



## **RADIUS Configurations Configuration Guide, Cisco IOS XE Release 3E**

### **Americas Headquarters**

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

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

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

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

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

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

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

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: <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)

© 2015 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Local AAA Server 1

Finding Feature Information 1

Prerequisites for Local AAA Server 1

Information About Local AAA Server 2

Local Authorization Attributes Overview 2

Local AAA Attribute Support 2

AAA Attribute Lists 2

    Converting from RADIUS Format to Cisco IOS AAA Format 3

Validation of Attributes 3

How to Configure Local AAA Server 3

    Defining a AAA Attribute List 3

    Monitoring and Troubleshooting a Local AAA Server 5

Configuration Examples for Local AAA Server 6

    Local AAA Server Example 6

    Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version

        Example 7

Additional References 7

    Related Document 7

    Standards 7

    MIBs 8

    RFCs 8

    Technical Assistance 8

Feature Information for Local AAA Server 8

---

### CHAPTER 2

#### Enhanced Test Command 11

Finding Feature Information 11

Restrictions for the Enhanced Test Command 11

How to Configure the Enhanced Test Command 12

Configuring a User Profile and Associating it with the RADIUS Record	12
Verifying the Enhanced Test Command Configuration	13
Configuration Example for Enhanced Test Command	13
User Profile Associated With a test aaa group command Example	13
Additional References	14
Feature Information for Enhanced Test Command	15
Glossary	16

---

**CHAPTER 3****RADIUS Progress Codes 17**

Finding Feature Information	17
Prerequisites for RADIUS Progress Codes	17
Information About RADIUS Progress Codes	18
How to Configure RADIUS Progress Codes	19
How to Verify Attribute 196	19
Troubleshooting Tips	19
Additional References	20
Feature Information for RADIUS Progress Codes	21
Glossary	22



## CHAPTER

# 1

## Local AAA Server

---

The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Local AAA Server, page 1](#)
- [Information About Local AAA Server, page 2](#)
- [How to Configure Local AAA Server, page 3](#)
- [Configuration Examples for Local AAA Server, page 6](#)
- [Additional References, page 7](#)
- [Feature Information for Local AAA Server, page 8](#)

## Finding Feature Information

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

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

## Prerequisites for Local AAA Server

- Before using this feature, you must have the **aaa new-model** command enabled.

# Information About Local AAA Server

## Local Authorization Attributes Overview

The AAA subsystem (authentication, authorization, and accounting) is responsible for managing all supported attributes that are available to the various services within the Cisco IOS software. As such, it maintains its own local dictionary of all supported attributes. However, prior to Cisco IOS Release 12.3(14)T, most of these authorization options were not available for local (on-box) authorizations.

## Local AAA Attribute Support

Effective with Cisco IOS Release 12.3(14)T, you can configure your router so that AAA authentication and authorization attributes currently available on AAA servers are made available on existing Cisco IOS devices. The attributes can be added to existing framework, such as the local user database or subscriber profile. For example, an attribute list can now be added to an existing username, providing the ability for the local user database to act as a local AAA server. For situations in which the local username list is relatively small, this flexibility allows you to provide complete user authentication or authorization locally within the Cisco IOS software without having a AAA server. This ability can allow you to maintain your user database locally or provide a failover local mechanism without having to sacrifice policy options when defining local users.

A subscriber profile allows domain-based clients to have policy applied at the end-user service level. This flexibility allows common policy to be set for all users under a domain in one place and applied there whether or not user authorization is done locally. Effective with Cisco IOS Release 12.3(14)T, an attribute list can be added to the subscriber profile, allowing the profile to apply all attributes that can be applied to services using AAA servers. Attributes that are configured under the AAA attribute list are merged with the existing attributes that are generated with the existing subscriber profile and passed to the Subscriber Server Switch (SSS) framework for application.

**Note**

---

Accounting is still done on a AAA server and is not supported by this feature.

---

## AAA Attribute Lists

AAA attribute lists define user profiles that are local to the router. Every attribute that is known to the AAA subsystem is made available for configuration.

The AAA attributes that are defined in the AAA attribute list are standard RADIUS or TACACS+ attributes. However, they are in the internal format for that attribute. The attributes must be converted from the RADIUS format (for a RADIUS case) to the Cisco IOS AAA interface format. TACACS+ attributes are generally identical to the AAA interface format.

## Converting from RADIUS Format to Cisco IOS AAA Format

You can use the **show aaa attributes protocol radius** command to get the Cisco IOS AAA format of the Internet Engineering Task Force (IETF) RADIUS attribute. The **show** command output provides a complete list of all the AAA attributes that are supported.

**Note**

The conversion from RADIUS to internal AAA is done internally within the AAA framework. RADIUS vendor-specific attributes (VSAs) are usually accurately reflected during conversion. TACACS+ attributes are also usually identical to the local attributes and do not require the conversion process. However, IETF numbered attributes and some special VSAs often require the conversion process.

## Validation of Attributes

Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation applies whether the AAA server is RADIUS or TACACS+. Thus, if you are not familiar with configuring a AAA server, it is advisable that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

## How to Configure Local AAA Server

### Defining a AAA Attribute List

To define an AAA attribute list, perform the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa attribute list** *list-name*
4. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
5. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
6. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
7. **attribute type** {*name*} {*value*}
8. **attribute type** {*name*} {*value*}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>aaa attribute list list-name</b>  <b>Example:</b> Device (config)# aaa attribute list TEST	Defines a AAA attribute list.
Step 4	<b>attribute type {name} {value} [service service] [protocol protocol]</b>  <b>Example:</b> Device (config-attr-list)# attribute type addr-pool poolname service ppp protocol ip	Defines an IP address pool to use.
Step 5	<b>attribute type {name} {value} [service service] [protocol protocol]</b>  <b>Example:</b> Device (config-attr-list)# attribute type ip-unnumbered loopbacknumber service ppp protocol ip	Defines the loopback interface to use.
Step 6	<b>attribute type {name} {value} [service service] [protocol protocol]</b>  <b>Example:</b> Device (config-attr-list)# attribute type vrf-id vrfname service ppp protocol ip	Defines the virtual route forwarding (VRF) to use.
Step 7	<b>attribute type {name} {value}</b>  <b>Example:</b> Device (config-attr-list)# attribute type ppp-authen-list aalistname	Defines the AAA authentication list to use.
Step 8	<b>attribute type {name} {value}</b>  <b>Example:</b> Device (config-attr-list)# attribute type ppp-acct-list "aaa list name"	Defines the AAA accounting list to use.



## Monitoring and Troubleshooting a Local AAA Server

The following debug commands may be helpful in monitoring and troubleshooting, especially to ensure that domain-based service authorization is being triggered and that location authorization is being called on the local AAA server, which triggers the service.

### SUMMARY STEPS

1. **enable**
2. **debug aaa authentication**
3. **debug aaa authorization**
4. **debug aaa per-user**
5. **debug radius**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug aaa authentication</b>  <b>Example:</b> Device# debug aaa authentication	Displays the methods of authentication being used and the results of these methods.
Step 3	<b>debug aaa authorization</b>  <b>Example:</b> Device# debug aaa authorization	Displays the methods of authorization being used and the results of these methods.
Step 4	<b>debug aaa per-user</b>  <b>Example:</b> Device# debug aaa per-user	Displays information about PPP session per-user activities.
Step 5	<b>debug radius</b>  <b>Example:</b> Device# debug radius	Displays information about the RADIUS server.

# Configuration Examples for Local AAA Server

## Local AAA Server Example

The following example shows a Point to Point over Ethernet (PPPoE) group named “bba-group” that is configured for subscriber profile cisco.com (thus, any user with the domain name cisco.com will execute the subscriber profile cisco.com authorization policy). The cisco.com subscriber profile is configured to attach the AAA attribute list “TEST,” which has both “ip vrf forwarding” and “ip unnumbered” configured for PPP service under Link Control Protocol (LCP) negotiation. This configuration will essentially cause the named attributes to be applied on the session with the cisco.com domain under the bba-group “pppoe grp1.”

```

aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
  attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
  attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
  description vrf blue template1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
subscriber authorization enable
!
policy-map type service example.com
  service local
  aaa attribute list TEST
!
bba-group pppoe grp1
  virtual-template 1
  service profile example.com
!
interface Virtual-Template1
  no ip address
  no snmp trap link-status
  no peer default ip address
  no keepalive
  ppp authentication pap template1
  ppp authorization template1
!

```



### Note

In some versions of Cisco IOS software, it is better to use the explicit attribute instead of interface- config because it provides better scalability (full VAccess interfaces are not required, and sub interfaces could be used to provide the service). In such a case, you might configure “attribute type ip-unnumbered ‘FastEthernet0’ service ppp protocol ip” instead of “attribute type interface-config ‘ip unnumbered FastEthernet0’ service ppp protocol lcp.”

## Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version Example

The following output example of the **show aaa attributes** command lists RADIUS attributes, which can be used when configuring this feature.

```
Device#
show aaa attributes protocol radius
IETF defined attributes:
  Type=4      Name=acl                      Format=Ulong
  Protocol:RADIUS
  Unknown    Type=11   Name=Filter-Id      Format=Binary
Converts attribute 11 (Filter-Id) of type Binary into an internal attribute
named "acl" of type Ulong. As such, one can configure this attributes locally
by using the attribute type "acl."
Cisco VSA attributes:
  Type=157   Name=interface-config      Format=String
Simply expects a string for the attribute of type "interface-config."
```



### Note

The **aaa attribute list** command requires the Cisco IOS AAA version of an attribute, which is defined in the "Name" field above.

## Additional References

### Related Document

Related Topic	Document Title
AAA, AAA attribute lists, AAA method lists, and subscriber profiles	Configuring Local AAA Server feature module and the User Database--Domain to VRF in <i>Cisco 10000 Series Broadband Aggregation and Leased-Line Configuration Guide</i>
Cisco IOS security commands	<i>Cisco IOS Security Command Reference</i>

### Standards

Standard	Title
None	--

## MIBs

MIB	MIBs Link
None	<a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> To locate and download MIBs for selected platforms, Cisco IOS 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>

## RFCs

RFC	Title
None	--

## Technical Assistance

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

## Feature Information for Local AAA Server

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 . An account on Cisco.com is not required.

**Table 1: Feature Information for Local AAA Server**

<b>Feature Name</b>	<b>Releases</b>	<b>Feature Information</b>
Local AAA Server	Cisco IOS XE 3.3SG Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	<p>The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>





## Enhanced Test Command

---

The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or dialed number identification service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.

- [Finding Feature Information, page 11](#)
- [Restrictions for the Enhanced Test Command, page 11](#)
- [How to Configure the Enhanced Test Command, page 12](#)
- [Configuration Example for Enhanced Test Command, page 13](#)
- [Additional References, page 14](#)
- [Feature Information for Enhanced Test Command, page 15](#)
- [Glossary, page 16](#)

## Finding Feature Information

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

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

## Restrictions for the Enhanced Test Command

The `test aaa group` command does not work with TACACS+.

# How to Configure the Enhanced Test Command

## Configuring a User Profile and Associating it with the RADIUS Record

This section describes how to create a named user profile with CLID or DNIS attribute values and associate it with the RADIUS record.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa user profile** *profile-name*
4. **aaa attribute** {dnis | clid}
5. **exit**
6. **test aaa group** {group-name | } *username password new-code* [**profile** *profile-name*]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>aaa user profile</b> <i>profile-name</i>  <b>Example:</b> Device(config)# aaa user profile profilename1	Creates a user profile.
<b>Step 4</b>	<b>aaa attribute</b> {dnis   clid}  <b>Example:</b> Device# configure terminal	Adds DNIS or CLID attribute values to the user profile and enters AAA-user configuration mode.
<b>Step 5</b>	<b>exit</b>	Exit Global Configuration mode.
<b>Step 6</b>	<b>test aaa group</b> {group-name   } <i>username password new-code</i> [ <b>profile</b> <i>profile-name</i> ]	Associates a DNIS or CLID named user profile with the record sent to the RADIUS server.



	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device# test aaa group username secret new-code profile profilename1</pre>	<p><b>Note</b> The <i>profile-name</i> must match the profile-name specified in the <b>aaa user profile</b> command.</p>

## Verifying the Enhanced Test Command Configuration

To verify the Enhanced Test Command configuration, use the following commands in privileged EXEC mode:

Command	Purpose
Device# <b>debug radius</b>	Displays information associated with RADIUS.
Device# <b>more system:running-config</b>	Displays the contents of the current running configuration file. (Note that the <b>more system:running-config</b> command has replaced the <b>show running-config</b> command.)

## Configuration Example for Enhanced Test Command

### User Profile Associated With a test aaa group command Example

The following example shows how to configure the dnis = dnisvalue user profile “prfl1” and associate it with a **test aaa group** command. In this example, the **debug radius** command has been enabled and the output follows the configuration.

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
!
!
! debug radius output, which shows that the dnis value has been passed to the radius !
server.
*Dec 31 16:35:48: RADIUS: Sending packet for Unique id = 0
*Dec 31 16:35:48: RADIUS: Initial Transmit unknown id 8 172.22.71.21:1645, Access-Request,
```

```

len 68
*Dec 31 16:35:48: RADIUS: code=Access-Request id=08 len=0068
    authenticator=1E CA 13 F2 E2 81 57 4C - 02 EA AF 9D 30 D9 97 90
    T=User-Password[2]                                L=12 V=*
    T=User-Name[1]                                    L=07 V="test"
    T=Called-Station-Id[30]                           L=0B V="dnisvalue"
    T=Service-Type[6]                                  L=06 V=Login
    T=NAS-IP-Address[4]                                L=06 V=10.0.1.81
                                                    [1]

*Dec 31 16:35:48: RADIUS: Received from id 8 172.22.71.21:1645, Access-Accept, len 38
*Dec 31 16:35:48: RADIUS: code=Access-Accept id=08 len=0038

```

## Additional References

The following sections provide references related to Enhanced Test Command.

### Related Documents

Related Topic	Document Title
Security Commands	<i>Cisco IOS Security Command Reference</i>

### Standards

Standard	Title
None	--

### MIBs

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

### RFCs

RFC	Title
None	--

**Technical Assistance**

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

## Feature Information for Enhanced Test Command

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 [http://www.cisco.com/featurenavigator](#). An account on Cisco.com is not required.

**Table 2: Feature Information for Enhanced Test Command**

Feature Name	Releases	Feature Information
Enhanced Test Command	Cisco IOS XE 3.3SG Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	<p>The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or Dialed Number Identification Service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.</p> <p>The following commands were introduced or modified: <b>aaa attribute</b>, <b>aaa user profile</b>, and <b>test aaa group</b></p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>

# Glossary

**attribute** --RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

CLID--calling line ID. CLID provides the number from which a call originates.

DNIS--dialed number identification service. DNIS provides the number that is dialed.

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. © 2001, 2006-2007 Cisco Systems, Inc. All rights reserved.



## RADIUS Progress Codes

---

The RADIUS Progress Codes feature adds additional progress codes to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.

- [Finding Feature Information, page 17](#)
- [Prerequisites for RADIUS Progress Codes, page 17](#)
- [Information About RADIUS Progress Codes, page 18](#)
- [How to Configure RADIUS Progress Codes, page 19](#)
- [Additional References, page 20](#)
- [Feature Information for RADIUS Progress Codes, page 21](#)
- [Glossary, page 22](#)

### Finding Feature Information

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

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

### Prerequisites for RADIUS Progress Codes

Before attribute 196 (Ascend-Connect-Progress) can be sent in accounting “start” and “stop” records, you must perform the following tasks:

- Enable AAA.
- Enable exec, network, or resource accounting.

For information on completing these tasks, refer to the AAA sections of the *Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0.

When these tasks are completed, attribute 196 is active by default.

## Information About RADIUS Progress Codes

Attribute 196 is sent in network, exec, and resource accounting “start” and “stop” records. This attribute can facilitate call failure debugging because each progress code identifies accounting information relevant to the connection state of a call. The attribute is activated by default; when an accounting “start” or “stop” accounting record is requested, authentication, authorization, and accounting (AAA) adds attribute 196 into the record as part of the standard attribute list. Attribute 196 is valuable because the progress codes, which are sent in accounting “start” and “stop” records, facilitate the debugging of call failures.


**Note**

In accounting “start” records, attribute 196 does not have a value.

**Table 3: Newly Supported Progress Codes for Attribute 196**

Code	Description
10	Modem allocation and negotiation is complete; the call is up.
30	The modem is up.
33	The modem is waiting for result codes.
41	The max TNT is establishing the TCP connection by setting up a TCP clear call.
60	Link control protocol (LCP) is the open state with PPP and IP Control Protocol (IPCP) negotiation; the LAN session is up.
65	PPP negotiation occurs and, initially, the LCP negotiation occurs; LCP is in the open state.
67	After PPP negotiation with LCP in the open state occurs, IPCP negotiation begins.


**Note**

Progress codes 33, 30, and 67 are generated and seen through debugs on the NAS; all other codes are generated and seen through debugs and the accounting record on the RADIUS server.

# How to Configure RADIUS Progress Codes

No configuration is required to configure RADIUS Progress Codes.

## How to Verify Attribute 196

To verify attribute 196 in accounting “start” and “stop” records, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug aaa accounting**
3. **show radius statistics**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>debug aaa accounting</b>  <b>Example:</b> Device# debug aaa accounting	Displays information on accountable events as they occur.
<b>Step 3</b>	<b>show radius statistics</b>  <b>Example:</b> Device# debug aaa authorization	Displays the RADIUS statistics for accounting and authentication packets.

## Troubleshooting Tips

The following example is a sample debug output from the **debug ppp negotiation** command. This debug output is used to verify that accounting “stop” records have been generated and that attribute 196 (Ascend-Connect-Progress) has a value of 65.

```
Tue Aug 7 06:21:03 2001
  NAS-IP-Address = 10.0.58.62
  NAS-Port = 20018
  Vendor-Specific = ""
  NAS-Port-Type = ISDN
```

```

User-Name = "peer_16a"
Called-Station-Id = "5213124"
Calling-Station-Id = "5212175"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed-User
Acct-Session-Id = "00000014"
Framed-Protocol = PPP
Framed-IP-Address = 172.16.0.2
Acct-Input-Octets = 3180
Acct-Output-Octets = 3186
Acct-Input-Packets = 40
Acct-Output-Packets = 40
Ascend-Connect-Pr = 65
Acct-Session-Time = 49
Acct-Delay-Time = 0
Timestamp = 997190463
Request-Authenticator = Unverified

```

## Additional References

The following sections provide references related to RADIUS Progress Codes.

### Related Documents

Related Topic	Document Title
Cisco IOS Security commands	<i>Cisco IOS Security Command Reference</i>
Configuring Accounting	Configuring Accounting module
RADIUS Attributes	RADIUS Attributes Overview and RADIUS IETF Attributes module

### Standards

Standard	Title
None	--

### MIBs

MIB	MIBs Links
None	To locate and download MIBs for selected platforms, Cisco IOS 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>



**RFCs**

RFC	Title
None	---

**Technical Assistance**

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

## Feature Information for RADIUS Progress Codes

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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

**Table 4: Feature Information for RADIUS Progress Codes**

Feature Name	Releases	Feature Information
RADIUS Progress Codes	Cisco IOS XE 3.3SG Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	<p>The RADIUS Progress Codes feature adds additional progress codes to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>

# Glossary

**AAA** --authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

**attribute** --RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information through IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

**EXEC accounting**--Provides information about user EXEC terminal sessions of the network access server.

**IPCP** --IP Control Protocol. A protocol that establishes and configures IP over PPP.

**LCP** --link control protocol. A protocol that establishes, configures, and tests data-link connections for use by PPP.

**network accounting**--Provides information for all PPP, Serial Line Internet Protocol (SLIP), or AppleTalk Remote Access Protocol (ARAP) sessions, including packet and byte counts.

**PPP** --Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

**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.

**resource accounting**--Provides "start" and "stop" records for calls that have passed user authentication, and provides "stop" records for calls that fail to authenticate.