Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T

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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

CONTENTS

CHAPTER 1

Configuring Authentication 1

Finding Feature Information 1

Prerequisites for Configuring Authentication 1

Restrictions for Configuring Authentication 2

Information About Configuring Authentication 2

Named Method Lists for Authentication 2

Method Lists and Server Groups 2

Method List Examples 3

AAA Authentication General Configuration Procedure 4

About RADIUS Change of Authorization 5

CoA Requests 5

RFC 5176 Compliance 5

CoA Request Response Code 7

Session Identification 7

CoA ACK Response Code 7

CoA NAK Response Code 7

CoA Request Commands 7

Session Reauthentication 8

Session Termination 8

CoA Request Disable Host Port 8

CoA Request Bounce Port 9

Domain Stripping 9

How to Configure AAA Authentication Methods 10

Configuring Login Authentication Using AAA 10

Preventing an Access-Request with an Expired Username from Being Sent to the RADIUS Server 13

Login Authentication Using Enable Password 14

Login Authentication Using Kerberos 14

- Login Authentication Using Line Password 15
- Login Authentication Using the Local Password 15
- Login Authentication Using Group LDAP 15
- Login Authentication Using Group RADIUS 15
- Configuring RADIUS Attribute 8 in Access Requests 16
- Login Authentication Using Group TACACS 16
- Login Authentication Using the group group-name method 16

Configuring PPP Authentication Using AAA 16

- PPP Authentication Using Kerberos 18
- PPP Authentication Using the Local Password 19
- PPP Authentication Using Group RADIUS 19
- Configuring RADIUS Attribute 44 in Access Requests 19
- PPP Authentication Using Group TACACS 19
- PPP Authentication Using group group-name 19

Configuring AAA Scalability for PPP Requests 20

Configuring ARAP Authentication Using AAA 21

- ARAP Authentication Allowing Authorized Guest Logins 22
- ARAP Authentication Allowing Guest Logins 23
- ARAP Authentication Using the Line Password 23
- ARAP Authentication Using the Local Password 23
- ARAP Authentication Using Group RADIUS 23
- ARAP Authentication Using Group TACACS 24
- ARAP Authentication Using Group group-name 24

Configuring NASI Authentication Using AAA 24

- NASI Authentication Using Enable Password 26
- NASI Authentication Using the Line Password 26
- NASI Authentication Using the Local Password 26
- NASI Authentication Using Group RADIUS 27
- NASI Authentication Using Group TACACS 27
- NASI Authentication Using group group-name 27

Specifying the Amount of Time for Login Input 28

Enabling Password Protection at the Privileged Level 28

Changing the Text Displayed at the Password Prompt 29

Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server 29

Configuring Message Banners for AAA Authentication 31

Configuring a Login Banner 31

Configuring a Failed-Login Banner 31

Configuring AAA Packet of Disconnect 32

Enabling Double Authentication 33

How Double Authentication Works 33

Configuring Double Authentication 34

Accessing the User Profile After Double Authentication 35

Enabling Automated Double Authentication 36

Configuring Automated Double Authentication 37

Troubleshooting Automated Double Authentication 38

Configuring the Dynamic Authorization Service for RADIUS CoA 39

Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests 40

Configuring Domain Stripping at the Server Group Level 42

Non-AAA Authentication Methods 43

Configuring Line Password Protection 43

Establishing Username Authentication 44

Enabling CHAP or PAP Authentication 46

Enabling PPP Encapsulation 47

Enabling PAP or CHAP 47

Inbound and Outbound Authentication 48

Enabling Outbound PAP Authentication 48

Refusing PAP Authentication Requests 49

Creating a Common CHAP Password 49

Refusing CHAP Authentication Requests 49

Delaying CHAP Authentication Until Peer Authenticates 50

Using MS-CHAP 50

Defining PPP Authentication using MS-CHAP 51

Authentication Examples 52

RADIUS Authentication Examples 52

TACACS Authentication Examples 53

Kerberos Authentication Examples 54

AAA Scalability Example 54

Example: Configuring Login and Failed-Login Banners for AAA Authentication 56

AAA Packet of Disconnect Server Key Example 56

Double Authentication Examples 56

Configuration of the Local Host for AAA with Double Authentication Examples 57

Configuration of the AAA Server for First-Stage PPP Authentication and Authorization Example 57

Configuration of the AAA Server for Second-Stage Per-User Authentication and Authorization Examples 58

Complete Configuration with TACACS Example 58

Automated Double Authentication Example 61

MS-CHAP Example 63

Additional References 64

Feature Information for Configuring Authentication 65

CHAPTER 2 RADIUS Change of Authorization 69

Finding Feature Information 69

Information About RADIUS Change of Authorization 69

About RADIUS Change of Authorization 69

CoA Requests 70

RFC 5176 Compliance 70

CoA Request Response Code 71

Session Identification 72

CoA ACK Response Code 72

CoA NAK Response Code 72

CoA Request Commands 72

Session Reauthentication 73

Session Termination 73

CoA Request Disable Host Port 73

CoA Request Bounce Port 74

How to Configure RADIUS Change of Authorization 74

Configuring RADIUS Change of Authorization 74

Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests 76

Configuring the Dynamic Authorization Service for RADIUS CoA 77

Monitoring and Troubleshooting RADIUS Change of Authorization 78

Configuration Examples for RADIUS Change of Authorization 79

Example: Configuring RADIUS Change of Authorization 79

Example: Configuring a Device to Ignore Bounce and Disable a RADIUS Requests 79

Example: Configuring the Dynamic Authorization Service for RADIUS CoA 80

Additional References for RADIUS Change of Authorization 80

Feature Information for RADIUS Change of Authorization 81

CHAPTER 3 **CWA URL Redirect support on C891FW** 83

Introduction 83

Prerequisites for CWA URL Redirect support on C891FW 84

Configuring CWA URL Redirect support on C891FW 85

HTTP Proxy Configuration 90

Configuration Examples for CWA URL Redirect support on C891FW 90

Important Notes 96

Additional References for CWA URL Redirect support on C891FW 96

Feature Information for CWA URL Redirect support on C891FW 97

CHAPTER 4 **Message Banners for AAA Authentication** 99

Finding Feature Information 99

Information About Message Banners for AAA Authentication 99

Login and Failed-Login Banners for AAA Authentication 99

How to Configure Message Banners for AAA Authentication 100

Configuring a Login Banner for AAA Authentication 100

Configuring a Failed-Login Banner for AAA Authentication 101

Configuration Examples for Message Banners for AAA Authentication 102

Example: Configuring Login and Failed-Login Banners for AAA Authentication 102

Additional References for Message Banners for AAA Authentication 103

Feature Information for Message Banners for AAA Authentication 104

CHAPTER 5 **AAA-Domain Stripping at Server Group Level** 105

Finding Feature Information 105

Information About AAA-Domain Stripping at Server Group Level 105

How to Configure AAA-Domain Stripping at Server Level Group 106

Configuring Domain Stripping at the Server Group Level 106

Configuration Example for AAA-Domain Stripping at Server Group Level 107

Example: AAA-Domain Stripping at Server Group Level 107

Additional References 107

Feature Information for AAA-Domain Stripping at Server Group Level 109

CHAPTER 6 AAA Double Authentication Secured by Absolute Timeout 111
Finding Feature Information 111
Prerequisites for AAA Double Authentication Secured by Absolute Timeout 112
Restrictions for AAA Double Authentication Secured by Absolute Timeout 112
Information About AAA Double Authentication Secured by Absolute Timeout 112
AAA Double Authentication 112
How to Apply AAA Double Authentication Secured by Absolute Timeout 113
Applying AAA Double Authentication Secured by Absolute Timeout 113
Verifying AAA Double Authentication Secured by Absolute Timeout 113
Configuration Examples for AAA Double Authentication Secured by Absolute Timeout 116
Example: RADIUS User Profile 116
Example: TACACS User Profile 116
Additional References 118
Related Documents 119
Standards 119
MIBs 119
RFCs 119
Technical Assistance 120
Feature Information for AAA Double Authentication Secured by Absolute Timeout 120

CHAPTER 7 Login Password Retry Lockout 121
Finding Feature Information 121
Prerequisites for Login Password Retry Lockout 121
Restrictions for Login Password Retry Lockout 122
Information About Login Password Retry Lockout 122
Lock Out of a Local AAA User Account 122
How to Configure Login Password Retry Lockout 122
Configuring Login Password Retry Lockout 122
Unlocking a Login Locked-Out User 124
Clearing the Unsuccessful Login Attempts of a User 124
Monitoring and Maintaining Login Password Retry Lockout Status 125
Configuration Examples for Login Password Retry Lockout 126
Displaying the Login Password Retry Lockout Configuration Example 126
Additional References 127

Feature Information for Login Password Retry Lockout 128
Glossary 129

CHAPTER 8 Throttling of AAA RADIUS Records 131
Finding Feature Information 131
Information About Throttling of AAA RADIUS Records 131
Benefits of the Throttling of AAA RADIUS Records Feature 131
Throttling Access Requests and Accounting Records 132
How to Configure Throttling of AAA RADIUS Records 132
Throttling Accounting and Access Request Packets Globally 133
Throttling Accounting and Access Request Packets Per Server Group 134
Configuration Examples for Throttling of AAA RADIUS Records 135
Throttling Accounting and Access Request Packets Globally Example 135
Throttling Accounting and Access Request Packets Per Server Group Example 135
Additional References 136
Feature Information for Throttling of AAA RADIUS Records 137

CHAPTER 9 MSCHAP Version 2 139
Finding Feature Information 139
Prerequisites for MSCHAP Version 2 140
Restrictions for MSCHAP Version 2 140
Information About MSCHAP Version 2 140
How to Configure MSCHAP Version 2 141
Configuring Password Aging for Crypto-Based Clients 141
Configuration Examples 142
Configuring Local Authentication Example 142
Configuring RADIUS Authentication Example 143
Configuring Password Aging with Crypto Authentication Example 143
Additional References 143
Feature Information for MSCHAP Version 2 145

CHAPTER 10 Define Interface Policy-Map AV Pairs AAA 147
Finding Feature Information 148
Prerequisites for Define Interface Policy-Map AV Pairs AAA 148
Restrictions for Define Interface Policy-Map AV Pairs AAA 148

Information About Define Interface Policy-Map AV Pairs AAA 148

Dynamically Applying and Modifying a Policy Map 148

New Cisco VSAs 150

Policy Map Troubleshooting Scenarios 150

How to Configure Define Interface Policy-Map AV Pairs AAA 151

Configuring AV Pairs Dynamic Authorization and the Policy Map on the RADIUS Server 151

Prerequisites 151

Configuring AV Pairs Dynamic Authorization and the Policy Map on the AAA Server 152

Configuring AV Pairs Dynamic Authorization and the Policy Map on the Router 154

Verifying Define Interface Policy-Map AV Pairs AAA 156

Configuration Examples for Define Interface Policy-Map AV Pairs AAA 158

Service-Policy Map Already Configured Example 158

Service-Policy Map Pulled Example 159

Service-Policy Map Pushed Example 159

Additional References 162

Feature Information for Define Interface Policy-Map AV Pairs AAA 164

CHAPTER 11 RADIUS Packet of Disconnect 167

Finding Feature Information 167

Prerequisites for RADIUS Packet of Disconnect 167

Restrictions for RADIUS Packet of Disconnect 168

Information About RADIUS Packet of Disconnect 168

When the POD is Needed 168

POD Parameters 168

How to Configure the RADIUS Packet of Disconnect 169

Configuring the RADIUS POD 169

Troubleshooting Tips 171

Additional References 172

Feature Information for RADIUS Packet of Disconnect 173

Glossary 174

CHAPTER 12 MAC Authentication Bypass 177

Finding Feature Information 177

Prerequisites for Configuring MAC Authentication Bypass 178

Information About Configuring MAC Authentication Bypass **178**

Overview of the Cisco IOS Auth Manager **178**

How to Configure MAC Authentication Bypass **179**

Enabling MAC Authentication Bypass **179**

Enabling Reauthentication on a Port **180**

Specifying the Security Violation Mode **182**

Configuration Examples for MAC Authentication Bypass **184**

Example: MAC Authentication Bypass Configuration **184**

Additional References **184**

Feature Information for MAC Authentication Bypass **185**

CHAPTER 13 **Standalone MAB Support** **187**

Finding Feature Information **187**

Information About Configuring Standalone MAB **188**

Standalone MAB **188**

How to Configure Standalone MAB Support **188**

Enabling Standalone MAB **188**

Troubleshooting Tips **190**

Configuration Examples for Standalone MAB Support **190**

Example: Standalone MAB Configuration **190**

Additional References **191**

Feature Information for Standalone MAB Support **192**

CHAPTER 14 **AAA Authorization and Authentication Cache** **193**

Finding Feature Information **193**

Prerequisites for Implementing Authorization and Authentication Profile Caching **194**

Information About Implementing Authorization and Authentication Profile Caching **194**

Network Performance Optimization Using Authorization and Authentication Profile Caching **194**

Authorization and Authentication Profile Caching as a Failover Mechanism **194**

Method Lists in Authorization and Authentication Profile Caching **195**

Authorization and Authentication Profile Caching Guidelines **195**

General Configuration Procedure for Implementing Authorization and Authentication Profile Caching **195**

How to Implement Authorization and Authentication Profile Caching **196**

Creating Cache Profile Groups and Defining Caching Rules 196
Defining RADIUS and TACACS Server Groups That Use Cache Profile Group Information 198
Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used 200
Configuration Examples for Implementing Authorization and Authentication Profile Caching 202
Implementing Authorization and Authentication Profile Caching for Network Optimization Example 202
Implementing Authorization and Authentication Profile Caching as a Failover Mechanism Example 202
Additional References 203
Feature Information for Implementing Authorization and Authentication Profile Caching 205

CHAPTER 15 Configuring Authorization 207
Finding Feature Information 207
Prerequisites 207
Information About Configuring Authorization 208
Named Method Lists for Authorization 208
AAA Authorization Methods 209
Authorization Methods 209
Method Lists and Server Groups 210
AAA Authorization Types 210
Authorization Types 211
Authorization Attribute-Value Pairs 211
How to Configure Authorization 211
Configuring AAA Authorization Using Named Method Lists 211
Disabling Authorization for Global Configuration Commands 213
Configuring Authorization for Reverse Telnet 214
Authorization Configuration Examples 215
Named Method List Configuration Example 215
TACACS Authorization Examples 216
RADIUS Authorization Example 217
LDAP Authorization Example 217
Reverse Telnet Authorization Examples 218

Additional References 219

Feature Information for Configuring Authorization 221

CHAPTER 16 Configuring Accounting 223

Finding Feature Information 223

Prerequisites for Configuring Accounting 223

Restrictions for Configuring Accounting 224

Information About Configuring Accounting 224

Named Method Lists for Accounting 224

Method Lists and Server Groups 225

AAA Accounting Methods 226

Accounting Record Types 226

Accounting Methods 226

AAA Accounting Types 228

Network Accounting 228

EXEC Accounting 230

Command Accounting 231

Connection Accounting 232

System Accounting 233

Resource Accounting 234

AAA Resource Failure Stop Accounting 234

AAA Resource Accounting for Start-Stop Records 236

VRRS Accounting 236

VRRS Accounting Plug-in 236

AAA Accounting Enhancements 237

AAA Broadcast Accounting 237

AAA Session MIB 237

Accounting Attribute-Value Pairs 239

How to Configure AAA Accounting 239

Configuring AAA Accounting Using Named Method Lists 239

Configuring RADIUS System Accounting 241

Suppressing Generation of Accounting Records for Null Username Sessions 243

Generating Interim Accounting Records 243

Generating Accounting Records for Failed Login or Session 243

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records 244

Configuring AAA Resource Failure Stop Accounting 245

Configuring AAA Resource Accounting for Start-Stop Records 245

Configuring AAA Broadcast Accounting 246

Configuring Per-DNIS AAA Broadcast Accounting 246

Configuring AAA Session MIB 246

Configuring VRRS Accounting 247

Establishing a Session with a Router if the AAA Server is Unreachable 249

Monitoring Accounting 249

Troubleshooting Accounting 249

Configuration Examples for AAA Accounting 250

Example Configuring Named Method List 250

Example Configuring AAA Resource Accounting 252

Example Configuring AAA Broadcast Accounting 252

Example Configuring Per-DNIS AAA Broadcast Accounting 253

Example AAA Session MIB 253

Example Configuring VRRS Accounting 253

Additional References 253

Feature Information for Configuring Accounting 255

CHAPTER 17 AAA Broadcast Accounting-Mandatory Response Support 257

Finding Feature Information 257

Prerequisites for AAA Broadcast Accounting-Mandatory Response Support 258

Restrictions for AAA Broadcast Accounting-Mandatory Response Support 258

Information About AAA Broadcast Accounting-Mandatory Response Support 258

AAA Broadcast Accounting 258

Simultaneous Broadcast and Wait Accounting 258

How AAA Broadcast Accounting is Supported for GGSN 259

Configuring Broadcast and Wait Accounting on the GGSN 259

Configuration Examples for AAA Broadcast Accounting-Mandatory Response Support 262

AAA Broadcast Accounting-Mandatory Response Support Example 262

Additional References 263

Feature Information for AAA Broadcast Accounting-Mandatory Response Support 264

CHAPTER 18 AAA Dead-Server Detection 267

Finding Feature Information 267

Prerequisites for AAA Dead-Server Detection 267
Restrictions for AAA Dead-Server Detection 268
Information About AAA Dead-Server Detection 268
Criteria for Marking a RADIUS Server As Dead 268
How to Configure AAA Dead-Server Detection 268
Configuring AAA Dead-Server Detection 268
Troubleshooting Tips 269
Verifying AAA Dead-Server Detection 270
Configuration Examples for AAA Dead-Server Detection 271
Configuring AAA Dead-Server Detection Example 271
debug aaa dead-criteria transactions Command Example 271
show aaa dead-criteria Command Example 271
Additional References 271
Feature Information for AAA Dead-Server Detection 273

CHAPTER 19 AAA-SERVER-MIB Set Operation 275
Finding Feature Information 275
Prerequisites for AAA-SERVER-MIB Set Operation 275
Restrictions for AAA-SERVER-MIB Set Operation 276
Information About AAA-SERVER-MIB Set Operation 276
CISCO-AAA-SERVER-MIB 276
CISCO-AAA-SERVER-MIB Set Operation 276
How to Configure AAA-SERVER-MIB Set Operation 276
Configuring AAA-SERVER-MIB Set Operations 276
Verifying SNMP Values 276
Configuration Examples for AAA-SERVER-MIB Set Operation 277
RADIUS Server Configuration and Server Statistics Example 277
Additional References 279
Feature Information for AAA-SERVER-MIB Set Operation 280

CHAPTER 20 Per VRF AAA 283
Finding Feature Information 283
Prerequisites for Per VRF AAA 284
Restrictions for Per VRF AAA 284
Information About Per VRF AAA 284

How Per VRF AAA Works 284

AAA Accounting Records 285

New Vendor-Specific Attributes 285

How to Configure Per VRF AAA 289

Configuring Per VRF AAA 289

Configuring AAA 289

Configuring Server Groups 290

Configuring Authentication Authorization and Accounting for Per VRF AAA 291

Configuring RADIUS-Specific Commands for Per VRF AAA 293

Configuring Interface-Specific Commands for Per VRF AAA 294

Configuring Per VRF AAA Using Local Customer Templates 295

Configuring AAA with Local Customer Templates 295

Configuring Server Groups with Local Customer Templates 295

Configuring Authentication Authorization and Accounting for Per VRF AAA with Local Customer Templates 295

Configuring Authorization for Per VRF AAA with Local Customer Templates 295

Configuring Local Customer Templates 296

Configuring Per VRF AAA Using Remote Customer Templates 298

Configuring AAA with Remote Customer Templates 298

Configuring Server Groups 298

Configuring Authentication for Per VRF AAA with Remote Customer Templates 298

Configuring Authorization for Per VRF AAA with Remote Customer Templates 299

Configuring the RADIUS Profile on the SP RADIUS Server 300

Verifying VRF Routing Configurations 300

Troubleshooting Per VRF AAA Configurations 302

Configuration Examples for Per VRF AAA 302

Per VRF Configuration Examples 302

Per VRF AAA Example 302

Per VRF AAA Using a Locally Defined Customer Template Example 303

Per VRF AAA Using a Remote RADIUS Customer Template Example 303

Customer Template Examples 304

Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example 304

Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example 305

AAA Accounting Stop Records Examples 305
AAA Accounting Stop Record and Successful Call Example 306
AAA Accounting Stop Record and Rejected Call Example 308
Additional References 310
Feature Information for Per VRF AAA 311
Glossary 314

CHAPTER 21 AAA Support for IPv6 315
Finding Feature Information 315
Information About AAA Support for IPv6 315
AAA over IPv6 315
AAA Support for IPv6 RADIUS Attributes 316
Prerequisites for Using AAA Attributes for IPv6 316
RADIUS Per-User Attributes for Virtual Access in IPv6 Environments 316
IPv6 Prefix Pools 318
How to Configure AAA Support for IPv6 318
Configuring the RADIUS Server over IPv6 318
Specifying the Source Address in RADIUS Server 320
Configuring RADIUS Server Group Options 321
Configuring the DHCPv6 Server to Obtain Prefixes from RADIUS Servers 322
Configuration Examples for AAA Support for IPv6 323
Example: Configuring RADIUS Server over IPv6 323
Example: RADIUS Configuration 323
Additional References 324
Feature Information for AAA Support for IPv6 324

CHAPTER 22 TACACS+ over IPv6 327
Finding Feature Information 327
Information About TACACS+ over IPv6 327
AAA over IPv6 328
TACACS+ Over an IPv6 Transport 328
How to Configure TACACS+ over IPv6 328
Configuring the TACACS+ Server over IPv6 328
Specifying the Source Address in TACACS+ Packets 330
Configuring TACACS+ Server Group Options 330

Configuration Examples for TACACS+ over IPv6 331

Example: Configuring TACACS+ Server over IPv6 331

Additional References 332

Feature Information for TACACS+ over IPv6 332

CHAPTER 23 Token Authentication 335

Finding Feature Information 335

Prerequisites for Token Authentication 335

Restrictions for Token Authentication 336

Information About Token Authentication 336

Token Authentication Overview 336

How to Configure Token Authentication 337

Configuring Token Authentication 337

Configuration Examples for Token Authentication 338

Example: Configuring Token Authentication Key 338

Additional References for Token Authentication 338

Feature Information for Token Authentication 339

CHAPTER 24 Secure Reversible Passwords for AAA 341

Finding Feature Information 341

Prerequisites for Secure Reversible Passwords for AAA 341

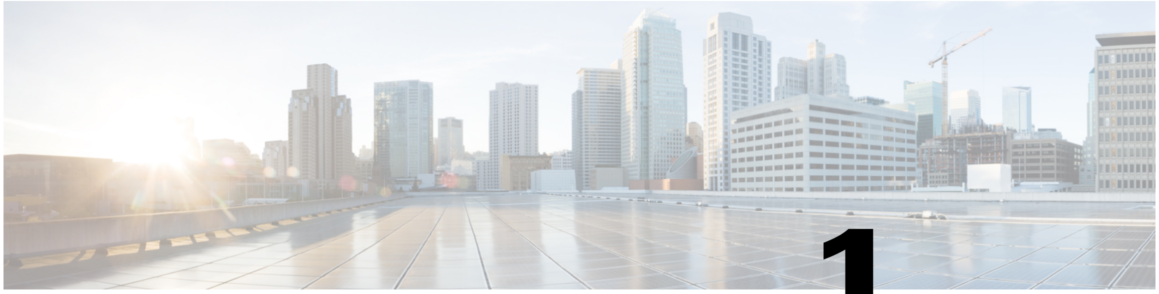
Information About Secure Reversible Passwords for AAA 342

Secure Reversible Passwords 342

Type 6 Encryption Configuration 342

Additional References for Secure Reversible Passwords for AAA 343

Feature Information for Secure Reversible Passwords for AAA 344



CHAPTER 1

Configuring Authentication

Authentication provides a method to identify users, which includes the login and password dialog, challenge and response, messaging support, and encryption, depending on the selected security protocol. Authentication is the way a user is identified prior to being allowed access to the network and network services.

- Finding Feature Information, page 1
- Prerequisites for Configuring Authentication, page 1
- Restrictions for Configuring Authentication, page 2
- Information About Configuring Authentication, page 2
- How to Configure AAA Authentication Methods, page 10
- Non-AAA Authentication Methods, page 43
- Authentication Examples, page 52
- Additional References, page 64
- Feature Information for Configuring Authentication, page 65

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 Authentication

The Cisco software implementation of authentication is divided into Authentication, Authorization, and Accounting (AAA) authentication and nonauthentication methods. Cisco recommends that, whenever possible, AAA security services be used to implement authentication.

Restrictions for Configuring Authentication

- The number of AAA method lists that can be configured is 250.
- If you configure one RADIUS server with the nonstandard option and another RADIUS server without the nonstandard option, the RADIUS-server host with the nonstandard option does not accept a predefined host. If you configure the same RADIUS server host IP address for a different UDP destination port for accounting requests by using the **acct-port** keyword and a UDP destination port for authentication requests by using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option.

Information About Configuring Authentication

The following sections describe how AAA authentication is configured by defining a named list of authentication methods and then applying that list to various interfaces. This section also describes how AAA authentication is handled by using RADIUS Change in Authorization (CoA):

Named Method Lists for Authentication

A named list of authentication methods is first defined before AAA authentication can be configured, and the named list is then applied to various interfaces. The method list defines the types of authentication and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces, except those that have a named method list explicitly defined. A defined method list overrides the default method list.

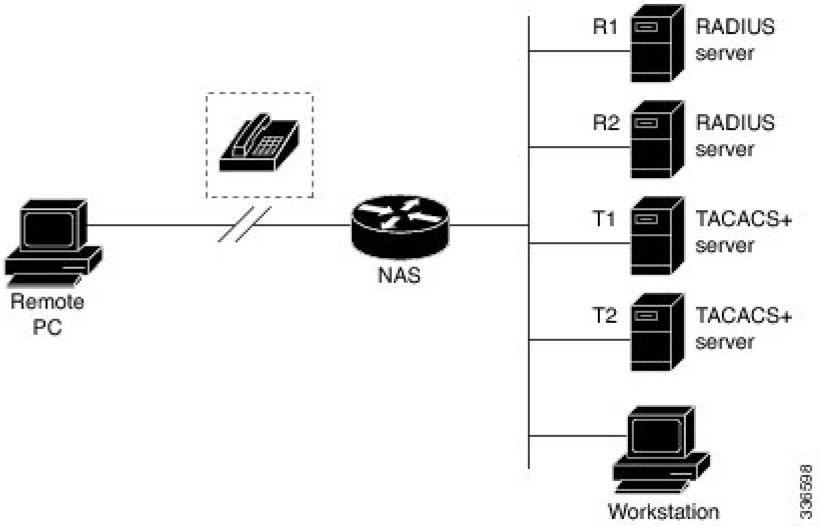
A method list is a sequential list describing the authentication methods to be queried to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco software uses the first listed method to authenticate users. If that method fails to respond, the Cisco software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted.

Note that the Cisco software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle, that is, the security server or local username database responds by denying the user access, then the authentication process stops and no other authentication methods are attempted.

Method Lists and Server Groups

A server group is a way to group existing Lightweight Directory Access Protocol (LDAP), RADIUS, or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Figure 1: Typical AAA Network Configuration



Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as one server group and T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for PPP authentication.

Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order in which they are configured.)

See the “Configuring LDAP,” “Configuring RADIUS,” or “Configuring TACACS+” feature modules for more information about configuring server groups and configuring server groups based on Dialed Number Identification Service (DNIS) numbers.

Method List Examples

Suppose the system administrator has decided on a security solution, where all interfaces will use the same authentication methods to authenticate PPP connections. In the RADIUS group, R1 is contacted first for authentication information; if there is no response, R2 is contacted. If R2 does not respond, T1 in the TACACS+ group is contacted; if T1 does not respond, T2 is contacted. If all designated servers fail to respond, authentication falls to the local username database on the access server. To implement this solution, the system administrator can create a default method list by entering the following command:

```
aaa authentication ppp default group radius group tacacs+ local
```

In the above example, “default” is the name of the method list. The protocols included in this method list are listed after the name in the order in which they are queried. The default list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected or until the session is terminated.

Note that a FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

If the system administrator wants to apply a method list only to a particular interface or set of interfaces, the system administrator creates a named method list and then applies this named list to the applicable interfaces. The following example shows how the system administrator can implement an authentication method that will be applied only to interface 3:

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
 interface async 3
 ppp authentication chap list1
```

In the above example, “list1” is the name of the method list, and the protocols included in this method list are listed after the name in the order in which they are to be performed. After the method list has been created, it is applied to the appropriate interface. Note that the method list name (list1) in both the **aaa authentication** and the **ppp authentication** commands must match.

In the following example, the system administrator uses server groups to specify that only R2 and T2 are valid servers for PPP authentication. To do this, the administrator must define specific server groups with R2 (192.0.2.3) and T2 (192.0.2.17) as members. In the below example, the RADIUS server group “rad2only” is defined as follows using the **aaa group server** command:

```
aaa group server radius rad2only
 server 192.0.2.3
```

The TACACS+ server group “tac2only” is defined as follows by using the **aaa group server** command:

```
aaa group server tacacs+ tac2only
 server 192.0.2.17
```

The administrator then applies PPP authentication using the server groups. In the below example, the default methods list for PPP authentication follows the order: **group rad2only**, **group tac2only**, and **local**:

```
aaa authentication ppp default group rad2only group tac2only local
```

AAA Authentication General Configuration Procedure

To configure AAA authentication, perform the following tasks:

1. Enable AAA by using the **aaa new-model** command in global configuration mode.
2. Configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos if you are using a security server. See “Configuring RADIUS,” “Configuring TACACS+,” and “Configuring Kerberos,” respectively for more information.

3 Define the method lists for authentication by using an AAA authentication command.

4 Apply the method lists to a particular interface or line, if required.

About RADIUS Change of Authorization

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network and the response is sent from the queried servers. The Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, in which the request originates from the external server to the device attached to the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

Use the following per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Security and Password
- Accounting

CoA Requests

CoA requests, as described in RFC 5176, are used in a pushed model to allow for session identification, host reauthentication, and session termination. The model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the device that acts as a listener.

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the device for a session termination.

The following table shows the IETF attributes that are supported for the RADIUS Change of Authorization (CoA) feature.

Table 1: Supported IETF Attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID

Attribute Number	Attribute Name
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

The following table shows the possible values for the Error-Cause attribute.

Table 2: Error-Cause Values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

CoA Request Response Code

The CoA Request Response code can be used to issue a command to the device. The supported commands are listed in the “CoA Request Commands” section.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format.

The Attributes field is used to carry Cisco VSAs.

Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco vendor-specific attribute (VSA))
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)

Unless all session identification attributes included in the CoA message match the session, the device returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

Note A CoA NAK message is not sent for all CoA requests with a key mismatch. The message is sent only for the first three requests for a client. After that, all the packets from that client are dropped. When there is a key mismatch, the response authenticator sent with the CoA NAK message is calculated from a dummy key value.

CoA ACK Response Code

If an authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within a CoA ACK can vary based on the CoA Request.

CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure.

CoA Request Commands

The commands supported on the device are shown in the table below. All CoA commands must include the session identifier between the device and the CoA client.

Table 3: CoA Request Commands Supported on the Device

Command	Cisco VSA
Bounce host port	Cisco:Avpair=“subscriber:command=bounce-host-port”

Command	Cisco VSA
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	This is a standard disconnect request that does not require a VSA

Session Reauthentication

To initiate session reauthentication, the authentication, authorization, and accounting (AAA) server sends a standard CoA-Request message that contains a Cisco VSA and one or more session identification attributes. The Cisco VSA is in the form of Cisco:Avpair="subscriber:command=reauthenticate".

The current session state determines the device's response to the message in the following scenarios:

- If the session is currently authenticated by IEEE 802.1*x*, the device responds by sending an Extensible Authentication Protocol over LAN (EAPoL)-RequestId message to the server.
- If the session is currently authenticated by MAC authentication bypass (MAB), the device sends an access request to the server, passing the same identity attributes used for the initial successful authentication.
- If session authentication is in progress when the device receives the command, the device terminates the process and restarts the authentication sequence, starting with the method configured to be attempted first.

Session Termination

A CoA Disconnect-Request terminates the session without disabling the host port. CoA Disconnect-Request termination causes reinitialization of the authenticator state machine for the specified host, but does not restrict the host's access to the network. If the session cannot be located, the device returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK message.

To restrict a host's access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism.

CoA Request Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has the following VSA:

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section. If the device cannot locate the session, it returns a

CoA-NAK message with the “Session Context Not Found” error-code attribute. If the device locates the session, it disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

To ignore the RADIUS server CoA disable port command, see the “Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests” section.

CoA Request Bounce Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair=“subscriber:command=bounce-host-port”

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the Session Identification. If the session cannot be located, the device returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the device disables the hosting port for a period of 10 seconds, reenables it (port-bounce), and returns a CoA-ACK.

To ignore the RADIUS server CoA bounce port, see the “Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests” section.

Domain Stripping

You can remove the domain name from the username received at the global level by using the **radius-server domain-stripping** command. When the **radius-server domain-stripping** command is configured, all the AAA requests with “user@example.com” go to the remote RADIUS server with the reformatted username “user.” The domain name is removed from the request.

Note Domain stripping will not be done in a TACACS configuration.

The AAA Broadcast Accounting feature allows accounting information to be sent to multiple AAA servers at the same time, that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows you to send accounting information to private and public AAA servers. It also provides redundant billing information for voice applications.

The Domain Stripping feature allows domain stripping to be configured at the server group level.

Per-server group configuration overrides the global configuration. If domain stripping is not enabled globally, but it is enabled in a server group, then it is enabled only for that server group. Also, if virtual routing and forwarding (VRF)-specific domain stripping is configured globally and in a server group for a different VRF, domain stripping is enabled in both the VRFs. VRF configurations are taken from server-group configuration mode. If server-group configurations are disabled in global configuration mode but are available in server-group configuration mode, all configurations in server-group configuration mode are applicable.

After the domain stripping and broadcast accounting are configured, you can create separate accounting records as per the configurations.

How to Configure AAA Authentication Methods

Note AAA features are not available for use until you enable AAA globally using the **aaa new-model** command.

Configuring Login Authentication Using AAA

AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication regardless of the supported login authentication methods you decide to use. With the **aaa authentication login** command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication line** command.

To configure login authentication by using AAA, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. Device(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]
4. Device(config-line)# **login authentication**
5. Device(config-line)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa new-model**	Enables AAA globally.
Step 2	Device(config)# **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Creates a local authentication list.
Step 3	Device(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]	Enters line configuration mode for the lines to which you want to apply the authentication list.
Step 4	Device(config-line)# **login authentication** **Example:**	Applies the authentication list to a line or set of lines.
Step 5	Device(config-line)# **end** **Example:**	Returns to privileged EXEC mode.

What to Do Next

The *list-name* is a character string used to name the list you are creating. The *method* argument refers to the actual method the authentication algorithm tries. Additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, enter **none** as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the LDAP server returns an error, enter the following command:

```
aaa authentication login default group ldap none
```

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

```
aaa authentication login default group tacacs+ none
```

Note Because the **none** keyword enables *any* user logging in to be successfully authenticated, use it only as a backup method of authentication.

To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa authentication login default group radius
```

The table below lists the supported login authentication methods.

Table 4: AAA Authentication Login Methods

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the device. If selected, this keyword must be listed as the first method in the method list.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group ldap	Uses the list of all LDAP servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Note The **login** command changes only the username and the privilege level but does not execute a shell; therefore, autocommands will not be executed. To execute autocommands, you must establish a Telnet session back into the device (loop-back). Ensure that the device has been configured for secure Telnet sessions if you choose to implement autocommands in this method.

Preventing an Access-Request with an Expired Username from Being Sent to the RADIUS Server

The following task is used to prevent an access-request with an expired username from being sent to the RADIUS server. The Easy VPN client is notified by the RADIUS server that its password has expired. The password-expiry feature also provides a generic way for the user to change the password.

Note The **radius-server vsa send authentication** command must be configured to make the password-expiry feature work.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*]
5. **radius-server vsa send authentication**
6. **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)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*] **Example:** `Device(config)# aaa authentication login userauthen passwd-expiry group radius`	Sets AAA authentication at login. The **default** keyword uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in. • The *list-name* argument is a character string used to name the list of authentication methods activated when a user logs in.

	Command or Action	Purpose
		• The **password-expiry** keyword enables password aging on a local authentication list. • The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. • The example configures password aging by using AAA with a crypto client.
Step 5	**radius-server vsa send authentication** **Example:** `Device(config)# radius-server vsa send authentication`	Sends vendor-specific attributes in access requests.

Step 6	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Login Authentication Using Enable Password

Use the **aaa authentication login** command with the **enable** keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default enable
```

Before you can use the enable password as the login authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the chapter “Configuring Passwords and Privileges.”

Login Authentication Using Kerberos

Authentication using Kerberos is different from most other authentication methods: the user’s password is never sent to the remote access server. Remote users logging in to the network are prompted for a username. If the key distribution center (KDC) has an entry for that user, it creates an encrypted ticket granting ticket (TGT) with the password for that user and sends it back to the device. The user is then prompted for a password, and the device attempts to decrypt the TGT with that password. If it succeeds, the user is authenticated and the TGT is stored in the user’s credential cache on the device.

Although **krb5** uses the KINIT program, a user need not run the KINIT program to get a TGT to authenticate to the device. This is because KINIT has been integrated into the login procedure in the Cisco implementation of Kerberos.

Use the **aaa authentication login** command with the **krb5** keyword to specify Kerberos as the login authentication method. For example, to specify Kerberos as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default krb5
```

Before you can use Kerberos as the login authentication method, you must enable communication with the Kerberos security server. See the chapter “Configuring Kerberos” for more information about establishing communication with a Kerberos server.

Login Authentication Using Line Password

Use the **aaa authentication login** command with the **line** keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you must define a line password. For more information about defining line passwords, see the section “Configuring Line Password Protection.”

Login Authentication Using the Local Password

Use the **aaa authentication login** command with the **local** keyword to specify that the Cisco device or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default local
```

For information about adding users into the local username database, see the chapter “Establishing Username Authentication.”

Login Authentication Using Group LDAP

Use the **aaa authentication login** command with the **group ldap** method to specify ldap as the login authentication method. For example, to specify ldap as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default group ldap
```

Login Authentication Using Group RADIUS

Use the **aaa authentication login** command with the **group radius** method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default group radius
```

Before you can use RADIUS as the login authentication method, you must enable communication with the RADIUS security server. See the chapter “Configuring RADIUS” for more information about establishing communication with a RADIUS server.

Configuring RADIUS Attribute 8 in Access Requests

After you have used the **aaa authentication login** command to specify RADIUS and your login host has been configured to request its IP address from the NAS, you can send attribute 8 (Framed-IP-Address) in access-request packets by using the **radius-server attribute 8 include-in-access-req** command in global configuration mode. This command makes it possible for NAS to provide the RADIUS server a hint of the user IP address in advance for user authentication. For more information about attribute 8, refer to the appendix “RADIUS Attributes” at the end of the book.

Login Authentication Using Group TACACS

Use the **aaa authentication login** command with the **group tacacs+** method to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default group tacacs+
```

Before you can use TACACS+ as the login authentication method, you must enable communication with the TACACS+ security server. See the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

Login Authentication Using the group group-name method

Use the **aaa authentication login** command with the **group** *group-name* method to specify a subset of LDAP, RADIUS, or TACACS+ servers to be used as the login authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group** *loginrad*:

```
aaa group server radius loginrad
 server 192.0.2.3
 server 192.0.2 17
 server 192.0.2.32
```

This command specifies RADIUS servers 192.0.2.3, 192.0.2.17, and 192.0.2.32 as members of the group *loginrad*.

To specify **group** *loginrad* as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication login default group loginrad
```

Before you can use a group name as the login authentication method, you must enable communication with the RADIUS or TACACS+ security server. See the chapter “Configuring RADIUS” for more information about establishing communication with a RADIUS server. See the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

Configuring PPP Authentication Using AAA

Many users access network access servers through dialup that uses async or ISDN. Dialup that uses async or ISDN bypasses the CLI completely; instead, a network protocol (such as PPP or AppleTalk Remote Access (ARA)) starts as soon as the connection is established.

The AAA security services facilitate a variety of authentication methods for use on serial interfaces running PPP. Use the **aaa authentication ppp** command to enable AAA authentication regardless of which of the supported PPP authentication methods you decide to use.

To configure AAA authentication methods for serial lines using PPP, use the following commands in global configuration mode:

SUMMARY STEPS

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
3. Device(config)# **interface** *interface-type interface-number*
4. Device(config-if)# **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**] [**optional**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa new-model**	Enables AAA globally.
Step 2	Device(config)# **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]	Creates a local authentication list.
Step 3	Device(config)# **interface** *interface-type interface-number*	Enters interface configuration mode for the interface to which you want to apply the authentication list.
Step 4	Device(config-if)# **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**] [**optional**]	Applies the authentication list to a line or set of lines. In this command, *protocol1* and *protocol2* represent the following protocols: Challenge Handshake Authentication Protocol (CHAP), Microsoft-CHAP (MS-CHAP), and Password Authentication Protocol (PAP). PPP authentication is attempted first using the first authentication method, specified by *protocol1*. If *protocol1* is unable to establish authentication, the next configured protocol is used to negotiate authentication.

What to Do Next

With the **aaa authentication ppp** command, you can create one or more lists of authentication methods that are tried when a user tries to authenticate by using PPP. These lists are applied by using the **ppp authentication** line configuration command.

To create a default list that is used when a named list is *not* specified in the **ppp authentication** command, use the **default** keyword followed by the methods you want used in default situations.

For example, to specify the local username database as the default method for user authentication, use the following command:

```
aaa authentication ppp default local
```

The *list-name* is any character string used to name the list you are creating. The *method* argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, use the following command:

```
aaa authentication ppp default group tacacs+ none
```

Note Because **none** allows all users logging in to authenticate successfully, it should be used as a backup method of authentication.

The table below lists the supported login authentication methods.

Table 5: AAA Authentication PPP Methods

Keyword	Description
if-needed	Does not authenticate if the user has already been authenticated on a TTY line.
krb5	Uses Kerberos 5 for authentication (can be used only for PAP authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

PPP Authentication Using Kerberos

Use the **aaa authentication ppp** command with the **krb5** *method* keyword to specify Kerberos as the authentication method for use on interfaces running PPP. For example, to specify Kerberos as the method of user authentication when no other method list has been defined, use the following command:

```
aaa authentication ppp default krb5
```

Before you can use Kerberos as the PPP authentication method, you must enable communication with the Kerberos security server. See the chapter “Configuring Kerberos” for more information about establishing communication with a Kerberos server.

Note Kerberos login authentication works only with PPP PAP authentication.

PPP Authentication Using the Local Password

Use the **aaa authentication ppp** command with the *method* keyword **local** to specify that the Cisco device or access server will use the local username database for authentication. For example, to specify the local username database as the method of authentication for use on lines running PPP when no other method list has been defined, use the following command:

```
aaa authentication ppp default local
```

For information about adding users into the local username database, see the section “Establishing Username Authentication.”

PPP Authentication Using Group RADIUS

Use the **aaa authentication ppp** command with the **group radius** *method* to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication ppp default group radius
```

Before you can use RADIUS as the PPP authentication method, you must enable communication with the RADIUS security server. See the chapter “Configuring RADIUS” for more information about establishing communication with a RADIUS server.

Configuring RADIUS Attribute 44 in Access Requests

After you have used the **aaa authentication ppp** command with the **group radius** *method* to specify RADIUS as the login authentication method, you can configure your device to send attribute 44 (Acct-Session-ID) in access-request packets by using the **radius-server attribute 44 include-in-access-req** command in global configuration mode. This command allows the RADIUS daemon to track a call from the beginning to the end.

PPP Authentication Using Group TACACS

Use the **aaa authentication ppp** command with the **group tacacs+** *method* to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication ppp default group tacacs+
```

Before you can use TACACS+ as the PPP authentication method, you must enable communication with the TACACS+ security server. See the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

PPP Authentication Using group group-name

Use the **aaa authentication ppp** command with the **group** *group-name* method to specify a subset of RADIUS or TACACS+ servers to be used as the login authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group ppprad**:

```
aaa group server radius ppprad
 server 192.0.2.3
 server 192.0.2 17
 server 192.0.2.32
```

This command specifies RADIUS servers 192.0.2.3, 192.0.2.17, and 192.0.2.32 as members of the group *ppprad*.

To specify **group ppprad** as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication ppp default group ppprad
```

Before you can use a group name as the PPP authentication method, you must enable communication with the RADIUS or TACACS+ security server. See the chapter "Configuring RADIUS" for more information about establishing communication with a RADIUS server, and the chapter "Configuring TACACS+" for more information about establishing communication with a TACACS+ server.

Configuring AAA Scalability for PPP Requests

You can configure and monitor the number of background processes allocated by the PPP manager in the NAS to deal with AAA authentication and authorization requests. Depending on the Cisco release, only one background process was allocated to handle all AAA requests for PPP. This meant that parallelism in AAA servers could not be fully exploited. The AAA Scalability feature enables you to configure the number of processes used to handle AAA requests for PPP, thus increasing the number of users that can be simultaneously authenticated or authorized.

To allocate a specific number of background processes to handle AAA requests for PPP, use the following command in global configuration mode:

Command or Action	Purpose
`Device(config)#` **aaa processes** *number*	Allocates a specific number of background processes to handle AAA authentication and authorization requests for PPP.

The *number* argument defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP and can be configured for any value from 1 to 2147483647. Because of the way the PPP manager handles requests for PPP, this argument also defines the number of new users that can be simultaneously authenticated. This argument can be increased or decreased at any time.

Note Allocating additional background processes can be expensive. You should configure the minimum number of background processes capable of handling the AAA requests for PPP.

Configuring ARAP Authentication Using AAA

Using the **aaa authentication arap** command, you can create one or more lists of authentication methods that are tried when AppleTalk Remote Access Protocol (ARAP) users attempt to log in to the device. These lists are used with the **arap authentication** line configuration command.

Use the following commands starting in global configuration mode:

SUMMARY STEPS

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication arap**
3. Device(config)# **line** *number*
4. Device(config-line)# **autoselect arap**
5. Device(config-line)# **autoselect during-login**
6. Device(config-line)# **arap authentication** *list-name*
7. Device(config-line)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa new-model**	Enables AAA globally.
Step 2	Device(config)# **aaa authentication arap** **Example:** Enables authentication for ARAP users.	
Step 3	Device(config)# **line** *number*	(Optional) Changes to line configuration mode.
Step 4	Device(config-line)# **autoselect arap**	(Optional) Enables autoselection of ARAP.
Step 5	Device(config-line)# **autoselect during-login**	(Optional) Starts the ARAP session automatically at user login.
Step 6	Device(config-line)# **arap authentication** *list-name*	(Optional—not needed if **default** is used in the **aaa authentication arap** command) Enables TACACS+ authentication for ARAP on a line.
Step 7	Device(config-line)# **end**	Returns to the privileged EXEC mode.

What to Do Next

The *list-name* is any character string used to name the list you are creating. The *method* argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

To create a default list that is used when a named list is *not* specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

Note Because **none** allows all users logging in to be authenticated, it should be used as a backup method of authentication.

The following table lists the supported login authentication methods.

Table 6: AAA Authentication ARAP Methods

Keyword	Description
auth-guest	Allows guest logins only if the user has already logged in to EXEC mode.
guest	Allows guest logins.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

For example, to create a default AAA authentication method list used with ARAP, use the following command:

```
aaa authentication arap default if-needed none
```

To create the same authentication method list for ARAP and name the list *MIS-access,* use the following command:

```
aaa authentication arap MIS-access if-needed none
```

This section includes the following sections:

ARAP Authentication Allowing Authorized Guest Logins

Use the **aaa authentication arap** command with the **auth-guest** keyword to allow guest logins only if the user has already successfully logged in to the EXEC mode. This method must be the first listed in the ARAP authentication method list, but it can be followed by other methods. For example, to allow all authorized guest logins—logins by users who have already successfully logged in to the EXEC mode—as the default method of authentication, using RADIUS only if that method fails, use the following command:

```
aaa authentication arap default auth-guest group radius
```

Note By default, guest logins through ARAP are disabled when you initialize AAA. To allow guest logins, you must use the **aaa authentication arap** command with either the **guest** or the **auth-guest** keyword.

ARAP Authentication Allowing Guest Logins

Use the **aaa authentication arap** command with the **guest** keyword to allow guest logins. This method must be the first listed in the ARAP authentication method list, but it can be followed by other methods if it does not succeed. For example, to allow all guest logins as the default method of authentication, using RADIUS only if that method fails, use the following command:

```
aaa authentication arap default guest group radius
```

ARAP Authentication Using the Line Password

Use the **aaa authentication arap** command with the keyword **line** to specify the line password as the authentication method. For example, to specify the line password as the method of ARAP user authentication when no other method list has been defined, use the following command:

```
aaa authentication arap default line
```

Before you can use a line password as the ARAP authentication method, you must define a line password. For more information about defining line passwords, refer to the section “Configuring Line Password Protection.”

ARAP Authentication Using the Local Password

Use the **aaa authentication arap** command with the keyword **local** to specify that the Cisco device or access server will use the local username database for authentication. For example, to specify the local username database as the method of ARAP user authentication when no other method list has been defined, use the following command:

```
aaa authentication arap default local
```

For information about adding users to the local username database, refer to the section “Establishing Username Authentication.”

ARAP Authentication Using Group RADIUS

Use the **aaa authentication arap** command with the **group radius** *method* to specify RADIUS as the ARAP authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication arap default group radius
```

Before you can use RADIUS as the ARAP authentication method, you must enable communication with the RADIUS security server.

ARAP Authentication Using Group TACACS

Use the **aaa authentication arap** command with the **group tacacs+** method to specify TACACS+ as the ARAP authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication arap default group tacacs+
```

Before you can use TACACS+ as the ARAP authentication method, you must enable communication with the TACACS+ security server. See the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

ARAP Authentication Using Group group-name

Use the **aaa authentication arap** command with the **group** *group-name* method to specify a subset of RADIUS or TACACS+ servers to use as the ARAP authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group araprad**:

```
aaa group server radius araprad
 server 192.0.2.3
 server 192.0.2.17
 server 192.0.2.32
```

This command specifies RADIUS servers 192.0.2.3, 192.0.2.17, and 192.0.2.32 as members of the group *araprad*.

To specify **group araprad** as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication arap default group araprad
```

Before you can use a group name as the ARAP authentication method, you must enable communication with the RADIUS or TACACS+ security server. See the chapter “Configuring RADIUS” for more information about establishing communication with a RADIUS server, and the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

Configuring NASI Authentication Using AAA

Using the **aaa authentication nasi** command, you can create one or more lists of authentication methods that are tried when NetWare Asynchronous Services Interface (NASI) users attempt to log in to the device. These lists are used with the **nasi authentication line** configuration command.

To configure NASI authentication using AAA, use the following commands starting in global configuration mode:

SUMMARY STEPS

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication nasi**
3. Device(config)# **line** *number*
4. Device(config-line)# **nasi authentication** *list-name*
5. Device(config-line)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa new-model**	Enables AAA globally.
Step 2	Device(config)# **aaa authentication nasi** **Example:**	Enables authentication for NASI users.
Step 3	Device(config)# **line** *number*	(Optional--not needed if **default** is used in the **aaa authentication nasi** command) Enters line configuration mode.
Step 4	Device(config-line)# **nasi authentication** *list-name*	(Optional--not needed if **default** is used in the **aaa authentication nasi** command) Enables authentication for NASI on a line.
Step 5	Device(config-line)# **end**	Returns to the privileged EXEC mode.

What to Do Next

The *list-name* is any character string used to name the list you are creating. The *method* argument refers to the actual list of methods that the authentication algorithm tries, in the sequence entered.

To create a default list that is used when a named list is *not* specified in the **aaa authentication nasi** command, use the **default** keyword followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

Note Because **none** allows all users logging in to be authenticated, it should be used as a backup method of authentication.

The table below lists the supported NASI authentication methods.

Table 7: AAA Authentication NASI Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

NASI Authentication Using Enable Password

Use the **aaa authentication nasi** command with the keyword **enable** to specify the enable password as the authentication method. For example, to specify the enable password as the method of NASI user authentication when no other method list has been defined, use the following command:

```
aaa authentication nasi default enable
```

Before you can use the enable password as the authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the chapter “Configuring Passwords and Privileges.”

NASI Authentication Using the Line Password

Use the **aaa authentication nasi** command with the keyword **line** to specify the line password as the authentication method. For example, to specify the line password as the method of NASI user authentication when no other method list has been defined, use the following command:

```
aaa authentication nasi default line
```

Before you can use a line password as the NASI authentication method, you must define a line password. For more information about defining line passwords, refer to the section “Configuring Line Password Protection.”

NASI Authentication Using the Local Password

Use the **aaa authentication nasi** command with the keyword **local** to specify that the Cisco device or access server will use the local username database for authentication information. For example, to specify the local username database as the method of NASI user authentication when no other method list has been defined, use the following command:

```
aaa authentication nasi default local
```

For information about adding users to the local username database, refer to the chapter “Establishing Username Authentication.”

NASI Authentication Using Group RADIUS

Use the **aaa authentication nasi** command with the **group radius** method to specify RADIUS as the NASI authentication method. For example, to specify RADIUS as the method of NASI user authentication when no other method list has been defined, use the following command:

```
aaa authentication nasi default group radius
```

Before you can use RADIUS as the NASI authentication method, you must enable communication with the RADIUS security server. See the chapter “Configuring RADIUS” for more information about establishing communication with a RADIUS server.

NASI Authentication Using Group TACACS

Use the **aaa authentication nasi** command with the **group tacacs+** keyword to specify TACACS+ as the NASI authentication method. For example, to specify TACACS+ as the method of NASI user authentication when no other method list has been defined, use the following command:

```
aaa authentication nasi default group tacacs+
```

Before you can use TACACS+ as the authentication method, you must enable communication with the TACACS+ security server. See the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

NASI Authentication Using group group-name

Use the **aaa authentication nasi** command with the **group** *group-name* method to specify a subset of RADIUS or TACACS+ servers to be used as the NASI authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group** *nasirad*:

```
aaa group server radius nasirad
 server 192.0.2.3
 server 192.0.2 17
 server 192.0.2.32
```

This command specifies RADIUS servers 192.0.2.3, 192.0.2.17, and 192.0.2.32 as members of the group *nasirad*.

To specify group nasirad as the method of user authentication at login when no other method list has been defined, use the following command:

```
aaa authentication nasi default group nasirad
```

Before you can use a group name as the NASI authentication method, you must enable communication with the RADIUS or TACACS+ security server. See the chapter “Configuring RADIUS” for more information about establishing communication with a RADIUS server and the chapter “Configuring TACACS+” for more information about establishing communication with a TACACS+ server.

Specifying the Amount of Time for Login Input

The **timeout login response** command allows you to specify how long the system will wait for login input (such as username and password) before timing out. The default login value is 30 seconds; with the **timeout login response** command, you can specify a timeout value from 1 to 300 seconds. To change the login timeout value from the default of 30 seconds, use the following command in line configuration mode:

Command or Action	Purpose
`Device(config-line)#` **timeout login response** *seconds*	Specifies how long the system will wait for login information before timing out.

Enabling Password Protection at the Privileged Level

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

Use the following command in global configuration mode:

Command or Action	Purpose
`Device(config)#` **aaa authentication enable default** *method1* `[`*method2...*`]`	Enables user ID and password checking for users requesting privileged EXEC level. **Note** All **aaa authentication enable default** requests sent by the device to a RADIUS server include the username "$enab15$." Requests sent to a TACACS+ server will include the username that is entered for login authentication.

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered. The table below lists the supported enable authentication methods.

Table 8: AAA Authentication Enable Default Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

Keyword	Description
group radius	Uses the list of all RADIUS hosts for authentication. **Note** The RADIUS method does not work on a per-username basis.
group tacacs+	Uses the list of all TACACS+ hosts for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Changing the Text Displayed at the Password Prompt

Use the **aaa authentication password-prompt** command to change the default text that the Cisco software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the following default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ or RADIUS server.

The **aaa authentication password-prompt** command works when RADIUS is used as the login method. You will see the password prompt defined in the command shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the NAS with the password prompt to be displayed to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt defined in the **aaa authentication password-prompt** command may be used.

Use the following command in global configuration mode:

Command or Action	Purpose
`Device(config)#` **aaa authentication password-prompt** *text-string*	Changes the default text displayed when a user is prompted to enter a password.

Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server

The following configuration steps provide the ability to prevent an Access Request with a blank username from being sent to the RADIUS server. This functionality ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.

Note The **aaa authentication suppress null-username** command is available only in Cisco IOS XE Release 2.4 and Cisco IOS Release 12.2(33)SRD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication suppress null-username**
5. **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)# aaa new-model`	Enables AAA globally.
Step 4	**aaa authentication suppress null-username** **Example:** `Device(config)# aaa authentication suppress null-username`	Prevents an access request with a blank username from being sent to the RADIUS server.

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

Configuring a Login Banner

To configure a banner that is displayed when a user logs in (replacing the default message for login), perform the following task:

Before You Begin

To create a login banner, you must configure a delimiting character that notifies the system that the following text string must be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string for the banner.

SUMMARY STEPS

1. **aaa new-model** Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication banner** *delimiter string delimiter*
3. Device(config)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**aaa new-model** Device(config)# **aaa new-model**	Enables AAA.
Step 2	Device(config)# **aaa authentication banner** *delimiter string delimiter*	Creates a personalized login banner.
Step 3	Device(config)# **end**	Returns to privileged EXEC mode.

What to Do Next

After you have configured a login banner, you must complete basic authentication configuration using AAA if you have not already done so. For information about the different types of AAA authentication available, please refer to “Configuring Authentication” in the *Authentication, Authorization, and Accounting Configuration Guide*.

Configuring a Failed-Login Banner

To configure a message that is displayed when a user login fails (replacing the default message for failed login), perform the following task:

Before You Begin

To create a failed-login banner, you must configure a delimiting character, which notifies the system that the following text string must be displayed as the banner, and then configure the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the failed-login banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

SUMMARY STEPS

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication fail-message** *delimiter string delimiter*
3. Device(config)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa new-model**	Enables AAA.
Step 2	Device(config)# **aaa authentication fail-message** *delimiter string delimiter*	Creates a message to be displayed when a user login fails.
Step 3	Device(config)# **end**	Returns to privileged EXEC mode.

What to Do Next

After you have configured a failed-login banner, you must complete basic authentication configuration using AAA if you have not already done so. For information about the different types of AAA authentication available, please refer to “Configuring Authentication” in the *Authentication, Authorization, and Accounting Configuration Guide*.

Configuring AAA Packet of Disconnect

Packet of disconnect (POD) terminates connections on the network access server (NAS) when particular session attributes are identified. By using the session information obtained from AAA, the POD client residing on a UNIX workstation sends disconnect packets to the POD server running on the network access server. The NAS terminates any inbound user session with one or more matching key attributes. It rejects requests when required fields are missing or when an exact match is not found.

To configure POD, perform the following tasks in global configuration mode:

SUMMARY STEPS

1. Device(config)# **aaa accounting network default**
2. Device(config)# **aaa accounting delay-start**
3. Device(config)# **aaa pod server server-key** *string*
4. Device(config)# **radius-server host** *IP address* **non-standard**
5. Device(config)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa accounting network default** **Example:** Enables AAA accounting records.	
Step 2	Device(config)# **aaa accounting delay-start**	(Optional) Delays generation of the start accounting record until the Framed-IP-Address is assigned, allowing the use of the start accounting record in the POD packet.
Step 3	Device(config)# **aaa pod server server-key** *string*	Enables POD reception.
Step 4	Device(config)# **radius-server host** *IP address* **non-standard**	Declares a RADIUS host that uses a vendor-proprietary version of RADIUS.
Step 5	Device(config)# **end**	Returns to the privileged EXEC mode.

Enabling Double Authentication

Depending on the Cisco release, PPP sessions could be authenticated only by using a single authentication method: either PAP or CHAP. Double authentication requires remote users to pass a second stage of authentication (after CHAP or PAP authentication) before gaining network access.

This second (“double”) authentication requires a password that is known to the user but *not* stored on the user’s remote host. Therefore, the second authentication is specific to a user, not to a host. This provides an additional level of security that will be effective even if information from the remote host is stolen. In addition, this also provides greater flexibility by allowing customized network privileges for each user.

The second stage authentication can use one-time passwords such as token card passwords, which are not supported by CHAP. If one-time passwords are used, a stolen user password is of no use to the perpetrator.

How Double Authentication Works

With double authentication, there are two authentication/authorization stages. These two stages occur after a remote user dials in and a PPP session is initiated.

In the first stage, the user logs in using the remote host name; CHAP (or PAP) authenticates the remote host, and then PPP negotiates with AAA to authorize the remote host. In this process, the network access privileges associated with the remote host are assigned to the user.

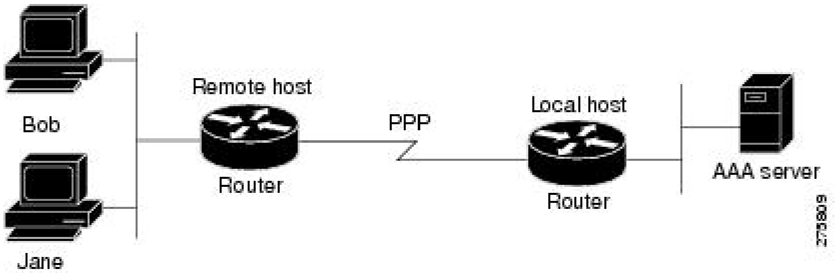
Note Cisco suggests that the network administrator restrict authorization at this first stage to allow only Telnet connections to the local host.

In the second stage, the remote user must Telnet to the network access server to be authenticated. When the remote user logs in, the user must be authenticated with AAA login authentication. The user must then enter the **access-profile** command to be reauthorized using AAA. When this authorization is complete, the user has been double authenticated, and can access the network according to per-user network privileges.

The system administrator determines the network privileges that the remote users will have after each stage of authentication by configuring appropriate parameters on a security server. To use double authentication, the user must activate it by using the **access-profile** command.

Caution Double authentication can cause certain undesirable events if multiple hosts share a PPP connection to a network access server, as shown in the figure below. First, if a user, Bob, initiates a PPP session and activates double authentication at the network access server (per the figure below), any other user will automatically have the same network privileges as Bob until Bob's PPP session expires. This happens because Bob's authorization profile is applied to the network access server's interface during the PPP session and any PPP traffic from other users will use the PPP session Bob established. Second, if Bob initiates a PPP session and activates double authentication, and then—before Bob's PPP session has expired—another user, Jane, executes the **access-profile** command (or, if Jane telnets to the network access server and the**autocommand access-profile** command is executed), a reauthorization will occur and Jane's authorization profile will be applied to the interface, replacing Bob's profile. This can disrupt or halt Bob's PPP traffic or grant Bob additional authorization privileges, which Bob should not have.

Figure 2: Possibly Risky Topology: Multiple Hosts Share a PPP Connection to a Network Access Server



Configuring Double Authentication

To configure double authentication, you must complete the following steps:

1 Enable AAA by using the **aaa-new model** global configuration command. For more information about enabling AAA, refer to the chapter "AAA Overview."

2 Use the **aaa authentication** command to configure your network access server to use login and PPP authentication method lists, and then apply those method lists to the appropriate lines or interfaces.

3 Use the **aaa authorization** command to configure AAA network authorization at login. For more information about configuring network authorization, refer to the "Configuring Authorization" chapter.

4 Configure security protocol parameters (for example, RADIUS or TACACS+). See the chapter "Configuring RADIUS" for more information about RADIUS and the chapter "Configuring TACACS+" for more information about TACACS+.

5 Use access control list AV pairs on the security server that the user can connect to the local host only by establishing a Telnet connection.

6 (Optional) Configure the **access-profile** command as an autocommand. If you configure the autocommand, remote users will not have to manually enter the **access-profile** command to access the authorized rights associated with their personal user profile. To learn about configuring autocommands, refer to the **autocommand** command in the *Dial Technologies Command Reference: Network Services.*

Note If the **access-profile** command is configured as an autocommand, users will still have to telnet to the local host and log in to complete double authentication.

Follow these rules when creating user-specific authorization statements (These rules relate to the default behavior of the **access-profile** command):

- Use valid AV pairs when configuring access control list AV pairs on the security server. For a list of valid AV pairs, refer to the chapter "Authentication Commands" in the *CiscoISecurity Command Reference*.
- If you want remote users to use the interface's existing authorization (which existed prior to the second stage authentication/authorization), but you want them to have different access control lists (ACLs), you should specify *only* ACL AV pairs in the user-specific authorization definition. This might be desirable if you set up a default authorization profile to apply to the remote host, but want to apply specific ACLs to specific users.
- When these user-specific authorization statements are later applied to the interface, they can either be *added to* the existing interface configuration or *replace* the existing interface configuration, depending on which form of the **access-profile** command is used to authorize the user. You should understand how the **access-profile** command works before configuring the authorization statements.
- If you are using ISDN or Multilink PPP, you must also configure virtual templates at the local host.

To troubleshoot double authentication, use the **debug aaa per-user** debug command. For more information about this command, refer to the *CiscoDebug Command Reference*.

Accessing the User Profile After Double Authentication

In double authentication, when a remote user establishes a PPP link to the local host using the local host name, the remote host is CHAP (or PAP) authenticated. After CHAP (or PAP) authentication, PPP negotiates with AAA to assign network access privileges associated with the remote host to the user. (Cisco suggests that privileges at this stage be restricted to allow the user to connect to the local host only by establishing a Telnet connection.)

When the user needs to initiate the second phase of double authentication, establishing a Telnet connection to the local host, the user enters a personal username and password (different from the CHAP or PAP username and password). This action causes AAA reauthentication to occur according to the personal username/password.

The initial rights associated with the local host, though, are still in place. By using the **access-profile** command, the rights associated with the local host are replaced by or merged with those defined for the user in the user's profile.

To access the user profile after double authentication, use the following command in EXEC configuration mode:

Command or Action	Purpose
Device> access-profile [**merge** | **replace**] [**ignore-sanity-checks**]	Accesses the rights associated for the user after double authentication.

If you configured the **access-profile** command to be executed as an autocommand, it will be executed automatically after the remote user logs in.

Enabling Automated Double Authentication

You can make the double authentication process easier for users by implementing automated double authentication. Automated double authentication provides all of the security benefits of double authentication, but offers a simpler, more user-friendly interface for remote users. With double authentication, a second level of user authentication is achieved when the user telnets to the network access server or device and enters a username and password. With automated double authentication, the user does not have to Telnet to the network access server; instead, the user responds to a dialog box that requests a username and password or personal identification number (PIN). To use the automated double authentication feature, the remote user hosts must be running a companion client application. As of Cisco IOS Release 12.0, the only client application software available is the Glacier Bay application server software for PCs.

Note Automated double authentication, like the existing double authentication feature, is for Multilink PPP ISDN connections only. Automated double authentication cannot be used with other protocols such as X.25 or SLIP.

Automated double authentication is an enhancement to the existing double authentication feature. To configure automated double authentication, you must first configure double authentication by completing the following steps:

1. Enable AAA by using the **aaa-new model** global configuration command. For more information about enabling AAA, refer to the chapter "AAA Overview."
2. Use the **aaa authentication** command to configure your network access server to use login and PPP authentication method lists, and then apply those method lists to the appropriate lines or interfaces.
3. Use the **aaa authorization** command to configure AAA network authorization at login. For more information about configuring network authorization, refer to the chapter "Configuring Authorization."
4. Configure security protocol parameters (for example, RADIUS or TACACS+). See the chapter "Configuring RADIUS" for more information about RADIUS and the chapter "Configuring TACACS+" for more information about TACACS+.
5. Use access control list AV pairs on the security server that the user can connect to the local host only by establishing a Telnet connection.

6 Configure the **access-profile** command as an autocommand. If you configure the autocommand, remote users will not have to manually enter the **access-profile** command to access authorized rights associated with their personal user profile. To learn about configuring autocommands, refer to the **autocommand** command in the *CiscoIOS Dial Technologies Command Reference*.

Note If the **access-profile** command is configured as an autocommand, users will still have to telnet to the local host and log in to complete double authentication.

Follow these rules when creating user-specific authorization statements. (These rules relate to the default behavior of the **access-profile** command):

- Use valid AV pairs when configuring access control list AV pairs on the security server. For a list of valid AV pairs, refer to the AAA part of the *Security Command Reference*.
- If you want remote users to use the interface's existing authorization (that which existed prior to the second stage authentication/authorization), but you want them to have different access control lists (ACLs), you should specify *only* ACL AV pairs in the user-specific authorization definition. This might be desirable if you set up a default authorization profile to apply to the remote host, but want to apply specific ACLs to specific users.
- When these user-specific authorization statements are later applied to the interface, they can either be *added to* the existing interface configuration, or *replace* the existing interface configuration, depending on which form of the **access-profile** command is used to authorize the user. You should understand how the **access-profile** command works before configuring the authorization statements.
- If you are using ISDN or Multilink PPP, you must also configure virtual templates at the local host.

To troubleshoot double authentication, use the **debug aaa per-user** debug command. For more information about this command, refer to the *Debug Command Reference*.

After you have configured double authentication, you are ready to configure the automation enhancement.

Configuring Automated Double Authentication

To configure automated double authentication, use the following commands, starting in global configuration mode:

SUMMARY STEPS

1. Device(config)# **ip trigger-authentication**
2. Enter one of the following:
   - **Device(config)# interface bri** *number*
   - **Device(config)# interface serial** *number* **:23**
3. Device(config-if)# **ip trigger-authentication**
4. Device(config-if)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **ip trigger-authentication** **Example:**	Enables automation of double authentication.
Step 2	Enter one of the following: • **Device(config)# interface bri** *number* • **Device(config)# interface serial** *number* **:23**	Selects an ISDN BRI or ISDN PRI interface and enters interface configuration mode.
Step 3	Device(config-if)# **ip trigger-authentication**	Applies automated double authentication to the interface.
Step 4	Device(config-if)# **end**	Returns to the privileged EXEC mode.

Troubleshooting Automated Double Authentication

To troubleshoot automated double authentication, use the following commands in privileged EXEC mode:

SUMMARY STEPS

1. Device# **show ip trigger-authentication**
2. Device# **clear ip trigger-authentication**
3. Device# **debug ip trigger-authentication**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device# **show ip trigger-authentication**	Displays the list of remote hosts for which automated double authentication has been attempted (successfully or unsuccessfully).
Step 2	Device# **clear ip trigger-authentication**	Clears the list of remote hosts for which automated double authentication has been attempted. This clears the table displayed by the **show ip trigger-authentication** command.
Step 3	Device# **debug ip trigger-authentication**	Displays **debug** output related to automated double authentication.

Configuring the Dynamic Authorization Service for RADIUS CoA

Perform the following steps to enable the device as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Sets up the local AAA server for the dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction, and enters dynamic authorization local server configuration mode. • In this mode, the RADIUS application commands are configured.
Step 5	**client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]	Configures the IP address or hostname of the AAA server client. • Use the optional **server-key** keyword and *string* argument to configure the server key at the client level.

	Command or Action	Purpose
	Example: `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	**Note** Configuring the server key at the client level overrides the server key configured at the global level.

Step 6	**domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
	Example:
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
		(Optional) Configures username domain options for the RADIUS application.
		• The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, /, **$**, **%**, \, #, or **-**.
		• The **stripping** keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.
		• The **right-to-left** keyword terminates the string at the first delimiter going from right to left.

Step 7	**port** *port-num* **Example:** `Device(config-locsvr-da-radius)# port 3799`	Configures the UDP port for CoA requests.

Step 8	**end**
	Example:
	`Device(config-locsvr-da-radius)# end`
		Returns to privileged EXEC mode.

Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests

When an authentication port is authenticated with multiple hosts and there is a Change of Authorization (CoA) request for one host to flap on this port or one host session to be terminated on this port, the other hosts on this port are also affected. Thus, an authenticated port with multiple hosts can trigger a DHCP renegotiation from one or more hosts in the case of a flap, or it can administratively shut down the authentication port that is hosting the session for one or more hosts.

Perform the following steps to configure the device to ignore RADIUS server Change of Authorization (CoA) requests in the form of a bounce port command or disable port command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **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)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**authentication command bounce-port ignore** **Example:** `Device(config)# authentication command bounce-port ignore`	(Optional) Configures the device to ignore a RADIUS server bounce port command that causes a host to link flap on an authentication port, which causes DHCP renegotiation from one or more hosts connected to this port.
Step 5	**authentication command disable-port ignore** **Example:** `Device(config)# authentication command disable-port ignore`	(Optional) Configures the device to ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions. • The shutting down of the port causes session termination.

Step 6	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring Domain Stripping at the Server Group Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-name*
4. **domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]
5. **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 group server radius** *server-name* **Example:** `Device(config)# aaa group server radius rad1`	Adds the RADIUS server and enters server group RADIUS configuration mode. • The *server-name* argument specifies the RADIUS server group name.
Step 4	**domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*] **Example:** `Device(config-sg-radius)# domain-stripping delimiter username@example.com`	Configures domain stripping at the server group level.

Step 5	**end**
	Example:
	`Device(config-sg-radius)# end`
		Exits server group RADIUS configuration mode and returns to the privileged EXEC mode.

Non-AAA Authentication Methods

Configuring Line Password Protection

This task is used to provide access control on a terminal line by entering the password and establishing password checking.

Note If you configure line password protection and then configure TACACS or extended TACACS, the TACACS username and password take precedence over line passwords. If you have not yet implemented a security policy, we recommend that you use AAA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
4. **password** *password*
5. **login**
6. **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	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Device(config)# line console 0`	Enters line configuration mode.

	Command or Action	Purpose
Step 4	**password** *password* **Example:** `Device(config-line)# secret word`	Assigns a password to a terminal or other device on a line. The password is case sensitive and can include spaces. For example, the password "Secret" is different than the password "secret," and "two words" is an acceptable password.
Step 5	**login** **Example:** `Device(config-line)# login`	Enables password checking at login. Line password verification can be disabled by using the **no** version of this command. **Note** The **login** command only changes the username and privilege level. It does not execute a shell; therefore autocommands are not executed. To execute autocommands under this circumstance, a Telnet session needs to be established to the device. Ensure the device is configured for secure Telnet sessions if autocommands are implemented this way.

Step 6	**end**
	Example:
	`Device(config-line)# end`
		Returns to the privileged EXEC mode.

Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:

- To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS
- To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and "no escape" situations

To establish username authentication, use the following commands in global configuration mode as needed for your system configuration:

SUMMARY STEPS

1. Enter one of the following:
    - **Device(config)# username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted password*]
    - **Device(config)# username** *name* [**access-class** *number*]
2. **Device(config)# username** *name* [**privilege** *level*]
3. **Device(config)# username** *name* [**autocommand** *command*]
4. **Device(config)# username** *name* [**noescape**] [**nohangup**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enter one of the following: • **Device(config)# username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted password*] • **Device(config)# username** *name* [**access-class** *number*]	(Optional) Establishes username authentication with encrypted passwords. or (Optional) Establishes username authentication by access list.
Step 2	**Device(config)# username** *name* [**privilege** *level*]	(Optional) Sets the privilege level for the user.
Step 3	**Device(config)# username** *name* [**autocommand** *command*]	(Optional) Specifies a command to be executed automatically.
Step 4	**Device(config)# username** *name* [**noescape**] [**nohangup**]	(Optional) Sets a “no escape” login environment.

What to Do Next

The **noescape** keyword prevents users from using escape characters on the hosts to which they are connected. The **nohangup** feature does not disconnect after using the autocommand.

Caution Passwords will be displayed in clear text in your configuration unless you enable the **service password-encryption** command. For more information about the **service password-encryption** command, refer to the chapter “Passwords and Privileges Commands” in the *Security Command Reference* .

Enabling CHAP or PAP Authentication

One of the most common transport protocols used in ISPs' dial solutions is the Point-to-Point Protocol PPP. Traditionally, remote users dial in to an access server to initiate a PPP session. After PPP has been negotiated, remote users are connected to the ISP network and to the Internet.

Because ISPs want only customers to connect to their access servers, remote users are required to authenticate to the access server before they can start up a PPP session. Normally, a remote user authenticates by typing in a username and password when prompted by the access server. Although this is a workable solution, it is difficult to administer and awkward for the remote user.

A better solution is to use the authentication protocols built into PPP. In this case, the remote user dials in to the access server and starts up a minimal subset of PPP with the access server. This does not give the remote user access to the ISP's network—it merely allows the access server to talk to the remote device.

PPP currently supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both are specified in RFC 1334 and are supported on synchronous and asynchronous interfaces. Authentication using PAP or CHAP is equivalent to typing in a username and password when prompted by the server. CHAP is considered to be more secure because the remote user's password is never sent across the connection.

PPP (with or without PAP or CHAP authentication) is also supported in dialout solutions. An access server utilizes a dialout feature when it initiates a call to a remote device and attempts to start up a transport protocol such as PPP.

See "Configuring Interfaces" in the *Configuration Fundamentals Configuration Guide* for more information about CHAP and PAP.

Note To use CHAP or PAP, you must be running PPP encapsulation.

When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or "challenges" the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local device.

When the remote device receives the challenge packet, it concatenates the ID, the remote device's password, and the random number, and then encrypts all of it using the remote device's password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process.

When the access server receives the response, it uses the name it received to retrieve a password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password—if the result matches the result sent in the response packet, authentication succeeds.

The benefit of using CHAP authentication is that the remote device's password is never transmitted in clear text. This prevents other devices from stealing it and gaining illegal access to the ISP's network.

CHAP transactions occur only at the time a link is established. The access server does not request a password during the rest of the call. (The local device can, however, respond to such requests from other devices during a call.)

When PAP is enabled, the remote device attempting to connect to the access server is required to send an authentication request. If the username and password specified in the authentication request are accepted, the Cisco software sends an authentication acknowledgment.

After you have enabled CHAP or PAP, the access server will require authentication from remote devices dialing in to the access server. If the remote device does not support the enabled protocol, the call will be dropped.

To use CHAP or PAP, you must perform the following tasks:

1. Enable PPP encapsulation.
2. Enable CHAP or PAP on the interface.
3. For CHAP, configure host name authentication and the secret or password for each remote system with which authentication is required.

Enabling PPP Encapsulation

To enable PPP encapsulation, use the following command in interface configuration mode:

Command or Action	Purpose
`Device(config-if)#` **encapsulation ppp**	Enables PPP on an interface.

Enabling PAP or CHAP

To enable CHAP or PAP authentication on an interface configured for PPP encapsulation, use the following command in interface configuration mode:

Command or Action	Purpose
Device(config-if)# ppp authentication {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**]	Defines the authentication protocols supported and the order in which they are used. In this command, *protocol1, protocol2* represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, which is *protocol1* . If *protocol1* is unable to establish authentication, the next configured protocol is used to negotiate authentication.

If you configure **ppp authentication chap** on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using CHAP; likewise, if you configure **ppp authentication pap**, all incoming calls that start a PPP connection will have to be authenticated using PAP. If you configure **ppp authentication chap pap**, the access server will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the access server will try to authenticate the call using PAP. If the remote device does not support either CHAP or PAP, authentication will fail and the call will be dropped. If you configure **ppp authentication pap chap**, the access server will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device does not support either protocol, authentication will fail and the call will be dropped. If you configure the **ppp authentication** command with the **callin** keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the **one-time** keyword are only available if you have enabled AAA--they will not be available if you are using TACACS or extended TACACS. If you specify the name of an authentication method list with the **ppp authentication** command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The **ppp authentication** command with the **one-time** keyword enables support for one-time passwords during authentication.

The **if-needed** keyword is only available if you are using TACACS or extended TACACS. The **ppp authentication**command with the **if-needed** keyword means that PPP will only authenticate the remote device using PAP or CHAP if they have not yet authenticated during the life of the current call. If the remote device authenticated via a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate via CHAP if **ppp authentication chap if-needed** is configured on the interface.

Caution If you use a *list-name* that has not been configured with the **aaa authentication ppp**command, you disable PPP on the line.

For information about adding a **username** entry for each remote system from which the local device or access server requires authentication, see Establishing Username Authentication, on page 44.

Inbound and Outbound Authentication

PPP supports two-way authentication. Normally, when a remote device dials in to an access server, the access server requests that the remote device prove that it is allowed access. This is known as inbound authentication. At the same time, the remote device can also request that the access server prove that it is who it says it is. This is known as outbound authentication. An access server also does outbound authentication when it initiates a call to a remote device.

Enabling Outbound PAP Authentication

To enable outbound PAP authentication, use the following command in interface configuration mode:

Command or Action	Purpose
Device(config-if)# ppp pap sent-username *username* **password** *password*	Enables outbound PAP authentication.

The access server uses the username and password specified by the **ppp pap sent-username** command to authenticate itself whenever it initiates a call to a remote device or when it has to respond to a remote device's request for outbound authentication.

Refusing PAP Authentication Requests

To refuse PAP authentication from peers requesting it, meaning that PAP authentication is disabled for all calls, use the following command in interface configuration mode:

Command or Action	Purpose
Device(config-if)# pap refuse	Refuses PAP authentication from peers requesting PAP authentication.

If the **refuse** keyword is not used, the device will not refuse any PAP authentication challenges received from the peer.

Creating a Common CHAP Password

For remote CHAP authentication only, you can configure your device to create a common CHAP secret password to use in response to challenges from an unknown peer; for example, if your device calls a rotary of devices (either from another vendor, or running an older version of the Cisco software) to which a new (that is, unknown) device has been added. The **ppp chap password** command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

To enable a device calling a collection of devices to configure a common CHAP secret password, use the following command in interface configuration mode:

Command or Action	Purpose
Device(config-if)# ppp chap password *secret*	Enables a device calling a collection of devices to configure a common CHAP secret password.

Refusing CHAP Authentication Requests

To refuse CHAP authentication from peers requesting it, meaning that CHAP authentication is disabled for all calls, use the following command in interface configuration mode:

Command or Action	Purpose
Device(config-if)# ppp chap refuse [**callin**]	Refuses CHAP authentication from peers requesting CHAP authentication.

If the **callin** keyword is used, the device will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the device sends.

If outbound PAP has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Delaying CHAP Authentication Until Peer Authenticates

To specify that the device will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the device, use the following command in interface configuration mode:

Command or Action	Purpose
Device(config-if)# ppp chap wait *secret*	Configures the device to delay CHAP authentication until after the peer has authenticated itself to the device.

This command (which is the default) specifies that the device will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the device. The **no ppp chap wait** command specifies that the device will respond immediately to an authentication challenge.

Using MS-CHAP

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension of RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco device or access server acting as a network access server.

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.*x*. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set of "reason-for failure" codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without AAA security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both TACACS+ and RADIUS. The table below lists the vendor-specific RADIUS attributes (IETF Attribute 26) that enable RADIUS to support MS-CHAP.

Table 9: Vendor-Specific RADIUS Attributes for MS-CHAP

Vendor-ID Number	Vendor-Type Number	Vendor-Proprietary Attribute	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets.
211	11	MSCHAP-Response	Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier.

Defining PPP Authentication using MS-CHAP

To define PPP authentication using MS-CHAP, use the following commands in interface configuration mode:

SUMMARY STEPS

1. **Device(config-if)# encapsulation ppp**
2. **Device(config-if)# ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Device(config-if)# encapsulation ppp**	Enables PPP encapsulation.
Step 2	**Device(config-if)# ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]	Defines PPP authentication using MS-CHAP.

What to Do Next

If you configure **ppp authentication ms-chap** on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using MS-CHAP. If you configure the **ppp authentication** command with the **callin** keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the **one-time** keyword are only available if you have enabled AAA—they will not be available if you are using TACACS or extended TACACS. If you specify the name of an authentication method list with the **ppp authentication** command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The **ppp authentication** command with the **one-time** keyword enables support for one-time passwords during authentication.

The **if-needed** keyword is only available if you are using TACACS or extended TACACS. The **ppp authentication** command with the **if-needed** keyword means that PPP will only authenticate the remote device via MS-CHAP if that device has not yet authenticated during the life of the current call. If the remote device authenticated through a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate through MS-CHAP if **ppp authentication chap if-needed** is configured.

Note If PPP authentication using MS-CHAP is used with username authentication, you must include the MS-CHAP secret in the local username/password database. For more information about username authentication, refer to the “Establish Username Authentication” section.

Authentication Examples

RADIUS Authentication Examples

This section provides two sample configurations using RADIUS.

The following example shows how to configure the device to authenticate and authorize using RADIUS:

```
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp if-needed group radius
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
line 3
login authentication radius-login
interface serial 0
ppp authentication radius-ppp
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login radius-login group radius local** command configures the device to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The **aaa authentication ppp radius-ppp if-needed group radius** command configures the Cisco software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.
- The **aaa authorization exec default group radius if-authenticated** command queries the RADIUS database for information that is used during EXEC authorization, such as autocommands and privilege levels, but only provides authorization if the user has successfully authenticated.
- The **aaa authorization network default group radius** command queries RADIUS for network authorization, address assignment, and other access lists.

- The **login authentication radius-login** command enables the radius-login method list for line 3.
- The **ppp authentication radius-ppp** command enables the radius-ppp method list for serial interface 0.

The following example shows how to configure the device to prompt for and verify a username and password, authorize the user's EXEC level, and specify it as the method of authorization for privilege level 2. In this example, if a local username is entered at the username prompt, that username is used for authentication.

If the user is authenticated using the local database, EXEC authorization using RADIUS will fail because no data is saved from the RADIUS authentication. The method list also uses the local database to find an autocommand. If there is no autocommand, the user becomes the EXEC user. If the user then attempts to use commands that are set at privilege level 2, TACACS+ is used to attempt to authorize the command.

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 192.0.2.3 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login default group radius local** command specifies that the username and password are verified by RADIUS or, if RADIUS is not responding, by the device's local user database.
- The **aaa authorization exec default group radius local**command specifies that RADIUS authentication information be used to set the user's EXEC level if the user authenticates with RADIUS. If no RADIUS information is used, this command specifies that the local user database be used for EXEC authorization.
- The **aaa authorization command 2 default group tacacs+ if-authenticated** command specifies TACACS+ authorization for commands set at privilege level 2, if the user has already successfully authenticated.
- The **radius-server host 172.16.71.146 auth-port 1645 acct-port 1646** command specifies the IP address of the RADIUS server host, the UDP destination port for authentication requests, and the UDP destination port for accounting requests.
- The **radius-server attribute 44 include-in-access-req** command sends RADIUS attribute 44 (Acct-Session-ID) in access-request packets.
- The **radius-server attribute 8 include-in-access-req** command sends RADIUS attribute 8 (Framed-IP-Address) in access-request packets.

TACACS Authentication Examples

The following example shows how to configure TACACS+ as the security protocol to be used for PPP authentication:

```
aaa new-model
aaa authentication ppp test group tacacs+ local
interface serial 0
ppp authentication chap pap test
tacacs-server host 192.0.2.3
tacacs-server key goaway
```

The lines in this sample TACACS+ authentication configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines a method list, “test,” to be used on serial interfaces running PPP. The keywords **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **interface** command selects the line.
- The **ppp authentication** command applies the test method list to this line.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 192.0.2.3.
- The **tacacs-server key** command defines the shared encryption key to be “goaway.”

The following example shows how to configure AAA authentication for PPP:

```
aaa authentication ppp default if-needed group tacacs+ local
```

In this example, the keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP is not necessary and can be skipped. If authentication is needed, the keywords **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

The following example shows how to create the same authentication algorithm for PAP, but it calls the method list “MIS-access” instead of “default”:

```
aaa authentication ppp MIS-access if-needed group tacacs+ local
interface serial 0
ppp authentication pap MIS-access
```

In this example, because the list does not apply to any interfaces (unlike the default list, which applies automatically to all interfaces), the administrator must select interfaces to which this authentication scheme should apply by using the **interface** command. The administrator must then apply this method list to those interfaces by using the **ppp authentication** command.

Kerberos Authentication Examples

To specify Kerberos as the login authentication method, use the following command:

```
aaa authentication login default krb5
```

To specify Kerberos authentication for PPP, use the following command:

```
aaa authentication ppp default krb5
```

AAA Scalability Example

The following example shows a general security configuration using AAA with RADIUS as the security protocol. In this example, the network access server is configured to allocate 16 background processes to handle AAA requests for PPP.

```
aaa new-model
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
```

```
aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication pap dialins
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **radius-server configure-nas** command defines that the Cisco device or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa processes** command allocates 16 background processes to handle AAA requests for PPP.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the "admins" method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication pap dialins**command applies the "dialins" method list to the specified interfaces.

Example: Configuring Login and Failed-Login Banners for AAA Authentication

The following example shows how to configure a login banner that is displayed when a user logs in to the system, (in this case, the phrase "Unauthorized Access Prohibited"). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

This configuration displays the following login banner:

```
Unauthorized Access Prohibited
Username:
```

The following example shows how to configure a failed-login banner that is displayed when a user tries to log in to the system and fails, (in this case, the phrase "Failed login. Try again"). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

This configuration displays the following login and failed-login banner:

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA Packet of Disconnect Server Key Example

The following example shows how to configure POD (packet of disconnect), which terminates connections on the network access server (NAS) when particular session attributes are identified.

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 192.0.2.3 non-standard
radius-server key rad123
```

Double Authentication Examples

The examples in this section illustrate possible configurations to be used with double authentication. Your configurations could differ significantly, depending on your network and security requirements.

Note These configuration examples include specific IP addresses and other specific information. This information is for illustration purposes only: your configuration will use different IP addresses, different usernames and passwords, and different authorization statements.

Configuration of the Local Host for AAA with Double Authentication Examples

These two examples show how to configure a local host to use AAA for PPP and login authentication, and for network and EXEC authorization. An example each is shown for RADIUS and for TACACS+.

In both the examples, the first three lines configure AAA with a specific server as the AAA server. The next two lines configure AAA for PPP and login authentication, and the last two lines configure network and EXEC authorization. The last line is necessary only if the **access-profile** command will be executed as an autocommand.

The following example shows device configuration with a RADIUS AAA server:

```
aaa new-model
radius-server host secureserver
radius-server key myradiuskey
aaa authentication ppp default group radius
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization exec default group radius
```

The following example shows device configuration with a TACACS+ server:

```
aaa new-model
tacacs-server host security
tacacs-server key mytacacskey
aaa authentication ppp default group tacacs+
aaa authentication login default group tacacs+
aaa authorization network default group tacacs+
aaa authorization exec default group tacacs+
```

Configuration of the AAA Server for First-Stage PPP Authentication and Authorization Example

This example shows a configuration on the AAA server. A partial sample AAA configuration is shown for RADIUS.

TACACS+ servers can be configured similarly. See Complete Configuration with TACACS Example for more information.

This example defines authentication/authorization for a remote host named “hostx” that will be authenticated by CHAP in the first stage of double authentication. Note that the ACL AV pair limits the remote host to Telnet connections to the local host. The local host has the IP address 10.0.0.2.

The following example shows a partial AAA server configuration for RADIUS:

```
hostx   Password = “welcome”
        User-Service-Type = Framed-User,
        Framed-Protocol = PPP,
        cisco-avpair = “lcp:interface-config=ip unnumbered ethernet 0”,
        cisco-avpair = “ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet”,
        cisco-avpair = “ip:inacl#4=deny icmp any any”,
        cisco-avpair = “ip:route#5=10.0.0.0 255.0.0.0”,
        cisco-avpair = “ip:route#6=10.10.0.0 255.0.0.0”,
        cisco-avpair = “ipx:inacl#3=deny any”
```

Configuration of the AAA Server for Second-Stage Per-User Authentication and Authorization Examples

This section contains partial sample AAA configurations on a RADIUS server. These configurations define authentication and authorization for a user (Pat) with the username “patuser,” who will be user-authenticated in the second stage of double authentication.

TACACS+ servers can be configured similarly. See Complete Configuration with TACACS Example for more information.

Three examples show sample RADIUS AAA configurations that could be used with each of the three forms of the **access-profile** command.

The first example shows a partial sample AAA configuration that works with the default form (no keywords) of the **access-profile** command. Note that only ACL AV pairs are defined. This example also sets up the **access-profile** command as an autocommand.

```
patuser   Password = “welcome”
          User-Service-Type = Shell-User,
          cisco-avpair = “shell:autocmd=access-profile”
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = “ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet”,
          cisco-avpair = “ip:inacl#4=deny icmp any any”
```

The second example shows a partial sample AAA configuration that works with the **access-profile merge** form of the **access-profile** command. This example also sets up the **access-profile merge** command as an autocommand.

```
patuser   Password = “welcome”
          User-Service-Type = Shell-User,
          cisco-avpair = “shell:autocmd=access-profile merge”
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = “ip:inacl#3=permit tcp any any”
          cisco-avpair = “ip:route=10.0.0.0 255.255.0.0",
          cisco-avpair = “ip:route=10.1.0.0 255.255.0.0",
          cisco-avpair = “ip:route=10.2.0.0 255.255.0.0"
```

The third example shows a partial sample AAA configuration that works with the **access-profile replace** form of the **access-profile** command. This example also sets up the **access-profile replace** command as an autocommand.

```
patuser   Password = “welcome”
          User-Service-Type = Shell-User,
          cisco-avpair = “shell:autocmd=access-profile replace”
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = “ip:inacl#3=permit tcp any any”,
          cisco-avpair = “ip:inacl#4=permit icmp any any”,
          cisco-avpair = “ip:route=10.10.0.0 255.255.0.0",
          cisco-avpair = “ip:route=10.11.0.0 255.255.0.0",
          cisco-avpair = “ip:route=10.12.0.0 255.255.0.0"
```

Complete Configuration with TACACS Example

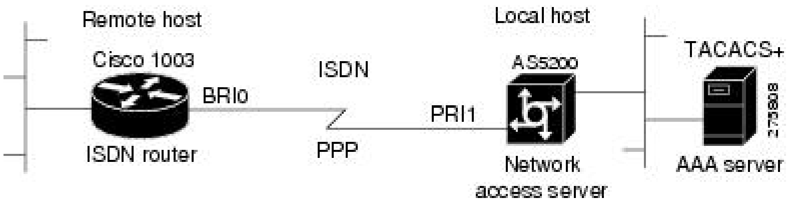
This example shows TACACS+ authorization profile configurations both for the remote host (used in the first stage of double authentication) and for specific users (used in the second stage of double authentication). This

TACACS+ example contains approximately the same configuration information as shown in the previous RADIUS examples.

This sample configuration shows authentication/authorization profiles on the TACACS+ server for the remote host “hostx” and for three users, with the usernames “pat_default,” “pat_merge,” and “pat_replace.” The configurations for these three usernames illustrate different configurations that correspond to the three different forms of the **access-profile** command. The three user configurations also illustrate setting up the autocommand for each form of the **access-profile** command.

The figure below shows the topology. The example that follows the figure shows a TACACS+ configuration file.

Figure 3: Example Topology for Double Authentication



This sample configuration shows authentication/authorization profiles on the TACACS+ server for the remote host “hostx” and for three users, with the usernames “pat_default,” “pat_merge,” and “pat_replace.”

```
key = “mytacacskey”
default authorization = permit
#-----------------------------Remote Host (BRI)-------------------------
#
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#
#-----------------------------------------------------------------------
user = hostx
{
    login = cleartext “welcome”
    chap = cleartext “welcome”
    service = ppp protocol = lcp {
                interface-config=”ip unnumbered ethernet 0"
    }
    service = ppp protocol = ip {
            # It is important to have the hash sign and some string after
            # it. This indicates to the NAS that you have a per-user
            # config.
            inacl#3=”permit tcp any 172.21.114.0 0.0.0.255 eq telnet”
            inacl#4=”deny icmp any any”
            route#5=”10.0.0.0 255.0.0.0"
            route#6=”10.10.0.0 255.0.0.0"
    }
    service = ppp protocol = ipx {
            # see previous comment about the hash sign and string, in protocol = ip
            inacl#3=”deny any”
    }
}
#------------------- “access-profile” default user “only acls” ------------------
#
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#
#--------------------------------------------------------------------------------
user = pat_default
```

```
{
        login = cleartext “welcome”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_default logs in.
                autocmd = “access-profile”
        }
        service = ppp protocol = ip {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any host 10.0.0.2 eq telnet”
                inacl#4=”deny icmp any any”
        }
        service = ppp protocol = ipx {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
#--------------------- “access-profile merge” user ---------------------------
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
# open the possibility of conflicting configurations.
#
#-----------------------------------------------------------------------------
user = pat_merge
{
        login = cleartext “welcome”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_merge logs in.
                autocmd = “access-profile merge”
        }
        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any any”
                route#2=”10.0.0.0 255.255.0.0"
                route#3=”10.1.0.0 255.255.0.0"
                route#4=”10.2.0.0 255.255.0.0"
        }
        service = ppp protocol = ipx
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
#--------------------- “access-profile replace” user ----------------------------
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
# Such AV pairs are considered to be “invalid” for this context.
#-------------------------------------------------------------------------------
user = pat_replace
{
        login = cleartex
t
“
welcome
”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_replace logs in.
                autocmd = “access-profile replace”
        }
        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any any”
                inacl#4=”permit icmp any any”
                route#2=”10.10.0.0 255.255.0.0"
                route#3=”10.11.0.0 255.255.0.0"
                route#4=”10.12.0.0 255.255.0.0"
        }
        service = ppp protocol = ipx
        {
                # put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
```

Automated Double Authentication Example

This example shows a complete configuration file for a Cisco 2509 router with automated double authentication configured. The configuration commands that apply to automated double authentication are preceded by descriptions with a double asterisk (**).

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the TACACS+ AAA server:
aaa authentication login default group tacacs+
aaa authentication login console none
! **The following command enables device authentication via the TACACS+ AAA server:
aaa authentication ppp default group tacacs+
! **The following command causes the remote user’s authorization profile to be
! downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization exec default group tacacs+
! **The following command causes the remote device’s authorization profile to be
! downloaded from the AAA server to the Cisco 2509 router when required:
```

```
aaa authorization network default group tacacs+
enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
ip name-server 172.16.2.75
! **The following command globally enables automated double authentication:
ip trigger-authentication timeout 60 port 7500
isdn switch-type basic-5ess
!
!
interface Ethernet0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 ip address 172.21.127.105 255.255.255.248
 encapsulation ppp
 no ip mroute-cache
 no keepalive
 shutdown
 clockrate 2000000
 no cdp enable
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no cdp enable
!
! **Automated double authentication occurs via the ISDN BRI interface BRI0:
interface BRI0
 ip unnumbered Ethernet0
! **The following command turns on automated double authentication at this interface:
 ip trigger-authentication
! **PPP encapsulation is required:
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 500
 dialer map ip 172.21.127.113 name myrouter 60074
 dialer-group 1
 no cdp enable
! **The following command specifies that device authentication occurs via PPP CHAP:
 ppp authentication chap
!
router eigrp 109
 network 172.21.0.0
 no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 171.69.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
```

```
tacacs-server key mytacacskey
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 login authentication console
line aux 0
 transport input all
line vty 0 4
 exec-timeout 0 0
 password lab
!
end
```

MS-CHAP Example

The following example shows how to configure a Cisco AS5200 Universal Access Server (enabled for AAA and communication with a RADIUS security server) for PPP authentication using MS-CHAP:

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
username root password ALongPassword
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication ms-chap dialins
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines another method list, “admins”, for login authentication.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.

- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication ms-chap dialins** command selects MS-CHAP as the method of PPP authentication and applies the "dialins" method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the "admins" method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

Additional References

Related Documents

Related Topic	Document Title
Authorization	Configuring Authorization module.
Accounting	Configuring Accounting module.
RADIUS server	Configuring RADIUS module.
TACACS+ server	Configuring TACACS+ module.
Kerberos	Configuring Kerberos module.

Standards and RFCs

Standard/RFC	Title
RFC 2903	*Generic AAA Architecture*
RFC 2904	*AAA Authorization Framework*
RFC 2906	*AAA Authorization Requirements*
RFC 2989	*Criteria for Evaluating AAA Protocols for Network Access*
RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

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

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 Authentication

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 Configuring Authentication

Feature Name	Releases	Feature Information
AAA Per-User Scalability	12.2(27)SB, 12.2(33)SR, 15.0(1)M	This feature was introduced in Cisco IOS Release 12.2(27)SB. This feature was integrated into Cisco IOS Release 12.2(33)SR. This feature was integrated into Cisco IOS Release 15.0(1)M.

Feature Name	Releases	Feature Information
Change of Authorization (CoA)	12.2(33)SXI4, 15.2(2)T	Depending on your release, the Cisco software supports the RADIUS Change of Authorization (CoA) extensions defined in RFC 5176. COA extensions are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers. The following commands were introduced: **aaa server radius dynamic author**, **authentication command bounce-port ignore**, **authentication command disable-port ignore**.
Domain Stripping at the Server Group Level	15.2(3)T	The Domain Stripping feature allows domain stripping to be configured at the server group level. Per-server group configuration overrides the global configuration. The following sections provide information about this feature: • Domain Stripping • Configuring Domain Stripping at the Server Group Level The following command was introduced: **domain-stripping**.

Feature Name	Releases	Feature Information
LDAP integration with Active Directory	15.1(1)T	This feature provides the authentication and authorization support for AAA. LDAP is a standard-based protocol used to access directories. It is based on a client server model similar to RADIUS. LDAP is deployed on Cisco devices to send authentication requests to a central LDAP server that contains all user authentication and network service access information. The following command was introduced: **aaa authentication login default group ldap**.

CHAPTER 2

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy.

- Finding Feature Information, page 69
- Information About RADIUS Change of Authorization, page 69
- How to Configure RADIUS Change of Authorization, page 74
- Configuration Examples for RADIUS Change of Authorization, page 79
- Additional References for RADIUS Change of Authorization, page 80
- Feature Information for RADIUS Change of Authorization, 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.

Information About RADIUS Change of Authorization

About RADIUS Change of Authorization

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network and the response is sent from the queried servers. The Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, in which the request originates from the external server to the device attached to the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

Use the following per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Security and Password
- Accounting

CoA Requests

CoA requests, as described in RFC 5176, are used in a pushed model to allow for session identification, host reauthentication, and session termination. The model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the device that acts as a listener.

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the device for a session termination.

The following table shows the IETF attributes that are supported for the RADIUS Change of Authorization (CoA) feature.

Table 11: Supported IETF Attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

The following table shows the possible values for the Error-Cause attribute.

Table 12: Error-Cause Values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

CoA Request Response Code

The CoA Request Response code can be used to issue a command to the device. The supported commands are listed in the “CoA Request Commands” section.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format.

The Attributes field is used to carry Cisco VSAs.

Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco vendor-specific attribute (VSA))
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)

Unless all session identification attributes included in the CoA message match the session, the device returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

Note A CoA NAK message is not sent for all CoA requests with a key mismatch. The message is sent only for the first three requests for a client. After that, all the packets from that client are dropped. When there is a key mismatch, the response authenticator sent with the CoA NAK message is calculated from a dummy key value.

CoA ACK Response Code

If an authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within a CoA ACK can vary based on the CoA Request.

CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure.

CoA Request Commands

The commands supported on the device are shown in the table below. All CoA commands must include the session identifier between the device and the CoA client.

Table 13: CoA Request Commands Supported on the Device

Command	Cisco VSA
Bounce host port	Cisco:Avpair=“subscriber:command=bounce-host-port”
Disable host port	Cisco:Avpair=“subscriber:command=disable-host-port”
Reauthenticate host	Cisco:Avpair=“subscriber:command=reauthenticate”
Terminate session	This is a standard disconnect request that does not require a VSA

Session Reauthentication

To initiate session reauthentication, the authentication, authorization, and accounting (AAA) server sends a standard CoA-Request message that contains a Cisco VSA and one or more session identification attributes. The Cisco VSA is in the form of Cisco:Avpair="subscriber:command=reauthenticate".

The current session state determines the device's response to the message in the following scenarios:

- If the session is currently authenticated by IEEE 802.1*x*, the device responds by sending an Extensible Authentication Protocol over LAN (EAPoL)-RequestId message to the server.
- If the session is currently authenticated by MAC authentication bypass (MAB), the device sends an access request to the server, passing the same identity attributes used for the initial successful authentication.
- If session authentication is in progress when the device receives the command, the device terminates the process and restarts the authentication sequence, starting with the method configured to be attempted first.

Session Termination

A CoA Disconnect-Request terminates the session without disabling the host port. CoA Disconnect-Request termination causes reinitialization of the authenticator state machine for the specified host, but does not restrict the host's access to the network. If the session cannot be located, the device returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK message.

To restrict a host's access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism.

CoA Request Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has the following VSA:

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section. If the device cannot locate the session, it returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the device locates the session, it disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

To ignore the RADIUS server CoA disable port command, see the "Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests" section.

CoA Request Bounce Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the Session Identification. If the session cannot be located, the device returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device disables the hosting port for a period of 10 seconds, reenables it (port-bounce), and returns a CoA-ACK.

To ignore the RADIUS server CoA bounce port, see the "Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests" section.

How to Configure RADIUS Change of Authorization

Configuring RADIUS Change of Authorization

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • 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 authentication, authorization, and accounting (AAA) globally.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server.
Step 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* **Example:** `Device(config-locsvr-da-radius)# client 10.0.0.1`	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 6	**port** *port-number* **Example:** `Device(config-locsvr-da-radius)# port 3799`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. **Note** The default port for packet of disconnect is 1700. Port 3799 is required to interoperate with ACS 5.1.

Step 7	**auth-type** {**any** | **all** | **session-key**}
	Example:
	`Device(config-locsvr-da-radius)# auth-type all`
		Specifies the type of authorization that the device must use for RADIUS clients. The client must match the configured attributes for authorization.

Step 8	**ignore session-key** **Example:** `Device(config-locsvr-da-radius)# ignore session-key`	(Optional) Configures the device to ignore the session key.
Step 9	**ignore server-key** **Example:** `Device(config-locsvr-da-radius)# ignore server-key`	(Optional) Configures the device to ignore the server key.
Step 10	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Returns to global configuration mode.

Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests

When an authentication port is authenticated with multiple hosts and there is a Change of Authorization (CoA) request for one host to flap on this port or one host session to be terminated on this port, the other hosts on this port are also affected. Thus, an authenticated port with multiple hosts can trigger a DHCP renegotiation from one or more hosts in the case of a flap, or it can administratively shut down the authentication port that is hosting the session for one or more hosts.

Perform the following steps to configure the device to ignore RADIUS server Change of Authorization (CoA) requests in the form of a bounce port command or disable port command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **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)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**authentication command bounce-port ignore** **Example:** `Device(config)# authentication command bounce-port ignore`	(Optional) Configures the device to ignore a RADIUS server bounce port command that causes a host to link flap on an authentication port, which causes DHCP renegotiation from one or more hosts connected to this port.

	Command or Action	Purpose
Step 5	**authentication command disable-port ignore** **Example:** `Device(config)# authentication command disable-port ignore`	(Optional) Configures the device to ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions. • The shutting down of the port causes session termination.

Step 6	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring the Dynamic Authorization Service for RADIUS CoA

Perform the following steps to enable the device as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
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.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Sets up the local AAA server for the dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction, and enters dynamic authorization local server configuration mode. • In this mode, the RADIUS application commands are configured.
Step 5	**client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*] **Example:** `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	Configures the IP address or hostname of the AAA server client. • Use the optional **server-key** keyword and *string* argument to configure the server key at the client level. **Note** Configuring the server key at the client level overrides the server key configured at the global level.

Step 6	**domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
	Example:
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
		(Optional) Configures username domain options for the RADIUS application.
		• The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, **/**, **$**, **%**, \, **#**, or **-**.
		• The **stripping** keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.
		• The **right-to-left** keyword terminates the string at the first delimiter going from right to left.

Step 7	**port** *port-num* **Example:** `Device(config-locsvr-da-radius)# port 3799`	Configures the UDP port for CoA requests.

Step 8	**end**
	Example:
	`Device(config-locsvr-da-radius)# end`
		Returns to privileged EXEC mode.

Monitoring and Troubleshooting RADIUS Change of Authorization

The following commands can be used to monitor and troubleshoot the RADIUS Change of Authorization feature:

Table 14: Monitoring and Troubleshooting RADIUS Change of Authorization

Command	Purpose
debug aaa coa	Displays debug information for CoA processing.
debug aaa pod	Displays debug messages related to packet of disconnect (POD) packets.
debug radius	Displays information associated with RADIUS.
show aaa attributes protocol radius	Displays the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name.

Configuration Examples for RADIUS Change of Authorization

Example: Configuring RADIUS Change of Authorization

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.0.0.1
Device(config-locsvr-da-radius)# server-key cisco123
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# auth-type all
Device(config-locsvr-da-radius)# ignore session-key
Device(config-locsvr-da-radius)# ignore server-key
Device(config-locsvr-da-radius)# end
```

Example: Configuring a Device to Ignore Bounce and Disable a RADIUS Requests

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# authentication command bounce-port ignore
Device(config)# authentication command disable-port ignore
Device(config)# end
```

Example: Configuring the Dynamic Authorization Service for RADIUS CoA

The following example shows how to configure the device as a authentication, authorization, and accounting (AAA) server to support Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1
Device(config-locsvr-da-radius)# domain delimiter @
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# end
```

Additional References for RADIUS Change of Authorization

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
Configuring AAA	*Authentication, Authorization, and Accounting Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2903	*Generic AAA Architecture*

Standard/RFC	Title
RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)*

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

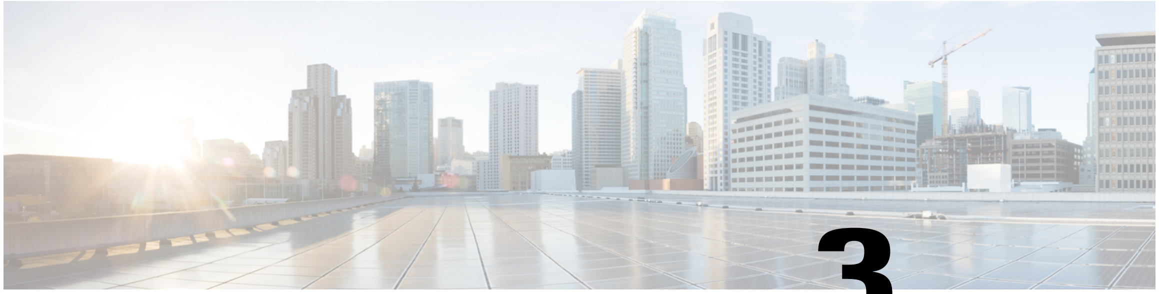
Feature Information for RADIUS Change of Authorization

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 RADIUS Change of Authorization

Feature Name	Releases	Feature Information
RADIUS Change of Authorization	12.2(33)SX14 15.2(2)T 15.1(1)SY	The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to reinitialize authentication and apply the new policy. The following commands were introduced or modified: **aaa server radius dynamic-author**, **authentication command bounce-port ignore**, and **authentication command disable-port ignore**.



CHAPTER 3

CWA URL Redirect support on C891FW

- Introduction, page 83
- Prerequisites for CWA URL Redirect support on C891FW, page 84
- Configuring CWA URL Redirect support on C891FW, page 85
- HTTP Proxy Configuration, page 90
- Configuration Examples for CWA URL Redirect support on C891FW, page 90
- Important Notes, page 96
- Additional References for CWA URL Redirect support on C891FW, page 96
- Feature Information for CWA URL Redirect support on C891FW, page 97

Introduction

The concept of central web authentication is opposed to local web authentication, which is the usual web authentication on the router itself. In that system, upon dot1x/mab failure, the router will failover to the webauth profile and will redirect client traffic to a web page on the router.

Central web authentication offers the possibility to have a central device that acts as a web portal (ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with mac/dot1x authentication. The concept also differs in that the radius server (ISE) returns special attributes that indicate to the router that a web redirection must occur. This solution has the advantage to eliminate any delay that was necessary for web authentication to kick. Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns redirection attributes, and the router authorizes the station (via MAC authentication bypass [MAB]) but places an access list to redirect the web traffic to the portal. Once the user logs in on the guest portal, it is possible via CoA (Change of Authorization) to bounce the router port so that a new Layer 2 MAB authentication occurs. The ISE can then remember it was a webauth user and apply Layer 2 attributes (like dynamic VAN assignment) to the user. An ActiveX component can also force the client PC to refresh its IP address.

This document describes how to configure central web authentication with wired clients connected to routers with the help of Identity Services Engine (ISE).

Prerequisites for CWA URL Redirect support on C891FW

Requirements

- Identity Services Engine (ISE)
- Cisco IOS router configuration

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine (ISE), Release 1.1.1

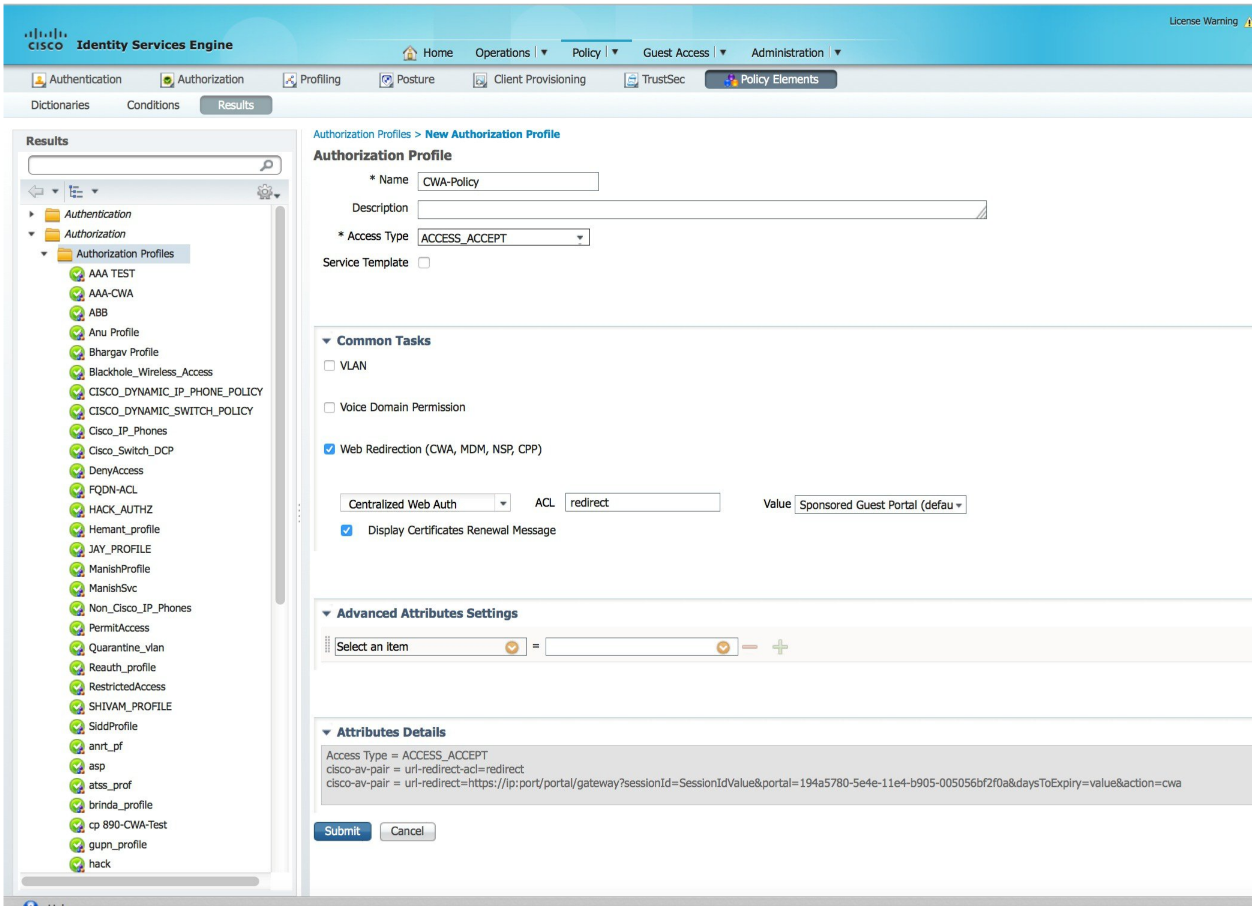
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuring CWA URL Redirect support on C891FW

Create an Authorization profile

The screenshot below displays the Authorization Profile configuration user interface:

Figure 4: Authorization Profile



Authorization Profile

* Name: CWA-Policy

Description:

* Access Type: ACCESS_ACCEPT

Service Template ☐

Common Tasks

☐ VLAN

☐ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth — ACL: redirect — Value: Sponsored Guest Portal (defau

☑ Display Certificates Renewal Message

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&daysToExpiry=value&action=cwa
```

1. Click **Policy**, and click **Policy Elements**.
2. Click **Results**.
3. Expand **Authorization**, and click **Authorization profile**.
4. Click the **Add** button in order to create a new authorization profile for central webauth.
5. In the **Name** field, enter a name for the profile.
6. Choose **ACCESS_ACCEPT** from the Access Type drop-down list.
7. Check the **Web Authentication** check box, and choose **Centralized** from the drop-down list.
8. In the **ACL** field, enter the name of the ACL on the switch that defines the traffic to be redirected.

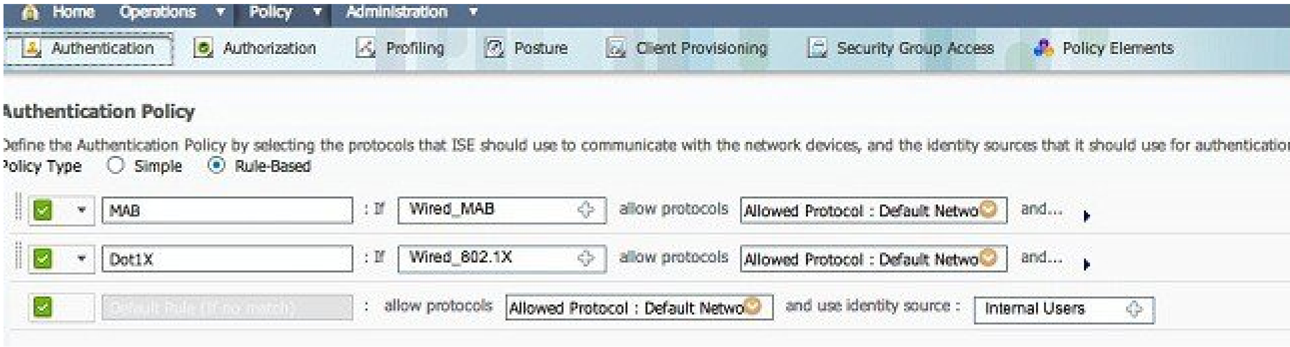
9 Choose **Default** from the Redirect drop-down list.

The Redirect attribute defines whether the ISE sees the default web portal or a custom web portal that the ISE admin created. For example, the redirect ACL in this example triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere. The ACL is defined on the switch later in this configuration example.

Create an Authentication Rule

The screenshot below displays the Authorization Profile configuration user interface:

Figure 5: Authentication Rule



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authenticatio

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netwo and...

☑ Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netwo and...

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Netwo and use identity source : Internal Users

1 Under the Policy menu, click **Authentication**.

The following image shows an example of how to configure the authentication policy rule. In this example, a rule is configured that triggers when MAB is detected.

2 Enter a name for your authentication rule.

3 Select the plus **(+)** icon in the **If** condition field.

4 Select **Compound condition**, and then select **Wired_MAB**.

5 Click the arrow located next to **and ...** to expand the rule.

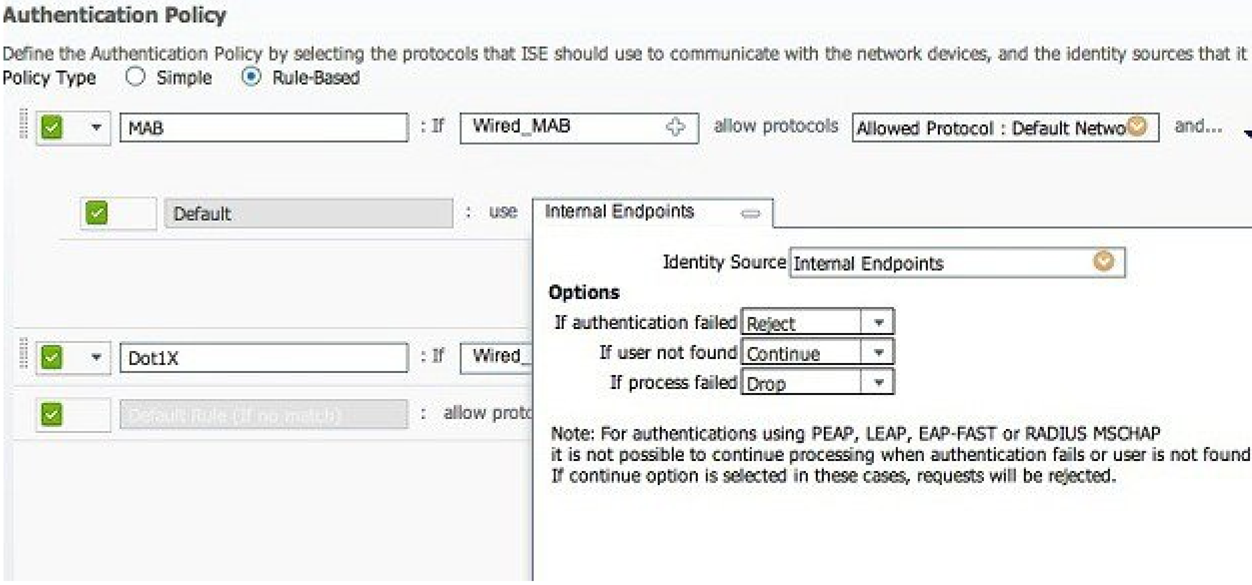
6 Click the + icon in the Identity Source field, and select **Internal endpoints**.

7 Select **Continue** from the If user not found drop-down list.

This option allows a device to be authenticated (through webauth) even if its MAC address is not known. Dot1x clients can still authenticate with their credentials and should not be concerned with this configuration.

The screenshot below displays the Internal Endpoints user interface:

Figure 6: Authentication Rule-Internal Endpoints



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netwo and...

☑ Default : use Internal Endpoints

Identity Source Internal Endpoints

Options

If authentication failed Reject

If user not found Continue

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP
it is not possible to continue processing when authentication fails or user is not found
If continue option is selected in these cases, requests will be rejected.

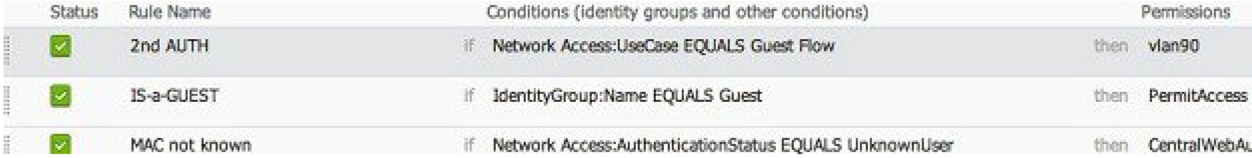
☑ Dot1X : If Wired_

☑ Default Rule (If no match) : allow proto

Create an Authorization Rule

Note There are several rules to configure in the authorization policy. When the PC is plugged in, it goes through MAB; it is assumed that the MAC address is not known, so the webauth and ACL are returned. This MAC not known rule is shown in the following image and is configured in this section:

Figure 7: Authorization Rule



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	2nd AUTH	if	Network Access:UseCase EQUALS Guest Flow	then	vlan90
☑	IS-a-GUEST	if	IdentityGroup:Name EQUALS Guest	then	PermitAccess
☑	MAC not known	if	Network Access:AuthenticationStatus EQUALS UnknownUser	then	CentralWebAu

1 Create a new rule, and enter a name.

2 Click the plus **(+)** icon in the condition field, and select **create a new condition**.

3 Select **Expression** from the drop-down list.

4 Select **Network Access** and expand.

5 Click **AuthenticationStatus**, and select **Equals** operator.

6 Select **UnknownUser**.

7 On the General Authorization page, select **CentralWebauth**.

Note This step allows the ISE to continue even though the user (or the MAC) is not known. Unknown users are now presented with the Login page. However, once they enter their credentials, they are presented again with an authentication request on the ISE; therefore, another rule must be configured with a condition that is met if the user is a guest user. In this example, If UseridentityGroup equals Guest is used, and it is assumed that all guests belong to this group.

8 Click the **actions** button located at the end of the MAC not known rule, and choose to insert a new rule above.

Note It is very important that this new rule comes before the MAC not known rule.

9 Enter a name for the new rule. Example, *IS-a-GUEST*.

10 Choose a condition that matches your guest users. Example, *InternalUser:IdentityGroup Equals Guest*. This is because all guest users are bound to the Guest group (or another group you configured in your sponsor settings).

11 Select **PermitAccess** in the result box (located to the right of the word then).

When the user is authorized on the Login page, ISE restarts a Layer 2 authentication on the switch port, and a new MAB occurs. In this scenario, the difference is that an invisible flag is set for ISE to remember that it was a guest-authenticated user. This rule is 2nd AUTH, and the condition is Network Access:UseCase Equals GuestFlow. This condition is met when the user authenticates via webauth, and the switch port is set again for a new MAB. You can assign any attributes you like. This example assigns a profile vlan90 so that the user is assigned the VLAN 90 in his second MAB authentication.

12 Click **Actions** (located at the end of the IS-a-GUEST rule), and select **Insert new rule above**.

13 Enter **2nd AUTH** in the name field.

14 In the condition field, click the **(+)** icon, and choose to create a new condition.

15 Select **Network Access**, and select **UseCase**.

16 Select **Equals** as the operator.

17 Select **GuestFlow** as the right operand.

18 On the authorization page, click the **(+)** icon to select a result for your rule.

In this example, a preconfigured profile (vlan90) is assigned; this configuration is not shown in this document.

Note You can use the **Permit Access** option or create a custom profile in order to return the VLAN or attributes.

Enable the IP Renewal

Note This task is optional.

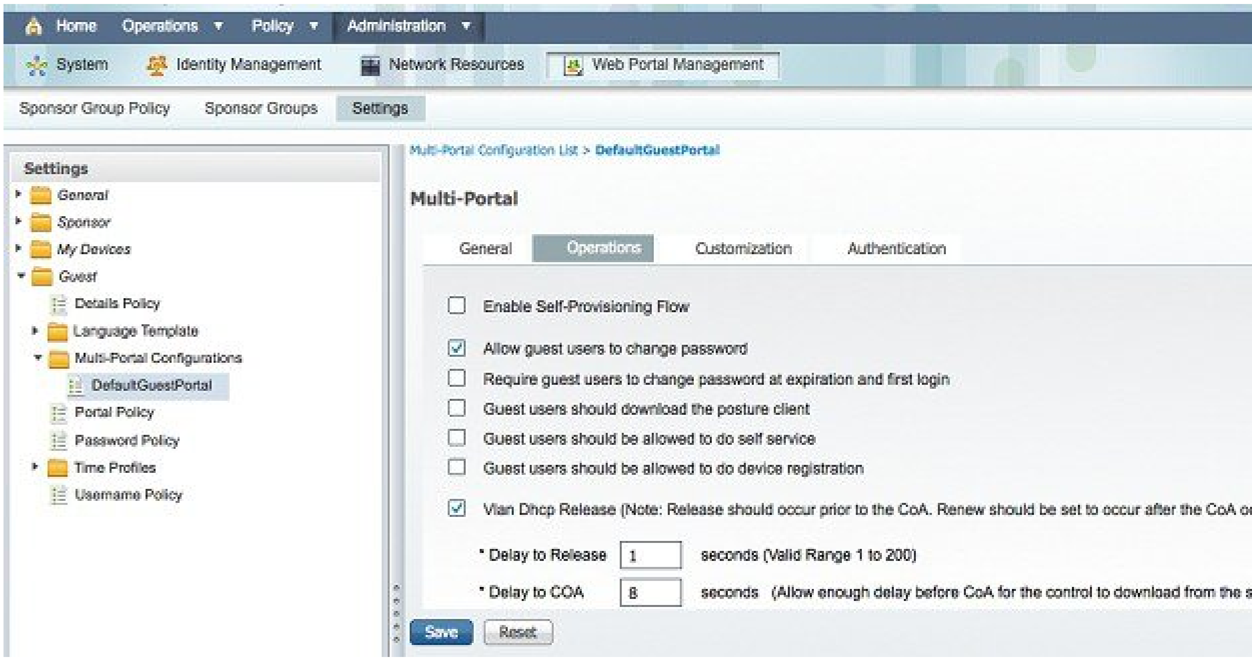
If you assign a VLAN, the final step is for the client PC to renew its IP address. This step is achieved by the guest portal for Windows clients. If you did not set a VLAN for the 2nd AUTH rule earlier, you can skip this task.

1. Click **Administration**, and select **Guest Management**.
2. Click **Settings**.
3. Select **Guest**, and expand **Multi-Portal Configuration**.
4. Click **DefaultGuestPortal** or the name of the custom portal you have created.
5. Select the **Vlan DHCP Release** check box.

Note This option works only for Windows clients.

The following screenshot displays the IP Renewal user interface:

Figure 8: IP Renewal



□ Enable Self-Provisioning Flow

☑ Allow guest users to change password

□ Require guest users to change password at expiration and first login

□ Guest users should download the posture client

□ Guest users should be allowed to do self service

□ Guest users should be allowed to do device registration

☑ Vlan Dhcp Release (Note: Release should occur prior to the CoA. Renew should be set to occur after the CoA o

* Delay to Release 1 seconds (Valid Range 1 to 200)

* Delay to COA 8 seconds (Allow enough delay before CoA for the control to download from the s

Task Result

The client PC plugs in and performs MAB. The MAC address is not known, so ISE pushes the redirection attributes back to the router. The user tries to go to a website and is redirected.

When the authentication of the Login page is successful, the ISE bounces the switchport through Change Of Authorization, which starts again a Layer 2 MAB authentication.

However, the ISE knows that it is a former webauth client and authorizes the client based on the webauth credentials (although this is a Layer 2 authentication).

In the ISE authentication logs, the MAB authentication appears at the bottom of the log. Although it is unknown, the MAC address was authenticated and profiled, and the webauth attributes were returned. Next, authentication occurs with the user's login credentials (at the Login page). Immediately after authentication, a new Layer 2 authentication occurs with the username as credentials; this authentication step is where you can return attributes such dynamic VLAN.

HTTP Proxy Configuration

If you use an HTTP proxy for your clients, it means that your clients:

- Use a unconventional port for HTTP protocol.
- Send all their traffic to that proxy.

You can use the **ip http port** command and the **ip port-map http port** command to enable the router to listen to specific ports.

You also need to configure all clients to keep using their proxy but to not use the proxy for the ISE IP address. All browsers include a feature that allows you to enter host names or IP addresses that should not use the proxy. If you do not add the exception for the ISE, you encounter a loop authentication page.

You also need to modify your redirection ACL to permit on the proxy port.

Configuration Examples for CWA URL Redirect support on C891FW

Example: MAB Configuration

```
enable
Configure terminal
interface GigabitEthernet 4
 switchport access vlan 5
 no ip address
 authentication order mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 spanning-tree portfast
 end
```

Example: ACL Configuration

VLAN 100 is the VLAN that provides full network connectivity. A default port ACL (named webauth) is applied and defined as shown here:

```
ip access-list extended webauth
permit ip any any
```

This sample configuration gives full network access even if the user is not authenticated; therefore, you might want to restrict access to unauthenticated users.

In this following configuration, HTTP and HTTPS browsing does not work without authentication (per the other ACL) since ISE is configured to use a redirect ACL (named redirect).

```
ip access-list extended redirect
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <ISE ip address>
permit tcp any any eq www
permit tcp any any eq 443
```

This access list must be defined on the router in order to define on which traffic the router will perform the redirection. (It matches on permit.) In this example, any HTTP or HTTPS traffic that the client sends triggers a web redirection. This example also denies the ISE IP address so traffic to the ISE goes to the ISE and does not redirect in a loop. (In this scenario, deny does not block the traffic; it just does not redirect the traffic.) If you use unusual HTTP ports or a proxy, you can add other ports.

You can also allow HTTP access to some web sites and redirect other websites. For example, if you define in the ACL a permit for internal web servers only, clients could browse the web without authenticating but would encounter the redirect if they try to access an internal web server.

You must allow the CoA on the router since ISE cannot force the switch to re-authenticate the client. To allow CoA:

```
aaa server radius dynamic-author
     client <ISE ip address> server-key <radius shared secret>
```

You can use the **ip http server** command to redirect based on HTTP traffic and **ip http secure-server** command to redirect based on HTTPS traffic.

Example: Verifying user authentication

You can use the **show authentication session int <interface num>** command to check if the user is authenticated. The following example shows a sample output of the **show authentication session int <interface num>** command when the user is not authenticated.

```
Device#show auth sess int gi1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000f.b049.5c4b
           IP Address:  192.168.33.201
            User-Name:  00-0F-B0-49-5C-4B
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-myDACL-51519b43
     URL Redirect ACL:  redirect
         URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
                        sessionId=C0A82102000002D8489E0E84&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A82102000002D8489E0E84
      Acct Session ID:  0x000002FA
               Handle:  0xF60002D9

Runnable methods list:

       Method   State
       mab      Authc Success
```

Note Despite a successful MAB authentication, the redirect ACL is placed since the MAC address was not known by the ISE.

Example: Router Configuration

This section lists the full router configuration. Some unnecessary interfaces and command lines have been omitted; therefore, this sample configuration should be used for reference only and should not be copied.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname autonet-4
!
boot-start-marker
boot system flash:c800-universalk9-mz.SSA.156-2.24.T
boot system flash:c800-universalk9-mz.SSA.156-2.19.T
boot-end-marker
!
!
logging buffered 30000000
enable password lab
!
aaa new-model
!
!
aaa authentication login NO_LOGIN none
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
 client 20.0.0.1 server-key cisco123
!
aaa session-id common
ethernet lmi ce
!
!
!
!
!
!
!
!
device-sensor filter-list cdp list CDP_FILTER
 tlv name address-type
 tlv number 10
device-sensor filter-spec cdp include list CDP_FILTER
device-sensor accounting
device-sensor notify all-changes
ip auth-proxy inactivity-timer 5
ip admission inactivity-timer 5
ip admission name CWA_TEST consent inactivity-time 5 absolute-timer 10
!
!
!
!
!
!
!
!
!
!
!
!


!
!
!
!
```

```
no ip domain lookup
ip inspect WAAS flush-timeout 10
ip device tracking
ip cef
ipv6 unicast-routing
ipv6 cef
ntp max-associations 1000
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
license udi pid C892FSP-K9 sn FTX192680ZR
!
!
username CISCO privilege 0 password 0 cisco
!
redundancy
 notification-timer 120000
!
!
!
autonomic
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0
 no ip address
!
interface GigabitEthernet1
 switchport access vlan 3
 no ip address
!
interface GigabitEthernet2
 switchport access vlan 2
 no ip address
!
interface GigabitEthernet3
 switchport access vlan 4
 no ip address
!
interface GigabitEthernet4
 switchport access vlan 5
 no ip address
 authentication order mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 spanning-tree portfast
!
interface GigabitEthernet5
 no ip address
!
interface GigabitEthernet6
```

```
 switchport access vlan 6
 no ip address
!
interface GigabitEthernet7
 switchport access vlan 7
 no ip address
!
interface GigabitEthernet8
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet9
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Vlan1
 ip address 126.53.1.4 255.255.255.0
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan2
 no ip address
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan3
 no ip address
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan4
 no ip address
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan5
 ip address 10.0.0.4 255.255.255.0
!
interface Vlan6
 ip address 20.0.0.4 255.255.255.0
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan7
 ip address 30.0.0.4 255.255.255.0
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
ip default-gateway 126.53.1.254
ip forward-protocol nd
ip http server
no ip http secure-server
ip http max-connections 10
!
!
ip nat pool inside-pool-2 16.1.1.1 16.1.1.1 prefix-length 24
ip route 0.0.0.0 0.0.0.0 126.53.1.254
!
ip access-list extended redirect
 deny   ip any host 20.0.0.1
 permit tcp any any eq www
 permit tcp any any eq 443
!
ipv6 ioam timestamp
!
access-list 2 permit 60.1.1.0 0.0.0.255
access-list 2 permit 60.0.0.0 0.0.0.255
!
radius server host
 address ipv4 20.0.0.1 auth-port 1812 acct-port 1813
 key cisco123
!
!
!
control-plane
!
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 no modem enable
line aux 0
line vty 0 4
 length 0
 transport input all
!
scheduler allocate 20000 1000
```

```
!
end
```

Example: HTTP Proxy Configuration

The following example shows how to configure the proxy port to 8080:

```
enable
configure terminal
ip http port 8080
ip port-map http port 8080
```

Important Notes

Important Note about Router SVIs

The router needs a switch virtual interface (SVI) in order to reply to the client and send the web portal redirection to the client. This SVI does not necessarily have to be on the client subnet/VLAN. However, if the router has no SVI in the client subnet/VLAN, it has to use any of the other SVIs and send traffic as defined in the client routing table. This typically means traffic is sent to another gateway in the core of the network; this traffic comes back to the access switch inside the client subnet.

Firewalls typically block traffic from and to the same router, as in this scenario, so redirection might not work properly. You can allow this behavior on the firewall or create an SVI on the access router in the client subnet.

Important Note about HTTPS Redirection

Routers are able to redirect HTTPS traffic. If the guest client has a homepage in HTTPS, the redirection occurs correctly.

The whole concept of redirection is based upon the fact that a device (in this case, the router) replaces the website IP address. However, a major issue arises when the router intercepts and redirects HTTPS traffic because the router can present only its own certificate in the Transport Layer Security (TLS) handshake. Since this is not the same certificate as the website originally requested, most browsers issue major alerts. The browsers correctly handle the redirection and presentation of another certificate as a security concern. There is no solution for this, you cannot use the router to replace your original website certificate.

Additional References for CWA URL Redirect support on C891FW

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Technical Assistance

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

Feature Information for CWA URL Redirect support on C891FW

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

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

Table 16: Feature Information for CWA URL Redirect support on C891FW

Feature Name	Releases	Feature Information
CWA URL Redirect support on C891FW	15.6(3)M	CWA URL Redirect support on C891FW feature enables you to manage Central Web Authentication (CWA) URL redirects to Identity Services Engine (ISE) or other websites. No commands were introduced or modified by this feature.

CHAPTER 4

Message Banners for AAA Authentication

The Message Banners for AAA authentication feature is used to configure personalized login and failed-login banners for user authentication. The message banners are displayed when a user logs in to the system to be authenticated using authentication, authorization, and accounting (AAA) and when an authentication fails.

- Finding Feature Information, page 99
- Information About Message Banners for AAA Authentication, page 99
- How to Configure Message Banners for AAA Authentication, page 100
- Configuration Examples for Message Banners for AAA Authentication, page 102
- Additional References for Message Banners for AAA Authentication, page 103
- Feature Information for Message Banners for AAA Authentication, page 104

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 Message Banners for AAA Authentication

Login and Failed-Login Banners for AAA Authentication

Login and failed-login banners use a delimiting character that notifies the system of the exact text string that must be displayed as the banner for authorization, authentication, and accounting (AAA) authentication. The delimiting character is repeated at the end of the text string to signify the end of the login or failed-login banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string for the banner.

You can display a maximum of 2996 characters in a login or failed-login banner.

How to Configure Message Banners for AAA Authentication

Configuring a Login Banner for AAA Authentication

Perform this task to configure a banner that is displayed when a user logs in (replacing the default message for login). Use the **no aaa authentication banner** command to disable a login banner.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **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)# aaa new-model`	Enables AAA globally.

Step 4	**aaa authentication banner** *delimiter-string delimiter*
	Example:
	`Device(config)# aaa authentication banner`
	`*Unauthorized Access Prohibited*`
		Creates a personalized login banner.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring a Failed-Login Banner for AAA Authentication

Perform this task to configure a failed-login banner that is displayed when a user login fails (replacing the default message for failed login). Use the **no aaa authentication fail-message** command to disable a failed-login banner.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **aaa authentication fail-message** *delimiter-string delimiter*
6. **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)# aaa new-model`	Enters AAA globally.

	Command or Action	Purpose
Step 4	**aaa authentication banner** *delimiter-string delimiter* **Example:** `Device(config)# aaa authentication banner *Unauthorized Access Prohibited*`	Creates a personalized login banner.
Step 5	**aaa authentication fail-message** *delimiter-string delimiter* **Example:** `Device(config)# aaa authentication fail-message *Failed login. Try again*`	Creates a message to be displayed when a user login fails.

Step 6	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuration Examples for Message Banners for AAA Authentication

Example: Configuring Login and Failed-Login Banners for AAA Authentication

The following example shows how to configure a login banner that is displayed when a user logs in to the system, (in this case, the phrase “Unauthorized Access Prohibited”). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

This configuration displays the following login banner:

```
Unauthorized Access Prohibited
Username:
```

The following example shows how to configure a failed-login banner that is displayed when a user tries to log in to the system and fails, (in this case, the phrase “Failed login. Try again”). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

This configuration displays the following login and failed-login banner:

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

Additional References for Message Banners for AAA Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
Configuring AAA	*Authentication, Authorization, and Accounting 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 Message Banners for AAA Authentication

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

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

Table 17: Feature Information for Message Banners for AAA Authentication

Feature Name	Releases	Feature Information
Message Banners for AAA Authentication	11.3(4)T 12.2(27)SBA 12.2(33)SRC 15.3(1)S	The Message Banners for AAA Authentication feature enables you to configure personalized login and failed-login banners for user authentication. The message banners are displayed when a user logs in to the system to be authenticated using authentication, authorization, and accounting (AAA) and when an authentication fails. The following commands were introduced or modified: **aaa authentication banner**, **aaa authentication fail-message**, **aaa new-model**.

CHAPTER 5

AAA-Domain Stripping at Server Group Level

The AAA-Domain Stripping at Server Group Level feature allows domain stripping to be configured at the server group level.

- Finding Feature Information, page 105
- Information About AAA-Domain Stripping at Server Group Level, page 105
- How to Configure AAA-Domain Stripping at Server Level Group, page 106
- Configuration Example for AAA-Domain Stripping at Server Group Level, page 107
- Additional References, page 107
- Feature Information for AAA-Domain Stripping at Server Group Level, page 109

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 AAA-Domain Stripping at Server Group Level

You can remove the domain name from the username received at the global level by using the **radius-server domain-stripping** command. When the **radius-server domain-stripping** command is configured, all the AAA requests with “user@example.com” go to the remote RADIUS server with the reformatted username “user”. The domain name is removed from the request.

Note Domain stripping will not be done in a TACACS configuration.

The AAA Broadcast Accounting feature allows accounting information to be sent to multiple AAA servers at the same time, that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows you to send accounting information to private and public AAA servers. It also provides redundant billing information for voice applications.

You can configure domain stripping at the server group level by using the **domain-stripping** command in server group RADIUS configuration mode. Per-server group configuration overrides the global configuration. If domain stripping is not enabled globally, but it is enabled in a server group, then it is enabled only for that server group. Also, if virtual routing and forwarding (VRF)-specific domain stripping is configured globally and in a server group for a different VRF, domain stripping is enabled in both the VRFs. VRF configurations are taken from server-group configuration mode. If server-group configurations are disabled in global configuration mode but are available in server-group configuration mode, all configurations in server-group configuration mode are applicable.

After the domain stripping and broadcast accounting are configured, you can create separate accounting records as per the configurations.

How to Configure AAA-Domain Stripping at Server Level Group

Configuring Domain Stripping at the Server Group Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *server-name*
5. **domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]
6. **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.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa group server radius** *server-name* **Example:** `Device(config)# aaa group server radius rad1`	Adds the RADIUS server and enters server group RADIUS configuration mode. • The *server-name* argument specifies the RADIUS server group name.
Step 5	**domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*] **Example:** `Device(config-sg-radius)# domain-stripping delimiter username@example.com`	Configures domain stripping at the server group level.

Step 6	**end**
	Example:
	`Device(config-sg-radius)# end`
		Exits server group RADIUS configuration mode and returns to the privileged EXEC mode.

Configuration Example for AAA-Domain Stripping at Server Group Level

Example: AAA-Domain Stripping at Server Group Level

The following example shows the domain stripping configuration at the server group level:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# domain-stripping right-to-left delimiter @$/
Device(config-sg-radius)# end
```

Additional References

The following sections provide references related to the Configuring Authentication feature.

Related Documents

Related Topic	Document Title
Authorization	Configuring Authorization in the *Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2.
Accounting	Configuring Accounting in the *Cisco IOS XE Security Configuration Guide: Securing User Service* , Release 2.
Security commands	*Cisco IOS Security 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 XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1334	PPP Authentication Protocols
RFC 2433	Microsoft PPP CHAP Extensions
RFC 2903	*Generic AAA Architecture*
RFC 2904	*AAA Authorization Framework*
RFC 2906	*AAA Authorization Requirements*
RFC 2989	*Criteria for Evaluating AAA Protocols for Network Access*

Technical Assistance

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

Feature Information for AAA-Domain Stripping at Server Group Level

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

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

Table 18: Feature Information for AAA-Domain Stripping at Server Group Level

Feature Name	Releases	Feature Information
AAA-Domain Stripping at Server Group Level	15.1(1)SY	The AAA-Domain Stripping at Server Group Level feature allows domain stripping to be configured at the server group level. The following command was introduced: **domain-stripping**.

CHAPTER 6

AAA Double Authentication Secured by Absolute Timeout

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

- Finding Feature Information, page 111
- Prerequisites for AAA Double Authentication Secured by Absolute Timeout, page 112
- Restrictions for AAA Double Authentication Secured by Absolute Timeout, page 112
- Information About AAA Double Authentication Secured by Absolute Timeout, page 112
- How to Apply AAA Double Authentication Secured by Absolute Timeout, page 113
- Configuration Examples for AAA Double Authentication Secured by Absolute Timeout, page 116
- Additional References, page 118
- Feature Information for AAA Double Authentication Secured by Absolute Timeout, page 120

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 AAA Double Authentication Secured by Absolute Timeout

- You need access to a Cisco RADIUS or TACACS+ server and should be familiar with configuring RADIUS or TACACS+.
- You should be familiar with configuring authentication, authorization, and accounting (AAA) and enabling AAA automated double authentication.

Restrictions for AAA Double Authentication Secured by Absolute Timeout

- The AAA Double Authentication Secured by Absolute Timeout feature is for PPP connections only. Automated double authentication cannot be used with other protocols, such as X.25 or Serial Line Internet Protocol (SLIP).
- There may be a minimal impact on performance if a TACACS+ server is used. However, there is no performance impact if a RADIUS server is used.

Information About AAA Double Authentication Secured by Absolute Timeout

AAA Double Authentication

Use the AAA double authentication mechanism to pass the first authentication using a host username and password. The second authentication, after the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) authentication, uses a login username and password. In the first authentication, a PPP session timeout is applied to the virtual access interface if it is configured locally or remotely.

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. The per-user session timeout, which can be customized, supersedes the generic absolute timeout value. This method works on the same principle as per-user access control lists (ACLs) in double authentication.

How to Apply AAA Double Authentication Secured by Absolute Timeout

Applying AAA Double Authentication Secured by Absolute Timeout

To apply the absolute timeout, you must configure session-timeout in the login user profile as a link control protocol (LCP) per-user attribute. Use the **access-profile** command to enable AAA double authentication. This command is used to apply your per-user authorization attributes to an interface during a PPP session. Before you use the **access-profile** command, you must first reauthorize LCP per-user attributes (for example, Session-Timeout) and then reauthorize Network Control Protocols (NCPs) to apply other necessary criteria, such as ACLs and routes. See the section "Examples for AAA Double Authentication Secured by Absolute Timeout."

Note The Timeout configuration in a TACACS+ user profile is different from the configuration in a RADIUS user profile. In a RADIUS profile, only one session-timeout is configured, along with the autocommand **access-profile**. The timeout is applied to the EXEC session and to the PPP session respectively. In TACACS+, however, the timeout must be configured under the service types "exec" and "ppp" (LCP) to apply a timeout to the EXEC session and to the PPP session. If the timeout is configured only under the service type "ppp," the timeout value will not be available during an EXEC authorization, and the timeout will not be applied to the EXEC session.

Verifying AAA Double Authentication Secured by Absolute Timeout

To verify that AAA double authentication has been secured by absolute timeout and to see information about various attributes associated with the authentication, perform the following steps. These **show** and **debug** commands can be used in any order.

Note If idle timeout is configured on a full virtual access interface and a subvirtual access interface, the **show users** command displays the idle time for both interfaces. However, if the idle timeout is not configured on both interfaces, the **show users** command will display the idle time for the full virtual access interface only.

SUMMARY STEPS

1. **enable**
2. **show users**
3. **show interfaces virtual-access** *number* [**configuration**]
4. **debug aaa authentication**
5. **debug aaa authorization**
6. **debug aaa per-user**
7. **debug ppp authentication**
8. Enter one of the following:
   - **debug radius**
     or
     debug tacacs

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show users** **Example:** `Device# show users`	Displays information about active lines on the device.
Step 3	**show interfaces virtual-access** *number* [**configuration**] **Example:** `Device# show interfaces virtual-access 2 configuration`	Displays status, traffic data, and configuration information about a specified virtual access interface.
Step 4	**debug aaa authentication** **Example:** `Device# debug aaa authentication`	Displays information about AAA TACACS+ authentication.
Step 5	**debug aaa authorization** **Example:** `Device# debug aaa authorization`	Displays information about AAA TACACS+ authorization.

	Command or Action	Purpose
Step 6	**debug aaa per-user** **Example:** `Device# debug aaa per-user`	Displays the attributes that are applied to each user as the user gets authenticated.
Step 7	**debug ppp authentication** **Example:** `Device# debug ppp authentication`	Displays whether a user is passing authentication.

Step 8	Enter one of the following:
	• **debug radius** or
	debug tacacs
	Example:
	`Device# debug radius`
	Example:
	`Device# debug tacacs`
		Displays the debug information associated with the RADIUS server.
		or
		Displays the debug information associated with the TACACS+ server.

Examples

The following sample output is from the **show users** command:

```
Device# show users

     Line       User        Host(s      Idle       Location
  *  0 con 0    aaapbx2     idle        00:00:00   aaacon2 10
     8 vty 0    broker_def  idle        00:00:08   192.168.1.8
     Interface  User            Mode        Idle       Peer Address
     Vi2        broker_default  VDP         00:00:01   192.168.1.8 <=========
     Se0:22     aaapbx2         Sync PPP    00:00:23
```

The following sample output is from the **show interfaces virtual-access** command:

```
Device# show interfaces virtual-access 2 configuration

Virtual-Access2 is a Virtual Profile (sub)interface
Derived configuration: 150 bytes
!
interface Virtual-Access2
  ip unnumbered Serial0:23
  no ip route-cache
  timeout absolute 3 0
! The above line shows that the per-user session timeout has been applied.
  ppp authentication chap
  ppp timeout idle 180000
! The above line shows that the absolute timeout has been applied.
```

Configuration Examples for AAA Double Authentication Secured by Absolute Timeout

Example: RADIUS User Profile

The following sample output shows that a RADIUS user profile has been applied and that AAA double authentication has been secured by an absolute timeout:

```
aaapbx2 Password = "password1",
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Session-Timeout = 180,
 Idle-Timeout = 180000,
 cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_default Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_merge Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile merge",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
broker_replace Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile replace",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

Example: TACACS User Profile

The following sample output shows that a TACACS+ user profile has been applied and that AAA double authentication has been secured by an absolute timeout.

Remote Host Authentication

The following example shows how to allow the remote host to be authenticated by the local host during the first-stage authentication and provides the remote host authorization profile.

```
user = aaapbx2
 chap = cleartext Cisco
 pap = cleartext cisco
 login = cleartext cisco
 service = ppp protocol = lcp
  idletime = 3000
  timeout = 3
 service = ppp protocol = ip
  inacl#1="permit tcp any any eq telnet"
 service = ppp protocol = ipx
```

Using the access-profile Command Without Any Arguments

Using the **access-profile** command without any arguments causes the removal of any access lists that are found in the old configuration (both per-user and per-interface) and ensures that the new profile contains only access-list definitions.

```
user = broker_default
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile"
! This is the autocommand that executes when broker_default logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  inacl#1="permit tcp any any"
  inacl#2="permit icmp host 10.0.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

Using the access-profile Command with the merge Keyword

The **merge** keyword in the **access-profile** command is used to remove all old access lists, and any attribute-value (AV) pair is allowed to be uploaded and installed. The use of the **merge** keyword will allow for the uploading of any custom static routes, Service Advertisement Protocol (SAP) filters, and other requirements that users may need in their profiles. Configure the **merge** keyword with care because it leaves everything open in terms of conflicting configurations.

```
user = broker_merge
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
  timeout = 6
 service = ppp protocol = lcp
 timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.4.0.0 255.0.0.0"
  route#2="10.5.0.0 255.0.0.0"
  route#3="10.6.0.0 255.0.0.0"
  inacl#5="permit tcp any any"
  inacl#6="permit icmp host 10.60.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

Using the access-profile Command with the replace Keyword

If you use the **access-profile** command with the **replace** keyword, any old configurations are removed and a new configuration is installed.

Note When the **access-profile** command is configured, the new configuration is checked for address pools and address-AV pairs. Because addresses cannot be renegotiated at this point, the command will fail to work when it encounters such an address-AV pair.

```
user = broker_replace
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.7.0.0 255.0.0.0"
  route#2="10.8.0.0 255.0.0.0"
  route#3="10.9.0.0 255.0.0.0"
  inacl#4="permit tcp any any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

Note The Timeout configuration in a TACACS+ user profile is different from the configuration in a RADIUS user profile. In a RADIUS profile, only one session-timeout is configured, along with the autocommand **access-profile**. The timeout will be applied to the EXEC session and to the PPP session. In the TACACS+ user profile, however, the timeout must be configured under the service types “exec” and “ppp” (LCP) to apply a timeout to the EXEC session and to the PPP session respectively. If the timeout is configured only under the service type “ppp,” the timeout value will not be available during an EXEC authorization, and the timeout will not be applied to the EXEC session.

Additional References

The following sections provide references related to AAA Double Authentication Secured by Absolute Timeout.

Related Documents

Related Topic	Document Title
AAA	Configuring Authentication feature module.
	Configuring Authorization feature module.
	Configuring Accounting feature module.
RADIUS	Configuring RADIUS feature module.
TACACS+	Configuring TACACS+ feature module
Security Commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

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

Feature Information for AAA Double Authentication Secured by Absolute Timeout

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

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

Table 19: Feature Information for AAA Double Authentication Secured by Absolute Timeout

Feature Name	Releases	Feature Information
AAA Double Authentication Secured by Absolute Timeout	Cisco IOS 12.3(7)T Cisco IOS 12.2(28)SB	The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

CHAPTER 7

Login Password Retry Lockout

The Login Password Retry Lockout feature allows system administrators to lock out a local authentication, authorization, and accounting (AAA) user account after a configured number of unsuccessful attempts by the user to log in.

- Finding Feature Information, page 121
- Prerequisites for Login Password Retry Lockout, page 121
- Restrictions for Login Password Retry Lockout, page 122
- Information About Login Password Retry Lockout, page 122
- How to Configure Login Password Retry Lockout, page 122
- Configuration Examples for Login Password Retry Lockout, page 126
- Additional References, page 127
- Feature Information for Login Password Retry Lockout, page 128
- Glossary, page 129

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 Login Password Retry Lockout

- You must be running a Cisco IOS image that contains the AAA component.

Restrictions for Login Password Retry Lockout

- Authorized users can lock themselves out because there is no distinction between an attacker who is guessing passwords and an authorized user who is entering the password incorrectly multiple times.
- A denial of service (DoS) attack is possible; that is, an authorized user could be locked out by an attacker if the username of the authorized user is known to the attacker.

Information About Login Password Retry Lockout

Lock Out of a Local AAA User Account

The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in using the username that corresponds to the AAA user account. A locked-out user cannot successfully log in again until the user account is unlocked by the administrator.

A system message is generated when a user is either locked by the system or unlocked by the system administrator. The following is an example of such a system message:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

The system administrator cannot be locked out.

Note The system administrator is a special user who has been configured using the maximum privilege level (root privilege--level 15). A user who has been configured using a lesser privilege level can change the privilege level using the **enable** command. A user that can change to the root privilege (level 15) is able to act as a system administrator.

This feature is applicable to any login authentication method, such as ASCII, Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP).

Note No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

How to Configure Login Password Retry Lockout

Configuring Login Password Retry Lockout

To configure the Login Password Retry Lockout feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **password** *encryption-type password*
4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default method**

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	**username** *name* [**privilege** *level*] **password** *encryption-type password* **Example:** `Device(config)# username user1 privilege 15 password 0 cisco`	Establishes a username-based authentication system.
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.
Step 5	**aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts* **Example:** `Device(config)# aaa local authentication attempts max-fail 3`	Specifies the maximum number of unsuccessful attempts before a user is locked out.

	Command or Action	Purpose
Step 6	**aaa authentication login default** **method** **Example:** `Device(config)# aaa authentication login default local`	Sets the authentication, authorization, and accounting (AAA) authentication method at login. For example, **aaa authentication login default** *local* specifies the local AAA user database.

Unlocking a Login Locked-Out User

To unlock a login locked-out user, perform the following steps.

Note This task can be performed only by users having the root privilege (level 15).

SUMMARY STEPS

1. **enable**
2. **clear aaa local user lockout** {**username** *username* | **all**}

DETAILED STEPS

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

Step 2	**clear aaa local user lockout** {**username** *username*	**all**}
		Example:
		`Device# clear aaa local user lockout username user1`
			Unlocks a locked-out user.

Clearing the Unsuccessful Login Attempts of a User

This task is useful for cases in which the user configuration was changed and the unsuccessful login attempts of a user that are already logged must be cleared.

To clear the unsuccessful login attempts of a user that have already been logged, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear aaa local user fail-attempts** {**username** *username* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear aaa local user fail-attempts** {**username** *username* | **all**} **Example:** `Device# clear aaa local user fail-attempts username user1`	Clears the unsuccessful attempts of the user. • This command is useful for cases in which the user configuration was changed and the unsuccessful attempts that are already logged must be cleared.

Monitoring and Maintaining Login Password Retry Lockout Status

To monitor and maintain the status of the Login Password Retry Lockout configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show aaa local user lockout**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**show aaa local user lockout** **Example:** `Device# show aaa local user lockout`	Displays a list of the locked-out users for the current login password retry lockout configuration.

Example

The following output shows that user1 is locked out:

```
Device# show aaa local user lockout
           Local-user          Lock time
           user1               04:28:49 UTC Sat Jun 19 2004
```

Configuration Examples for Login Password Retry Lockout

Displaying the Login Password Retry Lockout Configuration Example

The following **show running-config** command output illustrates that the maximum number of failed user attempts has been set for 2 as the login password retry lockout configuration:

```
Device # show running-config
Building configuration...
Current configuration : 1214 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC-2
!
boot-start-marker
boot-end-marker
!
!
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
```

Additional References

The following sections provide references related to Login Password Retry Lockout.

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

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

Feature Information for Login Password Retry Lockout

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 20: Feature Information for Login Password Retry Lockout

Feature Name	Releases	Feature Information
Login Password Retry Lockout	Cisco IOS 12.3(14)T Cisco IOS 12.2(33)SRE	The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in. This feature was introduced in Cisco IOS Release 12.3(14)T. This feature was integrated into Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **aaa local authentication attempts max-fail**, **clear aaa local user fail-attempts**, **clear aaa local user lockout**.

Glossary

- **local AAA method** --Method by which it is possible to configure a local user database on a router and to have AAA provision authentication or authorization of users from this database.
- **local AAA user** --User who is authenticated using the local AAA method.

CHAPTER 8

Throttling of AAA RADIUS Records

The Throttling of AAA (RADIUS) Records feature supports throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. This feature allows a user to configure the appropriate throttling rate to avoid network congestion and instability; such as when there is insufficient bandwidth to accommodate a sudden burst of records generated from the router to the RADIUS server.

- Finding Feature Information, page 131
- Information About Throttling of AAA RADIUS Records, page 131
- How to Configure Throttling of AAA RADIUS Records, page 132
- Configuration Examples for Throttling of AAA RADIUS Records, page 135
- Additional References, page 136
- Feature Information for Throttling of AAA RADIUS Records, page 137

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 Throttling of AAA RADIUS Records

Benefits of the Throttling of AAA RADIUS Records Feature

A Network Access Server (NAS), acting as RADIUS client, can generate a burst of accounting or access requests, causing severe network congestion or causing the RADIUS server to become overloaded with a burst of RADIUS traffic. This problem could be compounded when multiple NASs interact with the RADIUS servers.

The following conditions can trigger a sudden burst of RADIUS traffic:

- An interface flap, which in turn brings down all the subscriber sessions and generates accounting requests for each subscriber.
- The High Availability (HA) program generating a START record for every session that survived a switchover, such as the scenario described the preceding bullet.

A large number of generated requests can make the network unstable if there is insufficient bandwidth or if the RADIUS server is slow to respond. Neither the User Datagram Protocol (UDP) transport layer nor the RADIUS protocol has a flow control mechanism. The throttling mechanism provided by this feature provides a solution for these issues.

Throttling Access Requests and Accounting Records

The Throttling of AAA (RADIUS) Records feature introduces a mechanism to control packets (flow control) at the NAS level, which improves the RADIUS server performance.

Because of their specific uses, access requests and accounting records must be treated separately. Access request packets are time sensitive, while accounting record packets are not.

- If a response to an access request is not returned to the client in a timely manner, the protocol or the user will time out, impacting the device transmission rates.
- Accounting records packets are not real-time critical.

When configuring threshold values on the same server, it is important to prioritize threshold values for the handling of the time-sensitive access request packets and to place a lesser threshold value on the accounting records packets.

In some cases, when an Internet Service Provider (ISP) is using separate RADIUS servers for access requests and accounting records, only accounting records throttling may be required.

- The Throttling of AAA (RADIUS) Records is disabled, by default.
- Throttling functionality can be configured globally or at server group level.

How to Configure Throttling of AAA RADIUS Records

This section describes how to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server for both, global and server groups.

Server-group configurations are used to enable or disable throttling for a particular server group and to specify the threshold value for that server group.

Note Server-group configurations override any configured global configurations.

Throttling Accounting and Access Request Packets Globally

To globally configure the throttling of accounting and access request packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server throttle** { [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
4. **exit**

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	**radius-server throttle** { [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
	Example:
	`Device(config)# radius-server throttle accounting 100 access 200 access-timeout 2`
		Configures global throttling for accounting and access request packets.
		For this example:
		• The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200.
		Note The default threshold value is 0 (throttling disabled).
		• The number of timeouts per transaction value (the range is 1-10) is set to 2.

Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Throttling Accounting and Access Request Packets Per Server Group

The following server-group configuration can be used to enable or disable throttling for a specified server group and to specify the threshold value for that server group.

To configure throttling of server-group accounting and access request packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-group-name*
4. **throttle** {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
5. **exit**

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 group server radius** *server-group-name* **Example:** `Device(config)# aaa group server radius myservergroup`	Enters server-group configuration mode.

Step 4	**throttle** {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
	Example:
	`Device(config-sg-radius)# throttle accounting 100 access 200 access-timeout 2`
		Configures the specified server-group throttling values for accounting and access request packets.
		For this example:
		• The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200.
		Note The default threshold value is 0 (throttling disabled).
		• The number of time-outs per transaction value (the range is 1-10) is set to 2.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-sg-radius)# exit`	Exits server-group configuration mode.

Configuration Examples for Throttling of AAA RADIUS Records

Throttling Accounting and Access Request Packets Globally Example

The following example shows how to limit the number of accounting requests sent to a server to 100:

```
enable
configure terminal
radius-server throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to a server to 200 and sets the number of time-outs allowed per transactions to 2:

```
enable
configure terminal
radius-server throttle access 200
radius-server throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets:

```
enable
configure terminal
radius-server throttle accounting 100 access 200
```

Throttling Accounting and Access Request Packets Per Server Group Example

The following example shows how to limit the number of accounting requests sent to server-group-A to 100:

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to server-group-A to 200 and sets the number of time-outs allowed per transactions to 2:

```
enable
configure terminal
aaa group server radius server-group-A
throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets for server-group-A:

```
enable
configure terminal
```

```
aaa group server radius server-group-A
throttle accounting 100 access 200
```

Additional References

The following sections provide references related to the Throttling of AAA (RADIUS) Records feature.

Related Documents

Related Topic	Document Title
AAA and RADIUS	*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0.

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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for Throttling of AAA RADIUS Records

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 Throttling of AAA (RADIUS) Records

Feature Name	Releases	Feature Information
Throttling of AAA (RADIUS) Records	12.2(33)SRC 12.4(20)T	The Throttling of AAA (RADIUS) Records feature supports throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. This feature allows a user to configure the appropriate throttling rate to avoid network congestion and instability; such as when there is insufficient bandwidth to accommodate a sudden burst of records generated from the Cisco IOS router to the RADIUS server. In Release 12.2(33)SRC, this feature was introduced on the Cisco 7200 and Cisco 7200 routers. The following commands were introduced or modified by this feature: **radius-server throttle, throttle**

CHAPTER 9

MSCHAP Version 2

The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS).

For Cisco IOS Release 12.4(6)T, MSCHAP V2 now supports a new feature: AAA Support for MSCHAPv2 Password Aging. Prior to Cisco IOS Release 12.4(6)T, when Password Authentication Protocol (PAP)-based clients sent username and password values to the authentication, authorization, and accounting (AAA) subsystem, AAA generated an authentication request to the RADIUS server. If the password expired, the RADIUS server replied with an authentication failure message. The reason for the authentication failure was not passed back to AAA subsystem; thus, users were denied access because of authentication failure but were not informed why they were denied access.

The Password Aging feature, available in Cisco IOS Release 12.4(6)T, notifies crypto-based clients that the password has expired and provides a generic way for the user to change the password. The Password Aging feature supports only crypto-based clients.

- Finding Feature Information, page 139
- Prerequisites for MSCHAP Version 2, page 140
- Restrictions for MSCHAP Version 2, page 140
- Information About MSCHAP Version 2, page 140
- How to Configure MSCHAP Version 2, page 141
- Configuration Examples, page 142
- Additional References, page 143
- Feature Information for MSCHAP Version 2, page 145

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 MSCHAP Version 2

- Configure an interface type and enter interface configuration mode by using the **interface** command.
- Configure the interface for PPP encapsulation by using the **encapsulation** command.
- Be sure that the client operating system supports all MSCHAP V2 capabilities.
- For Cisco IOS Release 12.4(6)T, the Password Aging feature only supports RADIUS authentication for crypto-based clients.
- To ensure that the MSCHAP Version 2 features correctly interpret the authentication failure attributes sent by the RADIUS server, you must configure the **ppp max-bad-auth** command and set the number of authentication retries at two or more.

In addition, the **radius server vsa send authentication** command must be configured, allowing the RADIUS client to send a vendor-specific attribute to the RADIUS server. The Change Password feature is supported only for RADIUS authentication.

- The Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows NT operating systems have a known caveat that prevents the Change Password feature from working. You must download a patch from Microsoft at the following URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770

For more information on completing these tasks, see the section “PPP Configuration ” in the *Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T. The RADIUS server must be configured for authentication. Refer to vendor-specific documentation for information on configuring RADIUS authentication on the RADIUS server.

Restrictions for MSCHAP Version 2

- MSCHAP V2 authentication is not compatible with MSCHAP V1 authentication.
- The change password option is supported only for RADIUS authentication and is not available for local authentication.

Information About MSCHAP Version 2

MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Cisco routers that support this authentication method enable Microsoft Windows 2000 operating system users to establish remote PPP sessions without configuring an authentication method on the client.

MSCHAP V2 authentication introduced an additional feature not available with MSCHAP V1 or standard CHAP authentication: the Change Password feature. This features allows the client to change the account password if the RADIUS server reports that the password has expired.

Note MSCHAP V2 authentication is an updated version of MSCHAP that is similar to but incompatible with MSCHAP Version 1 (V1). MSCHAP V2 introduces mutual authentication between peers and a Change Password feature.

How to Configure MSCHAP Version 2

Configuring Password Aging for Crypto-Based Clients

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login**command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login**command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

After the RADIUS server requests a new password, AAA queries the crypto client, which in turn prompts the user to enter a new password.

To configure login authentication and password aging for crypto-based clients, use the following commands beginning in global configuration mode.

Note The AAA Password Expiry infrastructure notifies the Easy VPN client that the password has expired and provides a generic way for the user to change the password. Please use RADIUS-server domain-stripping feature wisely in combination with AAA password expiry support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*]
5. **crypto map** *map-name* **client authentication list** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • 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 AAA globally.
Step 4	**aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*] **Example:** `Device(config)# aaa authentication login userauthen passwd-expiry group radius`	Enables password aging for crypto-based clients on a local authentication list.
Step 5	**crypto map** *map-name* **client authentication list** *list-name* **Example:** **Example:** `Device(config)# crypto map clientmap client authentication list userauthen`	Configures user authentication (a list of authentication methods) on an existing crypto map.

Configuration Examples

Configuring Local Authentication Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

Configuring RADIUS Authentication Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

Configuring Password Aging with Crypto Authentication Example

The following example configures password aging by using AAA with a crypto-based client:

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group 3000client
 key cisco123
 dns 10.1.1.10
 wins 10.1.1.20
 domain cisco.com
 pool ippool
 acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
!
end
```

Additional References

The following sections provide references related to the MSCHAP Version 2 feature.

Related Documents

Related Topic	Document Title
Configuring PPP interfaces	PPP Configuration in the *Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T.
Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices	*Cisco IOS Dial Technologies Command Reference*
Lists of IOS Security Commands	*Cisco IOS Security Command Reference*
Configuring PPP authentication using AAA	Configuring PPP Authentication Using AAA in the Configuring Authentication module in the *Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T.
Configuring RADIUS Authentication	Configuring RADIUS module in the *Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T.

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
RFC 1661	*Point-to-Point Protocol (PPP)*
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*
RFC 2759	*Microsoft PPP CHAP Extensions, Version 2*

Technical Assistance

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

Feature Information for MSCHAP Version 2

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 MSCHAP Version 2

Feature Name	Releases	Feature Information
MSCHAP Version 2	12.2(2)XB5 12.2(13)T 12.4(6)T	The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS). In 12.2(2)XB5, this feature was introduced. In 12.2(13)T, this feature was integrated into Cisco IOS Release 12.2(13)T. In 12.4(6)T, this feature was updated to include the crypto-based Password Aging feature. The following commands were introduced or modified: **aaa authentication login**, and **ppp authentication ms-chap-v2.**

CHAPTER 10

Define Interface Policy-Map AV Pairs AAA

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco RADIUS vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level.

The Define Interface Policy-Map AV Pairs AAA has the following benefits:

- The ability to apply QoS policies transparently as required without the disruption of session reauthentication provides a high degree of flexibility, smaller configuration files, and more efficient usage of queuing resources. This ability eliminated the need to pre-provision subscribers.
- The ability to modify the applied policy map as needed without session disruption (session dropped and reauthenticated) is an advantage to service providers.
- Nondisruptive support for special event triggers is essential to support new dynamic bandwidth services such as pre-paid and turbo button services.

The QoS policy map is used to define the subscriber user experience for broadband service and can facilitate delivery of higher value services such as VoIP and video.

- Finding Feature Information, page 148
- Prerequisites for Define Interface Policy-Map AV Pairs AAA, page 148
- Restrictions for Define Interface Policy-Map AV Pairs AAA, page 148
- Information About Define Interface Policy-Map AV Pairs AAA, page 148
- How to Configure Define Interface Policy-Map AV Pairs AAA, page 151
- Configuration Examples for Define Interface Policy-Map AV Pairs AAA, page 158
- Additional References, page 162
- Feature Information for Define Interface Policy-Map AV Pairs AAA, page 164

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 Define Interface Policy-Map AV Pairs AAA

- Authentication, Authorization, and Accounting (AAA) must be enabled and already set up to use RADIUS.
- Configuring a service policy on the ATM subinterface requires enabling Dynamic Bandwidth Selection (DBS) on the VC.

Restrictions for Define Interface Policy-Map AV Pairs AAA

For the Cisco 7000 series routers:

- Only the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters are supported for this feature.

For the Cisco 10000 series routers:

- You cannot configure a service policy on a VC and on a session at the same time.
- All ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, are supported for this feature.

Information About Define Interface Policy-Map AV Pairs AAA

Dynamically Applying and Modifying a Policy Map

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco VSAs that allow you to dynamically apply a policy map and modify a policy map applied to a session, without session reauthentication, at the ATM VC level using RADIUS. The purpose of the Cisco VSA (attribute 26) is to communicate vendor-specific information between the network access server (NAS) and the RADIUS server. The Cisco VSA encapsulates vendor-specific attributes that allow vendors such as Cisco to support their own extended attributes.

The Define Interface Policy-Map AV Pairs AAA feature allows the two new Cisco VSAs to be installed on an ATM VC after a PPPoA or PPPoEoA session establishment. Using RADIUS, this feature allows a policy map to be applied ("pulled") and then modified by specific events ("pushed" by the policy server) while that session remains active.

Previously, a policy map could only be configured on a VC or ATM point-to-point subinterface by using the modular QoS CLI (MQC) or manually with the virtual template. Also previously, a service policy on a VC could be modified in the session but that session was dropped and reauthenticated. Currently for a PPPoA or PPPoEoA session, the pull part of the feature uses RADIUS to dynamically apply policy maps on an ATM VC and eliminates the need to statically configure a policy map on each VC. After a policy map is applied directly on the interface, certain events can signal the policy server to push a policy map onto a specific VC without the need for session reauthentication.

Note Configuring a service policy on the ATM subinterface still requires MQC configuration.

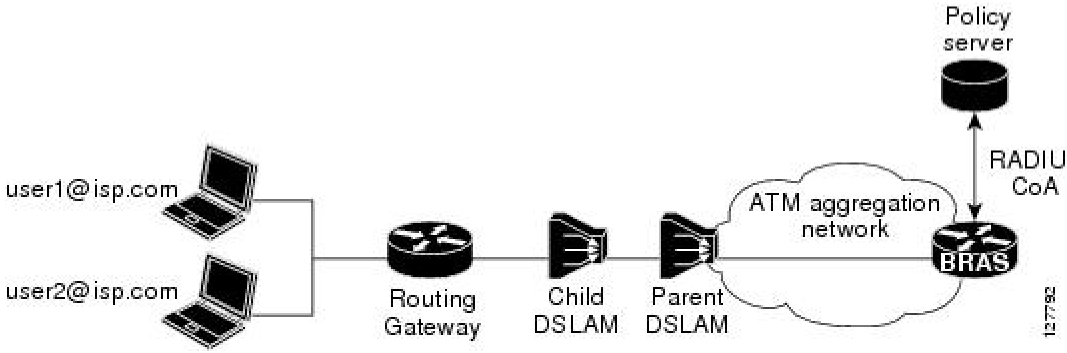
Two new Cisco AV pairs for service policy are set up in the user file on the RADIUS server. When the router requests the policy map name, the policy map name in the user file is pulled to the VC on the router when the PPPoA or PPPoEoA session is established. The Cisco AV pairs identify a "service policy-output" and "service policy-input" to identify QoS policies configured on the router from a RADIUS server. The Cisco AV pairs apply the appropriate policy map directly on the interface. Service policies are only applied at this time when the subscriber first authenticates the VC.

The "push" functionality of the feature allows you to modify an existing QoS profile (a policy map) applied to a session while that session remains active, thus allowing QoS policies to be applied as required without session reauthentication disruption. Specific events, including time-of-day, byte count, and user request, can signal the policy server to push a policy map onto a specific VC.

The policy server has the ability to send a Change of Authorization (CoA), which is the ability to change authorization of active sessions on the fly. The push functionality requires that CoA is enabled on the AAA server. One of the session attributes CoA pushes is the policy map, in an input and output direction.

The figure below shows that a CoA request is sent from the policy server to a broadband rate access server (BRAS), which causes a policy map change on PPPoA sessions set up between the BRAS and the routing gateway (RG).

Figure 9: Change of Authorization--Policy Map Change on PPPoA Sessions



For clarification, a policy map defines QoS actions and rules and associates these to a class map. In a policy map, you can define QoS actions for such things as policing and class-based weighted fair queuing (CBWFQ). After a policy map is configured on the router with the **policy-map** command, using the **service-policy** command attaches the configured policy map to a VC interface and specifies the direction (inbound or outbound) that the policy should be applied.

When a service policy is configured on the VC (or ATM point-to-point subinterface), the service policy is applied to all sessions that use that VC.

Note For the Cisco 7200 series routers, you can configure a service policy on a VC and on a session at the same time. On the Cisco 10000 series routers, you must either configure a service policy on a VC or on a session, but not both at the same time.

Note The Cisco 7200 series routers and Cisco 7301 router only support the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters for this feature. The Cisco 10000 series routers support all ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, for this feature.

New Cisco VSAs

To support the Define Interface Policy-Map AV Pairs AAA feature, the following two new Cisco AV pairs for policy map are defined at the ATM VC level:

- Cisco VSA attribute is vc-qos-policy-in
- Cisco VSA attribute is vc-qos-policy-out

They are formatted as:

- cisco-avpair = “atm:vc-qos-policy-in=<*in policy name*>”
- cisco-avpair = “atm:vc-qos-policy-out=<*out policy name*>”

To further support the Define Interface Policy-Map AV Pairs AAA feature, two existing Cisco Generic RADIUS VSAs will replace and deprecate two others that do not correctly follow the Cisco VSA naming guidelines.

The two replacement VSAs are:

- cisco-avpair = “ip:sub-qos-policy-in=<*in policy name*>”
- cisco-avpair = “ip:sub-qos-policy-out=<*out policy name*>”

The replacement VSAs replace the following existing VSAs:

- cisco-avpair = “ip:sub-policy-In=<*in policy name*>”
- cisco-avpair = “ip:sub-policy-Out=<*out policy name*>”

We recommend using the new VSAs. However, the replaced attributes are currently still supported.

Policy Map Troubleshooting Scenarios

- If a policy map is already configured on the ATM VC, the policy map pulled from the RADIUS server has higher precedence. This means that a **show policy-map** command shows the policy map pulled from the RADIUS server.

- After a policy map is successfully pulled on the VC, any configuration or unconfiguration after that using the **[no] service-policy input**/**output** *name* command does not affect the policy map used by the VC. Issuing a **show policy-map**command displays the pulled policy map. Issuing a **show run** command displays the current user configuration on the router.
- To remove the dynamic policy that is pulled from the RADIUS server, use the **no dbs enable** command or clear the PPPoA or PPPoEoA session associated with the VC.
- You should push both the input and output policy map together on the VC. If you push only one policy in one direction (for example, the input direction), then the output direction by default is a null policy push. The result is that on the VC, the input policy map is the policy pushed by the CoA. The output policy map is whatever policy was configured locally on the VC. If no output policy map was configured on the VC, there is no output policy map.

How to Configure Define Interface Policy-Map AV Pairs AAA

Configuring AV Pairs Dynamic Authorization and the Policy Map on the RADIUS Server

To configure the Define Interface Policy-Map AV Pairs AAA feature, follow the steps on the RADIUS server.

Prerequisites

AAA must be enabled and already set up to use RADIUS.

A PPPoEoA or PPPoA session is established.

The CoA functionality is enabled--required for the push functionality.

The **dbs enable** CLI is configured on the VC.

The policy map is configured on the router.

SUMMARY STEPS

1. atm:vc-qos-policy-in=<in policy name>

DETAILED STEPS

	Command or Action	Purpose
Step 1	atm:vc-qos-policy-in=<in policy name> **Example:** `atm:vc-qos-policy-out=<out policy name>`	Enters the two new Cisco AV pairs for service policy on the RADIUS server in the user file. When the router requests the policy name, this information in the user file is “pulled.” A RADIUS user file contains an entry for each user that the RADIUS server will authenticate. Each entry, which is also referred to as a *user profile*, establishes an attribute the user can access.

	Command or Action	Purpose

	Example:
	`userid    Password ="cisco"`
	Example:
	`   Service-Type = Framed,`
	Example:
	`   Framed-Protocol = PPP,`
	Example:
	`   cisco-avpair = "atm:vc-qos-policy-out=dyn_out",`
	Example:
	`   cisco-avpair = "atm:vc-qos-policy-in=test_vc"`
		When looking at a user file, the data to the left of the equal sign (=) is an attribute defined in the dictionary file, and the data to the right of the equal sign is the configuration data.
		In this example, you have configured a service policy that attaches a policy map to the ATM VC interface and specifies the direction (inbound for data packets traveling into the interface or outbound for data packets leaving the interface).
		The policy map applied in the outbound direction is dyn_out and the inbound policy map is test_vc.

Configuring AV Pairs Dynamic Authorization and the Policy Map on the AAA Server

On the local AAA server, configure dynamic authorization that supports CoA in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. Configure the **client** command and **server-key** keyword or the **client** command and **server-key** command.

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Sets up the local AAA server for dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction and enters dynamic authorization local server configuration mode. In this mode, the RADIUS application commands are configured.
Step 5	Configure the **client** command and **server-key** keyword or the **client** command and **server-key** command. **Example:** **aaa server radius dynamic-author** **Example:** **auth-type** {**any** | **all** | **session-key**} **Example:** **domain** {**delimiter** *character* | **stripping [right-to-left]**} **Example:** **client** {*ip_addr* | *hostname*} [**server-key** [**0** | **7**] *string*] [**vrf** *vrfname* [**server-key** [**0** | **7**] *string*]]	You can use the **client**command and **server-key** keyword and *string* argument to configure the server key at the “client” level, or use the **server-key** command and *string* argument to configure the server key at the “global” level, which allows all the clients configured with the **client** command to use the global server key. **Note** Configuring the server key at the client level overrides the server key configured at the global level. For security purposes, we recommend configuring each client and configuring different server-keys for each client. The example configuration enables change of authorization and configures two client routers with different server-keys (cisco1 and cisco2). The **auth-type**, **domain**, **ignore session-key**, **ignore server-key**, and **port** commands are optional. **Note** When using the **auth-type** command and **session-key** keyword, the session-key attribute must match for authorization to be successful. The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid. The **domain** command configures username domain options for the RADIUS application. • The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, **/**, **$**, **%**, \, **#** or **-**

	Command or Action	Purpose

	Example:
	ignore {**session-key** | **server-key**}
	Example:
	port {*port-num*}
	Example:
	server-key [**0** | **7**] *string*
	Example:
	`Router(config)aaa server radius dynamic-author`
	Example:
	`Router(config-locsvr-da-radius)#client 192.168.0.5 vrf coa server-key cisco1`
	Example:
	`Router(config-locsvr-da-radius)#client 192.168.1.5 vrf coa server-key cisco2`
		• The **stripping** keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.
		• The **right-to-left** keyword terminates the string at the first delimiter going from right to left.

Configuring AV Pairs Dynamic Authorization and the Policy Map on the Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** [*module*/*slot*/*port.subinterface*] **point-to-point**
4. **pvc vpi/vci**
5. **dbs enable**
6. **exit**
7. **policy-map** *policy-map-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** [*module*/*slot*/*port.subinterface*] **point-to-point** **Example:** `Router(config)# interface ATM 4/0/1 point-to-point`	Specifies the interface, for example ATM4/0, and the encapsulation type on an ATM PVC. Enters subinterface mode.
Step 4	**pvc vpi/vci** **Example:** `Router(config-if)# pvc 1/101`	Creates or assigns a name to an ATM permanent virtual circuit (PVC) in subinterface configuration mode. The **pvc** command creates a PVC and attaches it to the virtual path identifier (VPI) and virtual channel identifier (VCI) specified. Enters ATM virtual circuit configuration mode. The example specifies VPI 1 and VCI 101 for this PVC.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Enables Dynamic Bandwidth Selection (DBS) in ATM VC configuration mode. Enabling this command allows the ATM shaping parameters to be retrieved from the RADIUS user profile. **Note** The **no dbs enable** command re-creates the VC and removes the dynamic policy that is pulled from the RADIUS server. Consequently, any configured modular QoS CLI (MQC) policy map on the PVC will be installed on the VC. Do not issue the **no dbs enable** command when the VC is active.
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode and returns to subinterface configuration mode. Repeat this step one more time to exit subinterface configuration mode and return to global configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map voice`	Creates a policy map on the router. In the example, a policy map named voice is created.

	Command or Action	Purpose
	Example:	

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

Verifying Define Interface Policy-Map AV Pairs AAA

Perform this optional task to verify the configuration of the Define Interface Policy-Map AV Pairs AAA feature.

SUMMARY STEPS

1. **show policy-map interface**
2. **show running-config**
3. **show running-config**

DETAILED STEPS

Step 1 **show policy-map interface**

The **show policy-map interface**command shows the policy map voice attached to the ATM VC:

Example:

```
Router# show policy-map interface atm 4/0
ATM4/0: VC 1/101 -
 Service-policy input: voice
   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Step 2 **show running-config**

The following example displays the running configuration on the router showing the AAA setup; policy map configuration; ATM VC, PPPoA, and DBS-enabled CLI configuration; Virtual-Template configuration; and RADIUS server configuration:

Example:

```
Router# show running-config
.
.
```

```
.
aaa new-model
!
aaa user profile TEST
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
aaa session-id common
ip subnet-zero
.
.
.
policy-map voice
class Class-Default
fair-queue
.
.
.
!
interface ATM4/0.1 point-to-point
 pvc 1/101
  dbs enable
  encapsulation aal5mux ppp Virtual-Template1
 !
.
.
.
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp authentication chap
!
.
.
.
!
radius-server host 172.19.197.225 auth-port 1890 acct-port 1891
radius-server timeout 15
radius-server key 7 060506324F41
radius-server vsa send accounting
radius-server vsa send authentication
!
.
.
.
!
!
end
```

Step 3 **show running-config**

The following example displays the PPPoA client configuration:

Example:

```
.
.
.
!
interface ATM4/0.1 point-to-point
 pvc 1/101
  encapsulation aal5mux ppp Virtual-Template1
 !
!
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp chap hostname userid
 ppp chap password 7 030752180500
```

```
!
.
.
.
```

Configuration Examples for Define Interface Policy-Map AV Pairs AAA

Service-Policy Map Already Configured Example

The following example shows the existing MQC used to attach policy maps voice and outname under PVC 4/103. Using the **show policy-map interface**command shows that MQC-configured policy maps voice and outname are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
  service-policy input voice
  service-policy output outname
 !
Router# show policy-map interface atm 4/0.3
 ATM4/0.3: VC 4/103 -
  Service-policy input: voice
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
  Service-policy output: outname
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
Router#
```

The following example shows MQC used to establish a PPPoEoA session, which causes the policy maps (test_vc and dyn_out) set up on the RADIUS server to be downloaded or “pulled” to the VC. The policy maps downloaded from the RADIUS server have higher precedence than the MQC service-policy maps (voice and outname) configured on the PVC. Using the **show policy-map interface**command shows that the pulled policy maps are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
  dbs enable
  encapsulation aal5autoppp Virtual-Template1
  service-policy input voice
  service-policy output outname
 !
end
Router# show policy-map interface atm 4/0.3
```

```
 ATM4/0.3: VC 4/103 -
  Service-policy input: test_vc
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
  Service-policy output: dyn_out
    Class-map: class-default (match-any)
      5 packets, 370 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        5 packets, 370 bytes
        5 minute rate 0 bps
Router#
PPPoE Session Information
Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st
      2      2  0010.1436.bc70  ATM4/0.3                 1  Vi3.1      PTA
                0010.1436.b070  VC:  4/103                  UP
Router#
```

Service-Policy Map Pulled Example

The following example shows a policy named voice configured for input service policy on the RADIUS server. The router is already configured for PPPoA and AAA. The PPPoA session pulls the service policy name from the RADIUS server.

The **show policy-map interface**command displays the input service policy named voice attached to the ATM interface:

```
Router# show policy-map interface atm 4/0.1
ATM4/0: VC 1/101 -
 Service-policy input: voice
   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Using the **show run interface**command displays the currently running configuration, but not the pulled service policy:

```
Router# show run interface atm 4/0.1
Building configuration...
Current configuration : 107 bytes
!
interface ATM 4/0.1
    pvc 1/101
         dbs enable
         encapsulation aal5mux ppp Virtual-Template 1
    !
!
end
```

Service-Policy Map Pushed Example

This configuration example has five parts that show that PPPoA sessions are established between a broadband remote access server (BRAS) and a routing gateway (RG), the change of authorization (CoA push request) that passes between a policy server and the BRAS, and how the pulled policy maps are replaced by pushed policy maps after the CoA request.

The five parts are: BRAS PPPoA configuration, RG PPPoA configuration, session information on BRAS prior to a push, debug on BRAS after receiving the CoA request, and session information on BRAS after a CoA push request has taken place.

The following example shows the current PPPoA configuration on BRAS:

```
aaa new-model
 !
 aaa authentication ppp default group radius
 aaa authorization network default group radius
 !
 aaa server radius dynamic-author
  client <address> server-key <key>
 !
 aaa session-id common
 !
 ip routing
 !
 policy-map DefaultIn
   class class-default
   set ip precedence 0
 policy-map DefaultOut
   class class-default
   set ip precedence 0
 !
 policy-map PullMapIn
   class class-default
   set ip precedence 0
 policy-map PullMapOut
   class class-default
   set ip precedence 0
 !
 policy-map 7up
   class class-default
     fair-queue
 policy-map Sprite
   class class-default
     bandwidth 1000
 !
 policy-map PushMapIn
   class class-default
   set ip precedence 0
 policy-map PushMapOut
   class class-default
   set ip precedence 0
 !
 !
 vc-class atm xyz
   protocol ppp Virtual-Template1
   encapsulation aal5snap
 !
 interface Loopback0
  ip address 10.1.1.2 255.255.255.0
 !
 interface ATM4/0
  no ip address
  no atm ilmi-keepalive
  no atm enable-ilmi-trap
  no clns route-cache
  no shutdown
 !
 interface ATM4/0.1 point-to-point
  no atm enable-ilmi-trap
  pvc 0/101
   class-vc xyz
   vbr-nrt 400 300 50
   dbs enable
   service-policy in DefaultIn
   service-policy out DefaultOut
  !
 !
 interface Virtual-Template1
  ip unnumbered Loopback0
  ppp authentication chap
 !
 radius-server host <address> auth-port <port> acct-port <port>
 radius-server key <key>
 radius-server vsa send authentication
```

The following example shows the PPPoA configuration set up on the RG:

```
aaa new-model
 !
 aaa session-id common
 !
 ip routing
 !
 interface Loopback0
  ip address 10.1.1.1 255.255.255.0
 !
 interface ATM2/0/0
  no ip address
  no atm ilmi-keepalive
  no atm enable-ilmi-trap
  no clns route-cache
  no shutdown
 !
 interface ATM2/0/0.1 point-to-point
  pvc 0/101
   protocol ppp Virtual-Template1
  !
 !
 interface Virtual-Template1
  ip unnumbered Loopback0
  no peer default ip address
  ppp chap hostname InOut
  ppp chap password 0 <password>
```

The following example uses the **show subscriber session all** command to display session information on BRAS prior to policy maps being pushed. PullMapIn and PullMapOut are the profiles pulled from the AAA server. The CoA request pushes the BRAS to change its input policy map (PullMapIn) and output policy map (PullMapOut) to PushMapIn and PushMapOut respectively.

```
Router# show subscriber session all
Current Subscriber Information:Total sessions 1
--------------------------------------------------
Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:32, Last Changed:00:00:12
AAA unique ID:55
Interface:Virtual-Access1.1
Policy information:
  Context 6531F6AC:Handle C700008A
  Authentication status:authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    service-type         2 [Framed]
    ssg-account-info     "S10.1.1.1"
    vc-qos-policy-in     "PullMapIn"
    vc-qos-policy-out    "PullMapOut"
  Prepaid context:not present
Configuration sources associated with this session:
Interface:Virtual-Template1, Active Time = 00:00:32
```

The following example displays the output of the **debug aaa coa** and **debug pppatm event**commands to show that the input policy map, PushMapIn, and output policy map, PushMapOut, have been applied or pushed on the BRAS after the BRAS received the CoA push request from the policy server:

```
2d20h:RADIUS:COA  received from id 41 10.0.56.145:1700, CoA Request, len 122
2d20h:COA:10.0.56.145 request queued
2d20h: ++++++ CoA Attribute List ++++++
2d20h:6523AE20 0 00000001 service-type(276) 4 Framed
2d20h:6523AF4C 0 00000009 ssg-account-info(392) 9 S10.1.1.1
2d20h:6523AF5C 0 00000009 ssg-command-code(394) 1 17
2d20h:6523AF6C 0 00000009 vc-qos-policy-in(342) 7 PushMapIn
2d20h:6523AF7C 0 00000009 vc-qos-policy-out(343) 4 PushMapOut
2d20h:
2d20h: PPPATM:Received VALID vc policy PushMapIn
2d20h: PPPATM:Received VALID vc policy PushMapOut
2d20h:PPPATM:ATM4/0.1 0/101 [54], Event = SSS Msg Received = 5
2d20h:Service policy input PushMapIn policy output PushMapOut applied on 0/101
2d20h: PPPATM:Applied VALID vc policy PushMapIn and PushMapOut
2d20h:RADIUS(00000000):sending
2d20h:RADIUS(00000000):Send CoA Ack Response to 10.0.56.145:1700 id 41, len 20
2d20h:RADIUS: authenticator 04 D5 05 E2 FE A3 A6 E5 - B2 07 C0 A1 53 89 E0 FF
```

The following example uses the **show subscriber session all** command to display session information on the BRAS after the BRAS received the CoA push request from the policy server. The policy information shows that PushMapIn and PushMapOut are the current policy maps on the BRAS that were pushed by the CoA request:

```
Router# show subscriber session all
Current Subscriber Information:Total sessions 1
--------------------------------------------------
Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:44, Last Changed:00:00:22
AAA unique ID:55
Interface:Virtual-Access1.1
Policy information:
  Context 6531F6AC:Handle C700008A
  Authentication status:authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    service-type         2 [Framed]
    ssg-account-info     "S10.1.1.1"
    vc-qos-policy-in     "PushMapIn"
    vc-qos-policy-out    "PushMapOut"
  Prepaid context:not present
Configuration sources associated with this session:
Interface:Virtual-Template1, Active Time = 00:00:44
```

Additional References

The following sections provide references related to the Define Interface Policy-Map AV Pairs AAA feature.

Related Documents

Related Topic	Document Title
WAN commands: complete command syntax, command mode, defaults, usage guidelines, and examples.	*Cisco IOS Wide-Area Networking Command Reference*

Related Topic	Document Title
Quality of Service commands, such as **show policy-map**.	*Cisco IOS Quality of Service Solutions Command Reference*

MIBs

MIBs	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

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

Technical Assistance

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

Feature Information for Define Interface Policy-Map AV Pairs AAA

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 Define Interface Policy-Map AV Pairs AAA

Feature Name	Releases	Feature Information
Define Interface Policy-Map AV Pairs AAA	12.3(7)XI2 12.2(28)SB 12.2(33)SRC12.4(20)T 15.1(2)T	The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco Remote Authentication Dial-In User Service (RADIUS) vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level. This feature was integrated into Cisco IOS Release 12.3(7)XI2 and introduced for the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The “pull” functionality was implemented. This feature was integrated into Cisco IOS Release 12.2(28)SB. Support for the “push” functionality was added on the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The name for this functionality is RADIUS Push for MOD CLI Policies, which was integrated into the Define Interface Policy-Map AV Pairs AAA feature module. This feature was integrated into Cisco IOS Release 12.2(33)SRC. This feature was integrated into Cisco IOS Release 12.4(20)T. The **right-to-left** keyword was added to the **domain** command in Cisco IOS Release 15.1(2)T.

CHAPTER 11

RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect feature is used to terminate a connected voice call.

- Finding Feature Information, page 167
- Prerequisites for RADIUS Packet of Disconnect, page 167
- Restrictions for RADIUS Packet of Disconnect, page 168
- Information About RADIUS Packet of Disconnect, page 168
- How to Configure the RADIUS Packet of Disconnect, page 169
- Additional References, page 172
- Feature Information for RADIUS Packet of Disconnect, page 173
- Glossary, page 174

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 Packet of Disconnect

- Configure AAA as described in *Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0(1)M.
- Use Cisco IOS Release 12.2(11)T or later.

Restrictions for RADIUS Packet of Disconnect

Proper matching identification information must be communicated by the following:

- Billing server and gateway configuration
- Gateway’s original accounting start request
- Server’s POD request

Information About RADIUS Packet of Disconnect

The Packet of Disconnect (POD) is a RADIUS access_request packet and is intended to be used in situations where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet.

When the POD is Needed

The POD may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call. A price structure so complex that the maximum session duration cannot be estimated before accepting the call. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.
- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a call to be disconnected, all parameters must match their expected values at the gateway. If the parameters do not match, the gateway discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

POD Parameters

The POD has the following parameters:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte MD5 hash value that is carried in the *authentication* field of the POD request.
- Cisco allocated POD code 50 as the new code value for the Voice POD Request in Cisco IOS Release 12.2(27)SB and 12.4(15)T. This change was made because RFC 3576 *Dynamic Authorization Extensions to RADIUS* recently extended RADIUS standards to officially support both a Disconnect Message (DM) and Change-of-Authorization (CoA), which is supported through the POD.

RFC 3576 specifies the following POD codes:

- • 40 - Disconnect-Request

- 41 - Disconnect-ACK
- 42 - Disconnect-NAK
- 43 - CoA-Request
- 44 - CoA-ACK
- 45 - CoA-NAK

How to Configure the RADIUS Packet of Disconnect

Configuring the RADIUS POD

Use the following tasks to configure the RADIUS POD:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*
4. Router# exit
5. Router# **show running-configuration**

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	Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*	Enables inbound user sessions to be disconnected when specific session attributes are presented. • **port** *port-number* --(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700.

	Command or Action	Purpose
	Example: `Router(config)# aaa pod server server-key xyz123`	• **auth-type** --(Optional) The type of authorization required for disconnecting sessions. • any--Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). • **all** --Only a session that matches all four key attributes is disconnected. **all** is the default. • **session-key** --Session with a matching session-key attribute is disconnected. All other attributes are ignored. • **server-key** --Configures the shared-secret text string. • *encryption-type* --(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco. • *string* --The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.
Step 4	Router# exit	Exits global configuration mode.

Step 5	Router# **show running-configuration**
	Example:
	`Router# show running-configuration`
	Example:
	`!`
	Example:
	`aaa authentication login h323 group radius`
	Example:
	`aaa authorization exec h323 group radius`
	Example:
	`aaa accounting update newinfo`
		Verifies that the gateway is configured correctly in priveleged EXEC mode.

	Command or Action	Purpose
	Example: aaa accounting connection h323 start-stop group radius **Example:** aaa pod server server-key cisco **Example:** aaa session-id common **Example:** !	

Troubleshooting Tips

Use the following tips to troubleshoot POD issues:

- Ensure that the POD port is configured correctly in both the gateway (using **aaa pod server**command) and the radius server. Both should be the same.
- Ensure that the shared-secret key configured in the gateway (using **aaa pod server**command) and in the AAA server are the same.
- Turn on **debug aaa pod** command to see what's going on. This will let you know if the gateway receives the POD packet from the server and if so, it will display any errors encountered.

The following example shows output from a successful POD request, when using the **show debug** command.

```
Router# debug aaa podAAA POD packet processing debugging is on
Router# show debugGeneral OS:
  AAA POD packet processing debugging is on
Router#
Apr 25 17:15:59.318:POD:172.19.139.206 request queued
Apr 25 17:15:59.318:voice_pod_request:
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_guid:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-conf-id
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50 value_len=35
Apr 25 17:15:59.318:voip_pod_get_guid:conf-id=FFA7785F F7F607BB
00000000 993FB1F4 n_bytes=35
Apr 25 17:15:59.318:voip_pod_get_guid:GUID = FFA7785F F7F607BB 00000000
993FB1F4
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-originate
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23 value_len=6
Apr 25 17:15:59.318:voip_get_call_direction:
Apr 25 17:15:59.318:voip_get_call_direction:returning answer
Apr 25 17:15:59.318:voip_eval_pod_attr:
Apr 25 17:15:59.318:cc_api_trigger_disconnect:
Apr 25 17:15:59.322:POD:Sending ACK to 172.19.139.206/1700
Apr 25 17:15:59.322:voip_pod_clean:
```

Additional References

The following sections provide references related to the RADIUS Packet of Disconnect feature.

Related Documents

Related Topic	Document Title
AAA	*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0(1)M
Security commands	*Cisco IOS Security Command Reference*
CLI Configuration	*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T
Configuring AAA for voice gateways	*Configuring AAA for Cisco Voice Gateways*, Release 12.4T

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
RFC 2865	*Remote Authentication Dial-in User Service*
RFC 3576	*Dynamic Authorization Extensions to RADIUS*

Technical Assistance

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

Feature Information for RADIUS Packet of Disconnect

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 RADIUS Packet of Disconnect

Feature Name	Releases	Feature Information
RADIUS Packet of Disconnect	12.2(2)XB 12.1(2)XH 12.3(11)T 12.2(27)SB 12.4(15)T	The RADIUS Packet of Disconnect feature is used to terminate a connected voice call. In Cisco IOS Release12.2(2)XB, this feature was introduced on the Cisco 3600, Cisco 5350, and Cisco 5400. In Cisco IOS Release 12.1(2)XH and 12.1(3)T, this feature was introduced on the Cisco 5300 and Cisco 5800. In Cisco IOS Release 12.2(11)T, this feature was introduced on the Cisco 5400, Cisco 5850 In Cisco IOS Release 12.2(27)SB and 12.4(15)T, Cisco allocated POD code 50 as the new code value for the voice POD request The following commands were introduced or modified: **aaa pod server** and **debug aaa pod**

Glossary

AAA --authentication, authorization, and accounting.

NACK --negative acknowledgement message.

POD --packet of disconnect. An access_reject packet sent from a RADIUS server to the gateway in order to disconnect a call which has been connected already. After validation of the packet, the gateway disconnects the user. The packet contains the information to disconnect the call.

POD server--a Cisco gateway configured to accept and process POD requests from a RADIUS authentication/authorization agent.

RADIUS --Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet service providers.

UDP --User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

VoIP-- voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based (for example, H.323) approach to IP voice traffic.

VSA --vendor-specific attribute.

CHAPTER 12

MAC Authentication Bypass

The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco Identity Based Networking Services (IBNS) and Network Admission Control (NAC) strategy using the client MAC address. The MAC Authentication Bypass feature is applicable to the following network environments:

- Network environments in which a supplicant code is not available for a given client platform.
- Network environments in which the end client configuration is not under administrative control, that is, the IEEE 802.1X requests are not supported on these networks.

- Finding Feature Information, page 177
- Prerequisites for Configuring MAC Authentication Bypass, page 178
- Information About Configuring MAC Authentication Bypass, page 178
- How to Configure MAC Authentication Bypass, page 179
- Configuration Examples for MAC Authentication Bypass, page 184
- Additional References, page 184
- Feature Information for MAC Authentication Bypass, page 185

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 MAC Authentication Bypass

IEEE 802.1x—Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform. For more information, see the *Securing User Services Configuration Guide Library*.

RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Securing User Services Configuration Guide Library*.

The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *User Guide for Secure ACS Appliance 3.2*.

Information About Configuring MAC Authentication Bypass

Overview of the Cisco IOS Auth Manager

The capabilities of devices connecting to a given network can be different, thus requiring that the network support different authentication methods and authorization policies. The Cisco IOS Auth Manager handles network authentication requests and enforces authorization policies regardless of authentication method. The Auth Manager maintains operational data for all port-based network connection attempts, authentications, authorizations, and disconnections and, as such, serves as a session manager.

The possible states for Auth Manager sessions are as follows:

- Idle—In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.
- Running—A method is currently running. This is an intermediate state.
- Authc Success—The authentication method has run successfully. This is an intermediate state.
- Authc Failed—The authentication method has failed. This is an intermediate state.
- Authz Success—All features have been successfully applied for this session. This is a terminal state.
- Authz Failed—At least one feature has failed to be applied for this session. This is a terminal state.
- No methods—There were no results for this session. This is a terminal state.

How to Configure MAC Authentication Bypass

Enabling MAC Authentication Bypass

Perform this task to enable the MAC Authentication Bypass feature on an 802.1X port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **mab**
5. **end**
6. **show authentication sessions interface** *type slot* / *port* **details**

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	**interface** *type slot* / *port* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 4	**mab** **Example:** `Device(config-if)# mab`	Enables MAB.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show authentication sessions interface** *type slot* / *port* **details** **Example:** `Device# show authentication session interface Gigabitethernet 1/2/1 details`	Displays the interface configuration and the authenticator instances on the interface.

Enabling Reauthentication on a Port

By default, ports are not automatically reauthenticated. You can enable automatic reauthentication and specify how often reauthentication attempts are made.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication periodic**
9. **authentication timer reauthenticate** {*seconds* | **server**}
10. **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.

	Command or Action	Purpose
Step 3	**interface** *type slot* / *port* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Places interface in Layer 2 switched mode.
Step 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** `Device(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** `Device(config-if)# mab`	Enables MAB.
Step 8	**authentication periodic** **Example:** `Device(config-if)# authentication periodic`	Enables reauthentication.

Step 9	**authentication timer reauthenticate** {*seconds* | **server**}
	Example:
	`Device(config-if)# authentication timer reauthenticate 900`
		Configures the time, in seconds, between reauthentication attempts.

Step 10	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Specifying the Security Violation Mode

When there is a security violation on a port, the port can be shut down or traffic can be restricted. By default, the port is shut down. You can configure the period of time for which the port is shut down.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication violation** {**restrict** | **shutdown**}
9. **authentication timer restart** *seconds*
10. **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	**interface** *type slot* / *port* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Places interface in Layer 2 switched mode.

	Command or Action	Purpose
Step 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** `Device(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 7	**mab** [**eap**] **Example:** `Device(config-if)# mab`	Enables MAB.

Step 8	**authentication violation** {**restrict** | **shutdown**}
	Example:
	`Device(config-if)# authentication violation shutdown`
		Configures the action to be taken when a security violation occurs on the port.

Step 9	**authentication timer restart** *seconds* **Example:** `Device(config-if)# authentication timer restart 30`	Configures the period of time, in seconds, after which an attempt is made to authenticate an unauthorized port.

Step 10	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for MAC Authentication Bypass

Example: MAC Authentication Bypass Configuration

In the following example, the **mab** command has been configured to enable the MAC Authorization Bypass (MAB) feature on the specified interface. The optional **show authentication sessions** command has been enabled to display the interface configuration and the authentication instances on the interface.

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/2/1
Device(config-if)# mab
Device(config-if)# end
Device# show authentication sessions interface GigabitEthernet 1/2/1 details
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication commands	*Cisco IOS Security Command Reference*
IEEE 802.1x—Flexible Authentication	*Securing User Services Configuration Library*

MIBs

MIB	MIBs Link
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3580	*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*

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 MAC Authentication Bypass

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

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

Table 25: Feature Information for MAC Authentication Bypass

Feature Name	Releases	Feature Information
MAC Authentication Bypass (MAB)	12.1(22)T 12.2(31)SG 12.2(33)SXH 15.1(4)M	The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco IBNS and NAC strategy using the client MAC address. In Cisco IOS Release 15.1(4)M, support was extended for Integrated Services Router Generation 2 (ISR G2) platforms. The following commands were introduced or modified: **dot1x mac-auth-bypass**, **show dot1x interface**.

CHAPTER 13

Standalone MAB Support

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.

Before standalone MAB support was available, MAB could be configured only as a failover method for 802.1x authentication. Standalone MAB is independent of 802.1x authentication.

- Finding Feature Information, page 187
- Information About Configuring Standalone MAB, page 188
- How to Configure Standalone MAB Support, page 188
- Configuration Examples for Standalone MAB Support, page 190
- Additional References, page 191
- Feature Information for Standalone MAB Support, page 192

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 Configuring Standalone MAB

Standalone MAB

MAC Authentication Bypass (MAB) uses the MAC address of the connecting device to grant or deny network access. To support MAB, the RADIUS authentication server maintains a database of MAC addresses for devices that require access to the network. MAB generates a RADIUS request with a MAC address in the Calling-Station-Id (attribute 31) and with a Service-Type (attribute 6) 10. After a successful authentication, the Auth Manager enables various authorization features specified by the authorization policy, such as ACL assignment and VLAN assignment.

How to Configure Standalone MAB Support

Enabling Standalone MAB

Ports enabled with the Standalone MAB feature can use the MAC address of connecting devices to grant or deny network access. Perform the steps described in this section to enable standalone MAB on individual ports.

Before You Begin

Before you can configure standalone MAB, the device must be connected to a Cisco Secure ACS server and RADIUS authentication, authorization, and accounting (AAA) must be configured.

Note Standalone MAB can be configured on devices with switched ports only; it cannot be configured on devices with routed ports.

Note If you are unsure whether MAB or MAB Extensible Authentication Protocol (EAP) is enabled or disabled on the switched port, use the **default mab**or **default mab eap** commands in interface configuration mode to configure MAB or MAB EAP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab**
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	**interface** *type slot / port* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 4	**switchport** **Example:** `Switch(config-if)# switchport`	Places interface in Layer 2 switched mode.
Step 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets the interface type a as nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	**authentication port-control auto** **Example:** `Device(config-if)# authentication port-control auto`	Configures the authorization state of the port.

	Command or Action	Purpose
Step 7	**mab** **Example:** `Device(config-if)# mab`	Enables MAB.

Step 8	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can help troubleshoot standalone MAB:

- **debug authentication**
- **debug mab all**
- **show authentication registrations**
- **show authentication sessions**
- **show mab**

Configuration Examples for Standalone MAB Support

Example: Standalone MAB Configuration

The following example shows how to configure standalone MAB on a port. In this example, the client is reauthenticated every 1200 seconds and the connection is dropped after 600 seconds of inactivity.

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/2/1
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 2
Device(config-if)# authentication port-control auto
Device(config-if)# mab
Device(config-if)# authentication violation shutdown
Device(config-if)# authentication timer restart 30
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate 1200
Device(config-if)# authentication timer inactivity 600
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication commands	*Cisco IOS Security Command Reference*
IEEE 802.1x—Flexible Authentication	*Securing User Services Configuration Library*

MIBs

MIB	MIBs Link
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3580	*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*

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 Standalone MAB 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 26: Feature Information for Standalone MAB Support

Feature Name	Releases	Feature Information
Standalone MAB Support	12.2(33)SXI 15.2(2)T	This feature grants network access to devices based on MAC address regardless of 802.1x capability or credentials. The following commands were introduced or modified: **authentication periodic**, **authentication port-control**, **authentication timer inactivity**, **authentication timer reauthenticate**, **authentication timer restart**, **authentication violation**, **debug authentication**, **mab**, **show authentication interface**, **show authentication registrations**, **show authentication sessions**, and **show mab**.

CHAPTER 14

AAA Authorization and Authentication Cache

The AAA Authorization and Authentication Cache feature allows you to cache authorization and authentication responses for a configured set of users or service profiles, providing performance improvements and an additional level of network reliability because user and service profiles that are returned from authorization and authentication responses can be queried from multiple sources and need not depend solely on an offload server. This feature also provides a failover mechanism so that if a network RADIUS or TACACS+ server is unable to provide authorization and authentication responses network users and administrators can still access the network.

- Finding Feature Information, page 193
- Prerequisites for Implementing Authorization and Authentication Profile Caching, page 194
- Information About Implementing Authorization and Authentication Profile Caching, page 194
- How to Implement Authorization and Authentication Profile Caching, page 196
- Configuration Examples for Implementing Authorization and Authentication Profile Caching, page 202
- Additional References, page 203
- Feature Information for Implementing Authorization and Authentication Profile Caching, page 205

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.

PrerequisitesforImplementingAuthorizationandAuthentication Profile Caching

The following prerequisites apply to implementing authorization and authentication profile caching:

- Understand how you would want to implement profile caching, that is, are profiles being cached to improve network performance or as a failover mechanism if your network authentication and authorization (RADIUS and TACACS+) servers become unavailable.
- RADIUS and TACACS+ server groups must already be configured.

Information About Implementing Authorization and Authentication Profile Caching

Network Performance Optimization Using Authorization and Authentication Profile Caching

RADIUS and TACACS+ clients run on Cisco routers and send authentication requests to a central RADIUS or TACACS+ server that contains all user authentication and network service access information. The router is required to communicate with an offload RADIUS or TACACS+ server to authenticate a given call and then apply a policy or service to that call. Unlike authentication, authorization, and accounting (AAA) accounting, AAA authentication and authorization is a blocking procedure, which means the call setup may not proceed while the call is being authenticated and authorized. Thus, the time required to process the call setup is directly impacted by the time required to process such an authentication or authorization request from the router to the offload RADIUS or TACACS+ server, and back again. Any communication problems in the transmission, offload server utilization, and numerous other factors cause significant degradation in a router’s call setup performance due simply to the AAA authentication and authorization step. The problem is further highlighted when multiple AAA authentications and authorizations are needed for a single call or session.

A solution to this problem is to minimize the impact of such authentication requests by caching the authentication and authorization responses for given users on the router, thereby removing the need to send the requests to an offload server again and again. This profile caching adds significant performance improvements to call setup times. Profile caching also provides an additional level of network reliability because user and service profiles that are returned from authentication and authorization responses can be queried from multiple sources and need not depend solely on an offload server.

To take advantage of this performance optimization, you need to configure the authentication method list so that the AAA cache profile is queried first when a user attempts to authenticate to the router. See the Method Lists in Authorization and Authentication Profile Caching section for more information.

Authorization and Authentication Profile Caching as a Failover Mechanism

If, for whatever reason, RADIUS or TACACS+ servers are unable to provide authentication and authorization responses, network users and administrators can be locked out of the network. The profile caching feature allows usernames to be authorized without having to complete the authentication phase. For example, a user by the name of user100@example.com with a password secretpassword1 could be stored in a profile cache using the regular expression ".*@example.com". Another user by the name of user101@example.com with a password of secretpassword2 could also be stored using the same regular expression, and so on. Because the number of users in the ".*@example.com" profile could number in the thousands, it is not feasible to authenticate each user with their personal password. Therefore authentication is disabled and each user simply accesses authorization profiles from a common Access Response stored in cache.

The same reasoning applies in cases where higher end security mechanisms such as Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), or Extensible Authentication Protocol (EAP), which all use an encrypted password between the client and AAA offload server. To allow these unique, secure username and password profiles to retrieve their authorization profiles, authentication is bypassed.

To take advantage of this failover capability, you need to configure the authentication and authorization method list so that the cache server group is queried last when a user attempts to authenticate to the router. See the Method Lists in Authorization and Authentication Profile Caching section for more information.

Method Lists in Authorization and Authentication Profile Caching

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. We support methods such as local (use the local database), none (do nothing), RADIUS server group, or TACACS+ server group. Typically, more than one method can be configured into a method list. software uses the first listed method to authenticate users. If that method fails to respond, the software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or until all methods defined in the method list are exhausted.

To optimize network performance or provide failover capability using the profile caching feature you simply change the order of the authentication and authorization methods in the method list. To optimize network performance, make sure the cache server group appears first in the method list. For failover capability, the cache server group should appear last in the method list.

Authorization and Authentication Profile Caching Guidelines

Because the number of usernames and profiles that can request to be authenticated or authorized at a given router on a given point of presence (POP) can be quite extensive, it would not be feasible to cache all of them. Therefore, only usernames and profiles that are commonly used or that share a common authentication and authorization response should be configured to use caching. Commonly used usernames such as aolip and aolnet, which are used for America Online (AOL) calls, or preauthentication dialed number identification service (DNIS) numbers used to connect Public Switched Telephone Network (PSTN) calls to a network attached storage device, along with domain-based service profiles, are all examples of usernames and profiles that can benefit from authentication and authorization caching.

General Configuration Procedure for Implementing Authorization and Authentication Profile Caching

To implement authorization and authentication profile caching, you would complete the following procedure:

1 Create cache profile groups and define the rules for what information is cached in each group.

Entries that match based on exact username, regular expressions, or specify that all authentication and authorization requests can be cached.

1 Update existing server groups to reference newly defined cache groups.

2 Update authentication or authorization method lists to use the cached information to optimize network performance or provide a failover mechanism.

How to Implement Authorization and Authentication Profile Caching

Creating Cache Profile Groups and Defining Caching Rules

Perform this task to create a cache profile group, define the rules for what information is cached in that group, and verify and manage cache profile entries.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa cache profile** *group-name*
5. **profile** *name* [**no-auth**]
6. Repeat Step 5 for each username you want to add to the profile group in Step 4.
7. **regexp** *matchexpression* {**any**| **only**}[**no-auth**]
8. Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4.
9. **all** [**no-auth**]
10. **end**
11. **show aaa cache group** *name*
12. **clear aaa cache group** *name* {**profile** *name*| **all**}
13. **debug aaa cache group**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa cache profile** *group-name* **Example:** `Router(config)# aaa cache profile networkusers@companyname`	Defines an authentication and authorization cache profile server group and enters profile map configuration mode.
Step 5	**profile** *name* [**no-auth**] **Example:** `Router(config-profile-map)# profile networkuser1 no-auth`	Creates an individual authentication and authorization cache profile based on a username match. • The *name* argument must be an exact match to a username being queried by an authentication or authorization service request. • Use the **no-auth** keyword to bypass authentication for this user.
Step 6	Repeat Step 5 for each username you want to add to the profile group in Step 4.	--
Step 7	**regexp** *matchexpression* {**any**| **only**}[**no-auth**] **Example:** `Router(config-profile-map)# regexp .*@example.com any no-auth`	(Optional) Creates an entry in a cache profile group that matches based on a regular expression. • If you use the **any** keyword, all unique usernames matching the regular expression are saved. • If you use the **only** keyword, only one profile entry is cached for all usernames matching the regular expression. • Use the **no-auth** keyword to bypass authentication for this user or set of users. • Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.
Step 8	Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4.	--

	Command or Action	Purpose
Step 9	**all** [**no-auth**] **Example:** `Router(config-profile-map)# all no-auth`	(Optional) Specifies that all authentication and authorization requests are cached. • Use the **all** command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

Step 10	**end**
	Example:
	`Router(config-profile-map)# end`
		Returns to privileged EXEC mode.

Step 11	**show aaa cache group** *name* **Example:** `Router# show aaa cache group networkusers@companyname`	(Optional) Displays all cache entries for a specified group.
Step 12	**clear aaa cache group** *name* {**profile** *name*| **all**} **Example:** `Router# clear aaa cache group networkusers@companyname profile networkuser1`	(Optional) Clears an individual entry or all entries in the cache.
Step 13	**debug aaa cache group** **Example:** `Router# debug aaa cache group`	(Optional) Displays debug information about cached entries.

Defining RADIUS and TACACS Server Groups That Use Cache Profile Group Information

Perform this task to define how RADIUS and TACACS+ server groups use the information stored in each cache profile group.

Before You Begin

RADIUS and TACACS+ server groups must be created.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name* or**aaa group server tacacs+** *group-name*
5. **cache authorization profile** *name*
6. **cache authentication profile** *name*
7. **cache expiry** *hours* {**enforce**| **failover**}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa group server radius** *group-name* or**aaa group server tacacs+** *group-name* **Example:** `Router(config)# aaa group server radius networkusers@companyname`	Enters RADIUS server group configuration mode. • To enter TACACS+ server group configuration mode, use the **aaa group server tacacs+** *group-name* command.
Step 5	**cache authorization profile** *name* **Example:** `Router(config-sg-radius)# cache authorization profile networkusers@companyname`	Activates the authorization caching rules in the profile networkusers for this RADIUS or TACACS+ server group. • The *name* argument in this command is a AAA cache profile group name.

	Command or Action	Purpose
Step 6	**cache authentication profile** *name* **Example:** `Router(config-sg-radius)# cache authentication profile networkusers@companyname`	Activates the authentication caching rules in the profile networkusers for this RADIUS or TACACS+ server group.

Step 7	**cache expiry** *hours* {**enforce**| **failover**}
	Example:
	`Router(config-sg-radius)# cache expiry 240 failover`
		(Optional) Sets the amount of time before a cache profile entry expires (becomes stale).
		Use the **enforce** keyword to specify that once a cache profile entry expires it is not used again.
		Use the **failover** keyword to specify that an expired cache profile entry can be used if all other methods to authenticate and authorize the user fail.

Step 8	**end**
	Example:
	`Router(config-sg-radius)# end`
		Returns to privileged EXEC mode.

Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used

Perform this task to update authorization and authentication method lists to use the authorization and authentication cache information.

Before You Begin

Method lists must already be defined.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization** {**auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **exec** | **ipmobile** | **multicast** | **network** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default** | *list-name*} [*method1* [*method2...*]]
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa authorization** {**auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **exec** | **ipmobile** | **multicast** | **network** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default** | *list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname`	Enables AAA authorization and creates method lists, which define the authorization methods used when a user accesses a specified function.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname`	Specifies one or more authentication methods for use on serial interfaces that are running PPP.
Step 6	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login default cache adminusers group adminusers`	Sets the authentication at login.

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

Configuration Examples for Implementing Authorization and Authentication Profile Caching

Implementing Authorization and Authentication Profile Caching for Network Optimization Example

The following configuration example shows how to:

- Define a cache profile group adminusers that contains all administrator names on the network and sets it as the default list that is used for all login and exec sessions.
- Activate the new caching rules for a RADIUS server group.
- Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried first.

```
configure terminal
 aaa new-model
 ! Define aaa cache profile groups and the rules for what information is saved to cache.
 aaa cache profile admin_users
 profile adminuser1
 profile adminuser2
 profile adminuser3
 profile adminuser4
 profile adminuser5
 exit
 ! Define server groups that use the cache information in each profile group.
 aaa group server radius admins@companyname.com
 cache authorization profile admin_users
 cache authentication profile admin_users
 ! Update authentication and authorization method lists to specify how profile groups and
server groups are used.
 aaa authentication login default cache admins@companyname.com group admins@companyname.com

 aaa authorization exec default cache admins@companyname.com group admins@companyname.com
 end
```

Implementing Authorization and Authentication Profile Caching as a Failover Mechanism Example

The following configuration example shows how to:

- Create a cache profile group admin_users that contains all of the administrators on the network so that if the RADIUS or TACACS+ server should become unavailable the administrators can still access the network.
- Create a cache profile group abc_users that contains all of the ABC company users on the network so that if the RADIUS or TACACS+ server should become unavailable these users will be authorized to use the network.
- Activate the new caching rules for each profile group on a RADIUS server.

- Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried last.

```
configure terminal
 aaa new-model
 ! Define aaa cache profile groups and the rules for what information is saved to cache.
 aaa cache profile admin_users
 profile admin1
 profile admin2
 profile admin3
 exit
 aaa cache profile abcusers
 profile .*@example.com only no-auth
 exit
 ! Define server groups that use the cache information in each cache profile group.
 aaa group server tacacs+ admins@companyname.com
 server 10.1.1.1
 server 10.20.1.1
 cache authentication profile admin_users
 cache authorization profile admin_users
 exit
 aaa group server radius abcusers@example.com
 server 172.16.1.1
 server 172.20.1.1
 cache authentication profile abcusers
 cache authorization profile abcusers
 exit
 ! Update authentication and authorization method lists to specify how cache is used.
 aaa authentication login default cache admins@companyname.com group admins@companyname.com

 aaa authorization exec default cache admins@companyname.com group admins@companyname.com
 aaa authentication ppp default group abcusers@example.com cache abcusers@example.com
 aaa authorization network default group abcusers@example.com cache abcusers@example.com
 end
```

Additional References

The following sections provide references related to implementing authentication and authorization profile caching.

Related Documents

Related Topic	Document Title
Authentication configuring tasks	Configuring Authentication module.
Authorization configuration tasks	Configuring Authorization module.
RADIUS configuration tasks	Configuring RADIUS module.
Security commands	*Cisco IOS Security 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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for Implementing Authorization and Authentication Profile Caching

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 27: Feature Information for Implementing Authentication and Authorization Profile Caching

Feature Name	Releases	Feature Information
AAA Authorization and Authentication Cache	12.2(28)SB 12.2(33)SRC 12.2(33)SRC	This feature optimizes network performance and provides a failover mechanism in the event a network RADIUS or TACACS+ server becomes unavailable for any reason. This feature was integrated into Cisco IOS Release 12.2(33)SRC. This feature was integrated into Cisco IOS Release 15.0(1)M. The following commands were introduced or modified: **aaa authentication login**, **aaa authentication ppp**, **aaa authorization**, **aaa cache profile**, **all (profile map configuration)**, **cache authentication profile (server group configuration)**, **cache authorization profile (server group configuration)**, **cache expiry (server group configuration)**, **clear aaa cache group**, **debug aaa cache group**, **profile (profile map configuration)**, **regexp (profile map configuration)**, **show aaa cache group**.

CHAPTER 15

Configuring Authorization

The AAA authorization feature is used to determine what a user can and cannot do. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user is granted access to a requested service only if the information in the user profile allows it.

- Finding Feature Information, page 207
- Prerequisites, page 207
- Information About Configuring Authorization, page 208
- How to Configure Authorization, page 211
- Authorization Configuration Examples, page 215
- Additional References, page 219
- Feature Information for Configuring Authorization, page 221

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

Before configuring authorization using named method lists, the following tasks must be performed:

- Enable AAA on your network access server.
- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly.

- Define the characteristics of your Lightweight Directory Access Protocol (LDAP), RADIUS, or TACACS+ security server if RADIUS or TACACS+ authorization is issued so that the Cisco network access server can communicate with the RADIUS or TACACS+ security server.
- Define the rights associated with specific users by using the **username** command if local authorization is issued.
- See the Related Documents section for more information on documents related to these prerequisites.

Information About Configuring Authorization

Named Method Lists for Authorization

Method lists for authorization define the ways that authorization is performed and the sequence in which these methods are performed. A method list is simply a named list describing the authorization methods to be queried (such as LDAP, RADIUS, or TACACS+), in sequence. Method lists enable one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

Method lists are specific to the authorization type requested:

- **Auth-proxy** --Applies specific security policies on a per-user basis.
- **Commands** --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC** --Applies to the attributes associated with a user EXEC terminal session.
- **Network** --Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access** --Applies to reverse Telnet sessions.

When a named method list is created, a particular list of authorization methods for the indicated authorization type is defined.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named “default”). If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, local authorization takes place by default.

AAA Authorization Methods

AAA supports five different methods of authorization:

- TACACS+--The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- If-Authenticated--The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None** --The network access server does not request authorization information; authorization is not performed over this line/interface.
- Local--The router or access server consults its local database, as defined by the **username** command, for example, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- LDAP--The network access server requests authorization information from the RADIUS security server. LDAP authorization defines specific rights for users by associating attributes, which are stored in a database on the LDAP server, with the appropriate user.
- RADIUS--The network access server requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.

Note With CSCuc32663, passwords and authorization logs are masked before being sent to the TACACS+, LDAP, or RADIUS security servers. Use the **aaa authorization commands visible-keys** command to send unmasked information to the TACACS+, LDAP, or RADIUS security servers.

Authorization Methods

To have the network access server request authorization information through a TACACS+ security server, use the **aaa authorization** command with the **group tacacs+** *method* keyword. For more specific information about configuring authorization using a TACACS+ security server, see the Configuring TACACS+ feature module. For an example of how to enable a TACACS+ server to authorize the use of network services, including PPP and ARA, see the TACACS Authorization Examples for more information.

To allow users to have access to the functions they request as long as they have been authenticated, use the **aaa authorization** command with the **if-authenticated** *method* keyword. If this method is selected, all requested functions are automatically granted to authenticated users.

There may be times when it is not desirable to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the **none** *method* keyword. If this method is selected, authorization is disabled for all actions.

To select local authorization, which means that the router or access server consults its local user database to determine the functions a user is permitted to use, use the **aaa authorization** command with the **local** *method* keyword. The functions associated with local authorization are defined by using the **username** global configuration command. For a list of permitted functions, see the Configuring Authentication feature module.

To have the network access server request authorization through a LDAP security server, use the **ldap** *method* keyword. For more specific information about configuring authorization using a RADIUS security server, see the Configuring RADIUS feature module

To have the network access server request authorization through a RADIUS security server, use the **radius** *method* keyword. For more specific information about configuring authorization using a RADIUS security server, see the Configuring RADIUS feature module.

To have the network access server request authorization through a RADIUS security server, use the **aaa authorization** command with the **group radius** *method* keyword. For more specific information about configuring authorization using a RADIUS security server, see the Configuring RADIUS feature module. For an example of how to enable a RADIUS server to authorize services, see the RADIUS Authorization Example for more information.

Note Authorization method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for authorization applies.

Method Lists and Server Groups

A server group is a way to group existing LDAP, RADIUS, or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Using server groups, a subset of the configured server hosts can be specified and use them for a particular service. For example, server groups allows R1 and R2 to be defined as separate server groups, and T1 and T2 as separate server groups. This allows either R1 and T1 to be specified in the method list or R2 and T2 in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, authorization--the second host entry configured acts as fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers. See the Configuring LDAP, Configuring RADIUS or Configuring TACACS+ feature modules.

AAA Authorization Types

Cisco IOS software supports five different types of authorization:

- **Auth-proxy** --Applies specific security policies on a per-user basis. See the Configuring Authentication Proxy sectionfor more information about where to find authentication proxy configuration documentation.

- **Commands** --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC** --Applies to the attributes associated with a user EXEC terminal session.
- **Network** --Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access** --Applies to reverse Telnet sessions.
- Configuration--Applies to downloading configurations from the AAA server.
- IP Mobile--Applies to authorization for IP mobile services.

Authorization Types

Named authorization method lists are specific to the indicated type of authorization.

To create a method list to enable authorization that applies specific security policies on a per-user basis, use the **auth-proxy** keyword.

To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARAP), use the **network** keyword.

To create a method list to enable authorization to determine if a user is allowed to run an EXEC shell, use the **exec** keyword.

To create a method list to enable authorization for specific, individual EXEC commands associated with a specific privilege level, use the **commands**keyword. (This allows all commands associated with a specified command level from 0 to 15 to be authorized.)

To create a method list to enable authorization for reverse Telnet functions, use the **reverse-access** keyword.

Authorization Attribute-Value Pairs

RADIUS and TACACS+ authorization both define specific rights for users by processing attributes, which are stored in a database on the security server. For both RADIUS and TACACS+, attributes are defined on the security server, associated with the user, and sent to the network access server where they are applied to the user’s connection.

See the RADIUS Attributes and TACACS+ Attribute-Value Pairs sections for more information about supported RADIUS attributes and TACACS+ attribute-value pair documentation.

How to Configure Authorization

See Authorization Configuration Examples for more information.

Configuring AAA Authorization Using Named Method Lists

Perform this task to configure AAA authorization using named method lists:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
4. Do one of the following:
   - **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
   - **interface** *interface-type interface-number*
5. Do one of the following:
   - **authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}
   - **ppp authorization** {**default** | *list-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	**aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization auth-proxy default`	Creates an authorization method list for a particular authorization type and enable authorization.
Step 4	Do one of the following: • **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • **interface** *interface-type interface-number*	Enters the line configuration mode for the lines to which the authorization method list is applied. Alternately, enters the interface configuration mode for the interfaces to which the authorization method list is applied.

	Command or Action	Purpose

	Example:
	`Router(config)# line aux 0`
	Example:
	`Router(config)# interface interface-type interface-number`	

Step 5	Do one of the following:
	• **authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}
	• **ppp authorization** {**default** | *list-name*}
	Example:
	`Router(config-line)# authorization arap default`
	Example:
	`Router(config-line)# ppp authorization default`
		Applies the authorization list to a line or set of lines.
		Or
		Applies the authorization list to an interface or set of interfaces.

Disabling Authorization for Global Configuration Commands

The **aaa authorization** command with the keyword **commands** attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using **no aaa authorization config-commands** stops the network access server from attempting configuration command authorization.

To disable AAA authorization for all global configuration commands, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **no aaa authorization config-commands**	Disables authorization for all global configuration commands.

To disable AAA authorization on the console, use the following command in global configuration mode:

Note AAA authorization is disabled on the console by default. If AAA authorization is enabled on the console, disable it by configuring the **no aaa authorization console** command during the AAA configuration stage. AAA should be disabled on the console for user authentication.

Command	Purpose
`Device(config)#` **no aaa authorization console**	Disables authorization on the console.

Configuring Authorization for Reverse Telnet

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, a network access server is logged into and then Telnet is used to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction--from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to Telnet to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. Reverse Telnet authorization provides an additional (optional) level of security by requiring authorization in addition to authentication. When enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Reverse Telnet authorization offers the following benefits:

- An additional level of protection by ensuring that users engaged in reverse Telnet activities are indeed authorized to access a specific asynchronous port using reverse Telnet.
- An alternative method (other than access lists) to manage reverse Telnet authorization.

To configure a network access server to request authorization information from a TACACS+ or RADIUS server before allowing a user to establish a reverse Telnet session, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **aaa authorization reverse-access** *method1* [*method2* ...]	Configures the network access server to request authorization information before allowing a user to establish a reverse Telnet session.

This feature enables the network access server to request reverse Telnet authorization information from the security server, whether RADIUS or TACACS+. The specific reverse Telnet privileges for the user on the security server itself must be configured.

Authorization Configuration Examples

Named Method List Configuration Example

The following example shows how to configure a Cisco AS5300 (enabled for AAA and communication with a RADIUS security server) for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network scoobee group radius local
aaa accounting network charley start-stop group radius
username root password ALongPassword
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization scoobee
 ppp accounting charley
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines a method list, admins, for login authentication.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network scoobee group radius local** command defines the network authorization method list named scoobee, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.
- The **aaa accounting network charley start-stop group radius**command defines the network accounting method list named charley, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server host** command defines the name of the RADIUS server host.

- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication chap dialins**command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.
- The **ppp authorization scoobee**command applies the scoobee network authorization method list to the specified interfaces.
- The **ppp accounting charley**command applies the charley network accounting method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the admins method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

TACACS Authorization Examples

The following examples show how to use a TACACS+ server to authorize the use of network services, including PPP and ARA. If the TACACS+ server is not available or an error occurs during the authorization process, the fallback method (none) is to grant all authorization requests:

```
aaa authorization network default group tacacs+ none
```

The following example shows how to allow network authorization using TACACS+:

```
aaa authorization network default group tacacs+
```

The following example shows how to provide the same authorization, but it also creates address pools called mci and att:

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

These address pools can then be selected by the TACACS daemon. A sample configuration of the daemon follows:

```
user = mci_customer1 {
    login = cleartext “some password”
    service = ppp protocol = ip {
        addr-pool=mci
    }
}
user = att_customer1 {
    login = cleartext "some other password"
    service = ppp protocol = ip {
        addr-pool=att
     }
```

RADIUS Authorization Example

The following example shows how to configure the router to authorize using RADIUS:

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

The lines in this sample RADIUS authorization configuration are defined as follows:

- The **aaa authorization exec default group radius if-authenticated** command configures the network access server to contact the RADIUS server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the RADIUS server, the fallback method is to permit the CLI to start, provided the user has been properly authenticated.

The RADIUS information returned may be used to specify an autocommand or a connection access list be applied to this connection.

- The **aaa authorization network default group radius** command configures network authorization through RADIUS. This can be used to govern address assignment, the application of access lists, and various other per-user quantities.

Note Since no fallback method is specified in this example, authorization fails if, for any reason, there is no response from the RADIUS server.

LDAP Authorization Example

The following example shows how to configure the router to authorize using LDAP:

```
aaa new-model
aaa authorization exec default group ldap if-authenticated
aaa authorization network default group ldap
```

The lines in this sample RADIUS authorization configuration are defined as follows:

- The **aaa authorization exec default group ldap if-authenticated** command configures the network access server to contact the LDAP server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the LDAP server, the fallback method is to permit the CLI to start, provided the user has been properly authenticated.

The LDAP information returned may be used to specify an autocommand or a connection access list be applied to this connection.

The **aaa authorization network default group ldap** command configures network authorization through LDAP. This command can be used to govern address assignment, the application of access lists, and various other per-user quantities.

Reverse Telnet Authorization Examples

The following examples show how to cause the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs+** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host** command identifies the TACACS+ server.
- The **tacacs-server timeout**command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example shows how to configure a generic TACACS+ server to grant a user, pat, reverse Telnet access to port tty2 on the network access server named “maple” and to port tty5 on the network access server named “oak”:

```
user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
```

Note In this example, “maple” and “oak” are the configured host names of network access servers, not DNS names or alias.

The following example shows how to configure the TACACS+ server (CiscoSecure) to grant a user named pat reverse Telnet access:

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
default cmd=permit
}
```

```
service=raccess {
allow “c2511e0” “tty1” “.*”
refuse “.*” “.*” “.*”
password = clear “goaway”
```

Note CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(*x*) through version 2.2(1).

An empty “service=raccess {}” clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no “service=raccess” clause exists, the user is denied access to any port for reverse Telnet.

The following example shows how to cause the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example shows how to send a request to the RADIUS server to grant a user named “pat” reverse Telnet access at port tty2 on the network access server named “maple”:

```
Username = “pat”
Password = “goaway”
User-Service-Type = Shell-User
cisco-avpair = “raccess:port#1=maple/tty2”
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={*nasname* }/{*tty number* }" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

Additional References

The following sections provide references related to the Authorization feature.

Related Documents

Related Topic	Document Title
Authorization Commands	*Cisco IOS Security Command Reference*
RADIUS	Configuring RADIUS feature module.
LDAP	Configuring RADIUS feature Module.
RADIUS attributes	RADIUS Attributes Overview and RADIUS IETF Attributes feature module.
TACACS+	Configuring TACACS+ feature module.
TACACS+ Attribute-Value Pairs	TACACS+ Attribute-Value Pairs feature module.
Authentication	Configuring Authentication feature module.
Authentication Proxy	Configuring Authentication Proxy feature module.

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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

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

Feature Information for Configuring Authorization

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 Configuring Authorization

Feature Name	Releases	Feature Information
Configuring Authorization	10.0 Cisco IOS XE Release 2.1	The AAA authorization feature is used to determine what a user can and cannot do. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user is granted access to a requested service only if the information in the user profile allows it. This feature was introduced in Cisco IOS Release 10.0. This feature was introduced on Cisco ASR 1000 Series Routers.

Feature Name	Releases	Feature Information
LDAP integration with Active Directory	15.1(1)T	LDAP is a standard-based protocol used to access directories. It is based on client server model similar to RADIUS. LDAP is deployed on Cisco devices to send authentication requests to a central LDAP server that contains all user authentication and network service access information. This feature provides authentication and authorization support for AAA. The following command was modified: **aaa authorization**

CHAPTER 16

Configuring Accounting

The AAA Accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA Accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

- Finding Feature Information, page 223
- Prerequisites for Configuring Accounting, page 223
- Restrictions for Configuring Accounting, page 224
- Information About Configuring Accounting, page 224
- How to Configure AAA Accounting, page 239
- Configuration Examples for AAA Accounting, page 250
- Additional References, page 253
- Feature Information for Configuring Accounting, 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.

Prerequisites for Configuring Accounting

The following tasks must be performed before configuring accounting using named method lists:

- Enable AAA on the network access server by using the **aaa new-model**command in global configuration mode.
- Define the characteristics of the RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued. For more information about configuring the Cisco network access server to communicate with the RADIUS security server, see the Configuring RADIUS module. For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the Configuring TACACS+ module.

Restrictions for Configuring Accounting

- Accounting information can be sent simultaneously to a maximum of only four AAA servers.
- For Service Selection Gateway (SSG) systems, the **aaa accounting network broadcast** command broadcasts only **start-stop** accounting records. If interim accounting records are configured using the **ssg accounting interval** command, the interim accounting records are sent only to the configured default RADIUS server.

Information About Configuring Accounting

Named Method Lists for Accounting

Similar to authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow particular security protocol to be designated and used on specific lines or interfaces for accounting services. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists allow one or more security protocols to be designated and used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.

Note The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle--meaning that the security server responds by denying the user access--the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports seven different types of accounting:

- **Network** --Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

- **EXEC** --Provides information about user EXEC terminal sessions of the network access server.
- **Commands** --Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Connection** --Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
- **System** --Provides information about system-level events.
- **Resource** --Provides "start" and "stop" records for calls that have passed user authentication, and provides "stop" records for calls that fail to authenticate.
- **VRRS** --Provides information about Virtual Router Redundancy Service (VRRS).

Note System accounting does not use named accounting lists; only the default list for system accounting can be defined.

Once again, when a named method list is created, a particular list of accounting methods for the indicated accounting type are defined.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named "default"). If the **aaa accounting** command for a particular accounting type is issued without specifying a named method list, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined (A defined method list overrides the default method list). If no default method list is defined, then no accounting takes place.

This section includes the following subsections:

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 comprise the group of RADIUS servers. T1 and T2 comprise the group of TACACS+ servers.

Cisco IOS software, RADIUS and TACACS+ server configurations are global. A subset of the configured server hosts can be specified using server groups. These server groups can be used for a particular service. For example, server groups allow R1 and R2 to be defined as separate server groups (SG1 and SG2), and T1 and T2 as separate server groups (SG3 and SG4). This means either R1 and T1 (SG1 and SG3) or R2 and T2 (SG2 and SG4) can be specified in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server from the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, accounting--the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services (The RADIUS host entries are tried in the order in which they are configured).

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see the “Configuring RADIUS” or “Configuring TACACS+” module in the Cisco IOS Security Configuration Guide: Securing User Services .

AAA Accounting Methods

The Cisco IOS software supports the following two methods for accounting:

- TACACS+--The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.
- RADIUS--The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Note With CSCuc32663, passwords and accounting logs are masked before being sent to the TACACS+ or RADIUS security servers. Use the **aaa accounting commands visible-keys** command to send unmasked information to the TACACS+ or RADIUS security servers.

Accounting Record Types

For minimal accounting, use the **stop-only** keyword, which instructs the specified method (**RADIUS** or **TACACS+**) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the **start-stop** keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the **none** keyword.

Accounting Methods

The table below lists the supported accounting methods.

Table 29: AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for accounting.
group tacacs+	Uses the list of all TACACS+ servers for accounting.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

The method argument refers to the actual method the authentication algorithm tries. Additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all other methods return an error, specify additional methods in the command. For example, to create a method list named acct_tac1 that specifies RADIUS as the backup method of authentication in the event that TACACS+ authentication returns an error, enter the following command:

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

To create a default list that is used when a named list is not specified in the **aaa accounting**command, use the **default** keyword followed by the methods that are wanted to be used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa accounting network default stop-only group radius
```

AAA Accounting supports the following methods:

- **group tacacs** --To have the network access server send accounting information to a TACACS+ security server, use the **group tacacs+** *method* keyword.
- **group radius** --To have the network access server send accounting information to a RADIUS security server, use the **group radius** *method* keyword.

Note Accounting method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for accounting applies.

- **group** *group-name* --To specify a subset of RADIUS or TACACS+ servers to use as the accounting method, use the **aaa accounting**command with the **group** *group-name* method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group loginrad**:

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the **group loginrad**.

To specify **group loginrad** as the method of network accounting when no other method list has been defined, enter the following command:

```
aaa accounting network default start-stop group loginrad
```

Before a group name can be used as the accounting method, communication with the RADIUS or TACACS+ security server must be enabled.

AAA Accounting Types

Network Accounting

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through an EXEC session:

```
Wed Jun 27 04:44:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:45:00 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:47:46 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Input-Octets = 3075
        Acct-Output-Octets = 167
        Acct-Input-Packets = 39
        Acct-Output-Packets = 9
        Acct-Session-Time = 171
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:48:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “408”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who first started an EXEC session:

```
Wed Jun 27 04:00:35 2001 172.16.25.15    username1   tty4    562/4327528     starttask_id=28
      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15    username1   tty4 562/4327528     starttask_id=30
     addr=10.1.1.1   service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15    username1   tty4    408/4327528     update
task_id=30      addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=30
       addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1   bytes_in=2844
  bytes_out=1682  paks_in=36      paks_out=24     elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=28
       service=shell   elapsed_time=57
```

Note The precise format of accounting packets records may vary depending on the security server daemon.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:30:52 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 3
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000B”
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:36:49 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 3
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000B”
        Framed-Protocol = PPP
        Framed-IP-Address = “10.1.1.1”
        Acct-Input-Octets = 8630
        Acct-Output-Octets = 5722
        Acct-Input-Packets = 94
        Acct-Output-Packets = 64
        Acct-Session-Time = 357
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:02:19 2001 172.16.25.15    username1   Async5  562/4327528     starttask_id=35
      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15    username1   Async5  562/4327528     update
task_id=35      service=ppp     protocol=ip     addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15    username1   Async5  562/4327528     stoptask_id=35
       service=ppp     protocol=ip     addr=10.1.1.2   bytes_in=3366   bytes_out=2149
  paks_in=42      paks_out=28     elapsed_time=164
```

EXEC Accounting

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

```
Wed Jun 27 04:26:23 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 1
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329483”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “00000006”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:27:25 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 1
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329483”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “00000006”
        Acct-Session-Time = 62
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

```
Wed Jun 27 03:46:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=2       service=shell
Wed Jun 27 04:08:55 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=2       service=shell   elapsed_time=1354
```

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

```
Wed Jun 27 04:48:32 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 26
        User-Name = “username1”
        Caller-ID = “10.68.202.158”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “00000010”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:48:46 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 26
        User-Name = “username1”
        Caller-ID = “10.68.202.158”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “00000010”
        Acct-Session-Time = 14
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

```
Wed Jun 27 04:06:53 2001        172.16.25.15    username1   tty26   10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001        172.16.25.15    username1   tty26   10.68.202.158
stoptask_id=41       service=shell   elapsed_time=9
```

Command Accounting

Command accounting provides information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.

The following example shows the information contained in a TACACS+ command accounting record for privilege level 1:

```
Wed Jun 27 03:46:47 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=3       service=shell   priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=4       service=shell   priv-lvl=1      cmd=show interfaces Ethernet 0
<cr>
Wed Jun 27 03:47:03 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=5       service=shell   priv-lvl=1      cmd=show ip route <cr>
```

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

```
Wed Jun 27 03:47:17 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=6       service=shell   priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=7       service=shell   priv-lvl=15     cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop    task_id=8      service=shell   priv-lvl=15    cmd=ip address 10.1.1.1 255.255.255.0
 <cr>
```

Note The Cisco implementation of RADIUS does not support command accounting.

Connection Accounting

Connection accounting provides information about all outbound connections made from the network access server such as Telnet, LAT, TN3270, PAD, and rlogin.

The following example shows the information contained in a RADIUS connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 04:28:00 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 2
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329477”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = “00000008”
        Login-Service = Telnet
        Login-IP-Host = “10.68.202.158”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:28:39 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 2
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329477”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = “00000008”
        Login-Service = Telnet
        Login-IP-Host = “10.68.202.158”
        Acct-Input-Octets = 10774
        Acct-Output-Octets = 112
        Acct-Input-Packets = 91
        Acct-Output-Packets = 99
        Acct-Session-Time = 39
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 03:47:43 2001        172.16.25.15    username1   tty3    5622329430/4327528
start   task_id=10     service=connection     protocol=telnet addr=10.68.202.158 cmd=telnet
 username1-sun
Wed Jun 27 03:48:38 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop    task_id=10     service=connection     protocol=telnet addr=10.68.202.158 cmd=telnet
 username1-sun    bytes_in=4467  bytes_out=96    paks_in=61     paks_out=72 elapsed_time=55
```

The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 2
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329477”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = “0000000A”
        Login-Service = Rlogin
        Login-IP-Host = “10.68.202.158”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:30:09 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 2
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329477”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = “0000000A”
        Login-Service = Rlogin
        Login-IP-Host = “10.68.202.158”
        Acct-Input-Octets = 18686
        Acct-Output-Octets = 86
        Acct-Input-Packets = 90
        Acct-Output-Packets = 68
        Acct-Session-Time = 22
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 03:48:46 2001        172.16.25.15    username1   tty3    5622329430/4327528
start   task_id=12     service=connection     protocol=rlogin addr=10.68.202.158 cmd=rlogin
 username1-sun /user username1
Wed Jun 27 03:51:37 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop    task_id=12     service=connection     protocol=rlogin addr=10.68.202.158 cmd=rlogin
 username1-sun /user username1 bytes_in=659926 bytes_out=138   paks_in=2378    paks_
out=1251        elapsed_time=171
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound LAT connection:

```
Wed Jun 27 03:53:06 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
VAX
Wed Jun 27 03:54:15 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
VAX  bytes_in=0      bytes_out=0     paks_in=0      paks_out=0      elapsed_time=6
```

System Accounting

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

The following accounting record shows a typical TACACS+ system accounting record server indicating that AAA Accounting has been turned off:

```
Wed Jun 27 03:55:32 2001        172.16.25.15    unknown unknown unknown start   task_id=25
   service=system  event=sys_acct  reason=reconfigure
```

Note The precise format of accounting packets records may vary depending on the TACACS+ daemon.

The following accounting record shows a TACACS+ system accounting record indicating that AAA Accounting has been turned on:

```
Wed Jun 27 03:55:22 2001        172.16.25.15    unknown unknown unknown stop    task_id=23
   service=system  event=sys_acct  reason=reconfigure
```

Additional tasks for measuring system resources are covered in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the Configuring IP Services chapter in the *CiscoIOS Application Services Configuration Guide* .

Resource Accounting

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. The additional feature of generating “stop” records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

This section includes the following subsections:

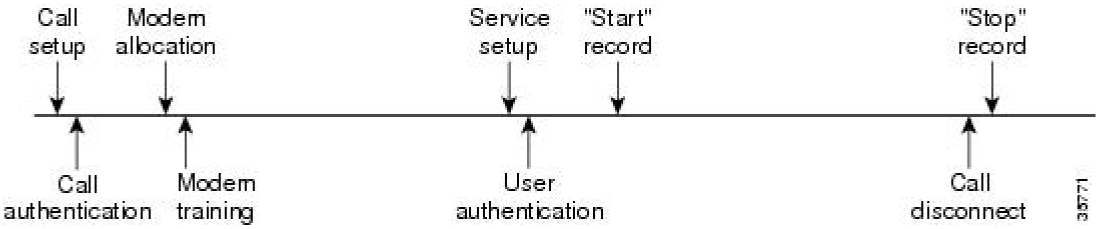
AAA Resource Failure Stop Accounting

Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This functionality generates a “stop” accounting record for any calls that do not reach user authentication; “stop” records are generated from the moment of call setup. All calls that pass user authentication behave as they did before; that is, no additional accounting records are seen.

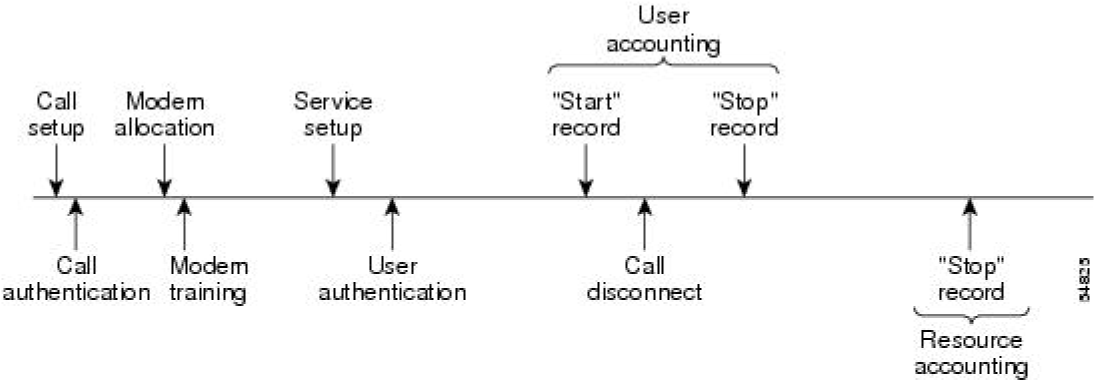
The figure below illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

Figure 10: Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled



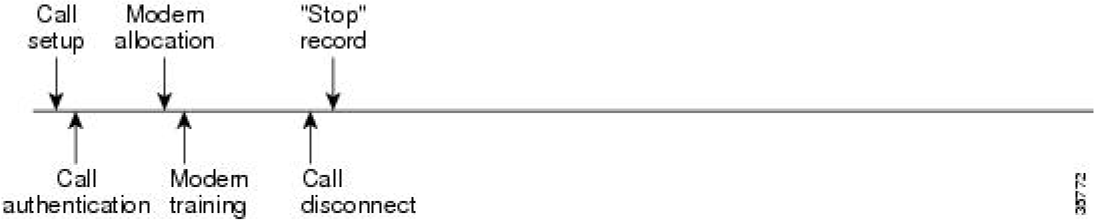
The figure below illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

Figure 11: Modem Dial-In Call Setup Sequence With Normal Flow and WIth Resource Failure Stop Accounting Enabled



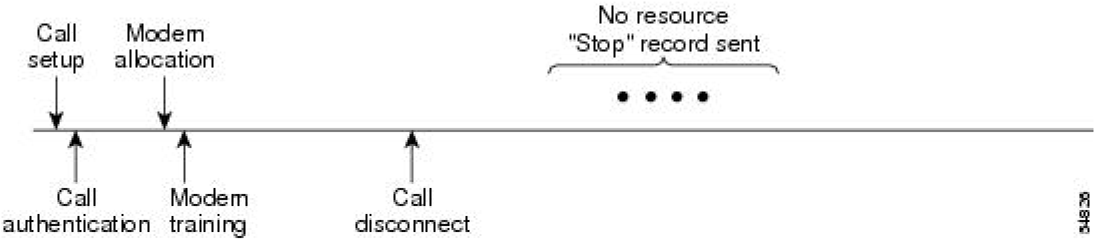
The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

Figure 12: Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and With Resource Failure Stop Accounting Enabled



The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and without AAA resource failure stop accounting enabled.

Figure 13: Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and Without Resource Failure Stop Accounting Enabled



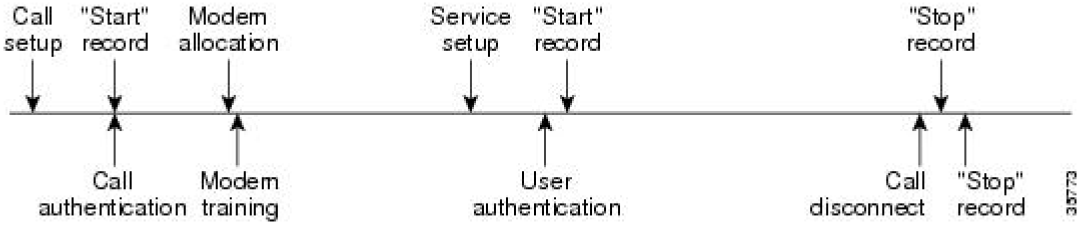
AAA Resource Accounting for Start-Stop Records

AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

With this feature, a call setup and call disconnect “start-stop” accounting record tracks the progress of the resource connection to the device. A separate user authentication “start-stop” accounting record tracks the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

The figure below illustrates a call setup sequence with AAA resource start-stop accounting enabled.

Figure 14: Modem Dial-In Call Setup Sequence With Resource Start-Stop Accounting Enabled



VRRS Accounting

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client. The VRRS multiclient service provides a consistent interface with FHRP protocols by abstracting over several FHRPs and providing an idealized view of their state. VRRS manages data updates, allowing interested clients to register in one place and receive updates for named FHRP groups or all registered FHRP groups.

Virtual Router Redundancy Protocol (VRRP) is an FHRP that acts as a server that pushes FHRP status information out to all registered VRRS clients. Clients obtain status on essential information provided by the FHRP, including current and previous redundancy states, active and inactive L3 and L2 addresses, and, in some cases, information about other redundant gateways in the network. Clients can use this information to provide stateless and stateful redundancy information to clients and protocols.

VRRS Accounting Plug-in

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state. The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode.

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state.

The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode. The VRRS Accounting plug-in sends an accounting-on message to RADIUS when a VRRS group transitions to the master state, and it sends an accounting-off message when a VRRS group transitions from the master state.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, VRRS Name
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Time
- Attribute 44, Acct-Session-Id

Accounting messages for a VRRS transitioning out of master state are sent after all PPPoE accounting stop messages for sessions that are part of that VRRS.

AAA Accounting Enhancements

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the **show radius statistics** command)
- Status of servers providing AAA functions
- Identities of external AAA servers
- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call

Note This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

Table 30: SNMP End-User Data Objects

SessionId	The session identification used by the AAA Accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).
UserId	The user login ID or zero-length string if a login is unavailable.
IpAddr	The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.
IdleTime	The elapsed time in seconds that the session has been idle.
Disconnect	The session termination object used to disconnect the given client.
CallId	The entry index corresponding to this accounting session that the Call Tracker record stored.

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

Table 31: SNMP AAA Session Summary

ActiveTableEntries	Number of sessions currently active.
ActiveTableHighWaterMark	Maximum number of sessions present at once since last system reinstallation.
TotalSessions	Total number of sessions since last system reinstallation.
DisconnectedSessions	Total number of sessions that have been disconnected using since last system reinstallation.

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ AV pairs or RADIUS attributes, depending on which security method is implemented.

How to Configure AAA Accounting

Configuring AAA Accounting Using Named Method Lists

To configure AAA Accounting using named method lists, perform the following steps:

Note System accounting does not use named method lists. For system accounting, define only the default method list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]
4. Do one of the following:
    - **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
    -
    -
    -
    - **interface** *interface-type interface-number*
5. Do one of the following:
    - **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}
    -
    -
    -
    - **ppp accounting**{**default** | *list-name*}
6. **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 accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]] **Example:** `Device(config)# aaa accounting system default start-stop`	Creates an accounting method list and enables accounting. The argument *list-name* is a character string used to name the created list.
Step 4	Do one of the following: • **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • • • • **interface** *interface-type interface-number* **Example:** `Device(config)# line aux line1`	Enters the line configuration mode for the lines to which the accounting method list is applied. or Enters the interface configuration mode for the interfaces to which the accounting method list is applied.
Step 5	Do one of the following: • **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} • • • • **ppp accounting**{**default** | *list-name*} **Example:** `Device(config-line)# accounting arap default`	Applies the accounting method list to a line or set of lines. or Applies the accounting method list to an interface or set of interfaces.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Device(config-line)# end`
		(Optional) Exits line configuration mode and returns to global configuration mode.

What to Do Next

This section includes the following subsection:

Configuring RADIUS System Accounting

Perform this task to configure RADIUS system accounting on the global RADIUS server:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server accounting system host-config**
5. **aaa group server radius** *server-name*
6. **server-private** {*host-name* | *ip-address*} **key** {[**0** *server-key* | **7** *server-key*] *server-key*
7. **accounting system host-config**
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.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA network security services.
Step 4	**radius-server accounting system host-config** **Example:** `Device(config)# radius-server accounting system host-config`	Enables the router to send a system accounting record for the addition and deletion of a RADIUS server.
Step 5	**aaa group server radius** *server-name* **Example:** `Device(config)# aaa group server radius radgroup1`	Adds the RADIUS server and enters server-group configuration mode. - The *server-name* argument specifies the RADIUS server group name.
Step 6	**server-private** {*host-name* | *ip-address*} **key** {[**0** *server-key* | **7** *server-key*] *server-key* **Example:** `Device(config-sg-radius)# server-private 172.16.1.11 key cisco`	Enters the hostname or IP address of the RADIUS server and hidden server key. - (Optional) **0** with the *server-key*argument specifies that an unencrypted (cleartext) hidden server key follows. - (Optional) **7** with the *server-key* argument specifies that an encrypted hidden server key follows. - The *server-key* argument specifies the hidden server key. If the *server-key*argument is configured without the **0** or **7** preceding it, it is unencrypted. **Note** Once the **server-private** command is configured, RADIUS system accounting is enabled.
Step 7	**accounting system host-config** **Example:** `Device(config-sg-radius)# accounting system host-config`	Enables the generation of system accounting records for private server hosts when they are added or deleted.

Step 8	**end**
	Example:
	`Device(config-sg-radius)# end`
		Exits server-group (config-sg-radius) configuration mode and returns to global configuration mode.

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA Accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the **aaa authentication login** *method-list* **none** command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting suppress null-username**	Prevents accounting records from being generated for users whose username string is NULL.

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting update** [**newinfo**] [**periodic**] *number*	Enables periodic interim accounting records to be sent to the accounting server.

When the **aaa accounting update**commandis activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the *number* argument. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.

Caution Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

Generating Accounting Records for Failed Login or Session

When AAA Accounting is activated, the Cisco IOS software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting send stop-record authentication failure**	Generates "stop" records for users who fail to authenticate at login or during session negotiation using PPP.
Device(config)# **aaa accounting send stop-record always**	Sends authentication, authorization, and accounting (AAA) stop records regardless of whether a start record was sent earlier.

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, you can specify the NETWORK records to be generated before EXEC-stop records. In cases such as billing customers for specific services, it can be desirable to keep network start and stop records together, essentially "nesting" them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

To nest accounting records for user sessions, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting nested**	Nests network accounting records.

Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting resource** *method-list* **stop-failure group** *server-group*	Generates a “stop” record for any calls that do not reach user authentication. **Note** Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 223 section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the Configuring SNMP Support chapter in the Cisco IOS Network Management Configuration Guide.

Configuring AAA Resource Accounting for Start-Stop Records

To enable full resource accounting for start-stop records, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting resource** *method-list* **start-stop group** *server-group*	Supports the ability to send a “start” record at each call setup. followed with a corresponding “stop” record at the call disconnect. **Note** Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 223 section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the Configuring SNMP Support chapter in the Cisco IOS Network Management Configuration Guide. **Note**

Configuring AAA Broadcast Accounting

To configure AAA broadcast accounting, use the aaa accounting command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] *method1* [*method2*. . .]	Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Configuring Per-DNIS AAA Broadcast Accounting

To configure AAA broadcast accounting per DNIS, use the **aaa dnis map accounting network**command in global configuration mode:

Command	Purpose
`Device(config)#` **aaa dnis map** *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] *method1* [*method2*. . .]	Allows per-DNIS accounting configuration. This command has precedence over the global **aaa accounting** command. Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Configuring AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP. For information on SNMP, see the chapter Configuring SNMP Support in the Cisco IOS Network Management Configuration Guide.
- Configure AAA.
- Define the RADIUS or TACACS+ server characteristics.

Note Overusing SNMP can affect the overall system performance; therefore, normal network management performance must be considered when this feature is used.

To configure AAA session MIB, use the following command in global configuration mode

SUMMARY STEPS

1. Device(config)# **aaa session-mib disconnect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **aaa session-mib disconnect**	Monitors and terminates authenticated client connections using SNMP. To terminate the call, the **disconnect** keyword must be used.

Configuring VRRS Accounting

Perform the following task to configure Virtual Router Redundancy Service (VRRS) to send AAA Accounting messages to the AAA server:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting vrrs** {**default** | *list-name*} **start-stop** *method1* [*method2...*]
4. **aaa attribute list** *list-name*
5. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*]
6. **exit**
7. **vrrs** *vrrs-group-name*
8. **accounting delay** *seconds*
9. **accounting method** {**default** | *accounting-method-list*}
10. **exit**

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.

	Command or Action	Purpose
Step 3	**aaa accounting vrrs** {**default** | *list-name*} **start-stop** *method1* [*method2...*] **Example:** `Device(config)# aaa accounting vrrs default start-stop`	Enables AAA accounting for VRRS.
Step 4	**aaa attribute list** *list-name* **Example:** `Device(config)# aaa attribute list list1`	Defines a AAA attribute list locally on a router, and enters attribute list configuration mode.
Step 5	**attribute type** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*] **Example:** `Device(config-attr-list)# attribute type example 1`	Defines an attribute type that is to be added to an attribute list locally on a router.
Step 6	**exit** **Example:** `Device(config-attr-list)# exit`	Exits attribute list configuration mode and returns to global configuration mode.
Step 7	**vrrs** *vrrs-group-name* **Example:** `Device(config)# vrrs vrrs1`	(Optional) Defines a VRRP group and configures parameters for the VRRS group, and enters VRRS configuration mode.
Step 8	**accounting delay** *seconds* **Example:** `Device(config-vrrs)# accounting delay 10`	(Optional) Specifies the delay time for sending accounting-off messages to the VRRS.

Step 9	**accounting method** {**default** | *accounting-method-list*}
	Example:
	`Device(config-vrrs)# accounting method default`
		(Optional) Enables VRRS accounting for a VRRP group.

Step 10	**exit** **Example:** `Device(config-vrrs)# exit`	Exits VRRS configuration mode.

Establishing a Session with a Router if the AAA Server is Unreachable

To establish a console or telnet session with a router if the AAA server is unreachable, use the following command in global configuration mode:

Command	Purpose
`Device(config)#` **no aaa accounting system guarantee-first**	The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, the **no aaa accounting system guarantee-first** command can be used.

Note Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users currently logged in, use the following command in privileged EXEC mode:

Command	Purpose
`Device#` **show accounting**	Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

Command	Purpose
`Device#` **debug aaa accounting**	Displays information on accountable events as they occur.

Configuration Examples for AAA Accounting

Example Configuring Named Method List

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization blue1
 ppp accounting red1
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines a method list “admins”, for login authentication.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins”, which specifies that first RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network blue1 group radius local** command defines the network authorization method list named “blue1”, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.
- The **aaa accounting network red1 start-stop group radius group tacacs+**command defines the network accounting method list named red1, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP. If the RADIUS server fails to respond, accounting services are handled by a TACACS+ server.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **tacacs-server host** command defines the name of the TACACS+ server host.

- The **tacacs-server key** command defines the shared secret text string between the network access server and the TACACS+ server host.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication chap dialins**command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the "dialins" method list to the specified interfaces.
- The **ppp authorization blue1**command applies the blue1 network authorization method list to the specified interfaces.
- The **ppp accounting red1**command applies the red1 network accounting method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the admins method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

The **show accounting**command yields the following output for the preceding configuration:

```
Active Accounted actions on tty1, User username2 Priv 1
 Task ID 5, Network Accounting record, 00:00:52 Elapsed
 task_id=5 service=ppp protocol=ip address=10.0.0.98
```

The table below describes the fields contained in the preceding output.

Table 32: show accounting Field Descriptions

Field	Description
Active Accounted actions on	Terminal line or interface name user with which the user logged in.
User	User's ID.
Priv	User's privilege level.
Task ID	Unique identifier for each accounting session.

Field	Description
Accounting record	Type of accounting session.
Elapsed	Length of time (hh:mm:ss) for this session type.
attribute=value	AV pairs associated with this accounting session.

Example Configuring AAA Resource Accounting

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method
 to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all start-stop
 accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
 use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

Example Configuring AAA Broadcast Accounting

The following example shows how to turn on broadcast accounting using the global **aaa accounting** command:

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

The **broadcast** keyword causes “start” and “stop” accounting records for network connections to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

Example Configuring Per-DNIS AAA Broadcast Accounting

The following example shows how to turn on per DNIS broadcast accounting using the global **aaa dnis map accounting network**command:

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

The **broadcast** keyword causes “start” and “stop” accounting records for network connection calls having DNIS number 7777 to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

Example AAA Session MIB

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for PPP users:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

Example Configuring VRRS Accounting

The following example shows how to configure VRRS to send AAA Accounting messages to the AAA server:

```
Device# configure terminal
Device(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Device(config)# aaa attribute list vrrp-1-attr
Device(config-attr-list)# attribute type account-delay 10
Device(config-attr-list)# exit
Device(config)# vrrs vrrp-group-1
Device(config-vrrs)# accounting delay 10
Device(config-vrrs)# accounting method vrrp-mlist-1
Device(config-vrrs)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Authorization	Configuring Authorization module

Related Topic	Document Title
Authentication	Configuring Authentication module
Accounting Commands	*Cisco IOS Security 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, 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
RFC 2903	*Generic AAA Architecture*
RFC 2904	*AAA Authorization Framework*
RFC 2906	*AAA Authorization Requirements*
RFC 2989	*Criteria for Evaluating AAA Protocols for Network Access*

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 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 33: Feature Information for Configuring Accounting

Feature Name	Releases	Feature Information
AAA Broadcast Accounting	12.2 12.2S 12.2SB 12.2SX 12.4T	AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously.
AAA Resource Accounting for Start-Stop Records	12.2 12.2S 12.2SB 12.2SX 12.4T	AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

Feature Name	Releases	Feature Information
AAA Session MIB	12.2 12.2S 12.2SB 12.2SX 12.4T	The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using SNMP. The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server.
AAA: IPv6 Accounting Delay Enhancements	15.1(1)S	VRRS provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client.

CHAPTER 17

AAABroadcastAccounting-MandatoryResponse Support

The AAA Broadcast Accounting--Mandatory Response Support feature provides a mechanism to support broadcast accounting under each server group through a Gateway GPRS Support Node (GGSN), which acts as a gateway between a General Packet Radio Service (GPRS) wireless data network and other networks such as the Internet or private networks.

- Finding Feature Information, page 257
- Prerequisites for AAA Broadcast Accounting-Mandatory Response Support, page 258
- Restrictions for AAA Broadcast Accounting-Mandatory Response Support, page 258
- Information About AAA Broadcast Accounting-Mandatory Response Support, page 258
- How AAA Broadcast Accounting is Supported for GGSN, page 259
- Configuration Examples for AAA Broadcast Accounting-Mandatory Response Support, page 262
- Additional References, page 263
- Feature Information for AAA Broadcast Accounting-Mandatory Response Support, page 264

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 AAA Broadcast Accounting-Mandatory Response Support

See the Cisco GGSN Release 8.0 Configuration Guide for more information on preparing for the GGSN configuration.

Restrictions for AAA Broadcast Accounting-Mandatory Response Support

Accounting information can be sent simultaneously to a maximum of ten AAA servers.

Information About AAA Broadcast Accounting-Mandatory Response Support

The AAA Broadcast Accounting--Mandatory Response Support feature allows up to 10 server groups (methods) to be configured in a method list. The following sections describe the types of AAA accounting used to support GGSN:

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple authentication, authorization, and accounting (AAA) servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of servers, which can be either RADIUS or TACACS+, and each server group can define its backup servers for failover independently of other groups. Failover is a process that may occur when more than one server has been defined within a server group. Failover refers to the process by which information is sent to the first server in a server group; if the first server is unavailable, the information is sent to the next server in the server group. This process continues until the information is successfully sent to one of the servers within the server group or until the list of available servers within the server group is exhausted.

Simultaneous Broadcast and Wait Accounting

With Cisco GGSN Release 8.0 and later releases, broadcast and wait accounting can be configured to work together. The wait accounting feature is configured at the Access Point Name (APN) level, while broadcast accounting is specified at the AAA method level.

Broadcast accounting sends start, stop, and interim accounting records to all the server groups that are configured in a method list. Within a server group, the accounting records are sent to the first active server. If the active server cannot be reached, the accounting records are sent to the next server within a group.

Additionally, one or more server groups within a method list can be configured as "mandatory," meaning that a server from that server group has to respond to the Accounting Start message. The APN-level wait accounting ensures that an accounting response has been received from all mandatory server groups before the packet data protocol (PDP) context is established.

The advantages of broadcast and wait accounting together include:

- Accounting records are sent to multiple servers, and once the entry is made, the user can start using different services.
- Records are sent to multiple AAA servers for redundancy purposes.
- A PDP context is established only when a valid Accounting Start record has been received by all essential servers, avoiding information loss.
- Broadcast records can be sent to as many as ten server groups within a method list.

When configuring broadcast and wait accounting together, note the following:

- Under the method list configuration, the **mandatory** keyword is available only if broadcast accounting is configured.
- If wait accounting is not required, broadcast accounting to all server groups is available without any mandatory groups defined.
- If you do not specify any mandatory server groups when configuring broadcast accounting, wait accounting will function as it does in Cisco GGSN Release 7.0 and earlier releases.
- Wait accounting does not apply to PPP PDP contexts.
- A PDP is successfully created only when a Accounting response is received from all the mandatory servers.
- The periodic timer starts when an Accounting Response (PDP creation) is received.

Note More than one server group can be defined as a mandatory server group in a method list.

How AAA Broadcast Accounting is Supported for GGSN

Configuring Broadcast and Wait Accounting on the GGSN

The tasks in this section describe how to configure broadcast and wait accounting on the GGSN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa accounting network** {*method-list-name* | **default**}
5. **action-type** {**start-stop** | **stop-only**| **none**}
6. **broadcast**
7. **group** *server-group* [**mandatory**]
8. **exit**
9. **gprs access-point-list** *list-name*
10. **access-point** *access-point-index*
11. **aaa-group accounting** *method-list name*
12. **gtp-response-message wait-accounting**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter the password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router# aaa new-model`	Enables new access control commands and functions (disables the old commands).

Step 4	**aaa accounting network** {*method-list-name* | **default**}
	Example:
	`Router(config)# aaa accounting network net1`
		Enables authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS and enters accounting method list mode.
		• The *method-list-name* argument is the named accounting list, which has a maximum of 31 characters. Any characters longer than the maximum are rejected.
		• The **default** keywork specifies the default accounting list.

Step 5	**action-type** {**start-stop** | **stop-only**| **none**}	Performs a type of action on accounting records. Possible values are:

	Command or Action	Purpose
	Example: `Router(cfg-acct-mlist)#action-type start-stop`	• **start-stop** --Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. • **stop-only** --Sends a "stop" accounting notice at the end of the requested user process. • **none** --Disables accounting services on this line or interface.
Step 6	**broadcast** **Example:** `Router(cfg-acct-mlist)#broadcast`	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
Step 7	**group** *server-group* [**mandatory**] **Example:** `Router(cfg-acct-mlist)#group server1`	Specifies the server group. Optionally, specify the **mandatory** keyword to define this server group as mandatory. If a server group is mandatory, a server from the server group must respond to the Accounting Start message. **Note** Up to ten server groups can be defined within a method list.
Step 8	**exit**	Exits accounting method list configuration mode.
Step 9	**gprs access-point-list** *list-name* **Example:** `Router(config)# gprs access-point-list public1`	Configures an access point list that you use to define public data network (PDN) access points on the GGSN and enters global configuration mode.
Step 10	**access-point** *access-point-index* **Example:** `Router(config-ap-list)# access-point 11`	Specifies an access point number and enters access point configuration mode.
Step 11	**aaa-group accounting** *method-list name* **Example:** `Router(config-access-point)#aaa-group accounting net1`	Specifies an accounting server group.
Step 12	**gtp-response-message wait-accounting** **Example:** `Router(config-access-point)# gtp-response-message wait-accounting`	Configures APN to wait for a RADIUS accounting response before sending a Create PDP Context response to the Serving GPRS Support Node (SGSN).

Configuration Examples for AAA Broadcast Accounting-Mandatory Response Support

AAA Broadcast Accounting-Mandatory Response Support Example

The following example globally configures the GGSN to wait for an accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN. The GGSN waits for a response for PDP context requests received across all access points, except access-point 1. RADIUS response message waiting has been overridden at access-point 1 by using the **no gtp response-message wait-accounting** command.

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.6.7.8 auth-port 1645 acct-port 1646
!
! Configures AAA authentication and authorization
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc
 action-type start-stop
 broadcast
 group SG1 mandatory
 group SG2
 group SG3 mandatory
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication abc
!
! Disables waiting for RADIUS response
! message at APN 1
!
  no gtp response-message wait-accounting
  exit
access-point 2
 access-mode non-transparent
 access-point-name www.pdn2.com
 aaa-group authentication abc
!
! Enables waiting for RADIUS response
! messages across all APNs (except APN 1)
!
gprs gtp response-message wait-accounting
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Additional References

The following sections provide references related to the AAA Broadcast Accounting--Mandatory Response Support feature.

Related Documents

Related Topic	Document Title
Preparation for the GGSN configuration	*Cisco GGSN Release 8.0 Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference Guide*
AAA features	*Cisco IOS Security Configuration Guide: Securing User Services*

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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for AAA Broadcast Accounting-Mandatory Response 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 34: Feature Information for AAA Broadcast Accounting--Mandatory Response Support

Feature Name	Releases	Feature Information
AAA Broadcast Accounting--Mandatory Response Support	12.4(22)T	The AAA Broadcast Accounting--Mandatory Response Support feature provides a mechanism to support broadcast accounting under each server group through a Gateway GPRS Support Node (GGSN), which acts as a gateway between a General Packet Radio Service (GPRS) wireless data network and other networks such as the Internet or private networks. In Release12.4(22)T, this feature was introduced. The following commands were introduced or modified: **aaa accounting network**, **aaa-group accounting**, **access-point**, **action-type**, **broadcast**, **gprs access-point-list**, **group**, **gtp-response-message wait-accounting**

CHAPTER 18

AAA Dead-Server Detection

The AAA Dead-Server Detection feature allows you to configure the criteria to be used to mark a RADIUS server as dead. If no criteria are explicitly configured, the criteria are computed dynamically on the basis of the number of outstanding transactions. Using this feature will result in less deadtime and quicker packet processing.

- Finding Feature Information, page 267
- Prerequisites for AAA Dead-Server Detection, page 267
- Restrictions for AAA Dead-Server Detection, page 268
- Information About AAA Dead-Server Detection, page 268
- How to Configure AAA Dead-Server Detection, page 268
- Configuration Examples for AAA Dead-Server Detection, page 271
- Additional References, page 271
- Feature Information for AAA Dead-Server Detection, page 273

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 AAA Dead-Server Detection

- You must have access to a RADIUS server.
- You should be familiar with configuring a RADIUS server.
- You should be familiar with configuring authentication, authorization, and accounting (AAA).

- Before a server can be marked as dead, you must first configure the **radius-server deadtime** command. If this command is not configured, even if the criteria are met for the server to be marked as dead, the server state will be the "up" state.

Restrictions for AAA Dead-Server Detection

- Original transmissions are not counted in the number of consecutive timeouts that must occur on the router before the server is marked as dead--only the number of retransmissions are counted.

Information About AAA Dead-Server Detection

Criteria for Marking a RADIUS Server As Dead

The AAA Dead-Server Detection feature allows you to determine the criteria that are used to mark a RADIUS server as dead. That is, you can configure the minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met.

In addition, you can configure the number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets are included in the number. Improperly constructed packets are counted as though they are timeouts. Only retransmissions are counted, not the initial transmission. (Each timeout causes one retransmission to be sent.)

Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The RADIUS dead-server detection configuration will result in the prompt detection of RADIUS servers that have stopped responding. This configuration will also result in the avoidance of servers being improperly marked as dead when they are "swamped" (responding slowly) and the avoidance of the state of servers being rapidly changed from dead to live to dead again. This prompt detection of nonresponding RADIUS servers and the avoidance of swamped and dead-to-live-to-dead-again servers will result in less deadtime and quicker packet processing.

How to Configure AAA Dead-Server Detection

Configuring AAA Dead-Server Detection

To configure AAA Dead-Server Detection, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server deadtime** *minutes*
5. **radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router (config)# aaa new-model`	Enables the AAA access control model.
Step 4	**radius-server deadtime** *minutes* **Example:** `Router (config)# radius-server deadtime 5`	Improves RADIUS response times when some servers might be unavailable and causes the unavailable servers to be skipped immediately.
Step 5	**radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] **Example:** `Router (config)# radius-server dead-criteria time 5 tries 4`	Forces one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant.

Troubleshooting Tips

After you have configured AAA Dead-Server Detection, you should verify your configuration using the **show running-config** command. This verification is especially important if you have used the **no** form of the **radius-server dead-criteria** command. The output of the **show running-config** command must show the same values in the “Dead Criteria Details” field that you configured using the **radius-server dead-criteria** command.

Verifying AAA Dead-Server Detection

To verify your AAA Dead-Server Detection configuration, perform the following steps. The **show** and **debug** commands may be used in any order.

SUMMARY STEPS

1. **enable**
2. **debug aaa dead-criteria transactions**
3. **show aaa dead-criteria**
4. **show aaa servers** [**private** | **public**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa dead-criteria transactions** **Example:** `Router# debug aaa dead-criteria transactions`	Displays AAA dead-criteria transaction values.
Step 3	**show aaa dead-criteria** **Example:** `Router# show aaa dead-criteria`	Displays dead-criteria information for a AAA server.
Step 4	**show aaa servers** [**private** | **public**] **Example:** `Router# show aaa server private`	Displays the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers. • The **private** keyword optionally displays the AAA servers only. • The **public** keyword optionally displays the AAA servers only.

Configuration Examples for AAA Dead-Server Detection

Configuring AAA Dead-Server Detection Example

The following example shows that the router will be considered dead after 5 seconds and four tries:

```
Router (config)# aaa new-model
Router (config)# radius-server deadtime 5
Router (config)# radius-server dead-criteria time 5 tries 4
```

debug aaa dead-criteria transactions Command Example

The following output example shows dead-criteria transaction information for a particular server group:

```
Router# debug aaa dead-criteria transactions
AAA Transaction debugs debugging is on
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 22, Current Max Tries: 22
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 25s, Current Max
Interval: 25s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transactions: 6, Current Max
Transactions: 6
```

show aaa dead-criteria Command Example

The following output example shows that dead-server-detection information has been requested for a RADIUS server at the IP address 172.19.192.80:

```
Router# show aaa dead-criteria radius 172.19.192.80 radius
RADIUS Server Dead Criteria:
=============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

Additional References

The following sections provide references related to the AAA Dead-Server Detection feature.

Related Documents

Related Topic	Document Title
Configuring RADIUS	Configuring RADIUS feature module.
Configuring AAA	Configuring Authentication
	Configuring Authorization
	Configuring Accounting
Security commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	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

RFCs	Title
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*

Technical Assistance

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

Feature Information for AAA Dead-Server Detection

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 AAA Dead-Server Detection

Feature Name	Releases	Feature Information
AAA Dead-Server Detection	12.3(6) 12.3(7)T Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG	Allows you to configure the criteria to be used to mark a RADIUS server as dead. The following commands were introduced or modified: **debug aaa dead-criteria transactions**, **radius-server dead-criteria**, **show aaa dead-criteria**, **show aaa servers**.

CHAPTER 19

AAA-SERVER-MIB Set Operation

The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the "KEY" under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration.

- Finding Feature Information, page 275
- Prerequisites for AAA-SERVER-MIB Set Operation, page 275
- Restrictions for AAA-SERVER-MIB Set Operation, page 276
- Information About AAA-SERVER-MIB Set Operation, page 276
- How to Configure AAA-SERVER-MIB Set Operation, page 276
- Configuration Examples for AAA-SERVER-MIB Set Operation, page 277
- Additional References, page 279
- Feature Information for AAA-SERVER-MIB Set Operation, page 280

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 AAA-SERVER-MIB Set Operation

AAA must have been enabled on the router, that is, the **aaa new-model** command must have been configured. If this configuration has not been accomplished, the set operation fails.

Restrictions for AAA-SERVER-MIB Set Operation

Currently, the CISCO SNMP set operation is supported only for the RADIUS protocol. Therefore, only RADIUS servers in global configuration mode can be added, modified, or deleted.

Information About AAA-SERVER-MIB Set Operation

CISCO-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB provides that statistics reflect both the state of the AAA server operation with the server itself and of AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:

- Statistics for each AAA operation
- Status of servers that are providing AAA functions
- Identities of external AAA servers

CISCO-AAA-SERVER-MIB Set Operation

Before Cisco IOS Release 12.4(4)T, the CISCO-AAA-SERVER-MIB supported only the “get” operation. Effective with this release, the CISCO-AAA-SERVER-MIB supports the set operation. With the set operation, you can do the following:

- Create or add a new AAA server.
- Modify the KEY under the CISCO-AAA-SERVER-MIB. This “secret key” is used for secure connectivity to the AAA server, which is present with the network access server (NAS) and the AAA server.
- Delete the AAA server configuration.

How to Configure AAA-SERVER-MIB Set Operation

Configuring AAA-SERVER-MIB Set Operations

No special configuration is required for this feature. The Simple Network Management Protocol (SNMP) framework can be used to manage MIBs. See the Additional References section for a reference to configuring SNMP.

Verifying SNMP Values

SNMP values can be verified by performing the following steps.

SUMMARY STEPS

1. **enable**
2. **show running-config | include radius-server host**
3. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config | include radius-server host** **Example:** `Device# show running-config | include radius-server host`	Displays all the RADIUS servers that are configured in the global configuration mode.
Step 3	**show aaa servers** **Example:** `Device# show aaa servers`	Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers.

Configuration Examples for AAA-SERVER-MIB Set Operation

RADIUS Server Configuration and Server Statistics Example

The following sample output shows the RADIUS server configuration and server statistics before and after the set operation.

Before the Set Operation

```
Device# show running-config | include radius-server host
! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

Server Statistics

```
Device# show aaa servers
```

```
RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 2
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m
RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

SNMP Get Operation to Check the Configuration and Statistics of the RADIUS Servers

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP Set Operation

The key of the existing RADIUS server is being changed. The index “1” is being used. That index acts as a wildcard for addition, deletion, or modification of any entries.

```
Change the key for server 1:=>
aaa-server5:/users/smetri>  setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

After the Set Operation

After the above SNMP set operation, the configurations on the router change. The following output shows the output after the set operation.

```
Device# show running-config | include radius-server host
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

```
! The following line shows a change in the key value to “king.”
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king

Device# show aaa servers
RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

Additional References

The following sections provide references related to the AAA-SERVER-MIB Set Operation feature.

Related Documents

Related Topic	Document Title
Configuring SNMP	Configuring SNMP Support in the *Cisco IOS Network Management Configuration Guide*

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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for AAA-SERVER-MIB Set Operation

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 36: Feature Information for AAA-SERVER-MIB Set Operation

Feature Name	Releases	Feature Information
AAA-SERVER-MIB Set Operation	12.3(11)T 12.4(4)T 12.2(33)SRE	The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the "KEY" under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration. The following commands were introduced or modified: **show aaa servers, show running-config, show running-config vrf.**

CHAPTER 20

Per VRF AAA

The Per VRF AAA feature allows ISPs to partition authentication, authorization, and accounting (AAA) services on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances, allowing their customers to control some of their own AAA services.

The list of servers in server groups is extended to include the definitions of private servers in addition to references to the hosts in the global configuration, allowing access to both customer servers and global service provider servers simultaneously.

For Cisco IOS Release 12.2(15)T or later releases, a customer template can be used, which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template. This feature has also been referred to as the Dynamic Per VRF AAA feature.

- Finding Feature Information, page 283
- Prerequisites for Per VRF AAA, page 284
- Restrictions for Per VRF AAA, page 284
- Information About Per VRF AAA, page 284
- How to Configure Per VRF AAA, page 289
- Configuration Examples for Per VRF AAA, page 302
- Additional References, page 310
- Feature Information for Per VRF AAA, page 311
- Glossary, page 314

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 Per VRF AAA

Before configuring the Per VRF AAA feature, AAA must be enabled. See “How to Configure Per VRF AAA” section on page 6 for more information.

Restrictions for Per VRF AAA

- This feature is supported only for RADIUS servers.
- Operational parameters should be defined once per VRF rather than set per server group, because all functionality must be consistent between the network access server (NAS) and the AAA servers.
- The ability to configure a customer template either locally or remotely is available only for Release 12.2(15)T and later releases.

Information About Per VRF AAA

When you use the Per VRF AAA feature, AAA services can be based on VRF instances. This feature permits the Provider Edge (PE) or Virtual Home Gateway (VHG) to communicate directly with the customer’s RADIUS server, which is associated with the customer’s Virtual Private Network (VPN), without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer have to use RADIUS proxies and ISPs can also provide their customers with additional flexibility.

How Per VRF AAA Works

To support AAA on a per customer basis, some AAA features must be made VRF aware. That is, ISPs must be able to define operational parameters--such as AAA server groups, method lists, system accounting, and protocol-specific parameters--and bind those parameters to a particular VRF instance. Defining and binding the operational parameters can be accomplished using one or more of the following methods:

- Virtual private dialup network (VPDN) virtual template or dialer interfaces that are configured for a specific customer
- Locally defined customer templates--Per VPN with customer definitions. The customer template is stored locally on the VHG. This method can be used to associate a remote user with a specific VPN based on the domain name or dialed number identification service (DNIS) and provide the VPN-specific configuration for virtual access interface and all operational parameters for the customer AAA server.
- Remotely defined customer templates--Per VPN with customer definitions that are stored on the service provider AAA server in a RADIUS profile. This method is used to associate a remote user with a specific VPN based on the domain name or DNIS and provide the VPN-specific configuration for the virtual access interface and all operational parameters for the AAA server of the customer.

Note The ability to configure locally or remotely defined customer templates is available only with Cisco IOS Release 12.2(15)T and later releases.

AAA Accounting Records

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. Start and stop records are necessary for users employing accounting records to manage and monitor their networks.

New Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (VSA) attribute 26. Attribute 26 encapsulates VSAs, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco’s vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string of the following format:

```
protocol : attribute sep value *
```

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This format allows the full set of features available for TACACS+ authorization to be used also for RADIUS.

The table below summarizes the VSAs that are now supported with Per VRF AAA.

Table 37: VSAs supported with Per VRF AAA

VSA Name	Value Type	Description
Note Each VSA must have the prefix “template:” before the VSA name, unless a different prefix is explicitly stated.		
account-delay	string	This VSA must be “on.” The functionality of this VSA is equal to the **aaa accounting delay-start**command for the customer template.
account-send-stop	string	This VSA must be “on.” The functionality of this VSA is equal to the **aaa accounting send stop-record authentication**command with the **failure** keyword.
account-send-success-remote	string	This VSA must be “on.” The functionality of this VSA is equal to the **aaa accounting send stop-record authentication**command with the **success** keyword.

VSA Name	Value Type	Description
attr-44	string	This VSA must be "access-req." The functionality of this VSA is equal to the **radius-server attribute 44 include-in-access-req** command.
ip-addr	string	This VSA specifies the IP address, followed by the mask that the router uses to indicate its own IP address and mask in negotiation with the client; for example, ip-addr=192.168.202.169 255.255.255.255
ip-unnumbered	string	This VSA specifies the name of an interface on the router. The functionality of this VSA is equal to the **ip unnumbered** command, which specifies an interface name such as "Loopback 0."
ip-vrf	string	This VSA specifies which VRF will be used for the packets of the end user. This VRF name should match the name that is used on the router via the **ip vrf forwarding** command.
peer-ip-pool	string	This VSA specifies the name of an IP address pool from which an address will be allocated for the peer. This pool should be configured using the **ip local pool**command or should be automatically downloadable via RADIUS.
ppp-acct-list	string	This VSA defines the accounting method list that is to be used for PPP sessions. The VSA syntax is as follows: "ppp-acct-list=[start-stop | stop-only | none] group X [group Y] [broadcast]." It is equal to the **aaa accounting network mylist** command functionality. The user must specify at least one of the following options: start-stop, stop-only, or none. If either start-stop or stop-only is specified, the user must specify at least one, but not more than four, group arguments. Each group name must consist of integers. The servers in the group should have already been identified in the access-accept via the VSA "rad-serv." After each group has been specified, the user can specify the broadcast option.

VSA Name	Value Type	Description
ppp-authen-list	string	This VSA defines which authentication method list is to be used for PPP sessions and, if more than one method is specified, in what order the methods should be used. The VSA syntax is as follows: “ppp-authen-list=[groupX | local | local-case | none | if-needed],” which is equal to the **aaa authentication ppp mylist** command functionality. The user must specify at least one, but no more than four, authentication methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA “rad-serv.”
ppp-authen-type	string	This VSA allows the end user to specify at least one of the following authentication types: pap, chap, eap, ms-chap, ms-chap-v2, any, or a combination of the available types that is separated by spaces. The end user will be permitted to log in using only the methods that are specified in this VSA. PPP will attempt these authentication methods in the order presented in the attribute.
ppp-author-list	string	This VSA defines the authorization method list that is to be used for PPP sessions. It indicates which methods will be used and in what order. The VSA syntax is as follows: “ppp-author-list=[groupX] [local] [if-authenticated] [none],” which is equal to the **aaa authorization network mylist**command functionality. The user must specify at least one, but no more than four, authorization methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA “rad-serv.”

VSA Name	Value Type	Description
Note The RADIUS VSAs--rad-serv, rad-server-filter, rad-serv-source-if, and rad-serv-vrf--must have the prefix "aaa:" before the VSA name.		
rad-serv	string	This VSA indicates the IP address, key, timeout, and retransmit number of a server, as well as the group of the server. The VSA syntax is as follows: "rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W]." Other than the IP address, all parameters are optional and can be issued in any order. If the optional parameters are not specified, their default values will be used. The key cannot contain any spaces; for "retransmit V," "V" can range from 1-100; for "timeout W," the "W" can range from 1-1000.
rad-serv-filter	string	The VSA syntax is as follows: "rad-serv-filter=authorization | accounting-request | reply-accept | reject-filtername." The filtername must be defined via the **radius-server attribute list filtername** command.
rad-serv-source-if	string	This VSA specifies the name of the interface that is used for transmitting RADIUS packets. The specified interface must match the interface configured on the router.
rad-serv-vrf	string	This VSA specifies the name of the VRF that is used for transmitting RADIUS packets. The VRF name should match the name that was specified via the **ip vrf forwarding** command.

How to Configure Per VRF AAA

Configuring Per VRF AAA

Configuring AAA

Perform this task to enable AAA:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **ip vrf default**

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 AAA globally.
Step 4	**ip vrf default** **Example:** `Router(config)# ip vrf default`	This command must be configured before any VRF-related AAA commands are configured, such as the **radius-server domain-stripping** command, to ensure that the default VRF name is a NULL value until a default VRF name is configured.

Configuring Server Groups

Perform this task to configure server groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *groupname*
5. **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa group server radius** *groupname* **Example:** `Router(config)# aaa group server radius v2.44.com`	Groups different RADIUS server hosts into distinct lists and distinct methods. Enters server-group configuration mode.
Step 5	**server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **Example:** `Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww`	Configures the IP address of the private RADIUS server for the group server. **Note** If private server parameters are not specified, global configurations will be used. If global configurations are not specified, default values will be used.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits from server-group configuration mode; returns to global configuration mode.

Configuring Authentication Authorization and Accounting for Per VRF AAA

Perform this task to configure authentication, authorization, and accounting for Per VRF AAA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
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 accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
7. **aaa accounting delay-start** [**vrf** *vrf-name*]
8. **aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-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	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA globally.

	Command or Action	Purpose
Step 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com`	Sets parameters that restrict user access to a network.
Step 6	**aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **Example:** `Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. **Note** The **stop-only** keyword is not available in Cisco IOS Release 12.4(24)T and later releases.
Step 7	**aaa accounting delay-start** [**vrf** *vrf-name*] **Example:** `Router(config)# aaa acounting delay-start vrf v2.44.com`	Displays generation of the start accounting records until the user IP address is established.
Step 8	**aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*] **Example:** `Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com`	Generates accounting stop records. When using the **failure** keyword a “stop” record will be sent for calls that are rejected during authentication. When using the **success** keyword a “stop” record will be sent for calls that meet one of the following criteria: • Calls that are authenticated by a remote AAA server when the call is terminated. • Calls that are not authenticated by a remote AAA server and the start record has been sent. • Calls that are successfully established and then terminated with the “stop-only” **aaa accounting** configuration. **Note** The **success** and **remote-server** keywords are available in Cisco IOS Release 12.4(2)T and later releases. **Note** The **success** and **remote-server** keywords are not available in Cisco IOS Release 12.2SX.

	Command or Action	Purpose

Configuring RADIUS-Specific Commands for Per VRF AAA

To configure RADIUS-specific commands for Per VRF AAA you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*]
4. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-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	**ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*] **Example:** `Router(config)# ip radius source-interface loopback55`	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets and enables the specification on a per-VRF basis.
Step 4	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] **Example:** `Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com`	Sends RADIUS attribute 44 in access request packets before user authentication and enables the specification on a per-VRF basis.

Configuring Interface-Specific Commands for Per VRF AAA

Perform this task to configure interface-specific commands for Per VRF AAA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip vrf forwarding** *vrf-name*
5. **ppp authentication** {*protocol1* [*protocol2*...]} *listname*
6. **ppp authorization** *list-name*
7. **ppp accounting default**
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	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface loopback11`	Configures an interface type and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding v2.44.com`	Associates a VRF with an interface.
Step 5	**ppp authentication** {*protocol1* [*protocol2*...]} *listname* **Example:** `Router(config-if)# ppp authentication chap callin V2_44_com`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

	Command or Action	Purpose
Step 6	**ppp authorization** *list-name* **Example:** `Router(config-if)# ppp authorization V2_44_com`	Enables AAA authorization on the selected interface.
Step 7	**ppp accounting default** **Example:** `Router(config-if)# ppp accounting default`	Enables AAA accounting services on the selected interface.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Configuring Per VRF AAA Using Local Customer Templates

Configuring AAA with Local Customer Templates

Perform the tasks as outlined in the Configuring AAA section.

Configuring Server Groups with Local Customer Templates

Perform the tasks as outlined in the Configuring Server Groups.

Configuring Authentication Authorization and Accounting for Per VRF AAA with Local Customer Templates

Perform the tasks as outlined in the Configuring Authentication Authorization and Accounting for Per VRF AAA, on page 291.

Configuring Authorization for Per VRF AAA with Local Customer Templates

Perform this task to configure authorization for Per VRF AAA with local templates.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default local**

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 authorization template** **Example:** `Router(config)# aaa authorization template`	Enables the use of local or remote templates.
Step 4	**aaa authorization network default local** **Example:** `Router(config)# aaa authorization network default local`	Specifies local as the default method for authorization.

Configuring Local Customer Templates

Perform this task to configure local customer templates.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn search-order domain**
4. **template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]
5. **peer default ip address pool** *pool-name*
6. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
7. **ppp authorization** [**default** | *list-name*]
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn search-order domain** **Example:** `Router (config)# vpdn search-order domain`	Looks up the profiles based on domain.
Step 4	**template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**] **Example:** `Router (config)# template v2.44.com`	Creates a customer profile template and assigns a unique name that relates to the customer that will be receiving it. Enters template configuration mode. **Note** Steps 5, 6, and 7 are optional. Enter **multilink**, **peer**, and **ppp** keywords appropriate to customer application requirements.
Step 5	**peer default ip address pool** *pool-name* **Example:** `Router(config-template)# peer default ip address pool v2_44_com_pool`	(Optional) Specifies that the customer profile to which this template is attached will use a local IP address pool with the specified name.

	Command or Action	Purpose
Step 6	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **Example:** `Router(config-template)# ppp authentication chap`	(Optional) Sets the PPP link authentication method.
Step 7	**ppp authorization** [**default** | *list-name*] **Example:** `Router(config-template)# ppp authorization v2_44_com`	(Optional) Sets the PPP link authorization method.
Step 8	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **Example:** `Router(config-template)# aaa accounting v2_44_com`	(Optional) Enables AAA operational parameters for the specified customer profile.
Step 9	**exit** **Example:** `Router(config-template)# exit`	Exits from template configuration mode; returns to global configuration mode.

Configuring Per VRF AAA Using Remote Customer Templates

Configuring AAA with Remote Customer Templates

Perform the tasks as outlined in the Configuring AAA section.

Configuring Server Groups

Perform the tasks as outlined in the Configuring Server Groups.

Configuring Authentication for Per VRF AAA with Remote Customer Templates

Perform this task to configure authentication for Per VRF AAA with remote customer templates.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# ppp authentication ppp default group radius`	Specifies one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP.
Step 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] **Example:** `Router(config)# aaa authorization network default group sp`	Sets parameters that restrict user access to a network.

Configuring Authorization for Per VRF AAA with Remote Customer Templates

Perform this task to configure authorization for Per VRF AAA with remote customer templates.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

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 authorization template** **Example:** `Router(config)# aaa authorization template`	Enables use of local or remote templates.
Step 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] **Example:** `Router(config)# aaa authorization network default sp`	Specifies the server group that is named as the default method for authorization.

Configuring the RADIUS Profile on the SP RADIUS Server

See the Per VRF AAA Using a Remote RADIUS Customer Template Example for an example of how to update the RADIUS profile.

Verifying VRF Routing Configurations

Perform this task to verify VRF routing configurations:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show ip route vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**show ip route vrf** *vrf-name* **Example:** `Router(config)# show ip route vrf northvrf`	Displays the IP routing table associated with a VRF.

Troubleshooting Per VRF AAA Configurations

To troubleshoot the Per VRF AAA feature, use at least one of the following commands in EXEC mode:

Command	Purpose
Router# **debug aaa accounting**	Displays information on accountable events as they occur.
Router# **debug aaa authentication**	Displays information on AAA authentication.
Router# **debug aaa authorization**	Displays information on AAA authorization.
Router# **debug ppp negotiation**	Displays information on traffic and exchanges in an internetwork implementing PPP.
Router# **debug radius**	Displays information associated with RADIUS.
Router# **debug vpdn event**	Displays Layer 2 Transport Protocol (L2TP) errors and events that are a part of normal tunnel establishment or shutdown for VPNs.
Router# **debug vpdn error**	Displays debug traces for VPN.

Configuration Examples for Per VRF AAA

Per VRF Configuration Examples

Per VRF AAA Example

The following example shows how to configure the Per VRF AAA feature using a AAA server group with associated private servers:

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com
aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com
ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

Per VRF AAA Using a Locally Defined Customer Template Example

The following example shows how to configure the Per VRF AAA feature using a locally defined customer template with a AAA server group that has associated private servers:

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
  ip vrf forwarding V1.55.com
template V1.55.com
  peer default ip address pool V1_55_com_pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req
  ip vrf forwarding v1.55.com
  ip radius source-interface Loopback55
```

Per VRF AAA Using a Remote RADIUS Customer Template Example

The following examples shows how to configure the Per VRF AAA feature using a remotely defined customer template on the SP RADIUS server with a AAA server group that has associated private servers:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp
aaa group server radius sp
   server 10.3.3.3
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

The following RADIUS server profile is configured on the SP RADIUS server:

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

Customer Template Examples

Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example

The following example shows how to create a locally configured template for a single customer, configuring additional features including RADIUS attribute screening and broadcast accounting:

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server
aaa group server radius SP_AAA_server
 server 10.10.100.7 auth-port 1645 acct-port 1646
aaa group server radius V1_55_com
 server-private 10.10.132.4 auth-port 1645 acct-port 1646
 authorization accept min-author
 accounting accept usage-only
 ip vrf forwarding V1.55.com
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
template V1.55.com
 peer default ip address pool V1.55-pool
 ppp authentication chap callin V1_55_com
 ppp authorization V1_55_com
 ppp accounting V1_55_com
 aaa accounting delay-start
 aaa accounting send stop-record authentication failure
 radius-server attribute 44 include-in-access-req
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 ip vrf forwarding V1.55.com
 ip unnumbered Loopback55
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww
```

Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example

The following example shows how to create a remotely configured template for a single customer, configuring additional features including RADIUS attribute screening and broadcast accounting:

```
aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 no ip address
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

The customer template is stored as a RADIUS server profile for v1.55.com.

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

AAA Accounting Stop Records Examples

The following AAA accounting stop record examples show how to configure the **aaa accounting send stop-record authentication** command to control the generation of “stop” records when the **aaa accounting** command is issued with the **start-stop** or **stop-only** keyword.

Note The **success** and **remote-server** keywords are available in Cisco IOS Release 12.4(2)T and later releases.

AAA Accounting Stop Record and Successful Call Example

The following example shows “start” and “stop” records being sent for a successful call when the **aaa accounting send stop-record authentication** command is issued with the **failure** keyword.

```
Router# show running-config | include aaa

.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

AAA Accounting Stop Record and Rejected Call Example

The following example shows the “stop” record being sent for a rejected call during authentication when the **aaa accounting send stop-record authentication**command is issued with the **success** keyword.

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius
Router#
*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                   [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=10.0.0.2"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
```

```
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                    [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                 [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                      [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
```

```
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

Additional References

The following sections provide references related to Per VRF AAA.

Related Documents

Related Topic	Document Title
AAA: Configuring Server Groups	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T
Cisco IOS Security Commands	*Cisco IOS Security Command Reference*
Cisco IOS Switching Services Commands	*Cisco IOS IP Switching Command Reference*
Configuring Multiprotocol Label Switching	*Cisco IOS Multiprotocol Label Switching Configuration Guide* , Release 12.4T
Configuring Virtual Templates section	Virtual Templates, Profiles, and Networks chapter in the *Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	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

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

Technical Assistance

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

Feature Information for Per VRF AAA

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 Per VRF AAA

Feature Name	Releases	Feature Information
Per VRF AAA Dynamic Per VRF AAA Attribute Filtering Per-Domain and VRF Aware Framed-Routes RADIUS Per-VRF Server Group	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(13)T 12.2(15)T 12.4(2)T 12.2(28)SB 12.2(33)SR 12.2(33)SXI 12.2(33)SXH4	

Feature Name	Releases	Feature Information
		The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances. For Cisco IOS Release 12.2(15)T or later releases, you can use a customer template, which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template. In 12.2(1)DX, the Per VRF AAA feature was introduced on the Cisco 7200 series and the Cisco 7401ASR. In 12.2(2)DD, the **ip vrf forwarding** (server-group) and **radius-server domain-stripping** commands were added. The Per VRF AAA, Dynamic Per VRF AAA, and Attribute Filtering Per-Domain and VRF Aware Framed-Routes features were introduced in Cisco IOS Release 12.2(15)T. Also, the **aaa authorization template** command was added to this release. In 12.4(2)T, the **aaa accounting send stop-record authentication** command was updated with additional support for AAA accounting stop records. In 12.2(33)SRC, RADIUS Per-VRF Server Group feature was introduced. In Cisco IOS Release 12.2(33)SXI, these features were introduced. In Cisco IOS Release 12.2(33)SXH4, these features were introduced. The following commands were introduced or modified: **aaa accounting**, **aaa accounting delay-start**, **ip radius**

Feature Name	Releases	Feature Information
		source-interface, **radius-server attribute 44 include-in-access-req**, **server-private (RADIUS)**.

Glossary

AAA --authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

L2TP --Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

PE --Provider Edge. Networking devices that are located on the edge of a service provider network.

RADIUS --Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VPN --Virtual Private Network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

VRF --Virtual Route Forwarding. Initially, a router has only one global default routing/forwarding table. VRFs can be viewed as multiple disjoined routing/forwarding tables, where the routes of a user have no correlation with the routes of another user.

CHAPTER 21

AAA Support for IPv6

Authentication, authorization, and accounting (AAA) support for IPv6 is in compliance with RFC 3162. This module provides information about how to configure AAA options for IPv6.

- Finding Feature Information, page 315
- Information About AAA Support for IPv6, page 315
- How to Configure AAA Support for IPv6, page 318
- Configuration Examples for AAA Support for IPv6, page 323
- Additional References, page 324
- Feature Information for AAA Support for IPv6, page 324

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 AAA Support for IPv6

AAA over IPv6

Vendor-specific attributes (VSAs) are used to support Authentication, Authorization and Accounting(AAA) over IPv6. Cisco VSAs are inacl, outacl, prefix, and route.

You can configure prefix pools and pool names by using the AAA protocol. Customers can deploy an IPv6 RADIUS server or a TACACS+ server to communicate with Cisco devices.

AAA Support for IPv6 RADIUS Attributes

The following RADIUS attributes, as described in RFC 3162, are supported for IPv6:

- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Login-IPv6-Host

The following RADIUS attributes are also supported for IPv6:

- Delegated-IPv6-Prefix (RFC 4818)
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route

The attributes listed above can be configured on a RADIUS server and downloaded to access servers, where they can be applied to access connections.

Prerequisites for Using AAA Attributes for IPv6

AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162.

RADIUS Per-User Attributes for Virtual Access in IPv6 Environments

The following IPv6 attributes for RADIUS attribute-value (AV) pairs are supported for virtual access:

Framed-Interface-Id

The Framed-Interface-Id attribute indicates the IPv6 interface identifier to be configured. This per-user attribute is used during the IPv6CP negotiations and may be used in access-accept packets. If the Interface-Identifier IPv6CP option has been successfully negotiated, this attribute must be included in an Acc-0Request packet as a hint by the NAS to the server that it would prefer that value.

Framed-IPv6-Pool

The Framed-IPv6-Pool attribute is a per-user attribute that contains the name of an assigned pool that should be used to assign an IPv6 prefix for the user. This pool should either be defined locally on the router or defined on a RADIUS server from which pools can be downloaded.

Framed-IPv6-Prefix

The Framed-IPv6-Prefix attribute performs the same function as the Cisco VSA--it is used for virtual access only and indicates an IPv6 prefix (and corresponding route) to be configured. This attribute is a per-user attribute and lets the user specify which prefixes to advertise in Neighbor Discovery Router Advertisement messages. The Framed-IPv6-Prefix attribute may be used in access-accept packets and can appear multiple times. The NAS will create a corresponding route for the prefix.

To use this attribute for DHCP for IPv6 prefix delegation, create a profile for the same user on the RADIUS server. The username associated with the second profile has the suffix "-dhcpv6."

The Framed-IPv6-Prefix attribute in the two profiles is treated differently. If a NAS needs both to send a prefix in router advertisements (RAs) and delegate a prefix to a remote user's network, the prefix for RA is placed in the Framed-IPv6-Prefix attribute in the user's regular profile, and the prefix used for prefix delegation is placed in the attribute in the user's separate profile.

Framed-IPv6-Route

The Framed-IPv6-Route attribute performs the same function as the Cisco VSA: It is a per-user attribute that provides routing information to be configured for the user on the NAS. This attribute is a string attribute and is specified using the **ipv6 route** command.

IPv6 ACL

You can specify a complete IPv6 access list. The unique name of the access list is generated automatically. The access list is removed when its user logs out. The previous access list on the interface is reapplied.

The inacl and outacl attributes allow you to a specific existing access list configured on the router. The following example shows ACL number 1 specified as the access list:

```
cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:outacl#1=deny 2001:DB8::/10",
```

IPv6 Pool

For RADIUS authentication, the IPv6 Pool attribute extends the IPv4 address pool attributed to support the IPv6 protocol. It specifies the name of a local pool on the NAS from which to get the prefix and is used whenever the service is configured as PPP and whenever the protocol is specified as IPv6. Note that the address pool works in conjunction with local pooling. It specifies the name of the local pool that has been preconfigured on the NAS.

IPv6 Prefix

The IPv6 Prefix# attribute lets you indicate which prefixes to advertise in Neighbor Discovery Router Advertisement messages. When the IPv6 Prefix# attribute is used, a corresponding route (marked as a per-user static route) is installed in the routing information base (RIB) tables for the given prefix.

```
cisco-avpair = "ipv6:prefix#1=2001:DB8::/64",
cisco-avpair = "ipv6:prefix#2=2001:DB8::/64",
```

IPv6 Route

The IPv6 route attribute allows you to specify a per-user static route. A static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination. See the description of the **ipv6 route** command for more information about building static routes.

The following example shows the IPv6 route attribute used to define a static route:

```
cisco-avpair = "ipv6:route#1=2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:route#2=2001:DB8:cc00:2::/48",
```

Login-IPv6-Host

The Login-IPv6-Host attribute is a per-user attribute that indicates the IPv6 system with which to connect the user when the Login-Service attribute is included.

IPv6 Prefix Pools

The function of prefix pools in IPv6 is similar to that of address pools in IPv4. The main difference is that IPv6 assigns prefixes rather than single addresses.

As in IPv4, a pool or a pool definition in IPv6 can be configured locally or it can be retrieved from an AAA server. Overlapping membership between pools is not permitted.

Once a pool is configured, it cannot be changed. If you change the configuration, the pool will be removed and re-created. All prefixes previously allocated will be freed.

Prefix pools can be defined so that each user is allocated a 64-bit prefix or so that a single prefix is shared among several users. In a shared prefix pool, each user may receive only one address from the pool.

How to Configure AAA Support for IPv6

Configuring the RADIUS Server over IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius server** *name*
5. **address ipv6** {*hostname* | *ipv6address*} [**acct-port** *port* | **alias** {*hostname* | *ipv6address*} | **auth-port** *port* [**acct-port** *port*]]
6. **key** {**0** *string* | **7** *string*} *string*
7. **timeout** *seconds*
8. **retransmit** *retries*
9. **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)# aaa new-model`	Configures the RADIUS server for IPv6 and enters RADIUS server configuration mode.
Step 4	**radius server** *name* **Example:** `Device(config)# radius server myserver`	Configures the RADIUS server for IPv6 and enters RADIUS server configuration mode.
Step 5	**address ipv6** {*hostname* | *ipv6address*} [**acct-port** *port* | **alias** {*hostname* | *ipv6address*} | **auth-port** *port* [**acct-port** *port*]] **Example:** `Device(config-radius-server)# address ipv6 2001:DB8:1::1 acct-port 1813 auth-port 1812`	Configures the IPv6 address for the RADIUS server accounting and authentication parameters.
Step 6	**key** {**0** *string* | **7** *string*} *string* **Example:** `Device(config-radius-server)# key 0 key1`	Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server.
Step 7	**timeout** *seconds* **Example:** `Device(config-radius-server)# timeout 10`	Specifies the time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting.
Step 8	**retransmit** *retries* **Example:** `Device(config-radius-server)# retransmit 5`	Specifies the number of times a RADIUS request is re-sent to a server when that server is not responding or responding slowly.

	Command or Action	Purpose

Step 9	**end**
	Example:
	`Device(config-radius-server)# end`
		Exits RADIUS server configuration mode and returns to privileged EXEC mode.

Specifying the Source Address in RADIUS Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 radius source-interface** *type number*
4. **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	**ipv6 radius source-interface** *type number* **Example:** `Device(config)# ipv6 radius source-interface ethernet 0/0`	Specifies an interface to use for the source address in RADIUS server.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring RADIUS Server Group Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server name** *server-name*
5. **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]
6. **ipv6 radius source-interface** *type number*
7. **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 group server radius** *group-name* **Example:** `Device(config)# aaa group server radius group1`	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 4	**server name** *server-name* **Example:** `Device(config-sg-radius)# server name server1`	Specifies an IPv6 RADIUS server and enters RADIUS group server configuration mode.
Step 5	**server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] **Example:** `Device(config-sg-radius)# server-private 2001:DB8:3333:4::5 port 19 key key1`	Configures the IPv6 address of the private TACACS+ server for the group server.

	Command or Action	Purpose
Step 6	**ipv6 radius source-interface** *type number* **Example:** `Device(config-sg-radius)# ipv6 radius source-interface ethernet 0/0`	Specifies an interface to use for the source address in RADIUS server under the RADIUS group server configuration.

Step 7	**end**
	Example:
	`Device(config-sg-radius)# end`
		Exits RADIUS group server configuration mode and returns to privileged EXEC mode.

Configuring the DHCPv6 Server to Obtain Prefixes from RADIUS Servers

Before You Begin

Before you perform this task, you must configure the AAA client and PPP on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd prefix framed-ipv6-prefix**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 nd prefix framed-ipv6-prefix** **Example:** `Router(config-if)# ipv6 nd prefix framed-ipv6-prefix`	Adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue.

Configuration Examples for AAA Support for IPv6

Example: Configuring RADIUS Server over IPv6

```
Device> enable
Device# show radius server-group all

Server group radius
  Sharecount = 1 sg_unconfigured = FALSE
  Type = standard Memlocks = 1
  Server(2001:DB8:3333:4::5,6) Transactions:
  Authen: 0 Author: 0 Acct: 0
  Server_auto_test_enabled: FALSE
   Keywrap enabled: FALSE
Server group rad_ser1
  Sharecount = 1 sg_unconfigured = FALSE
  Type = standard Memlocks = 1
  Server(2001:DB8:3333:4::5,6) Transactions:
  Authen: 0 Author: 0 Acct: 0
  Server_auto_test_enabled: FALSE
   Keywrap enabled: FALSE
```

Example: RADIUS Configuration

The following sample RADIUS configuration shows the definition of AV pairs to establish static routes:

```
campus1 Auth-Type = Local, Password = "mypassword"
                 User-Service-Type = Framed-User,
                 Framed-Protocol = PPP,
                 cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:1::/64 any",
                 cisco-avpair = "ipv6:route=2001:DB8:2::/64",
                 cisco-avpair = "ipv6:route=2001:DB8:3::/64",
                 cisco-avpair = "ipv6:prefix=2001:DB8:2::/64 0 0 onlink autoconfig",
                 cisco-avpair = "ipv6:prefix=2001:DB8:3::/64 0 0 onlink autoconfig",
                 cisco-avpair = "ip:route=10.0.0.0 255.0.0.0",
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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 AAA Support for IPv6

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 AAA Support for IPv6

Feature Name	Releases	Feature Information
AAA Support for Cisco VSA IPv6 Attributes	12.2(33)SRC 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	VSAs were developed to support AAA for IPv6.
IPv6 Access Services: AAA Support for RFC 3162 IPv6 RADIUS Attributes	12.3(4)T 12.4 12.2(58)SE 12.2(33)SRC	The AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162. The following commands were introduced or modified: **ipv6 nd prefix framed-ipv6-prefix**.
IPv6 Access Services: Prefix Pools	12.2(13)T	This feature is supported.
RADIUS over IPv6	15.2(1)T 12.2(58)SE 15.1(1)SY	Authentication, authorization, and accounting (AAA) support for IPv6 is in compliance with RFC 3162. This feature provides information about how to configure AAA options for IPv6.

CHAPTER 22

TACACS+ over IPv6

An IPv6 server can be configured to be used with TACACS+.

- Finding Feature Information, page 327
- Information About TACACS+ over IPv6, page 327
- How to Configure TACACS+ over IPv6, page 328
- Configuration Examples for TACACS+ over IPv6, page 331
- Additional References, page 332
- Feature Information for TACACS+ over IPv6, page 332

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 TACACS+ over IPv6

The Terminal Access Controller Access-Control System (TACACS+) security protocol provides centralized validation of users. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your devices are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service (authentication, authorization, and accounting) independently. Each service is associated with its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

AAA over IPv6

Vendor-specific attributes (VSAs) are used to support Authentication, Authorization and Accounting(AAA) over IPv6. Cisco VSAs are inacl, outacl, prefix, and route.

You can configure prefix pools and pool names by using the AAA protocol. Customers can deploy an IPv6 RADIUS server or a TACACS+ server to communicate with Cisco devices.

TACACS+ Over an IPv6 Transport

An IPv6 server can be configured to use TACACS+. Both IPv6 and IPv4 servers can be configured to use TACACS+ using a name instead of an IPv4 or IPv6 address.

How to Configure TACACS+ over IPv6

Configuring the TACACS+ Server over IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tacacs server** *name*
4. **address ipv6** *ipv6-address*
5. **key** [**0** | **7**] *key-string*
6. **port** [*number*
7. **send-nat-address**
8. **single-connection**
9. **timeout** *seconds*

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.

	Command or Action	Purpose
Step 3	**tacacs server** *name* **Example:** `Device(config)# tacacs server server1`	Configures the TACACS+ server for IPv6 and enters TACACS+ server configuration mode.
Step 4	**address ipv6** *ipv6-address* **Example:** `Device(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5`	Configures the IPv6 address of the TACACS+ server.
Step 5	**key** [**0** | **7**] *key-string* **Example:** `Device(config-server-tacacs)# key 0 key1`	Configures the per-server encryption key on the TACACS+ server.
Step 6	**port** [*number* **Example:** `Device(config-server-tacacs)# port 12`	Specifies the TCP port to be used for TACACS+ connections.
Step 7	**send-nat-address** **Example:** `Device(config-server-tacacs)# send-nat-address`	Sends a client's post-NAT address to the TACACS+ server.
Step 8	**single-connection** **Example:** `Device(config-server-tacacs)# single-connection`	Enables all TACACS packets to be sent to the same server using a single TCP connection.
Step 9	**timeout** *seconds* **Example:** `Device(config-server-tacacs)# timeout 10`	Configures the time to wait for a reply from the specified TACACS server.

Specifying the Source Address in TACACS+ Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 tacacs source-interface** *type number*

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	**ipv6 tacacs source-interface** *type number* **Example:** `Device(config)# ipv6 tacacs source-interface Gigabitethernet 1/2/1`	Specifies an interface to use for the source address in TACACS+ packets.

Configuring TACACS+ Server Group Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server tacacs+** *group-name*
4. **server name** *server-name*
5. **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

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 group server tacacs+** *group-name* **Example:** `Device(config)# aaa group server tacacs+ group1`	Groups different TACACS+ server hosts into distinct lists and distinct methods.
Step 4	**server name** *server-name* **Example:** `Device(config-sg-tacacs+)# server name server1`	Specifies an IPv6 TACACS+ server.
Step 5	**server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] **Example:** `Device(config-sg-tacacs+)# server-private 2001:DB8:3333:4::5 port 19 key key1`	Configures the IPv6 address of the private TACACS+ server for the group server.

Configuration Examples for TACACS+ over IPv6

Example: Configuring TACACS+ Server over IPv6

```
Device# show tacacs

            Tacacs+ Server:          server1
            Server Address:          FE80::200:F8FF:FE21:67CF
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
           Socket Timeouts:          0
   Failed Connect Attempts:          0
```

```
        Total Packets Sent:          0
        Total Packets Recv:          0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Commands	Cisco IOS Master Command List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
IPv6 features	CiscoIOS_IPv6_Feature_Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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 TACACS+ over IPv6

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 40: Feature Information for TACACS+ over IPv6

Feature Name	Releases	Feature Information
TACACS+ over IPv6	12.2(33)SXJ 12.2(58)SE 15.1(1)S 15.2(1)T	The TACACS+ over IPv6 feature allows you to configure an IPv6 server to use the TACACS+ security protocol. The following commands were introduced or modified: **aaa group server tacacs+**, **address ipv6 (TACACS+)**, **ipv6 tacacs source-interface**, **key (TACACS+)**, **port (TACACS+)**, **send-nat-address**, **server name (IPv6 TACACS+)**, **server-private (TACACS+)**, **single-connection**, **tacacs server**, **timeout (TACACS+)**.

CHAPTER 23

Token Authentication

The Token Authentication feature allows you to secure the authentication mechanism by protecting it with a temporary authentication access. This feature increases the security to the network by providing a time-bound access without revealing the password to the login user.

- Finding Feature Information, page 335
- Prerequisites for Token Authentication, page 335
- Restrictions for Token Authentication, page 336
- Information About Token Authentication, page 336
- How to Configure Token Authentication, page 337
- Configuration Examples for Token Authentication, page 338
- Additional References for Token Authentication, page 338
- Feature Information for Token Authentication, page 339

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 Token Authentication

- Ensure that AAA authentication is configured on the device. For more information, see the "Configuring Authentication" chapter in the *Authentication, Authorization, and Accounting Configuration Guide*.
- You must configure the user account using the **token** keyword before configuring the token authentication.

Restrictions for Token Authentication

- The Token Authentication feature requires the Connected Grid (CG) network management system (NMS) to generate the authentication token.

Information About Token Authentication

Token Authentication Overview

Token Authentication is a method to provide a device-bound and time-bound access to a Cisco IOS device that is offline and therefore not able to reach the AAA database for a proper authentication. The access is unauthenticated and should be used in caution, in particular the privilege level granted to the session.

Token authentication can configure the privilege level for the technician to grant access for any operation on the device. This feature is used to grant a technician access to the Cisco IOS device to perform simple device management such as statistics collection or even restarting an interface while the Cisco IOS device is in an error state and disconnected from the rest of the network.

The local technician accounts are authorized with a temporary time-bound authentication token without exposing the password. The token structure is encrypted and not visible to the technician. The technician uses this encrypted token as the password.

The generated token is encrypted with the token encryption key and provided to the technician. Once the temporary time-bound authentication token is used as the login credential, it is decrypted and verified by the local AAA database by using the token encryption key.

The network security is protected by ensuring that the technician is given access to the network after authenticating the technician's token credentials (shared by the Connected Grid [CG] network management system [NMS] and the device). In addition, this access is for a limited time period that is embedded inside the token structure. Beyond that specific time period in which the token is valid, the technician's session is disconnected and no future network session is allowed with the same token.

How to Configure Token Authentication

Configuring Token Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **token password** *encryption-type password*
4. **aaa new-model**
5. **aaa authentication login default** *method1* [*method2 ...*]
6. **aaa authentication token key** *string*
7. **exit**

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	**username** *name* [**privilege** *level*] **token password** *encryption-type password* **Example:** `Device(config)# username user1 privilege 1 token password 0 cisco123`	Establishes a username-based authentication system.
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) network security services.

	Command or Action	Purpose
Step 5	**aaa authentication login default** *method1* [*method2* ...] **Example:** `Device(config)# aaa authentication login default local`	Sets AAA authentication at login.
Step 6	**aaa authentication token key** *string* **Example:** `Device(config)# aaa authentication token key abcdefghcisco123`	Creates a token authentication key to provide temporary access to the network.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuration Examples for Token Authentication

Example: Configuring Token Authentication Key

```
Device> enable
Device# configure terminal
Device(config)# username user1 privilege 1 token password 0 cisco123
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authentication token key abcdefghcisco123
Device(config)# exit
```

Additional References for Token Authentication

Related Documents

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

Related Topic	Document Title
Security commands	- Cisco IOS Security Command Reference: Commands A to C - Cisco IOS Security Command Reference: Commands D to L - Cisco IOS Security Command Reference: Commands M to R - Cisco IOS Security Command Reference: Commands S to Z
AAA authentication	"Configuring Authentication" chapter in the *Authentication, Authorization, and Accounting Configuration Guide*

Technical Assistance

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

Feature Information for Token Authentication

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 Token Authentication

Feature Name	Releases	Feature Information
Token Authentication	15.4(1)T	The Token Authentication feature allows you to secure the authentication mechanism by protecting it with a temporary authentication access. This feature increases the security to the network by providing a time-bound access without revealing the password to the login user. The following command was introduced or modified: **aaa authentication token key**.

CHAPTER 24

Secure Reversible Passwords for AAA

The Secure Reversible Passwords for AAA feature enables secure reversible encryption for authentication, authorization, and accounting (AAA) configurations using type 6 advanced encryption scheme (AES) passwords.

- Finding Feature Information, page 341
- Prerequisites for Secure Reversible Passwords for AAA, page 341
- Information About Secure Reversible Passwords for AAA, page 342
- Additional References for Secure Reversible Passwords for AAA, page 343
- Feature Information for Secure Reversible Passwords for AAA, page 344

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 Secure Reversible Passwords for AAA

The following commands should be enabled for the type 6 password encryption:

- **password encryption aes**
- **key config-key password-encrypt** [*password*]
- **aaa new-model**

Information About Secure Reversible Passwords for AAA

Secure Reversible Passwords

Passwords in Cisco IOS configurations require a secure storage so that the key for the reversible encryption can be stored to ensure that authentication methods can access the user credentials whenever required.

Reversible encryption is the process by which a password is encrypted with a reversible, symmetric encryption algorithm. To check if the password entered by the user is valid, the password is decrypted and compared to the user-input password. To perform this encryption, the symmetric encryption algorithm requires a key.

The type 6 advanced encryption scheme (AES) encrypted passwords help to secure the reversible passwords for authentication, authorization, and accounting (AAA) features. This type 6 encryption key is stored in a private NVRAM and secured.

AAA network configurations use Lightweight Directory Access Protocol (LDAP), RADIUS, or TACACS+ server hosts. Use the **radius server host**, **tacacs-server host**, and **ldap server** commands to configure RADIUS, TACACS+, or LDAP host servers respectively.

Type 6 Encryption Configuration

The following commands have been updated with the type **6** keyword to enable secure reversible passwords to configure authentication, authorization, and accounting (AAA) features. For more information about the security commands, see the *Cisco IOS Security Command Reference*. For more information about AAA configuration, see the *Authentication, Authorization, and Accounting Configuration Guide*.

- **aaa configuration**
  - **aaa configuration** {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*}
- **bind authenticate root-dn (config-ldap-server)**
  - **bind authenticate root-dn** *username* **password** {**0** *string* | **6** *string* | **7** *string*} *string*
- **client (config-locsvr-da-radius)**
  - **client** *ip-address* **server-key** [**0** | **6** | **7**] *word*
- **key (config-radius-server)**
  - **key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **key (config-server-tacacs)**
  - **key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **pac key (config-radius-server)**
  - **pac key** {**0** *string* | **6** *string* | **7** *string*} *string*

- **password (config-filter)**
    - **password** [**0** | **6** | **7**] *password*
- **server-private (RADIUS)**
    - **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** [**0** | **6** | **7**] *string*]
- **server-private (TACACS+)**
    - **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **6** | **7**] *string*]
- **tacacs-server host**
    - **tacacs-server host** {*host-name* | *host-ip-address*} [**key** {**0** *string* | **6** *string* | **7** *string*} *string*] [[**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]]
- **tacacas-server key**
    - **tacacs-server key** {**0** *string* | **6** *string* | **7** *string*} *string*

Additional References for Secure Reversible Passwords for AAA

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
AAA configuration	*Authentication, Authorization, and Accounting Configuration Guide*

Technical Assistance

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

Feature Information for Secure Reversible Passwords for AAA

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 Secure Reversible Passwords for AAA

Feature Name	Releases	Feature Information
Secure Reversible Passwords for AAA	15.4(1)T	The Secure Reversible Passwords for AAA feature enables secure reversible encryption for authentication, authorization, and accounting (AAA) configurations using type 6 advanced encryption scheme (AES) passwords. The following commands were introduced or modified: **aaa configuration**, **bind authenticate root-dn (config-ldap-server)**, **client (config-locsvr-da-radius)**, **key (config-radius-server)**, **key (config-server-tacacs)**, **pac key (config-radius-server)**, **password (config-filter)**, **server-private (RADIUS)**, **server-private (TACACS+)**, **tacacs-server host**, and **tacacas-server key**.