

# L2TP Large-Scale Dial-Out per-User Attribute via AAA

**First Published: March 16, 2012**

**Last Updated: November 20, 2014**

This feature makes it possible for IP per-user attributes to be applied to a Layer 2 Tunneling Protocol (L2TP) dial-out session.

## Feature Specifications for L2TP Large-Scale Dial-Out per-User Attribute via AAA

### Feature History

Release	Modification
12.2(15)T	This feature was introduced.
Cisco IOS Release XE 3.9S	In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V.

### Supported Platforms

Cisco 7200, Cisco 7400

## 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 Using L2TP Large-Scale Dial-Out per-User Attribute via AAA, page 1](#)
- [Information About L2TP Large-Scale Dial-Out per-User Attribute via AAA, page 2](#)
- [How to Configure L2TP Large-Scale Dial-Out per-User Attribute via AAA, page 3](#)
- [Configuration Examples for L2TP Large-Scale Dial-Out per-User Attribute via AAA, page 7](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)

## Restrictions for Using L2TP Large-Scale Dial-Out per-User Attribute via AAA

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature does *not* support the following features associated with L2TP dial-out:

- Dialer Watch

- Dialer backup
- Dialer redial
- Dialer multiple number dial
- Callback initiated by an L2TP network server (LNS), the Bandwidth Allocation Protocol (BAP), and so on

## Information About L2TP Large-Scale Dial-Out per-User Attribute via AAA

To configure the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature, you need to understand the following concept:

- [How the L2TP Large-Scale Dial-Out per-User Attribute via AAA Feature Works, page 2](#)

## How the L2TP Large-Scale Dial-Out per-User Attribute via AAA Feature Works

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature makes it possible for IP and other per-user attributes to be applied to an L2TP dial-out session from an LNS. Before this feature was released, IP per-user configurations from authentication, authorization, and accounting (AAA) servers were not supported; the IP configuration would come from the dialer interface defined on the device.

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature works in a way similar to virtual profiles and L2TP dial-in. The L2TP virtual access interface is first cloned from the virtual template, which means that configurations from the virtual template interface will be applied to the L2TP virtual access interface. After authentication, the AAA per-user configuration is applied to the virtual access interface. Because AAA per-user attributes are applied only after the user has been authenticated, the LNS must be configured to authenticate the dial-out user (configuration authentication is needed for this feature).

With the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature, all software components can now use the configuration present on the virtual access interface rather than what is present on the dialer interface. For example, IP Control Protocol (IPCP) address negotiation uses the local address of the virtual access interface as the device address while negotiating with the peer.

All Cisco IOS commands that can be configured as AAA per-user commands are supported by the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature. Following is a list of some of the commands that are typically configured on a per-user basis:

- The **ip vrf forwarding** interface configuration command
- The **ip unnumbered loopback0** interface configuration command
- Per-user static routes
- Access lists
- Multilink bundles
- Idle timers

# How to Configure L2TP Large-Scale Dial-Out per-User Attribute via AAA

This section contains the following procedures:

- [Configuring the VPDN Group on the LNS, page 3](#) (required)
- [Verifying the Configuration on the Virtual Access Interface, page 5](#) (optional)
- [Troubleshooting the Configuration on the Virtual Access Interface, page 5](#) (optional)

## Configuring the VPDN Group on the LNS

You will need to configure the virtual template under the request dial-out configuration. You will also need to select the tunneling protocol and assign the virtual private dial-up network (VPDN) subgroup to a rotary group.

AAA per-user configuration is supported only on legacy dialer or dialer rotary groups and does not make sense on dialer profiles.

Be sure to configure the virtual template so that the LNS authenticates the dial-out user.

If a virtual template is not configured, L2TP dial-out per-user is not supported, but the configuration is backward compatible for all IP configurations that come from the dialer interface.

## Prerequisites

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature provides additional functionality for large-scale dial-out networks and Layer 2 tunneling. It is assumed that a network is already configured and operational, and that the tasks in this document will be performed on an operational network. See the “[Additional References](#)” section for more information about large-scale dial-out networks, Layer 2 tunneling, and virtual template interfaces.

## Restrictions

If the tasks in this section are not performed, the software will operate in the original mode, that is, IP per-user configurations from a AAA server will not be recognized and IP addresses will come from the dialer interface defined on the device.

To configure the VPDN group that makes it possible for IP per-user attributes to be applied to an L2TP dial-out session, use the following commands:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **request-dialout**
5. **protocol l2tp**
6. **rotary-group** *group-number*
7. **virtual-template** *template-number*

## 8. exit

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>vpdn-group</b> <i>name</i>  <b>Example:</b> Device(config)# vpdn-group 1	Creates a VPDN group and starts VPDN group configuration mode.
Step 4	<b>request-dialout</b>  <b>Example:</b> Device(config-vpdn)# request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP, and starts VPDN request-dialout configuration mode.
Step 5	<b>protocol l2tp</b>  <b>Example:</b> Device(config-vpdn-req-ou)# protocol l2tp	Specifies the L2TP tunneling protocol.
Step 6	<b>rotary-group</b> <i>group-number</i>  <b>Example:</b> Device(config-vpdn-req-ou)# rotary-group 1	Assigns a request-dialout VPDN subgroup to a dialer rotary group.
Step 7	<b>virtual-template</b> <i>template-number</i>  <b>Example:</b> Device(config-vpdn-req-ou)# virtual-template 1	Clones the configuration from a corresponding virtual template interface, and supports IP per-user configurations from a AAA server.
Step 8	<b>exit</b>  <b>Example:</b> Device(config-vpdn-req-ou)# exit	Exits VPDN request-dialout configuration mode.

## What to Do Next

The configuration for the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature must include a AAA profile to specify the per-user attributes. See the [“Per-User AAA Attributes Profile Example”](#) for an example of such a profile.

## Verifying the Configuration on the Virtual Access Interface

This task verifies that the per-user AAA commands are successfully parsed on the virtual access interface.

### SUMMARY STEPS

1. **enable**
2. **show interfaces virtual-access *number* [configuration]**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show interfaces virtual-access <i>number</i> [configuration]</b>  <b>Example:</b> Device# show interfaces virtual-access 3 configuration	Displays status, traffic data, and configuration information about a specified virtual access interface. <ul style="list-style-type: none"> <li>• <b>configuration</b>—(Optional) Restricts output to configuration information.</li> </ul>

## Troubleshooting the Configuration on the Virtual Access Interface

This task displays additional information about the per-user AAA commands that are parsed on the virtual access interface.

### SUMMARY STEPS

1. Attach a console directly to a device.
2. **enable**
3. **configure terminal**
4. **no logging console**
5. Use Telnet to access a device port and repeat Steps 2 and 3.
6. **terminal monitor**
7. **exit**
8. **debug aaa per-user**
9. **debug vtemplate events**
10. **debug vtemplate cloning**
11. **configure terminal**
12. **no terminal monitor**
13. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	Attach a console directly to a device.	—
Step 2	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 3	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 4	<b>no logging console</b>  <b>Example:</b> Device(config)# no logging console	Disables all logging to the console terminal. <ul style="list-style-type: none"> <li>To reenable logging to the console, use the <b>logging console</b> command in global configuration mode.</li> </ul>
Step 5	Use Telnet to access a Device port and repeat Steps 2 and 3.	Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port.
Step 6	<b>terminal monitor</b>  <b>Example:</b> Device(config)# terminal monitor	Enables logging output on the virtual terminal.
Step 7	<b>exit</b>  <b>Example:</b> Device(config)# exit	Exits to privileged EXEC mode.
Step 8	<b>debug aaa per-user</b>  <b>Example:</b> Device# debug aaa per-user	Displays what attributes are applied to each user as the user authenticates.
Step 9	<b>debug vtemplate events</b>  <b>Example:</b> Device# debug vtemplate events	Displays the virtual template events to form a virtual access interface.
Step 10	<b>debug vtemplate cloning</b>  <b>Example:</b> Device# debug vtemplate cloning	Displays the virtual template cloning to form a virtual access interface. <ul style="list-style-type: none"> <li>Use this command to verify when the interface is created (cloned from the virtual template) at the beginning of the dialup connection and when the interface is destroyed when the connection is terminated.</li> </ul>

	Command or Action	Purpose
Step 11	<code>configure terminal</code>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
Step 12	<code>no terminal monitor</code>  <b>Example:</b> Device(config)# <code>no terminal monitor</code>	Disables logging on the virtual terminal.
Step 13	<code>exit</code>  <b>Example:</b> DeviceDevice(config)# <code>exit</code>	Exits to privileged EXEC mode.

## Configuration Examples for L2TP Large-Scale Dial-Out per-User Attribute via AAA

This section provides the following configuration examples to show how to configure the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature:

- [LNS Configuration Example, page 7](#)
- [Per-User AAA Attributes Profile Example, page 8](#)
- [Virtual Access Interface Configuration Verification Example, page 8](#)
- [Virtual Access Interface Configuration Troubleshooting Example, page 8](#)

### LNS Configuration Example

The following partial example shows how to configure an LNS for the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature:

```
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
.
.
.
request-dialout
protocol l2tp
rotary-group 1
virtual-template 1
initiate-to ip 10.0.1.194.2
local name lns
l2tp tunnel password 7094F3$!5^3
source-ip 10.0.194.53
!
```

## Per-User AAA Attributes Profile Example

The following example shows the attribute-value pair (avpair) statements for a AAA profile to specify the per-user attributes:

```
5300-Router1-out Password = "cisco"
    Service-Type = Outbound
    cisco-avpair = "outbound:dial-number=5553021"
7200-Router1-1 Password = "cisco"
    Service-Type = Outbound
    cisco-avpair = "ip:route=10.17.17.1 255.255.255.255 Dialer1 100 name 5300-Router1"
5300-Router1 Password = "cisco"
    Service-Type = Framed
    Framed-Protocol = PPP
    cisco-avpair = "lcp:interface-config=ip unnumbered loopback 0"
    cisco-avpair = "ip:outacl#1=deny ip host 10.5.5.5 any log"
    cisco-avpair = "ip:outacl#2=permit ip any any"
    cisco-avpair = "ip:inacl#1=deny ip host 10.5.5.5 any log"
    cisco-avpair = "ip:inacl#2=permit ip any any"
    cisco-avpair = "multilink:min-links=2"
    Framed-Route = "10.5.5.6/32 Ethernet4/0"
    Framed-Route = "10.5.5.5/32 Ethernet4/0"
    Idle-Timeout = 100
```

## Virtual Access Interface Configuration Verification Example

The following example shows the virtual access interface configuration so you can check that the per-user AAA commands are correctly parsed:

```
Device# show interfaces virtual-access 3 configuration

Virtual-Access3 is an VPDN link (sub)interface

Derived configuration : 212 bytes
!
interface Virtual-Access3
 ip vrf forwarding V1.25.com
 ip unnumbered Loopback25
 no peer default ip address
 ppp authentication chap
end
```

## Virtual Access Interface Configuration Troubleshooting Example

This section provides the following debugging session examples for a network configured with the L2TP Large-Scale Dial-Out per-User Attribute via AAA feature. Output is displayed for each command in the task.

### Sample Output for the debug aaa per-user Command

```
Device# debug aaa per-user

%LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
AAA/AUTHOR: Processing PerUser AV interface-config
AAA/AUTHOR: Processing PerUser AV route
AAA/AUTHOR: Processing PerUser AV route
AAA/AUTHOR: Processing PerUser AV outacl
AAA/AUTHOR: Processing PerUser AV outacl
```



```

AAA/AUTHOR: Processing PerUser AV inacl
AAA/AUTHOR: Processing PerUser AV inacl
Vi3 AAA/PERUSER/ROUTE: vrf name for vaccess: V1.25.com
Vi3 AAA/PERUSER/ROUTE: route string: IP route vrf V1.25.com 10.1.25.10 255.255.255.255 10.1.25.20 tag 120
Vi3 AAA/PERUSER/ROUTE: vrf name for vaccess: V1.25.com
Vi3 AAA/PERUSER/ROUTE: route string: IP route vrf V1.25.com 172.30.35.0 255.255.255.0 10.1.25.20 tag 120

AAA/PER-USER: mode = config; command = [ip access-list extended Virtual-Access3#41
permit icmp any any log
permit ip any any]
AAA/PER-USER: line = [ip access-list extended Virtual-Access3#41]
AAA/PER-USER: line = [permit icmp any any log]
AAA/PER-USER: line = [permit ip any any]
AAA/PER-USER: mode = config; command = [ip access-list extended Virtual-Access3#42
permit icmp any any log
permit ip any any]
AAA/PER-USER: line = [ip access-list extended Virtual-Access3#42]
AAA/PER-USER: line = [permit icmp any any log]
AAA/PER-USER: line = [permit ip any any]
AAA/PER-USER: mode = config; command = [IP route vrf V1.25.com 10.1.25.10 255.255.255.255 10.1.25.20 tag
120 IP route vrf V1.25.com 172.30.35.0 255.255.255.0 10.1.25.20 tag 120]
AAA/PER-USER: line = [IP route vrf V1.25.com 10.1.25.10 255.255.255.255 10.1.25.20 tag 120]
AAA/PER-USER: line = [IP route vrf V1.25.com 172.30.35.0 255.255.255.0 10.1.25.20 tag 120]
*Feb 28 07:35:19.616: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3, changed state to
up

```

### Sample Output for the debug vtemplate events and debug vtemplate cloning Commands

```

Device# debug vtemplate events
Device# debug vtemplate cloning

VT[Vi3]:Reuse interface, recycle queue size 1
VT[Vi3]:Set to default using 'encap ppp'
VT[Vi3]:Vaccess created
VT[Vi3]:Added new vtemplate cloneblk, now cloning from vtemplate
VT[Vi3]:Clone Vaccess from Virtual-Template25 (19 bytes)
VT[Vi3]:no ip address
VT[Vi3]:end
VT[Vi3]:Applying config commands on process "Dialer event" (25)
VT[Vi3]:no ip address
VT[Vi3]:end
%LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
VT:Sending vaccess request, id 0x6401947C
VT:Processing vaccess requests, 1 outstanding
VT[Vi3]:Added new AAA cloneblk, now cloning from vtemplate/AAA
VT[Vi3]:Clone Vaccess from AAA (60 bytes)
VT[Vi3]:ip vrf forwarding V1.25.com
VT[Vi3]:ip unnumbered loopback25
VT[Vi3]:end
VT[Vi3]:Applying config commands on process "VTEMPLATE Background Mgr" (160)
VT[Vi3]:ip vrf forwarding V1.25.com
VT[Vi3]:ip unnumbered loopback25
VT[Vi3]:end
VT[Vi3]:MTUs ip 1500, sub 0, max 1500, default 1500
VT[Vi3]:Processing vaccess response, id 0x6401947C, result success (1)
VT[Vi3]:Added new AAA cloneblk, now cloning from vtemplate/AAA
VT[Vi3]:Clone Vaccess from AAA (82 bytes)
VT[Vi3]:IP access-group Virtual-Access3#51 in
VT[Vi3]:IP access-group Virtual-Access3#52 out
VT[Vi3]:end
VT[Vi3]:Applying config commands on process "PPP IP Route" (62)
VT[Vi3]:IP access-group Virtual-Access3#51 in
VT[Vi3]:IP access-group Virtual-Access3#52 out
VT[Vi3]:end

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3, changed state to up

## Additional References

For additional information related to L2TP large-scale dial-out per-user attributes using a AAA server, see to the following sections:

- [Related Documents](#), page 10
- [Standards](#), page 10
- [MIBs](#), page 10
- [RFCs](#), page 11
- [Technical Assistance](#), page 11

## Related Documents

Related Topic	Document Title
Large-scale dial-out	<a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.2; refer to the chapter “ <a href="#">Configuring Large-Scale Dial-Out</a> .”
VPDN groups	<a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.2; refer to the chapter “ <a href="#">Configuring Virtual Private Networks</a> .”
Virtual interfaces	<a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.2; refer to the chapter “ <a href="#">Configuring Virtual Template Interfaces</a> .”
Per-user configuration	<a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.2; refer to the chapter “ <a href="#">Configuring Per-User Configuration</a> .”
Descriptions of debug command output	<a href="#">Cisco IOS Debug Command Reference</a> , Release 12.2.

## Standards

Standards	Title
None	—

## MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

RFCs	Title
None	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Dial Technologies Command Reference* at [http://www.cisco.com/en/US/docs/ios/dial/command/reference/dia\\_book.html](http://www.cisco.com/en/US/docs/ios/dial/command/reference/dia_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **virtual-template**

```
x25 route 11111 interface Dialer0
x25 route 44444 interface Dialer0
!
```

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)

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.

© 2007–2009 Cisco Systems, Inc. All rights reserved.