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

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Cisco and the Cisco logo are trademarks 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. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012 Cisco Systems, Inc. All rights reserved.
CONTENTS

Configuring Authentication 1
  Finding Feature Information 1
  Prerequisites for Configuring Authentication 1
  Restrictions for Configuring Authentication 1
  Information About Configuring Authentication 2
    Named Method Lists for Authentication 2
      Method Lists and Server Groups 2
      Method List Examples 3
    RADIUS Change of Authorization 4
      Change-of-Authorization Requests 5
        RFC 5176 Compliance 5
        CoA Request Response Code 6
          Session Identification 6
          CoA ACK Response Code 7
          CoA NAK Response Code 7
        CoA Request Commands 7
          Session Reauthentication 8
          Session Termination 8
          CoA Request Disable Host Port 8
          CoA Request Bounce-Port 9
        Domain Stripping 9
      How to Configure AAA Authentication Methods 10
        Configuring Login Authentication Using AAA 10
          Login Authentication Using Enable Password 12
          Login Authentication Using Kerberos 13
          Login Authentication Using Line Password 13
          Login Authentication Using Local Password 13
          Login Authentication Using Group RADIUS 14
        Configuring RADIUS Attribute 8 in Access Requests 14
Contents

How Double Authentication Works 30
Configuring Double Authentication 31
Accessing the User Profile After Double Authentication 32
Enabling Automated Double Authentication 33
Configuring Automated Double Authentication 34
Troubleshooting Automated Double Authentication 35
Configuring the Dynamic Authorization Service for RADIUS CoA 35
Configuring the Router 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 41
Enabling CHAP or PAP Authentication 42
   Enabling PPP Encapsulation 43
   Enabling PAP or CHAP 43
Inbound and Outbound Authentication 44
   Enabling Outbound PAP Authentication 45
   Refusing PAP Authentication Requests 45
Creating a Common CHAP Password 45
   Refusing CHAP Authentication Requests 45
   Delaying CHAP Authentication Until Peer Authenticates 46
Using MS-CHAP 46
   Defining PPP Authentication using MS-CHAP 47
Authentication Examples 48
   RADIUS Authentication Examples 48
   TACACS Authentication Examples 49
   Kerberos Authentication Examples 50
AAA Scalability Example 50
Login and Failed Banner Examples 52
AAA Packet of Disconnect Server Key Example 52
Double Authentication Examples 52
   Configuration of the Local Host for AAA with Double Authentication Examples 53
   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 54
Complete Configuration with TACACS Example 54
Automated Double Authentication Example 57
Additional References 59
Feature Information for Configuring Authentication 60
AAA Double Authentication Secured by Absolute Timeout 67
Finding Feature Information 67
Prerequisites for AAA Double Authentication Secured by Absolute Timeout 67
Restrictions for AAA Double Authentication Secured by Absolute Timeout 68
Information About AAA Double Authentication Secured by Absolute Timeout 68
AAA Double Authentication 68
How to Apply AAA Double Authentication Secured by Absolute Timeout 68
Applying AAA Double Authentication Secured by Absolute Timeout 68
Verifying AAA Double Authentication Secured by Absolute Timeout 69
Examples for AAA Double Authentication Secured by Absolute Timeout 72
RADIUS User Profile Example 72
TACACS User Profile Example 72
Additional References 74
Related Documents 75
Standards 75
MIBs 75
RFCs 75
Technical Assistance 76
Feature Information for AAA Double Authentication Secured by Absolute Timeout 76
Throttling of AAA RADIUS Records 79
Finding Feature Information 79
Information About Throttling of AAA RADIUS Records 79
Benefits of the Throttling of AAA RADIUS Records Feature 79
Throttling Access Requests and Accounting Records 80
How to Configure Throttling of AAA RADIUS Records 80
Throttling Accounting and Access Request Packets Globally 80
Throttling Accounting and Access Request Packets Per Server Group 81
Configuration Examples for Throttling of AAA RADIUS Records 83
Throttling Accounting and Access Request Packets Globally Example 83
Contents

Throttling Accounting and Access Request Packets Per Server Group Example 83
Additional References 84
Feature Information for Throttling of AAA RADIUS Records 85

RADIUS Packet of Disconnect 87
Finding Feature Information 87
Prerequisites for RADIUS Packet of Disconnect 87
Restrictions for RADIUS Packet of Disconnect 87
Information About RADIUS Packet of Disconnect 88
  When the POD is Needed 88
  POD Parameters 88
How to Configure the RADIUS Packet of Disconnect 88
  Configuring the RADIUS POD 89
    Troubleshooting Tips 91
    Verifying the RADIUS POD Configuration 92
Additional References 92
Feature Information for RADIUS Packet of Disconnect 94
Glossary 94

AAA Authorization and Authentication Cache 97
Finding Feature Information 97
Prerequisites for Implementing Authorization and Authentication Profile Caching 97
Information About Implementing Authorization and Authentication Profile Caching 98
  Network Performance Optimization Using Authorization and Authentication Profile Caching 98
  Authorization and Authentication Profile Caching as a Failover Mechanism 98
  Method Lists in Authorization and Authentication Profile Caching 99
  Authorization and Authentication Profile Caching Guidelines 99
  General Configuration Procedure for Implementing Authorization and Authentication Profile Caching 99
How to Implement Authorization and Authentication Profile Caching 100
  Creating Cache Profile Groups and Defining Caching Rules 100
  Defining RADIUS and TACACS Server Groups That Use Cache Profile Group Information 102
  Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used 104
Configuration Examples for Implementing Authorization and Authentication Profile Caching 106
  Implementing Authorization and Authentication Profile Caching for Network Optimization Example 106
AAA Accounting Types 132
   Network Accounting 132
   EXEC Accounting 134
   Command Accounting 135
   Connection Accounting 136
   System Accounting 138
   Resource Accounting 138
      AAA Resource Failure Stop Accounting 138
      AAA Resource Accounting for Start-Stop Records 140
AAA Accounting Enhancements 140
   AAA Broadcast Accounting 140
   AAA Session MIB 141
Accounting Attribute-Value Pairs 142
How to Configure AAA Accounting 142
   Configuring AAA Accounting Using Named Method Lists 142
   Suppressing Generation of Accounting Records for Null Username Sessions 144
   Generating Interim Accounting Records 144
   Configuring an Alternate Method to Enable Periodic Accounting Records 144
   Generating Interim Service Accounting Records 146
   Generating Accounting Records for a Failed Login or Session 146
   Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records 147
   Suppressing System Accounting Records over Switchover 147
   Configuring AAA Resource Failure Stop Accounting 147
   Configuring AAA Resource Accounting for Start-Stop Records 148
   Configuring AAA Broadcast Accounting 148
   Configuring per-DNIS AAA Broadcast Accounting 149
   Configuring the AAA Session MIB 149
   Establishing a Session with a Router if the AAA Server Is Unreachable 150
   Monitoring Accounting 150
   Troubleshooting Accounting 150
Configuration Examples for AAA Accounting 150
   Configuring a Named Method List Example 151
   Configuring AAA Resource Accounting Example 152
   Configuring AAA Broadcast Accounting Example 153
   Configuring per-DNIS AAA Broadcast Accounting Example 153
Configuring Authorization for Per VRF AAA with Local Customer Templates 181
Configuring Local Customer Templates 182
Configuring Per VRF AAA Using Remote Customer Templates 184
Configuring AAA 184
Configuring Server Groups 184
Configuring Authentication for Per VRF AAA with Remote Customer Profiles 184
Configuring Authorization for Per VRF AAA with Remote Customer Profiles 185
Configuring the RADIUS Profile on the SP RADIUS Server 186
Verifying VRF Routing Configurations 186
Troubleshooting Per VRF AAA Configurations 187
Configuration Examples for Per VRF AAA 187
Per VRF Configuration Examples 188
Per VRF AAA Example 188
Per VRF AAA Using a Locally Defined Customer Template Example 188
Per VRF AAA Using a Remote RADIUS Customer Template Example 188
Customer Template Examples 189
Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example 189
Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example 190
AAA Accounting Stop Record Examples 191
AAA Accounting Stop Record and Rejected Call Example 191
AAA Accounting Stop Record and Successful Call Example 193
Additional References 195
Feature Information for Per VRF AAA 196
Glossary 198
Configuring Authentication

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

- Finding Feature Information, page 1
- Prerequisites for Configuring Authentication, page 1
- Restrictions for Configuring Authentication, page 1
- Information About Configuring Authentication, page 2
- How to Configure AAA Authentication Methods, page 10
- Non-AAA Authentication Methods, page 39
- Authentication Examples, page 48
- Additional References, page 59
- Feature Information for Configuring Authentication, page 60

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Configuring 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.
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, and how AAA authentication is handled through RADIUS Change in Authorization (CoA):

- Named Method Lists for Authentication, page 2
- RADIUS Change of Authorization, page 4
- Domain Stripping, page 9

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, page 2
- Method List Examples, page 3

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
```

**RADIUS Change of Authorization**

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

Beginning with Cisco IOS Release 12.2(5) SXI, per-session CoA requests are supported in:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Security and Password--see the Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices feature module for more information.
- Accounting--see the Configuring Accounting feature module for more information.

This section describes how RADIUS CoA messaging works:

- Change-of-Authorization Requests, page 5
- CoA Request Response Code, page 6
- CoA Request Commands, page 7

**Change-of-Authorization Requests**

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

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

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

- RFC 5176 Compliance, page 5

**RFC 5176 Compliance**

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

The table below shows the IETF attributes that are supported for this feature.

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>101</td>
<td>Error-Cause</td>
</tr>
</tbody>
</table>

The table below shows the possible values for the Error-Cause attribute.
<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual Session Context Removed</td>
</tr>
<tr>
<td>202</td>
<td>Invalid EAP Packet (Ignored)</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported Attribute</td>
</tr>
<tr>
<td>402</td>
<td>Missing Attribute</td>
</tr>
<tr>
<td>403</td>
<td>NAS Identification Mismatch</td>
</tr>
<tr>
<td>404</td>
<td>Invalid Request</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported Service</td>
</tr>
<tr>
<td>406</td>
<td>Unsupported Extension</td>
</tr>
<tr>
<td>407</td>
<td>Invalid Attribute Value</td>
</tr>
<tr>
<td>501</td>
<td>Administratively Prohibited</td>
</tr>
<tr>
<td>502</td>
<td>Request Not Routable (Proxy)</td>
</tr>
<tr>
<td>503</td>
<td>Session Context Not Found</td>
</tr>
<tr>
<td>504</td>
<td>Session Context Not Removable</td>
</tr>
<tr>
<td>505</td>
<td>Other Proxy Processing Error</td>
</tr>
<tr>
<td>506</td>
<td>Resources Unavailable</td>
</tr>
<tr>
<td>507</td>
<td>Request Initiated</td>
</tr>
<tr>
<td>508</td>
<td>Multiple Session Selection Unsupported</td>
</tr>
</tbody>
</table>

**CoA Request Response Code**

The CoA Request response code can be used to issue a command to the router. The supported commands are listed in the CoA Request Commands section.

- Session Identification, page 6
- CoA ACK Response Code, page 7
- CoA NAK Response Code, page 7

**Session Identification**

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

- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- Audit-Session-Id (Cisco VSA)
- Acct-Session-Id (IETF attribute #44)
Unless all session identification attributes included in the CoA message match the session, the router returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

For disconnect and CoA requests targeted to a particular session, any one of the following session identifiers can be used:

- Calling-Station-ID (IETF attribute #31, which contains the MAC address)
- Audit-Session-ID (Cisco vendor-specific attribute)
- Accounting-Session-ID (IETF attribute #44).

If more than one session identification attribute is included in the message, all of the attributes must match the session or the router returns a Disconnect- negative acknowledgement (NAK) or CoA-NAK with the error code “Invalid Attribute Value.”

**CoA ACK Response Code**

If the authorization state is changed successfully, a positive acknowledgement (ACK) is sent. The attributes returned within CoA ACK vary based on the CoA Request and are discussed in individual CoA Commands.

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

```
+----------------------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+----------------------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
+----------------------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...              |
+----------------------------------+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The attributes field is used to carry Cisco VSAs.

**CoA NAK Response Code**

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

**CoA Request Commands**

The router supports the commands shown in the table below.

<table>
<thead>
<tr>
<th>Command1</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthenticate host</td>
<td>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</td>
</tr>
</tbody>
</table>

1 All CoA commands must include the session identifier between the router and the CoA client.
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate session</td>
<td>This is a standard disconnect request that does not require a VSA</td>
</tr>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</td>
</tr>
</tbody>
</table>

- Session Reauthentication, page 8
- Session Termination, page 8
- CoA Request Disable Host Port, page 8
- CoA Request Bounce-Port, page 9

### Session Reauthentication

To initiate session authentication, the AAA server sends a standard CoA-Request message that contains a Cisco vendor-specific attribute (VSA) in this form: `Cisco:Avpair="subscriber:command=reauthenticate"` and one or more session identification attributes.

The current session state determines the router response to the message in the following scenarios:

- If the session is currently authenticated by IEEE 802.1x, the router responds by sending an EAPoL­ RequestId message (see footnote below) to the server.
- If the session is currently authenticated by MAC authentication bypass (MAB), the router 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 router receives the command, the router terminates the process and restarts the authentication sequence, starting with the method configured to be attempted first.

### Session Termination

A CoA Disconnect-Request command terminates the session without disabling the host port. This command causes re-initialization 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 router returns a Disconnect-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the router terminates the session. After the session has been completely removed, the router returns a Disconnect-ACK.

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 be causing problems on the network and network access needs to be immediately blocked for the host. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

### CoA Request Disable Host Port

---

1. All CoA commands must include the session identifier between the router and the CoA client.
2. Extensible Authentication Protocol over LAN
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 carried in a standard CoA-Request message that has this new 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. If the router cannot locate the session, it returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the router locates the session, it disables the hosting port and returns a CoA-ACK message.

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

If the RADIUS server CoA disable port command needs to be ignored, see Configuring the Router to Ignore Bounce and Disable RADIUS CoA Requests for more information.

### CoA Request Bounce-Port

A RADIUS server CoA bounce port command 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 command is carried in a standard CoA-Request message that contains the following new 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 router returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the router disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the RADIUS server CoA bounce port command needs to be ignored, see Configuring the Router to Ignore Bounce and Disable RADIUS CoA Requests for more information.

### Domain Stripping

You can remove the domain name from the username received at the global level. This can be done using the `radius-server domain-stripping` command. When the `radius-server domain-stripping` command is configured, all the authentication, authorization and accounting (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. That is, if domain stripping is not enabled globally, but it is enabled in a server group, it is enabled only for that server group. Also, if Virtual
Forwarding and Routing (VRF)-specific domain stripping is configured globally and in a server group for different VRFs, domain stripping is enabled in both the VRFs. VRF configurations are taken from server-group configuration mode. If the server-group configurations are disabled in global configuration mode, but they are available in server-group configuration mode, all configurations in server-group configuration mode are applicable.

Once 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, page 10
- Configuring PPP Authentication Using AAA, page 15
- Configuring AAA Scalability for PPP Requests, page 18
- Configuring ARAP Authentication Using AAA, page 19
- Configuring NASI Authentication Using AAA, page 22
- Specifying the Amount of Time for Login Input, page 26
- Enabling Password Protection at the Privileged Level, page 26
- Changing the Text Displayed at the Password Prompt, page 27
- Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server, page 27
- Configuring Message Banners for AAA Authentication, page 28
- Configuring AAA Packet of Disconnect, page 29
- Enabling Double Authentication, page 30
- Enabling Automated Double Authentication, page 33
- Configuring the Dynamic Authorization Service for RADIUS CoA, page 35
- Configuring the Router to Ignore Bounce and Disable RADIUS CoA Requests, page 37
- Configuring Domain Stripping at the Server Group Level, page 38

### Configuring Login Authentication UsingAAA

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router(config)# aaa new-model</td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td>Step 2 Router(config)# aaa authentication login{default</td>
<td>list-name} method1[method2...]</td>
</tr>
<tr>
<td>Step 3 Router(config)# line [aux</td>
<td>console</td>
</tr>
<tr>
<td>Step 4 Router(config-line)# login authentication</td>
<td>Applies the authentication list to a line or set of lines.</td>
</tr>
</tbody>
</table>

Example:

(login authentication methods)

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>krb5</td>
<td>Uses Kerberos 5 for authentication.</td>
</tr>
<tr>
<td>krb5-telnet</td>
<td>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.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.</td>
</tr>
</tbody>
</table>

**Note**

The `login` command only changes username and privilege level but does not execute a shell; therefore autocmds will not be executed. To execute autocmds 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 autocmds this way.

- Login Authentication Using Enable Password, page 12
- Login Authentication Using Kerberos, page 13
- Login Authentication Using Line Password, page 13
- Login Authentication Using Local Password, page 13
- Login Authentication Using Group RADIUS, page 14
- Configuring RADIUS Attribute 8 in Access Requests, page 14
- Login Authentication Using Group TACACS, page 14
- Login Authentication Using group group-name, page 14
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

Once 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 a NAS to provide the RADIUS server with a hint of the user IP address in advance of 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>Router(config)# aaa new-model</code></td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td><strong>Step 2</strong> `Router(config)# aaa authentication ppp {default</td>
<td>list-name} method1[</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>Router(config)# interface interface-type interface-number</code></td>
<td>Enters interface configuration mode for the interface to which you want to apply the authentication list.</td>
</tr>
<tr>
<td><strong>Step 4</strong> `Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] {default</td>
<td>list-name} [callin] [one-time][optional]`</td>
</tr>
</tbody>
</table>

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

• PPP Authentication Using Kerberos, page 16
• PPP Authentication Using Local Password, page 17
• PPP Authentication Using Group RADIUS, page 17
• Configuring RADIUS Attribute 44 in Access Requests, page 17
• PPP Authentication Using Group TACACS, page 17
• PPP Authentication Using group group-name, page 18
Use the `aaa authentication ppp` command with the `krb5` 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:

```plaintext
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:

```plaintext
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:

```plaintext
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**

Once 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 router 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 of the call to the end of the call. For more information on attribute 44, refer to the appendix “RADIUS Attributes” at the end of the book.

---

**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:

```
Router(config)# aaa processes number
```

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.
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

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

Use the following commands starting in global configuration mode:

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router(config)# aaa new-model</td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td>Step 2 Router(config)# aaa authentication arap</td>
<td>Enables authentication for ARAP users.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>{default</td>
<td>list-name} method1 {method2...}</td>
</tr>
<tr>
<td>Step 3 Router(config)# line number</td>
<td>(Optional) Changes to line configuration mode.</td>
</tr>
<tr>
<td>Step 4 Router(config-line)# autoselect arap</td>
<td>(Optional) Enables autoselection of ARAP.</td>
</tr>
<tr>
<td>Step 5 Router(config-line)# autoselect during-login</td>
<td>(Optional) Starts the ARAP session automatically at user login.</td>
</tr>
<tr>
<td>Step 6 Router(config-line)# arap authentication list-name</td>
<td>(Optional--not needed if default is used in the <strong>aaa authentication arap</strong> command) Enables TACACS+ authentication for ARAP on a line.</td>
</tr>
</tbody>
</table>

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 be used 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 authenticate successfully, it should be used as a backup method of authentication.

The following table lists the supported login authentication methods.

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

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

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

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

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

This section includes the following sections:

- ARAP Authentication Allowing Authorized Guest Logins, page 21
- ARAP Authentication Allowing Guest Logins, page 21
- ARAP Authentication Using Line Password, page 21
- ARAP Authentication Using Local Password, page 21
- ARAP Authentication Using Group RADIUS, page 21
- ARAP Authentication Using Group TACACS, page 22
- ARAP Authentication Using Group group-name, page 22
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

With the `aaa authentication nasi` command, you create one or more lists of authentication methods that are tried when NetWare Asynchronous Services Interface (NASI) users attempt to log in to the router. 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. Router(config)# aaa new-model
2. Router(config)# aaa authentication nasi
3. Router(config)# line number
4. Router(config-line)# nasi authentication list-name

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config)# aaa new-model</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# aaa authentication nasi</td>
</tr>
<tr>
<td>Example:</td>
<td>{default</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config)# line number</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-line)# nasi authentication list-name</td>
</tr>
</tbody>
</table>

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 **aaa authentication nasi** command, use the **default** keyword followed by the methods you want to be used 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 authenticate successfully, it should be used as a backup method of authentication.

The table below lists the supported NASI authentication methods.

**Table 7**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.</td>
</tr>
</tbody>
</table>

- NASI Authentication Using Enable Password, page 24
- NASI Authentication Using Line Password, page 24
- NASI Authentication Using Local Password, page 24
- NASI Authentication Using Group RADIUS, page 25
- NASI Authentication Using Group TACACS, page 25
- NASI Authentication Using group group-name, page 25

**NASI Authentication Using Enable Password**

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

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

Before you can use TACACS+ as the method of user authentication, you need to enable communication with the TACACS+ 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 nasi` command with the `group group-name` method to specify a subset of RADIUS or TACACS+ servers to use as the NASI authentication method. To 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 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout login response seconds</code></td>
<td>Specifies how long the system will wait for login information before timing out.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authentication enable default method1 [method2...]</code></td>
<td>Enables user ID and password checking for users requesting privileged EXEC level.</td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td><code>group radius</code></td>
<td>Uses the list of all RADIUS hosts for authentication.</td>
</tr>
</tbody>
</table>

**Note**

The RADIUS method does not work on a per-username basis.
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ hosts for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config)# aaa authentication password-prompt text-string</code></td>
<td>Changes the default text displayed when a user is prompted to enter a password.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa authentication suppress null-username</td>
<td>Prevents an Access Request with a blank username from being sent to the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa authentication suppress null-username</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Message Banners for AAA Authentication**

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that 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, page 28
- Configuring a Failed-Login Banner, page 29

**Configuring a Login Banner**

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

To configure a banner that will be displayed whenever a user logs in (replacing the default message for login), use the following commands in global configuration mode:

**SUMMARY STEPS**

1. `Router(config)# aaa new-model`
2. `Router(config)# aaa authentication banner delimiter string delimiter`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  
 `Router(config)# aaa new-model` | Enables AAA. |
| Step 2  
 `Router(config)# aaa authentication banner delimiter string delimiter` | Creates a personalized login banner. |

The maximum number of characters that can be displayed in the login banner is 2996 characters.

### Configuring a Failed-Login Banner

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

To configure a message that will be displayed whenever a user fails login (replacing the default message for failed login), use the following commands in global configuration mode:

**SUMMARY STEPS**

1. `Router(config)# aaa new-model`
2. `Router(config)# aaa authentication fail-message delimiter string delimiter`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  
 `Router(config)# aaa new-model` | Enables AAA. |
| Step 2  
 `Router(config)# aaa authentication fail-message delimiter string delimiter` | Creates a message to be displayed when a user fails login. |

The maximum number of characters that can be displayed in the failed-login banner is 2996 characters.

### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router(config)# aaa accounting network default</td>
<td>Enables AAA accounting records.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>( \text{start-stop radius} )</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Router(config)# aaa accounting delay-start</td>
<td>(Optional) Delays generation of the start accounting record until the Framed-IP-Address is assigned, allowing its use in the POD packet.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config)# aaa pod server server-keystring</td>
<td>Enables POD reception.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router(config)# radius-server host IP address non-standard</td>
<td>Declares a RADIUS host that uses a vendor-proprietary version of RADIUS.</td>
</tr>
</tbody>
</table>

**Enabling Double Authentication**

Previously, PPP sessions could only be authenticated 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, page 30
- Configuring Double Authentication, page 31
- Accessing the User Profile After Double Authentication, page 32

**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:
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 *CiscoIOS 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, page 34

• Troubleshooting Automated Double Authentication, page 35

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router(config)# ip trigger-authentication</td>
<td>Enables automation of double authentication.</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
timeout seconds [port number]
```
Command or Action | Purpose
--- | ---
**Step 2** | Do one of the following:
- Router(config)# interface bri number
-  
- Router(config)# interface serial number :23

**Step 3** | Router(config-if)# ip trigger-authentication

Selects an ISDN BRI or ISDN PRI interface and enter the interface configuration mode.

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# aaa new-model</td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa server radius dynamic-author</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# aaa server radius dynamic-author</td>
</tr>
<tr>
<td><strong>Step 5</strong> client {ip_addr</td>
<td>hostname} [server-key [0</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-locsvr-da-radius)#client 192.168.0.5 server-key cisco1</td>
</tr>
</tbody>
</table>

Note: Configuring the server key at the client level overrides the server key configured at the global level.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> domain [delimiter <em>character</em>] stripping [right-to-left]]</td>
<td>(Optional) Configures username domain options for the RADIUS application.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-locsvr-da-radius)# domain stripping right-to-left</td>
<td>• The <strong>delimiter</strong> keyword specifies the domain delimiter. One of the following options can be specified for the <em>character</em> argument: @, /, $, %, , # or -</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-locsvr-da-radius)# domain delimiter @</td>
<td>• The <strong>stripping</strong> keyword compares the incoming username with the names oriented to the left of the @ domain delimiter.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>right-to-left</strong> keyword terminates the string at the first delimiter going from right to left.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7 port <em>port-num</em></th>
<th>Configures UDP port 3799 for CoA requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-locsvr-da-radius)# port 3799</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring the Router to Ignore Bounce and Disable RADIUS CoA Requests**

Use the following procedure to configure the router to ignore RADIUS server CoA requests in the form of a bounce port command or disable port command.

When an authentication port is authenticated with multiple hosts and there is a 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. This can trigger a DHCP renegotiation from one or more hosts in the case of a flap, or the administratively shut down the authentication port hosting the session for one or more hosts, which may be undesirable.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa new-model
4. authentication command bounce-port ignore
5. authentication command disable-port ignore
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | 
Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | 
Router# configure terminal |
| **Step 3** aaa new-model | Enables AAA. |
| **Example:** | 
Router(config)# aaa new-model |
| **Step 4** authentication command bounce-port ignore | (Optional) Configures the router 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. |
| **Example:** | 
Router(config)# authentication command bounce-port ignore |
| **Step 5** authentication command disable-port ignore | (Optional) Configures the router to ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions. The shutting down of the port leads to session termination. |
| **Example:** | 
Router(config)# authentication command disable-port ignore |

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal |
| **Step 3** aaa group server radius server-name | Adds the RADIUS server and enters server group RADIUS configuration mode.  
  • The `server-name` argument specifies the RADIUS server group name. |
| **Example:** Router(config)# aaa group server radius rad1 |
| **Step 4** domain-stripping [strip-suffix word] [right-to-left] [prefix-delimiter word] [delimiter word] | Configures domain stripping at the server group level. |
| **Example:** Router(config-sg-radius)# domain-stripping delimiter username@example.com |
| **Step 5** end | Exits server group RADIUS configuration mode and returns to privileged EXEC mode. |
| **Example:** Router(config-sg-radius)# end |

## Non-AAA Authentication Methods

- Configuring Line Password Protection, page 39  
- Establishing Username Authentication, page 41  
- Enabling CHAP or PAP Authentication, page 42  
- Using MS-CHAP, page 46

## 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.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:**       |         |
| Router> enable     |         |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**       |         |
| Router# configure terminal |         |
| **Step 3** line [aux | console | tty | vty] line-number [ending-line-number] | Enters line configuration mode. |
| **Example:**       |         |
| Router(config)# line console 0 |         |
| **Step 4** password password | 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. |
| **Example:**       |         |
| Router(config-line)# secret word |         |
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Do one of the following:</td>
<td>Establishes username authentication with encrypted passwords.</td>
</tr>
<tr>
<td>• Router(config)# username name [nopassword</td>
<td>password password</td>
</tr>
<tr>
<td>• Router(config)# username name [access-class number]</td>
<td>(Optional) Establishes username authentication by access list.</td>
</tr>
</tbody>
</table>
## Command or Action

**Step 2**  
```
Router(config)# username name [privilege level]
```
(Optional) Sets the privilege level for the user.

**Step 3**  
```
Router(config)# username name [autocommand command]
```
(Optional) Specifies a command to be executed automatically.

**Step 4**  
```
Router(config)# username name [noescape] [nohangup]
```
(Optional) Sets a “no escape” login environment.

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, page 43
   - Enabling PAP or CHAP, page 43
   - Inbound and Outbound Authentication, page 44
   - Enabling Outbound PAP Authentication, page 45
   - Refusing PAP Authentication Requests, page 45
   - Creating a Common CHAP Password, page 45
   - Refusing CHAP Authentication Requests, page 45
   - Delaying CHAP Authentication Until Peer Authenticates, page 46

### Enabling PPP Encapsulation

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config-if)# encapsulation ppp</code></td>
<td>Enables PPP on an interface.</td>
</tr>
</tbody>
</table>

### 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:
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.

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`, page 41.

### Inbound and Outbound Authentication

PPP supports two-way authentication. Normally, when a remote device dials into 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# <code>ppp pap sent-username username password password</code></td>
<td>Enables outbound PAP authentication.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# <code>ppp pap refuse</code></td>
<td>Refuses PAP authentication from peers requesting PAP authentication.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# <code>ppp chap password secret</code></td>
<td>Enables a router calling a collection of routers to configure a common CHAP secret password.</td>
</tr>
</tbody>
</table>

### 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:
Delivering CHAP Authentication Until Peer Authenticates

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# ppp chap refuse [callin]</td>
<td>Refuses CHAP authentication from peers requesting CHAP authentication.</td>
</tr>
</tbody>
</table>

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.

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 router 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

<table>
<thead>
<tr>
<th>Vendor-ID Number</th>
<th>Vendor-Type Number</th>
<th>Vendor-Proprietary Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>311</td>
<td>11</td>
<td>MSCHAP-Challenge</td>
<td>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.</td>
</tr>
<tr>
<td>211</td>
<td>11</td>
<td>MSCHAP-Response</td>
<td>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.</td>
</tr>
</tbody>
</table>

• Defining PPP Authentication using MS-CHAP, page 47

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enables PPP encapsulation.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Defines PPP authentication using MS-CHAP.</td>
</tr>
</tbody>
</table>

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, page 48
- TACACS Authentication Examples, page 49
- Kerberos Authentication Examples, page 50
- AAA Scalability Example, page 50
- Login and Failed Banner Examples, page 52
- AAA Packet of Disconnect Server Key Example, page 52
- Double Authentication Examples, page 52
- Automated Double Authentication Example, page 57

### 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:

```plaintext
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 10.1.2.3
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 10.1.2.3.
- 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 dialins` command applies the “dialins” method list to the specified interfaces.
Login and Failed Banner Examples

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

```
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized Access Prohibited
Username:
```

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

```
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

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

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 172.16.0.0 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, page 53
These two examples show how to configure a local host to use AAA for PPP and login authentication, and for network and EXEC authorization. One example is shown for RADIUS and one example for TACACS+.

In both 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 router configuration with a RADIUS AAA server:

```plaintext
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 router configuration with a TACACS+ server:

```plaintext
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+
```

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:

```plaintext
hostx   Password = ªwelcomeº
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = ªlcp:interface-config-ip unnumbered fastethernet 0º,
cisco-avpair = ªip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnetº,
cisco-avpair = ªip:inacl#4=deny icmp any anyº,
cisco-avpair = ªip:route#5=10.0.0.0 255.0.0.0º,
cisco-avpair = ªip:route#6=10.10.0.0 255.0.0.0º,
cisco-avpair = ªipx:inacl#3=deny anyº
```
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.”

```plaintext
key = ªmytacacskeyº  
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 ªwelcomeº  
  chap = cleartext ªwelcomeº  
  service = exec  
  {  
    # This is the autocommand that executes when pat_default logs in.  
    interface-config=ºip unnumbered fastethernet 0º  
  }  
  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=ºpermit tcp any 172.21.114.0 0.0.0.255 eq telnetº  
    inacl#4=ºdeny icmp any anyº  
    route#5=º10.0.0.0 255.0.0.0º  
    route#6=º10.10.0.0 255.0.0.0º  
  }  
  service = ppp protocol = ipx {  
    # see previous comment about the hash sign and string, in protocol = ip  
    inacl#3=ºdeny anyº  
  }  
}  
#------------------- ªaccess-profileº default user ªonly aclsº ------------------  
# 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 ªwelcomeº  
  chap = cleartext ªwelcomeº  
  service = exec  
  {  
    # This is the autocommand that executes when pat_default logs in.  
  }  
}
```
autcmt = "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)!
    inacli#3="permit tcp any host 10.0.0.2 eq telnet"
    inacli#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.
#--------------------- "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_merge {
    login = cleartext "welcome"
    chap = cleartext "welcome"
    service = exec {
        # This is the autocmd that executes when pat_merge logs in.
        autcmt = "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)!
        inacli#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)!
    }
}

user = pat_replace {
    login = cleartext "welcome"

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
```

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 (**).
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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security commands</td>
<td><em>Cisco IOS Security Command Reference</em></td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1334</td>
<td>PPP Authentication Protocols</td>
</tr>
<tr>
<td>RFC 2433</td>
<td>Microsoft PPP CHAP Extensions</td>
</tr>
<tr>
<td>RFC 2903</td>
<td>Generic AAA Architecture</td>
</tr>
<tr>
<td>RFC 2904</td>
<td>AAA Authorization Framework</td>
</tr>
<tr>
<td>RFC 2906</td>
<td>AAA Authorization Requirements</td>
</tr>
<tr>
<td>RFC 2989</td>
<td>Criteria for Evaluating AAA Protocols for Network Access</td>
</tr>
</tbody>
</table>

Technical Assistance

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

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Method Lists Enhancement</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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. 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 or modified: <code>aaa authentication ppp</code>.</td>
</tr>
<tr>
<td>AAA Per-User Scalability</td>
<td>Cisco IOS XE Release 2.3</td>
<td>The AAA Per-User Scalability feature supports two RADIUS VSAs for <code>ip vrf</code> and <code>ip unnumbered</code> commands and creates subvirtual access interfaces if specified instead of full VA interface to achieve higher scalability. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Challege Handshake Authentication Protocol (CHAP)</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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: <code>ppp authentication</code>, <code>ppp chap password</code>, <code>ppp chap refuse</code>.</td>
</tr>
</tbody>
</table>
| Domain Stripping at the Server Group Level       | Cisco IOS XE Release 3.4S         | The Domain Stripping feature allows domain stripping to be configured at the server group level. Per-server group configuration overrides the global configuration. The following sections provide information about this feature:  
  - Domain Stripping, page 9  
  - Configuring Domain Stripping at the Server Group Level, page 38  
  The following command was introduced: `domain-stripping`. |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double Authentication</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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: aaa authentication, aaa authorization, access-profile.</td>
</tr>
<tr>
<td>Message Banners for AAA</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>MS-CHAP Version 1</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Password Authentication Protocol (PAP)</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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: <code>ppp authentication</code>, <code>ppp pap sent-username</code>, <code>ppp pap refuse</code>.</td>
</tr>
<tr>
<td>RADIUS—CLI to Prevent Sending of Access Request with a Blank Username</td>
<td>Cisco IOS XE Release 2.4</td>
<td>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: <code>aaa authentication suppress null-username</code>.</td>
</tr>
</tbody>
</table>
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.
AAA Double Authentication Secured by Absolute Timeout

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

• Finding Feature Information, page 67
• Prerequisites for AAA Double Authentication Secured by Absolute Timeout, page 67
• Restrictions for AAA Double Authentication Secured by Absolute Timeout, page 68
• Information About AAA Double Authentication Secured by Absolute Timeout, page 68
• How to Apply AAA Double Authentication Secured by Absolute Timeout, page 68
• Examples for AAA Double Authentication Secured by Absolute Timeout, page 72
• Additional References, page 74
• Feature Information for AAA Double Authentication Secured by Absolute Timeout, page 76

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for 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).
• You should be familiar with enabling AAA automated double authentication.
Restrictions for AAA Double Authentication Secured by Absolute Timeout

- The AAA Double Authentication Secured by Absolute Timeout feature, like the existing double authentication 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, page 68

AAA Double Authentication

With the current AAA double authentication mechanism, a user must pass the first authentication using a host username and password. The second authentication, after Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), uses a login username and password. In the first authentication, a PPP session timeout will be 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 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, page 68
- Verifying AAA Double Authentication Secured by Absolute Timeout, page 69

Applying AAA Double Authentication Secured by Absolute Timeout

To apply the absolute timeout, you need to configure “Session-Timeout” in the login user profile as a link control protocol (LCP) per-user attribute. There is no new or modified command-line interface (CLI) for this feature, but before you use the access-profile command when enabling AAA double authentication, 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 Example for AAA Double Authentication Secured by Absolute Timeout.
Timeout configuration in a TACACS+ user profile is a little 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 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 is not available while doing an EXEC authorization--and the timeout will not be applied to the EXEC session.

Verifying AAA Double Authentication Secured by Absolute Timeout

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

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

```
or

depug tacacs
```

**SUMMARY STEPS**

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

**DETAILED STEPS**

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

```
Example:

Router> enable
```

Verifying AAA Double Authentication Secured by Absolute Timeout

How to Apply AAA Double Authentication Secured by Absolute Timeout

Authentication Authorization and Accounting Configuration Guide Cisco IOS XE Release 2
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> show users</td>
<td>Displays information about the active lines on the router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Step 3</strong> show interfaces virtual-access number [configuration]</td>
<td>Displays status, traffic data, and configuration information about a specified virtual access interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show interfaces virtual-access 2 configuration</td>
</tr>
<tr>
<td><strong>Step 4</strong> debug aaa authentication</td>
<td>Displays information about AAA TACACS+ authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug aaa authentication</td>
</tr>
<tr>
<td><strong>Step 5</strong> debug aaa authorization</td>
<td>Displays information about AAA TACACS+ authorization.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug aaa authorization</td>
</tr>
<tr>
<td><strong>Step 6</strong> debug aaa per-user</td>
<td>Displays the attributes that are applied to each user as the user authenticates.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug aaa per-user</td>
</tr>
<tr>
<td><strong>Step 7</strong> debug ppp authentication</td>
<td>Displays whether a user is passing authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug ppp authentication</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Do one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• debug radius</td>
</tr>
</tbody>
</table>

**Example:**

```
Router# debug radius
```

**Example:**

```
Example:
```

**Example:**

```
Example:
```

**Example:**

```
Example:
```

**Debug tacacs**

**Example:**

```
Router# debug tacacs
```

### Examples

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

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

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

```
Router# show interfaces virtual-access 2 configuration
Virtual-Access2 is a Virtual Profile (sub)interface
Derived configuration: 150 bytes
!
interface Virtual-Access2
 ip unnumbered Serial0:23
 no ip route-cache
 timeout absolute 3 0
 !
 ! The above line shows that the per-user session timeout has been applied.
 ppp authentication chap
 ppp timeout idle 180000
 ! The above line shows that the absolute timeout has been applied.
```
Examples for AAA Double Authentication Secured by Absolute Timeout

- RADIUS User Profile Example, page 72
- TACACS User Profile Example, page 72

RADIUS User Profile Example

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"
```

TACACS User Profile Example

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

The following allows the remote host to be authenticated by the local host during 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
```
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 = 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)!

access-profile Command with merge Keyword

With the "merge" option, all old access lists are removed (as before), but then almost any AV pair is allowed to be uploaded and installed. This merge will allow for the uploading of any custom static routes, Service Advertisement Protocol (SAP) filters, and other requirements that the user may need in his or her profile. This merge must be used 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 = 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)!
access-profile Command with the replace Keyword

If you use the `access-profile` command with the `replace` keyword, the command works as it does currently; that is, any old configuration is removed and any new configuration is installed.

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

```plaintext
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)!
```

Timeout configuration in a TACACS+ user profile is a little 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 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 is not available while doing an EXEC authorization--and the timeout will not be applied to the EXEC session.

Additional References

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

- Related Documents, page 75
- Standards, page 75
- MIBs, page 75
- RFCs, page 75
- Technical Assistance, page 76
## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
</tbody>
</table>

## Standards

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

## MIBs

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## RFCs

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>
Technical Assistance

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

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 11  Feature Information for AAA Double Authentication Secured by Absolute Timeout

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Double Authentication Secured by Absolute Timeout</td>
<td>Cisco IOS XE Release 2.3</td>
<td>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. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

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. (1110R)

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.
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 Cisco IOS XE router to the RADIUS server.

- Finding Feature Information, page 79
- Information About Throttling of AAA RADIUS Records, page 79
- How to Configure Throttling of AAA RADIUS Records, page 80
- Configuration Examples for Throttling of AAA RADIUS Records, page 83
- Additional References, page 84
- Feature Information for Throttling of AAA RADIUS Records, page 85

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Information About Throttling of AAA RADIUS Records

- Benefits of the Throttling of AAA RADIUS Records Feature, page 79
- Throttling Access Requests and Accounting Records, page 80

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 Cisco IOS XE 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, page 80
• Throttling Accounting and Access Request Packets Per Server Group, page 81

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. • Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 radius-server throttle { accounting threshold [access threshold [access-timeout number-of-timeouts]]}</td>
<td>Configures global throttling for accounting and access request packets. For this example: • The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. <strong>Note</strong> The default threshold value is 0 (throttling disabled). • The number of timeouts per transaction value (the range is 1-10) is set to 2.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# radius-server throttle accounting 100 access 200 access-timeout 2</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** aaa group server radius `server-group-name` | Enters server-group configuration mode. |
| **Example:** | Router(config)# aaa group server radius myservergroup |
| **Step 4** throttle `{[accounting threshold] [access threshold [access-timeout number-of-timeouts]]}` | Configures the specified server-group throttling values for accounting and access request packets.  
For this example:  
- The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200.  
**Note** The default threshold value is 0 (throttling disabled).  
- The number of time-outs per transaction value (the range is 1-10) is set to 2. |
| **Example:** | Router(config-sg-radius)# throttle accounting 100 access 200 access-timeout 2 |
| **Step 5** exit | Exits server-group configuration mode. |
| **Example:** | Router(config-sg-radius)# exit |
Configuration Examples for Throttling of AAA RADIUS Records

- Throttling Accounting and Access Request Packets Globally Example, page 83
- Throttling Accounting and Access Request Packets Per Server Group Example, page 83

## 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.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security features</td>
<td>Cisco IOS XE Security Configuration Guide:</td>
</tr>
<tr>
<td></td>
<td>Securing User Services, Release 2</td>
</tr>
<tr>
<td>Security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified</td>
<td>--</td>
</tr>
<tr>
<td>standards are</td>
<td>supported by this feature, and support for</td>
</tr>
<tr>
<td>supported by this</td>
<td>existing standards has not been modified by this</td>
</tr>
<tr>
<td>feature, and</td>
<td>feature.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified</td>
<td>To locate and download MIBs for selected platforms,</td>
</tr>
<tr>
<td>MIBs are supported</td>
<td>Cisco IOS XE software releases, and feature sets,</td>
</tr>
<tr>
<td>by this feature,</td>
<td>use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td>and support for</td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>existing MIBs has</td>
<td></td>
</tr>
<tr>
<td>not been modified</td>
<td></td>
</tr>
<tr>
<td>by this feature.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified</td>
<td>--</td>
</tr>
<tr>
<td>RFCs are supported</td>
<td></td>
</tr>
<tr>
<td>by this feature,</td>
<td>and support for existing RFCs has not been</td>
</tr>
<tr>
<td>and support for</td>
<td>modified by this feature.</td>
</tr>
<tr>
<td>existing RFCs has</td>
<td></td>
</tr>
<tr>
<td>not been modified</td>
<td></td>
</tr>
<tr>
<td>by this feature.</td>
<td></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 12  Feature Information for Throttling of AAA (RADIUS) Records

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throttling of AAA (RADIUS) Records</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: <code>radius-server throttle</code>, <code>throttle</code></td>
</tr>
</tbody>
</table>

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. (1110R)

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.
RADIUS Packet of Disconnect

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

- Finding Feature Information, page 87
- Prerequisites for RADIUS Packet of Disconnect, page 87
- Restrictions for RADIUS Packet of Disconnect, page 87
- Information About RADIUS Packet of Disconnect, page 88
- How to Configure the RADIUS Packet of Disconnect, page 88
- Additional References, page 92
- Feature Information for RADIUS Packet of Disconnect, page 94
- Glossary, page 94

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for RADIUS Packet of Disconnect


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, page 88
- POD Parameters, page 88

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, page 89
- Verifying the RADIUS POD Configuration, page 92
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

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

**Step 3**

```
Router (config)# aaa pod server [port port-number] [auth-type [any | all | session-key]] server-key [encryption-type] string
```

**Example:**

```
Router(config)# aaa pod server server-key xyz123
```

### Purpose

Enables inbound user sessions to be disconnected when specific session attributes are presented, where:

- **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.
  - **any** -- Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
  - **all** -- Only a session that matches all four key attributes is disconnected. All is the default.
  - **session-key** -- Session with a matching session-key attribute is disconnected. All other attributes are ignored.
- **server-key** -- Configures the shared-secret text string.
- **encryption-type** -- (Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco.
- **string** -- The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

### Step 4

```
Router# end
```

Exits global configuration mode and returns to privileged EXEC mode.
### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Router# show running-configuration</td>
<td>Verifies that the gateway is configured correctly in privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router# show running-configuration
```

**Example:**

```
! aaa authentication login h323 group radius
```

**Example:**

```
aaa authorization exec h323 group radius
```

**Example:**

```
aaa accounting update newinfo
```

**Example:**

```
aaa accounting connection h323 start-stop group radius
```

**Example:**

```
aaa pod server server-key cisco
```

**Example:**

```
aaa session-id common
```

**Example:**

```
!
```

- **Troubleshooting Tips, page 91**

---

**Troubleshooting Tips**
Use the following tips to troubleshoot POD issues:

- Ensure that the POD port is configured correctly in both the gateway (using `aaa pod server` command) and the radius server. Both should be the same.
- Ensure that the shared-secret key configured in the gateway (using `aaa pod server` command) and in the AAA server are the same.
- Turn on `debug aaa pod` command to see what’s going on. This will let you know if the gateway receives the POD packet from the server and if so, it will display any errors encountered.

The following example shows output from a successful POD request, when using the `show debug` command.

```
Router# debug aaa pod
AAA POD packet processing debugging is on
Router# show debug
General OS:
AAA POD packet processing debugging is on
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
```

### 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2865</td>
<td>Remote Authentication Dial-in User Service</td>
</tr>
<tr>
<td>RFC 3576</td>
<td>Dynamic Authorization Extensions to RADIUS</td>
</tr>
</tbody>
</table>
Technical Assistance

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

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 13  Feature Information for RADIUS Packet of Disconnect

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

Glossary

AAA --authentication, authorization, and accounting.

NACK --negative acknowledgement message.
**POD** -- packet of disconnect. An access_reject packet sent from a RADIUS server to the gateway in order to disconnect a call which has been connected already. After validation of the packet, the gateway disconnects the user. The packet contains the information to disconnect the call.

**POD server** -- a Cisco gateway configured to accept and process POD requests from a RADIUS authentication/authorization agent.

**RADIUS** -- Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet service providers.

**UDP** -- User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

**VoIP** -- voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based (for example, H.323) approach to IP voice traffic.

**VSA** -- vendor-specific attribute.

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. (1110R)

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.
AAA Authorization and Authentication Cache

The AAA Authorization and Authentication Cache feature allows you to cache authorization and authentication responses for a configured set of users or service profiles, providing performance improvements and an additional level of network reliability because user and service profiles that are returned from authorization and authentication responses can be queried from multiple sources and need not depend solely on an offload server. This feature also provides a failover mechanism so that if a network RADIUS or TACACS+ server is unable to provide authorization and authentication responses network users and administrators can still access the network.

- Finding Feature Information, page 97
- Prerequisites for Implementing Authorization and Authentication Profile Caching, page 97
- Information About Implementing Authorization and Authentication Profile Caching, page 98
- How to Implement Authorization and Authentication Profile Caching, page 100
- Configuration Examples for Implementing Authorization and Authentication Profile Caching, page 106
- Additional References, page 109
- Feature Information for Implementing Authorization and Authentication Profile Caching, page 110

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for 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, page 98
- Authorization and Authentication Profile Caching as a Failover Mechanism, page 98
- Method Lists in Authorization and Authentication Profile Caching, page 99
- Authorization and Authentication Profile Caching Guidelines, page 99
- General Configuration Procedure for Implementing Authorization and Authentication Profile Caching, page 99

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 Cisco IOS XE database), none (do nothing), RADIUS server group, or TACACS+ server group. Typically, more than one method can be configured into a method list. 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 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.

2. Update existing server groups to reference newly defined cache groups.

3. 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, page 100
• Defining RADIUS and TACACS Server Groups That Use Cache Profile Group Information, page 102
• Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used, page 104

Creating Cache Profile Groups and Defining Caching Rules

Perform this task to create a cache profile group, define the rules for what information is cached in that group, and verify and manage cache profile entries.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa cache profile group-name
5. profile name [no-auth]
6. Repeat Step 5 for each username you want to add to the profile group in Step 4.
7. regexp matchexpression {any|only}[no-auth]
8. Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4.
9. all [no-auth]
10. end
11. show aaa cache group name
12. clear aaa cache group name {profile name|all}
13. debug aaa cache group

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

Router> enable
### AAA Authorization and Authentication Cache

#### How to Implement Authorization and Authentication Profile Caching

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa cache profile group-name</td>
<td>Defines an authentication and authorization cache profile server group and enters profile map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa cache profile networkusers@companyname</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> profile name [no-auth]</td>
<td>Creates an individual authentication and authorization cache profile based on a username match.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-profile-map)# profile networkuser1 no-auth</td>
<td></td>
</tr>
</tbody>
</table>

- Use the **no-auth** keyword to bypass authentication for this user.

**Step 6** Repeat Step 5 for each username you want to add to the profile group in Step 4.

**Step 7** regexp matchexpression [any] [only] [no-auth] | (Optional) Creates an entry in a cache profile group that matches based on a regular expression. |
| **Example:** | |
| Router(config-profile-map)# regexp .*@example.com any no-auth | |

- If you use the **any** keyword, all unique usernames matching the regular expression are saved.
- If you use the **only** keyword, only one profile entry is cached for all usernames matching the regular expression.
- Use the **no-auth** keyword to bypass authentication for this user or set of users.
- Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.

**Step 8** Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4. | -- |
### Command or Action | Purpose
--- | ---
**Step 9** all [no-auth] | (Optional) Specifies that all authentication and authorization requests are cached.

  - Use the all command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

**Step 10** end | Returns to privileged EXEC mode.

**Step 11** show aaa cache group name | (Optional) Displays all cache entries for a specified group.

**Step 12** clear aaa cache group name {profile name|all} | (Optional) Clears an individual entry or all entries in the cache.

**Step 13** 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.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 aaa new-model</strong></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4 aaa group server radius group-name</strong> or <strong>aaa group server tacacs+ group-name</strong></td>
<td>Enters RADIUS server group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>* To enter TACACS+ server group configuration mode, use the <code>aaa group server tacacs+ group-name</code> command.</td>
</tr>
<tr>
<td><code>Router(config)# aaa group server radius networkusers@companyname</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5 cache authorization profile name</strong></td>
<td>Activates the authorization caching rules in the profile networkusers for this RADIUS or TACACS+ server group.</td>
</tr>
<tr>
<td>Example:</td>
<td>* The <code>name</code> argument in this command is a AAA cache profile group name.</td>
</tr>
<tr>
<td><code>Router(config-sg-radius)# cache authorization profile networkusers@companyname</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

Step 6 cache authentication profile name

**Example:**

Router(config-sq-radius)# cache authentication profile networkusers@companyname

Purpose:
Activates the authentication caching rules in the profile networkusers for this RADIUS or TACACS+ server group.

Step 7 cache expiry hours {enforce failover}

**Example:**

Router(config-sq-radius)# cache expiry 240 failover

(Optional) Sets the amount of time before a cache profile entry expires (becomes stale).

- Use the enforce keyword to specify that once a cache profile entry expires it is not used again.
- Use the failover keyword to specify that an expired cache profile entry can be used if all other methods to authenticate and authorize the user fail.

Step 8 end

**Example:**

Router(config-sq-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.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** | 
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | 
  Router# configure terminal |
| **Step 3** aaa new-model | Enables the AAA access control model. |
| **Example:** | 
  Router(config)# aaa new-model |
| **Step 4** aaa authorization {network | exec | commands level | reverse-access| configuration} {default | list-name} [method1 [method2...]] | Enables AAA authorization and creates method lists, which define the authorization methods used when a user accesses a specified function. |
| **Example:** | 
  Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname |
| **Step 5** aaa authentication ppp {default | list-name} method1 [method2...] | Specifies one or more authentication methods for use on serial interfaces that are running PPP. |
| **Example:** | 
  Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname |
| **Step 6** aaa authentication login {default | list-name} method1 [method2...] | Sets the authentication at login. |
| **Example:** | 
  Router(config)# aaa authentication login default cache adminusers group adminusers |
| **Step 7** end | Returns to privileged EXEC mode. |
| **Example:** | 
  Router(config)# end |
Configuration Examples for Implementing Authorization and Authentication Profile Caching

- Implementing Authorization and Authentication Profile Caching for Network Optimization Example, page 106
- Implementing Authorization and Authentication Profile Caching as a Failover Mechanism Example, page 107

Implementing Authorization and Authentication Profile Caching for Network Optimization Example

The following configuration example shows how to:

- Define a cache profile group adminusers that contains all administrator names on the network and sets it as the default list that is used for all login and exec sessions.
- Activate the new caching rules for a RADIUS server group.
Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried first.

```
configure terminal

aaa new-model

! Define aaa cache profile groups and the rules for what information is saved to cache.

aaa cache profile admin_users

profile adminuser1
profile adminuser2
profile adminuser3
profile adminuser4
profile adminuser5

exit

! Define server groups that use the cache information in each profile group.

aaa group server radius admins@companyname.com

cache authorization profile admin_users

cache authentication profile admin_users

! Update authentication and authorization method lists to specify how profile groups and server groups are used.

aaa authentication login default cache admins@companyname.com group admins@companyname.com

aaa authorization exec default cache admins@companyname.com group admins@companyname.com

end
```

Implementing Authorization and Authentication Profile Caching as a Failover Mechanism Example

The following configuration example shows how to:

- Create a cache profile group admin_users that contains all of the administrators on the network so that if the RADIUS or TACACS+ server should become unavailable the administrators can still access the network.
- Create a cache profile group abc_users that contains all of the ABC company users on the network so that if the RADIUS or TACACS+ server should become unavailable these users will be authorized to use the network.
- Activate the new caching rules for each profile group on a RADIUS server.
Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried last.

```
configure terminal
  aaa new-model
  ! Define aaa cache profile groups and the rules for what information is saved to cache.
  aaa cache profile admin_users
    profile admin1
    profile admin2
    profile admin3
    exit
  aaa cache profile abcusers
    profile .*@example.com only no-auth
    exit
  ! Define server groups that use the cache information in each cache profile group.
  aaa group server tacacs+ admins@companyname.com
    server 10.1.1.1
    server 10.20.1.1
    cache authentication profile admin_users
    cache authorization profile admin_users
    exit
  aaa group server radius abcusers@example.com
    server 172.16.1.1
    server 172.20.1.1
    cache authentication profile abcusers
    cache authorization profile abcusers
    exit
  ! Update authentication and authorization method lists to specify how cache is used.
  aaa authentication login default cache admins@companyname.com group
    admins@companyname.com
  aaa authorization exec default cache admins@companyname.com group
    admins@companyname.com
  aaa authentication ppp default group abcusers@example.com cache abcusers@example.com
  aaa authorization network default group abcusers@example.com cache
    abcusers@example.com
end
```
## Additional References

The following sections provide references related to implementing authentication and authorization profile caching.

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS configuration tasks</td>
<td>Configuring RADIUS chapter in the <em>Cisco IOS XE Security Configuration Guide: Securing User Services, Release 2</em></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. --</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. --</td>
</tr>
</tbody>
</table>
Technical Assistance

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

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 14  Feature Information for Implementing Authentication and Authorization Profile Caching

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Authorization and Authentication Cache</td>
<td>Cisco IOS XE Release 2.3</td>
<td>This feature optimizes network performance and provides a failover mechanism in the event a network RADIUS or TACACS+ server becomes unavailable for any reason. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: <code>aaa authentication login</code>, <code>aaa authentication ppp</code>, <code>aaa authorization</code>, <code>aaa cache profile</code>, <code>all (profile map configuration)</code>, <code>cache authentication profile (server group configuration)</code>, <code>cache authorization profile (server group configuration)</code>, <code>cache expiry (server group configuration)</code>, <code>clear aaa cache group</code>, <code>debug aaa cache group</code>, <code>profile (profile map configuration)</code>, <code>regexp (profile map configuration)</code>, <code>show aaa cache group</code>.</td>
</tr>
</tbody>
</table>

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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
Configuring 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, page 113
- AAA Authorization Prerequisites, page 113
- Information About Configuring Authorization, page 114
- How to Configure Authorization, page 117
- Authorization Configuration Examples, page 120
- Additional References, page 123
- Feature Information for Configuring Authorization, page 124

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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, page 114
- AAA Authorization Methods, page 115
- Method Lists and Server Groups, page 116
- AAA Authorization Types, page 117
- Authorization Attribute-Value Pairs, page 117

### 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.


**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.
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.

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, page 118
- Disabling Authorization for Global Configuration Commands, page 119
- Configuring Authorization for Reverse Telnet, page 119

### 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 | vty] 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates an authorization method list for a particular authorization type and enable authorization.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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

### 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**

`Router(config)# no aaa authorization config-commands`

**Purpose**

Disables authorization for all global configuration commands.

### 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:

```
Router(config)# aaa authorization reverse-access method1 [method2 ...]
```

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, page 120
- RADIUS Authorization Example, page 121
- Reverse Telnet Authorization Examples, page 121

### 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 “c251e0” “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**

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

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

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

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 15  Feature Information for Configuring Authorization

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Named Method Lists for AAA Authorization and Accounting</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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.</td>
</tr>
</tbody>
</table>

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. (1110R)

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

The AAA accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

- Finding Feature Information, page 127
- Prerequisites for Configuring Accounting, page 127
- Restrictions for Configuring Accounting, page 128
- Information About Configuring Accounting, page 128
- How to Configure AAA Accounting, page 142
- Configuration Examples for AAA Accounting, page 150
- Additional References, page 154
- Feature Information for Configuring Accounting, page 155

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Configuring 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, page 128
- AAA Accounting Types, page 132
- AAA Accounting Enhancements, page 140
- Accounting Attribute-Value Pairs, page 142

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.

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, page 129
- AAA Accounting Methods, page 130

**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.

![Typical AAA Network Configuration](image-url)
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.

- Accounting Record Types, page 130
- Accounting Methods, page 130

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>
<thead>
<tr>
<th>Table 16</th>
<th>AAA Accounting Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keyword</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for accounting.</td>
</tr>
</tbody>
</table>

Authentication Authorization and Accounting Configuration Guide Cisco IOS XE Release 2
### Configuring Accounting

#### Accounting Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group tacacs</strong></td>
<td>Uses the list of all TACACS+ servers for accounting.</td>
</tr>
<tr>
<td><strong>group group-name</strong></td>
<td>Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <strong>group-name</strong>.</td>
</tr>
</tbody>
</table>

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 the `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. For example, to create a method list that provides accounting information for ARAP (network) sessions, use the `arap` keyword.

- **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 create 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 = “00000000”
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:

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
```
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:

    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”

    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:

    start    task_id=41      service=shell
    stop     task_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"
```

```
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
```
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
       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:

```
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
       bytes_in=659926 bytes_out=138   paks_in=2378
       paks_out=1251        elapsed_time=171
```

The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:
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, page 138
- AAA Resource Accounting for Start-Stop Records, page 140

**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 6**  
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 7**  
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 8**  
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 9**  
**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 10**  
**Modem Dial-In Call Setup Sequence with Resource Start-Stop Accounting Enabled**

---

AAA Accounting Enhancements

- AAA Broadcast Accounting, page 140
- AAA Session MIB, page 141

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 17  SNMP End-User Data Objects

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SessionId</td>
<td>The session identification used by the AAA accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).</td>
</tr>
<tr>
<td>UserId</td>
<td>The user login ID or zero-length string if a login is unavailable.</td>
</tr>
<tr>
<td>IpAddr</td>
<td>The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.</td>
</tr>
<tr>
<td>IdleTime</td>
<td>The elapsed time in seconds that the session has been idle.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>The session termination object used to disconnect the given client.</td>
</tr>
<tr>
<td>CallId</td>
<td>The entry index corresponding to this accounting session that the Call Tracker record stored.</td>
</tr>
</tbody>
</table>

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

#### Table 18  SNMP AAA Session Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
</table>
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, page 142
- Suppressing Generation of Accounting Records for Null Username Sessions, page 144
- Generating Interim Accounting Records, page 144
- Configuring an Alternate Method to Enable Periodic Accounting Records, page 144
- Generating Interim Service Accounting Records, page 146
- Generating Accounting Records for a Failed Login or Session, page 146
- Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records, page 147
- Suppressing System Accounting Records over Switchover, page 147
- Configuring AAA Resource Failure Stop Accounting, page 147
- Configuring AAA Resource Accounting for Start-Stop Records, page 148
- Configuring AAA Broadcast Accounting, page 148
- Configuring per-DNIS AAA Broadcast Accounting, page 149
- Configuring the AAA Session MIB, page 149
- Establishing a Session with a Router if the AAA Server Is Unreachable, page 150
- Monitoring Accounting, page 150
- Troubleshooting Accounting, page 150

Configuring AAA Accounting Using Named Method Lists

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

<table>
<thead>
<tr>
<th>Attribute-Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveTableEntries</td>
<td>Number of sessions currently active.</td>
</tr>
<tr>
<td>ActiveTableHighWaterMark</td>
<td>Maximum number of sessions present since last system reinstallation.</td>
</tr>
<tr>
<td>TotalSessions</td>
<td>Total number of sessions since the last system reinstallation.</td>
</tr>
<tr>
<td>DisconnectedSessions</td>
<td>Total number of sessions that have been disconnected since the last system reinstallation.</td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. Router(config)# aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [method1 [method2...]]

2. Do one of the following:
   - Router(config)# line [aux | console | tty | vty] line-number [ending-line-number]
   - 
   - 
   -

3. Do one of the following:
   - Router(config-line)# accounting {arap | commands level | connection | exec} {default | list-name}
   - 
   - 

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa accounting {system</td>
<td>network</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Do one of the following:</td>
<td>Enters line configuration mode for the lines to which the accounting method list is applied.</td>
</tr>
<tr>
<td>• Router(config)# line [aux</td>
<td>console</td>
</tr>
</tbody>
</table>
|   • 
|   • 
|   • |
| **Example:** | |
| Router(config)# interface interface-type interface-number | |

| **Step 3**        |         |
| Do one of the following: | Applies the accounting method list to a line or set of lines. |
|   • Router(config-line)# accounting {arap | commands level | connection | exec} {default | list-name} | or Applies the accounting method list to an interface or set of interfaces. |
|   • 
|   • 
|   • |
| **Example:** | |
| Router(config-if)# ppp accounting {default | list-name} | |
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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config)# aaa accounting suppress null-username</code></td>
<td>Prevents accounting records from being generated for users whose username string is NULL.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config)# aaa accounting update [newinfo] [periodic] number</code></td>
<td>Enables periodic interim accounting records to be sent to the accounting server.</td>
</tr>
</tbody>
</table>

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 the `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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 aaa accounting network default</strong></td>
<td>Configures the default accounting for all network-related service requests and enters accounting method list configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa accounting network default</td>
<td></td>
</tr>
<tr>
<td>**Step 4 action-type { none</td>
<td>start-stop { periodic { disable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(cfg-acct-mlist)# action-type start-stop</td>
<td>• (Optional) The periodic keyword specifies periodic accounting action.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>periodic interval 5</td>
<td>• The interval keyword specifies the periodic accounting interval.</td>
</tr>
<tr>
<td><strong>Step 5 exit</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(cfg-acct-mlist)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Generating Interim Service Accounting Records

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

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** | |
| Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | |
| Router# configure terminal | |
| **Step 3** subscriber service accounting interim-interval *minutes* | Enables the generation of interim service accounting records at periodic intervals for subscribers. The *minutes* argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes. |
| **Example:** | |
| Router(config)# subscriber service accounting interim-interval 10 | |

---

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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| ```
Router(config)# aaa accounting send stop-record authentication failure
``` | Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP. |

**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, is 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| ```
Router(config)# 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| ```
Router(config)# 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:
### 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting resource method-list start-stop group server-group</code></td>
<td>Supports the ability to send a “start” record at each call setup, followed with a corresponding “stop” record at the call disconnect.</td>
</tr>
</tbody>
</table>

**Note** Before configuring this feature, the tasks described in the section Prerequisites for Configuring Accounting, page 127 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting broadcast</code></td>
<td>Supports the ability to send a “stop” record for any calls that do not reach user authentication.</td>
</tr>
</tbody>
</table>

**Note** Before configuring the AAA Resource Failure Stop Accounting feature, the tasks described in the Prerequisites for Configuring Accounting, page 127 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.

---

**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.
### 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`Router(config)# aaa dnis map dnis-number accounting network [start-stop</td>
<td>stop-only</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config)# aaa session-mib disconnect</code></td>
<td>Monitors and terminates authenticated client connections using SNMP.</td>
</tr>
<tr>
<td></td>
<td>To terminate the call, use the disconnect keyword.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# no aaa accounting system guarantee-first</td>
<td>The <code>aaa accounting system guarantee-first</code> 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 <code>no aaa accounting system guarantee-first</code> command.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show accounting</td>
<td>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.</td>
</tr>
</tbody>
</table>

Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# debug aaa accounting</td>
<td>Displays information on accountable events as they occur.</td>
</tr>
</tbody>
</table>

Configuration Examples for AAA Accounting

- Configuring a Named Method List Example, page 151
- Configuring AAA Resource Accounting Example, page 152
- Configuring AAA Broadcast Accounting Example, page 153
- Configuring per-DNIS AAA Broadcast Accounting Example, page 153
- AAA Session MIB Example, page 154
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.

```plaintext
global
cisco
aaa new-model
aaa authentication login admins 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Accounted actions on</td>
<td>Terminal line or interface name user with which the user logged in.</td>
</tr>
<tr>
<td>User</td>
<td>User’s ID.</td>
</tr>
<tr>
<td>Priv</td>
<td>User’s privilege level.</td>
</tr>
<tr>
<td>Task ID</td>
<td>Unique identifier for each accounting session.</td>
</tr>
<tr>
<td>Accounting Record</td>
<td>Type of accounting session.</td>
</tr>
<tr>
<td>Elapsed</td>
<td>Length of time (hh:mm:ss) for this session type.</td>
</tr>
<tr>
<td>attribute=value</td>
<td>AV pairs associated with this accounting session.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SNMP</td>
<td>Cisco IOS XE Network Management Configuration Guide</td>
</tr>
<tr>
<td>SNMP commands</td>
<td>Cisco IOS Network Management Command Reference</td>
</tr>
<tr>
<td>Security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
<tr>
<td>Configuring Radius</td>
<td>Configuring RADIUS</td>
</tr>
<tr>
<td>Configuring TACACS+</td>
<td>Configuring TACACS+</td>
</tr>
<tr>
<td>Configuring IP Services</td>
<td>Cisco IOS XE Application Services Configuration Guide</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>- No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
<tr>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-AAA-SESSION-MIB</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
</tr>
</tbody>
</table>

Technical Assistance

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

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
### AAA Broadcast Accounting

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Broadcast Accounting</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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. 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: <code>aaa accounting</code>.</td>
</tr>
</tbody>
</table>

### AAA Session MIB

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Session MIB</td>
<td>Cisco IOS XE Release 2.1</td>
<td>The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). 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: <code>aaa session-mib disconnect</code>.</td>
</tr>
</tbody>
</table>

### Connection Accounting

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Accounting</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AAA Interim Accounting</td>
<td>Cisco IOS XE Release 2.4</td>
<td>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. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: <strong>aaa accounting update</strong> and <strong>subscriber service accounting interim-interval</strong>.</td>
</tr>
</tbody>
</table>
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, page 159
Prerequisites for AAA-SERVER-MIB Set Operation, page 159
Restrictions for AAA-SERVER-MIB Set Operation, page 159
Information About AAA-SERVER-MIB Set Operation, page 160
How to Configure AAA-SERVER-MIB Set Operation, page 160
Configuration Examples for AAA-SERVER-MIB Set Operation, page 161
Additional References, page 163
Feature Information for AAA-SERVER-MIB Set Operation, page 164

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for 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, page 160
- CISCO-AAA-SERVER-MIB Set Operation, page 160

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, page 160

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 show running-config</td>
<td>include radius-server host</td>
</tr>
<tr>
<td>Example: Router# show running-config</td>
<td>include radius-server host</td>
</tr>
<tr>
<td>Step 3 show aaa servers</td>
<td>Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers.</td>
</tr>
<tr>
<td>Example: Router# show aaa servers</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for AAA-SERVER-MIB Set Operation

- RADIUS Server Configuration and Server Statistics Example, page 161

### 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
Authen: request 0, timeouts 0
  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 0a, 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 0a, count 2
Authen: request 8, timeouts 8
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 4
Author: request 0, timeouts 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Account: request 0, timeouts 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
Dead: total time 0s, count 7
Authen: request 0, timeouts 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Author: request 0, timeouts 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Account: request 0, timeouts 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms

Additional References

The following sections provide references related to the AAA-SERVER-MIB Set Operation feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SNMP</td>
<td>Configuring SNMP Support in the Cisco IOS XE Network Management Configuration Guide, Release 2</td>
</tr>
<tr>
<td>SNMP commands</td>
<td>Cisco IOS Network Management Command Reference</td>
</tr>
<tr>
<td>Security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
<tr>
<td>Cisco IOS XE commands</td>
<td>Cisco IOS Master Commands List</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>

Authentication Authorization and Accounting Configuration Guide Cisco IOS XE Release 2
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-AAA-SERVER-MIB</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. --</td>
</tr>
</tbody>
</table>

Technical Assistance

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

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 21 Feature Information for AAA-SERVER-MIB Set Operation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA-SERVER-MIB Set</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

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. (1110R)

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.
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, page 167
- Restrictions for Per VRF AAA, page 167
- Information About Per VRF AAA, page 168
- How to Configure Per VRF AAA, page 174
- Configuration Examples for Per VRF AAA, page 187
- Additional References, page 195
- Feature Information for Per VRF AAA, page 196
- Glossary, page 198

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 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, page 168
- AAA Accounting Records, page 168
- New Vendor-Specific Attributes, page 168
- VRF Aware Framed-Routes, page 174

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 22**  
**VSAs Supported with Per VRF AAA**

<table>
<thead>
<tr>
<th>VSA Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> Each VSA must have the prefix “template:” before the VSA name, unless a different prefix is explicitly stated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account-delay</td>
<td>string</td>
<td>This VSA must be “on.” The functionality of this VSA is equal to the aaa accounting delay-start command for the customer template.</td>
</tr>
<tr>
<td>account-send-stop</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>account-send-success-remote</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>attr-44</td>
<td>string</td>
<td>This VSA must be “access-req.” The functionality of this VSA is equal to the radius-server attribute 44 include-in-access-req command.</td>
</tr>
<tr>
<td>VSA Name</td>
<td>Value Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip-addr</td>
<td>string</td>
<td>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</td>
</tr>
<tr>
<td>ip-unnumbered</td>
<td>string</td>
<td>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.”</td>
</tr>
<tr>
<td>ip-vrf</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>peer-ip-pool</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>VSA Name</td>
<td>Value Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ppp-acct-list</td>
<td>string</td>
<td>This VSA defines the accounting method list that is to be used for PPP sessions. The VSA syntax is as follows: “ppp-acct-list=[start-stop</td>
</tr>
<tr>
<td>ppp-authen-list</td>
<td>string</td>
<td>This VSA defines which authentication method list is to be used for PPP sessions and, if more than one method is specified, in what order the methods should be used. The VSA syntax is as follows: “ppp-authen-list=[groupX</td>
</tr>
<tr>
<td>VSA Name</td>
<td>Value Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ppp-authen-type</td>
<td>string</td>
<td>This VSA allows the end user to specify at least one of the following authentication types: pap, chap, eap, ms-chap, ms-chap-v2, any, or a combination of the available types that is separated by spaces. The end user will be permitted to log in using only the methods that are specified in this VSA. PPP will attempt these authentication methods in the order presented in the attribute.</td>
</tr>
<tr>
<td>ppp-author-list</td>
<td>string</td>
<td>This VSA defines the authorization method list that is to be used for PPP sessions. It indicates which methods will be used and in what order. The VSA syntax is as follows: “ppp-author-list=[groupX] [local] [if-authenticated] [none],” which is equal to the <code>aaa authorization network mylist</code> command functionality. The user must specify at least one, but no more than four, authorization methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA “rad-serv.”</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>VSA Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rad-serv</td>
<td>string</td>
<td>This VSA indicates the IP address, key, timeout, and retransmit number of a server, as well as the group of the server. The VSA syntax is as follows: “rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W].” Other than the IP address, all parameters are optional and can be issued in any order. If the optional parameters are not specified, their default values will be used. The key cannot contain any spaces; for “retransmit V,” “V” can range from 1-100; for “timeout W,” the “W” can range from 1-1000.</td>
</tr>
<tr>
<td>rad-serv-filter</td>
<td>string</td>
<td>The VSA syntax is as follows: “rad-serv-filter=authorization</td>
</tr>
<tr>
<td>rad-serv-source-if</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>rad-serv-vrf</td>
<td>string</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 rout is applied accordingly.

How to Configure Per VRF AAA

- Configuring Per VRF AAA, page 174
- Configuring Per VRF AAA Using Local Customer Templates, page 180
- Configuring Per VRF AAA Using Remote Customer Templates, page 184
- Verifying VRF Routing Configurations, page 186
- Troubleshooting Per VRF AAA Configurations, page 187

Configuring Per VRF AAA

- Configuring AAA, page 174
- Configuring Server Groups, page 175
- Configuring Authentication Authorization and Accounting for Per VRF AAA, page 176
- Configuring RADIUS-Specific Commands for Per VRF AAA, page 178
- Configuring Interface-Specific Commands for Per VRF AAA, page 179

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

```
Router> enable
```
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa group server radius <em>groupname</em></td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods. Enters server-group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa group server radius v2.44.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> server-private ip-address [auth-port port-number</td>
<td>acct-port port-number] [non-standard] [timeout seconds] [retransmit retries] [key string]</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If private server parameters are not specified, global configurations will be used. If global configurations are not specified, default values will be used.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits from server-group configuration mode; returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sg-radius)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**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

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

Example:

```
Router> enable
```

| **Step 2** configure terminal | Enters global configuration mode. |

Example:

```
Router# configure terminal
```

| **Step 3** aaa new-model | Enables AAA globally. |

Example:

```
Router(config)# aaa new-model
```

| **Step 4** aaa authentication ppp [default | list-name] method1 [method2...] | Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. |

Example:

```
Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com
```

| **Step 5** aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} method1 [method2...] | Sets parameters that restrict user access to a network. |

Example:

```
Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com
```

| **Step 6** aaa accounting system default [vrf vrf-name] [start-stop | stop-only | none] [broadcast] group groupname | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. |

Example:

```
Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com
```
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

```
Router> enable
```
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number [name-tag]</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface loopback11</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip vrf forwarding vrf-name</td>
<td>Associates a VRF with an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip vrf forwarding v2.44.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ppp authentication [protocol1 [protocol2...]] listname</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp authentication chap callin V2_44_com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ppp authorization list-name</td>
<td>Enables AAA authorization on the selected interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp authorization V2_44_com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ppp accounting default</td>
<td>Enables AAA accounting services on the selected interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ppp accounting default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Per VRF AAA Using Local Customer Templates**

- Configuring AAA, page 181
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
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 {protocol [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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Per VRF AAA

**Configuring Local Customer Templates**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> vpdn search-order domain</td>
<td>Looks up the profiles based on domain.</td>
</tr>
</tbody>
</table>

**Example:**

Router (config)# vpdn search-order domain

| **Step 4** template name [default | exit | multilink | no | peer | ppp] | Creates a customer profile template and assigns a unique name that relates to the customer that will be receiving it. |
|-------------------|---------|
| **Example:** | Enters template configuration mode. |

Router (config)# template v2.44.com

| **Note** | Steps 5, 6, and 7 are optional. Enter multilink, peer, and ppp keywords appropriate to customer application requirements. |

<table>
<thead>
<tr>
<th><strong>Step 5</strong> peer default ip address pool pool-name</th>
<th>(Optional) Specifies that the customer profile to which this template is attached will use a local IP address pool with the specified name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>

Router(config-template)# peer default ip address pool v2_44_com_pool

| **Step 6** ppp authentication {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time] | (Optional) Sets the PPP link authentication method. |
|-------------------|---------|
| **Example:** | |

Router(config-template)# ppp authentication chap

| **Step 7** ppp authorization [default | list-name] | (Optional) Sets the PPP link authorization method. |
|-------------------|---------|
| **Example:** | |

Router(config-template)# ppp authorization v2_44_com

| **Step 8** aaa accounting [auth-proxy | system | network | exec | connection | commands level] {default | list-name} [vrf vrf-name] [start-stop | stop-only | none] [broadcast] group groupname | (Optional) Enables AAA operational parameters for the specified customer profile. |
|-------------------|---------|
| **Example:** | |

Router(config-template)# aaa accounting v2_44_com
### Configuring Per VRF AAA Using Remote Customer Templates

- Configuring AAA, page 184
- Configuring Server Groups, page 181
- Configuring Authentication for Per VRF AAA with Remote Customer Profiles, page 184
- Configuring Authorization for Per VRF AAA with Remote Customer Profiles, page 185
- Configuring the RADIUS Profile on the SP RADIUS Server, page 186

#### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits from template configuration mode; returns to global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

```bash
Router(config-template)# exit
```
## 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

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

  - Enter your password if prompted.

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

Router> enable
Step 2  configure terminal

Example:
Router# configure terminal

Step 3  show ip route vrf vrf-name

Example:
Router(config)# show ip route vrf northvrf

Troubleshooting Per VRF AAA Configurations

To troubleshoot the Per VRF AAA feature, use at least one of the following commands in EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# debug aaa accounting</td>
<td>Displays information on accountable events as they occur.</td>
</tr>
<tr>
<td>Router# debug aaa authentication</td>
<td>Displays information on AAA authentication.</td>
</tr>
<tr>
<td>Router# debug aaa authorization</td>
<td>Displays information on AAA authorization.</td>
</tr>
<tr>
<td>Router# debug ppp negotiation</td>
<td>Displays information on traffic and exchanges in an internetwork implementing PPP.</td>
</tr>
<tr>
<td>Router# debug radius</td>
<td>Displays information associated with RADIUS.</td>
</tr>
<tr>
<td>Router# debug vpdn event</td>
<td>Displays Layer 2 Transport Protocol (L2TP) errors and events that are a part of normal tunnel establishment or shutdown for VPNs.</td>
</tr>
<tr>
<td>Router# debug vpdn error</td>
<td>Displays debug traces for VPN.</td>
</tr>
</tbody>
</table>

Configuration Examples for Per VRF AAA

- Per VRF Configuration Examples, page 188
- Customer Template Examples, page 189
- AAA Accounting Stop Record Examples, page 191
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:

```plaintext
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 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:

```plaintext
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
    ip 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 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:

```plaintext
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp
aaa group server radius sp
```
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-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

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
daas authorization network default local group radius
daas authorization network V1_55_com group V1_55_com
daas accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server
daas group server radius SP_AAA_server
server 10.10.100.7 auth-port 1645 acct-port 1646
daas group server radius V1_55_com
daas 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

Customer Template Examples

- Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example, page 189
- Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting Example, page 190
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
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 1645 key ww
```

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-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**

- AAA Accounting Stop Record and Rejected Call Example, page 191
- AAA Accounting Stop Record and Successful Call Example, page 193

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 = PPPoE
*Jul  7 03:39:42.199: RADIUS: AAA Unsupported [156] 7
*Jul  7 03:39:42.199: RADIUS: 30 2F 30 2F
   [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: 1645
*Jul  7 03:39:42.199: RADIUS: sending
*Jul  7 03:39:42.199: RADIUS: authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D 16 BE AC 7E 5F A6
  [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]
  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]
  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 59 OC E4 6C - BA 11 23 63 81 DE 6F D7
  PPP [1]
*Jul  7 03:39:42.275: RADIUS: Service-Type [6] 6
  Framed [2]
```
AAA Accounting Stop Record and Rejected Call Example

Authentication Authorization and Accounting Configuration Guide Cisco IOS XE Release 2
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 failure` 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

  AAA/BIND(00000018): Bind i/f Virtual-Template2
  AAA/AUTHOR/LCP: Authorization succeeds trivially
  AAA/BIND(00000019): Bind i/f Tnl 5192 L2TP: O SCCRP
  AAA/BIND(00000018): Bind i/f Virtual-Template2
  AAA/AUTHOR/LCP: Authorization succeeds trivially
  AAA/BIND(00000019): Bind i/f Tnl 5192 L2TP: O SCCRP
```

Authentication Authorization and Accounting Configuration Guide Cisco IOS XE Release 2
Additional References

The following sections provide references related to Per VRF AAA.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Security Commands</td>
<td><em>Cisco IOS Security Command Reference</em></td>
</tr>
<tr>
<td>Cisco IOS Switching Services Commands</td>
<td><em>Cisco IOS IP Switching Command Reference</em></td>
</tr>
<tr>
<td>Configuring Multiprotocol Label Switching</td>
<td><em>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</em>, Release 2</td>
</tr>
<tr>
<td>Configuring virtual templates</td>
<td>Virtual Templates and Profiles section of the <em>Cisco IOS XE Dial Technologies Configuration Guide</em>, Release 2</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

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

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 23 Feature Information for Per VRF AAA

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per VRF AAA</td>
<td>Cisco IOS XE Release 2.1</td>
<td>The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances. 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: <code>aaa accounting</code>, <code>aaa accounting delay-start</code>, <code>ip radius source-interface</code>, <code>server-private (RADIUS)</code>, <code>ip vrf forwarding (server-group)</code>, <code>radius-server domain-stripping</code>, <code>aaa authorization template</code>.</td>
</tr>
<tr>
<td>RADIUS Per-VRF Server Group</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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 &quot;aaa: rad-serv-vrf&quot; VSA. 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: <code>ip vrf forwarding</code>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attribute Filtering Per-Domain and VRF Aware Framed-Routes</td>
<td>Cisco IOS XE Release 2.3</td>
<td>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. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>AAA CLI Stop Record Enhancement</td>
<td>Cisco IOS XE Release 2.4</td>
<td>The AAA CLI Stop Record Enhancement feature enables sending an accounting stop record only when an access accept is received from the AAA server. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: <code>aaa accounting send stop-record authentication</code>.</td>
</tr>
<tr>
<td>Dynamic Per VRF AAA</td>
<td>Cisco IOS XE Release 2.4</td>
<td>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. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Glossary**

AAA--authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

L2TP--Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with...
the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

**PE**--Provider Edge. Networking devices that are located on the edge of a service provider network.

**RADIUS** --Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

**VPN** --Virtual Private Network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

**VRF** --Virtual Route Forwarding. Initially, a router has only one global default routing/forwarding table. VRFs can be viewed as multiple disjoined routing/forwarding tables, where the routes of a user have no correlation with the routes of another user.

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. (1110R)

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.