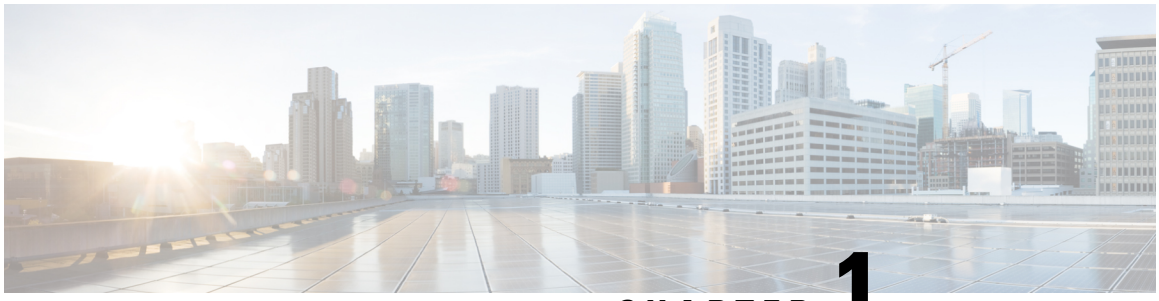
General RADIUS Configurations Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

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

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

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

Feature Information

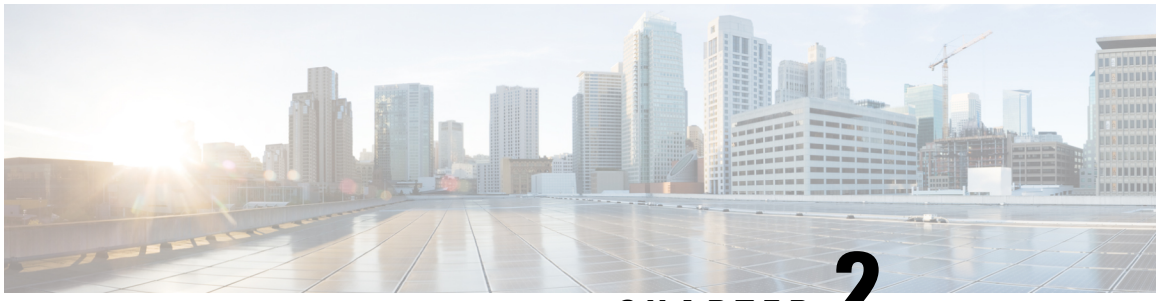
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

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



CHAPTER 2

Attribute Screening for Access Requests

The Attribute Screening for Access Requests feature allows you to configure your network access server (NAS) to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.

Finding Feature Information

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

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

Prerequisites for Attribute Screening for Access Requests

- You must be familiar with configuring attribute lists.

Restrictions for Attribute Screening for Access Requests

- Attributes 1 (Username), 2 (User-Password), and 3 (Chap-Password) cannot be filtered.

Information About Attribute Screening for Access Requests

Configuring an NAS to Filter Attributes in Outbound Access Requests

The Attribute Screening for Access Requests feature allows you to configure your NAS to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. The filters can be configured on the NAS, or they can be downloaded via downloadable vendor-specific attributes (VSAs) from the authentication, authorization, and accounting (AAA) server.

The following are some examples of the downloadable VSAs:

```
Cisco:Cisco-Avpair="ppp-authen-type=chap"
Cisco:Cisco-Avpair="ppp-authen-list=group 1"
Cisco:Cisco-Avpair="ppp-author-list=group 1"
Cisco:Cisco-Avpair="vpdn:tunnel-id=B53"
Cisco:Cisco-Avpair="vpdn:ip-addresses=10.0.58.35"
```

Note You must be aware of which attributes you want to filter. Filtering certain key attributes can result in authentication failure (for example, attribute 60 should not be filtered).

How to Configure Attribute Screening for Access Requests

Configuring Attribute Screening for Access Requests

or

accounting [**request** | **reply**] [**accept** | **reject**] *listname*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute list** *listname*
4. **attribute** *value1* [*value2*[*value3* **...**]]
5. **aaa group server radius** *group-name*
6. Do one of the following:
   - **authorization** [**request** | **reply**][**accept** | **reject**] *listname*
   -
   -
   - **accounting** [**request** | **reply**] [**accept** | **reject**] *listname*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute list** *listname* **Example:** `Router (config)# radius-server attribute list attrlist`	Defines an attribute list.
Step 4	**attribute** *value1* [*value2*[*value3* **...**]] **Example:** `Router (config)# attribute 6-10, 12`	Adds attributes to an accept or reject list.
Step 5	**aaa group server radius** *group-name* **Example:** `Router (config)# aaa group server radius rad1`	Applies the attribute list to the AAA server group and enters server-group configuration mode.
Step 6	Do one of the following: • **authorization** [**request** | **reply**][**accept** | **reject**] *listname* • • • **accounting** [**request** | **reply**] [**accept** | **reject**] *listname* **Example:** `Router (config-sg-radius)# authorization request accept attrlist` **Example:** **Example:** **Example:**	Filters attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. • The **request** keyword defines filters for outgoing authorization Access Requests. • The **reply** keyword defines filters for incoming authorization Accept and Reject packets and for outgoing accounting requests.

	Command or Action	Purpose
	`Router (config-sg-radius)# accounting request accept attrlist`	

Configuring a Router to Support Downloadable Filters

To configure your router to support downloadable filters, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default group radius**
5. **radius-server attribute list** *list-name*
6. **attribute** *value1* [*value2* [*value3*...]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization template** **Example:** `Router (config)# aaa authorization template`	Enables usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF).
Step 4	**aaa authorization network default group radius** **Example:** `Router (config)# aaa authorization network default group radius`	Sets parameters that restrict user access to a network.
Step 5	**radius-server attribute list** *list-name* **Example:** `Router (config)# radius-server attribute list attlist`	Defines an accept or reject list name.

	Command or Action	Purpose
Step 6	**attribute** *value1* [*value2* [*value3...*]] **Example:** `Router (config)# attribute 10-14, 24`	Adds attributes to an accept or reject list.

Troubleshooting Tips

If attribute filtering is not working, ensure that the attribute list is properly defined.

Monitoring and Maintaining Attribute Filtering for Access Requests

To monitor and maintain attribute filtering, you can use the **debug radius**command.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS, including filtering information.

Configuration Examples for Attribute Filtering for Access Requests

Attribute Filtering for Access Requests Example

The following example shows that the attributes 30-31 that are defined in “all-attr” will be rejected in all outbound Access Request messages:

```
aaa group server radius ras
 server 172.19.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
!
```

```
.
.
.
radius-server attribute list all-attr
 attribute 30-31
!
.
.
.
```

Attribute Filtering User Profile Example

The following is a sample user profile after attribute filtering has been configured for Access Requests:

```
cisco.com Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Cisco:Cisco-Avpair = :1:"rad-serv=172.19.192.87 key rad123",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=authorization request reject range1",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=accounting request reject range1",
Cisco:Cisco-Avpair = "ppp-authen-type=chap"
Cisco:Cisco-Avpair = "ppp-authen-list=group 1",
Cisco:Cisco-Avpair = "ppp-author-list=group 1",
Cisco:Cisco-Avpair = "ppp-acct-list=start-stop group 1",
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
user2@cisco.com
Service-Type = Outbound,
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
```

When a session for user2@cisco.com “comes up” at the Layer 2 Tunneling Protocol (L2TP) Network Server (LNS)--as is shown above--because the **aaa authorization template** command has been configured, a RADIUS request is sent to the server for Cisco.com. The server then sends an Access Accept message if authentication is successful, along with the VSAs that are configured as part of the Cisco.com profile. If filters are configured as part of the Cisco.com profile, these filters will be parsed and applied to the RADIUS requests for user2@cisco.com.

In the above profile example, filter range1 has been applied to the authorization and accounting requests.

debug radius Command Example

If the attribute you are trying to filter is rejected, you will see an **debug radius** output statement similar to the following:

```
RADIUS: attribute 31 rejected
```

If you try to filter an attribute that cannot be filtered, you will see an output statement similar to the following:

```
RADIUS: attribute 1 cannot be rejected
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring RADIUS	Configuring RADIUS feature module.
Security commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None.	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

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

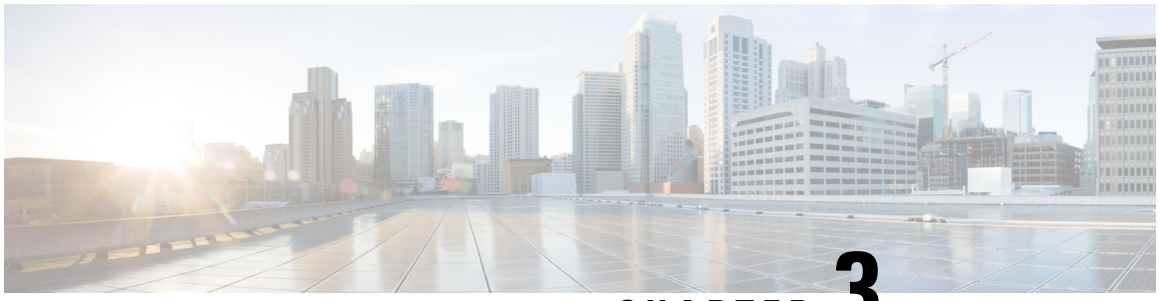
Feature Information for Attribute Screening for Access Requests

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

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

Table 1: Feature Information for Attribute Screening for Access Requests

Feature Name	Releases	Feature Information
Attribute Screening for Access Requests	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3S	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The Attribute Screening for Access Requests feature allows a network access server (NAS) to be configured to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. The following commands were introduced or modified by this feature: **authorization (server-group)**.



CHAPTER 3

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

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

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

Restrictions for 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. Router# **test aaa group** {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*]

DETAILED STEPS

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

	Command or Action	Purpose
	`Router# test aaa group radius secret new-code profile profilename1`	

Verifying the Enhanced Test Command Configuration

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

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

Configuration Examples 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 profl1
!
!
!
! 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                    [1]
         T=NAS-IP-Address[4]               L=06 V=10.0.1.81
```

```
*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	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. 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 Release 2.1 Cisco IOS XE Release 3.3S	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 In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified by this feature: **aaa attribute**, **aaa user profile**, **test aaa group.**

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.

Acct-Session-ID (attribute 44) --A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Class (attribute 25) --An accounting attribute. Arbitrary value that the network access server includes in all accounting packets for this user if the attribute is supplied by the RADIUS server.

L2F --Layer 2 Forwarding. 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.

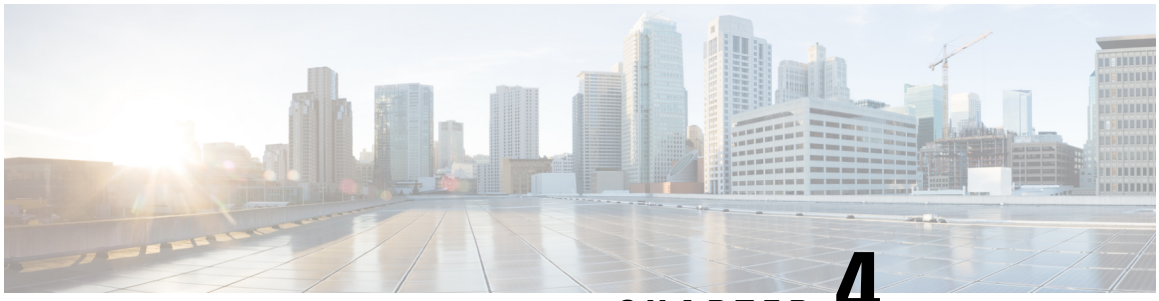
NAS --network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network).

NAS-IP Address (attribute 4) --Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.

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.

VPN --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.



CHAPTER 4

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 XE supported attributes.

Finding Feature Information

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

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

Prerequisites for Local AAA Server

The **aaa new-model**command must be issued in global configuration mode to enable AAA services before using this feature.

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 XE software. As such, it maintains its own local dictionary of all supported attributes.

Local AAA Attribute Support

You can configure your router so that AAA authentication and authorization attributes currently available on AAA servers are made available on existing Cisco IOS XE 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 XE 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. 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 XE AAA Format

You can use the **show aaa attributes protocol radius** command to get the Cisco IOS XE 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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa attribute list** *list-name* **Example:** `Device (config)# aaa attribute list TEST`	Defines a AAA attribute list.
Step 4	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Device (config-attr-list)# attribute type addr-pool poolname service ppp protocol ip`	Defines an IP address pool to use.
Step 5	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Device (config-attr-list)# attribute type ip-unnumbered loopbacknumber service ppp protocol ip`	Defines the loopback interface to use.
Step 6	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Device (config-attr-list)# attribute type vrf-id vrfname service ppp protocol ip`	Defines the virtual route forwarding (VRF) to use.
Step 7	**attribute type** {*name*} {*value*} **Example:** `Device (config-attr-list)# attribute type ppp-authen-list aaalistname`	Defines the AAA authentication list to use.
Step 8	**attribute type** {*name*} {*value*} **Example:** `Device (config-attr-list)# attribute type ppp-acct-list "aaa list name"`	Defines the AAA accounting list to use.

Defining a Subscriber Profile

To define a subscriber profile, perform the following steps.

Note RADIUS users should use the **show aaa attributes** command to map the RADIUS version of the particular attribute to the AAA version of the string attribute. See the example Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version Example.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber authorization enable**
4. **policy-map type service** *domain-name*
5. **service local**
6. **exit**
7. **aaa attribute list** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber authorization enable** **Example:** `Router (config)# subscriber authorization enable`	Enables subscriber authorization.
Step 4	**policy-map type service** *domain-name* **Example:** `Router (config)# policy-map type example.com`	Specifies the username domain that has to be matched and enters subscriber profile configuration mode.
Step 5	**service local** **Example:** `Router (subscriber-profile)# service local`	Specifies that local subscriber authorization should be performed.
Step 6	**exit** **Example:** `Router (subscriber-profile)# exit`	Exits subscriber profile configuration mode.
Step 7	**aaa attribute list** *list-name* **Example:** `Router (config)# aaa attribute list TEST`	Defines the AAA attribute list from which RADIUS attributes are retrieved.

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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa authentication** **Example:** `Device# debug aaa authentication`	Displays the methods of authentication being used and the results of these methods.
Step 3	**debug aaa authorization** **Example:** `Device# debug aaa authorization`	Displays the methods of authorization being used and the results of these methods.
Step 4	**debug aaa per-user** **Example:** `Device# debug aaa per-user`	Displays information about PPP session per-user activities.
Step 5	**debug radius** **Example:** `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 Loopback0" 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 XE software, it is better to use the explicit attribute instead of interface-configuration 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 ‘Loopback0’ service ppp protocol ip” instead of “attribute type interface-config ‘ip unnumbered Loopback0’ service ppp protocol lcp.”

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

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

```
Router# 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 XE AAA version of an attribute, which is defined in the “Name” field above.

Additional References

Related Document

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
None.	--

MIBs

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

RFCs

RFC	Title
None.	--

Technical Assistance

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

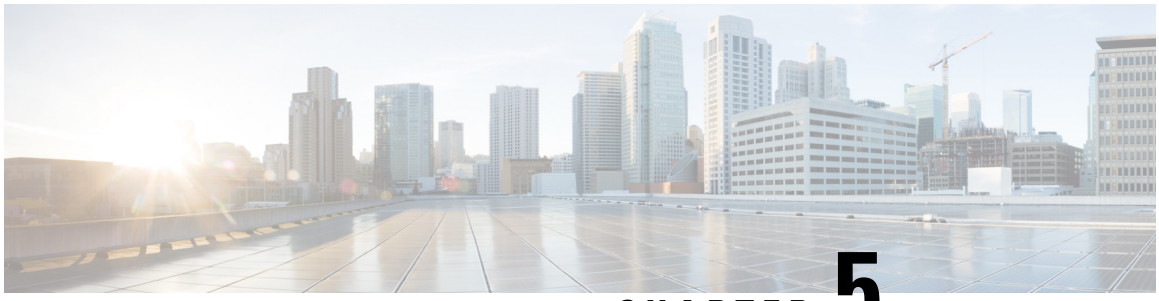
Feature Information for Local AAA Server

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Local AAA Server

Feature Name	Releases	Feature Information
Local AAA Server	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3S	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. 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 **attribute list**, **attribute type**



CHAPTER 5

Per-User QoS via AAA Policy Name

The Per-User QoS via AAA Policy Name feature provides the ability to download a policy name that describes quality of service (QoS) parameters for a user session from a RADIUS server and apply them for the particular session.

Finding Feature Information

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

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

Prerequisites for Per-User QoS via AAA Policy Name

Before you configure the Per-User QoS via AAA Policy Name feature, you must locally define on your router the policy whose name is received from the RADIUS server.

Information About Per-User QoS via AAA Policy Name

Effective with Cisco IOS XE Release 2.1, separate Cisco vendor-specific attributes (VSAs) are added for the service map.

VSAs Added for Per-User QoS via AAA Policy Name

Two new VSAs have been added for the service map, and the VSAs will bypass the parser while applying the policy for a particular user or session. The new VSAs are as follows:

- vendor-id=9 (Cisco) Vendor type 37 for upstream traffic to input policy name
- vendor-id=9 (Cisco) Vendor type 38 for downstream traffic to output policy name

Cisco AV Pairs for Policy-Maps

In Cisco IOS XE Release 2.1, the following two Cisco AV pairs for policy maps are defined at the ATM VC level:

- Cisco VSA attribute vc-qos-policy-in
- Cisco VSA attribute vc-qos-policy-out

These VSA attributes are formatted as:

- cisco-avpair = “atm:vc-qos-policy-in=<in policy name>”
- cisco-avpair = “atm:vc-qos-policy-out=<out policy name>”

In addition, two Cisco Generic RADIUS VSAs replace two others that do not correctly follow the Cisco VSA naming guidelines.

The two replacement VSAs are:

- cisco-avpair = “ip:sub-qos-policy-in=<in policy name>”
- cisco-avpair = “ip:sub-qos-policy-out=<out policy name>”

These VSAs should be used in place of the following outdated, generic VSAs:

- cisco-avpair = “ip:sub-policy-In=<in policy name>”
- cisco-avpair = “ip:sub-policy-Out=<out policy name>”

Note We recommend using the new VSAs. However, the replaced attributes are currently still supported.

How to Configure Per-User QoS via AAA Policy Name

To configure per-user QoS, use the authentication, authorization, and accounting (AAA) policy name that you have received from the RADIUS server.

Monitoring and Maintaining Per-User QoS via AAA Policy Name

To monitor and maintain per-user QoS using the AAA policy name, use the following **debug** commands:

SUMMARY STEPS

1. **enable**
2. **debug aaa authorization**
3. **debug aaa per-user**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays information about AAA/TACACS+ authorization.
Step 3	**debug aaa per-user** **Example:** `Router# debug aaa per-user`	Displays information about per-user QoS parameters.

Configuration Example for Per-User QoS via AAA Policy Name

The following example shows per-user QoS being configured using the AAA policy name “policy_class_1_2”:

```
!NAS configuration
class-map match-all class1
 match access-group 101
class-map match-all class2
 match qos-group 4
 match access-group 101
policy-map policy_class_1_2
 class class1
 bandwidth 3000
 queue-limit 30
 class class2
 bandwidth 2000
 class class-default
 bandwidth 500
!RADIUS Profile Configuration
peruser_qos_1    Password = "password1"
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Cisco:Cisco-avpair = "ip:sub-qos-policy-in=ssspolicy"
!ssspolicy in the above line is the name of the policy.
peruser_qos_2    Password = "password1"
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Cisco:Cisco-avpair = "ip:sub-qos-policy-out=ssspolicy”
```

Additional References

The following sections provide references related to the Per-User QoS via AAA Policy Name.

Related Documents

Related Topic	Document Title
AAA per-user and QoS configurations and information about the **policy-map** command	• Configuring Per-User Configuration • Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for Per-User QoS via AAA Policy Name

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 4: Feature Information for Per-User QoS via AAA Policy Name

Feature Name	Releases	Feature Information
Per-User QoS via AAA Policy Name	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3S	You can use the Per-User QoS via AAA Policy Name feature to download a policy name that describes QoS parameters for a user session from a RADIUS server and apply them for a particular session. In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

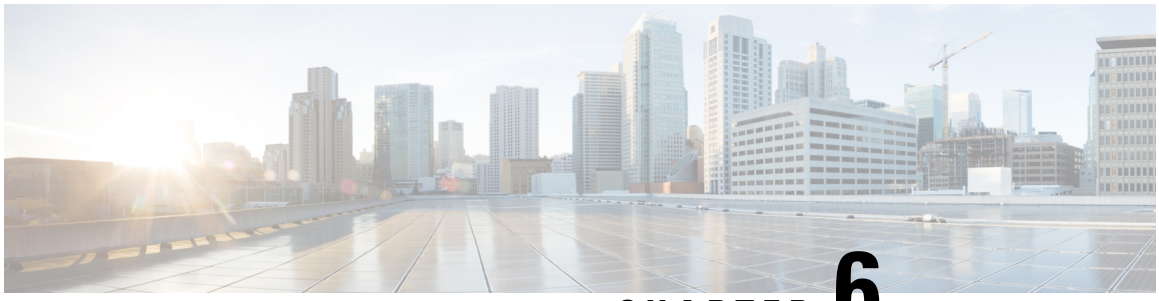
Glossary

RADIUS --Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

VSA --vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

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.



CHAPTER 6

RADIUS Timeout Set During Pre-Authentication

Some call sessions for Internet Service Provider (ISP) subscribers are billed through authentication, authorization, and accounting (AAA) messages in a prepaid time model. When these subscribers are preauthenticated, a RADIUS server checks for any remaining credit in the prepaid time model and sets a session timeout based on the credit available. The RADIUS Timeout Set During Pre-Authentication feature is useful in situations where the PPP authentication that follows the preauthentication phase of these call sessions does not return the Session-Timeout value (RADIUS attribute 27), and therefore allows the ISP to add call setup time to the subscriber's bill.

Finding Feature Information

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

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

Prerequisites for the RADIUS Timeout Set During Pre-Authentication Feature

- This feature is specific to RADIUS. Basic AAA authentication and preauthentication must be configured.
- Preauthentication and normal PPP authentication are required for legacy functionality.

Information About the RADIUS Timeout Set During Pre-Authentication Feature

RADIUS Attribute 27 and the PPP Authentication Phase

The RADIUS Timeout Set During Pre-Authentication feature was developed for ISPs that want to bill dial-in subscribers for call setup time and the entire duration of the call session. These subscribers are billed through AAA messages in a prepaid time model. When the subscribers are preauthenticated, a RADIUS server checks for any remaining credit in the prepaid time model and sets a session timeout (in minutes or seconds) based on the credit available. This time can range from a few seconds for ISDN users, to much longer for asynchronous dial-up subscribers.

Until the RADIUS Timeout Set During Pre-Authentication feature was developed, the value of RADIUS attribute 27, which is returned during the preauthentication phase of a call, was either ignored or overwritten during the PPP authentication phase. Even when the PPP authentication phase did not return a value for attribute 27, the old value obtained during the preauthentication phase was being ignored.

With the RADIUS Timeout Set During Pre-Authentication feature introduced for Cisco IOS Release 12.2(15)T, if the PPP authentication phase does not return a value for attribute 27, the old value that was returned during the preauthentication phase is saved and used to time out the session; attribute 27 is saved in a preauthentication database for future use. However, if the PPP authentication user profile has a session timeout configured and PPP authentication succeeds, the new value downloaded during PPP authentication overwrites the old attribute 27 value. By setting the session timeout value in the preauthentication phase itself, the service provider can bill the subscriber for the call setup time and the call duration.

How to Configure the RADIUS Timeout Set During Pre-Authentication Feature

No new configuration is required. The RADIUS Timeout Set During Pre-Authentication feature is included in all Cisco platforms that support preauthentication, and that have RADIUS attribute 27, Session-Timeout, specified in a preauthentication user profile.

Additional References

The following sections provide references related to the ACL Default Direction feature.

Related Documents

Related Topic	Document Title
Cisco IOS Dial Technologies configuration	*Cisco IOS Dial Technologies Configuration Guide,* Release 12.4T
Cisco IOS security configuration	*Cisco IOS Security Configuration Guide: Securing User Services,* Release 12.4T

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command Reference*
Configuring IP services	*Cisco IOS IP Addressing Services Configuration Guide* , Release 12.4T.

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial-In User Service (RADIUS)*

Technical Assistance

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

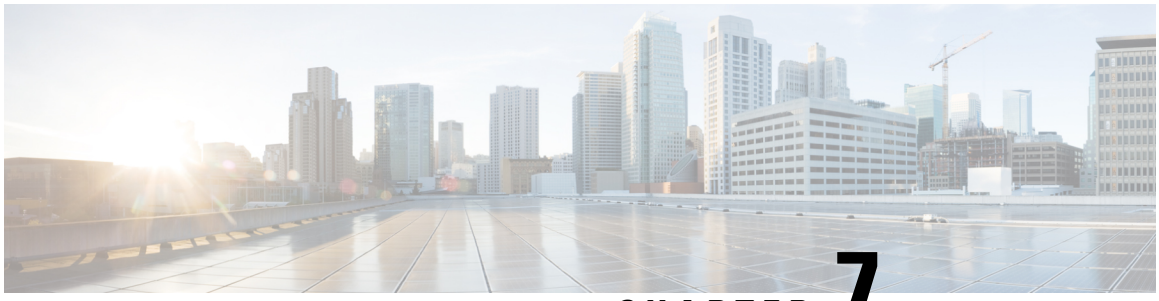
Feature Information for RADIUS Timeout Set During Pre-Authentication

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 5: Feature Information for RADIUS Timeout Set During Pre-Authentication

Feature Name	Releases	Feature Information
RADIUS Timeout Set During Pre-Authentication	Cisco IOS XE Release 3.9S	The RADIUS Timeout Set During Pre-Authentication feature is useful in situations where the PPP authentication that follows the preauthentication phase of these call sessions does not return the Session-Timeout value (RADIUS attribute 27), and therefore allows the ISP to add call setup time to the subscriber's bill.



CHAPTER 7

Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows tunnel authentication and authorization to occur through a remote RADIUS server instead of local configuration on the tunnel terminator. Thus, users no longer have to configure L2TP access concentrator (LAC) or Layer 2 Tunneling Protocol (L2TP) network server (LNS) data in a virtual private dialup network (VPDN) group when an LNS or LAC is configured for incoming dialin or dialout L2TP tunnel termination; this information can now be added to a remote RADIUS server, providing a more manageable and scalable solution for L2TP tunnel authentication and authorization on the tunnel terminator.

Finding Feature Information

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

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

Prerequisites for Tunnel Authentication via RADIUS on Tunnel Terminator

Before configuring this feature, you should define a RADIUS server group. For information on completing this task, refer to the chapter "Configuring RADIUS " in the *Cisco IOS Security Configuration Guide: Securing User Services*

Note The service-type in the RADIUS user's profile for the tunnel initiator should always be set to "Outbound."

Restrictions for Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature is applicable only to L2TP; that is, protocols such as (Layer 2 Forwarding) L2F and Point-to-Point Tunneling Protocol (PPTP) are not supported.

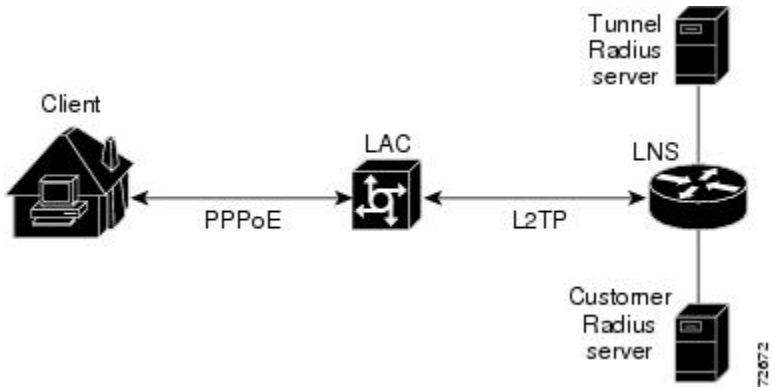
Information About Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows the LNS to perform remote authentication and authorization with RADIUS on incoming LAC dialin connection requests. This feature also allows the L2TP LAC to perform remote authentication and authorization with RADIUS on incoming L2TP LNS dialout connection requests.

Before the introduction of this feature, the LNS could only perform L2TP tunnel authentication and authorization locally. These processes can be difficult to maintain across numerous LNSs, especially if the number of VPDN groups is large, because the LAC information must be configured under the VPDN group configurations of the LNS. Remote RADIUS authentication and authorization allows users to store the LAC configurations on the RADIUS server, thereby avoiding the need to store information locally. Thus, the new LAC information can be added to the RADIUS server as necessary, and the group of LNSs can authenticate and authorize by using a common user database on RADIUS.

The figure below and the corresponding steps explain how this feature works.

Figure 1: LNS Remote RADIUS Tunnel Authentication and Authorization for L2TP Dialin Calls Topology



- After the LNS receives a start-control-connection request (SCCRQ), it starts tunnel authentication and submits a request to RADIUS with the LAC hostname and the dummy password "cisco." (If the LNS determines that authorization should be performed locally, it will search the VPDN group configurations.)

Note To change the dummy password, use the **vpdn tunnel authorization password** command.

- If the password sent by the LNS matches the password that is configured in the RADIUS server, the server will return attribute 90 (Tunnel-Client-Auth-ID) and attribute 69 (Tunnel-Password) after the LAC information is located. Otherwise, the RADIUS server replies back with an access-reject, and the LNS drops the tunnel.
- The LNS will check for the following attribute information from the RADIUS reply:
  - Attribute 90 (Tunnel-Client-Auth-ID), which is used as the LAC hostname. If this attribute does not match the LAC hostname, the tunnel will be dropped.
  - Attribute 69 (Tunnel-Password), which is used for the L2TP CHAP-like authentication shared secret. This attribute is compared against the LAC challenge attribute-value pair (AVP) that was received in the SCCRQ. If this attribute does not match the AVP, the tunnel will be dropped.
- If both attributes match, the L2TP tunnel will be established. Thereafter, you can proceed with PPP negotiation and authentication with the remote client.

Note PPP remote authentication is done to a potential different customer RADIUS server by a separate access-request/access-accept sequence. The tunnel authorization may be done by a different tunnel RADIUS server.

New RADIUS Attributes

To help implement this feature, the following two new Cisco-specific RADIUS attributes have been introduced:

- Cisco:Cisco-Avpair = "vpdn:dout-dialer = <LAC dialer number>"--Specifies which LAC dialer to use on the LAC for a dialout configuration.

- Cisco:Cisco-Avpair = “vpdn:vpdn-vtemplate = <vtemplate number>”--Specifies the virtual template number that will be used for cloning on the LNS for a dialin configuration. (This attribute is the RADIUS counterpart for the virtual-template under the vpdn-group configuration.)

How to Configure Tunnel Authentication via RADIUS on Tunnel Terminator

Configuring the LNS or LAC for Remote RADIUS Tunnel Authentication and Authorization

The following task is used to configure an LNS or LAC for incoming dialin or dialout L2TP tunnel termination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network** {**default** | *list-name*} *method1* [*method2...*]
4. **vpdn tunnel authorization network** {*method-list-name* | **default**}
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization network** {**default**	*list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	Defines an AAA authorization method list for network services.
Step 4	**vpdn tunnel authorization network** {*method-list-name*	**default**} **Example:**	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization.

	Command or Action	Purpose
	`Router(config)# vpdn tunnel authorization network mymethodlist`	• If the *list-name* argument was specified in the **aaa authorization** command, you use that list name here. • If the default keyword was specified in the **aaa authorization** command, you must choose that keyword, which specifies the default authorization methods that are listed with the **aaa authorization** command here.
Step 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* **Example:** `Router(config)# vpdn tunnel authorization virtual-template 10`	(Optional) Selects the default virtual template from which to clone virtual access interfaces.
Step 6	**vpdn tunnel authorization password** *password* **Example:** `Router(config)# vpdn tunnel authorization password cisco`	(Optional) Configures a "dummy" password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname. **Note** If this command is not enabled, the password will always be "cisco."

Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations

To verify that the L2TP tunnel is up, use the **show vpdn tunnel** command in EXEC mode. One tunnel and one session must be set up.

```
Router# show vpdn tunnel
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions VPDN Group
4571  61568 csidtw13 est    10.0.195.4      1701  1        ?
LocID RemID TunID Intf          Username               State  Last Chg
4     11    4571  Vi4.1         csidtw9@cisco.com       est    00:02:29
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
To verify that the AAA authorization RADIUS server is configured on the LNS and that the
LNS can receive attributes 90 and 69 from the RADIUS server, perform the following steps:
```

SUMMARY STEPS

1. Enable the **debug radius** command on the LNS.
2. Enable the **show logging**command on the LNS and ensure that "access-accept" is in the output and that attributes 90 and 69 can be seen in the RADIUS reply.

DETAILED STEPS

Step 1 Enable the **debug radius** command on the LNS.

Step 2 Enable the **show logging**command on the LNS and ensure that "access-accept" is in the output and that attributes 90 and 69 can be seen in the RADIUS reply.

Example:

```
00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept, len 81
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
00:32:56: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:32:56: RADIUS:  Tunnel-Medium-Type  [65]  6   00:IPv4                   [1]
00:32:56: RADIUS:  Tunnel-Client-Auth-I[90]  6   00:"csidtw13"
00:32:56: RADIUS:  Tunnel-Password     [69]  8   *
00:32:56: RADIUS:  Vendor, Cisco       [26]  29
00:32:56: RADIUS:   Cisco AVpair       [1]   23  "vpdn:vpdn-vtemplate=1"
```

Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations

To verify that the L2TP tunnel has been established and that the LNS can perform PPP negotiation and authentication with the remote client, perform the following steps:

SUMMARY STEPS

1. Enable the **debug ppp negotiation** and **debug ppp authentication** commands on LNS.
2. Enable the **show logging** command on LNS and observe that LNS receives a PPP CHAP challenge and then sends a PPP CHAP "SUCCESS" to the client.
3. After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the LNS has received LCP (IPCP) packets, and that negotiation is successful.

DETAILED STEPS

Step 1 Enable the **debug ppp negotiation** and **debug ppp authentication** commands on LNS.

Step 2 Enable the **show logging** command on LNS and observe that LNS receives a PPP CHAP challenge and then sends a PPP CHAP "SUCCESS" to the client.

Example:

```
00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1  Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection to established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4
```

Step 3 After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the LNS has received LCP (IPCP) packets, and that negotiation is successful.

Example:

```
00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 200.1.1.4
```

Configuration Examples for Tunnel Authentication via RADIUS on Tunnel Terminator

L2TP Network Server Configuration Example

The following example shows how to configure the LNS to enable remote RADIUS tunnel authentication and authorization:

```
! Define a RADIUS server group
aaa group server radius VPDN-group
 server 64.102.48.91 auth-port 1645 acct-port 1646
!
! RADIUS configurations only
aaa authorization network mymethodlist group VPDN-Group
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 10
```

RADIUS User Profile for Remote RADIUS Tunnel Authentication Example

The following are examples of RADIUS user profiles for the LNS to terminate L2TP tunnels from a LAC. In the first user profile, the final line is optional if the **vpdn tunnel authorization virtual-template** command is used. Also, the first RADIUS user profile is for L2TP dialin, and the second RADIUS user profile is for L2TP dialout.

The service-type in the RADIUS user's profile for the tunnel initiator should always be set to "Outbound."

```
csidtw13  Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw13",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"
csidtw1 Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw1",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:dout-dialer=2"
```

Additional References

The following sections provide references related to the Tunnel Authentication via RADIUS on Tunnel Terminator feature.

Related Documents

Related Topic	Document Title
VPNs	*Cisco IOS VPDN Configuration Guide* , Release 12.4T
RADIUS Attributes	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0.

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2868	RADIUS Attributes for Tunnel Protocol Support

Technical Assistance

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

Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator

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

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

Table 6: Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator

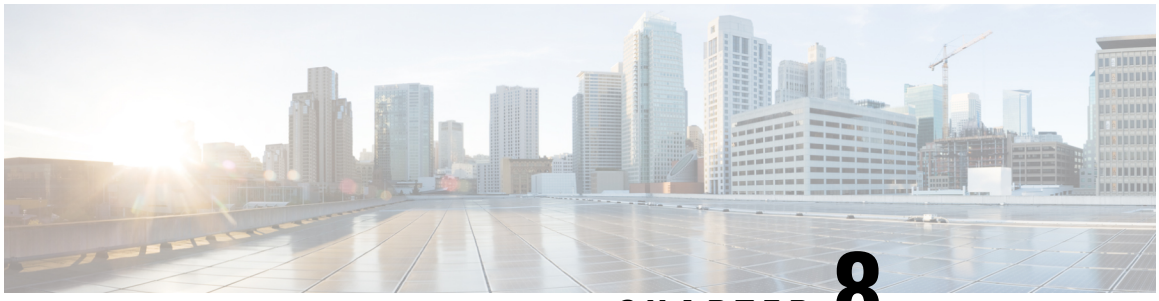
Feature Name	Releases	Feature Information
Tunnel Authentication via RADIUS on Tunnel Terminator	Cisco IOS XE Release 3.9S	The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows tunnel authentication and authorization to occur through a remote RADIUS server instead of local configuration on the tunnel terminator. The following commands were introduced or modified: **vpdn tunnel authorization network**, **vpdn tunnel authorization password**, **vpdn tunnel authorization virtual-template**.

Glossary

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.

LAC --L2TP access concentrator. A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

LNS --L2TP network server. A termination point for L2TP tunnels and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.



CHAPTER 8

ACL Default Direction

The ACL Default Direction feature allows the filter direction to be changed on the server (where the filter direction is not specified) to inbound packets (packets coming into the network) only.

Finding Feature Information

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

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

Prerequisites for ACL Default Direction

Before you can change the default direction of filters from RADIUS, you must perform the following tasks:

- Configure your network access server (NAS) for authentication, authorization, and accounting (AAA) and to accept incoming calls.

For more information, refer to the AAA chapters of the *Cisco IOS Security Configuration Guide: Securing User Services,* Release 12.4T and the *Cisco IOS Dial Technologies Configuration Guide,* Release 12.4T .

- Create a filter on your NAS.

For more information, see *Cisco IOS IP Addressing Services Configuration Guide* , Release 12.4T.

- Add a filter definition for a RADIUS user; for example, Filter-Id = “myfilter”.

Information About ACL Default Direction

The radius-server attribute 11 direction default Command

The **radius-server attribute 11 direction default** command allows you to change the default direction of filters for your ACLs via RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound--which stops traffic from entering a router, and reduces resource consumption--rather than keeping the outbound default direction, where filtering occurs only as the traffic is about to leave the network.

Benefits of ACL Default Direction

The ACL Default Direction feature allows you to change the default direction, which is outbound, of filters for your ACLs to inbound via the **radius-server attribute 11 direction default** command.

How to Configure ACL Default Direction

Configuring the ACL Default Direction from RADIUS via Attribute 11 Filter-Id

Perform this task to configure the default direction of filters from RADIUS via attribute 11.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 11 direction default** [**inbound** | **outbound**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 11 direction default** [**inbound** | **outbound**] **Example:**	Specifies the default direction of filters from RADIUS to inbound or outbound.

	Command or Action	Purpose
	`Router(config)# radius-server attribute 11 direction default inbound`	

Verifying the ACL Default Direction from RADIUS via Attribute 11 Filter-Id

Perform this task to verify the default direction of filters from RADIUS and to verify that RADIUS attribute 11 is being sent in access accept requests.

SUMMARY STEPS

1. **enable**
2. **more system:running-config**
3. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**more system:running-config** **Example:** `Router# more system:running-config`	Displays the contents of the current running configuration file.
Step 3	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS. The output of this command shows whether attribute 11 is being sent in access accept requests.

Configuration Examples for ACL Default Direction

Default Direction of Filters via RADIUS Attribute 11 Filter-Id Example

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

```
radius-server attribute 11 direction default inbound
```

RADIUS User Profile with Filter-Id Example

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "password1"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Filter-Id = "myfilter.out"
```

The RADIUS user profile shown in this example produces the following reply from the NAS:

```
RADIUS: Send to unknown id 79 10.51.13.4:1645, Access-Request, len 85
RADIUS: authenticator 84 D3 B5 7D C2 5B 70 AD - 1E 5C 56 E8 3A 91 D0 6E
RADIUS: User-Name           [1]   8  "client"
RADIUS: CHAP-Password       [3]   19  *
RADIUS: NAS-Port            [5]   6   20030
RADIUS: NAS-Port-Type       [61]  6   ISDN                      [2]
RADIUS: Called-Station-Id   [30]  6   "4321"
RADIUS: Calling-Station-Id  [31]  6   "1234"
RADIUS: Service-Type        [6]   6   Framed                    [2]
RADIUS: NAS-IP-Address      [4]   6   10.1.73.74
RADIUS: Received from id 79 10.51.13.4:1645, Access-Accept, len 46
RADIUS: authenticator 9C 6C 66 E2 F1 42 D6 4B - C1 7D D4 5E 9D 09 BB A1
RADIUS: Service-Type        [6]   6   Framed                    [2]
RADIUS: Framed-Protocol     [7]   6   PPP                       [1]
RADIUS: Filter-Id           [11]  14
RADIUS: 6D 79 66 69 6C 74 65 72 2E 6F 75 74             [myfilter.out]
```

Additional References

The following sections provide references related to the ACL Default Direction feature.

Related Documents

Related Topic	Document Title
Cisco IOS Dial Technologies configuration	*Cisco IOS Dial Technologies Configuration Guide,* Release 12.4T
Cisco IOS security configuration	*Cisco IOS Security Configuration Guide: Securing User Services,* Release 12.4T
Cisco IOS security commands	*Cisco IOS Security Command Reference*
Configuring IP services	*Cisco IOS IP Addressing Services Configuration Guide* , Release 12.4T.

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial-In User Service (RADIUS)*

Technical Assistance

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

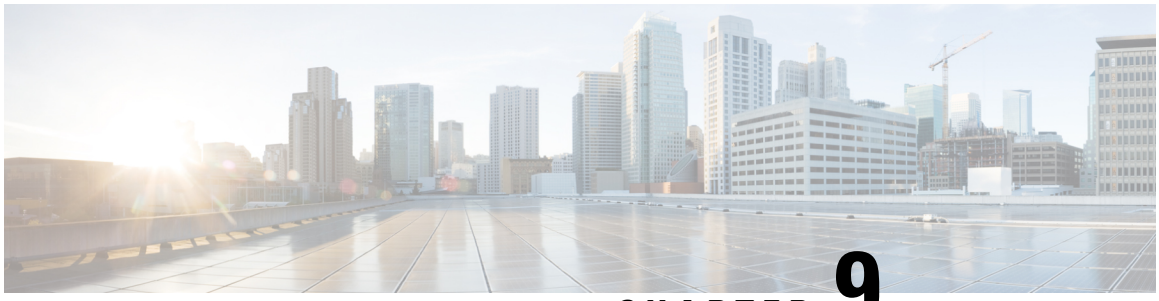
Feature Information for ACL Default Direction

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

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

Table 7: Feature Information for ACL Default Direction

Feature Name	Releases	Feature Information
ACL Default Direction	Cisco IOS XE Release 3.9S	The ACL Default Direction feature allows the filter direction to be changed on the server (where the filter direction is not specified) to inbound packets (packets coming into the network) only. The following command was introduced: **radius-server attribute 11 direction default**.



CHAPTER 9

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

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

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

Prerequisites for RADIUS 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 o f 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 8: 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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa accounting** **Example:** `Device# debug aaa accounting`	Displays information on accountable events as they occur.
Step 3	**show radius statistics** **Example:** `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	*Cisco IOS Security Command Reference*
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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	---

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: Feature Information for RADIUS Progress Codes

Feature Name	Releases	Feature Information
RADIUS Progress Codes	Cisco IOS XE Release 3.9S	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.

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.

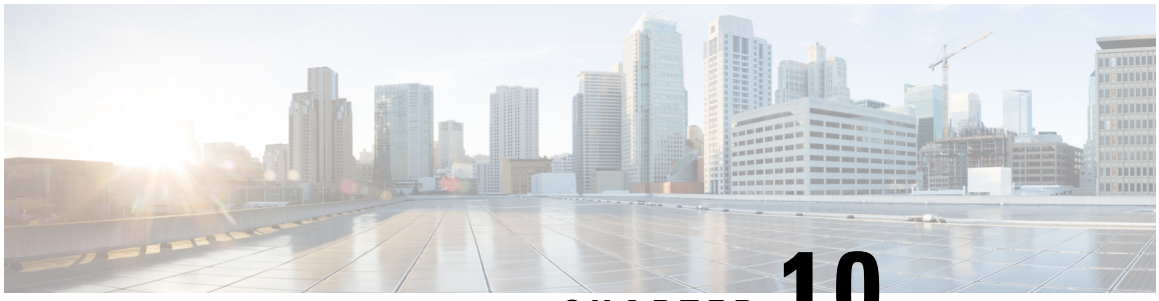
LCP --link control protocol. A protocol that establishes, configures, and tests data-link connections for use by PPP.

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.



CHAPTER 10

Offload Server Accounting Enhancement

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the offload server.

Although NASs can already synchronize information with an offload server, this feature extends the functionality to include a unique session-id, adding the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and Class (attribute 25) information collected by the NASs.

Finding Feature Information

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

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

Prerequisites

Before configuring the Offload Server Accounting Enhancement feature, you must perform the following tasks:

- Enable AAA. See the Configuring Authentication feature module for more information.
- Enable VPN. See the *Cisco IOS Security Configuration Guide: Secure Connectivity* , Release 12.4T for more information.

Information About Offload Server Accounting Enhancement

The Offload Server Accounting Enhancement feature allows users to configure their network access servers (NAS) to synchronize authentication and accounting information--NAS-IP-Address (attribute 4) and Class (attribute 25)--with the offload server.

An offload server interacts with a NAS through a Virtual Private Network (VPN) to perform required Point-to-Point Protocol (PPP) negotiation for calls. The NAS performs call preauthentication, whereas the offload server performs user authentication. T his feature allows the authentication and accounting data of the NAS to synchronize with the offload server as follows:

- During preauthentication, the NAS generates a unique session-id, adding the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and retrieves a Class attribute. The new session-id is sent in preauthentication requests and resource accounting requests; the Class attribute is sent in resource accounting requests.

Note Unique session-ids are needed when multiple NASs are being processed by one offload server.

- The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted to the offload server through Layer 2 Forwarding (L2F) options.
- The offload server includes the new, unique session-id in user access requests and user session accounting requests. The Class attribute that is passed from the NAS is included in the user access request, but a new Class attribute is received in the user access reply; this new Class attribute should be included in user session accounting requests.

How to Configure the Offload Server Accounting Enhancement

Configuring Unique Session IDs

To maintain unique session IDs among NASs, use the following global configuration command. When multiple NASs are being processed by one offload server, this feature must be enabled by all NASs and by the offload server to ensure a common and unique session-id.

Command	Purpose
`Router(config)# radius-server attribute 44 extend-with-addr`	Adds the accounting IP address in front of the existing AAA session ID. **Note** The unique session-id is different from other NAS session-ids because it adds the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address).

Configuring Offload Server to Synchronize with NAS Clients

To configure the offload server to synchronize accounting session information with the NAS clients, use the following global configuration command:

Command	Purpose
`Router(config)# radius-server attribute 44 sync-with-client`	Configures the offload server to synchronize accounting session information with the NAS clients.

Verifying Offload Server Accounting

To verify whether the NAS has synchronized authentication and accounting data with the offload server, use the following commands in privileged EXEC mode:

Command	Purpose
`Router# more system:running-config`	Displays the contents of the current running configuration file. (Note that the **more system:running-config** command has replaced the **show running-config** command.)
`Router(config)# debug radius`	Displays information associated with RADIUS. The output of this command shows whether attribute 44 is being sent in access requests. The output, however, does not show the entire value for attribute 44. To view the entire value for attribute 44, refer to your RADIUS server log.

Configuration Examples for the Offload Server Accounting Enhancement

Unique Session ID Configuration Example

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
radius-server attribute 44 extend-with-addr
```

Offload Server Synchronization with NAS Clients Example

The following example shows how to configure the offload server to synchronize accounting session information with NAS clients:

```
radius-server attribute 44 sync-with-client
```

Additional References

The following sections provide references related to the Offload Server Accounting Enhancement.

Related Documents

Related Topic	Document Title
Enable VPN	*Cisco IOS Security Configuration Guide: Secure Connectivity* , Release 12.4T.
Enable AAA	Configuring Authentication module.

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for Offload Server Accounting Enhancement

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

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

Table 10: Feature Information for Offload Server Accounting Enhancement

Feature Name	Releases	Feature Information
Offload Server Accounting Enhancement	Cisco IOS XE Release 3.9S	The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the offload server. The following commands were introduced or modified: **radius-server attribute 44 extend-with-addr**, **radius-server attribute 44 sync-with-client**

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.

Acct-Session-ID (attribute 44) --A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Class (attribute 25) --An accounting attribute. Arbitrary value that the network access server includes in all accounting packets for this user if the attribute is supplied by the RADIUS server.

L2F --Layer 2 Forwarding. 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.

NAS --network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network).

NAS-IP Address (attribute 4) --Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.

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.

VPN --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.