RADIUS Configurations Configuration Guide, Cisco IOS Release 15S

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

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 at the end of this module.

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.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 11 direction default** [**inbound** | **outbound**] **Example:** `Router(config)# radius-server attribute 11 direction default inbound`	Specifies the default direction of filters from RADIUS to inbound or outbound.

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.

	Command or Action	Purpose
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 1 Feature Information for ACL Default Direction

Feature Name	Releases	Feature Information
ACL Default Direction	12.2(4)T 12.2(28)SB 12.2(31)SB3	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. In Cisco IOS Release 12.2(4)T, this feature was introduced. In Cisco IOS Release 12.2(28)SB, this feature was integrated. In Cisco IOS Release 12.2(31)SB3, this feature was integrated. The following command was introduced: **radius-server attribute 11 direction default**.

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 at the end of this module.

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

To configure the attribute screening for access requests, perform the following steps.

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

Perform this task to configure your router to support downloadable filters.

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 13

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

The following sections provide references related to Attribute Filtering for Access Requests.

Related Documents

Related Topic	Document Title
Configuring RADIUS	Configuring RADIUS feature document.
Security commands	*Cisco IOS Security Command Reference*

Related Topic	Document Title
RADIUS attribute lists	RADIUS Attribute Screening feature document.

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
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 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 2 Feature Information for Attribute Screening for Access Requests

Feature Name	Releases	Feature Information
Attribute Screening for Access Requests	12.3(3)B 12.3(7)T 12.2(28)SB 12.2(33)SRC	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. In 12.3(3)B, this feature was introduced. This feature was integrated into Cisco IOS Release 12.3(7)T This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified by this feature: **authorization (server-group)**.

Enable Multilink PPP via RADIUS for Preauthentication User

The Enable Multilink PPP via RADIUS for Preauthentication User feature allows an administrator to selectively enable and disable Multilink PPP (MLP) negotiation for different users through RADIUS vendor-specific attribute (VSA) preauth:ppp-multilink=1 to the preauthentication profile.

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 at the end of this module.

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 Enable Multilink PPP via RADIUS for Preauthentication User

Before enabling MLP via RADIUS VSA preauth:ppp-multilink=1, you should perform the following tasks:

- Enable the network access server (NAS) to recognize and use VSAs as defined by RADIUS IETF attribute 26 by using the **radius-server vsa send** command.

For more information about using VSAs, refer to the section “Configuring Router to Use Vendor-Specific RADIUS Attributes” section of the Configuring RADIUS feature module.

- Enable preauthentication.

For information about configuring preauthentication, refer to the section “Configuring AAA Preauthentication ” section of the Configuring RADIUS feature module.

Information About the Enable Multilink PPP via RADIUS for Preauthentication User Feature

The Multilink PPP via RADIUS for Preauthentication User feature is enabled by configuring the **ppp multilink** command on an interface, but then this command enables MLP negotiation for all connections and users on that interface; that is, you cannot selectively enable or disable MLP negotiation for specific connections and users on an interface.

Note To enable this feature, the **ppp multilink** command should not be configured on the interface; this command disables MLP by default. If the **ppp multilink**command is already configured on the interface, the attribute “preauth:ppp-multilink=1” will not override this command.

How MLP via RADIUS Works

Because MLP parameters are negotiated at the time of link control protocol (LCP) negotiation, RADIUS VSA preauth:ppp-multilink=1 should only be a part of preauthentication user authorization. You should add this VSA to the preauthentication profile of the user to enable MLP. Thus, MLP will be enabled only for preauthentication users whose profiles contain this VSA; MLP will be disabled for all other users. If the MLP VSA is received during PPP user authorization (as opposed to preauthentication user authorization), it will be too late to negotiate MLP, and MLP will not be enabled.

When this VSA is received during preauthentication user authorization, MLP negotiation for the user is enabled. MLP is enabled when the VSA value is 1. All attribute values other than 1 are ignored.

Roles of the L2TP Access Server and L2TP Network Server

With this feature, you do not need to configure MLP on the interface of the L2TP access concentrator (LAC); during preauthentication user authorization, the LAC will selectively choose to enable MLP for preauthentication users who receive preauth:ppp-multilink=1. On the L2TP network server (LNS), you can control the maximum number of links allowed in the multilink bundle by sending RADIUS VSA multilink:max-links=n during PPP user authorization.

New Vendor-Specific Attributes

This feature introduces the following new VSAs:

- Cisco-AVpair = preauth:ppp-multilink=1

Turns on MLP on the interface and is applied to the preauthentication profile.

- Cisco-AVpair = multilink:max-links=n

Restricts the maximum number of links that a user can have in a multilink bundle and is used with the service=ppp attribute. The range of “n” is from 1 to 255.

- Cisco-AVpair = multilink:min-links=1

Sets the minimum number of links for MLP. The range of “n” is from 0 to 255.

- Cisco-AVpair = multilink:load-threshold=n

Sets the load threshold for the caller for which additional links are added or deleted from the multilink bundle. If the load exceeds the specified value, links are added; if the load drops below the specified value, links are deleted. This attribute is used with the service=ppp attribute. The range of “n” is from 1 to 255.

Note RADIUS VSAs multilink:max-links, multilink:min-links, and multilink:load-threshold serve the same purpose as TACACS+ per-user attributes, max-links, min-links, and load-threshold respectively.

Verifying MLP Negotiation via RADIUS in Preauthentication

To display bundle information for the MLP bundles, use the **show ppp multilink** EXEC command.

```
Router# show ppp multilink
Virtual-Access1, bundle name is mlpuser
  Bundle up for 00:00:15
  Dialer interface is Serial0:23
  0 lost fragments, 0 reordered, 0 unassigned
  0 discarded, 0 lost received, 1/255 load
  0x0 received sequence, 0x0 sent sequence
  Member links: 1 (max 7, min 1)
    Serial0:22, since 00:00:15, no frags rcvd
```

The table below describes the significant fields shown when MLP is enabled.

Table 3 show ppp multilink Field Descriptions

Field	Description
Virtual-Access1	Multilink bundle virtual interface.
Bundle	Configured name of the multilink bundle.
Dialer Interface is Serial0:23	Name of the interface that dials the calls.
1/255 load	Load on the link in the range 1/255 to 255/255. (255/255 is a 100% load.)
Member links: 1	Number of child interfaces.

Configuration Examples for Enable Multilink PPP via RADIUS for Preauthentication User

LAC for MLP Configuration Example

The following example is a sample configuration that can be used to configure a LAC for MLP via RADIUS:

```
! Enable preauthentication
aaa preauth
  group radius
  dnis required

!Enable VPDN
vpdn enable
!
vpdn-group 1
  request-dialin
  protocol l2tp
  dnis 56118
  initiate-to ip 10.0.1.22
  local name lac-router

! Don't need to configure multilink on the interface
! Multilink will be enabled by “ppp-multilink” attribute
interface Serial0:23
  ip address 15.0.1.7 255.0.0.0
  encapsulation ppp
  dialer-group 1
  isdn switch-type primary-5ess
  isdn calling-number 56118
  peer default ip address pool pool1
  no cdp enable
  ppp authentication chap
```

LAC RADIUS Profile for Preauthentication Example

The following example shows a LAC RADIUS profile for a preauthentication user who has applied the preauth:ppp-multilink=1 VSA:

```
56118   Password = “cisco”
        Service-Type = Outbound,
        Framed-Protocol = PPP,
        Framed-MTU = 1500,
        Cisco-Avpair = "preauth:auth-required=1",
        Cisco-Avpair = "preauth:auth-type=chap",
        Cisco-Avpair = "preauth:username=dnis:56118",
        Cisco-Avpair = "preauth:ppp-multilink=1"
```

LNS for MLP Configuration Example

The following example is a sample configuration that can be used to configure a LNS to limit the number of links in a MLP bundle:

```
! Enable VPDN
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol any
 virtual-template 1
```

```
 terminate-from hostname lac-router
 local name lns-router
!
! Configure multilink on interface
interface Virtual-Template 1
 ip unnumbered Ethernet 0/0
 ppp authentication chap
 ppp multilink
```

LNS RADIUS Profile Example

The following example shows a LNS RADIUS profile for specifying the maximum number of links in a multilink bundle. The following multilink VSAs should be specified during PPP user authorization.

```
mascot  password = "cisco"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Cisco-Avpair = "multilink:max-links=7"
        Cisco-Avpair = "multilink:min-links=1"
        Cisco-Avpair = "multilink:load-threshold=128"
```

Additional References

The following sections provide references related to the Enable Multilink PPP via RADIUS for Preauthentication User feature.

Related Documents

Related Topic	Document Title
RADIUS	Configuring RADIUS feature module.
Dial Technology	*Cisco IOS Dial Technologies Configuration Guid*e , Release 12.4T
RADIUS Attributes	RADIUS Attributes Overview and RADIUS IETF Attributes feature module.
TACACS+ Attributes	TACACS+ Attribute-Value Pairs feature 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
No new or modified RFCs are supported.	--

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 Enable Multilink PPP via RADIUS for Preauthentication User

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 Enable Multilink PPP via RADIUS for Preauthentication User

Feature Name	Releases	Feature Information
Enable Multilink PPP via RADIUS for Preauthentication User	12.2(11)T	The Enable Multilink PPP via RADIUS for Preauthentication User feature allows an administrator to selectively enable and disable Multilink PPP (MLP) negotiation for different users through RADIUS vendor-specific attribute (VSA) preauth:ppp-multilink=1 to the preauthentication profile. This feature was introduced in Cisco IOS Release 12.2(11)T.

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 that 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.

L2F --Layer 2 Forwarding. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

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.

MLP--Multilink PPP. MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either,

as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over synchronous and asynchronous serial and BRI and PRI types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

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.

VSA --Vendor-Specific Attribute. VSAs derived from one IETF attribute--vendor-specific (attribute 26). Attribute 26 allows a vendor to create and implement an additional 255 attributes. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26: essentially, Vendor-Specific = “protocol:attribute=value.”

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 at the end of this module.

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 Example for Enhanced Test Command

User Profile Associated With a test aaa group command Example

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

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile 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
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 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 5 Feature Information for Enhanced Test Command

Feature Name	Releases	Feature Information
Enhanced Test Command	Cisco IOS XE Release 3.3SG	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. The following commands were introduced or modified: **aaa attribute**, **aaa user profile**, and **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.

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.

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.

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 at the end of this module.

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 6 Feature Information for Offload Server Accounting Enhancement

Feature Name	Releases	Feature Information
Offload Server Accounting Enhancement	12.2(4)T 12.2(28)SB 12.2(33)SRC	The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the offload server. This feature was introduced in Cisco IOS Release 12.2(4)T. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRC. 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.

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.

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.

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 at the end of this module.

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.

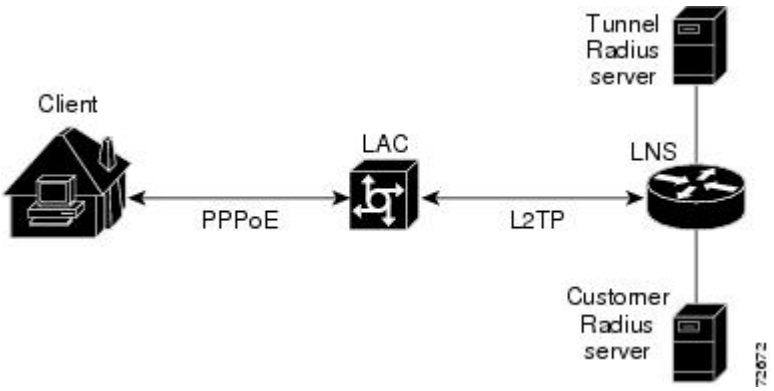
Information About Tunnel Authentication via RADIUS on Tunnel Terminator

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, page 43

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, page 44
- Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations, page 45
- Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations, page 46

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:** `Router(config)# vpdn tunnel authorization network mymethodlist`	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization. • 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.

	Command or Action	Purpose
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 7 Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator

Feature Name	Releases	Feature Information
Tunnel Authentication via RADIUS on Tunnel Terminator	12.2(15)B 12.3(4)T	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. In 12.2(15)B, this feature was introduced on the Cisco 6400 series, Cisco 7200 series, and Cisco 7400 series. In 12.3(4)T, this feature was integrated into the Cisco IOS. 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.