



Enable Multilink PPP via RADIUS for Preauthentication User

First Published: 12.2(11)T
Last Updated: February 28, 2006

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

History for the Enable Multilink PPP via RADIUS for Preauthentication User Feature

Release	Modification
12.2(11)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 4](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 7](#)



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

© 2001, 2005–2006 Cisco Systems, Inc. All rights reserved.

Feature Overview

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

You can enable MLP 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 will disable 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 server (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.

Benefits

Selective Multilink PPP Configuration

MLP negotiation can be selectively enabled and disabled for different users by applying RADIUS VSA preauth:ppp-multilink=1 to the preauthentication profile.

Prerequisites

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” of the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

- Enable preauthentication.

For information about configuring preauthentication, refer to the section “Configuring AAA Preauthentication” of the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

None

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
```

Table 1 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.)
Member links: 1	Number of child interfaces.

Configuration Examples

This section provides dialin VPDN configurations using Cisco VSA ppp-multilink examples:

- [LAC for MLP Configuration: Example](#)
- [LAC RADIUS Profile for Preauthentication: Example](#)
- [LNS for MLP Configuration: Example](#)
- [LNS RADIUS Profile: Example](#)

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 10.0.1.7 255.0.0.0
  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 Attributes	<ul style="list-style-type: none"> “RADIUS Attributes” appendix in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.4
TACACS + Attribute-Value Pairs	<ul style="list-style-type: none"> “TACACS + Attribute-Value Pairs” appendix in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.4
Configuring Radius	<ul style="list-style-type: none"> “Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.4
Dial Technologies	<ul style="list-style-type: none"> <i>Cisco IOS Dial Technologies Command Reference</i>, Release 12.4T

Standards

Standard	Title
None	—

MIBs

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

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

None

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.”

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2001, 2005–2006 Cisco Systems, Inc. All rights reserved.