

Configuración de VPDNs por Usuario sin Información de Dominio o DNIS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del servidor de RADIUS](#)

[Verificación](#)

[Ejemplo de Resultado del Comando show](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Información Relacionada](#)

Introducción

Este documento proporciona una configuración de ejemplo para VPDN por usuario sin información de dominio o DNIS.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 12.1(4) o posterior del software del IOS® de Cisco.
- Versión 12.1(4)T o posterior del software del IOS de Cisco.

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.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

[Antecedentes](#)

En los escenarios de red de acceso telefónico privada virtual (VPDN), el servidor de acceso a la red (NAS) (un concentrador de acceso L2TP o LAC) establece el túnel VPDN para la puerta de enlace doméstica (LNS) en función de la información específica del usuario. Este túnel VPDN puede ser el protocolo de reenvío de nivel 2 (L2F) o el protocolo de tunelación de capa 2 (L2TP). Para determinar si un usuario debe utilizar un túnel VPDN, verifique:

- Si el nombre de dominio se incluye como parte del nombre de usuario. Por ejemplo, con el nombre de usuario tunnelme@cisco.com, el NAS reenvía este usuario al túnel para cisco.com.
- El servicio de información de números marcados (DNIS). Este es el reenvío de llamadas basado en el número al que se llama. Esto significa que el NAS puede reenviar todas las llamadas con un número llamado particular al túnel apropiado. Por ejemplo, si una llamada entrante tiene el número llamado 5551111, la llamada se puede reenviar al túnel VPDN, mientras que una llamada a 5552222 no se reenvía. Esta función requiere que la red de la compañía telefónica proporcione la información del número llamado.

Para obtener más información sobre la configuración de VPDN, vea [Introducción a VPDN](#).

En algunas situaciones, puede requerir que se inicie un túnel VPDN por nombre de usuario, con o sin la necesidad de un nombre de dominio en absoluto. Por ejemplo, el usuario **ciscouser** se puede tunelizar a **cisco.com**, mientras que otros usuarios pueden terminar localmente en el NAS.

Nota: Este nombre de usuario no incluye la información del dominio como en el ejemplo anterior.

La función de configuración VPDN por usuario envía el nombre de usuario estructurado completo al servidor de autenticación, autorización y contabilidad (AAA) la primera vez que el router se pone en contacto con el servidor AAA. Esto permite que el software Cisco IOS personalice los atributos de túnel para usuarios individuales que utilizan un nombre de dominio común o DNIS.

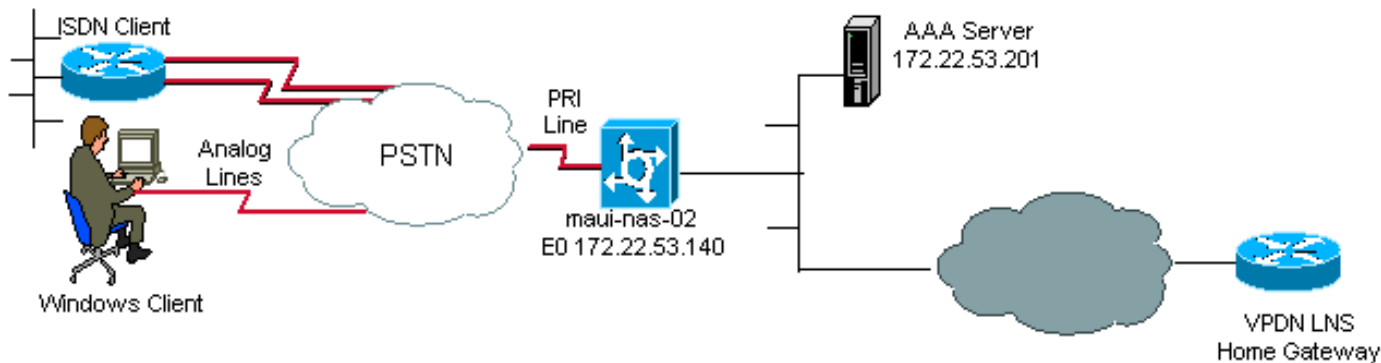
[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Configuraciones

Los únicos comandos VPDN necesarios en el NAS (LAC) para soportar VPDN por usuario son los comandos de configuración global **vpdn enable** y **vpdn authen-before-forward**. El comando **vpdn authen-before-forward** indica al NAS (LAC) que autentique el nombre de usuario completo antes de tomar una decisión de reenvío. Luego se establece un túnel VPDN, basado en la información devuelta por el servidor AAA para este usuario individual; si no se devuelve información VPDN del servidor AAA, el usuario finaliza localmente. La configuración de esta sección muestra los comandos requeridos para soportar túneles sin la información de dominio en el nombre de usuario.

Nota: Esta configuración no es completa. Sólo se incluyen los comandos VPDN, interfaz y AAA relevantes.

Nota: Está fuera del alcance de este documento discutir cada protocolo de túnel posible y protocolo AAA. Por lo tanto, esta configuración implementa un túnel L2TP con el servidor RADIUS AAA. Adapte los principios y la configuración aquí descritos para configurar otros tipos de túnel o protocolos AAA.

Este documento usa esta configuración:

- 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.
```

Configuración del servidor de RADIUS

Estas son algunas configuraciones de usuario en un servidor RADIUS Cisco Secure para Unix (CSU):

1. Un usuario que se terminará localmente en el NAS:

```
user1 Password = "cisco"  
Service-Type = Framed-User
```

2. Usuario para el que se debe establecer una sesión VPDN:

```
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"
```

El NAS (LAC) utiliza los atributos especificados con Cisco-AVPair VPDN para iniciar el túnel VPDN a la gateway de inicio. Asegúrese de configurar el gateway de inicio para aceptar túneles VPDN del NAS.

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

- **show caller user:** muestra parámetros para un usuario determinado, como la línea TTY utilizada, la interfaz asincrónica (estante, ranura o puerto), el número de canal DS0, el número de módem, la dirección IP asignada, los parámetros de agrupamiento PPP y PPP, etc. Si su versión del software del IOS de Cisco no es compatible con este comando, utilice el comando show user.
- **show vpdn:** muestra información sobre los túneles de protocolo L2F y L2TP activos y los identificadores de mensaje en una VPDN.

Ejemplo de Resultado del Comando show

Cuando la llamada se conecta, utilice el comando **show caller user *username***, así como el comando **show vpdn** para verificar que la llamada es exitosa. A continuación, se muestra un ejemplo de salida:

```
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](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

[Comandos para resolución de problemas](#)

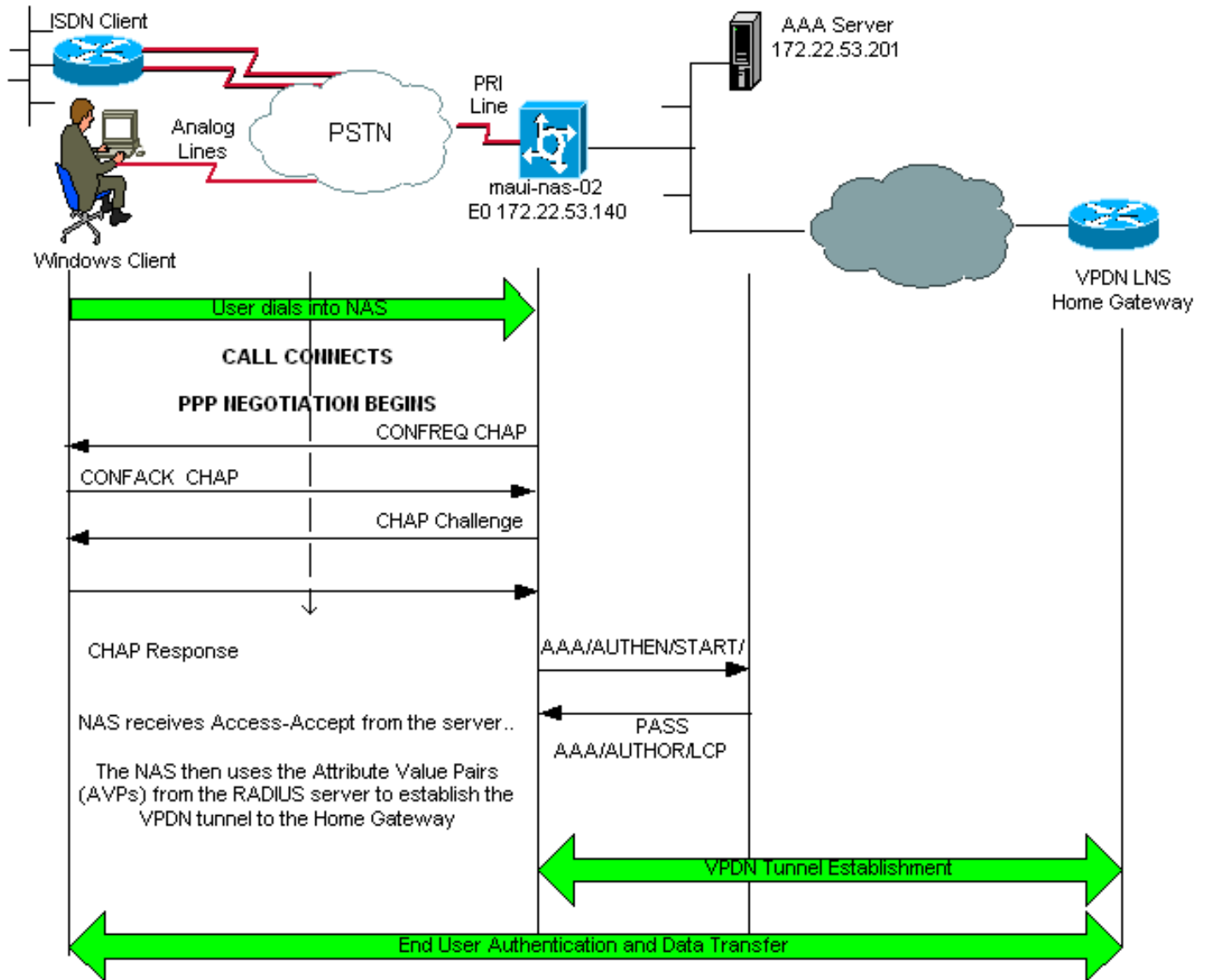
Nota: Antes de ejecutar un comando **debug**, consulte [Información Importante sobre Comandos Debug](#).

- **debug ppp authentication:** muestra los mensajes del protocolo de autenticación PPP e incluye intercambios de paquetes del protocolo de autenticación por desafío mutuo (CHAP) e intercambios de protocolo de autenticación de contraseña (PAP).
- **debug aaa authentication:** muestra información sobre la autenticación AAA/RADIUS.
- **debug aaa authorization:** muestra información sobre la autorización AAA/RADIUS.
- **debug radius:** muestra información de depuración detallada asociada con RADIUS. Utilice la [herramienta Output Interpreter Tool](#) (sólo clientes [registrados](#)) para decodificar los mensajes debug radius. Por ejemplo, refiérase a la [sección Ejemplo debug Output](#). Utilice la información de **debug radius** para determinar qué atributos se negocian.
- **debug tacacs:** muestra información detallada de depuración asociada con el TACACS+.
- **debug vpdn event:** muestra los errores L2x y los eventos que forman parte del establecimiento o cierre normal del túnel para VPDNs.
- **debug vpdn error:** muestra los errores del protocolo VPDN.
- **debug vpdn l2x-event:** muestra errores L2x detallados y eventos que forman parte del establecimiento o cierre normal del túnel para VPDNs.

- `debug vpdn l2x-error`: muestra los errores de protocolo VPDN L2x.

Ejemplo de resultado del comando debug

Este es el resultado `debug` para una llamada exitosa. En este ejemplo, observe que el NAS obtiene los atributos para el túnel VPDN del Servidor Radius.



```
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 Serial10:5 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: Async12 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

```

Los pares de valores de atributo (AVP) necesarios para el túnel VPDN se envían hacia abajo desde el servidor RADIUS. Sin embargo, **debug radius** produce un resultado codificado que indica los AVP y sus valores. Puede pegar la salida mostrada en la fuente **en negrita** anterior en la [Herramienta Output Interpreter](#) (sólo [clientes registrados](#)). El siguiente resultado en negrita es el resultado descodificado obtenido de la herramienta:

```

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.

Información Relacionada

- [Introducción a VPDN'](#)
- [Configuración de Redes de Marcación Privadas Virtuales](#)
- [Cómo Configurar la Autenticación de Layer 2 Tunnel Protocol con RADIUS](#)
- [Cómo Configurar la Autenticación de Layer 2 Tunnel Protocol con TACACS+](#)
- [Páginas de soporte de la tecnología de acceso](#)
- [Soporte Técnico - Cisco Systems](#)