

VPDN-Konfiguration ohne AAA

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument zeigt ein Konfigurationsbeispiel, in dem das Layer 2 Tunneling Protocol (L2TP) für Virtual Private Dialup Network (VPDN) für ISDN- und analoge Einwahlanrufe konfiguriert wird. Bei dieser Konfiguration ist kein AAA-Server (Authentication, Authorization, and Accounting) erforderlich.

L2TP ist ein IETF-Standard (Internet Engineering Task Force), der die besten Funktionen zweier bestehender Tunneling-Protokolle kombiniert:

- Cisco Layer 2 Forwarding (L2F)
- Microsoft Point-to-Point Tunneling Protocol (PPTP)

In dieser Konfiguration wird L2TP verwendet, indem das Befehlsprotokoll **L2TP** hinzugefügt wird. Der Standardwert ist "L2F".

Cisco empfiehlt die Verwendung des Befehls **vpdn-group**, der in der Cisco IOS[®] Softwareversion 12.0(1)T eingeführt wurde, um die VPDN-Parameter in L2TP Access Concentrator (LAC) und L2TP Network Server (LNS) zu definieren. Wenn Sie die Befehle **vpdn incoming** und **vpdn outgoing** verwenden möchten, lesen Sie [Konfiguration von Virtual Private Dialup Networks \(Virtual Private Dialup-Netzwerke konfigurieren\)](#).

Diese Konfiguration zeichnet sich durch folgende Hauptmerkmale aus:

- Die LAC:identifiziert einen VPDN-Client basierend auf dem Domännennamen, der in der Antwort für die Authentifizierung (Challenge Handshake Authentication Protocol [CHAP] in dieser Konfiguration empfangen wurde) empfangen wurde.verwendet seine lokalen VPDN-Parameter, um den Tunnel und die Sitzung mit dem LNS aufzurufen.
- Das LNS:verwendet seine lokalen VPDN-Parameter, um den VPDN-Tunnel und die VPDN-

Sitzung von der LAC zu akzeptieren. Authentifiziert den Remote-Benutzer lokal. weist dem Client eine IP-Adresse aus seinem lokalen Pool zu.

Voraussetzungen

Verwendete Komponenten

Diese Konfiguration wurde mit den unten stehenden Software- und Hardwareversionen entwickelt und getestet.

- Hauptproduktreihe der Cisco IOS Software, Version 12.2 Die IP+-Funktion ist für VPDN erforderlich.
- Ein Cisco AS5300 (die LAC) mit einer E1-Karte und einer Mikrokarte. Sie kann ISDN- und analoge Anrufe annehmen.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

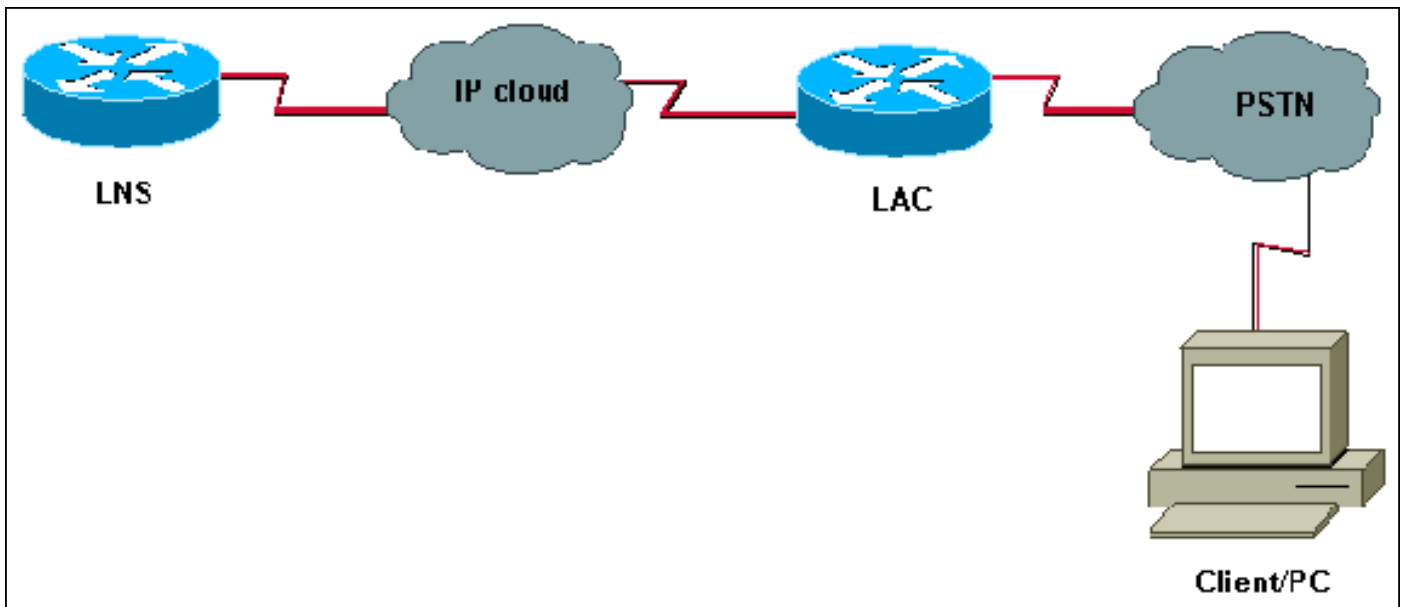
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

LAC

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname LAC
! spe 2/0 2/9
  firmware location system:/ucode/mica_port_firmware
!
!
modem country mica belgium
!
vpdn enable
! -- Enables VPDN. ! vpdn search-order domain ! -- VPDN
tunnel authorization is based on the domain name ! --
(the default is DNIS). ! vpdn-group GroupCisco request-
dialin protocol l2tp ! -- L2TP is used instead of the
default (L2F). domain cisco.com ! -- The domain name
cisco.com is used to identify a VPDN user when ! --
receiving the CHAP response from the user. initiate-to
ip 10.48.74.35 ! -- The tunnel and session are
initialized to the ethernet ip address of the ! -- LNS
10.48.74.35. l2tp tunnel password cisco ! -- for tunnel
authentication ! isdn switch-type primary-net5 !
controller E1 0 clock source line primary pri-group
timeslots 1-31 ! interface Ethernet0 ip address
10.48.75.7 255.255.254.0 ! interface Serial0:15 no ip
address encapsulation ppp dialer rotary-group 1 isdn
switch-type primary-net5 isdn incoming-voice modem !
interface Group-Async1 no ip address encapsulation ppp
async mode dedicated ppp authentication chap pap group-
range 1 120 ! interface Dialer1 no ip address
encapsulation ppp ppp authentication chap pap ! ip
classless ip route 0.0.0.0 0.0.0.0 10.48.74.1 ! line con
0 exec-timeout 0 0 line 1 120 modem InOut transport
input all line aux 0 line vty 0 4 exec-timeout 0 0
password cisco login !

```

LNS

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname LNS
!
username UserISDN@cisco.com password 0 cisco
username UserAnalog@cisco.com password 0 cisco
! -- The LNS authenticates the remote users locally. !
vpdn enable ! -- Enables VPDN. ! vpdn-group VPDN accept-
dialin ! -- Enables the LNS to accept VPDN request.
protocol l2tp !-- L2TP is used instead of the L2F
(default). virtual-template 1 ! -- For each user, the
virtual-template 1 is used to terminate the PPP session.
terminate-from hostname LAC ! -- The LNS accepts VPDN
request from router LAC. l2tp tunnel password cisco ! --
for tunnel authentication ! ! ! interface Loopback1 ip
address 12.12.12.1 255.255.255.255 no ip route-cache no
ip mroute-cache ! interface Ethernet0 ip address
10.48.74.35 255.255.254.0 no ip route-cache no ip
mroute-cache no cdp enable ! interface Virtual-Template1
! -- The PPP session is terminated in the virtual-access
cloned from this ! -- virtual-template ip unnumbered
Loopback1 peer default ip address pool GroupCisco ppp
authentication chap pap ! ip local pool GroupCisco
12.12.12.2 12.12.12.50 ! -- The LNS assigns an ip
address to the remote user ip classless ip route 0.0.0.0
0.0.0.0 10.48.74.1

```

Hinweis: In den obigen Konfigurationen haben wir die Dialer 1- und die Group-async1-Schnittstellen mit den mindestens verfügbaren PPP-Optionen (Point to Point Protocol) konfiguriert.

Um mehr Funktionen auf PPP-Ebene (ppp multilink, komprimieren usw.) zu ermöglichen, müssen diese Funktionen auf diesen Schnittstellen und auf der virtuellen Vorlage 1 des LNS hinzugefügt werden.

Wichtig: Die Regel ist, dass alle PPP-Optionen, die Sie in der Dialer 1- und der Group-Async1-Schnittstelle definieren, in der virtuellen Vorlage 1 des LNS konfiguriert werden müssen.

Die virtuelle Vorlage 1 erhält eine "Kopie" der zwischen der LAC und dem Client ausgehandelten LCP-Optionen. Wenn eine zwischen der LAC und dem Client ausgehandelte Option nicht in der virtuellen Vorlage 1 konfiguriert ist, löscht das LNS die VPDN-Sitzung. Damit das LNS jedoch das LCP mit dem Client neu verhandeln kann, legen Sie die Befehle **lcp reNegotiation immer** oder **lcp reNegotiation on-Mismatch** in der VPDN-Gruppe fest.

Hinweis: Standardmäßig verwenden die LAC und das LNS ihren Hostnamen in den L2TP-Austauschpaketen. Um dieses Verhalten zu ändern, definieren Sie den **lokalen** Befehl in der vpdn-Gruppe. Sehen wir uns ein Beispiel einer LNS-Konfiguration an:

```

vpdn-group VPDN
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname LAC
local name LNS-cental

```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

- **show vpdn tunnel** - Zeigt Informationen zu allen aktiven L2F- und L2TP-Tunneln im Zusammenfassungsformat an.
- **show caller ip**: Zeigt eine Zusammenfassung der Anruferinformationen für die von Ihnen angegebene IP-Adresse an.

[Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

[Befehle zur Fehlerbehebung](#)

Hinweis: Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug**-Befehlen finden Sie unter [Wichtige Informationen](#).

Auf LAC:

- **debug vpdn event** - Zeigt L2TP-Fehler und -Ereignisse an, die Teil der normalen Tunneleinrichtung oder -abschaltung für VPDNs sind.
- **debug vpdn l2x-event**: Zeigt Meldungen über Ereignisse an, die zum normalen Tunnelaufbau oder -abfahren für 12x gehören.
- **debug vpdn l2x-error** - Zeigt l2x-Protokollfehler an, die das Erstellen von l2x verhindern oder dessen normalen Betrieb verhindern.
- **debug ppp negotiation** - Veranlasst den Befehl debug ppp, während des PPP-Starts übertragene PPP-Pakete anzuzeigen, über die PPP-Optionen ausgehandelt werden.
- **debug isdn q931** - Zeigt Informationen zum Einrichten und Beenden von ISDN-Netzwerkverbindungen (Layer 3) zwischen dem lokalen Router (Benutzerseite) und dem Netzwerk an.
- **debug modem** - Zeigt die Aktivität der Modemleitung auf einem Zugriffsserver an.

Im LNS:

- **debuggen vpdn ereignis**
- **debug vpdn l2x-event**
- **debug vpdn l2x-Fehler**
- **debug vtemplate** - Zeigt Informationen zum Klonen einer virtuellen Zugriffsschnittstelle an, vom Zeitpunkt des Klonens von einer virtuellen Vorlage bis hin zum Zeitpunkt des Abbruchs der virtuellen Zugriffsschnittstelle beim Beenden des Anrufs.
- **Debug-ppp-Aushandlung**

Unten sehen Sie einen ISDN-Anruf vom Client UserISDN@cisco.com.

Debuggen Befehle auf der LAC

Die LAC erhält einen ISDN-Anruf von der Nummer 8101.

LAC#
*Feb 1 14:45:09.684: ISDN Se0:15: RX <- SETUP pd = 8 callref = 0x3D03
*Feb 1 14:45:09.688: Sending Complete
*Feb 1 14:45:09.688: Bearer Capability i = 0x8890
*Feb 1 14:45:09.688: Channel ID i = 0xA18387
*Feb 1 14:45:09.688: Calling Party Number i = 0xA1, '8101', Plan:ISDN,
Type:National
*Feb 1 14:45:09.688: Called Party Number i = 0x81, '214', Plan:ISDN,
Type:Unknown
*Feb 1 14:45:09.692: %LINK-3-UPDOWN: Interface Serial0:6,
changed state to up
*Feb 1 14:45:09.692: Se0:6 PPP: Treating connection as a callin
*Feb 1 14:45:09.692: Se0:6 PPP: Phase is ESTABLISHING, Passive Open
[0 sess, 0 load]
*Feb 1 14:45:09.692: Se0:6 LCP: State is Listen
*Feb 1 14:45:09.696: ISDN Se0:15: TX -> CALL_PROC pd = 8 callref = 0xBD03
*Feb 1 14:45:09.696: Channel ID i = 0xA98387
*Feb 1 14:45:09.696: ISDN Se0:15: TX -> CONNECT pd = 8 callref = 0xBD03
*Feb 1 14:45:09.696: Channel ID i = 0xA98387
*! -- The ISDN phase is finished and the B channel is up ! -- as soon as the LAC receives RX <-
CONNECT_ACK. *Feb 1 14:45:09.752: ISDN Se0:15: RX <- CONNECT_ACK pd = 8 callref = 0x3D03 *Feb 1
14:45:09.752: ISDN Se0:15: CALL_PROGRESS: CALL_CONNECTED call id 0x90, bchan 6, dsl 0 ! -- PPP
starts with LCP phase : authentication protocol and other LCP ! -- options (compression,
multilink, and so on) are negotiated. ! -- In the debug below, only chap is negotiated. *Feb 1
14:45:09.844: Se0:6 LCP: I CONFREQ [Listen] id 179 len 10 *Feb 1 14:45:09.844: Se0:6 LCP:
MagicNumber 0x5B90B785 (0x05065B90B785) *Feb 1 14:45:09.844: Se0:6 LCP: O CONFREQ [Listen] id 1
len 15 *Feb 1 14:45:09.844: Se0:6 LCP: AuthProto CHAP (0x0305C22305) *Feb 1 14:45:09.844: Se0:6
LCP: MagicNumber 0x1A9DC8A5 (0x05061A9DC8A5) *Feb 1 14:45:09.844: Se0:6 LCP: O CONFACK [Listen]
id 179 len 10 *Feb 1 14:45:09.844: Se0:6 LCP: MagicNumber 0x5B90B785 (0x05065B90B785) *Feb 1
14:45:09.876: Se0:6 LCP: I CONFACK [ACKsent] id 1 len 15 *Feb 1 14:45:09.876: Se0:6 LCP:
AuthProto CHAP (0x0305C22305) *Feb 1 14:45:09.876: Se0:6 LCP: MagicNumber 0x1A9DC8A5
(0x05061A9DC8A5) *Feb 1 14:45:09.876: Se0:6 LCP: State is Open *Feb 1 14:45:09.876: Se0:6 PPP:
Phase is AUTHENTICATING, by this end [0 sess, 0 load] ! -- The LAC sends the client a CHAP
challenge. *Feb 1 14:45:09.876: Se0:6 CHAP: O CHALLENGE id 1 len 24 from "LAC". ! -- The LAC
receives the CHAP response from the client with username ! -- UserISDN@cisco.com. *Feb 1
14:45:09.924: Se0:6 CHAP: I RESPONSE id 1 len 39 from "UserISDN@cisco.com" ! -- The LAC checks
out if UserISDN@cisco.com is a VPDN client or not. ! -- Because the domain cisco.com is
configured in the vpdn-group ! -- GroupCisco, UserISDN@cisco.com is a VPDN client. The LAC takes
! -- the VPDN parameters in the vpdn-group where the domain name ! -- cisco.com is located. *Feb
1 14:45:09.924: Se0:6 PPP: Phase is FORWARDING [0 sess, 0 load] *Feb 1 14:45:09.924: Se0:6 VPDN:
Got DNIS string 214 *Feb 1 14:45:09.924: Se0:6 VPDN: Looking for tunnel -- cisco.com -- *Feb 1
14:45:09.928: Se0:6 VPDN/RPMS/GroupCisco: Got tunnel info for cisco.com *Feb 1 14:45:09.928:
Se0:6 VPDN/RPMS/GroupCisco: LAC *Feb 1 14:45:09.928: Se0:6 VPDN/RPMS/GroupCisco: l2tp-busy-
disconnect yes *Feb 1 14:45:09.928: Se0:6 VPDN/RPMS/GroupCisco: IP 10.48.74.35 *Feb 1
14:45:09.928: Se0:6 VPDN/GroupCisco: curlvl 1 Address 0: 10.48.74.35, priority 1 *Feb 1
14:45:09.928: Se0:6 VPDN/GroupCisco: Select non-active address 10.48.74.35, priority 1 *Feb 1
14:45:09.928: Se0:6 VPDN: Find LNS process created *Feb 1 14:45:09.928: Tnl 2027 L2TP: SM State
idle ! -- In order to bring up the tunnel, the LAC sends SCCRQ (Start Control ! -- Connection
Request) to the LNS. ! -- A CHAP challenge is included in the packet. *Feb 1 14:45:09.928: Tnl
2027 L2TP: O SCCRQ *Feb 1 14:45:09.928: Tnl 2027 L2TP: Tunnel state change from idle to wait-
ctl-reply *Feb 1 14:45:09.928: Tnl 2027 L2TP: SM State wait-ctl-reply *Feb 1 14:45:09.928: Se0:6
VPDN: Forward to address 10.48.74.35 *Feb 1 14:45:09.928: Se0:6 VPDN: Pending *Feb 1
14:45:09.932: Se0:6 VPDN: Process created ! -- The LAC receives from the LNS SCCRQ (Start
Control Connection Reply). ! -- The response to its own challenge and another chap challenge from
the LNS ! -- are included in the packet. *Feb 1 14:45:09.956: Tnl 2027 L2TP: I SCCRQ from LNS
*Feb 1 14:45:09.956: Tnl 2027 L2TP: Got a challenge from remote peer, LNS *Feb 1 14:45:09.956:
Tnl 2027 L2TP: Got a response from remote peer, LNS *Feb 1 14:45:09.956: Tnl 2027 L2TP: Tunnel
Authentication success *Feb 1 14:45:09.956: Tnl 2027 L2TP: Tunnel state change from wait-ctl-
reply to established ! -- The LAC sends to the LNS SCCCN (Start Control Connection Connected). !
-- The response to LNS's challenge is included in the packet. *Feb 1 14:45:09.956: Tnl 2027
L2TP: O SCCCN to LNS tnlid 11514 *Feb 1 14:45:09.956: Tnl 2027 L2TP: SM State established *Feb 1
14:45:09.956: Se0:6 VPDN: Forwarding... *Feb 1 14:45:09.956: Se0:6 VPDN: Bind interface*

direction=1 *Feb 1 14:45:09.956: Tnl/Cl 2027/18 L2TP: Session FS enabled *Feb 1 14:45:09.956: Tnl/Cl 2027/18 L2TP: Session state change from idle to wait-for-tunnel *Feb 1 14:45:09.960: Se0:6 Tnl/Cl 2027/18 L2TP: Create session *Feb 1 14:45:09.960: Tnl 2027 L2TP: SM State established ! -- *The Tunnel is up. The LAC brings up the session for the user ! -- UserISDN@cisco.com. For that, it sends ICRQ (Incoming Call ReQuest).* *Feb 1 14:45:09.960: Se0:6 Tnl/Cl 2027/18 L2TP: O ICRQ to LNS 11514/0 *Feb 1 14:45:09.960: Se0:6 Tnl/Cl 2027/18 L2TP: Session state change from wait-for-tunnel to wait-reply *Feb 1 14:45:09.960: Se0:6 VPDN: UserISDN@cisco.com is forwarded ! -- *After receiving ICRP (Incoming Call Reply, we don't see it in the debug) ! -- the LAC sends ICCN Incoming Call Connected. The VPDN session is up . ! -- Then the LAC forwards to the LNS what it has negotiated with the client ! -- (LCP options) along with the username and chap password of the client.* *Feb 1 14:45:10.008: Se0:6 Tnl/Cl 2027/18 L2TP: O ICCN to LNS 11514/6 *Feb 1 14:45:10.008: Se0:6 Tnl/Cl 2027/18 L2TP: Session state change from wait-reply to established *Feb 1 14:45:10.960: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:6, changed state to up *Feb 1 14:45:15.692: %ISDN-6-CONNECT: Interface Serial0:6 is now connected to 8101 UserISDN@cisco.com LAC#

Debuggen Befehle im LNS

Das LNS empfängt SCCRQ von der LAC.

LNS#
*Mar 1 02:13:06.499: L2TP: I SCCRQ from LAC tnl 2027
*Mar 1 02:13:06.507: Tnl 11514 L2TP: Got a challenge in SCCRQ, LAC
*Mar 1 02:13:06.511: Tnl 11514 L2TP: New tunnel created for remote LAC, address 10.48.75.7
! -- The LNS replies with SCCRP which includes the CHAP response to LAC's ! -- challenge and a CHAP challenge. *Mar 1 02:13:06.515: Tnl 11514 L2TP: O SCCRP to LAC tnlid 2027 *Mar 1 02:13:06.523: Tnl 11514 L2TP: Tunnel state change from idle to wait-ctl-reply ! -- *The LNS receives SCCCN.* *Mar 1 02:13:06.535: Tnl 11514 L2TP: I SCCCN from LAC tnl 2027 *Mar 1 02:13:06.539: Tnl 11514 L2TP: Got a Challenge Response in SCCCN from LAC *Mar 1 02:13:06.543: Tnl 11514 L2TP: Tunnel Authentication success *Mar 1 02:13:06.543: Tnl 11514 L2TP: Tunnel state change from wait-ctl-reply to established *Mar 1 02:13:06.547: Tnl 11514 L2TP: SM State established ! -- *The tunnel is up. The LNS receives ICRQ to bring up the session.* *Mar 1 02:13:06.555: Tnl 11514 L2TP: I ICRQ from LAC tnl 2027 *Mar 1 02:13:06.559: Tnl/Cl 11514/6 L2TP: Session FS enabled *Mar 1 02:13:06.563: Tnl/Cl 11514/6 L2TP: Session state change from idle to wait-connect *Mar 1 02:13:06.567: Tnl/Cl 11514/6 L2TP: New session created ! -- *The LNS replies with ICRP (Incoming Call Reply).* *Mar 1 02:13:06.567: Tnl/Cl 11514/6 L2TP: O ICRP to LAC 2027/18 ! -- *The LNS receives ICCN (Incoming Call coNnected). The VPDN sesion is up, ! -- then the LNS receives the LCP layer along with the username ! -- and chap password of the client. ! -- A virtual-access is cloned from the virtual-template 1.* *Mar 1 02:13:06.583: Tnl/Cl 11514/6 L2TP: I ICCN from LAC tnl 2027, cl 18 *Mar 1 02:13:06.591: Tnl/Cl 11514/6 L2TP: Session state change from wait-connect to established *Mar 1 02:13:06.591: Vt1 VTEMPLATE: Unable to create and clone vaccess *Mar 1 02:13:06.595: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 1 *Mar 1 02:13:06.595: Vi1 VTEMPLATE: Hardware address 0000.0c4a.4314 *Mar 1 02:13:06.599: Vi1 VPDN: Virtual interface created for UserISDN@cisco.com *Mar 1 02:13:06.603: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load] *Mar 1 02:13:06.603: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking *Mar 1 02:13:06.607: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate *Mar 1 02:13:06.611: Vi1 VTEMPLATE: ***** CLONE VACCESS1 ***** *Mar 1 02:13:06.615: Vi1 VTEMPLATE: Clone from Virtual-Template1 interface Virtual-Access1 default ip address no ip address encaps ppp ip unnumbered Loopback1 end *Mar 1 02:13:07.095: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up *Mar 1 02:13:07.099: Vi1 PPP: Using set call direction *Mar 1 02:13:07.103: Vi1 PPP: Treating connection as a callin *Mar 1 02:13:07.103: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load] *Mar 1 02:13:07.107: Vi1 LCP: State is Listen *Mar 1 02:13:07.111: Vi1 VPDN: Bind interface direction=2 *Mar 1 02:13:07.111: Vi1 LCP: I FORCED CONFREQ len 11 *Mar 1 02:13:07.115: Vi1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 02:13:07.119: Vi1 LCP: MagicNumber 0x1A9DC8A5 (0x05061A9DC8A5) *Mar 1 02:13:07.119: Vi1 VPDN: PPP LCP accepted rcv CONFACK *Mar 1 02:13:07.123: Vi1 LCP: I FORCED CONFACK len 6 *Mar 1 02:13:07.127: Vi1 LCP: MagicNumber 0x5B90B785 (0x05065B90B785) *Mar 1 02:13:07.131: Vi1 VPDN: PPP LCP accepted sent CONFACK ! -- *The LNS authenticates the user. It doesn't send a new CHAP challenge ! -- (the debug may be confusing) since it has received the CHAP challenge ! -- and response from the LAC.* *Mar 1 02:13:07.131: Vi1 PPP: Phase is AUTHENTICATING, by this end [0 sess, 0 load] *Mar 1 02:13:07.135: Vi1 CHAP: O CHALLENGE id 2 len 24 from "LNS" *Mar 1 02:13:07.143: Vi1 CHAP: I RESPONSE id 1 len 39 from "UserISDN@cisco.com" *Mar 1 02:13:07.151: Vi1 CHAP: O SUCCESS id 1 len

```
4 *Mar 1 02:13:07.155: Vi1 PPP: Phase is UP [0 sess, 0 load] ! -- The IPCP phase starts. ! --
The IP address 12.12.12.2 is assigned to the client. *Mar 1 02:13:07.159: Vi1 IPCP: O CONFREQ
[Closed] id 1 len 10 *Mar 1 02:13:07.163: Vi1 IPCP: Address 12.12.12.1 (0x03060C0C0C01) *Mar 1
02:13:07.215: Vi1 IPCP: I CONFREQ [REQsent] id 34 len 10 *Mar 1 02:13:07.219: Vi1 IPCP: Address
0.0.0.0 (0x030600000000) *Mar 1 02:13:07.223: Vi1 IPCP: Pool returned 12.12.12.2 *Mar 1
02:13:07.227: Vi1 IPCP: O CONFNAK [REQsent] id 34 len 10 *Mar 1 02:13:07.231: Vi1 IPCP: Address
12.12.12.2 (0x03060C0C0C02) *Mar 1 02:13:07.235: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10 *Mar
1 02:13:07.239: Vi1 IPCP: Address 12.12.12.1 (0x03060C0C0C01) *Mar 1 02:13:07.271: Vi1 IPCP: I
CONFREQ [ACKrcvd] id 35 len 10 *Mar 1 02:13:07.275: Vi1 IPCP: Address 12.12.12.2
(0x03060C0C0C02) *Mar 1 02:13:07.279: Vi1 IPCP: O CONFACK [ACKrcvd] id 35 len 10 *Mar 1
02:13:07.283: Vi1 IPCP: Address 12.12.12.2 (0x03060C0C0C02) *Mar 1 02:13:07.287: Vi1 IPCP: State
is Open *Mar 1 02:13:07.295: Vi1 IPCP: Install route to 12.12.12.2 ! -- The virtual-access is
up. *Mar 1 02:13:08.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up LNS#
```

zeigen Befehle

```
LAC#show vpdn tunnel
```

```
L2TP Tunnel Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions
 36556 45655 LNS est 10.48.74.35 1701 1
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
LAC#
```

```
LNS#show vpdn tunnel
```

```
L2TP Tunnel Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions
 45655 36556 LAC est 10.48.75.7 1701 1
%No active L2F tunnels
%No active PPTP tunnels
%No active
```

```
LNS#show caller ip
```

```
Line User IP Address Local Number Remote Number <->
Vi1 UserISDN@cisco.com \
12.12.12.2 214 8101 in
LNS#
```

Zugehörige Informationen

- [Unterstützung von DFÜ- und Zugriffstechnologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)