



RADIUS Logical Line ID

First Published: November 25, 2002
Last Updated: December 5, 2006

The RADIUS Logical Line ID feature, also known as the LLID Blocking feature, enables users to track their customers on the basis of the physical lines on which the calls of the customers originate. Thus, users can better maintain the profile database of their customers as the customers move from one physical line to another.

This feature provides users with a virtual port that will not change as customers move. Thus, the Logical Line Identification (LLID) can also be used for additional security checks.

History for the RADIUS Logical Line ID Feature

Release	Modification
12.2(13)T	This feature was introduced.
12.2(15)B	This feature was integrated into Cisco IOS Release 12.2(15)B.
12.3(14)YM1	This feature was integrated into Cisco IOS Release 12.3(14)YM1, and the send username keyword was added to the subscriber access command.
12.4(2)T	This feature was integrated into Cisco IOS Release 12.4(2)T.
12.3(14)YM2	This feature was integrated into Cisco IOS Release 12.3(14)YM2.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This feature was integrated into Cisco IOS Release 12.2(31)SB2.

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

- [Restrictions for RADIUS Logical Line ID, page 2](#)



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

© 2002–2003, 2005–2006 Cisco Systems, Inc. All rights reserved.

- [Information About RADIUS Logical Line ID, page 2](#)
- [How to Configure RADIUS Logical Line ID, page 3](#)
- [Configuration Examples for RADIUS Logical Line ID, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)

Restrictions for RADIUS Logical Line ID

RADIUS Server Compatibility

Although this feature can be used with any RADIUS server, some RADIUS servers may require modifications to their dictionary files to allow the Calling-Station-ID attribute to be returned in Access-Accept messages. For example, the Merit RADIUS server will not support LLID downloading unless you modify its dictionary as follows: “ATTRIBUTE Calling-Station-Id 31 string (*, *)”

Support Restrictions

- This feature supports only RADIUS; TACACS+ is not supported.
- This feature can be applied only toward PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN) (Dot1Q) calls; no other calls, such as ISDN, can be used.

Information About RADIUS Logical Line ID

Background: RADIUS Logical Line ID

The RADIUS Logical Line ID feature enables users to track their customers on the basis of the physical lines in which the calls of the customers originate. Thus, users can better maintain the profile database of their customers as the customers move from one physical line to another.

LLID is an alphanumeric string (which must be a minimum of one character and a maximum of 253 characters) that is a logical identification of a subscriber line. LLID is maintained in a customer profile database on a RADIUS server. When the customer profile database receives a preauthorization request from the access router, the RADIUS server sends the LLID to the router as the Calling-Station-ID attribute (attribute 31).

The Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sends a preauthorization request to the customer profile database when the LAC is configured for preauthorization. Configure the LAC for preauthorization using the **subscriber access** command.



Note

Downloading the LLID is referred to as “preauthorization” because it occurs before either service (domain) authorization or user authentication and authorization occur.

The customer profile database on the RADIUS server consists of user profiles for each physical network access server (NAS) port that is connected to the router. Each user profile contains a profile matched to a username (attribute 1) representing the physical port on the router. When the router is configured for preauthorization, it queries the customer profile database using a username representative of the physical

NAS port making the connection to the router. When a match is found in the customer profile database, the customer profile database returns an Access-Accept message containing the LLID in the user profile. The LLID is defined in the Access-Accept record as the Calling-Station-ID attribute.

The preauthorization process can also provide the real username being used for authentication to the RADIUS server. Because the physical NAS port information is being used as the username (attribute 1), RADIUS attribute 77 (Connect-Info) can be configured to contain the authentication username. This configuration allows the RADIUS server to provide additional validation on the authorization request if it chooses, such as analyzing the username for privacy rules, before returning an LLID back to the router.

Benefits

Stability and Security

This feature provides users with a virtual port that will not change as customers move. Thus, the LLID can also be used for additional security checks.

How to Configure RADIUS Logical Line ID

See the following sections for configuration tasks for the RADIUS Logical Line ID feature. Each task in the list is identified as either required or optional.

- [Configuring Preauthorization, page 3](#) (required)
- [Configuring the LLID in a RADIUS User Profile, page 4](#) (required)
- [Verifying Logical Line ID, page 6](#) (optional)

Configuring Preauthorization

To download the LLID and configure the LAC for preauthorization, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **subscriber access** {pppoe | pppoa} **pre-authorize nas-port-id** [default | *list-name*][**send username**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ip radius source-interface interface-name</code> Example: Router (config)# ip radius source-interface Loopback1	Specifies the IP address portion of the username for the preauthorization request.
Step 4	<code>subscriber access {pppoe pppoa} pre-authorize nas-port-id [default list-name] [send username]</code> Example: Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username	Enables the LLID to be downloaded so the router can be configured for preauthorization. The send username option specifies that you include the authentication username of the session inside the Connect-Info (attribute 77) in the Access-Request message.

Configuring the LLID in a RADIUS User Profile

To configure the user profile for preauthorization, add a NAS port user to the customer profile database and add RADIUS Internet Engineering Task Force (IETF) attribute 31 (Calling-Station-ID) to the user profile.

SUMMARY STEPS

1. UserName=nas_port: ip-address:slot/module/port/vpi.vci
2. UserName=nas-port: ip-address:slot/module/port/vlan-id
3. Calling-Station-Id = "string (*,*)"

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>UserName=nas_port: ip-address:slot/module/port/vpi.vci</code>	(Optional) Adds a PPPoE over ATM NAS port user.
Step 2	<code>User-Name=nas-port: ip-address:slot/module/port/vlan-id</code>	(Optional) Adds a PPPoE over VLAN NAS port user.
Step 3	<code>Calling-Station-Id = "string (*,*)"</code>	Adds attribute 31 to the user profile. <ul style="list-style-type: none">• String—One or more octets, containing the phone number from which the user placed the call.

Verifying Logical Line ID

To verify feature functionality, perform the following steps.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug radius Example: Router# debug radius	Checks to see that RADIUS attribute 31 is the LLID in the Accounting-Request on LAC and in the Access-Request and Accounting-Request on the LNS.

Configuration Examples for RADIUS Logical Line ID

This section provides the following configuration examples:

- [LAC for Preauthorization Configuration: Example, page 6](#)
- [RADIUS User Profile for LLID: Example, page 7](#)

LAC for Preauthorization Configuration: Example

The following example shows how to configure your LAC for preauthorization by downloading the LLID:

```

aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization cfg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2

```

```

request-dialin
protocol l2tp
domain water.com
domain water.com#184
initiate-to ip 10.1.1.1
local name s7200_2
l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
accept dialin
  protocol pppoe
  virtual-template 1
!
! Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.1.1.8 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
 pvc 1/100
 encapsulation aal5snap
 protocol pppoe
!
interface virtual-templatel
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1

```

RADIUS User Profile for LLID: Example

The following example shows how to configure the user profile for LLID querying for PPPoEoVLAN and PPPoEoATM and how to add attribute 31:

```

pppoeovlan
-----
nas-port:10.1.0.3:6/0/0/0 Password = "cisco",
  Service-Type = Outbound,
  Calling-Station-ID = "cat-example"

pppoeoa
-----
nas-port:10.1.0.3:6/0/0/1.100 Password = "cisco",
  Service-Type = Outbound,
  Calling-Station-ID = "cat-example"

```

Additional References

The following sections provide references related to RADIUS Logical Line ID.

Related Documents

Related Topic	Document Title
AAA authentication	“Configuring AAA Preauthentication” section in the “Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Attribute screening for access requests	“RADIUS Attribute Screening” section in the “Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Broadband access: PPP and routed bridge encapsulation	“Configuring Broadband Access: PPP and Routed Bridge Encapsulation” chapter in the <i>Cisco IOS Wide-Area Networking Configuration Guide</i> , Release 12.2
Dial technologies	<i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4

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 Technical Support & Documentation 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

This section documents modified commands only.

- [subscriber access](#)

subscriber access

To configure a network access server (NAS) to enable Subscriber Service Switch (SSS) to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name, use the **subscriber access** command in global configuration mode. To disable SSS preauthorization, use the **no** form of this command.

```
subscriber access {pppoe | pppoa} pre-authorize nas-port-id [default | list-name] [send
username]
```

```
no subscriber access {pppoe | pppoa} pre-authorize nas-port-id
```

Syntax Description

pppoe	Specifies PPP over Ethernet (PPPoE).
pppoa	Specifies PPP over ATM (PPPoATM).
pre-authorize nas-port-id	Signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name.
default	(Optional) Uses the default method list name instead of the named <i>list-name</i> argument.
<i>list-name</i>	(Optional) Authentication, authorization, and accounting (AAA) authorization configured on the LAC.
send username	(Optional) Specifies to send the authentication username of the session in the Change_Info attribute (attribute 77).

Defaults

Preauthorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced on the Cisco 6400 series, the Cisco 7200 series, and the Cisco 7401 Application Specific Router (ASR).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and the pppoe and pppoa keywords were added.
12.4(2)T	The send username keyword was added.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The NAS-Port-ID string is used to locate the first service record, which may contain one of three attributes, as follows:

- A restricted set of values for the domain substring of the unauthenticated PPP name.
This filtered service key then locates the final service. See the **vpdn authorize domain** command for more information.
- PPPoE session limit.
- The logical line ID (LLID).

Once NAS port authorization has taken place, normal authorization, which is usually the domain authorization, continues.

Logical Line ID

The LLID is an alphanumeric string of 1 to 253 characters that serves as the logical identification of a subscriber line. The LLID is maintained in a RADIUS server customer profile database and enables users to track their customers on the basis of the physical lines on which customer calls originate.

Downloading the LLID is also referred to as “preauthorization” because it occurs before normal virtual private dialup network (VPDN) authorization downloads layer two tunnel protocol (L2TP) information.

This command enables LLID and SSS querying only for PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN or Dot1Q) calls; all other calls, such as ISDN, are not supported.

Per-NAS-Port Session Limits for PPPoE

Use this command to configure SSS preauthorization on the L2TP Access Concentrator (LAC) so that the PPPoE per-NAS-port session limit can be downloaded from the customer profile database. To use PPPoE per-NAS-port session limits, you must also configure the PPPoE Session-Limit per NAS-Port Cisco attribute-value pair in the user profile.

Examples

The following example signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to sessions that have a PPPoE access type.

```
aaa new-model
aaa group server radius sg-llid
  server 172.20.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg-group
  server 172.20.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization cfg-commands
aaa authorization network default group sg-group
aaa authorization network mlist_llid group sg-llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg-group password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol l2tp
  domain group.com
  initiate-to ip 10.1.1.1
  local name s7200-2
!
vpdn-group 3
```

```

accept dialin
  protocol pppoe
  virtual-template 1
!
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist-llid
!
interface Loopback0
  ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
  ip address 10.2.2.2 255.255.255.0 secondary
  ip address 10.0.58.111 255.255.255.0
  no cdp enable
!
interface ATM4/0
  no ip address
  no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
  pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
  no ip unnumbered Loopback0
  no peer default ip address
  ppp authentication chap
!
radius-server host 172.20.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.20.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1

```

The following example is identical to the previous example except that it also adds support for sending the PPP authenticating username with the preauthorization in the Connect-Info attribute. This example also includes command-line interface (CLI) suppression on the LLID if the username that is used to authenticate has a domain that includes #184.

```

aaa new-model
aaa group server radius sg-llid
  server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg-group
  server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group sg-group
aaa authorization network mlist-llid group sg-llid
aaa session-id common
!
username s7200-2 password 0 lab
username s5300 password 0 lab
username sg-group password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol l2tp
  domain domain1.com
  domain domain1.com#184

```

```

initiate-to ip 10.1.1.1
local name s7200-2
l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
accept dialin
procotol pppoe
virtual-template 1
!
subscriber access pppoe pre-authorize nas-port-id mlist-llid send username
!

```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
l2tp attribute clid mask-method	Configures a NAS to provide L2TP calling line ID suppression for calls belonging to a VPDN group.
subscriber authorization enable	Enables SSS type authorization.
vpdn authorize domain	Enables domain preauthorization on a NAS.
vpdn l2tp attribute clid mask-method	Configures a NAS to provide L2TP calling line ID suppression globally on the router.

Glossary

LLID Blocking—A feature that enables users to track their customers on the basis of the physical lines on which the calls of the customers originate. Also known as RADIUS Logical Line ID.

RADIUS Logical Line ID—A feature that enables users to track their customers on the basis of the physical lines on which the calls of the customers originate. Also known as LLID Blocking.



Note

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

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.

© 2002–2003, 2005–2006 Cisco Systems, Inc. All rights reserved.