



Authentication Authorization and Accounting Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

Americas Headquarters

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

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

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

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

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

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Read Me First 1

CHAPTER 2

Configuring Authentication 3

- Finding Feature Information 3
- Prerequisites for Configuring Authentication 3
- Restrictions for Configuring Authentication 3
- Information About Configuring Authentication 4
 - Named Method Lists for Authentication 4
 - Method Lists and Server Groups 4
 - Method List Examples 5
 - About RADIUS Change of Authorization 6
 - CoA Requests 7
 - CoA Request Response Code 8
 - CoA Request Commands 9
 - Domain Stripping 11
- How to Configure AAA Authentication Methods 11
- Configuring Login Authentication Using AAA 11
 - Login Authentication Using Enable Password 13
 - Login Authentication Using Kerberos 13
 - Login Authentication Using Line Password 14
 - Login Authentication Using Local Password 14
 - Login Authentication Using Group RADIUS 14
 - Configuring RADIUS Attribute 8 in Access Requests 14
 - Login Authentication Using Group TACACS 15
 - Login Authentication Using group group-name 15
- Configuring PPP Authentication Using AAA 15

| | |
|---|----|
| PPP Authentication Using Kerberos | 17 |
| PPP Authentication Using Local Password | 17 |
| PPP Authentication Using Group RADIUS | 18 |
| Configuring RADIUS Attribute 44 in Access Requests | 18 |
| PPP Authentication Using Group TACACS | 18 |
| PPP Authentication Using group group-name | 18 |
| Configuring AAA Scalability for PPP Requests | 19 |
| Configuring ARAP Authentication Using AAA | 19 |
| ARAP Authentication Allowing Authorized Guest Logins | 21 |
| ARAP Authentication Allowing Guest Logins | 21 |
| ARAP Authentication Using Line Password | 21 |
| ARAP Authentication Using Local Password | 22 |
| ARAP Authentication Using Group RADIUS | 22 |
| ARAP Authentication Using Group TACACS | 22 |
| ARAP Authentication Using Group group-name | 22 |
| Configuring NASI Authentication Using AAA | 23 |
| NASI Authentication Using Enable Password | 24 |
| NASI Authentication Using Line Password | 25 |
| NASI Authentication Using Local Password | 25 |
| NASI Authentication Using Group RADIUS | 25 |
| NASI Authentication Using Group TACACS | 25 |
| NASI Authentication Using group group-name | 25 |
| Specifying the Amount of Time for Login Input | 26 |
| Enabling Password Protection at the Privileged Level | 26 |
| Changing the Text Displayed at the Password Prompt | 27 |
| Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server | 28 |
| Configuring Message Banners for AAA Authentication | 29 |
| Configuring a Login Banner | 29 |
| Configuring a Failed-Login Banner | 29 |
| Configuring AAA Packet of Disconnect | 30 |
| Enabling Double Authentication | 31 |
| How Double Authentication Works | 31 |
| Configuring Double Authentication | 32 |
| Accessing the User Profile After Double Authentication | 33 |

| | |
|---|----|
| Enabling Automated Double Authentication | 33 |
| Configuring Automated Double Authentication | 35 |
| Troubleshooting Automated Double Authentication | 35 |
| Configuring the Dynamic Authorization Service for RADIUS CoA | 36 |
| Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests | 37 |
| Configuring Domain Stripping at the Server Group Level | 38 |
| Non-AAA Authentication Methods | 39 |
| Configuring Line Password Protection | 39 |
| Establishing Username Authentication | 40 |
| Enabling CHAP or PAP Authentication | 42 |
| Enabling PPP Encapsulation | 43 |
| Enabling PAP or CHAP | 43 |
| Inbound and Outbound Authentication | 44 |
| Enabling Outbound PAP Authentication | 44 |
| Refusing PAP Authentication Requests | 44 |
| Creating a Common CHAP Password | 45 |
| Refusing CHAP Authentication Requests | 45 |
| Delaying CHAP Authentication Until Peer Authenticates | 45 |
| Using MS-CHAP | 46 |
| Defining PPP Authentication using MS-CHAP | 46 |
| Authentication Examples | 47 |
| RADIUS Authentication Examples | 47 |
| TACACS Authentication Examples | 49 |
| Kerberos Authentication Examples | 49 |
| AAA Scalability Example | 50 |
| Example: Configuring Login and Failed-Login Banners for AAA Authentication | 51 |
| AAA Packet of Disconnect Server Key Example | 52 |
| Double Authentication Examples | 52 |
| Configuration of the Local Host for AAA with Double Authentication Examples | 52 |
| Configuration of the AAA Server for First-Stage PPP Authentication and Authorization Example | 53 |
| Configuration of the AAA Server for Second-Stage Per-User Authentication and Authorization Examples | 53 |
| Complete Configuration with TACACS Example | 54 |

Automated Double Authentication Example 57
 Additional References 59
 Feature Information for Configuring Authentication 60

CHAPTER 3

RADIUS Change of Authorization 63

Finding Feature Information 63
 Information About RADIUS Change of Authorization 63
 About RADIUS Change of Authorization 63
 CoA Requests 64
 CoA Request Response Code 65
 CoA Request Commands 66
 How to Configure RADIUS Change of Authorization 68
 Configuring RADIUS Change of Authorization 68
 Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests 69
 Configuring the Dynamic Authorization Service for RADIUS CoA 70
 Monitoring and Troubleshooting RADIUS Change of Authorization 72
 Configuration Examples for RADIUS Change of Authorization 72
 Example: Configuring RADIUS Change of Authorization 72
 Example: Configuring a Device to Ignore Bounce and Disable a RADIUS Requests 73
 Example: Configuring the Dynamic Authorization Service for RADIUS CoA 73
 Additional References for RADIUS Change of Authorization 73
 Feature Information for RADIUS Change of Authorization 74

CHAPTER 4

Message Banners for AAA Authentication 77

Finding Feature Information 77
 Information About Message Banners for AAA Authentication 77
 Login and Failed-Login Banners for AAA Authentication 77
 How to Configure Message Banners for AAA Authentication 78
 Configuring a Login Banner for AAA Authentication 78
 Configuring a Failed-Login Banner for AAA Authentication 79
 Configuration Examples for Message Banners for AAA Authentication 80
 Example: Configuring Login and Failed-Login Banners for AAA Authentication 80
 Additional References for Message Banners for AAA Authentication 81
 Feature Information for Message Banners for AAA Authentication 81

CHAPTER 5**AAA-Domain Stripping at Server Group Level 83**

- Finding Feature Information 83
- Information About AAA-Domain Stripping at Server Group Level 83
- How to Configure AAA-Domain Stripping at Server Level Group 84
 - Configuring Domain Stripping at the Server Group Level 84
- Configuration Example for AAA-Domain Stripping at Server Group Level 85
 - Example: AAA-Domain Stripping at Server Group Level 85
- Additional References 85
- Feature Information for AAA-Domain Stripping at Server Group Level 87

CHAPTER 6**AAA Double Authentication Secured by Absolute Timeout 89**

- Finding Feature Information 89
- Prerequisites for AAA Double Authentication Secured by Absolute Timeout 89
- Restrictions for AAA Double Authentication Secured by Absolute Timeout 90
- Information About AAA Double Authentication Secured by Absolute Timeout 90
 - AAA Double Authentication 90
- How to Apply AAA Double Authentication Secured by Absolute Timeout 90
 - Applying AAA Double Authentication Secured by Absolute Timeout 90
- Configuration Examples for AAA Double Authentication Secured by Absolute Timeout 91
 - Example: RADIUS User Profile 91
 - Example: TACACS User Profile 92
- Additional References 94
- Feature Information for AAA Double Authentication Secured by Absolute Timeout 95

CHAPTER 7**Throttling of AAA RADIUS Records 97**

- Finding Feature Information 97
- Information About Throttling of AAA RADIUS Records 97
 - Benefits of the Throttling of AAA RADIUS Records Feature 97
 - Throttling Access Requests and Accounting Records 98
- How to Configure Throttling of AAA RADIUS Records 98
 - Throttling Accounting and Access Request Packets Globally 99
 - Throttling Accounting and Access Request Packets Per Server Group 99
- Configuration Examples for Throttling of AAA RADIUS Records 101

Throttling Accounting and Access Request Packets Globally Example 101

Throttling Accounting and Access Request Packets Per Server Group Example 101

Additional References 102

Feature Information for Throttling of AAA RADIUS Records 103

CHAPTER 8

RADIUS Packet of Disconnect 105

Finding Feature Information 105

Prerequisites for RADIUS Packet of Disconnect 105

Restrictions for RADIUS Packet of Disconnect 105

Information About RADIUS Packet of Disconnect 106

 When the POD is Needed 106

 POD Parameters 106

How to Configure the RADIUS Packet of Disconnect 107

 Configuring the RADIUS POD 107

 Troubleshooting Tips 109

 Verifying the RADIUS POD Configuration 109

Additional References 109

Feature Information for RADIUS Packet of Disconnect 110

Glossary 111

CHAPTER 9

AAA Authorization and Authentication Cache 113

Finding Feature Information 113

Prerequisites for Implementing Authorization and Authentication Profile Caching 113

Information About Implementing Authorization and Authentication Profile Caching 114

 Network Performance Optimization Using Authorization and Authentication Profile Caching 114

 Authorization and Authentication Profile Caching as a Failover Mechanism 114

 Method Lists in Authorization and Authentication Profile Caching 115

 Authorization and Authentication Profile Caching Guidelines 115

 General Configuration Procedure for Implementing Authorization and Authentication Profile Caching 115

How to Implement Authorization and Authentication Profile Caching 116

 Creating Cache Profile Groups and Defining Caching Rules 116

 Defining RADIUS and TACACS Server Groups That Use Cache Profile Group Information 118

| | |
|---|-----|
| Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used | 119 |
| Configuration Examples for Implementing Authorization and Authentication Profile Caching | 121 |
| Implementing Authorization and Authentication Profile Caching for Network Optimization Example | 121 |
| Implementing Authorization and Authentication Profile Caching as a Failover Mechanism Example | 122 |
| Additional References for RADIUS Change of Authorization | 124 |
| Feature Information for Implementing Authorization and Authentication Profile Caching | 125 |

CHAPTER 10**Configuring Authorization 127**

| | |
|---|-----|
| Finding Feature Information | 127 |
| AAA Authorization Prerequisites | 127 |
| Information About Configuring Authorization | 128 |
| Named Method Lists for Authorization | 128 |
| AAA Authorization Methods | 129 |
| Authorization Methods | 129 |
| Method Lists and Server Groups | 130 |
| AAA Authorization Types | 130 |
| Authorization Types | 131 |
| Authorization Attribute-Value Pairs | 131 |
| How to Configure Authorization | 131 |
| Configuring AAA Authorization Using Named Method Lists | 131 |
| Disabling Authorization for Global Configuration Commands | 132 |
| Configuring Authorization for Reverse Telnet | 133 |
| Authorization Configuration Examples | 134 |
| TACACS Authorization Examples | 134 |
| RADIUS Authorization Example | 134 |
| Reverse Telnet Authorization Examples | 135 |
| Additional References | 137 |
| Feature Information for Configuring Authorization | 138 |

CHAPTER 11**Configuring Accounting 139**

| | |
|-----------------------------|-----|
| Finding Feature Information | 139 |
|-----------------------------|-----|

| | |
|---|-----|
| Prerequisites for Configuring Accounting | 139 |
| Restrictions for Configuring Accounting | 140 |
| Information About Configuring Accounting | 140 |
| Named Method Lists for Accounting | 140 |
| Method Lists and Server Groups | 141 |
| AAA Accounting Methods | 142 |
| AAA Accounting Types | 143 |
| Network Accounting | 144 |
| EXEC Accounting | 146 |
| Command Accounting | 147 |
| Connection Accounting | 148 |
| System Accounting | 150 |
| Resource Accounting | 150 |
| AAA Accounting Enhancements | 152 |
| AAA Broadcast Accounting | 152 |
| AAA Session MIB | 153 |
| Accounting Attribute-Value Pairs | 154 |
| How to Configure AAA Accounting | 154 |
| Configuring AAA Accounting Using Named Method Lists | 154 |
| Suppressing Generation of Accounting Records for Null Username Sessions | 155 |
| Generating Interim Accounting Records | 155 |
| Configuring an Alternate Method to Enable Periodic Accounting Records | 155 |
| Generating Interim Service Accounting Records | 156 |
| Generating Accounting Records for a Failed Login or Session | 157 |
| Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records | 157 |
| Suppressing System Accounting Records over Switchover | 158 |
| Configuring AAA Resource Failure Stop Accounting | 158 |
| Configuring AAA Resource Accounting for Start-Stop Records | 158 |
| Configuring AAA Broadcast Accounting | 159 |
| Configuring per-DNIS AAA Broadcast Accounting | 159 |
| Configuring the AAA Session MIB | 159 |
| Establishing a Session with a Router if the AAA Server Is Unreachable | 160 |
| Monitoring Accounting | 160 |
| Troubleshooting Accounting | 160 |

| | |
|---|-----|
| Configuration Examples for AAA Accounting | 161 |
| Configuring a Named Method List Example | 161 |
| Configuring AAA Resource Accounting Example | 163 |
| Configuring AAA Broadcast Accounting Example | 163 |
| Configuring per-DNIS AAA Broadcast Accounting Example | 164 |
| AAA Session MIB Example | 164 |
| Additional References | 164 |
| Feature Information for Configuring Accounting | 165 |

CHAPTER 12

| | |
|---|------------|
| AAA-SERVER-MIB Set Operation | 167 |
| Finding Feature Information | 167 |
| Prerequisites for AAA-SERVER-MIB Set Operation | 167 |
| Restrictions for AAA-SERVER-MIB Set Operation | 168 |
| Information About AAA-SERVER-MIB Set Operation | 168 |
| CISCO-AAA-SERVER-MIB | 168 |
| CISCO-AAA-SERVER-MIB Set Operation | 168 |
| How to Configure AAA-SERVER-MIB Set Operation | 168 |
| Verifying RADIUS Server Configuration and Server Statistics | 168 |
| Configuration Examples for AAA-SERVER-MIB Set Operation | 169 |
| RADIUS Server Configuration and Server Statistics Example | 169 |
| Additional References | 171 |
| Feature Information for AAA-SERVER-MIB Set Operation | 172 |

CHAPTER 13

| | |
|--------------------------------|------------|
| Per VRF AAA | 173 |
| Prerequisites for Per VRF AAA | 173 |
| Restrictions for Per VRF AAA | 173 |
| Information About Per VRF AAA | 174 |
| How Per VRF AAA Works | 174 |
| AAA Accounting Records | 174 |
| New Vendor-Specific Attributes | 174 |
| VRF Aware Framed-Routes | 178 |
| How to Configure Per VRF AAA | 178 |
| Configuring Per VRF AAA | 178 |
| Configuring AAA | 178 |

| | |
|--|-----|
| Configuring Server Groups | 178 |
| Configuring Authentication Authorization and Accounting for Per VRF AAA | 179 |
| Configuring RADIUS-Specific Commands for Per VRF AAA | 181 |
| Configuring Interface-Specific Commands for Per VRF AAA | 182 |
| Configuring Per VRF AAA Using Local Customer Templates | 183 |
| Configuring AAA | 183 |
| Configuring Server Groups | 183 |
| Configuring Authentication Authorization and Accounting for Per VRF AAA | 183 |
| Configuring Authorization for Per VRF AAA with Local Customer Templates | 184 |
| Configuring Local Customer Templates | 184 |
| Configuring Per VRF AAA Using Remote Customer Templates | 186 |
| Configuring AAA | 186 |
| Configuring Server Groups | 186 |
| Configuring Authentication for Per VRF AAA with Remote Customer Profiles | 186 |
| Configuring Authorization for Per VRF AAA with Remote Customer Profiles | 187 |
| Configuring the RADIUS Profile on the SP RADIUS Server | 188 |
| Verifying VRF Routing Configurations | 188 |
| Troubleshooting Per VRF AAA Configurations | 188 |
| Configuration Examples for Per VRF AAA | 189 |
| Per VRF Configuration Examples | 189 |
| Per VRF AAA Example | 189 |
| Per VRF AAA Using a Locally Defined Customer Template Example | 189 |
| Per VRF AAA Using a Remote RADIUS Customer Template Example | 190 |
| Customer Template Examples | 190 |
| Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example | 190 |
| Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example | 191 |
| AAA Accounting Stop Record Examples | 192 |
| AAA Accounting Stop Record and Rejected Call Example | 192 |
| AAA Accounting Stop Record and Successful Call Example | 195 |
| Additional References | 197 |
| Feature Information for Per VRF AAA | 198 |
| Glossary | 200 |

| | | |
|-------------------|---|------------|
| CHAPTER 14 | AAA Support for IPv6 | 201 |
| | Finding Feature Information | 201 |
| | Information About AAA Support for IPv6 | 201 |
| | AAA over IPv6 | 201 |
| | AAA Support for IPv6 RADIUS Attributes | 201 |
| | How to Configure AAA Support for IPv6 | 206 |
| | Configuring DHCPv6 AAA Options | 206 |
| | Configuration Examples for AAA Support for IPv6 | 207 |
| | Example: DHCPv6 AAA Options Configuration | 207 |
| | Example: RADIUS Configuration | 207 |
| | Additional References | 207 |
| | Feature Information for RADIUS over IPv6 | 209 |

| | | |
|-------------------|--|------------|
| CHAPTER 15 | TACACS+ over IPv6 | 211 |
| | Finding Feature Information | 211 |
| | Information About TACACS+ over IPv6 | 211 |
| | AAA over IPv6 | 211 |
| | TACACS+ Over an IPv6 Transport | 212 |
| | How to Configure TACACS+ over IPv6 | 212 |
| | Configuring the TACACS+ Server over IPv6 | 212 |
| | Specifying the Source Address in TACACS+ Packets | 213 |
| | Configuring TACACS+ Server Group Options | 214 |
| | Configuration Examples for TACACS+ over IPv6 | 215 |
| | Example: Configuring TACACS+ Server over IPv6 | 215 |
| | Additional References | 215 |
| | Feature Information for TACACS+ over IPv6 | 217 |

| | | |
|-------------------|--|------------|
| CHAPTER 16 | AAA Dead-Server Detection | 219 |
| | Finding Feature Information | 219 |
| | Prerequisites for AAA Dead-Server Detection | 219 |
| | Restrictions for AAA Dead-Server Detection | 220 |
| | Information About AAA Dead-Server Detection | 220 |
| | Criteria for Marking a RADIUS Server As Dead | 220 |

How to Configure AAA Dead-Server Detection 220

- Configuring AAA Dead-Server Detection 220
 - Troubleshooting Tips 221
 - Verifying AAA Dead-Server Detection 221
- Configuration Examples for AAA Dead-Server Detection 222
 - Configuring AAA Dead-Server Detection Example 222
 - debug aaa dead-criteria transactions Command Example 222
 - show aaa dead-criteria Command Example 223
- Additional References 223
- Feature Information for AAA Dead-Server Detection 224

CHAPTER 17

Login Password Retry Lockout 227

- Finding Feature Information 227
- Prerequisites for Login Password Retry Lockout 227
- Restrictions for Login Password Retry Lockout 227
- Information About Login Password Retry Lockout 228
 - Lock Out of a Local AAA User Account 228
- How to Configure Login Password Retry Lockout 228
 - Configuring Login Password Retry Lockout 228
 - Unlocking a Login Locked-Out User 229
 - Clearing the Unsuccessful Login Attempts of a User 230
 - Monitoring and Maintaining Login Password Retry Lockout Status 231
- Configuration Examples for Login Password Retry Lockout 231
 - Displaying the Login Password Retry Lockout Configuration Example 231
- Additional References 232
- Feature Information for Login Password Retry Lockout 233
- Glossary 233

CHAPTER 18

MSCHAP Version 2 235

- Finding Feature Information 235
- Prerequisites for MSCHAP Version 2 236
- Restrictions for MSCHAP Version 2 236
- Information About MSCHAP Version 2 236
- How to Configure MSCHAP Version 2 237

| | |
|---|-----|
| Configuring MSCHAP V2 Authentication | 237 |
| Verifying MSCHAP V2 Configuration | 238 |
| Configuring Password Aging for Crypto-Based Clients | 239 |
| Configuration Examples | 240 |
| Configuring Local Authentication Example | 240 |
| Configuring RADIUS Authentication Example | 240 |
| Configuring Password Aging with Crypto Authentication Example | 241 |
| Additional References | 241 |
| Feature Information for MSCHAP Version 2 | 243 |

CHAPTER 19**AAA Broadcast Accounting-Mandatory Response Support 245**

| | |
|--|-----|
| Finding Feature Information | 245 |
| Prerequisites for AAA Broadcast Accounting-Mandatory Response Support | 245 |
| Restrictions for AAA Broadcast Accounting-Mandatory Response Support | 246 |
| Information About AAA Broadcast Accounting-Mandatory Response Support | 246 |
| AAA Broadcast Accounting | 246 |
| Simultaneous Broadcast and Wait Accounting | 246 |
| How AAA Broadcast Accounting is Supported for GGSN | 247 |
| Configuring Broadcast and Wait Accounting on the GGSN | 247 |
| Configuration Examples for AAA Broadcast Accounting-Mandatory Response Support | 249 |
| AAA Broadcast Accounting-Mandatory Response Support Example | 249 |
| Additional References | 250 |
| Feature Information for AAA Broadcast Accounting-Mandatory Response Support | 252 |

CHAPTER 20**Password Strength and Management for Common Criteria 253**

| | |
|--|-----|
| Finding Feature Information | 253 |
| Restrictions for Password Strength and Management for Common Criteria | 254 |
| Information About Password Strength and Management for Common Criteria | 254 |
| Password Composition Policy | 254 |
| Password Length Policy | 254 |
| Password Lifetime Policy | 254 |
| Password Expiry Policy | 255 |
| Password Change Policy | 255 |
| User Reauthentication Policy | 255 |

- Support for Framed (noninteractive) Session 256
- How to Configure Password Strength and Management for Common Criteria 256
 - Configuring the Password Security Policy 256
 - Verifying the Common Criteria Policy 258
 - Troubleshooting Tips 259
- Configuration Example for the Password Strength and Management for Common Criteria Feature 259
 - Example: Password Strength and Management for Common Criteria 259
- Additional References 260
- Feature Information for Password Strength and Management for Common Criteria 261

CHAPTER 21

- Secure Reversible Passwords for AAA 263**
 - Finding Feature Information 263
 - Prerequisites for Secure Reversible Passwords for AAA 263
 - Information About Secure Reversible Passwords for AAA 264
 - Secure Reversible Passwords 264
 - Type 6 Encryption Configuration 264
 - Additional References for Secure Reversible Passwords for AAA 265
 - Feature Information for Secure Reversible Passwords for AAA 266



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).



CHAPTER 2

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, on page 3](#)
- [Prerequisites for Configuring Authentication, on page 3](#)
- [Restrictions for Configuring Authentication, on page 3](#)
- [Information About Configuring Authentication, on page 4](#)
- [How to Configure AAA Authentication Methods, on page 11](#)
- [Non-AAA Authentication Methods, on page 39](#)
- [Authentication Examples, on page 47](#)
- [Additional References, on page 59](#)
- [Feature Information for Configuring Authentication, on page 60](#)

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 IOS XE implementation of authentication is divided into AAA Authentication and non-authentication 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.

- Web authentication is not supported on Cisco IOS XE software.

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

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

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

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

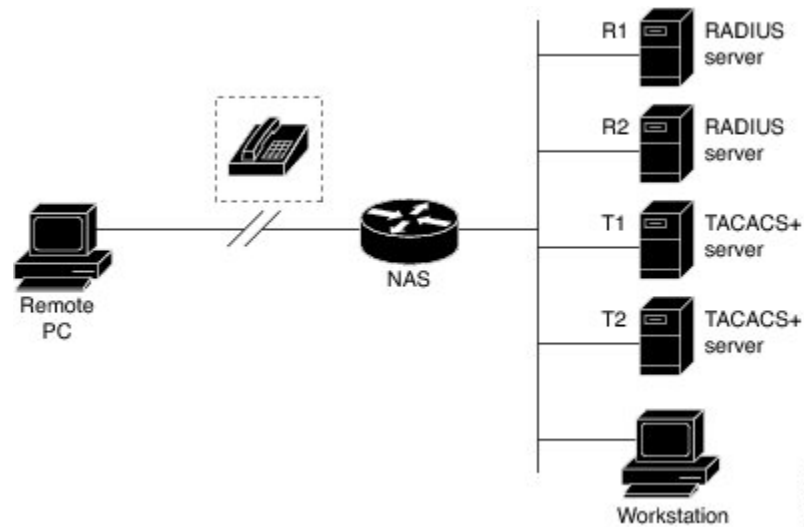


Note The number of AAA method lists that can be configured is 250.

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS 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 a server group, and define T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for PPP authentication.

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

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, then if there is no response, R2 is contacted. If R2 does not respond, T1 in the TACACS+ group is contacted; if T1 does not respond, T2 is contacted. If all designated servers fail to respond, authentication falls to the local username database on the access server itself. To implement this solution, the system administrator would create a default method list by entering the following command:

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

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

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

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

Suppose the system administrator wants to apply a method list only to a particular interface or set of interfaces. In this case, 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 apple
```

In this example, “apple” 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 (apple) in both the AAA and 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 whose members are R2 (172.16.2.7) and T2 (172.16.2.77), respectively. In this example, the RADIUS server group “rad2only” is defined as follows using the **aaa group server** command:

```
aaa group server radius rad2only
 server 172.16.2.7
```

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

```
aaa group server tacacs+ tac2only
 server 172.16.2.77
```

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

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

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 |
| 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) |

| Value | Explanation |
|-------|--|
| 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" |
| 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 802.1x, 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, reenale 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, reenale 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 until you enable AAA globally using the **aaa new-model** command.

For authentication configuration examples using the commands in this chapter, refer to the Authentication Examples.

Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login** command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

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

SUMMARY STEPS

1. Router(config)# **aaa new-model**

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | Router(config)# aaa new-model | Enables AAA globally. |
| Step 2 | Router(config)# aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2</i> ...] | Creates a local authentication list. |
| Step 3 | Router(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 | Router(config-line)# login authentication Example: { default <i>list-name</i> } | Applies the authentication list to a line or set of lines. |

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. 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, enter the following command:

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



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

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 router. 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 radius | Uses the list of all RADIUS servers for authentication. |
| group tacacs+ | Uses the list of all TACACS+ servers for authentication. |
| group <i>group-name</i> | 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 only changes username and privilege level but does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way.

Login Authentication Using Enable Password

Use the **aaa authentication login** command with the **enable method** keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter 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 via 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 router. The user is then prompted for a password, and the router 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 router.

While `krb5` does use the KINIT program, a user does not need to run the KINIT program to get a TGT to authenticate to the router. This is because KINIT has been integrated into the login procedure in the Cisco IOS XE implementation of Kerberos.

Use the **aaa authentication login** command with the **krb5** *method* 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, enter the following command:

```
aaa authentication login default krb5
```

Before you can use Kerberos as the login authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the chapter “Configuring Kerberos.”

Login Authentication Using Line Password

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

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you need to define a line password. For more information about defining line passwords, refer to the Configuring Line Password Protection.

Login Authentication Using Local Password

Use the **aaa authentication login** command with the **local** *method* keyword to specify that the Cisco router 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, enter the following command:

```
aaa authentication login default local
```

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

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, enter the following command:

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

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

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, enter the following command:

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

Before you can use TACACS+ as the login authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Login Authentication Using group group-name

Use the **aaa authentication login** command with the **group group-name** method to specify a subset of RADIUS or TACACS+ servers to use as the login authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define 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 user authentication at login when no other method list has been defined, enter the following command:

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

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

Configuring PPP Authentication Using AAA

Many users access network access servers through dialup via async or ISDN. Dialup via async or ISDN bypasses the CLI completely; instead, a network protocol (such as PPP or 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 no matter 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. Router(config)# **aaa new-model**
2. Router(config)# **aaa authentication ppp** {default | list-name} method1[method2...]
3. Router(config)# **interface** interface-type interface-number
4. Router(config-if)# **ppp authentication** {protocol1 [protocol2...]} [if-needed] {default | list-name} [callin] [one-time][optional]

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | Router(config)# aaa new-model | Enables AAA globally. |
| Step 2 | Router(config)# aaa authentication ppp {default list-name} method1[method2...] | Creates a local authentication list. |
| Step 3 | Router(config)# interface interface-type interface-number | Enters interface configuration mode for the interface to which you want to apply the authentication list. |
| Step 4 | Router(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, <i>protocol1</i> and <i>protocol2</i> represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, specified by <i>protocol1</i> . If <i>protocol1</i> 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 create one or more lists of authentication methods that are tried when a user tries to authenticate via PPP. These lists are applied 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, enter 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, enter 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 user has already been authenticated on a TTY line. |
| krb5 | Uses Kerberos 5 for authentication (can only be used 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 <i>group-name</i> | 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 **krb5method** 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, enter the following command:

```
aaa authentication ppp default krb5
```

Before you can use Kerberos as the PPP authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the chapter “Configuring Kerberos”.



Note Kerberos login authentication works only with PPP PAP authentication.

PPP Authentication Using Local Password

Use the **aaa authentication ppp** command with the *method* keyword **local** to specify that the Cisco router 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, enter the following command:

```
aaa authentication ppp default local
```

For information about adding users into the local username database, refer to the 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, enter the following command:

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

Before you can use RADIUS as the PPP authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

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, enter the following command:

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

Before you can use TACACS+ as the PPP authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

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 use as the login authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group ppprad**:

```
aaa group server radius ppprad
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 *ppprad*.

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

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

Before you can use a group name as the PPP authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS”. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Configuring AAA Scalability for PPP Requests

You can configure and monitor the number of background processes allocated by the PPP manager in the network access server (NAS) to deal with AAA authentication and authorization requests. 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 | Purpose |
|---|--|
| Router(config)# aaa processes <i>number</i> | Allocates a specific number of background processes to handle AAA authentication and authorization requests for PPP. |

The argument *number* 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. |

| Keyword | Description |
|--------------------------------|--|
| 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 <i>group-name</i> | 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. 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 authorized guest logins--meaning logins by users who have already successfully logged in to the EXEC--as the default method of authentication, using RADIUS only if that method fails, enter 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, enter the following command:

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

ARAP Authentication Using Line Password

Use the **aaa authentication arap** command with the *method* 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, enter the following command:

```
aaa authentication arap default line
```

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

ARAP Authentication Using Local Password

Use the **aaa authentication arap** command with the *method* keyword **local** to specify that the Cisco router 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, enter the following command:

```
aaa authentication arap default local
```

For information about adding users to the local username database, refer to the 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, enter the following command:

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

Before you can use RADIUS as the ARAP authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

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, enter the following command:

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

Before you can use TACACS+ as the ARAP authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

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 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 *araprad*.

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

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

Before you can use a group name as the ARAP authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.” For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

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 <i>group-name</i> | 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 Line Password

Use the **aaa authentication nasicommand** with the *method* 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, enter the following command:

```
aaa authentication nasi default line
```

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

NASI Authentication Using Local Password

Use the **aaa authentication nasicommand** with the *method* keyword **local** to specify that the Cisco router 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, enter the following command:

```
aaa authentication nasi default local
```

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

NASI Authentication Using Group RADIUS

Use the **aaa authentication nasicommand** 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, enter the following command:

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

Before you can use RADIUS as the NASI authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

NASI Authentication Using Group TACACS

Use the **aaa authentication nasicommand** with the **group tacacs+** *method* 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, enter the following command:

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

Before you can use TACACS+ as the authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

NASI Authentication Using group group-name

Use the **aaa authentication nasicommand** with the **group group-name** *method* to specify a subset of RADIUS or TACACS+ servers to use 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 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 *nasirad*.

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

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

Before you can use a group name as the NASI authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS”. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

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 | Purpose |
|---|--|
| Router(config-line)# timeout login response <i>seconds</i> | 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 | Purpose |
|---|--|
| Router(config)# aaa authentication enable default <i>method1</i> [<i>method2...</i>] | <p>Enables user ID and password checking for users requesting privileged EXEC level.</p> <p>Note All aaa authentication enable default requests sent by the router to a RADIUS server include the username “\$enab15\$.” Requests sent to a TACACS+ server will include the username that is entered for login authentication.</p> |

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. |
| 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 <i>group-name</i> | 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 IOS XE 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 be able to see the password prompt defined in the command shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the NAS with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt defined in the **aaa authentication password-prompt** command may be used.

Use the following command in global configuration mode:

| Command | Purpose |
|--|---|
| Router(config)# aaa authentication password-prompt <i>text-string</i> | 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 beginning in Cisco IOS XE Release 2.4.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication suppress null-username`

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Router(config)# configure terminal</pre> | Enables AAA globally. |
| Step 4 | aaa authentication suppress null-username Example: <pre>Router(config)# aaa authentication suppress null-username</pre> | Prevents an Access Request with a blank username from being sent to the RADIUS server. |

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 <i>delimiter string delimiter</i> | 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 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. Router(config)# **aaa accounting network default**
2. Router(config)# **aaa accounting delay-start**
3. Router(config)# **aaa pod server server-keystring**
4. Router(config)# **radius-server host IP address non-standard**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---------------------------------|
| Step 1 | Router(config)# aaa accounting network default Example: | Enables AAA accounting records. |

| | Command or Action | Purpose |
|---------------|---|--|
| | <code>start-stop radius</code> | |
| Step 2 | Router(config)# aaa accounting delay-start | (Optional) Delays generation of the start accounting record until the Framed-IP-Address is assigned, allowing its use in the POD packet. |
| Step 3 | Router(config)# aaa pod server server-keystring | Enables POD reception. |
| Step 4 | Router(config)# radius-server host IP address non-standard | Declares a RADIUS host that uses a vendor-proprietary version of RADIUS. |

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 We suggest that the network administrator restrict authorization at this first stage to allow only Telnet connections to the local host.

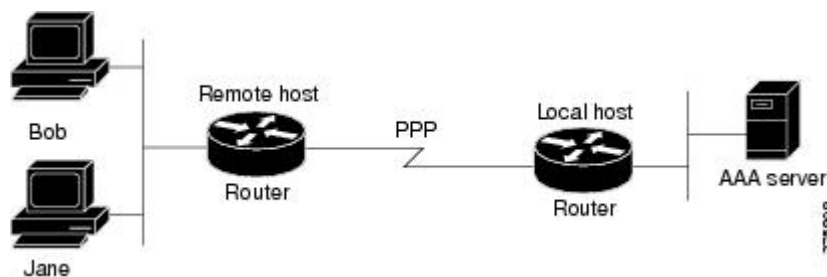
In the second stage, the remote user must Telnet to the network access server to be authenticated. When the remote user logs in, the user must be authenticated with AAA login authentication. The user then must enter the **access-profile** command to be reauthorized using AAA. When this authorization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

The system administrator determines what network privileges 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 issuing 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 **autocommand access-profile** 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 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, 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+). For more information about RADIUS, refer to the chapter "Configuring RADIUS". For more information about TACACS+, refer to the chapter "Configuring 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 authorized rights associated with their personal user profile.

**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 the 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.
- 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 they can *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 will be 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 *Cisco IOS Debug 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. (We suggest 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 | Purpose |
|---|--|
| Router> 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 router 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.



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.
2. Use the **aaa authentication** command to configure your network access server to use login and PPP authentication method lists, 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+). For more information about RADIUS, refer to the chapter “Configuring RADIUS”. For more information about TACACS+, refer to the chapter “Configuring 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 *Cisco IOS Dial Technologies Command Reference*, Release 12.2.



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 the 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.
- 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 will be 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 *Cisco IOS 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. Router(config)# **ip trigger-authentication**
2. Do one of the following:
 - Router(config)# **interface bri number**
 -
 -
 - Router(config)# **interface serial number :23**
3. Router(config-if)# **ip trigger-authentication**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | Router(config)# ip trigger-authentication Example: [timeout seconds] [port number] | Enables automation of double authentication. |
| Step 2 | Do one of the following: <ul style="list-style-type: none"> • Router(config)# interface bri number • • • Router(config)# interface serial number :23 | Selects an ISDN BRI or ISDN PRI interface and enter the interface configuration mode. |
| Step 3 | Router(config-if)# ip trigger-authentication | Applies automated double authentication to the interface. |

Troubleshooting Automated Double Authentication

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

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | Router# show ip trigger-authentication | Displays the list of remote hosts for which automated double authentication has been attempted (successfully or unsuccessfully). |
| Step 2 | Router# 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 | Router# debug ip trigger-authentication | Displays debug output related to automated double authentication. |

Configuring the Dynamic Authorization Service for RADIUS CoA

Use the following procedure to enable the router as an authentication, authorization, and accounting (AAA) server for dynamic authorization service to support the 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*}

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. |

| | Command or Action | Purpose |
|--------|---|---|
| Step 4 | aaa server radius dynamic-author Example: <pre>Router(config)# aaa server radius dynamic-author</pre> | 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 enter 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: <pre>Router(config-locsvr-da-radius)#client 192.168.0.5 server-key cisco1</pre> | Configures the IP address or hostname of the AAA server client. Use the optional server-key keyword and <i>string</i> 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: <pre>Router(config-locsvr-da-radius)# domain stripping right-to-left</pre> Example: <pre>Router(config-locsvr-da-radius)# domain delimiter @</pre> | (Optional) Configures username domain options for the RADIUS application. <ul style="list-style-type: none"> • The delimiter keyword specifies the domain delimiter. One of the following options can be specified for the <i>character</i> 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: <pre>Router(config-locsvr-da-radius)# port 3799</pre> | Configures UDP port 3799 for CoA requests. |

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enables 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa group server radius <i>server-name</i> Example: Device(config)# aaa group server radius rad1 | Adds the RADIUS server and enters server group RADIUS configuration mode. <ul style="list-style-type: none">• The <i>server-name</i> argument specifies the RADIUS server group name. |
| Step 4 | domain-stripping [strip-suffix <i>word</i>] [right-to-left] [prefix-delimiter <i>word</i>] [delimiter <i>word</i>] 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

You can 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`

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Router> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre> | <p>Enters global configuration mode.</p> |
| Step 3 | <p>line [aux console tty vty] line-number [ending-line-number]</p> <p>Example:</p> <pre>Router(config)# line console 0</pre> | <p>Enters line configuration mode.</p> |
| Step 4 | <p>password password</p> <p>Example:</p> <pre>Router(config-line)# secret word</pre> | <p>Assigns a password to a terminal or other device on a line. The password checker is case sensitive and can include spaces; for example, the password “Secret” is different from the password “secret,” and “two words” is an acceptable password.</p> |
| Step 5 | <p>login</p> <p>Example:</p> <pre>Router(config-line)# login</pre> | <p>Enables password checking at login.</p> <p>You can disable line password verification by disabling password checking by using the no version of this command.</p> <p>Note The login command only changes username and privilege level but it does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way.</p> |

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | Do one of the following: <ul style="list-style-type: none"> • Router(config)# username <i>name</i> [nopassword password <i>password</i> password <i>encryption-type encrypted password</i>] • • Router(config)# username <i>name</i> [access-class <i>number</i>] | Establishes username authentication with encrypted passwords. or (Optional) Establishes username authentication by access list. |
| Step 2 | Router(config)# username <i>name</i> [privilege <i>level</i>] | (Optional) Sets the privilege level for the user. |
| Step 3 | Router(config)# username <i>name</i> [autocommand <i>command</i>] | (Optional) Specifies a command to be executed automatically. |
| Step 4 | Router(config)# username <i>name</i> [noescape] [nohangup] | (Optional) Sets a “no escape” login environment. |

What to do next

The keyword **noescape** 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 *Cisco IOS Security Command Reference*.

Enabling CHAP or PAP Authentication

One of the most common transport protocols used in Internet service providers' (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 via 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 the *Cisco IOS XE Dial Technologies Configuration Guide*, Release 2 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 router.

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 router 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 IOS XE 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 | Purpose |
|---|------------------------------|
| Router (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 | Purpose |
|--|--|
| Router (config-if) # ppp authentication { <i>protocol1</i> [<i>protocol2...</i>] [if-needed] { default <i>list-name</i> } [callin] [one-time] | Defines the authentication protocols supported and the order in which they are used. In this command, <i>protocol1</i> , <i>protocol2</i> represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, which is <i>protocol1</i> . If <i>protocol1</i> 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 via 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 via 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 router or access server requires authentication, see the [Establishing Username Authentication, on page 40](#).

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 | Purpose |
|--|--------------------------------------|
| Router(config-if)# ppp pap sent-username <i>username</i> password <i>password</i> | 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 | Purpose |
|--|--|
| Router(config-if)# ppp pap refuse | Refuses PAP authentication from peers requesting PAP authentication. |

If the refuse keyword is not used, the router 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 router to create a common CHAP secret password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor, or running an older version of the Cisco IOS software) to which a new (that is, unknown) router 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 router calling a collection of routers to configure a common CHAP secret password, use the following command in interface configuration mode:

| Command | Purpose |
|---|--|
| Router(config-if)# ppp chap password <i>secret</i> | Enables a router calling a collection of routers 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 | Purpose |
|---|--|
| Router(config-if)# ppp chap refuse [callin] | Refuses CHAP authentication from peers requesting CHAP authentication. |

If the **callin** keyword is used, the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router 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 router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router, use the following command in interface configuration mode:

| Command | Purpose |
|---|---|
| Router(config-if)# ppp chap wait <i>secret</i> | Configures the router to delay CHAP authentication until after the peer has authenticated itself to the router. |

This command (which is the default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no ppp chap wait** command specifies that the router 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. Router(config-if)# **encapsulation ppp**
2. Router(config-if)# **ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | Router(config-if)# encapsulation ppp | Enables PPP encapsulation. |
| Step 2 | Router(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 router 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 router 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 IOS XE 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 router to prompt for and verify a username and password, authorize the user's EXEC level, and specify it as the method of authorization for privilege level 2. In this example, if a local username is entered at the username prompt, that username is used for authentication.

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

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 172.16.71.146 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 router'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 router 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 allows 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 dialin** command applies the “dialin” 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 the Complete Configuration with TACACS Example.)

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 fastethernet 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 the Complete Configuration with TACACS Example.)

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"
```

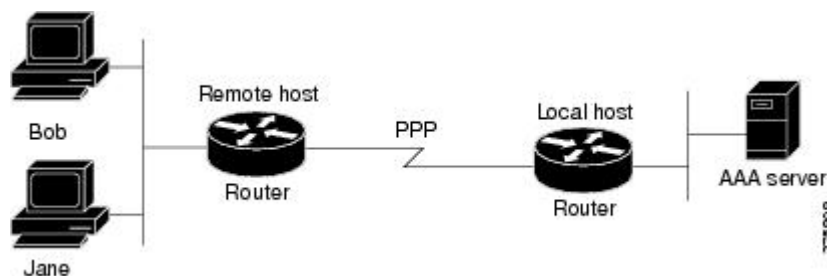
Complete Configuration with TACACS Example

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 fastethernet 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 acs" -----
#
# 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 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 RADIUS AAA server:
!
aaa authentication login default none
aaa authentication ppp default group radius
! **The following command causes the remote user's authorization profile to be
! downloaded from the AAA server to the router when required:
!
aaa authorization network default group radius
!
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
!
!
interface FastEthernet0/0/0
 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 loopback0
 no ip route-cache
 no ip mroute-cache
!
! **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 172.16.57.35 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

```

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 allows 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

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

Related Documents

| Related Topic | Document Title |
|-------------------|--|
| Authorization | Configuring Authorization in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2. |
| Accounting | Configuring Accounting in the <i>Cisco IOS XE Security Configuration Guide: Securing User Service</i> , Release 2. |
| Security commands | <i>Cisco IOS Security Command Reference</i> |

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 | <i>Generic AAA Architecture</i> |
| RFC 2904 | <i>AAA Authorization Framework</i> |
| RFC 2906 | <i>AAA Authorization Requirements</i> |
| RFC 2989 | <i>Criteria for Evaluating AAA Protocols for Network Access</i> |

Technical Assistance

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

Feature Information for 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 Method Lists Enhancement | Cisco IOS XE Release 2.1 | <p>This feature allows you to enable fallback methods for authentication, authorization or accounting. The fallback methods could include trying groups of RADIUS or TACACS+ servers or a local database in some cases.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following command was introduced or modified: aaa authentication ppp.</p> |
| AAA Per-User Scalability | Cisco IOS XE Release 2.3 | <p>The AAA Per-User Scalability feature supports two RADIUS VSAs for ip vrf and ip unnumbered commands and creates subvirtual access interfaces if specified instead of full VA interface to achieve higher scalability.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |
| Challenge Handshake Authentication Protocol (CHAP) | Cisco IOS XE Release 2.1 | <p>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 via 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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: ppp authentication, ppp chap password, ppp chap refuse.</p> |
| Domain Stripping at the Server Group Level | Cisco IOS XE Release 3.4S | <p>The Domain Stripping feature allows domain stripping to be configured at the server group level. Per-server group configuration overrides the global configuration.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Domain Stripping • Configuring Domain Stripping at the Server Group Level <p>The following command was introduced: domain-stripping.</p> |
| Double Authentication | Cisco IOS XE Release 2.1 | <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa authentication, aaa authorization, access-profile.</p> |

| Feature Name | Releases | Feature Information |
|---|--------------------------|---|
| Message Banners for AAA Authentication | Cisco IOS XE Release 2.1 | In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following command was introduced: aaa authentication banner . |
| MS-CHAP Version 1 | Cisco IOS XE Release 2.1 | 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 router or access server acting as a network access server. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: ppp authentication . |
| Password Authentication Protocol (PAP) | Cisco IOS XE Release 2.1 | 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 via 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. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: ppp authentication, ppp pap sent-username, ppp pap refuse . |
| RADIUS—CLI to Prevent Sending of Access Request with a Blank Username | Cisco IOS XE Release 2.4 | This authentication feature prevents 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. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following command was introduced: aaa authentication suppress null-username . |



CHAPTER 3

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, on page 63](#)
- [Information About RADIUS Change of Authorization, on page 63](#)
- [How to Configure RADIUS Change of Authorization, on page 68](#)
- [Configuration Examples for RADIUS Change of Authorization, on page 72](#)
- [Additional References for RADIUS Change of Authorization, on page 73](#)
- [Feature Information for RADIUS Change of Authorization, on page 74](#)

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 |

| Value | Explanation |
|-------|--|
| 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 802.1x, 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, reenabling 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, reenabling 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. |
| 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 { <i>ip-address</i> <i>name</i> [<i>vrf vrf-name</i>]} server-key [0 7] <i>string</i> Example: Device(config-locsvr-da-radius)# client 10.0.0.1 | Configures the RADIUS key to be shared between a device and RADIUS clients. |

| | Command or Action | Purpose |
|---------|---|--|
| Step 6 | port <i>port-number</i> 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enables 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enables 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. <ul style="list-style-type: none"> • In this mode, the RADIUS application commands are configured. |
| Step 5 | client { <i>ip-addr</i> <i>hostname</i> } [server-key [0 7] <i>string</i>] 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. <ul style="list-style-type: none"> • Use the optional server-key keyword and <i>string</i> argument to configure the server key at the client level. <p>Note Configuring the server key at the client level overrides the server key configured at the global level.</p> |
| Step 6 | domain { <i>delimiter character</i> stripping [right-to-left]} Example: Device(config-locsvr-da-radius)# domain stripping right-to-left | (Optional) Configures username domain options for the RADIUS application. <ul style="list-style-type: none"> • The delimiter keyword specifies the domain delimiter. One of the following options can be specified for the <i>character</i> 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. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 7 | port <i>port-num</i> 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 | <ul style="list-style-type: none"> • 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 |

| Related Topic | Document Title |
|-----------------|--|
| Configuring AAA | <i>Authentication, Authorization, and Accounting Configuration Guide</i> |

Standards and RFCs

| Standard/RFC | Title |
|--------------|---|
| RFC 2903 | <i>Generic AAA Architecture</i> |
| RFC 5176 | <i>Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)</i> |

Technical Assistance

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

Feature Information for 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 | | <p>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.</p> <p>The following commands were introduced or modified: aaa server radius dynamic-author, authentication command bounce-port ignore, and authentication command disable-port ignore.</p> |



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, on page 77](#)
- [Information About Message Banners for AAA Authentication, on page 77](#)
- [How to Configure Message Banners for AAA Authentication, on page 78](#)
- [Configuration Examples for Message Banners for AAA Authentication, on page 80](#)
- [Additional References for Message Banners for AAA Authentication, on page 81](#)
- [Feature Information for Message Banners for AAA Authentication, on page 81](#)

Finding Feature Information

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

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

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. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enables AAA globally. |
| Step 4 | aaa authentication banner <i>delimiter-string delimiter</i> Example: Device(config)# aaa authentication banner *Unauthorized Access Prohibited* | Creates a personalized login banner. |
| 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enters AAA globally. |
| Step 4 | aaa authentication banner <i>delimiter-string delimiter</i> Example: Device(config)# aaa authentication banner *Unauthorized Access Prohibited* | Creates a personalized login banner. |
| Step 5 | aaa authentication fail-message <i>delimiter-string delimiter</i> Example: Device(config)# aaa authentication fail-message *Failed login. Try again* | Creates a message to be displayed when a user login fails. |

| | Command or Action | Purpose |
|--------|--|----------------------------------|
| 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 | <ul style="list-style-type: none"> • 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 | <i>Authentication, Authorization, and Accounting Configuration Guide</i> |

Technical Assistance

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

Feature Information for 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 16: Feature Information for Message Banners for AAA Authentication

| Feature Name | Releases | Feature Information |
|--|----------|--|
| Message Banners for AAA Authentication | | <p>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.</p> <p>The following commands were introduced or modified: aaa authentication banner, aaa authentication fail-message, and aaa new-model.</p> |



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, on page 83](#)
- [Information About AAA-Domain Stripping at Server Group Level, on page 83](#)
- [How to Configure AAA-Domain Stripping at Server Level Group, on page 84](#)
- [Configuration Example for AAA-Domain Stripping at Server Group Level, on page 85](#)
- [Additional References, on page 85](#)
- [Feature Information for AAA-Domain Stripping at Server Group Level, on page 87](#)

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. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enables AAA. |
| Step 4 | aaa group server radius <i>server-name</i> Example: Device(config)# aaa group server radius rad1 | Adds the RADIUS server and enters server group RADIUS configuration mode. <ul style="list-style-type: none">• The <i>server-name</i> argument specifies the RADIUS server group name. |

| | Command or Action | Purpose |
|--------|--|---|
| Step 5 | domain-stripping [strip-suffix <i>word</i>] [right-to-left] [prefix-delimiter <i>word</i>] [delimiter <i>word</i>] 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 <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2. |
| Accounting | Configuring Accounting in the <i>Cisco IOS XE Security Configuration Guide: Securing User Service</i> , Release 2. |
| Security commands | <i>Cisco IOS Security Command Reference</i> |

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 | <i>Generic AAA Architecture</i> |
| RFC 2904 | <i>AAA Authorization Framework</i> |
| RFC 2906 | <i>AAA Authorization Requirements</i> |
| RFC 2989 | <i>Criteria for Evaluating AAA Protocols for Network Access</i> |

Technical Assistance

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

Feature Information for 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 17: Feature Information for AAA-Domain Stripping at Server Group Level

| Feature Name | Releases | Feature Information |
|--|---------------------------|---|
| AAA-Domain Stripping at Server Group Level | Cisco IOS XE Release 3.4S | 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 connections to the network that are authorized by service providers and increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

- [Finding Feature Information, on page 89](#)
- [Prerequisites for AAA Double Authentication Secured by Absolute Timeout, on page 89](#)
- [Restrictions for AAA Double Authentication Secured by Absolute Timeout, on page 90](#)
- [Information About AAA Double Authentication Secured by Absolute Timeout, on page 90](#)
- [How to Apply AAA Double Authentication Secured by Absolute Timeout, on page 90](#)
- [Configuration Examples for AAA Double Authentication Secured by Absolute Timeout, on page 91](#)
- [Additional References, on page 94](#)
- [Feature Information for AAA Double Authentication Secured by Absolute Timeout, on page 95](#)

Finding Feature Information

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

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

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.

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

Related Documents

| Related Topic | Document Title |
|--------------------|--|
| Cisco IOS commands | Master Command List, All Releases |
| Security commands | <ul style="list-style-type: none"> • 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 |

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 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 18: Feature Information for AAA Double Authentication Secured by Absolute Timeout

| Feature Name | Releases | Feature Information |
|---|----------|---|
| 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. |



CHAPTER 7

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, on page 97](#)
- [Information About Throttling of AAA RADIUS Records, on page 97](#)
- [How to Configure Throttling of AAA RADIUS Records, on page 98](#)
- [Configuration Examples for Throttling of AAA RADIUS Records, on page 101](#)
- [Additional References, on page 102](#)
- [Feature Information for Throttling of AAA RADIUS Records, on page 103](#)

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.

Summary

- 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: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | radius-server throttle { accounting <i>threshold</i> } [access <i>threshold</i> [access-timeout <i>number-of-timeouts</i>]] Example: <pre>Router(config)# radius-server throttle accounting 100 access 200 access-timeout 2</pre> | Configures global throttling for accounting and access request packets. For this example: <ul style="list-style-type: none"> • The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. <p>Note The default threshold value is 0 (throttling disabled).</p> <ul style="list-style-type: none"> • The number of timeouts per transaction value (the range is 1-10) is set to 2. |
| Step 4 | exit Example: <pre>Router(config)# exit</pre> | 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa group server radius <i>server-group-name</i> 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. <p>For this example:</p> <ul style="list-style-type: none"> • The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. <p>Note The default threshold value is 0 (throttling disabled).</p> <ul style="list-style-type: none"> • The number of time-outs per transaction value (the range is 1-10) is set to 2. |
| 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 |
|-------------------|---|
| Security features | <i>Cisco IOS XE Security Configuration Guide: Securing User Services, Release 2</i> |
| Security commands | <i>Cisco IOS Security Command Reference</i> |

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

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 19: Feature Information for Throttling of AAA (RADIUS) Records

| Feature Name | Releases | Feature Information |
|------------------------------------|--------------------------|---|
| Throttling of AAA (RADIUS) Records | Cisco IOS XE Release 2.1 | <p>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 XE router to the RADIUS server.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified by this feature: radius-server throttle, throttle</p> |



CHAPTER 8

RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect feature is used to terminate a connected voice call.

- [Finding Feature Information, on page 105](#)
- [Prerequisites for RADIUS Packet of Disconnect, on page 105](#)
- [Restrictions for RADIUS Packet of Disconnect, on page 105](#)
- [Information About RADIUS Packet of Disconnect, on page 106](#)
- [How to Configure the RADIUS Packet of Disconnect, on page 107](#)
- [Additional References, on page 109](#)
- [Feature Information for RADIUS Packet of Disconnect, on page 110](#)
- [Glossary, on page 111](#)

Finding Feature Information

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

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

Prerequisites for RADIUS Packet of Disconnect

Configure AAA as described in the *Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2.

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 IOS XE software allocates POD code 50 as the code value for the Voice POD Request based on RFC 3576 *Dynamic Authorization Extensions to RADIUS*, which extends RADIUS standards to officially support both a Disconnect Message (DM) and Change-of-Authorization (CoA) that are 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# **end**
5. Router# **show running-configuration**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | Router (config)# aaa pod server [<i>port port-number</i>] [<i>auth-type {any all session-key}</i>] <i>server-key</i> [<i>encryption-type</i>] <i>string</i> Example: Router (config)# aaa pod server server-key xyz123 | Enables inbound user sessions to be disconnected when specific session attributes are presented, where: <ul style="list-style-type: none"> • port port-number --(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700. • auth-type --(Optional) The type of authorization required for disconnecting sessions. <ul style="list-style-type: none"> • 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. |

| | Command or Action | Purpose |
|---------------|--|---|
| | | <ul style="list-style-type: none"> • 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# end | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 5 | Router# show running-configuration Example: <pre>Router# show running-configuration</pre> Example: <pre>!</pre> Example: <pre>aaa authentication login h323 group radius</pre> Example: <pre>aaa authorization exec h323 group radius</pre> Example: <pre>aaa accounting update newinfo</pre> Example: <pre>aaa accounting connection h323 start-stop group radius</pre> Example: <pre>aaa pod server server-key cisco</pre> Example: <pre>aaa session-id common</pre> Example: | Verifies that the gateway is configured correctly in privileged EXEC mode. |

| | Command or Action | Purpose |
|--|-------------------|---------|
| | ! | |

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 the RADIUS POD Configuration

To verify the RADIUS POD configuration, use the **show running configuration** privileged EXEC command as shown in the following example:

```
Router# show running-configuration
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting update newinfo
aaa accounting connection h323 start-stop group radius
aaa pod server server-key cisco
aaa session-id common
.
.
.
```

Additional References

The following sections provide references related to the RADIUS Packet of Disconnect feature.

Related Documents

| Related Topic | Document Title |
|-------------------|--|
| AAA | Authentication, Authorization, and Accounting (AAA) section of the <i>Cisco IOS XE Security Configuration Guide, Securing User Services</i> , Release 2. |
| Security commands | <i>Cisco IOS Security Command Reference</i> |
| CLI Configuration | <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i> , Release 2 |

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 2865 | <i>Remote Authentication Dial-in User Service</i> |
| RFC 3576 | <i>Dynamic Authorization Extensions to RADIUS</i> |

Technical Assistance

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

Feature Information for 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 20: Feature Information for RADIUS Packet of Disconnect

| Feature Name | Releases | Feature Information |
|-----------------------------|--------------------------|---|
| RADIUS Packet of Disconnect | Cisco IOS XE Release 2.1 | <p>The RADIUS Packet of Disconnect feature is used to terminate a connected voice call.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the on Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa pod server, debug aaa pod</p> |

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 disjointed routing/forwarding tables, where the routes of a user have no correlation with the routes of another user.



CHAPTER 9

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, on page 113](#)
- [Prerequisites for Implementing Authorization and Authentication Profile Caching, on page 113](#)
- [Information About Implementing Authorization and Authentication Profile Caching, on page 114](#)
- [How to Implement Authorization and Authentication Profile Caching, on page 116](#)
- [Configuration Examples for Implementing Authorization and Authentication Profile Caching, on page 121](#)
- [Additional References for RADIUS Change of Authorization, on page 124](#)
- [Feature Information for Implementing Authorization and Authentication Profile Caching, on page 125](#)

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 Implementing Authorization and Authentication 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, are used. 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. **regex** *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. |
| 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 <i>group-name</i> Example: | Defines an authentication and authorization cache profile server group and enters profile map configuration mode. |

| | Command or Action | Purpose |
|----------------|---|---|
| | Router(config)# aaa cache profile networkusers@companyname | |
| Step 5 | <p>profile <i>name</i> [no-auth]</p> <p>Example:</p> <pre>Router(config-profile-map)# profile networkuser1 no-auth</pre> | <p>Creates an individual authentication and authorization cache profile based on a username match.</p> <ul style="list-style-type: none"> • The <i>name</i> 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 | <p>regexp <i>matchexpression</i> {any only}[no-auth]</p> <p>Example:</p> <pre>Router(config-profile-map)# regexp .*@example.com any no-auth</pre> | <p>(Optional) Creates an entry in a cache profile group that matches based on a regular expression.</p> <ul style="list-style-type: none"> • 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. | -- |
| Step 9 | <p>all [no-auth]</p> <p>Example:</p> <pre>Router(config-profile-map)# all no-auth</pre> | <p>(Optional) Specifies that all authentication and authorization requests are cached.</p> <ul style="list-style-type: none"> • Use the all command for specific service authorization requests, but it should be avoided when dealing with authentication requests. |
| Step 10 | <p>end</p> <p>Example:</p> <pre>Router(config-profile-map)# end</pre> | Returns to privileged EXEC mode. |
| Step 11 | <p>show aaa cache group <i>name</i></p> <p>Example:</p> | (Optional) Displays all cache entries for a specified group. |

| | Command or Action | Purpose |
|----------------|--|--|
| | Router# show aaa cache group networkusers@companyname | |
| Step 12 | clear aaa cache group <i>name</i> { 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Router# configure terminal | |
| Step 3 | aaa new-model Example: Router(config)# aaa new-model | Enables the AAA access control model. |
| Step 4 | aaa group server radius <i>group-name</i> or aaa group server tacacs+ <i>group-name</i> Example: Router(config)# aaa group server radius networkusers@companyname | Enters RADIUS server group configuration mode. <ul style="list-style-type: none"> To enter TACACS+ server group configuration mode, use the aaa group server tacacs+ <i>group-name</i> command. |
| Step 5 | cache authorization profile <i>name</i> 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. <ul style="list-style-type: none"> The <i>name</i> argument in this command is a AAA cache profile group name. |
| Step 6 | cache authentication profile <i>name</i> Example: Router(config-sq-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 <i>hours</i> {enforce failover} Example: Router(config-sq-radius)# cache expiry 240 failover | (Optional) Sets the amount of time before a cache profile entry expires (becomes stale). <ul style="list-style-type: none"> 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** {network | exec | commands *level* | reverse-access| configuration} {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: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Router(config)# aaa new-model</pre> | Enables the AAA access control model. |
| Step 4 | aaa authorization {network exec commands <i>level</i> reverse-access configuration} {default <i>list-name</i> } [<i>method1</i> [<i>method2</i> ...]] Example: <pre>Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname</pre> | 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 <i>list-name</i> } <i>method1</i> [<i>method2</i> ...] Example: <pre>Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname</pre> | Specifies one or more authentication methods for use on serial interfaces that are running PPP. |

| | Command or Action | Purpose |
|--------|---|-----------------------------------|
| Step 6 | aaa authentication login {default list-name} method1 [method2...] Example: <pre>Router(config)# aaa authentication login default cache adminusers group adminusers</pre> | Sets the authentication at login. |
| Step 7 | end Example: <pre>Router(config)# end</pre> | 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 for RADIUS Change of Authorization

Related Documents

| Related Topic | Document Title |
|--------------------|--|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | <ul style="list-style-type: none"> • 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 | <i>Authentication, Authorization, and Accounting Configuration Guide</i> |

Standards and RFCs

| Standard/RFC | Title |
|--------------|---|
| RFC 2903 | <i>Generic AAA Architecture</i> |
| RFC 5176 | <i>Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)</i> |

Technical Assistance

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

Feature Information for 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 21: Feature Information for Implementing Authorization and Authentication Profile Caching

| Feature Name | Release | Feature Information |
|--|--------------------------|--|
| AAA Authorization and Authentication Cache | Cisco IOS XE Release 2.3 | <p>This feature optimizes network performance and provides a failover mechanism in the event a network RADIUS or TACACS+ server becomes unavailable for any reason.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>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.</p> |



CHAPTER 10

Configuring Authorization

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

- [Finding Feature Information, on page 127](#)
- [AAA Authorization Prerequisites, on page 127](#)
- [Information About Configuring Authorization, on page 128](#)
- [How to Configure Authorization, on page 131](#)
- [Authorization Configuration Examples, on page 134](#)
- [Additional References, on page 137](#)
- [Feature Information for Configuring Authorization, on page 138](#)

Finding Feature Information

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

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

AAA Authorization Prerequisites

Before configuring authorization using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server.
- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly. For more information about AAA authentication, refer to the “Configuring Authentication” module.
- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS security server, refer to the chapter “Configuring RADIUS”. For more

information about configuring your Cisco network access server to communicate with your TACACS+ security server, refer to the “Configuring TACACS+” module.

- Define the rights associated with specific users by using the **username** command if you are issuing local authorization. For more information about the **username** command, refer to the *Cisco IOS Security Command Reference*.

Information About Configuring Authorization

Named Method Lists for Authorization

Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS XE software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS XE software selects the next method listed in the list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.



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

Method lists are specific to the authorization type requested:

- **Commands**--Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**--Applies to the attributes associated with a user EXEC terminal session.
- **Network**--Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access**--Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be 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 via the local database.
- **RADIUS**—The network access server requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.



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 via a TACACS+ security server, use the **aaa authorization** command with the **group tacacs+ method** keyword. For more specific information about configuring authorization using a TACACS+ security server, refer to the chapter “Configuring TACACS+.” 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.

To allow users to have access to the functions they request as long as they have been authenticated, use the **aaa authorization** command with the **if-authenticated method** keyword. If you select this method, all requested functions are automatically granted to authenticated users.

There may be times when you do not want to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the **none method** keyword. If you select this method, authorization is disabled for all actions.

To select local authorization, which means that the 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, refer to the chapter “Configuring Authentication.”

To have the network access server request authorization via a RADIUS security server, use the **radius method** keyword. For more specific information about configuring authorization using a RADIUS security server, refer to the Configuring RADIUS chapter.

To have the network access server request authorization via 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, refer to the chapter Configuring RADIUS. For an example of how to enable a RADIUS server to authorize services, see the RADIUS Authorization Example.



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 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, 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 separate server groups, and T1 and T2 as separate server groups. This means you can specify either R1 and T1 in the method list or R2 and T2 in the method list, which provides more flexibility in the way that you assign RADIUS and TACACS+ resources.

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 will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers, refer to the chapter Configuring RADIUS or the chapter Configuring TACACS+.

AAA Authorization Types

Cisco IOS XE software supports five different types of authorization:

- **Commands**--Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**--Applies to the attributes associated with a user EXEC terminal session.
- **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. For detailed information on the authentication proxy feature, refer to the chapter “Configuring Authentication Proxy” in the “Traffic Filtering and Firewalls” part of this book.

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 you to authorize all commands associated with a specified command level from 0 to 15.)

To create a method list to enable authorization for reverse Telnet functions, use the **reverse-access** keyword.

For information about the types of authorization supported by the Cisco IOS XE software, refer to the AAA Authorization Types.

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.

For a list of supported RADIUS attributes, refer to the “RADIUS Attributes Overview and RADIUS IETF Attributes” chapter. For a list of supported TACACS+ AV pairs, refer to the “Configuring TACACS+” chapter.

How to Configure Authorization

For authorization configuration examples using the commands in this chapter, refer to the Authorization Configuration Examples.

Configuring AAA Authorization Using Named Method Lists

To configure AAA authorization using named method lists, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2*...]]
2. Do one of the following:
 - Router(config)# **line** [**aux** | **console** | **tty** | **vtty**] *line-number* [*ending-line-number*]
 -
 -

- Router(config)# **interface** *interface-type interface-number*

3. Do one of the following:

- Router(config-line)# **authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}
-
- Router(config-line)# **ppp authorization** {**default** | *list-name*}

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | Router(config)# aaa authorization { auth-proxy network exec commands <i>level</i> reverse-access configuration ipmobile } { default <i>list-name</i> } [<i>method1</i> [<i>method2...</i>]] | Creates an authorization method list for a particular authorization type and enable authorization. |
| Step 2 | Do one of the following: <ul style="list-style-type: none"> • Router(config)# line [aux console tty vtty] <i>line-number</i> [<i>ending-line-number</i>] • • Router(config)# interface <i>interface-type interface-number</i> | Enters the line configuration mode for the lines to which you want to apply the authorization method list. Alternately, enters the interface configuration mode for the interfaces to which you want to apply the authorization method list. |
| Step 3 | Do one of the following: <ul style="list-style-type: none"> • Router(config-line)# authorization {arap commands <i>level</i> exec reverse-access} {default <i>list-name</i>} • • Router(config-line)# ppp authorization {default <i>list-name</i>} | Applies the authorization list to a line or set of lines. Alternately, 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, you log in to a network access server (typically through a dialup connection) and then use Telnet 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 <i>method1</i> [<i>method2</i> ...] | 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+. You must configure the specific reverse Telnet privileges for the user on the security server itself.

Authorization Configuration Examples

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 via RADIUS. This can be used to govern address assignment, the application of access lists, and various other per-user quantities.



Note Because no fallback method is specified in this example, authorization will fail if, for any reason, there is no response from the RADIUS server.

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.

For more information about configuring TACACS+, refer to the “Configuring TACACS” chapter. For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide*, version 2.1(2) or greater.

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.

For more information about configuring RADIUS, refer to the chapter “Configuring RADIUS.”

Additional References

Related Documents

| Related Topic | Document Title |
|--------------------|--|
| Cisco IOS commands | Master Command List, All Releases |
| Security commands | <ul style="list-style-type: none"> • 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 |

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 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 22: Feature Information for Configuring Authorization

| Feature Name | Releases | Feature Information |
|---|--------------------------|---|
| Named Method Lists for AAA Authorization and Accounting | Cisco IOS XE Release 2.1 | Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |



CHAPTER 11

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, on page 139](#)
- [Prerequisites for Configuring Accounting, on page 139](#)
- [Restrictions for Configuring Accounting, on page 140](#)
- [Information About Configuring Accounting, on page 140](#)
- [How to Configure AAA Accounting, on page 154](#)
- [Configuration Examples for AAA Accounting, on page 161](#)
- [Additional References, on page 164](#)
- [Feature Information for Configuring Accounting, on page 165](#)

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.
- 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 chapter [Configuring RADIUS](#). For more

information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the chapter *Configuring TACACS+*.

Restrictions for Configuring Accounting

The AAA Accounting feature has the following restrictions:

- Accounting information can be sent simultaneously to a maximum of four AAA servers.
- Service Selection Gateway (SSG) restriction--For 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

Like authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow a 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, by coincidence, is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is 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 if the initial method fails. Cisco IOS XE software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS XE 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 XE 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 six 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.
- Command--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.



Note System accounting does not use named accounting lists; only the default list for system accounting can be defined.

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 a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

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.

In Cisco IOS XE 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) can be specified in the method list or R2 and T2 (SG2 and SG4) 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, 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 DNIS numbers, see *Configuring RADIUS module* or *Configuring TACACS+ module* in the *Cisco IOS XE Security Configuration Guide: Securing User Services* Release 2.

AAA Accounting Methods

Cisco IOS XE supports the following two methods for accounting:

- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.



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 keywords.

Table 23: 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 <i>group-name</i> . |

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

Named accounting method lists are specific to the indicated type of accounting.

- **network** --To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARAP protocols), use the **network** keyword in the **aaa accounting** command. For example, to create a method list that provides accounting information for ARAP (network) sessions, use the **arap** keyword in the **accounting** command.
- **exec** --To create a method list that provides accounting records about user EXEC terminal sessions on the network access server, including username, date, start and stop times, use the **exec** keyword.
- **commands** --To create a method list that provides accounting information about specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword.

- **connection** --To create a method list that provides accounting information about all outbound connections made from the network access server, use the **connection** keyword.
- **resource** --To creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.



Note System accounting does not support named method lists.

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 <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 GigabitEthernet0/0/0
<cr>
Wed Jun 27 03:47:29 2001      172.16.25.15  username1  tty3  56223294304327528 stop
      task_id=8      service=shell  priv-lvl=15  cmd=ip address 10.1.1.1 255.255.255.0
      <cr>

```



Note The Cisco Systems 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 XE software configuration guides. For example, IP accounting tasks are described in the Configuring IP Services chapter in the *Cisco IOS XE Application Services Configuration Guide*, Release 2.

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:

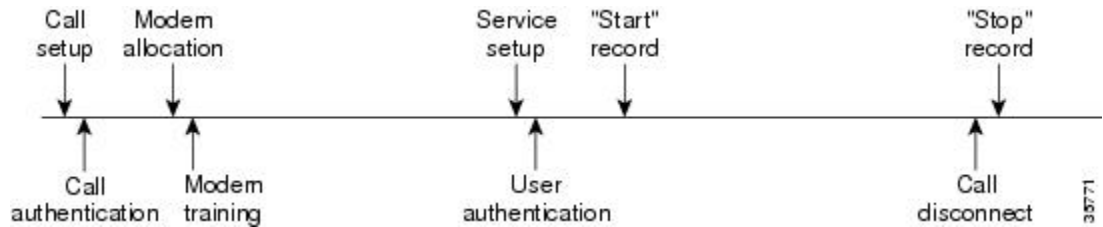
AAA Resource Failure Stop Accounting

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.

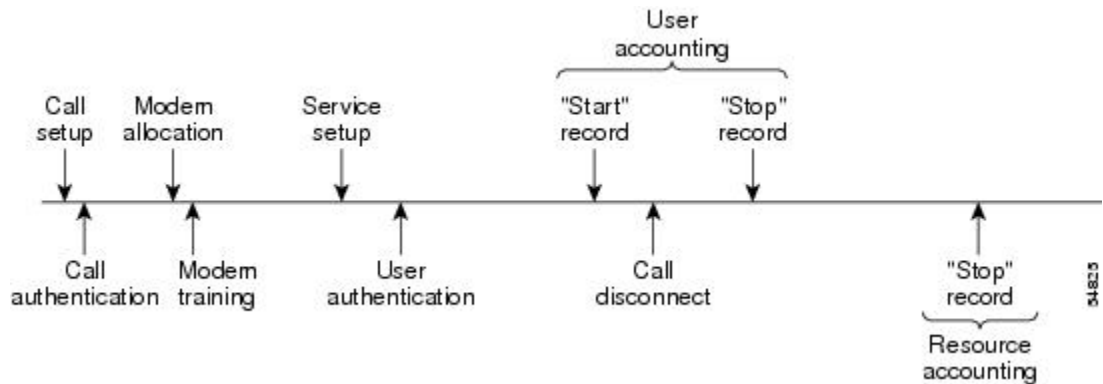
The figure below illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

Figure 4: Modem Dial-In Call Setup Sequence with Normal Flow and Without Resource Failure Stop Accounting Enabled



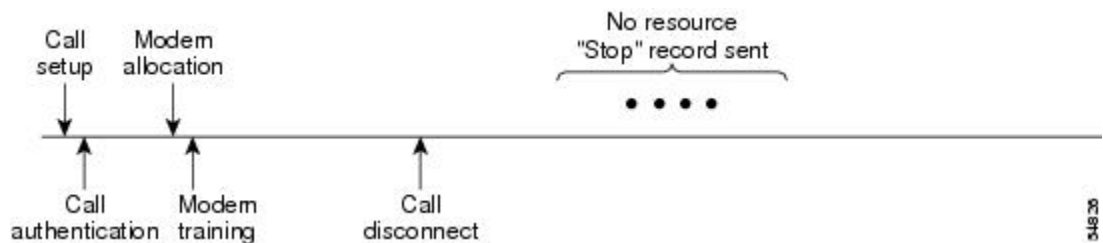
The figure below illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

Figure 5: Modem Dial-In Call Setup Sequence with Normal Flow and with Resource Failure Stop Accounting Enabled



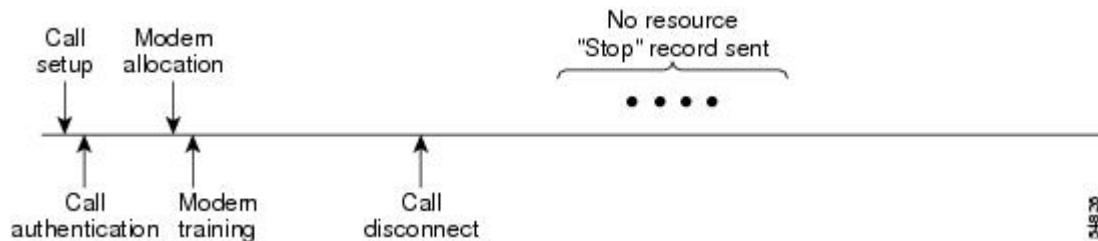
The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

Figure 6: 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 7: Modem Dial-In Call Setup Sequence with Call Disconnect Occurring Before User Authentication and Without Resource Failure Stop Accounting Enabled



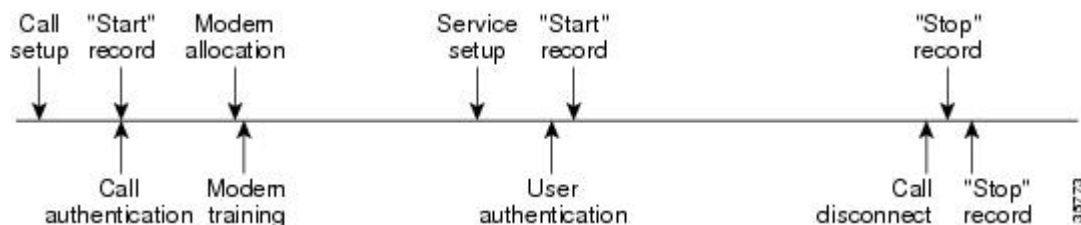
AAA Resource Accounting for Start-Stop Records

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 8: Modem Dial-In Call Setup Sequence with Resource Start-Stop Accounting Enabled



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 to terminate an active call

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

Table 24: SNMP End-User Data Objects

| Field | Descriptions |
|------------|---|
| 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 25: SNMP AAA Session Summary

| Field | Descriptions |
|--------------------------|--|
| ActiveTableEntries | Number of sessions currently active. |
| ActiveTableHighWaterMark | Maximum number of sessions present since last system reinstallation. |
| TotalSessions | Total number of sessions since the last system reinstallation. |
| DisconnectedSessions | Total number of sessions that have been disconnected since the last system reinstallation. |

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ attribute-value (AV) pairs or RADIUS attributes, depending on which security method is implemented.

How to Configure AAA Accounting

Configuring AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. `aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [method1 [method2...]]`
2. `line [aux | console | tty | vty] line-number [ending-line-number]`
3. `accounting {arap | commands level | connection | exec} {default | list-name}`

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | <code>aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [method1 [method2...]]</code> | Creates an accounting method list and enables accounting. The <i>list-name</i> argument is a character string used to name the created list. |
| Step 2 | <code>line [aux console tty vty] line-number [ending-line-number]</code> Example: <pre>Router(config)# interface interface-type interface-number</pre> | Enters line configuration mode for the lines to which the accounting method list is applied or enters interface configuration mode for the interfaces to which the accounting method list is applied. |
| Step 3 | <code>accounting {arap commands level connection exec} {default list-name}</code> Example: <pre>Router(config-if)# ppp accounting {default list-name}</pre> | 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. |

What to do next



Note System accounting does not use named method lists. For system accounting, define only the default method list.

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA accounting is activated, the Cisco IOS XE 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 or Action | Purpose |
|--|---|
| Router(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 or Action | Purpose |
|---|--|
| Router(config)# aaa accounting update [newinfo] [periodic] number | Enables periodic interim accounting records to be sent to the accounting server. |

When the `aaa accounting update` command is activated, the Cisco IOS XE software issues interim accounting records for all users on the system. If the `newinfo` keyword 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 Internet Protocol Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When `aaa accounting update` command is used with the keyword `periodic`, interim accounting records are sent periodically as defined by the argument number. 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.

Configuring an Alternate Method to Enable Periodic Accounting Records

You can use the following alternative method to enable periodic interim accounting records to be sent to the accounting server.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa accounting network default`
4. `action-type {none | start-stop [periodic {disable | interval minutes}] | stop-only}`

5. exit

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa accounting network default Example: <pre>Router(config)# aaa accounting network default</pre> | Configures the default accounting for all network-related service requests and enters accounting method list configuration mode. |
| Step 4 | action-type {none start-stop [periodic {disable interval <i>minutes</i>}]} stop-only} Example: <pre>Router(cfg-acct-mlist)# action-type start-stop</pre> Example: <pre>periodic interval 5</pre> | Specifies the type of action to be performed on accounting records. <ul style="list-style-type: none"> • (Optional) The periodic keyword specifies periodic accounting action. • The interval keyword specifies the periodic accounting interval. • The value argument specifies the intervals for accounting update records (in minutes). • The disable keyword disables periodic accounting. |
| Step 5 | exit Example: <pre>Router(cfg-acct-mlist)# exit</pre> | Returns to global configuration mode. |

Generating Interim Service Accounting Records

Perform this task to enable the generation of interim service accounting records at periodic intervals for subscribers.

Before you begin

RADIUS Attribute 85 in the user service profile always takes precedence over the configured interim-interval value. RADIUS Attribute 85 must be in the user service profile. See the RADIUS Attributes Overview and RADIUS IETF Attributes feature document for more information.



Note If RADIUS Attribute 85 is not in the user service profile, then the interim-interval value configured in Generating Interim Accounting Records is used for service interim accounting records.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber service accounting interim-interval *minutes***

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | subscriber service accounting interim-interval <i>minutes</i> Example: Router(config)# subscriber service accounting interim-interval 10 | Enables the generation of interim service accounting records at periodic intervals for subscribers. The <i>minutes</i> argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes. |

Generating Accounting Records for a Failed Login or Session

When AAA accounting is activated, the Cisco IOS XE 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 or Action | Purpose |
|---|---|
| aaa accounting send stop-record authentication failure | Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP. |

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, it can be specified that NETWORK records be generated before EXEC-stop records. In some 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 network 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 or Action | Purpose |
|------------------------------|-----------------------------------|
| aaa accounting nested | Nests network accounting records. |

Suppressing System Accounting Records over Switchover

To suppress the system accounting-on and accounting-off messages during switchover, use the following command in global configuration mode:

| Command or Action | Purpose |
|--|--|
| aaa accounting redundancy suppress system-records | Suppresses the system accounting messages during switchover. |

Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration:

| Command or Action | Purpose |
|--|--|
| aaa accounting resource <i>method-list</i> stop-failure group <i>server-group</i> | <p>Generates a “stop” record for any calls that do not reach user authentication.</p> <p>Note Before configuring the AAA Resource Failure Stop Accounting feature, the tasks described in the Prerequisites for Configuring Accounting, on page 139 section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco ASR 1000 Series Aggregation Services Router, see the Configuring SNMP Support chapter in the Cisco IOS XE Network Management Configuration Guide.</p> |

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 or Action | Purpose |
|--|--|
| aaa accounting resource <i>method-list</i> start-stop group <i>server-group</i> | 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 section Prerequisites for Configuring Accounting, on page 139 must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco ASR 1000 Series Aggregation Services Router, see the chapter Configuring SNMP Support in the Cisco IOS XE Network Management Configuration Guide, Release 2 . |

Configuring AAA Broadcast Accounting

To configure AAA broadcast accounting, use the **aaa accounting** command in global configuration mode. This command has been modified to allow the **broadcast** keyword.

| Command or Action | Purpose |
|---|--|
| aaa accounting { system network exec connection commands level } { default <i>list-name</i> } { start-stop stop-only none } [broadcast] <i>method1</i> [<i>method2...</i>] | 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. This command has been modified to allow the **broadcast** keyword and multiple server groups.

| Command or Action | Purpose |
|---|--|
| aaa dnis map dnis-number accounting network [start-stop stop-only none] [broadcast] <i>method1</i> [<i>method2...</i>] | 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 the AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP. For information on SNMP, see the [Configuring SNMP Support](#) chapter in the [Cisco IOS XE 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 the AAA session MIB, use the following command in global configuration mode:

| Command or Action | Purpose |
|-----------------------------------|---|
| aaa session-mib disconnect | Monitors and terminates authenticated client connections using SNMP. To terminate the call, use the disconnect keyword . |

Establishing a Session with a Router if the AAA Server Is Unreachable

To establish a console session with a router if the AAA server is unreachable, use the following command in global configuration mode:

| Command or Action | Purpose |
|---|--|
| 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, use the no aaa accounting system guarantee-first command. |

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users logged in, use the following command in privileged EXEC mode:

| Command or Action | Purpose |
|------------------------|--|
| 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 or Action | Purpose |
|-----------------------------|---|
| debug aaa accounting | Displays information on accountable events as they occur. |

Configuration Examples for AAA Accounting

Configuring a Named Method List Example

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database 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 network1 group radius local
aaa accounting network network2 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 network1
  ppp accounting network2
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 network1 group radius local** command defines the network authorization method list named “network1”, 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 network2 start-stop group radius group tacacs+** command defines the network accounting method list named “network2”, 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 network1** command applies the blue1 network authorization method list to the specified interfaces.
- The **ppp accounting network2** 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 XE 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 accept only 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 26: 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. |

Configuring AAA Resource Accounting Example

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
```

Configuring AAA Broadcast Accounting Example

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.

Configuring per-DNIS AAA Broadcast Accounting Example

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`.

AAA Session MIB Example

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
```

Additional References

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

Related Documents

| Related Topic | Document Title |
|-------------------------|--|
| Configuring SNMP | <i>Cisco IOS XE Network Management Configuration Guide</i> |
| SNMP commands | <i>Cisco IOS Network Management Command Reference</i> |
| Security commands | <i>Cisco IOS Security Command Reference</i> |
| Configuring Radius | Configuring RADIUS |
| Configuring TACACS+ | Configuring TACACS+ |
| Configuring IP Services | <i>Cisco IOS XE Application Services Configuration Guide</i> |

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 |
|---|---|
| <ul style="list-style-type: none"> CISCO-AAA-SESSION-MIB | 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 |
|---|-------|
| 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 |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | http://www.cisco.com/techsupport |

Feature Information for Configuring 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 27: Feature Information for Configuring Accounting

| Feature Name | Releases | Feature Information |
|--------------------------|--------------------------|---|
| AAA Broadcast Accounting | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa accounting.</p> |
| AAA Session MIB | Cisco IOS XE Release 2.1 | <p>The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP).</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa session-mib disconnect.</p> |
| Connection Accounting | Cisco IOS XE Release 2.1 | <p>Connection accounting 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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |
| AAA Interim Accounting | Cisco IOS XE Release 2.4 | <p>AAA interim accounting allows accounting records to be sent to the accounting server every time there is new accounting information to report, or on a periodic basis.</p> <p>In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa accounting update and subscriber service accounting interim-interval.</p> |



CHAPTER 12

AAA-SERVER-MIB Set Operation

The AAA-SERVER-MIB Set Operation feature allows you to extend and expand your ability to configure authentication, authorization, and accounting (AAA) servers using the CISCO-AAA-SERVER-MIB. Using this feature, you can do the following:

- Create and add new AAA servers.
- Modify the “KEY” under the CISCO-AAA-SERVER-MIB.
- Delete the AAA server configuration.
- [Finding Feature Information, on page 167](#)
- [Prerequisites for AAA-SERVER-MIB Set Operation, on page 167](#)
- [Restrictions for AAA-SERVER-MIB Set Operation, on page 168](#)
- [Information About AAA-SERVER-MIB Set Operation, on page 168](#)
- [How to Configure AAA-SERVER-MIB Set Operation, on page 168](#)
- [Configuration Examples for AAA-SERVER-MIB Set Operation, on page 169](#)
- [Additional References, on page 171](#)
- [Feature Information for AAA-SERVER-MIB Set Operation, on page 172](#)

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

In Cisco IOS XE Release 2.1, the CISCO-AAA-SERVER-MIB supports both the get and set operations. 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

No special configuration is required for this feature. The Simple Network Management Protocol (SNMP) framework can be used to manage MIBs. See the section Additional References for a reference to configuring SNMP.

Verifying RADIUS Server Configuration and Server Statistics

RADIUS server configuration and server statistics 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: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show running-config include radius-server host Example: Router# 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: Router# 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 output example shows the RADIUS server configuration and server statistics before and after the set operation.

Before the Set Operation

```
Router# 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

```
Router# 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
Authn: 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.

```

Router# 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

Router# 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

Related Documents

| Related Topic | Document Title |
|-------------------------------------|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Authentication commands | <i>Cisco IOS Security Command Reference</i> |
| IEEE 802.1x—Flexible Authentication | <i>Securing User Services Configuration Library</i> |

MIBs

| MIB | MIBs Link |
|--|---|
| <ul style="list-style-type: none"> • 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 | <i>IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)</i> |

Technical Assistance

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

Feature Information for 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 28: Feature Information for AAA-SERVER-MIB Set Operation

| Feature Name | Releases | Feature Information |
|------------------------------|--------------------------|--|
| AAA-SERVER-MIB Set Operation | Cisco IOS XE Release 2.1 | This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |



CHAPTER 13

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.

In Cisco IOS XE Release 2.4 and 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 is referred to as the Dynamic Per VRF AAA feature.

- [Prerequisites for Per VRF AAA, on page 173](#)
- [Restrictions for Per VRF AAA, on page 173](#)
- [Information About Per VRF AAA, on page 174](#)
- [How to Configure Per VRF AAA, on page 178](#)
- [Configuration Examples for Per VRF AAA, on page 189](#)
- [Additional References, on page 197](#)
- [Feature Information for Per VRF AAA, on page 198](#)
- [Glossary, on page 200](#)

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 Cisco IOS XE Release 2.4 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 XE Release 2.4 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 29: 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. |
| 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. |

| VSA Name | Value Type | Description |
|-----------------|------------|--|
| 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 | <p>This VSA defines the accounting method list that is to be used for PPP sessions.</p> <p>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.</p> <p>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</p> |
| ppp-authen-list | string | <p>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.</p> <p>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.</p> <p>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.”</p> |
| ppp-authen-type | string | <p>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.</p> <p>The end user will be permitted to log in using only the methods that are specified in this VSA.</p> <p>PPP will attempt these authentication methods in the order presented in the attribute.</p> |

| VSA Name | Value Type | Description |
|---|------------|---|
| ppp-author-list | string | <p>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.</p> <p>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.</p> <p>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.”</p> |
| <p>Note The RADIUS VSAs--rad-serv, rad-serv-filter, rad-serv-source-if, and rad-serv-vrf--must have the prefix “aaa:” before the VSA name.</p> | | |
| rad-serv | string | <p>This VSA indicates the IP address, key, timeout, and retransmit number of a server, as well as the group of the server.</p> <p>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.</p> <p>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.</p> |
| rad-serv-filter | string | <p>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.</p> <p>Note This VSA is supported in Cisco IOS XE Release 2.3 and later releases.</p> |
| rad-serv-source-if | string | <p>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.</p> |
| rad-serv-vrf | string | <p>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.</p> |

VRF Aware Framed-Routes

In Cisco IOS XE Release 2.3 and later, the Cisco ASR 1000 Series Aggregation Services Routers support VRF aware framed-routes. No configuration is required to enable support for this feature. Framed-routes are automatically detected and if the framed-route is part of a VRF associated with an interface, the route is applied accordingly.

How to Configure Per VRF AAA

Configuring Per VRF AAA

Configuring AAA

To enable AAA you need to complete the following steps.

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Router(config)# aaa new-model | Enables AAA globally. |

Configuring Server Groups

To configure server groups you need to complete the following steps.

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: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Router(config)# aaa new-model</pre> | Enables AAA globally. |
| Step 4 | aaa group server radius groupname Example: <pre>Router(config)# aaa group server radius v2.44.com</pre> | 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: <pre>Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww</pre> | 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. |
| Step 6 | exit Example: <pre>Router(config-sg-radius)# exit</pre> | Exits from server-group configuration mode; returns to global configuration mode. |

Configuring Authentication Authorization and Accounting for Per VRF AAA

To configure authentication, authorization, and accounting for Per VRF AAA, you need to complete the following steps.

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: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Router(config)# aaa new-model</pre> | Enables AAA globally. |
| Step 4 | aaa authentication ppp {default list-name} method1 [method2...] Example: <pre>Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com</pre> | Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. |
| Step 5 | aaa authorization {network exec commands level reverse-access configuration} {default list-name} method1 [method2...] Example: <pre>Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com</pre> | 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: | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. |

| | Command or Action | Purpose |
|---------------|--|--|
| | Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com | |
| Step 7 | aaa accounting delay-start [<i>vrf vrf-name</i>] Example: Router(config)# aaa accounting 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 } [<i>vrf vrf-name</i>] 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: <ul style="list-style-type: none"> • 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 XE Release 2.4 and later releases. |

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. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | ip radius source-interface <i>subinterface-name</i> [vrf <i>vrf-name</i>] 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 <i>vrf-name</i>] 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

To configure interface-specific commands for Per VRF AAA, you need to complete the following steps.

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

| | Command or Action | Purpose |
|--------|---|--|
| Step 3 | interface <i>type number</i> [<i>name-tag</i>] Example: <pre>Router(config)# interface loopback11</pre> | Configures an interface type and enters interface configuration mode. |
| Step 4 | ip vrf forwarding <i>vrf-name</i> Example: <pre>Router(config-if)# ip vrf forwarding v2.44.com</pre> | Associates a VRF with an interface. |
| Step 5 | ppp authentication <i>{protocol1 [protocol2...]} listname</i> Example: <pre>Router(config-if)# ppp authentication chap callin V2_44_com</pre> | 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. |
| Step 6 | ppp authorization <i>list-name</i> Example: <pre>Router(config-if)# ppp authorization V2_44_com</pre> | Enables AAA authorization on the selected interface. |
| Step 7 | ppp accounting default Example: <pre>Router(config-if)# ppp accounting default</pre> | Enables AAA accounting services on the selected interface. |
| Step 8 | exit Example: <pre>Router(config)# exit</pre> | Exits interface configuration mode. |

Configuring Per VRF AAA Using Local Customer Templates

Configuring AAA

Perform the tasks as outlined in the Configuring Per VRF AAA.

Configuring Server Groups

Perform the tasks as outlined in the Configuring Server Groups.

Configuring Authentication Authorization and Accounting for Per VRF AAA

Perform the tasks as outlined in the Configuring Authentication Authorization and Accounting for Per VRF AAA.

Configuring Authorization for Per VRF AAA with Local Customer Templates

To configure authorization for Per VRF AAA with local templates, you need to complete the following steps.

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa 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

To configure local customer templates, you need to complete the following steps.

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | vpdn search-order domain Example: Router (config)# vpdn search-order domain | Looks up the profiles based on domain. |
| Step 4 | template <i>name</i> [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 <i>pool-name</i> 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. |
| Step 6 | ppp authentication { <i>protocol1</i> [<i>protocol2...</i>]} [if-needed] [<i>list-name</i> default] [callin] [one-time] Example: Router(config-template)# ppp authentication chap | (Optional) Sets the PPP link authentication method. |
| Step 7 | ppp authorization [default <i>list-name</i>] Example: Router(config-template)# ppp authorization v2_44_com | (Optional) Sets the PPP link authorization method. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 8 | aaa accounting {auth-proxy system network exec connection commands <i>level</i> } {default list-name} [vrf <i>vrf-name</i>] {start-stop stop-only none} [broadcast] group <i>groupname</i> 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

Perform the tasks as outlined in the Configuring Per VRF AAA.

Configuring Server Groups

Perform the tasks as outlined in the Configuring Server Groups.

Configuring Authentication for Per VRF AAA with Remote Customer Profiles

To configure authentication for Per VRF AAA with remote customer profiles, you need to perform the following steps.

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

| | Command or Action | Purpose |
|---------------|--|---|
| | Router# configure terminal | |
| Step 3 | 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 Profiles

To configuring authorization for Per VRF AAA with remote customer profiles, you need to perform the following step.

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa authorization template Example: Router(config)# aaa authorization template | Enables use of local or remote templates. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 4 | aaa authorization {network exec commands <i>level</i> reverse-access configuration} {default list-name} [[<i>method1</i> [<i>method2</i> ...]] 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

Configure the RADIUS profile on the Service Provider (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

To verify VRF routing configurations, you need to complete the following steps:

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | show ip route vrf <i>vrf-name</i> 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 Record 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 XE Release 2.4 and later releases.

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

```

AAA Accounting Stop Record and Rejected Call Example

```

*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 01 00 00 80 08 00 00
      00 00 00 04 80 1E 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

```

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 SCCRQ
*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

```

AAA Accounting Stop Record and Successful Call Example

```

      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 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

```

Additional References

The following sections provide references related to Per VRF AAA.

Related Documents

| Related Topic | Document Title |
|---|---|
| Configuring server groups | Configuring RADIUS chapter in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2. |
| RADIUS attribute screening | RADIUS Attribute Value Screening chapter in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2. |
| Configuring broadcast accounting | Configuring Accounting chapter in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2. |
| Cisco IOS Security Commands | <i>Cisco IOS Security Command Reference</i> |
| Cisco IOS Switching Services Commands | <i>Cisco IOS IP Switching Command Reference</i> |
| Configuring Multiprotocol Label Switching | <i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i> , Release 2 |
| Configuring virtual templates | Virtual Templates and Profiles section of the <i>Cisco IOS XE Dial Technologies Configuration Guide</i> , Release 2 |

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

Feature Information for 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 30: Feature Information for Per VRF AAA

| Feature Name | Releases | Feature Information |
|--|--------------------------|---|
| Per VRF AAA | Cisco IOS XE Release 2.1 | <p>The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa accounting, aaa accounting delay-start, ip radius source-interface, server-private (RADIUS), ip vrf forwarding (server-group), radius-server domain-stripping, aaa authorization template.</p> |
| RADIUS Per-VRF Server Group | Cisco IOS XE Release 2.1 | <p>Using the Radius Per-VRF Server Group feature, Internet Service Providers (ISPs) can partition RADIUS server groups based on Virtual Route Forwarding (VRF). This means that you can define RADIUS server groups that belong to a VRF. This feature is supported by “aaa: rad-serv-vrf” VSA.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: ip vrf forwarding.</p> |
| Attribute Filtering Per-Domain and VRF Aware Framed-Routes | Cisco IOS XE Release 2.3 | <p>The Attribute Filtering Per-Domain and VRF Aware Framed-Routes feature allows for attribute filtering per-domain and VRF aware Framed-Routes. It introduces support for the “aaa:rad-serv-filter” VSA.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |
| AAA CLI Stop Record Enhancement | Cisco IOS XE Release 2.4 | <p>The AAA CLI Stop Record Enhancement feature enables sending an accounting stop record only when an access accept is received from the AAA server.</p> <p>In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: aaa accounting send stop-record authentication.</p> |
| Dynamic Per VRF AAA | Cisco IOS XE Release 2.4 | <p>The Dynamic Per VRF AAA feature allows you to 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.</p> <p>In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

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 disjointed routing/forwarding tables, where the routes of a user have no correlation with the routes of another user.



CHAPTER 14

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, on page 201](#)
- [Information About AAA Support for IPv6, on page 201](#)
- [How to Configure AAA Support for IPv6, on page 206](#)
- [Configuration Examples for AAA Support for IPv6, on page 207](#)
- [Additional References, on page 207](#)
- [Feature Information for RADIUS over IPv6, on page 209](#)

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 `inac1`, `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 RADIUS attributes are supported for virtual access and can be used as attribute-value (AV) pairs:

- Delegated-IPv6-Prefix
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#

- IPv6 Route
- Login-IPv6-Host

Delegated-IPv6-Prefix

The Delegated-IPv6-Prefix attribute indicates an IPv6 prefix to be delegated to a user for use in a network. This attribute is used during DHCP prefix delegation between a RADIUS server and a delegating device. A Network Access Server (NAS) that hosts a DHCP Version 6 (DHCPv6) server can act as a delegating device.

The following example shows how to use the Delegated-IPv6-Prefix attribute:

```
ipv6:delegated-prefix=2001:DB8::/64
```



Note The Cisco VSA format is not supported for this attribute. If you try to add this attribute in the Cisco VSA format into a user profile, the RADIUS server response fails. Use only the IETF attribute format for this attribute.

Delegated-IPv6-Prefix-Pool

The Delegated-IPv6-Prefix-Pool attribute indicates the name of a prefix pool from which a prefix is selected and delegated to a device.

Prefix delegation is a DHCPv6 option for delegating IPv6 prefixes. Prefix delegation involves a delegating device that selects a prefix and assigns it on a temporary basis to a requesting device. A delegating device uses many strategies to choose a prefix. One method is to choose a prefix from a prefix pool with a name that is defined locally on a device.

The Delegated-IPv6-Prefix-Pool attribute indicates the name of an assigned prefix pool. A RADIUS server uses this attribute to communicate the name of a prefix pool to a NAS hosting a DHCPv6 server and acting as a delegating device.

You may use DHCPv6 prefix delegation along with ICMPv6 stateless address autoconfiguration (SLAAC) on a network. In this case, both the Delegated-IPv6-Prefix-Pool attribute and the Framed-IPv6-Pool attribute may be included within the same packet. To avoid ambiguity, the Delegated-IPv6-Prefix-Pool attribute should be restricted to the authorization and accounting of prefix pools used in DHCPv6 delegation, and the Framed-IPv6-Pool attribute should be used for the authorization and accounting of prefix pools used in SLAAC.

The following example shows how an address prefix is selected from a pool named pool1. The prefix pool pool1 is downloaded to a delegating device from a RADIUS server by using the Delegated-IPv6-Prefix-Pool attribute. The device then selects the address prefix 2001:DB8::/64 from this prefix pool.

```
Cisco:Cisco-AVpair = "ipv6:delegated-ipv6-pool = pool1"
!
ipv6 dhcp pool pool1
address prefix 2001:DB8::/64
!
```

DNS-Server-IPv6-Address

The DNS-Server-IPv6-Address attribute indicates the IPv6 address of a Domain Name System (DNS) server. A DHCPv6 server can configure a host with the IPv6 address of a DNS server. The IPv6 address of the DNS server can also be conveyed to the host using router advertisement messages from ICMPv6 devices.

A NAS may host a DHCPv6 server to handle DHCPv6 requests from hosts. The NAS may also act as a device that provides router advertisement messages. Therefore, this attribute is used to provide the NAS with the IPv6 address of the DNS server.

If a NAS has to announce more than one recursive DNS server to a host, this attribute can be included multiple times in Access-Accept packets sent from the NAS to the host.

The following example shows how you can define the IPv6 address of a DNS server by using the DNS-Server-IPv6-Address attribute:

```
Cisco:Cisco-AVpair = "ipv6:ipv6-dns-servers-addr=2001:DB8::"
```

Framed-Interface-Id

The Framed-Interface-Id attribute indicates an IPv6 interface identifier to be configured for a user.

This attribute is used during IPv6 Control Protocol (IPv6CP) negotiations of the Interface-Identifier option. If negotiations are successful, the NAS uses this attribute to communicate a preferred IPv6 interface identifier to the RADIUS server by using Access-Request packets. This attribute may also be used in Access-Accept packets.

Framed-IPv6-Pool

The Framed-IPv6-Pool attribute indicates the name of a pool that is used to assign an IPv6 prefix to a user. This pool should be either defined locally on a device or defined on a RADIUS server from where pools can be downloaded.

Framed-IPv6-Prefix

The Framed-IPv6-Prefix attribute indicates an IPv6 prefix (and a corresponding route) to be configured for a user. So this attribute performs the same function as a Cisco VSA and is used for virtual access only. A NAS uses this attribute to communicate a preferred IPv6 prefix to a RADIUS server by using Access-Request packets. This attribute may also be used in Access-Accept packets and can appear multiple times in these packets. The NAS creates a corresponding route for the prefix.

This attribute is used by a user to specify which prefixes to advertise in router advertisement messages of the Neighbor Discovery Protocol.

This attribute can also be used for DHCPv6 prefix delegation, and a separate profile must be created for a user on the RADIUS server. The username associated with this separate profile has the suffix “-dhcpv6”.

The Framed-IPv6-Prefix attribute is treated differently in this separate profile and the regular profile of a user. If a NAS needs to send a prefix through router advertisement messages, the prefix is placed in the Framed-IPv6-Prefix attribute of the regular profile of the user. If a NAS needs to delegate a prefix to the network of a remote user, the prefix is placed in the Framed-IPv6-Prefix attribute of the separate profile of the user.



Note The RADIUS IETF attribute format and the Cisco VSA format are supported for this attribute.

Framed-IPv6-Route

The Framed-IPv6-Route attribute indicates the routing information to be configured for a user on a NAS. This attribute performs the same function as a Cisco VSA. The value of the attribute is a string and is specified by using the **ipv6 route** command.

IPv6 ACL

The IPv6 ACL attribute is used to specify a complete IPv6 access list. The unique name of an access list is generated automatically. An access list is removed when the respective user logs out. The previous access list on the interface is then reapplied.

The `inacl` and `outacl` attributes enable you to specify an existing access list configured on a device. The following example shows how to define an access list identified with number 1:

```
cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:cc00:1::/48",  
cisco-avpair = "ipv6:outacl#1=deny 2001:DB8::/10",
```

IPv6_DNS_Servers

The IPv6_DNS_Servers attribute is used to send up to two DNS server addresses to the DHCPv6 server. The DNS server addresses are saved in the interface DHCPv6 subblock and override other configurations in the DHCPv6 pool. This attribute is also included in attributes returned for AAA start and stop notifications.

IPv6 Pool

The IPv6 Pool attribute extends the IPv4 address pool attribute to support the IPv6 protocol for RADIUS authentication. This attribute specifies the name of a local pool on a NAS from which a prefix is chosen and used whenever PPP is configured and the protocol is specified as IPv6. The address pool works with local pooling and specifies the name of a local pool that is preconfigured on the NAS.

IPv6 Prefix#

The IPv6 Prefix# attribute indicates which prefixes to advertise in router advertisement messages of the Neighbor Discovery Protocol. When this attribute is used, a corresponding route (marked as a per-user static route) is installed in the routing information base (RIB) tables for a given prefix.

The following example shows how to specify which prefixes to advertise:

```
cisco-avpair = "ipv6:prefix#1=2001:DB8::/64",  
cisco-avpair = "ipv6:prefix#2=2001:DB8::/64",
```

IPv6 Route

The IPv6 Route attribute is used to specify a static route for a user. A static route is appropriate when Cisco software cannot dynamically build a route to the destination. See the **ipv6 route** command for more information about building static routes.

The following example shows how to use the IPv6 Route attribute 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 indicates IPv6 addresses of hosts with which to connect a user when the Login-Service attribute is included. A NAS uses the Login-IPv6-Host attribute in Access-Request packets to communicate to a RADIUS server that it prefers to use certain hosts.

How to Configure AAA Support for IPv6

Configuring DHCPv6 AAA Options

Perform the following task to configure the option of acquiring prefixes from the AAA server:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *pool-name*
4. **prefix-delegation aaa** [**method-list** *method-list*] [*lifetime*]
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 | ipv6 dhcp pool <i>pool-name</i> Example: Device(config)# ipv6 dhcp pool pool1 | Configures a DHCPv6 configuration information pool and enters IPv6 DHCP pool configuration mode. |
| Step 4 | prefix-delegation aaa [method-list <i>method-list</i>] [<i>lifetime</i>] Example: Device(config-dhcpv6)# prefix-delegation aaa method-list list1 | Specifies that prefixes are to be acquired from AAA servers. |
| Step 5 | end Example: Device(config-dhcpv6)# end | Exits IPv6 DHCP pool configuration mode and returns to privileged EXEC mode. |

Configuration Examples for AAA Support for IPv6

Example: DHCPv6 AAA Options Configuration

The following example shows how to configure the DHCPv6 option of acquiring prefixes from the AAA server:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# prefix-delegation aaa method-list list1
Device(config-dhcpv6)# end
```

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

The following sections provide references related to the Authorization feature.

Related Documents

| Related Topic | Document Title |
|-------------------------------|---|
| Authorization Commands | <i>Cisco IOS Security Command Reference</i> |
| 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. |

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

Feature Information for RADIUS 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 31: Feature Information for RADIUS over IPv6

| Feature Name | Releases | Feature Information |
|------------------|-----------|--|
| RADIUS over IPv6 | 15.1(1)SY | RADIUS attributes defined in RFC 3162 are supported. |



CHAPTER 15

TACACS+ over IPv6

An IPv6 server can be configured to be used with TACACS+.

- [Finding Feature Information, on page 211](#)
- [Information About TACACS+ over IPv6, on page 211](#)
- [How to Configure TACACS+ over IPv6, on page 212](#)
- [Configuration Examples for TACACS+ over IPv6, on page 215](#)
- [Additional References, on page 215](#)
- [Feature Information for TACACS+ over IPv6, on page 217](#)

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | tacacs server <i>name</i> Example: Device(config)# tacacs server server1 | Configures the TACACS+ server for IPv6 and enters TACACS+ server configuration mode. |
| Step 4 | address ipv6 <i>ipv6-address</i> Example: | Configures the IPv6 address of the TACACS+ server. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5 | |
| Step 5 | key [0 7] <i>key-string</i> Example: Device(config-server-tacacs)# key 0 key1 | Configures the per-server encryption key on the TACACS+ server. |
| Step 6 | port [<i>number</i>] 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 <i>seconds</i> 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: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | ipv6 tacacs source-interface <i>type number</i> Example: Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0 | 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa group server tacacs+ <i>group-name</i> Example: Device(config)# aaa group server tacacs+ group1 | Groups different TACACS+ server hosts into distinct lists and distinct methods. |
| Step 4 | server name <i>server-name</i> Example: Device(config-sg-tacacs+)# server name server1 | Specifies an IPv6 TACACS+ server. |

| | Command or Action | Purpose |
|--------|---|---|
| Step 5 | <pre>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</pre> | 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

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 <i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4T. |
| Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices | <i>Cisco IOS Dial Technologies Command Reference</i> |
| Lists of IOS Security Commands | <i>Cisco IOS Security Command Reference</i> |
| Configuring PPP authentication using AAA | Configuring PPP Authentication Using AAA in the Configuring Authentication module in the <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , Release 12.4T. |

| Related Topic | Document Title |
|-----------------------------------|---|
| Configuring RADIUS Authentication | Configuring RADIUS module in the <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , 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 | <i>Point-to-Point Protocol (PPP)</i> |
| RFC 2548 | <i>Microsoft Vendor-specific RADIUS Attributes</i> |
| RFC 2759 | <i>Microsoft PPP CHAP Extensions, Version 2</i> |

Technical Assistance

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

Feature Information for 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 32: Feature Information for TACACS+ over IPv6

| Feature Name | Releases | Feature Information |
|-------------------|---------------------------|--|
| TACACS+ over IPv6 | Cisco IOS XE Release 3.2S | TACACS+ over IPv6 is supported. 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 16

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 downtime and quicker packet processing.

- [Finding Feature Information, on page 219](#)
- [Prerequisites for AAA Dead-Server Detection, on page 219](#)
- [Restrictions for AAA Dead-Server Detection, on page 220](#)
- [Information About AAA Dead-Server Detection, on page 220](#)
- [How to Configure AAA Dead-Server Detection, on page 220](#)
- [Configuration Examples for AAA Dead-Server Detection, on page 222](#)
- [Additional References, on page 223](#)
- [Feature Information for AAA Dead-Server Detection, on page 224](#)

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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 | <i>Cisco IOS Security Command Reference</i> |

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 | <i>Remote Authentication Dial In User Service (RADIUS)</i> |

Technical Assistance

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

Feature Information for 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 33: Feature Information for AAA Dead-Server Detection

| Feature Name | Releases | Feature Information |
|---------------------------|---------------------------|--|
| AAA Dead-Server Detection | Cisco IOS XE Release 3.9S | 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 17

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, on page 227](#)
- [Prerequisites for Login Password Retry Lockout, on page 227](#)
- [Restrictions for Login Password Retry Lockout, on page 227](#)
- [Information About Login Password Retry Lockout, on page 228](#)
- [How to Configure Login Password Retry Lockout, on page 228](#)
- [Configuration Examples for Login Password Retry Lockout, on page 231](#)
- [Additional References, on page 232](#)
- [Feature Information for Login Password Retry Lockout, on page 233](#)
- [Glossary, on page 233](#)

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: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | username <i>name</i> [privilege level] password <i>encryption-type password</i> Example: <pre>Device(config)# username user1 privilege 15 password 0 cisco</pre> | Establishes a username-based authentication system. |
| Step 4 | aaa new-model Example: <pre>Device(config)# aaa new-model</pre> | Enables the AAA access control model. |
| Step 5 | aaa local authentication attempts max-fail <i>number-of-unsuccessful-attempts</i> Example: <pre>Device(config)# aaa local authentication attempts max-fail 3</pre> | Specifies the maximum number of unsuccessful attempts before a user is locked out. |
| Step 6 | aaa authentication login default <code>method</code> Example: <pre>Device(config)# aaa authentication login default local</pre> | 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | clear aaa local user lockout {username <i>username</i> 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | clear aaa local user fail-attempts {username <i>username</i> all} Example: Device# clear aaa local user fail-attempts username user1 | Clears the unsuccessful attempts of the user. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Enter your password if prompted. |
| 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 | <i>Cisco IOS Security Command Reference</i> |

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

Feature Information for 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 34: Feature Information for Login Password Retry Lockout

| Feature Name | Releases | Feature Information |
|------------------------------|---------------------------|---|
| Login Password Retry Lockout | Cisco IOS XE Release 3.9S | <p>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.</p> <p>The following commands were introduced or modified: aaa local authentication attempts max-fail, clear aaa local user fail-attempts, clear aaa local user lockout.</p> |

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 18

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, on page 235](#)
- [Prerequisites for MSCHAP Version 2, on page 236](#)
- [Restrictions for MSCHAP Version 2, on page 236](#)
- [Information About MSCHAP Version 2, on page 236](#)
- [How to Configure MSCHAP Version 2, on page 237](#)
- [Configuration Examples, on page 240](#)
- [Additional References, on page 241](#)
- [Feature Information for MSCHAP Version 2, on page 243](#)

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 feature 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 MSCHAP V2 Authentication

To configure the NAS to accept MSCHAP V2 authentication for local or RADIUS authentication and to allow proper interpretation of authentication failure attributes and vendor-specific RADIUS attributes for RADIUS authentication, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **ppp max-bad-auth** *number*
6. **ppp authentication ms-chap-v2**
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 | radius-server vsa send authentication Example: Device(config)# radius-server vsa send authentication | Configures the NAS to recognize and use vendor-specific attributes. |
| Step 4 | interface <i>type number</i> Example: | Configures an interface type and enters interface configuration mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| | Device(config)# interface GigabitEthernet 1/0/1 | |
| Step 5 | <p>ppp max-bad-auth <i>number</i></p> <p>Example:</p> <pre>Device(config-if)# ppp max-bad-auth 2</pre> | <p>Configures a point-to-point interface to reset immediately after an authentication failure or within a specified number of authentication retries.</p> <ul style="list-style-type: none"> • The default value for the <i>number</i> argument is 0 seconds (immediately). • The range is between 0 and 255. <p>Note The <i>number</i> argument must be set to a value of at least 2 for authentication failure attributes to be interpreted by the NAS.</p> |
| Step 6 | <p>ppp authentication ms-chap-v2</p> <p>Example:</p> <pre>Device(config-if)# ppp authentication ms-chap-v2</pre> | Enables MSCHAP V2 authentication on a NAS. |
| Step 7 | <p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> | Returns to privileged EXEC mode. |

Verifying MSCHAP V2 Configuration

To verify that the MSCHAP Version 2 feature is configured properly, perform the following steps.

SUMMARY STEPS

1. **show running-config interface** *type number*
2. **debug ppp negotiation**
3. **debug ppp authentication**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | <p>show running-config interface <i>type number</i></p> <p>Example:</p> <pre>Device# show running-config interface Async65</pre> | Verifies the configuration of MSCHAP V2 as the authentication method for the specified interface. |
| Step 2 | <p>debug ppp negotiation</p> <p>Example:</p> | Verifies successful MSCHAP V2 negotiation. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device# debug ppp negotiation | |
| Step 3 | debug ppp authentication Example: Device# debug ppp authentication | Verifies successful MSCHAP V2 authentication. |

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

| | Command or Action | Purpose |
|---------------|--|--|
| Step 3 | aaa new-model Example: <pre>Device(config)# aaa new-model</pre> | Enables AAA globally. |
| Step 4 | aaa authentication login {default list-name} passwd-expiry method1 [method2...] Example: <pre>Device(config)# aaa authentication login userauthen passwd-expiry group radius</pre> | 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: <pre>Device(config)# crypto map clientmap client authentication list userauthen</pre> | 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 <i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4T. |

| Related Topic | Document Title |
|---|---|
| Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices | <i>Cisco IOS Dial Technologies Command Reference</i> |
| Lists of IOS Security Commands | <i>Cisco IOS Security Command Reference</i> |
| Configuring PPP authentication using AAA | Configuring PPP Authentication Using AAA in the Configuring Authentication module in the <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , Release 12.4T. |
| Configuring RADIUS Authentication | Configuring RADIUS module in the <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , 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 | <i>Point-to-Point Protocol (PPP)</i> |
| RFC 2548 | <i>Microsoft Vendor-specific RADIUS Attributes</i> |
| RFC 2759 | <i>Microsoft PPP CHAP Extensions, Version 2</i> |

Technical Assistance

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

Feature Information for 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 35: Feature Information for MSCHAP Version 2

| Feature Name | Releases | Feature Information |
|------------------|---------------------------|---|
| MSCHAP Version 2 | Cisco IOS XE Release 3.9S | <p>The MSCHAP Version 2 feature 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).</p> <p>The following commands were introduced or modified: aaa authentication login, and ppp authentication ms-chap-v2.</p> |



CHAPTER 19

AAA Broadcast Accounting-Mandatory Response 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, on page 245](#)
- [Prerequisites for AAA Broadcast Accounting-Mandatory Response Support, on page 245](#)
- [Restrictions for AAA Broadcast Accounting-Mandatory Response Support, on page 246](#)
- [Information About AAA Broadcast Accounting-Mandatory Response Support, on page 246](#)
- [How AAA Broadcast Accounting is Supported for GGSN, on page 247](#)
- [Configuration Examples for AAA Broadcast Accounting-Mandatory Response Support, on page 249](#)
- [Additional References, on page 250](#)
- [Feature Information for AAA Broadcast Accounting-Mandatory Response Support, on page 252](#)

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: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter the password if prompted. |
| Step 2 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Router# aaa new-model</pre> | Enables new access control commands and functions (disables the old commands). |
| Step 4 | aaa accounting network {method-list-name default} Example: <pre>Router(config)# aaa accounting network net1</pre> | 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. <ul style="list-style-type: none"> • The <i>method-list-name</i> argument is the named accounting list, which has a maximum of 31 characters. Any characters longer than the maximum are rejected. • The default keyword specifies the default accounting list. |
| Step 5 | action-type {start-stop stop-only none} Example: <pre>Router(cfg-acct-mlist)#action-type start-stop</pre> | Performs a type of action on accounting records. Possible values are: <ul style="list-style-type: none"> • 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: <pre>Router(cfg-acct-mlist)#broadcast</pre> | (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. |

| | Command or Action | Purpose |
|---------|--|---|
| Step 7 | group <i>server-group</i> [mandatory] Example: <pre>Router(cfg-acct-mlist)#group server1</pre> | 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 <i>list-name</i> Example: <pre>Router(config)# gprs access-point-list public1</pre> | 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 <i>access-point-index</i> Example: <pre>Router(config-ap-list)# access-point 11</pre> | Specifies an access point number and enters access point configuration mode. |
| Step 11 | aaa-group accounting <i>method-list name</i> Example: <pre>Router(config-access-point)#aaa-group accounting net1</pre> | Specifies an accounting server group. |
| Step 12 | gtp-response-message wait-accounting Example: <pre>Router(config-access-point)# gtp-response-message wait-accounting</pre> | 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 | <i>Cisco GGSN Release 8.0 Configuration Guide</i> |
| AAA commands | <i>Cisco IOS Security Command Reference Guide</i> |

| Related Topic | Document Title |
|---------------|---|
| AAA features | <i>Cisco IOS Security Configuration Guide: Securing User Services</i> |

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

Feature Information for 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 36: Feature Information for AAA Broadcast Accounting--Mandatory Response Support

| Feature Name | Releases | Feature Information |
|--|---------------------------|--|
| AAA Broadcast Accounting--Mandatory Response Support | Cisco IOS XE Release 3.9S | <p>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.</p> <p>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</p> |



CHAPTER 20

Password Strength and Management for Common Criteria

The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.

For local users, the user profile and the password information with the key parameters are stored on the Cisco device, and this profile is used for local authentication of users. The user can be an administrator (terminal access) or a network user (for example, PPP users being authenticated for network access).

For remote users, where the user profile information is stored in a remote server, a third-party authentication, authorization, and accounting (AAA) server may be used for providing AAA services, both for administrative and network access.

- [Finding Feature Information, on page 253](#)
- [Restrictions for Password Strength and Management for Common Criteria, on page 254](#)
- [Information About Password Strength and Management for Common Criteria, on page 254](#)
- [How to Configure Password Strength and Management for Common Criteria, on page 256](#)
- [Configuration Example for the Password Strength and Management for Common Criteria Feature, on page 259](#)
- [Additional References, on page 260](#)
- [Feature Information for Password Strength and Management for Common Criteria, on page 261](#)

Finding Feature Information

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

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

Restrictions for Password Strength and Management for Common Criteria

- Only four concurrent users can log on to the system by using vty at any moment.
- For local users, password common criteria full evaluation is applicable only to the **username** *username* **common-criteria-policy** *policy-name* **password** *cleartext-password* command.
- For local users that have been defined using the **username** *username* **common-criteria-policy** *policy-name* **secret** 5|8|9<*HASH*> commands, they are not evaluated against the password common criteria. Only the common criteria lifetime is applied to the username.
- Use of other configuration options are not supported, including the following commands:
 - **username** *username* **common-criteria-policy** AAA-CC **secret** *cleartext-secret*
 - **username** *username* **common-criteria-policy** AAA-CC **algorithm-type** md5 | **script** | sha256 **secret** *cleartext-secret*

Information About Password Strength and Management for Common Criteria

Password Composition Policy

The password composition policy allows you to create passwords of any combination of upper and lowercase characters, numbers, and special characters that include “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “)”.

Password Length Policy

The administrator has the flexibility to set the password's minimum and maximum length. The recommended minimum password length is 8 characters. The administrator can specify both the minimum (1) and the maximum (64) length for the password.

Password Lifetime Policy

The security administrator can provide a configurable option for a password to have a maximum lifetime. If the lifetime parameter is not configured, the configured password will never expire. The maximum lifetime can be configured by providing the configurable value in years, months, days, hours, minutes, and seconds. The lifetime configuration will survive across reloads as it is a part of the configuration, but every time the system reboots, the password creation time will be updated to the new time. For example, if a password is configured with a lifetime of one month and on the 29th day, the system reboots, then the password will be valid for one month after the system reboots.

When you configure the lifetime using months, the policy sets the lifetime to 30 days regardless of the number of days in the specified month.

Password Expiry Policy

If the user attempts to log on and if the user's password credentials have expired, then the following happens:

1. The user is prompted to set the new password after successfully entering the expired password.
2. When the user enters the new password, the password is validated against the password security policy.
3. If the new password matches the password security policy, then the AAA database is updated, and the user is authenticated with the new password.
4. If the new password does not match the password security policy, then the user is prompted again for the password. From AAA perspective, there is no restriction on the number of retries. The number of retries for password prompt in case of unsuccessful authentication is controlled by the respective terminal access interactive module. For example, for telnet, after three unsuccessful attempts, the session will be terminated.

If the password's lifetime is not configured for a user and the user has already logged on and if the security administrator configures the lifetime for that user, then the lifetime will be set in the database. When the same user is authenticated the next time, the system will check for password expiry. The password expiry is checked only during the authentication phase.

If the user has been already authenticated and logged on to the system and if the password expires, then no action will be taken. The user will be prompted to change the password only during the next authentication for the same user.

Password Change Policy

The new password must contain a minimum of 4 character changes from the previous password. A password change can be triggered by the following scenarios:

- The security administrator wants to change the password.
- The user is trying to get authenticated using a profile, and the password for that profile has expired.

When the security administrator changes the password security policy and the existing profile does not meet the password security policy rules, no action will be taken if the user has already logged on to the system. The user will be prompted to change the password only when the user tries to get authenticated using the profile that does not meet the password security restriction.

When the user changes the password, the lifetime parameters set by the security administrator for the old profile will be the lifetime parameters for the new password.

For noninteractive clients such as dot1x, when the password expires, appropriate error messages will be sent to the clients, and the clients must contact the security administrator to renew the password.

User Reauthentication Policy

Users are reauthenticated when they change their passwords.

When users change their passwords on expiry, they will be authenticated against the new password. In such cases, the actual authentication happens based on the previous credentials, and the new password is updated in the database.



Note Users can change their passwords only when they are logging on and after the expiry of the old password; however, a security administrator can change the user's password at any time.

Support for Framed (noninteractive) Session

When a client such as dot1x uses the local database for authentication, the Password Strength and Management for Common Criteria feature will be applicable; however, upon password expiry, clients will not be able to change the password. An appropriate failure message will be sent to such clients, and the user must request the security administrator to change the password.

How to Configure Password Strength and Management for Common Criteria

Configuring the Password Security Policy

Perform this task to create a password security policy and to apply the policy to a specific user profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa common-criteria policy *policy-name***
5. **char-changes *number***
6. **max-length *number***
7. **min-length *number***
8. **numeric-count *number***
9. **special-case *number***
10. **exit**
11. **username *username* common-criteria-policy *policy-name* password *password***
12. **end**

DETAILED STEPS

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

| | 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 common-criteria policy <i>policy-name</i> Example: Device(config)# aaa common-criteria policy policy1 | Creates the AAA security password policy and enters common criteria configuration policy mode. |
| Step 5 | char-changes <i>number</i> Example: Device(config-cc-policy)# char-changes 4 | (Optional) Specifies the number of changed characters between old and new passwords. |
| Step 6 | max-length <i>number</i> Example: Device(config-cc-policy)# max-length 25 | (Optional) Specifies the maximum length of the password. |
| Step 7 | min-length <i>number</i> Example: Device(config-cc-policy)# min-length 8 | (Optional) Specifies the minimum length of the password. |
| Step 8 | numeric-count <i>number</i> Example: Device(config-cc-policy)# numeric-count 4 | (Optional) Specifies the number of numeric characters in the password. |
| Step 9 | special-case <i>number</i> Example: Device(config-cc-policy)# special-case 3 | (Optional) Specifies the number of special characters in the password. |
| Step 10 | exit Example: Device(config-cc-policy)# exit | (Optional) Exits common criteria configuration policy mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|---------|---|--|
| Step 11 | username <i>username</i> common-criteria-policy <i>policy-name</i> password <i>password</i> Example: <pre>Device(config)# username user1 common-criteria-policy policy1 password password1</pre> | (Optional) Applies a specific policy and password to a user profile. |
| Step 12 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Verifying the Common Criteria Policy

Perform this task to verify all the common criteria security policies.

SUMMARY STEPS

1. **enable**
2. **show aaa common-criteria policy name** *policy-name*
3. **show aaa common-criteria policy all**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show aaa common-criteria policy name** *policy-name*

Displays the password security policy information for a specific policy.

Example:

```
Device# show aaa common-criteria policy name policy1
```

```
Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
```

Step 3 **show aaa common-criteria policy all**

Displays password security policy information for all the configured policies.

Example:

```
Device# show aaa common-criteria policy all
=====
Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
=====
Policy name: policy2
Minimum length: 1
Maximum length: 34
Upper Count: 10
Lower Count: 5
Numeric Count: 4
Special Count: 2
Number of character changes 2
Valid forever. User tied to this policy will not expire.
=====
```

Troubleshooting Tips

Use the `debug aaa common-criteria` command to troubleshoot AAA common criteria.

Configuration Example for the Password Strength and Management for Common Criteria Feature

Example: Password Strength and Management for Common Criteria

The following example shows how to create a common criteria security policy and apply the specific policy to a user profile:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end
```

Additional References

The following sections provide references related to the RADIUS Packet of Disconnect feature.

Related Documents

| Related Topic | Document Title |
|-------------------|--|
| AAA | Authentication, Authorization, and Accounting (AAA) section of the <i>Cisco IOS XE Security Configuration Guide, Securing User Services</i> , Release 2. |
| Security commands | <i>Cisco IOS Security Command Reference</i> |
| CLI Configuration | <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i> , Release 2 |

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 2865 | <i>Remote Authentication Dial-in User Service</i> |
| RFC 3576 | <i>Dynamic Authorization Extensions to RADIUS</i> |

Technical Assistance

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

Feature Information for Password Strength and Management for Common Criteria

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 37: Feature Information for Password Strength and Management for Common Criteria

| Feature Name | Releases | Feature Information |
|--|--|--|
| Password Strength and Management for Common Criteria | Cisco IOS XE Everest 16.5.1 and later. | <p>The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.</p> <p>The following commands were introduced or modified: aaa common-criteria policy, debug aaa common-criteria, and show aaa common-criteria policy.</p> |
| Password Strength and Management for Common Criteria | Cisco IOS XE Fuji 16.7.1 and later. | <p>The following commands were introduced or modified: username <i>username</i> common-criteria-policy <i>policy-name</i> secret <i>cleartext-secret</i>.</p> |



CHAPTER 21

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, on page 263](#)
- [Prerequisites for Secure Reversible Passwords for AAA, on page 263](#)
- [Information About Secure Reversible Passwords for AAA, on page 264](#)
- [Additional References for Secure Reversible Passwords for AAA, on page 265](#)
- [Feature Information for Secure Reversible Passwords for AAA, on page 266](#)

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*]]]
- **tacacs-server key**
 - **tacacs-server key** {0 *string* | 6 *string* | 7 *string*} *string*



Note We recommend to use type 6 to reduce the vulnerability of a malicious attack against password integrity. When the AAA commands that support type 6 are configured with either type 0 or type 7 encryption option, warning messages are displayed.

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 | <ul style="list-style-type: none"> • 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 | <i>Authentication, Authorization, and Accounting Configuration Guide</i> |

Technical Assistance

| Description | Link |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | http://www.cisco.com/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 38: Feature Information for Secure Reversible Passwords for AAA

| Feature Name | Releases | Feature Information |
|-------------------------------------|----------|--|
| Secure Reversible Passwords for AAA | 15.4(1)T | <p>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.</p> <p>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 tacacs-server key.</p> |