



L2TP Calling Station ID Suppression

When a Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) connects to an L2TP network server (LNS), the LAC transfers numerous attribute-value pairs as part of the session setup process. One of these attribute-value pairs is the Calling Station ID (L2TP AVP 22). The Calling Station ID provides detailed information about the originator of the session, such as the phone number of the originator, the Logical Line ID (LLID) used to make the connection on the LAC, or the MAC address of the PC connecting to the network. However, the Calling Station ID can be considered to be sensitive information in cases where the LAC and LNS are being managed by different entities. Therefore, depending on security requirements of the LAC or end users, it may be necessary for the LAC to suppress parts or all of the Calling Station ID.

Management of L2TP tunnels and sessions is available through router command-line interface (CLI) configuration commands or through the use of RADIUS vendor-specific attributes (VSAs) via authorization responses. This feature provides commands using both methods that allow you to mask parts or remove completely the Calling Station ID. Calling station ID suppression will be done on any Calling Station ID seen by L2TP when it sends it to an LNS via L2TP AVP 22 for any sessions matching the required criteria.

History for the L2TP Calling Station ID Suppression Feature

Release	Modification
12.3(14)YM1	This feature was introduced.
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.

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.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for L2TP Calling Station ID Suppression, page 2](#)
- [How to Configure L2TP Calling Station ID Suppression, page 2](#)
- [Configuration Examples for L2TP Calling Station ID Suppression, page 6](#)
- [Additional References, page 11](#)
- [Command Reference, page 11](#)

Prerequisites for L2TP Calling Station ID Suppression

This feature is enabled on the LAC. Before proceeding, a basic LAC setup should be configured on the router. For an example configuration, see the “Layer 2 Tunnel Protocol” chapter of the *Cisco 6400 Feature Guide*, Release 12.3 at http://www.cisco.com/en/US/products/hw/routers/ps314/products_feature_guide_chapter09186a00801bf067.html

How to Configure L2TP Calling Station ID Suppression

This section contains the following procedures:

- [Configuring L2TP Calling Station ID Suppression for Local Authorization, page 2](#)
- [Configuring L2TP Calling Station ID Suppression As a Global Router Authorization Setting, page 4](#)
- [Configuring L2TP Calling Station ID Suppression with RADIUS Domain Authorization, page 6](#)

Configuring L2TP Calling Station ID Suppression for Local Authorization

To configure L2TP Calling Station ID suppression on a virtual private dial-up network (VPDN) group for local authorization to mask characters in the L2TP calling line ID, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. **vpdn-group** *name*
5. **request-dialin**
6. **protocol** *protocol-name*
7. **domain** *domain-name*
8. **domain** *domain-name*
9. **initiate-to ip** *address*
10. **local name** *name*

11. `l2tp tunnel password password`

12. `l2tp attribute clid mask-method {right mask-character bytes | remove} [match match-string]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters configuration mode.
Step 3	<code>vpdn enable</code> Example: Router (config)# vpdn enable	Enables VPDN and informs the router to look for tunnel definitions from an LNS.
Step 4	<code>vpdn-group name</code> Example: Router (config)# vpdn-group L2TP	Enters VPDN configuration mode and defines a local group identifier for which other VPDN variables can be assigned.
Step 5	<code>request-dialin</code> Example: Router (config-vpdn)# request-dialin	Enables the router to request a dial-in tunnel and enters request dial-in VPDN subgroup configuration mode.
Step 6	<code>protocol protocol-name</code> Example: Router(config-vpdn-req-in)# protocol l2tp	Specifies the protocol; in the example, specifies Layer 2 Tunnel Protocol.
Step 7	<code>domain domain-name</code> Example: Router (config-vpdn-req-in)# domain cisco.com	Initiates a tunnel based on the client-supplied domain name; in the example, this domain name is cisco.com.
Step 8	<code>domain domain-name</code> Example: Router (config-vpdn-req-in)# domain cisco.com#184	Initiates a tunnel based on the client-supplied domain name; in the example, this domain name is cisco.com#184.
Step 9	<code>initiate-to ip address</code> Example: Router (config-vpdn)# initiate-to ip 192.168.1.4	Specifies the LNS IP address.

	Command or Action	Purpose
Step 10	<p>local name <i>name</i></p> <p>Example: Router (config-vpdn)# local name flets</p>	Specifies the username used by LNS to authenticate the tunnel.
Step 11	<p>l2tp tunnel password <i>password</i></p> <p>Example: Router (config-vpdn)# l2tp tunnel password 0 cisco</p>	Specifies the password used by the LNS to authenticate the tunnel.
Step 12	<p>l2tp attribute clid mask-method remove [match <i>match-string</i>]</p> <p>or</p> <p>l2tp attribute clid mask-method right <i>mask-character bytes</i> [match <i>match-string</i>]</p> <p>Example: Router (config-vpdn)# l2tp attribute clid mask-method remove</p> <p>or</p> <p>Example: Router (config-vpdn)# l2tp attribute clid mask-method right # 5 match %321</p>	<p>Removes or masks the Calling Station ID from the L2TP attribute-value pairs sent to the LNS.</p> <ul style="list-style-type: none"> • The right keyword masks the Calling Station ID starting from the right side, using the specified <i>mask-character</i> for the defined number of <i>bytes</i>. • The remove keyword removes the Calling Station ID. • The match option removes or masks only when the username contains the <i>match-string</i> as part of the username. This option is useful when supporting username extensions that trigger privacy options. <p>In the second example, the LAC masks AVP 22 with the pound sign (#) for the last 5 bytes, if and only if the username contains the string <i>%321</i>. Thus, the Calling Station ID for a user <i>anyuser@cisco.com</i> would not be masked, but the Calling Station ID for user <i>anyuser@cisco.com%321</i> would be masked.</p>

Configuring L2TP Calling Station ID Suppression As a Global Router Authorization Setting

To globally configure a LAC router to remove the L2TP calling line ID, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. **vpdn l2tp attribute clid mask-method remove** [**match** *match-string*]
or
vpdn l2tp attribute clid mask-method right *mask-character bytes* [**match** *match-string*]
5. **vpdn search-order domain**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>vpdn enable</p> <p>Example: Router (config)# vpdn enable</p>	<p>Enables VPDN and informs the router to look for tunnel definitions from an LNS.</p>
Step 4	<p>vpdn l2tp attribute clid mask-method remove [match <i>match-string</i>]</p> <p>or</p> <p>vpdn l2tp attribute clid mask-method right <i>mask-character bytes</i> [match <i>match-string</i>]</p> <p>Example: Router (config)# vpdn l2tp attribute clid mask-method remove</p> <p>or</p> <p>Example: Router (config)# vpdn l2tp attribute clid mask-method right # 6 match %321</p>	<p>Removes or masks the Calling Station ID from the L2TP attribute-value pairs sent to the LNS.</p> <ul style="list-style-type: none"> The remove keyword removes the Calling Station ID. The right keyword masks the Calling Station ID starting from the right side, using the specified <i>mask-character</i> for the defined number of <i>bytes</i>. The match option removes or masks only when the username contains the <i>match-string</i> as part of the username.
Step 5	<p>vpdn search-order domain</p> <p>Example: Router (config)# vpdn search-order domain</p>	<p>Specifies a search order.</p> <p>You can specify the search by configured ingress tunnel name (multihop-hostname), domain, or dialed number identification service (DNIS). The order in which you specify the command controls the order of the resulting search.</p>

Configuring L2TP Calling Station ID Suppression with RADIUS Domain Authorization

To configure a RADIUS server to “tell” the LAC router to mask or remove the L2TP calling line ID, add an attribute to the domain authorization response with the following format:

Cisco-Avpair = vpdn:l2tp-clid-mask-method=<rule>

Where <rule> is either the word “remove” or a masking rule in the format **right:<mask char>:<bytes>**.

The following example attribute tells the LAC to completely remove the L2TP Calling Station ID:

Cisco-Avpair = vpdn:l2tp-clid-mask-method=remove

The following example attribute tells the LAC to mask the 5 right characters with the character %:

Cisco-Avpair = vpdn:l2tp-clid-mask-method=right:%:5

Configuration Examples for L2TP Calling Station ID Suppression

This section provides the following configuration examples:

- [Calling Station ID Suppression for Local Authorization: Example, page 6](#)
- [Calling Station ID Suppression with RADIUS Authorization: Example, page 8](#)

Calling Station ID Suppression for Local Authorization: Example

The following example shows a LAC router managing PPP over Ethernet over virtual LAN (PPPoEoVLAN) end users. The router obtains a Calling Station ID from Logical Line ID network access server (NAS) port preauthorization through RADIUS and supports a per-user privacy option on the username (when including #184 in username), using local domain authorization.

```
Current configuration : 3158 bytes
!
version 12.3
loader bypass-init
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$8qtb$MHcYeW2kn8VNYgz932eX1.
enable password lab
!
aaa new-model
!
!
aaa group server radius LLID-Radius
 server 192.168.1.5 auth-port 1645 acct-port 1646
!
aaa group server radius LAC-Radius
 server 192.168.1.6 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
```

```
aaa authorization network default local
aaa authorization network LLID group LLID-Radius
aaa accounting network default start-stop group LAC-Radius
aaa nas port extended
aaa session-id common
!
resource manager
!
clock timezone GMT 1
ip subnet-zero
ip cef
no ip domain lookup
!
!
virtual-profile virtual-template 1
vpdn enable
vpdn search-order domain
!
vpdn-group L2TP
 request-dialin
  protocol l2tp
  domain cisco.com
  domain cisco.com#184
  initiate-to ip 192.168.1.4
  local name test
  l2tp tunnel password 0 cisco
  l2tp attribute clid mask-method remove match #184
!
vpdn-group UUT
 accept-dialin
  protocol pppoe
  virtual-template 1
!
subscriber access pppoe pre-authorize nas-port-id LLID send username
!
interface Loopback0
 no ip address
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 192.168.1.3 255.255.255.0
 no cdp enable
!
interface Ethernet0/0.20
 encapsulation dot1Q 1024
 no snmp trap link-status
 pppoe enable
 pppoe max-sessions 200
 no cdp enable
!
interface Ethernet1/0
 ip address 10.1.1.10 255.255.255.0
 no cdp enable
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
```

```

serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mroute-cache
 no peer default ip address
 ppp authentication pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
ip route 10.0.0.0 255.0.0.0 Ethernet1/0
!
no ip http server
!
!
radius-server attribute 69 clear
radius-server host 192.168.1.5 auth-port 1645 acct-port 1646
radius-server host 192.168.1.6 auth-port 1645 acct-port 1646
radius-server domain-stripping delimiter #
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab

```

Calling Station ID Suppression with RADIUS Authorization: Example

The following example shows a LAC router managing PPPoEoVLAN end users. The router obtains a Calling Station ID from Logical Line ID NAS port preauthorization through RADIUS and supports a per-user privacy option on the username (when including #184 in username), using RADIUS domain authorization that includes the Cisco VSA l2tp-clid-mask-method.

```

Current configuration : 3158 bytes
!
version 12.3
loader bypass-init
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$8qtb$MHCYew2kn8VNYgz932eX1.
enable password lab
!
aaa new-model
!
!
aaa group server radius LLID-Radius
 server 192.168.1.5 auth-port 1645 acct-port 1646
!

```

```
aaa group server radius LAC-Radius
  server 192.168.1.6 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authorization network default group LAC-Radius
aaa authorization network LLID group LLID-Radius
aaa accounting network default start-stop group LAC-Radius
aaa nas port extended
aaa session-id common
!
resource manager
!
clock timezone GMT 1
ip subnet-zero
ip cef
no ip domain lookup
!
!
virtual-profile virtual-template 1
vpdn enable
vpdn search-order domain
!
vpdn-group UUT
  accept-dialin
  protocol pppoe
  virtual-template 1
!
subscriber access pppoe pre-authorize nas-port-id LLID send username
!
interface Loopback0
  no ip address
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/0
  ip address 192.168.1.3 255.255.255.0
  no cdp enable
!
interface Ethernet0/0.20
  encapsulation dot1Q 1024
  no snmp trap link-status
  pppoe enable
  pppoe max-sessions 200
  no cdp enable
!
interface Ethernet1/0
  ip address 10.1.1.10 255.255.255.0
  no cdp enable
!
interface Serial2/0
  no ip address
  shutdown
  serial restart-delay 0
!
interface Serial3/0
  no ip address
  shutdown
  serial restart-delay 0
!
interface Virtual-Template1
  ip unnumbered Ethernet1/0
  ip mroute-cache
  no peer default ip address
```

```

ppp authentication pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
ip route 10.0.0.0 255.0.0.0 Ethernet1/0
!
no ip http server
!
!
radius-server attribute 69 clear
radius-server host 192.168.1.5 auth-port 1645 acct-port 1646
radius-server host 192.168.1.6 auth-port 1645 acct-port 1646
radius-server domain-stripping delimiter #
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password lab

```

In the RADIUS server pointed to by LAC-Radius, configure an entry for cisco.com with the following authorization attributes:

Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco

Cisco-Avpair = vpdn:tunnel-type=l2tp

Cisco-Avpair = vpdn:tunnel-id=test

Cisco-Avpair = vpdn:ip-addresses=192.168.1.4

Cisco-Avpair = vpdn:l2tp-clid-mask-method=right:X:6

Additional References

The following sections provide references related to the L2TP Calling Station ID Suppression feature.

Related Documents

Related Topic	Document Title
Layer 2 Tunnel Protocol	“ Layer 2 Tunnel Protocol ” chapter in the <i>Cisco 6400 Feature Guide</i> , Release 12.3

MIBs

MIB	MIBs Link
No new or modified MIBs are supported 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

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

This section documents new commands only.

- [l2tp attribute clid mask-method](#)
- [vpdn l2tp attribute clid mask-method](#)

I2tp attribute clid mask-method

To configure a network access server (NAS) to provide Layer 2 Tunnel Protocol (L2TP) calling line ID suppression for local authorization, use the **l2tp attribute clid mask-method** command in VPDN group configuration mode. To disable this function, use the **no** form of this command.

l2tp attribute clid mask-method {**right** *mask-character bytes* | **remove**} [**match** *match-string*]

no l2tp attribute clid mask-method {**right** *mask-character bytes* | **remove**} [**match** *match-string*]

Syntax Description

right	Masks the Calling Station ID by replacing characters, starting from the end of the string.
<i>mask-character</i>	Character to be used as a replacement.
<i>bytes</i>	Number of characters to be replaced.
remove	Removes the Calling Station ID.
match	(Optional) Applies the rule only if the Calling Station ID contains the specified match string in the username.
<i>match-string</i>	(Optional) Match string in the username that must be found for the rule to be applied.

Command Default

The Calling Station ID is not masked or dropped.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
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.

Usage Guidelines

Use the **l2tp attribute clid mask-method** command in VPDN group configuration mode to mask the caller ID for calls belonging to that virtual private dialup network (VPDN) group.

Use the **vpdn l2tp attribute clid mask-method** command to mask the caller ID globally for all VPDN groups configured on the NAS.

You can either substitute characters for a portion of the calling line ID or drop the calling line ID.

Examples

The following example shows how to use the **l2tp attribute clid mask-method** command to remove the caller ID during local authorization if the username contains the string #184:

```
vpdn-group L2TP
 request-dialin
 protocol l2tp
 domain cisco.com
 domain cisco.com#184
 initiate-to ip 192.168.1.4
 local name router32
 l2tp tunnel password 0 cisco
 l2tp attribute clid mask-method remove match #184
```

Related Commands

Command	Description
vpdn l2tp attribute clid mask-method	Configures a NAS to provide L2TP calling line ID suppression globally on the router.

vpdn l2tp attribute clid mask-method

To configure a network access server (NAS) to provide Layer 2 Tunnel Protocol (L2TP) calling line ID suppression globally on the router, use the **vpdn l2tp attribute clid mask-method** command in global configuration mode. To disable this function, use the **no** form of this command.

```
vpdn l2tp attribute clid mask-method {right mask-character bytes | remove} [match
match-string]
```

```
no vpdn l2tp attribute clid mask-method {right mask-character bytes | remove} [match
match-string]
```

Syntax Description

right	Masks the Calling Station ID by replacing characters, starting from the right end of the string.
<i>mask-character</i>	Character to be used as a replacement.
<i>bytes</i>	Number of characters to be replaced.
remove	Removes the Calling Station ID.
match	(Optional) Applies the rule only if the Calling Station ID contains the specified match string.
<i>match-string</i>	(Optional) Match string in the username that must be found for the rule to be applied.

Command Default

The Calling Station ID is not masked or dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
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.

Usage Guidelines

Use the **vpdn l2tp attribute clid mask-method** command to mask the caller ID globally for all virtual private dialup network (VPDN) groups configured on the NAS. Use the **l2tp attribute clid mask-method** command in VPDN group configuration mode to mask the caller ID for calls belonging only to that VPDN group.

You can either substitute characters for a portion of the calling line ID or drop the calling line ID.

Examples

The following example shows how to use the **vpdn l2tp attribute clid mask-method** command globally to mask the L2TP calling line ID during authorization if the username contains the string #184.

```
vpdn enable
vpdn l2tp attribute clid mask-method right # 255 match #184
vpdn search-order domain
```

Related Commands

Command	Description
l2tp attribute clid mask-method	Configures a NAS to provide L2TP calling line ID suppression for local authorization.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSI Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Inter iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your 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 partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

