> Example: <pre>Router(config-flow-exporter)# transport udp 650</pre>	Specifies the UDP port on which the destination system is listening for exported datagrams.
Step 7	export-protocol <i>netflow-v9</i> Example: <pre>Router(config-flow-exporter)# export-protocol netflow-v9</pre>	(Optional) Specifies the version of the NetFlow export protocol used by the exporter. <ul style="list-style-type: none"> • Default is netflow-v9.
Step 8	template data timeout <i>seconds</i> Example: <pre>Router(config-flow-exporter)# template data timeout 120</pre>	(Optional) Configure resending of templates based on a timeout.
Step 9	exit Example: <pre>Router(config-flow-exporter)# exit</pre>	Exits flow exporter configuration mode and returns to global configuration mode.
Step 10	redirect log translations <i>{basic extended} exporter exporter-name</i> Example: <pre>Router(config)# redirect log translations basic exporter L4R-EXPORTER</pre>	Enables the Layer 4 Redirect Logging feature for ISG. <ul style="list-style-type: none"> • For the <i>exporter-name</i> argument, enter the name of the exporter you configured in step 3.
Step 11	exit Example: <pre>Router(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 12	show flow exporter <i>exporter-name</i> Example: <pre>Router# show flow exporter L4R-EXPORTER</pre>	(Optional) Displays the current status of the specified flow exporter.

Configuration Examples for Layer 4 Redirect Logging

Example: Enabling Layer 4 Redirect Logging

The following example shows that a flow exporter named L4R-EXPORTER is enabled to send Layer 4 Redirect logging information to an external collector:

```
flow exporter L4R-EXPORTER
 destination 172.16.10.2
 source GigabitEthernet 0/0/0
 transport udp 650
 template data timeout 120
!
!
redirect log translations basic exporter L4R-EXPORTER
```

Example: Layer 4 Redirect Logging Events

Layer4 Redirect IPv4 Translation Entry Creation Event

```
Source IPv4 Address 10.1.1.1, Port 1024,
Destination IPv4 Address 10.10.1.1, Port 80,
L4R Server IPv4 Address 10.1.10.1, Port 8000,
Protocol TCP, Translation Entry Create Event
```

Layer 4 Redirect IPv6 Translation Entry Deletion Event

```
Source IPv6 Address 1000::1, Port 1024,
Destination IPv6 Address 2000::1, Port 80,
L4R Server IPv6 Address 2001:ABCD:14::6, Port 8000,
Protocol UDP, Translation Entry Delete Event
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring Layer 4 redirect	“Redirecting Subscriber Traffic Using ISG Layer 4 Redirect” module in the <i>Intelligent Services Gateway Configuration Guide, Cisco IOS XE</i>

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Layer 4 Redirect Logging

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 38: Feature Information for Layer 4 Redirect Logging

Feature Name	Releases	Feature Information
Layer 4 Redirect Logging Enhancement	Cisco IOS XE Release 3.5S	Allows ISG to export Layer 4 redirect logging information to an external collector. The following command was introduced: redirect log translations .
RaBaPol Web Traffic L4 Redirect Logging Enhancement	Cisco IOS XE Release 3.5S	Allows ISG to export Layer 4 redirect logging information to an external collector.



CHAPTER 26

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, on page 339](#)
- [Information About ISG Policies for Regulating Network Access, on page 339](#)
- [How to Configure ISG Policies for Regulating Network Access, on page 341](#)
- [Configuration Examples for ISG Policies for Regulating Network Access, on page 344](#)
- [Additional References, on page 345](#)
- [Feature Information for ISG Policies for Regulating Network Access, on page 345](#)

Finding Feature Information

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

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

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

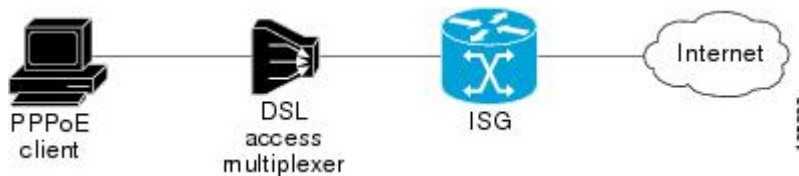
Traffic policing allows you to control the maximum rate of traffic sent or received on an interface. Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds the 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 10: Session-Based Policing



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 11: Flow-Based Policing



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

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.
Step 3	policy-map type service <i>policy-map-name</i> Example:	Creates or modifies a service policy map, which is used to define an ISG service.

What to Do Next

	Command or Action	Purpose
	Router(config)# policy-map type service service1	
Step 4	<i>[priority]class type traffic class-map-name</i> Example: Router(config-service-policymap)# class type traffic silver	Associates a previously configured traffic class with the policy map.
Step 5	police input <i>committed-rate normal-burst excess-burst</i> Example: Router(config-service-policymap-class-traffic)# police input 20000 30000 60000	Configures ISG policing of upstream traffic. <ul style="list-style-type: none"> • These parameters will be used to limit traffic flowing from the subscriber toward the network.
Step 6	police output <i>committed-rate normal-burst excess-burst</i> Example: Router(config-service-policymap-class-traffic)# police output 21000 31500 63000	Configures ISG policing of downstream traffic. <ul style="list-style-type: none"> • These parameters will be used to limit the traffic flowing from the network toward the subscriber.

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: <ul style="list-style-type: none"> • 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" 	Enables ISG policing of upstream and downstream traffic. <ul style="list-style-type: none"> • If you specify the committed rate and normal burst, excess burst will be calculated automatically. • You can specify upstream or downstream parameters first.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • Add the following Policing VSA to the service profile on the AAA server. <p>Example:</p> <pre>26,9,251 "Q;committed-rate;normal-burst;excess-burst;D;committed-rate;normal-burst;excess-burst"</pre>	

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	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show subscriber session [detailed] [identifier <i>identifier</i> uid <i>session-id</i>] username <i>name</i>]</p> <p>Example:</p> <pre>Router# show subscriber session detailed</pre>	<p>Displays ISG subscriber session information.</p>

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

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 <i>Quality of Service Configuration Guide</i>
How to configure DBS	"Controlling Subscriber Bandwidth" module in the <i>Broadband Access Aggregation and DSL Configuration Guide</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 39: 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.



CHAPTER 27

Configuring ISG Integration with SCE

Intelligent Services Gateway (ISG) is a 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, on page 347](#)
- [Prerequisites for Configuring ISG Integration with SCE, on page 347](#)
- [Restrictions for Configuring ISG Integration with SCE, on page 348](#)
- [Information About Configuring ISG Integration with SCE, on page 349](#)
- [How to Configure ISG Integration with SCE, on page 350](#)
- [Configuration Examples for ISG Integration with SCE, on page 357](#)
- [Additional References, on page 359](#)
- [Feature Information for Configuring ISG Integration with SCE, on page 359](#)

Finding Feature Information

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

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

- 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 *Intelligent 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

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 40: 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 <ul style="list-style-type: none"> • Quality of service (QoS) • Multiprotocol label switching (MPLS) virtual private network (VPN) • Redirection • Session termination • Postpaid billing 	Policy enforcement for <ul style="list-style-type: none"> • 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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa server radius {sesm proxy policy-device} Example:	Enters RADIUS server configuration mode and configures the RADIUS profile.

	Command or Action	Purpose
	Router(config)# aaa server radius policy-device	
Step 4	client <i>ipaddress</i> [port <i>coa destination port</i>] [key <i>shared secret</i>] Example: Router(config-locsvr-radius)# client 10.10.10.1 key cisco port 1431	Configures client-specific details. <ul style="list-style-type: none"> • 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 <i>port-number</i> 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. <ul style="list-style-type: none"> • If no port is specified, the default port (1645) is used.
Step 6	accounting port <i>port-number</i> 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. <ul style="list-style-type: none"> • If no port is specified, the default port (1646) is used.
Step 7	key <i>shared-secret</i> Example: Router(config-locsvr-radius)# key xxxxxxxxxxxx	Configures the secret shared between the EPD handler and SCE. <ul style="list-style-type: none"> • 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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-peer address <i>ip-address</i> keepalive <i>seconds</i> Example: <pre>Router(config)# policy-peer address 10.10.10.1 keepalive 6</pre>	Configures the keepalive value, in seconds, for a specific policy defined by the given IP address. <ul style="list-style-type: none"> • 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 <i>seconds</i> Example: <pre>Router(config)# policy-peer keepalive 10</pre>	Configures the keepalive value, in seconds, globally. <ul style="list-style-type: none"> • 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: <pre>Router(config)# exit</pre>	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

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type control <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type control GOLD_POLICY</pre>	Configures the specified policy-map on the ISG and enters policy map configuration mode.
Step 4	class type control { <i>class-map-name</i> always } event session-start Example: <pre>Router(config-control-policymap)# class type control always event acct-notification</pre>	Specifies to apply actions matching conditions defined by the class-map-name or always for an event type. <ul style="list-style-type: none"> • Event types include the following: account-logout, 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	<i>action-number</i> service-policy type service name <i>service-name</i> Example: <pre>Router(config-control-policymap)# 1 service-policy type service name sce-service</pre>	Defines the list of actions to be performed when the control policy is matched.

	Command or Action	Purpose
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

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type service <i>service-map-name</i> Example: <pre>Router(config-traffic-classmap)# policy-map type service SVC</pre>	Creates a service and enters traffic class map configuration mode.
Step 4	class-map type traffic <i>class-map-name</i> Example: <pre>Router(config-control-policymap-class-control)# class-map type traffic bar</pre>	Defines a traffic class and enters control policy-map class configuration mode.
Step 5	accounting aaa list <i>listname</i> Example: <pre>Router(config-service-policymap)# accounting aaa list list1</pre>	Configures accounting for ISG and enters service policy map configuration mode.
Step 6	sg-service-type external-policy Example: <pre>Router(config-control-policymap)# sg-service-type external-policy</pre>	Defines the service as an external policy and enters policy map configuration mode.
Step 7	policy-name <i>name</i> Example: <pre>Router(config-control-policymap)# policy-name gold</pre>	Defines a corresponding external policy name on the SCE.
Step 8	service-monitor enable Example: <pre>Router(config-control-policymap)# service-monitor enable</pre>	Enables service monitoring for the external policy device.

	Command or Action	Purpose
	Example:	
Step 9	exit Example: <pre>Router(config-pol-map)# exit</pre>	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

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
  192.168.12.0:0xffffffff00 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
  192.168.12.0:0xffffffff00 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 <i>Security Configuration Guide</i>
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" module in the <i>Cisco IOS Security Command Reference</i>
SCE configuration	Cisco Service Control Engine (SCE) Software Configuration Guide , Release 3.1

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 41: 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	<p>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.</p> <p>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.</p>



CHAPTER 28

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, on page 361](#)
- [Information About Service Gateway Interface, on page 361](#)
- [How to Enable Service Gateway Interface, on page 362](#)
- [Configuration Examples for Service Gateway Interface, on page 364](#)
- [Additional References, on page 365](#)
- [Feature Information for Service Gateway Interface, on page 366](#)

Finding Feature Information

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

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

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 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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	sgi beep listener [<i>port</i>][acl <i>access-list</i>][sasl <i>sasl-profile</i>][encrypt <i>trustpoint</i>] Example: Router(config)# sgi beep listener 2089	Enables the SGI feature.

	Command or Action	Purpose
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 of an 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

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	<i>Intelligent Services Gateway Configuration Guide</i>

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
•	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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 42: 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.



CHAPTER 29

ISG MIB

The Intelligent Services Gateway (ISG) MIB feature defines all objects relevant to subscriber session details, subscriber session statistics, and subscriber service information as MIB objects. These MIB objects are accessed using Simple Network Management Protocol (SNMP), and the network administrators can monitor their ISG box's session in a centralized management server for public wireless LAN deployment requirements.

- [Information About ISG MIB, on page 367](#)
- [Additional References, on page 368](#)
- [Feature Information for ISG MIB, on page 369](#)

Information About ISG MIB

ISG MIB Overview

The ISG MIB feature introduces MIB support in Cisco software. The ISG MIB is accessed using remote SNMP software clients. MIB table objects are accessed as read-only through GET, GETNEXT, GETBULK, SET, and TRAP (notification) requests.

Subscriber Session MIB

The CISCO-SUBSCRIBER-SESSION-MIB contains objects to monitor subscriber session details, session statistics, and job tables to query specific subscriber information.

The following tables are implemented from this MIB:

- **Subscriber Session Table**—This table contains detailed information about a subscriber session. Each row in the table represents a subscriber session. The table row (subscriber session) can be indexed through the ifIndex object, which is unique for each subscriber session.
- **Subscriber Session Statistics Table**—This table provides ISG box-wide subscriber session aggregate statistics information. Each subscriber's session statistics are accessed based on the scope of aggregation. Session type and entity are used to define the scope of aggregation.
- **Subscriber Session Job Tables and Notification**—These tables allow an Element Management System (EMS) or Network Management System (NMS) to submit a job to perform a query on a subset of the current subscriber sessions maintained by the ISG system. The EMS or NMS can create a job and provision it to perform an operation with specified parameters. Every query is a job for the ISG MIB and has a unique Job ID associated with it.

Dynamic Template MIB

The CISCO-DYNAMIC-TEMPLATE-MIB contains subscriber service information. This information is captured through Dynamic Template MIB definitions and presented in Object Identification (OID) format.

The following tables from the Dynamic Template MIB capture information about subscriber services, subscriber service association with sessions, and subscriber service usage:

- **Template Table**—This table stores basic subscriber service profile information. Each entry in the template table corresponds to a unique subscriber service. This table entry is uniquely identified with a service name.
- **Template Association Table**—This table is used to identify the list of subscriber services associated with each session.
- **Template Usage Table**—This table is used to identify the list of subscriber sessions using a particular subscriber service.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-DYNAMIC-TEMPLATE-MIB • CISCO-SUBSCRIBER-SESSION-MIB 	<p>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG MIB

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 43: Feature Information for ISG MIB

Feature Name	Releases	Feature Information
ISG MIB	Cisco IOS XE Release 3.7S	The Intelligent Services Gateway (ISG) MIB feature defines all objects relevant to subscriber session details, subscriber session statistics, and subscriber service information as MIB objects. These MIB objects are accessed using Simple Network Management Protocol (SNMP), and the network administrators can monitor their ISG box's session in a centralized management server for public wireless LAN deployment requirements.



CHAPTER 30

ISG SSO and ISSU

The SSO and ISSU feature for Intelligent Services Gateway (ISG) adds high availability (HA) support to ISG features.

- [Finding Feature Information, on page 371](#)
- [Prerequisites for ISG SSO and ISSU, on page 371](#)
- [Information About ISG SSO and ISSU, on page 371](#)
- [Additional References, on page 372](#)
- [Feature Information for ISG SSO and ISSU, on page 373](#)

Finding Feature Information

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

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 SSO and ISSU

SSO and ISSU must be enabled on the ISG router. For configuration information, see the [High Availability Configuration Guide, Cisco IOS XE Release 3S](#).

Information About ISG SSO and ISSU

High Availability for ISG Features

The SSO and ISSU feature provides high availability (HA) support for the following ISG features during a stateful switchover (SSO) or In Service Software Upgrade (ISSU) event:

Feature	Description	Configuration Information
Absolute timeout (session timer)	Timer is restarted on the new standby Route Processor (RP). During bulk synchronization to the standby RP, the remaining timeout duration is sent to the standby RP and used while the feature is being installed.	“Configuring ISG Policies for Session Maintenance” module in this guide
Idle timeout (connection timer)	Timer is restarted on the new standby RP.	“Configuring ISG Policies for Session Maintenance” module in this guide
ISG accounting	Cumulative counters and accounting ID are checkpointed to the standby RP.	“Configuring ISG Accounting” module in this guide
ISG policer (dynamic rate limiting)	HA support was enabled for this feature.	“Configuring MQC Support for IP Sessions” module in this guide
Keepalive	Associated timers are restarted after the control plane switchover.	“Configuring ISG Policies for Session Maintenance” module in this guide
Layer 4 redirect	Layer 4 redirect includes the selected service group in its checkpoint data during the initial session and bulk synchronization. The standby RP uses the service group instead of selecting a new one.	“Redirecting Subscriber Traffic Using ISG Layer 4 Redirect” module in this guide
Port-bundle host key (PBHK)	PBHK includes the allocated bundle ID in its checkpoint data during the initial session and bulk synchronization. Upon session replay, the standby RP reserves the bundle ID instead of allocating a new one.	“Configuring ISG Port-Bundle Host Key” module in this guide
Traffic classes	ISG traffic classes are checkpointed to the standby RP and established during session replay.	“Configuring ISG Subscriber Services” module in this guide

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

Related Topic	Document Title
HA commands	Cisco IOS High Availability Command Reference
HA configuration	High Availability Configuration Guide, Cisco IOS XE Release 3S
Configuring ISG accounting	“Configuring ISG Accounting” module in this guide
Configuring ISG timers	“Configuring ISG Policies for Session Maintenance” module in this guide
Configuring Layer 4 redirect	“Redirecting Subscriber Traffic Using ISG Layer 4 Redirect” module in this guide
Configuring port-bundle host key	“Configuring ISG Port-Bundle Host Key” module in this guide
Configuring traffic classes	“Configuring ISG Subscriber Services” module in this guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG SSO and ISSU

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 44: Feature Information for ISG SSO and ISSU

Feature Name	Releases	Feature Information
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for the following ISG features: <ul style="list-style-type: none">• Absolute Timeout• Idle Timeout• ISG Accounting• ISG Policer• Keepalive• Layer 4 Redirect• Port-Bundle Host Key• Traffic Classes



CHAPTER 31

ISG Debuggability

The ISG Debuggability feature supports conditional debugging of simple IP subscriber sessions whereby debugs of only specified sessions appear in the debug log. The conditions that can be applied to the subscriber sessions include IP address, VRF (IPv4 or IPv6), and MAC address. This module describes how to enable conditional debuggability on Cisco Intelligent Services Gateway (ISG) subscriber sessions.

- [Restrictions for ISG Debuggability, on page 375](#)
- [Information About ISG Debuggability, on page 375](#)
- [Additional References for ISG Debuggability, on page 376](#)
- [Feature Information for ISG Debuggability, on page 376](#)

Restrictions for ISG Debuggability

- Conditional debugging is not available for service manager, QOS policy, most of the command handler, EPD controller, ANCP, and CCM. Also, L2TP, VPDN, PPP, and PPP-based sessions can not be conditionally debugged.

Information About ISG Debuggability

ISG Debugging Behavior

Prior to this enhancement, debugging could be enabled for individual modules through module-wise debugging commands. These debugs provide the flexibility to limit the debugs to a specified subset of modules. However, when these debugs were enabled to debug session-related issues, the logs contained debug information for all sessions which would sometimes be unmanageable depending on the scale. With the conditional debugging enhancement, the debug logs are limited to only specified sessions.

To determine if session debug logs are printed for the specified module, check the following conditions:

- Debug condition is configured for the session identifier
- Debug condition is enabled on the device
- Module debugging is enabled

Additional References for ISG Debuggability

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for ISG Debuggability

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 45: Feature Information for ISG Debuggability

Feature Name	Releases	Feature Information
ISG Debuggability		<p>The ISG Debuggability feature supports conditional debugging of simple IP subscriber sessions whereby debugs of only specified sessions appear in the debug log. The conditions that can be applied to the subscriber sessions include IP address, VRF (IPv4 or IPv6), and MAC address..</p> <p>The following commands were introduced: subscriber per-session debug, show subscriber log, show subscriber per-session debug sessions-hit, clear subscriber log.</p>



CHAPTER 32

Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging

Intelligent Services Gateway (ISG) is a 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, on page 377](#)
- [Prerequisites for ISG Session Monitoring and Distributed Conditional Debugging, on page 377](#)
- [Restrictions for Distributed Conditional Debugging, on page 378](#)
- [Information About ISG Session Monitoring and Distributed Conditional Debugging, on page 378](#)
- [How to Enable ISG Session Monitoring and Distributed Conditional Debugging, on page 379](#)
- [Configuration Examples for ISG Distributed Conditional Debugging, on page 385](#)
- [Additional References, on page 386](#)
- [Feature Information for Distributed Conditional Debugging, on page 387](#)

Finding Feature Information

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

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

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

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 components that a session traverses. For this reason, the conditional debugging previously offered in the software has been enhanced to facilitate debug filtering for ISG and is available as distributed conditional debugging.

Cisco IOS XE Software Components Supported by Distributed Conditional Debugging

The following components are supported for ISG distributed conditional debugging:

- Authentication, authorization, and accounting (AAA) and RADIUS
- 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

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show interface <i>type number</i> monitor [interval seconds] Example: Router# show interface gigabitethernet 3/0/0 monitor interval 10	Displays interface statistics that are updated at specified intervals.
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

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 46: Supported Conditional Debug Commands

Command	Purpose
debug condition domain <i>domain-name</i>	Filters messages on the specified domain name.
debug condition interface {Fast Ethernet Gigabit Ethernet TenGigabit Ethernet} vlan-id <i>ID</i>	Filters messages on the specified VLAN identifier.
debug condition mac-address <i>hexadecimal-MAC-address</i>	Filters messages on the specified MAC address.
debug condition portbundle ip <i>IP-address</i> bundle <i>bundle-number</i>	Filters messages on the specified Port-Bundle Host Key (PBHK).
debug condition session-id <i>session-ID</i>	Filters messages on the specified session identifier. Note The session identifier can be obtained by entering the show subscriber session command.
debug condition username <i>email-address</i>	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 below table.

Table 47: Debug Commands Supported by ISG Distributed Conditional Debugging

AAA Debug Commands
debug aaa accounting
debug aaa authentication
debug aaa authorization
debug aaa id
PPP Debug Commands
debug ppp authentication
debug ppp bap error
debug ppp bap events
debug ppp bap negotiation

AAA Debug Commands
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
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

AAA Debug Commands
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
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

AAA Debug Commands
<code>debug vpdn call event</code>
<code>debug vpdn call fsm</code>
<code>debug vpdn error</code>
<code>debug vpdn event</code>
<code>debug vpdn event disconnect</code>

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	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>debug condition command</code></p> <p>Example:</p> <pre>Router# debug condition username user@cisco.com</pre>	<p>Enter one or more of the <code>debug condition</code> commands to enable distributed conditional debugging.</p>
Step 3	<p><code>debug command</code></p> <p>Example:</p>	<p>Enter one or more of the supported <code>debug</code> commands.</p>

	Command or Action	Purpose
	Router# debug subscriber aaa authorization fsm	

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. <ul style="list-style-type: none"> • 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

The following example shows sample output for the **show interface monitor** command. The display will be updated every 10 seconds.

```
Router> show interface gigabitethernet 0/0/0 monitor interval 10
Router Name: Scale3-Router8      Update Secs: 10
Interface Name: GigabitEthernet 0/0/0 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	<i>Cisco IOS Debug Command Reference</i>
Conditional debugging	"Conditionally Triggered Debugging" chapter in the <i>Cisco IOS Debug Command Reference</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

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 48: Feature Information for ISG Session Monitoring and Distributed Conditional Debugging

Feature Name	Releases	Feature Configuration Information
<p>ISG: Instrumentation: Session and Flow Monitoring</p>	<p>Cisco IOS XE Release 2.2</p>	<p>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.</p>
<p>ISG: Instrumentation: Advanced Conditional Debugging</p>	<p>Cisco IOS XE Release 2.2</p>	<p>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.</p>



CHAPTER 33

Configuring ISG Troubleshooting Enhancements

The Intelligent Services Gateway (ISG) debugging enhancements enable you to more easily isolate issues with ISG subscriber sessions in a production network, such as a session getting stuck in a dangling state (never reaches the established state). The troubleshooting enhancements described in this module allow you to diagnose these issues by introducing expanded statistics collection and event tracing.

- [Information About ISG Troubleshooting Enhancements, on page 389](#)
- [How to Enable ISG Troubleshooting Enhancements, on page 390](#)
- [Additional References, on page 392](#)
- [Feature Information for ISG Troubleshooting Enhancements, on page 393](#)

Information About ISG Troubleshooting Enhancements

Event Tracing for Subscriber Sessions

When trying to reproduce or capture customer issues, collecting debug output is not always practical or even possible. Network administrators often do not detect an error until long after the event that caused the error has occurred. By the time a fault is detected, it is usually too late to enable debug commands because the session is already in an error state, or the session was terminated because of an error.

Event tracing allows you to capture traces for existing sessions on the router and to retain the history of any past sessions that were marked as interesting, such as a session that became stuck in a dangling state. This enables you to look at existing sessions, as well as past sessions, and review the data after the session gets into an unexpected state or never comes up.

If a session is marked as interesting, its event trace information is sent to a history log, if history logging is enabled. A session is considered interesting if it becomes stuck in a state, enters an error state, or terminates without transitioning into a target state, because of a programming error, end-user action, packet drop, or other reason. The decision whether to log an event trace is determined by the after-the-fact status of the object. Event traces for uninteresting sessions are removed to free up space in the history log buffer.

Previously, the event trace data for each subscriber session was attached to its session context. This data was purged when the session was terminated. These enhancements preserve the event trace data even after the sessions are gone.

Each session context that supports event trace creates a new event trace log to hold the event traces for that session context. The event trace logs can be displayed independently through **show** commands.

Dumping Event Traces

ISG event traces are enabled to capture the trace logs by default. All the event trace logs are stored in the device memory. When the device reloads due to crash, the trace logs are lost and it becomes difficult to debug issues that causes the crash.

To prevent losing the trace logs, event trace logs are saved in a pre-configured file. ISG event traces are collected and saved in a file that is pre-configured in the device. If the filename is not configured, event traces cannot be collected. So, it is recommended to configure the filename to collect and save event trace logs during a crash.



Note To collect the event traces, ensure to configure the file location as bootflash. You cannot collect the event traces in a hard disk.

This example shows how to collect the event traces in a text file.

```
Device #
Device # configure terminal
Device(config)# monitor event-trace subscriber dump-file bootflash:isg_dump_file.txt
```

How to Enable ISG Troubleshooting Enhancements

Enabling Event Tracing for ISG Sessions

Perform the following steps to enable event tracing for ISG subscriber sessions.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `monitor event-trace subscriber dump-file`
4. `monitor event-trace subscriber enable`
5. `exit`
6. `no monitor event-trace subscriber`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	monitor event-trace subscriber <i>dump-file</i> Example: <pre>Router(config)# monitor event-trace subscriber dump-file</pre>	Sets the dump file name to be used to collect traces.
Step 4	monitor event-trace subscriber enable Example: <pre>Router(config)# monitor event-trace subscriber enable Router(config)# monitor event-trace subscriber ? feature Feature manager traces gx GX traces ip-sip IP-SIP traces policy Policy manager trace ppp PPP traces service Service manager trace session Subscriber Subsystem trace vpdn VPDN Traces</pre>	Enables event tracing for all the subscriber sessions. Note You can enable event tracing for ISG componets, IP-SIP, policy, PPP, service, session, VPDN, and feature.
Step 5	exit Example: <pre>Router(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	no monitor event-trace subscriber Example: <pre>Router(config)# no monitor event-trace subscriber</pre>	Disables traces for all components at all levels.

Displaying Event Traces for ISG Sessions

Use the following commands to display information about the event traces that are saved in text file.

SUMMARY STEPS

1. **show monitor event-trace subscriber**

DETAILED STEPS

show monitor event-trace subscriber

Use this command to display about the event traces that were saved in text file.

Example:

```

Router# show monitor event-trace subscriber
all-traces Show all the event traces
feature Feature manager trace
gx GX trace
identifier Filter traces based on identity of session
ip-sip IP-SIP trace
policy SSS Policy manager trace
ppp PPP trace
service Service manager trace
session SSS trace
vpdn VPDN trace

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Debug commands	Cisco IOS Debug Command Reference.
DHCP Configuration	Part 3, "DHCP," <i>IP Addressing Configuration Guide</i> .
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
ISG subscriber sessions	"Configuring ISG Access for IP Subscriber Sessions" module in this guide

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified.	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 by this feature, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Troubleshooting Enhancements

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 49: Feature Information for ISG Troubleshooting Enhancements

Feature Name	Releases	Feature Information
Dumping event-traces along with the crash	Cisco IOS XE Fuji 16.9.1	ISG event traces are enabled to track trace logs. The following command is introduced. monitor event-trace subscriber <i>dump-file</i> <i>bootflash:isg_dump_file.txt</i>

