Enable Multilink PPP via RADIUS for Preauthentication User

Last Updated: January 15, 2012

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 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 Enable Multilink PPP via RADIUS for Preauthentication User

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- 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 1 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.)

Field	Description
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 2 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.”