



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

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.

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 2](#)
- [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 12](#)

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 router.

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 router 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 6](#) (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 router.

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn-group <i>name</i> Example: Router(config)# vpdn-group 1	Creates a VPDN group and starts VPDN group configuration mode.
Step 4	request-dialout Example: Router(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	protocol l2tp Example: Router(config-vpdn-req-ou)# protocol l2tp	Specifies the L2TP tunneling protocol.
Step 6	rotary-group <i>group-number</i> Example: Router(config-vpdn-req-ou)# rotary-group 1	Assigns a request-dialout VPDN subgroup to a dialer rotary group.

	Command or Action	Purpose
Step 7	<code>virtual-template</code> <i>template-number</i> Example: Router(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	<code>exit</code> Example: Router(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	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>show interfaces virtual-access</code> <i>number</i> [<code>configuration</code>] Example: Router# 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"> • configuration—(Optional) Restricts output to configuration information.

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 router.
2. **enable**
3. **configure terminal**
4. **no logging console**
5. Use Telnet to access a router 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 router.	—
Step 2	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	no logging console Example: Router(config)# no logging console	Disables all logging to the console terminal. <ul style="list-style-type: none"> • To reenable logging to the console, use the logging console command in global configuration mode.
Step 5	Use Telnet to access a router 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	terminal monitor Example: Router(config)# terminal monitor	Enables logging output on the virtual terminal.

	Command or Action	Purpose
Step 7	<code>exit</code> Example: Router(config)# exit	Exits to privileged EXEC mode.
Step 8	<code>debug aaa per-user</code> Example: Router# debug aaa per-user	Displays what attributes are applied to each user as the user authenticates.
Step 9	<code>debug vtemplate events</code> Example: Router# debug vtemplate events	Displays the virtual template events to form a virtual access interface.
Step 10	<code>debug vtemplate cloning</code> Example: Router# debug vtemplate cloning	Displays the virtual template cloning to form a virtual access interface. <ul style="list-style-type: none"> 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.
Step 11	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 12	<code>no terminal monitor</code> Example: Router(config)# no terminal monitor	Disables logging on the virtual terminal.
Step 13	<code>exit</code> Example: Router(config)# exit	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 8](#)
- [Per-User AAA Attributes Profile Example, page 8](#)
- [Virtual Access Interface Configuration Verification Example, page 8](#)
- [Virtual Access Interface Configuration Troubleshooting Example, page 9](#)

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:

```
Router# 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

```
Router# 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

```
Router# debug vtemplate events
Router# 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

```

Additional References

```

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 11](#)
- [MIBs, page 11](#)
- [RFCs, page 11](#)
- [Technical Assistance, page 11](#)

Related Documents

Related Topic	Document Title
Large-scale dial-out	Cisco IOS Dial Technologies Configuration Guide , Release 12.2; refer to the chapter “Configuring Large-Scale Dial-Out.”
VPDN groups	Cisco IOS Dial Technologies Configuration Guide , Release 12.2; refer to the chapter “Configuring Virtual Private Networks.”
Virtual interfaces	Cisco IOS Dial Technologies Configuration Guide , Release 12.2; refer to the chapter “Configuring Virtual Template Interfaces.”
Per-user configuration	Cisco IOS Dial Technologies Configuration Guide , Release 12.2; refer to the chapter “Configuring Per-User Configuration.”
Descriptions of debug command output	Cisco IOS Debug Command Reference , 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: http://www.cisco.com/public/sw-center/netmgmt/ctk/mibs.shtml

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/ctk/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. 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
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the modified **virtual-template** VPDN subgroup configuration command. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

virtual-template

To specify which virtual template will be used to clone virtual access interfaces, use the **virtual-template** command in virtual private dial-up network (VPDN) subgroup configuration mode. To remove the virtual template from a VPDN group, use the **no** form of this command.

virtual-template *template-number*

no virtual-template

Syntax Description

template-number Number of the virtual template that will be used to clone virtual access interfaces.

Defaults

No virtual template is enabled.

Command Modes

VPDN subgroup

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was enhanced to enable PPPoE on ATM to accept dialin PPP over Ethernet (PPPoE) sessions.
12.2(15)T	This command was enhanced to allow IP per-user attributes to be applied to a Layer 2 Tunneling Protocol (L2TP) dial-out session.

Usage Guidelines

You must first enable a tunneling protocol on the VPDN group using the **protocol VPDN** subgroup command before you can enable the **virtual-template** command. Removing or modifying the **protocol** command will remove **virtual-template** command from the VPDN group.

Each VPDN group can clone only virtual access interfaces using one virtual template. If you enter a second **virtual-template** command on a VPDN group, it will replace the first **virtual-template** command.

[Table 1](#) lists the VPDN group commands under which the **virtual-template** command can be entered. Entering the VPDN group command starts VPDN subgroup mode. The table includes the command-line prompt for the VPDN subgroup mode and the type of service configured.

Table 1 VPDN Subgroups

VPDN Group Command	Command Mode Prompt	Type of Service
accept-dialin	router(config-vpdn-acc-in)#	Tunnel server
request-dialout	router(config-vpdn-req-ou)#	L2TP network server (LNS)

When the **virtual-template** command is entered under a **request-dialout** VPDN subgroup, IP and other per-user attributes can be applied to an L2TP dial-out session from an L2TP network server (LNS). Before this command was enhanced, 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 router.

The enhanced **virtual-template** command works in a way similar to configuring 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 command).

With the enhanced **virtual-template** command, 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 router address while negotiating with the peer.

Examples

The following example enables the LNS to accept an L2TP tunnel from an L2TP access concentrator (LAC) named LAC2. A virtual access interface will be cloned from virtual template 1.

```
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname LAC2
```

The following example enables PPPoE on ATM to accept dialin PPPoE sessions. A virtual access interface for the PPP session is cloned from virtual template 1.

```
vpdn-group 1
  accept-dialin
  protocol pppoe
  virtual-template 1
```

The following partial example shows how to configure an LNS to support IP per-user configurations from a AAA server:

```
!
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
!
```

The previous configuration requires a AAA profile such as the following example 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
```

Related Commands

Command	Description
accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and to create an accept-dialin VPDN subgroup.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP and to create a request-dialout VPDN subgroup.
vpdn-group	Defines a local, unique group number identifier.

