General RADIUS Configurations Configuration Guide Cisco IOS XE Release 2

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

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for 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.

Command or Action	Purpose

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:
`Router (config-sg-radius)# accounting request accept attrlist`
	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.

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

• Troubleshooting Tips, page 5

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.

Related Topic	Document Title
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	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)**.

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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.

	Command or Action	Purpose
Step 6	Router# **test aaa group** {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*] **Example:** `Router# test aaa group radius secret new-code profile profilename1`	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.

Verifying the Enhanced Test Command Configuration

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

Command	Purpose
`Router#` **debug radius**	Displays information associated with RADIUS.
`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.)

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	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

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

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

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

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for 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 Cisco IOS XE 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 Cisco IOS XE AAA interface format.

- Converting from RADIUS Format to Cisco IOS XE AAA Format, page 18

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*}
9. **attribute type** {*name*} {*value*}

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 attribute list** *list-name* **Example:** `Router (config)# aaa attribute list TEST`	Defines a AAA attribute list.
Step 4	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Router (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:** `Router (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:** `Router (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:** `Router (config-attr-list)# attribute type ppp-authen-list aaalistname`	Defines the AAA authentication list to use.

	Command or Action	Purpose
Step 8	**attribute type** {*name*} {*value*} **Example:** `Router (config-attr-list)# attribute type ppp-author-list aaalistname`	Defines the AAA authorization list to use.
Step 9	**attribute type** {*name*} {*value*} **Example:** `Router (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 Cisco IOS XE 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.

	Command or Action	Purpose
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 ppp authentication**
6. **debug ppp error**
7. **debug ppp forward**
8. **debug ppp negotiation**
9. **debug radius**
10. **debug sss error**

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 authentication** **Example:** `Router# debug aaa authentication`	Displays the methods of authentication being used and the results of these methods.
Step 3	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays the methods of authorization being used and the results of these methods.
Step 4	**debug aaa per-user** **Example:** `Router# debug aaa per-user`	Displays information about PPP session per-user activities.
Step 5	**debug ppp authentication** **Example:** `Router# debug ppp authentication`	Indicates whether a client is passing authentication.

	Command or Action	Purpose
Step 6	**debug ppp error** **Example:** `Router (config)# debug ppp error`	Displays protocol errors and error statistics that are associated with PPP connection negotiation and operation.
Step 7	**debug ppp forward** **Example:** `Router# debug ppp forward`	Displays who is taking control of a session.
Step 8	**debug ppp negotiation** **Example:** `Router# debug ppp negotiation`	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
Step 9	**debug radius** **Example:** `Router# debug radius`	Displays information about the RADIUS server.
Step 10	**debug sss error** **Example:** `Router# debug sss error`	Displays diagnostic information about errors that may occur during SSS call setup.

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	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**

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for 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. To configure QoS policy, refer to the How to Configure Per-User QoS via AAA Policy Name, page 30. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt11/dafprusr.htm

- Monitoring and Maintaining Per-User QoS via AAA Policy Name, page 30

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	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.