تكوين شبكات VPDN لكل مستخدم بدون معلومات حول المجال أو DNIS

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
تكوين خادم RADIUS
التحقق من الصحة
عينة عرض أمر إنتاج
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
إخراج تصحيح الأخطاء للعينة
معلومات ذات صلة

المقدمة

يزود هذا وثيقة عينة تشكيل ل VPDNs لكل مستعمل دون مجال أو DNIS معلومة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج IOS® الإصدار 12.1(4) من Cisco أو إصدار أحدث.
- برنامج IOS الإصدار 12.1(4)T من Cisco أو إصدار أحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

في سيناريوهات شبكة الطلب الهاتفي الخاصة الظاهرية (VPDN)، يقوم خادم الوصول إلى الشبكة (NAS) (مركز وصول L2TP، أو LAC) بإنشاء نفق VPDN إلى البوابة الرئيسية (LNS) استنادا إلى المعلومات الخاصة بالمستخدم. يمكن أن يكون نفق VPDN هذا إعادة توجيه المستوى 2 (L2F) أو بروتوكول نفق الطبقة 2 (L2TP). لتحديد ما إذا كان يجب على المستخدم إستخدام نفق VPDN، تحقق من:

- ما إذا كان اسم المجال مضمنا كجزء من اسم المستخدم. على سبيل المثال، باستخدام اسم المستخدم tunnelme@cisco.com، تقوم NAS بإعادة توجيه هذا المستخدم إلى النفق ل cisco.com.
- خدمة معلومات الرقم المطلوب (DNIS). وهذا إعادة توجيه المكالمات استنادا إلى الرقم المستدعى. وهذا يعني أنه يمكن ل NAS إعادة توجيه جميع المكالمات برقم مسمى محدد إلى النفق المناسب. على سبيل المثال، إذا كانت مكالمة واردة تحمل الرقم المستدعى 555111، يمكن إعادة توجيه المكالمة إلى نفق VPDN، بينما لا يتم إعادة توجيه مكالمة إلى 5552222. تتطلب هذه الميزة أن توفر شبكة Telco معلومات الرقم المستدعى.

لمزيد من المعلومات حول تكوين VPDN، راجع فهم VPDN.

في بعض الحالات، قد تحتاج إلى إنشاء نفق VPDN على أساس كل اسم مستخدم، مع أو بدون الحاجة إلى اسم مجال على الإطلاق. على سبيل المثال، يمكن إنشاء قنوات اتصال **خاصة** بالمستخدم إلى **Cisco.com**، بينما يمكن إنهاء المستخدمين الآخرين محليا على NAS.

ملاحظة: لا يتضمن اسم المستخدم هذا معلومات المجال كما هو الحال في المثال السابق.

تقوم ميزة التكوين الخاص بشبكة VPDN لكل مستخدم بإرسال اسم المستخدم المنظم بالكامل إلى خادم المصادقة والتفويض والمحاسبة (AAA) في أول مرة يتصل فيها الموجه بخادم AAA. وهذا يمكن برنامج Cisco IOS software من تخصيص سمات النفق للمستخدمين الفرديين الذين يستخدمون اسم مجال عام أو DNIS.

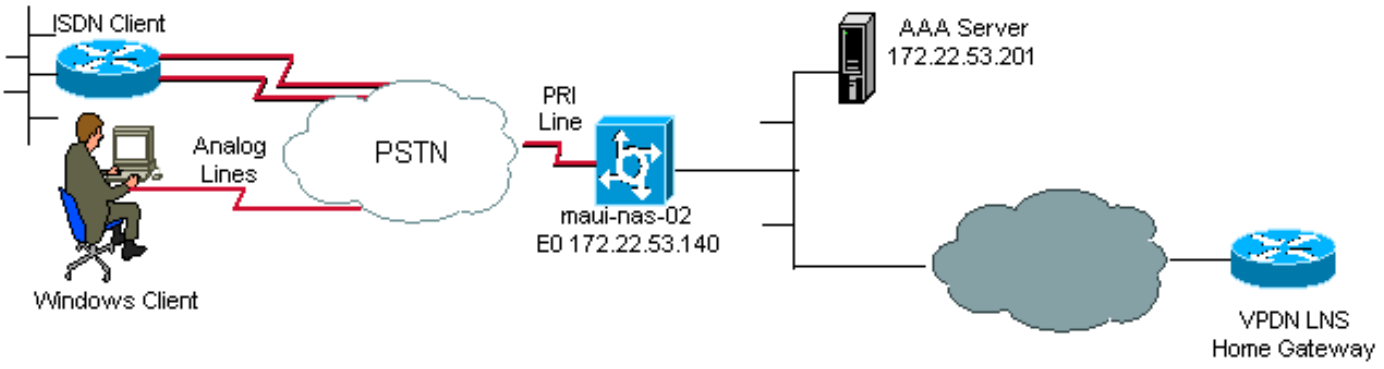
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

أوامر VPDN الوحيدة الضرورية على NAS (LAC) لدعم شبكات VPDN لكل مستخدم هي أوامر التكوين العام **vpdn enable** و**VPDN authen-before-forward**. يرشد الأمر **VPDN authen-before-forward** NAS (LAC) لمصادقة اسم المستخدم الكامل قبل أن يتخذ قرار إعادة التوجيه. يتم بعد ذلك إنشاء نفق VPDN، استنادا إلى المعلومات التي تم إرجاعها من قبل خادم AAA لهذا المستخدم الفردي؛ إذا لم يتم إرجاع معلومات VPDN من خادم AAA، يتم إنهاء المستخدم محليا. يوضح التكوين في هذا القسم الأوامر المطلوبة لدعم الأنفاق دون معلومات المجال في اسم المستخدم.

ملاحظة: هذا التكوين غير شامل. يتم تضمين أوامر VPDN والواجهة و AAA ذات الصلة فقط.

ملاحظة: يتجاوز نطاق هذا المستند مناقشة كل بروتوكول نفق محتمل وبروتوكول AAA. وبالتالي، يطبق هذا التكوين نفق L2TP مع خادم AAA RADIUS. عدل المبادئ والتكوين الذي تمت مناقشته هنا لتكوين أنواع النفق الأخرى أو بروتوكولات AAA.

يستعمل هذا وثيقة هذا تشكيل:

- (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
```

تكوين خادم RADIUS

فيما يلي بعض تكوينات المستخدم على خادم Cisco Secure ل RADIUS (CSU) Unix:

1. مستخدم سيتم إنهاؤه محليا على NAS:

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

2. مستخدم يجب إنشاء جلسة VPDN له:

```
"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
```

تستخدم NAS (LAC) السمات المحددة مع VPDN Cisco-AVPair لبدء نفق VPDN إلى البوابة الرئيسية. تأكد من تكوين البوابة الرئيسية لقبول أنفاق VPDN من وحدات التخزين المتصلة بالشبكة (NAS).

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show caller user**—يعرض المعلمات لمستخدم معين، مثل خط tty المستخدم والواجهة غير المتزامنة (رف أو فتحة أو منفذ) ورقم قناة DS0 ورقم المودم وعنوان IP المعين ومعلمات حزمة PPP و PPP وما إلى ذلك. إذا لم يدعم إصدار برنامج Cisco IOS هذا الأمر، فاستخدم الأمر **show user**.
- **show vpdn**— يعرض معلومات حول أنفاق بروتوكول L2F و L2TP النشطة ومعرفات الرسائل في شبكة VPDN.

عينة عرض أمر إنتاج

عند اتصال المكالمة، أستخدم الأمر username **show caller user** وكذلك الأمر **show vpdn** للتحقق من نجاح المكالمة. ويرد أدناه نموذج للمخرجات:

```
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
      HGW           est    172.22.53.141   1701  1     3  6318

LocID RemID TunID Intf       Username      State  Last Chg Fastswitch
   As12       vpdn_authen    est     00:09:33 enabled  6318     3     4
The tunnel for user vpdn_authen is in established state. %No active L2F tunnels %No active ---!
PPTP tunnels %No active PPPoE tunnel
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

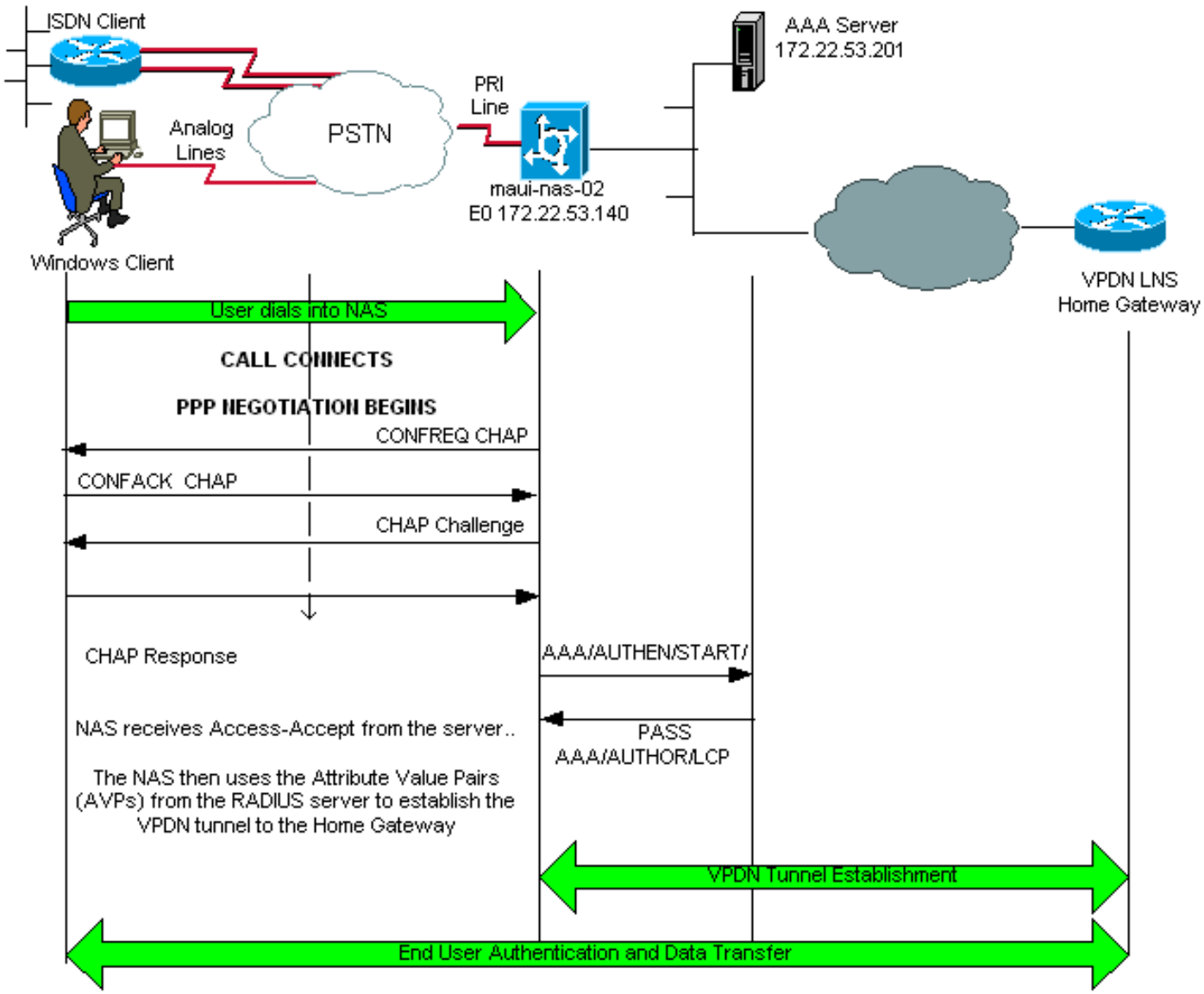
أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug ppp authentication**—يعرض رسائل بروتوكول مصادقة PPP، ويتضمن عمليات تبادل حزم بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (CHAP) وعمليات تبادل بروتوكول مصادقة كلمة المرور (PAP).
- **debug aaa authentication**—يعرض معلومات حول مصادقة AAA/RADIUS.
- **debug aaa authorization**—يعرض معلومات حول تفويض AAA/RADIUS.
- **debug radius** —يعرض معلومات تصحيح تفصيلية مرتبطة ب RADIUS. أستخدم أداة مترجم الإخراج (العملاء المسجلون فقط) لفك ترميز رسائل نصف قطر تصحيح الأخطاء. على سبيل المثال، راجع قسم إخراج **تصحيح الأخطاء** للعينة. أستخدم المعلومات من **debug radius** لتحديد السمات التي يتم التفاوض عليها.
- **debug tacacs**—يعرض معلومات تصحيح الأخطاء التفصيلية المرتبطة ب TACACS+.
- **debug vpdn event**— يعرض أخطاء L2x والأحداث التي هي جزء من إنشاء النفق العادي أو إيقاف تشغيله لشبكات VPDN.
- **debug vpdn خطأ**—يعرض أخطاء بروتوكول VPDN.
- **debug vpdn l2x-event**—يعرض أخطاء L2x والأحداث التفصيلية التي تعد جزءا من إنشاء نفق عادي أو إيقاف تشغيله لشبكات VPDN.
- **debug vpdn l2x-error**—يعرض أخطاء بروتوكول VPDN L2x.

إخراج تصحيح الأخطاء للعينة

فيما يلي إخراج **تصحيح الأخطاء** لإجراء مكالمة ناجحة. في هذا المثال، لاحظ أن NAS يحصل على سمات نفق VPDN من خادم 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 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
Access-Request, len 89 ,172.22.53.201:1645 6
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*
```

يتم دفع أزواج قيم السمات (AVPs) الضرورية لنفق VPDN إلى أسفل من خادم RADIUS. ومع ذلك، ينتج **نصف قطر تصحيح الأخطاء** مخرجات مشفرة تشير إلى AVPs وقيمها. يمكنك لصق المخرجات الموضحة بالخط **الغامق** أعلاه في أداة مترجم الإخراج (للعملاء المسجلين فقط). الناتج التالي بالأسود هو المخرج المفكك الذي تم الحصول عليه من الأداة:

```
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
```

معلومات ذات صلة

- يفهم VPDN
- تكوين شبكات الاتصال الخاصة الظاهرية
- كيفية تكوين مصادقة بروتوكول نفق الطبقة 2 باستخدام RADIUS
- كيفية تكوين مصادقة بروتوكول النفق للطبقة 2 باستخدام TACACS+
- صفحات دعم تقنية الوصول
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).