Configuring Per−User VPDNs Without Domain or DNIS Information

Document ID: 10388

Contents

Introduction

This document provides a sample configuration for per−user VPDNs without domain or DNIS information.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software Release 12.1(4) or later.
- Cisco IOS Software Release 12.1(4)T or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

In virtual private dial−up network (VPDN) scenarios, the network access server (NAS) (an L2TP access concentrator, or LAC) establishes the VPDN tunnel to the Home Gateway (LNS) based on user−specific information. This VPDN tunnel can be Level 2 Forwarding (L2F) or Layer 2 Tunneling Protocol (L2TP). To determine whether a user should use a VPDN tunnel, check:

- Whether the domain name is included as part of the username. For example, with the username tunnelme@cisco.com, the NAS forwards this user to the tunnel for cisco.com.
- The Dialed Number Information Service (DNIS). This is call−forwarding based on the called number. This means that the NAS can forward all calls with a particular called number to the appropriate tunnel. For example, if an incoming call has the called number 5551111, the call can be forwarded to the VPDN tunnel, while a call to 5552222 is not forwarded. This feature requires that the Telco network delivers called number information.

For more information about VPDN configuration, see Understanding VPDN.

In some situations, you may require a VPDN tunnel to be intiated on a per−username basis, with or without the need for a domain−name at all. For example the user **ciscouser** can be tunneled to **cisco.com**, while other users may be terminated locally on the NAS.

Note: This username does not include the domain information as in the previous example.

The VPDN per−user configuration feature sends the entire structured username to the authentication, authorization, and accounting (AAA) server the first time the router contacts the AAA server. This enables the Cisco IOS software to customize tunnel attributes for individual users who use a common domain name or DNIS.

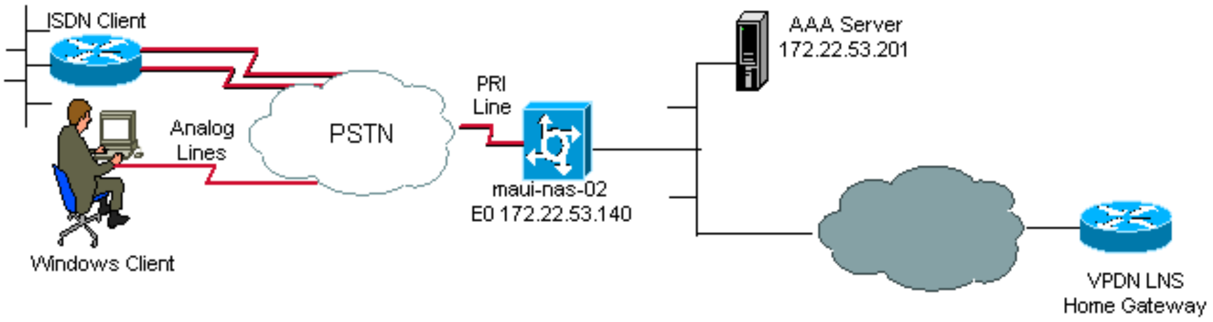
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Configurations

The only VPDN commands necessary on the NAS (LAC) to support per−user VPDNs are the global configuration commands **vpdn enable** and **vpdn authen−before−forward**. The **vpdn authen−before−forward** command instructs the NAS (LAC) to authenticate the complete username before it makes a forwarding decision. A VPDN tunnel is then established, based on the information returned by the AAA server for this individual user; if no VPDN information is returned from the AAA server, the user is terminated locally. The configuration in this section shows the commands required to support tunnels without the domain information in the username.

Note: This configuration is not comprehensive. Only the relevant VPDN, interface and AAA commands are included.

Note: It is beyond the scope of this document to discuss every possible tunnel protocol and AAA protocol. Hence, this configuration implements an L2TP tunnel with AAA RADIUS server. Adapt the principles and configuration discussed here to configure other tunnel types or AAA protocols.

This document uses this configuration:

- VPDN NAS (LAC)

VPDN NAS (LAC)

```
aaa new−model
aaa authentication ppp default group radius

!−−− Use RADIUS authentication for PPP authentication.

aaa authorization network default group radius

!−−− Obtain authorization information from the Radius server.
!−−− This command is required for the AAA server to provide VPDN attributes.

!
vpdn enable

!−−− VPDN is enabled.

vpdn authen−before−forward

!−−− Authenticate the complete username before making a forwarding decision.
!−−− The LAC sends the username to the AAA server for VPDN attributes.

!
controller E1 0
pri−group timeslots 1−31
!
interface Serial0:15
dialer rotary−group 1

!−−− D−channel for E1 0 is a member of the dialer rotary group 1.

!
interface Dialer1

!−−− Logical interface for dialer rotary group 1.

ip unnumbered Ethernet0
encapsulation ppp
dialer in−band
dialer−group 1
```

```
ppp authentication chap pap callin
!
radius-server host 172.22.53.201

!--- The IP address of the RADIUS server host.
!--- This AAA server will supply the NAS(LAC) with the VPDN attributes for the user.

radius-server key cisco

!--- The RADIUS server key.
```

RADIUS Server Configuration

Here are some user configurations on a Cisco Secure for Unix (CSU) RADIUS server:

1. A user who is to be terminated locally on the NAS:

   ```
   user1 Password = "cisco"
   Service-Type = Framed-User
   ```
2. A user for whom a VPDN session should be established:

   ```
   user2           Password = "cisco"
   Service-Type = Framed-User,
   Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
   Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
   Cisco-AVPair = "vpdn:tunnel-type=l2tp"
   ```

The NAS (LAC) uses the attributes specified with the Cisco−AVPair VPDN to intiate the VPDN tunnel to the Home Gateway. Ensure that you configure the Home Gateway to accept VPDN tunnels from the NAS.

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show caller user** shows parameters for a particular user, such as the TTY line used, asynchronous interface (shelf, slot or port), DS0 channel number, modem number, IP address assigned, PPP and PPP bundle parameters, and so on. If your version of Cisco IOS Software does not support this command, use the **show user** command.
- **show vpdn** displays information about active L2F and L2TP protocol tunnels and message identifiers in a VPDN.

Sample show Command Output

When the call connects use the **show caller user** *username* command as well as the **show vpdn** command to verify that the call is successful. A sample output is shown below:

```
maui-nas-02#show caller user vpdn_authen

  User: vpdn_authen, line tty 12, service Async
        Active time 00:09:01, Idle time 00:00:05
  Timeouts:            Absolute  Idle      Idle
                                 Session   Exec
```

```
      Limits:          -         -         00:10:00
      Disconnect in:   -         -         -
  TTY: Line 12, running PPP on As12
  DS0: (slot/unit/channel)=0/0/5
  Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
  Status: Ready, Active, No Exit Banner, Async Interface Active
          HW PPP Support Active
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
                Modem Callout, Modem RI is CD,
                Line is permanent async interface, Integrated Modem
  Modem State: Ready

  User: vpdn_authen, line As12, service PPP
        Active time 00:08:58, Idle time 00:00:05
  Timeouts:            Absolute  Idle
      Limits:          -         -
      Disconnect in:   -         -
  PPP: LCP Open, CHAP (<- AAA)
  IP: Local 172.22.53.140
  VPDN: NAS , MID 4, MID Unknown
        HGW , NAS CLID 0, HGW CLID 0, tunnel open

!--- The VPDN tunnel is open.

  Counts: 85 packets input, 2642 bytes, 0 no buffer
          0 input errors, 0 CRC, 0 frame, 0 overrun
          71 packets output, 1577 bytes, 0 underruns
          0 output errors, 0 collisions, 0 interface resets

maui-nas-02#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions
6318  3     HGW           est    172.22.53.141   1701  1

LocID RemID TunID Intf       Username      State  Last Chg Fastswitch
4     3     6318  As12       vpdn_authen   est    00:09:33 enabled

!--- The tunnel for user vpdn_authen is in established state.

%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnel
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

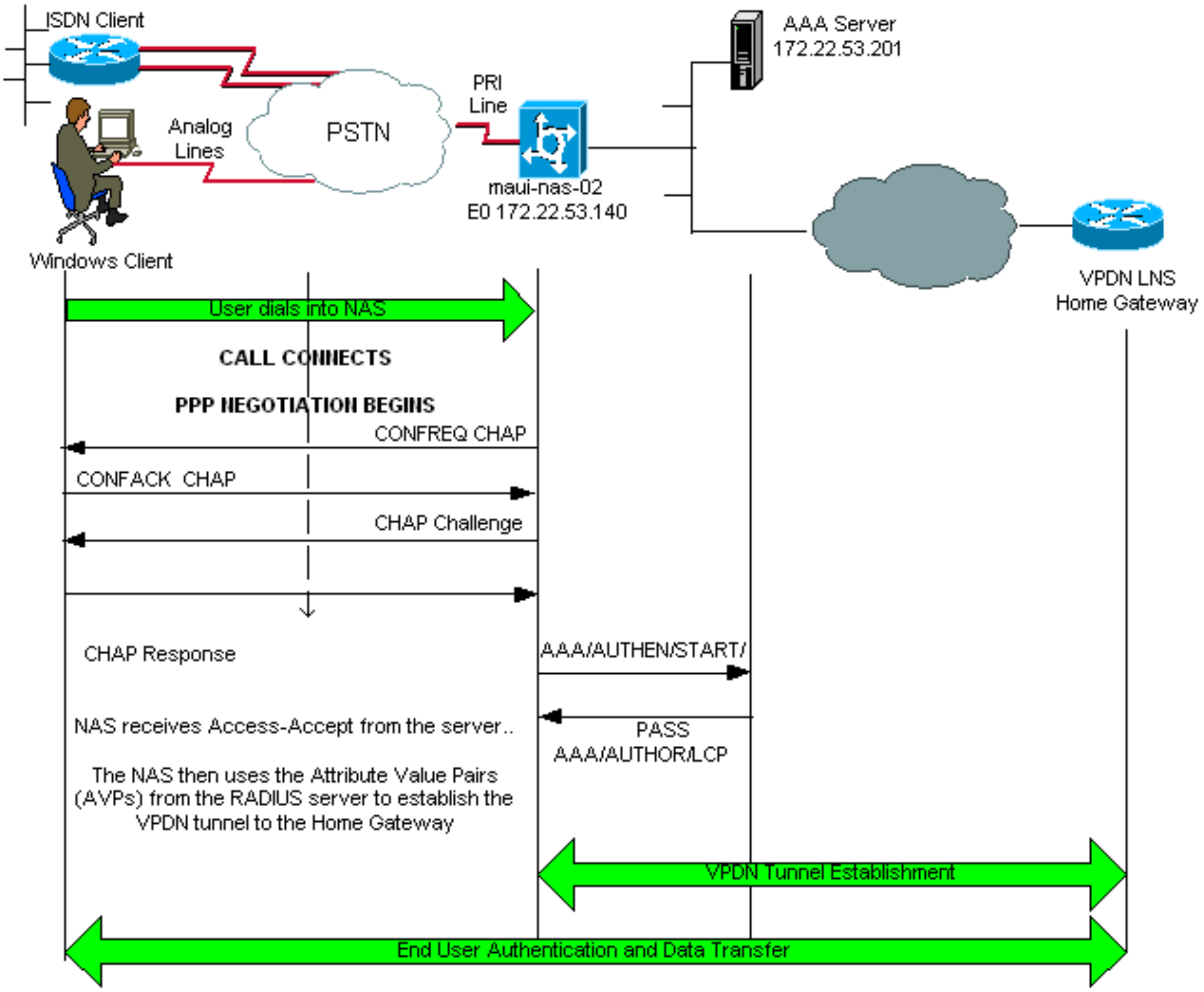
- **debug ppp authentication** displays PPP authentication protocol messages, and includes Challenge Handshake Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
- **debug aaa authentication** displays information on AAA/RADIUS authentication.
- **debug aaa authorization** displays information on AAA/RADIUS authorization.
- **debug radius** displays detailed debugging information associated with the RADIUS. Use the Output Interpreter Tool (registered customers only) to decode the debug radius messages. For example, refer to the Sample **debug** Output section. Use the information from **debug radius** to determine what

attributes are negotiated.

- **debug tacacs** displays detailed debugging information associated with the TACACS+.
- **debug vpdn event** displays L2x errors and events that are a part of normal tunnel establishment or shutdown for VPDNs.
- **debug vpdn error** displays VPDN protocol errors.
- **debug vpdn l2x−event** displays detailed L2x errors and events that are a part of normal tunnel establishment or shutdown for VPDNs.
- **debug vpdn l2x−error** displays VPDN L2x protocol errors.

Sample debug Output

Here is the **debug** output for a successful call. In this example, note that the NAS obtains the attributes for the VPDN tunnel from the Radius Server.



```
maui-nas-02#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
PPP:
  PPP authentication debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is onRadius protocol debugging is on
maui-nas-02#
*Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface Serial0:5 is now connected
```

```
to N/A N/A

!--- Incoming call.

*Jan 21 19:07:55.352: %LINK-3-UPDOWN: Interface Async12, changed state to up
*Jan 21 19:07:55.352: As12 PPP: Treating connection as a dedicated line
*Jan 21 19:07:55.352: As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Jan 21 19:07:55.604: As12 CHAP: O CHALLENGE id 1 len 32 from "maui-nas-02"
*Jan 21 19:07:55.732: As12 CHAP: I RESPONSE id 1 len 32 from "vpdn_authen"

!--- Incoming CHAP response from user vpdn_authen.

*Jan 21 19:07:55.732: AAA: parse name=Async12 idb type=10 tty=12
*Jan 21 19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=12 channel=0
*Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1
*Jan 21 19:07:55.732: AAA: name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0
adapter=0 port=0 channel=5
*Jan 21 19:07:55.732: AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5
*Jan 21 19:07:55.732: AAA/MEMORY: create_user (0x628C79EC) user='vpdn_authen'
ruser='' port='Async12' rem_addr='async/81560' authen_type=CHAP service=PPP priv=1
*Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807): port='Async12' list=''
action=LOGIN service=PPP
*Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807): using "default" list
*Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807): Method=radius (radius)
*Jan 21 19:07:55.736: RADIUS: ustruct sharecount=1
*Jan 21 19:07:55.736: RADIUS: Initial Transmit Async12 id
6 172.22.53.201:1645, Access-Request, len 89
*Jan 21 19:07:55.736:         Attribute 4 6 AC16358C
*Jan 21 19:07:55.736:         Attribute 5 6 0000000C
*Jan 21 19:07:55.736:         Attribute 61 6 00000000
*Jan 21 19:07:55.736:         Attribute 1 13 7670646E
*Jan 21 19:07:55.736:         Attribute 30 7 38313536
*Jan 21 19:07:55.736:         Attribute 3 19 014CF9D6
*Jan 21 19:07:55.736:         Attribute 6 6 00000002
*Jan 21 19:07:55.736:         Attribute 7 6 00000001
*Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645,
Access-Accept, len 136
*Jan 21 19:07:55.740:         Attribute 6 6 00000002
*Jan 21 19:07:55.740:         Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:         Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:         Attribute 26 30 0000000901187670
```

The attribute value pairs (AVPs) neccessary for the VPDN tunnel are pushed down from the RADIUS server. However, **debug radius** produces a coded output indicating the AVPs and their values. You can paste the output shown in **bold** font above into the Output Interpreter Tool (registered customers only) . The following output in bold is the decoded output obtained from the tool:

```
Access-Request 172.22.53.201:1645 id 6
Attribute Type 4:  NAS-IP-Address is 172.22.53.140
Attribute Type 5:  NAS-Port is 12
Attribute Type 61: NAS-Port-Type is Asynchronous
Attribute Type 1:  User-Name is vpdn
Attribute Type 30: Called-Station-ID(DNIS) is 8156
Attribute Type 3:  CHAP-Password is (encoded)
Attribute Type 6:  Service-Type is Framed
Attribute Type 7:  Framed-Protocol is PPP
        Access-Accept 172.22.53.201:1645 id 6
Attribute Type 6:  Service-Type is Framed
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS
...
```

```
...
...
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip−addresses=172.22.53.141"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp−tunnel−password=cisco"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel−type=l2tp"
*Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip−addresses=172.22.53.141
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp−tunnel−password=cisco
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel−type=l2tp

!−−− Tunnel information.
!−−− The VPDN Tunnel will now be established and the call will be authenticated.
!−−− Since the debug information is similar to that for a normal VPDN call,
!−−− the VPDN tunnel establishment debug output is omitted.
```

Related Information

- **Understanding VPDN**
- **Configuring Virtual Private Dialup Networks**
- **How−To Configure Layer 2 Tunnel Protocol Authentication with RADIUS**
- **How−To Configure Layer 2 Tunnel Protocol Authentication with TACACS+**
- **Access Technology Support Pages**
- **Technical Support − Cisco Systems**

Updated: Feb 04, 2010 Document ID: 10388