Настройка инициируемого клиентом туннельного соединения L2TP с компьютером под управлением Windows 2000

Содержание

Введение

В большинстве сценариев виртуальной частной коммутируемой сети (VPDN) клиент набирает сервер доступа к сети (NAS). NAS тогда инициирует протокол туннелирования на уровне 2 (L2TP) VPDN или протокол туннеля переадресации уровня 2 (L2F) к Домашнему шлюзу (HGW). Это создает соединение VPDN между NAS, который является оконечной точкой Концентратора доступа L2TP (LAC) и HGW, который является оконечной точкой L2TP Network Server (LNS). Это означает, что только ссылка между NAS и HGW использует L2TP, и что туннель не включает ссылку от клиентского компьютера до NAS. Однако ПК - клиенты, выполняющие операционную систему Windows 2000, теперь в состоянии стать LAC и инициировать туннель L2TP от ПК через NAS и завершенный на HGW/LNS. Этот пример конфигурации показывает, как можно настроить такой туннель.

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются эти требования:

- Знакомство с пониманием VPDN
- Знакомство с резюме наборного (телефонный) доступа VPDN доступа Использование L2TP

Примечание: Конфигурация NAS не включена в этот документ.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- LNS: Маршрутизатор Cisco серии 7200 рабочий релиз 12.2 программного обеспечения Cisco IOS (1)
- Клиент: ПК Windows 2000 с модемом

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Конфигурация для LNS, включенного в этот документ, не является определенной платформой и может быть применена к любому МАРШРУТИЗАТОРУ С ПОДДЕРЖКОЙ VPDN.

Процедура для настройки клиентского компьютера Windows 2000 применима только к Windows 2000 а не к любой другой операционной системе.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Общие сведения

Как упомянуто во Введении, с Windows 2000 можно инициировать туннель L2TP от клиентского компьютера и завершать туннель где угодно в сети интернет-провайдера (ISP). Использование терминологии VPDN, эта настройка упоминается как "инициируемый клиентами" туннель. Так как инициированные клиентом туннели являются туннелями, инициируемыми клиентским программным обеспечением на ПК, ПК берет на себя роль LAC. Так как клиент будет аутентифицироваться с помощью Протокола PPP, Протокола аутентификации по квитированию вызова (CHAP) или Протокола аутентификации пароля (PAP) так или иначе, сам туннель не должен аутентифицироваться.

Преимущества и недостатки использования инициированных клиентом туннелей

Инициированные клиентом туннели имеют оба преимущества и недостатка, некоторые из которых выделены здесь:

Преимущества:

- Это защищает все соединение от клиента через общую сеть интернет-провайдера и к корпоративной сети.
- Это *не* требует дополнительной настройки на сети ISP. Без инициированного клиентом туннеля NAS интернет-провайдера или его RADIUS/TACACS + сервер должен быть настроен для инициирования туннеля к HGW. Поэтому предприятие должно выполнить согласование со многими интернет-провайдерами, чтобы позволить пользователям туннелировать через их сеть. С инициированным клиентом туннелем конечный пользователь может соединиться с любым интернет-провайдером и затем вручную инициировать туннель к корпоративной сети.

Недостатки:

- Это не является столь же масштабируемым как инициируемый ИНТЕРНЕТ-ПРОВАЙДЕРОМ туннель. Так как инициированные клиентом туннели создают отдельные туннели для каждого клиента, HGW должен индивидуально завершить большое число туннелей.
- Клиент должен управлять, клиентское программное обеспечение использовало инициировать туннель. Это часто - источник связанных с поддержкой проблем для предприятия.
- У клиента должна быть учетная запись с интернет-провайдером. Так как инициированные клиентом туннели могут только быть созданы после того, как соединение с интернет-провайдером установлено, у клиента должна быть учетная запись для соединения с сетью ISP.

Принцип работы

Thjs - то, как работает пример в этом документе:

1. Диски клиентского компьютера в NAS, аутентифицирует использование учетной записи интернет-провайдера клиента и получает IP-адрес из интернет-провайдера.
2. Клиент инициирует и создает туннель L2TP к HGW L2TP Network Server (LNS). Клиент пересмотрит IP Control Protocol (IPCP) и получит новый IP-адрес из LNS.

Настройте клиента Windows 2000 для L2TP

Создайте два соединения удаленного доступа к сети (DUN):

- Одно подключение DUN к наборному (телефонный) доступу к интернет-провайдеру. См. вашего интернет-провайдера для получения дополнительной информации об этом предмете.
- Другое подключение DUN для туннеля L2TP.

Чтобы создать и настроить подключение DUN для L2TP, выполните эти шаги в клиентский компьютер Windows 200:

1. От Меню Пуск выберите **Settings> Control Panel> Network и Dial-up Connections> Make New Connection**.Используйте Мастера для создания соединения, названного L2TP. Удостоверьтесь, что выбрали **Connect к частной сети через Интернет** в окне **Network Connection Type**. Необходимо также задать IP-адрес или название LNS/HGW.
2. Новое соединение (названный L2TP) появляется в окне **Network и Dial-up Connections** под Панелью управления. Отсюда, щелкните правой кнопкой мыши для

редактирования **Свойств**.

3. Нажмите Вкладку Сеть и удостоверьтесь, что **Type of Server I Am Calling** установлен в **L2TP**.
4. Если вы планируете выделить динамическое внутреннее (корпоративная сеть), адрес этому клиенту от HGW, или через локальный пул или через DHCP, выбирает протокол **TCP/IP**. Удостоверьтесь, что клиент настроен для получения IP-адреса автоматически. Можно также выполнить информацию о Domain Naming System (DNS) автоматически.**Кнопка Advanced позволяет определять статический сервис Windows назначения имен в Интернете (WINS) и информацию DNS. Вкладка Options позволяет выключать IPSec или назначать другую политику для подключения.** На вкладке Security можно определить параметры аутентификации пользователя. Например, PAP, CHAP или MS-CHAP, а также вход в систему домена Windows. Консультируйтесь с администратором для получения сведений сетевых систем на параметрах, которые должны быть настроены на клиенте.
5. Как только соединение настроено, можно дважды нажать его, чтобы появиться экран входа в систему, и затем соединиться.

Дополнительные замечания

Если ваш туннель L2TP использует IP-безопасность (IPSec) и/или Средства шифрования Microsoft точка-точка (MPPE), то необходимо определить эту команду под конфигурацией virtual-template на LNS/HGW.

```
ppp encrypt mppe 40
```

Следует иметь в виду, что это требует зашифрованного набора функции ПО Cisco IOS (по крайней мере, набор функций IPSec или IPSec с 3DES).

По умолчанию IPSec включен на Windows 2000. Если вы хотите отключить его, необходимо модифицировать Реестр Windows с помощью Редактора реестра:

Отключите IPSec на ПК Win2K

% Warning: Примите соответствующие меры (такие как выполнение резервное копирование реестра) до изменения реестра. Необходимо также обратиться к узлу Веб-узла Microsoft для корректной процедуры для изменения реестра.

Для добавления Значения ключа ProhibitIPSec в реестре к основанному на Windows 2000 компьютеру используйте Regedt32.exe для определения местоположения этого ключа в реестре:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Добавьте это значение реестра в следующий раздел:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

Примечание: Необходимо перезагрузить основанный на Windows 2000 компьютер для изменений для вступления в силу. См. эти статьи microsoft для получения дальнейшей информации.

- Q258261 - Отключение политики IPsec, используемой с L2TP
- Q240262 - Как Настроить Соединение L2TP/IPSec Использование Предварительного общего ключа

Для более сложной настройки с помощью Windows 2000 обратитесь к Cisco IOS Настройки и Клиентам Windows 2000 для L2TP Использование Microsoft IAS.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

Схема сети ниже показов различные согласования, которые происходят среди клиентского компьютера, NAS интернет-провайдера и HGW Предприятия. Пример отладки в разделе Устранения неполадок изображает эти транзакции также.

Конфигурации

В данном документе используется следующая конфигурация:

- fifi (LNS/HGW VPDN)

Примечание: Только соответствующий раздел конфигурации LNS включен.

fifi (LNS/HGW VPDN)

```
hostname fifi
!
username l2tp-w2k password 0 ww
!--- This is the password for the Windows 2000 client.
!--- With AAA, the username and password can be
offloaded to the external !--- AAA server. ! vpdn enable
!--- Activates VPDN. ! vpdn-group l2tp-w2k !--- This is
the default L2TP VPDN group. accept-dialin protocol l2tp
!--- This allows L2TP on this VPDN group. virtual-
template 1 !--- Use virtual-template 1 for the virtual-
interface configuration. no l2tp tunnel authentication
!--- The L2TP tunnel is not authenticated. !--- Tunnel
authentication is not needed because the client will be
!--- authenticated using PPP CHAP/PAP. Keep in mind that
the client is the !--- only user of the tunnel, so
client authentication is sufficient. ! interface
loopback 0 ip address 1.1.1.1 255.255.255.255 !
interface Ethernet1/0 ip address 200.0.0.14
255.255.255.0 ip router isis duplex half tag-switching
ip ! interface Virtual-Template1 !--- Virtual-Template
interface specified in the vpdn-group configuration. ip
unnumbered Loopback0 peer default ip address pool pptp
!--- IP address for the client obtained from IP pool
named pptp (defined below). ppp authentication chap ! ip
local pool pptp 1.100.0.1 1.100.0.10 !--- This defines
the "Internal" IP address pool (named pptp) for the
```

```
client. ip route 199.0.0.0 255.255.255.0 200.0.0.45
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show vpdn** об активном туннеле L2x и идентификаторах сообщения в VPDN.
- **show vpdn session window** — Отображает информацию на окне для сеанса VPDN.
- **show user** — Предоставляет всестороннюю распечатку всех пользователей, связанных с маршрутизатором.
- *show caller user username detail* — Для показа параметров для индивидуального пользователя, таких как Протокол управления каналом (LCP), NCP и состояния IPCP, а также назначенный IP-адрес, PPP и параметры пакета PPP, и так далее.

```
show vpdn --------- L2TP Tunnel and Session Information Total tunnels 1 sessions 1 !--- Note
that there is one tunnel and one session. LocID RemID Remote Name State Remote Address Port
Sessions 25924 1 JVEYNE-W2K1.c est 199.0.0.8 1701 1 !--- This is the tunnel information. !---
The Remote Name shows the client PC's computer name, as well as the !--- IP address that was
originally given to the client by the NAS. (This !--- address has since been renegotiated by the
LNS.) LocID RemID TunID Intf Username State Last Chg Fastswitch 2 1 25924 Vi1 l2tp-w2k est
00:00:13 enabled !--- This is the session information. !--- The username the client used to
authenticate is l2tp-w2k. %No active L2F tunnels %No active PPTP tunnels %No active PPPoE
tunnels show vpdn session window -------------------- L2TP Session Information Total tunnels 1
sessions 1 LocID RemID TunID ZLB-tx ZLB-rx Rbit-tx Rbit-rx WSize MinWS Timeouts Qsize 2 1 25924
0 0 0 0 0 0 0 0 %No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnels show
user ---------- Line User Host(s) Idle Location * 0 con 0 idle 00:00:00 Interface User Mode Idle
Peer Address Vi1 l2tp-w2k Virtual PPP (L2TP ) 00:00:08 !--- User l2tp-w2k is connected on
Virtual-Access Interface 1. !--- Also note that the connection is identified as an L2TP tunnel.
show caller user l2tp-w2k detail ------------------------- User: l2tp-w2k, line Vi1, service
PPP L2TP Active time 00:01:08, Idle time 00:00:00 Timeouts: Absolute Idle Limits: - - Disconnect
in: - - PPP: LCP Open, CHAP (<- local), IPCP !--- The LCP state is Open. LCP: -> peer,
AuthProto, MagicNumber <- peer, MagicNumber, EndpointDisc NCP: Open IPCP !--- The IPCP state is
Open. IPCP: <- peer, Address -> peer, Address IP: Local 1.1.1.1, remote 1.100.0.2 !--- The IP
address assigned to the client is 1.100.0.2 (from the IP pool !--- on the LNS). VPDN: NAS , MID
2, MID Unknown HGW , NAS CLID 0, HGW CLID 0, tunnel open !--- The VPDN tunnel is open. Counts:
48 packets input, 3414 bytes, 0 no buffer 0 input errors, 0 CRC, 0 frame, 0 overrun 20 packets
output, 565 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу Важные сведения

о командах отладки.

- **debug ppp negotiation** — Отображает информацию на трафике PPP и обменивается при согласовании о компонентах PPP включая LCP, Аутентификацию и NCP. Успешное согласование PPP сначала открывает состояние LCP, затем аутентифицируется, и наконец выполняет согласование о NCP (обычно IPCP).
- **debug vpdn event– показывает сообщения о событиях, являющихся частью обычного процесса установки или завершения работы туннеля.**
- **debug vpdn error– показывает ошибки, не позволяющие установить туннель или вызывающие закрытие установленного туннеля.**
- **debug vpdn l2x-event** — Отображает сообщения о событиях, которые являются частью обычного создания туннеля или завершением для L2x.
- **debug vpdn l2x-error - отображает ошибки протокола L2x, мешающих установлению L2x или его нормальной работе.**

Примечание: Некоторые из этих линий **выходных данных отладки** разделены на составные строки для печатей.

Включите **команды отладки**, заданные выше на LNS, и инициируйте вызов от клиентского компьютера Windows 2000. Отладки здесь показывают запрос туннеля от клиента, установления туннеля, аутентификации клиента и пересмотра IP-адреса:

```
LNS: Incoming session from PC Win2K :
=====================================

*Jun  6 04:02:05.174: L2TP: I SCCRQ from JVEYNE-W2K1.cisco.com tnl 1 !--- This is the incoming
tunnel initiation request from the client PC. *Jun 6 04:02:05.178: Tnl 25924 L2TP: New tunnel
created for remote JVEYNE-W2K1.cisco.com, address 199.0.0.8 !--- The tunnel is created. Note
that the client IP address is the one !--- assigned by the NAS. !--- This IP address will be
renegotiatied later. *Jun 6 04:02:05.178: Tnl 25924 L2TP: O SCCRP to JVEYNE-W2K1.cisco.com tnlid
1 *Jun 6 04:02:05.178: Tnl 25924 L2TP: Tunnel state change from idle to wait-ctl-reply *Jun 6
04:02:05.346: Tnl 25924 L2TP: I SCCCN from JVEYNE-W2K1.cisco.com tnl 1 *Jun 6 04:02:05.346: Tnl
25924 L2TP: Tunnel state change from wait-ctl-reply to established !--- The tunnel is now
established. *Jun 6 04:02:05.346: Tnl 25924 L2TP: SM State established *Jun 6 04:02:05.358: Tnl
25924 L2TP: I ICRQ from JVEYNE-W2K1.cisco.com tnl 1 *Jun 6 04:02:05.358: Tnl/Cl 25924/2 L2TP:
Session FS enabled *Jun 6 04:02:05.358: Tnl/Cl 25924/2 L2TP: Session state change from idle to
wait-connect *Jun 6 04:02:05.358: Tnl/Cl 25924/2 L2TP: New session created *Jun 6 04:02:05.358:
Tnl/Cl 25924/2 L2TP: O ICRP to JVEYNE-W2K1.cisco.com 1/1 *Jun 6 04:02:05.514: Tnl/Cl 25924/2
L2TP: I ICCN from JVEYNE-W2K1.cisco.com tnl 1, cl 1 !--- The LNS receives ICCN (Incoming Call
coNnected). The VPDN session is up, then !--- the LNS receives the LCP layer along with the
username and CHAP password !--- of the client. A virtual-access will be cloned from the virtual-
template 1. *Jun 6 04:02:05.514: Tnl/Cl 25924/2 L2TP: Session state change from wait-connect to
established !--- A VPDN session is being established within the tunnel. *Jun 6 04:02:05.514: Vi1
VPDN: Virtual interface created for *Jun 6 04:02:05.514: Vi1 PPP: Phase is DOWN, Setup [0 sess,
0 load] *Jun 6 04:02:05.514: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking *Jun 6
04:02:05.566: Tnl/Cl 25924/2 L2TP: Session with no hwidb *Jun 6 04:02:05.570: %LINK-3-UPDOWN:
Interface Virtual-Access1, changed state to up *Jun 6 04:02:05.570: Vi1 PPP: Using set call
direction *Jun 6 04:02:05.570: Vi1 PPP: Treating connection as a callin *Jun 6 04:02:05.570: Vi1
PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load] *Jun 6 04:02:05.570: Vi1 LCP: State is
Listen *Jun 6 04:02:05.570: Vi1 VPDN: Bind interface direction=2 *Jun 6 04:02:07.546: Vi1 LCP: I
CONFREQ [Listen] id 1 len 44 !--- LCP negotiation begins. *Jun 6 04:02:07.546: Vi1 LCP:
MagicNumber 0x21A20F49 (0x050621A20F49) *Jun 6 04:02:07.546: Vi1 LCP: PFC (0x0702) *Jun 6
04:02:07.546: Vi1 LCP: ACFC (0x0802) *Jun 6 04:02:07.546: Vi1 LCP: Callback 6 (0x0D0306) *Jun 6
04:02:07.546: Vi1 LCP: MRRU 1614 (0x1104064E) *Jun 6 04:02:07.546: Vi1 LCP: EndpointDisc 1 Local
*Jun 6 04:02:07.546: Vi1 LCP: (0x131701708695CDF2C64730B5B6756CE8) *Jun 6 04:02:07.546: Vi1 LCP:
(0xB1AB1600000001) *Jun 6 04:02:07.550: Vi1 LCP: O CONFREQ [Listen] id 1 len 19 *Jun 6
04:02:07.550: Vi1 LCP: MRU 1460 (0x010405B4) *Jun 6 04:02:07.550: Vi1 LCP: AuthProto CHAP
(0x0305C22305) *Jun 6 04:02:07.550: Vi1 LCP: MagicNumber 0xFA95EEC3 (0x0506FA95EEC3) *Jun 6
04:02:07.550: Vi1 LCP: O CONFREJ [Listen] id 1 len 11 *Jun 6 04:02:07.550: Vi1 LCP: Callback 6
```

(0x0D0306) *Jun 6 04:02:07.550: Vi1 LCP: MRRU 1614 (0x1104064E) *Jun 6 04:02:07.710: Vi1 LCP: I CONFNAK [REQsent] id 1 len 8 *Jun 6 04:02:07.710: Vi1 LCP: MRU 1514 (0x010405EA) *Jun 6 04:02:07.710: Vi1 LCP: O CONFREQ [REQsent] id 2 len 15 *Jun 6 04:02:07.710: Vi1 LCP: AuthProto CHAP (0x0305C22305) *Jun 6 04:02:07.710: Vi1 LCP: MagicNumber 0xFA95EEC3 (0x0506FA95EEC3) *Jun 6 04:02:07.718: Vi1 LCP: I CONFREQ [REQsent] id 2 len 37 *Jun 6 04:02:07.718: Vi1 LCP: MagicNumber 0x21A20F49 (0x050621A20F49) *Jun 6 04:02:07.718: Vi1 LCP: PFC (0x0702) *Jun 6 04:02:07.718: Vi1 LCP: ACFC (0x0802) *Jun 6 04:02:07.718: Vi1 LCP: EndpointDisc 1 Local *Jun 6 04:02:07.718: Vi1 LCP: (0x131701708695CDF2C64730B5B6756CE8) *Jun 6 04:02:07.718: Vi1 LCP: (0xB1AB1600000001) *Jun 6 04:02:07.718: Vi1 LCP: O CONFACK [REQsent] id 2 len 37 *Jun 6 04:02:07.718: Vi1 LCP: MagicNumber 0x21A20F49 (0x050621A20F49) *Jun 6 04:02:07.718: Vi1 LCP: PFC (0x0702) *Jun 6 04:02:07.718: Vi1 LCP: ACFC (0x0802) *Jun 6 04:02:07.718: Vi1 LCP: EndpointDisc 1 Local *Jun 6 04:02:07.718: Vi1 LCP: (0x131701708695CDF2C64730B5B6756CE8) *Jun 6 04:02:07.718: Vi1 LCP: (0xB1AB1600000001) *Jun 6 04:02:07.858: Vi1 LCP: I CONFACK [ACKsent] id 2 len 15 *Jun 6 04:02:07.858: Vi1 LCP: AuthProto CHAP (0x0305C22305) *Jun 6 04:02:07.858: Vi1 LCP: MagicNumber 0xFA95EEC3 (0x0506FA95EEC3) *Jun 6 04:02:07.858: Vi1 **LCP: State is Open** *!--- LCP negotiation is complete.* *Jun 6 04:02:07.858: Vi1 PPP: Phase is AUTHENTICATING, by this end [0 sess, 0 load] *Jun 6 04:02:07.858: Vi1 **CHAP: O CHALLENGE id 5 len 25 from "fifi"** *Jun 6 04:02:07.870: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic 0x21A20F49 MSRASV5.00 *Jun 6 04:02:07.874: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic 0x21A20F49 MSRAS-1-JVEYNE-W2K1 *Jun 6 04:02:08.018: Vi1 **CHAP: I RESPONSE id 5 len 29 from "l2tp-w2k"** *Jun 6 04:02:08.018: Vi1 **CHAP: O SUCCESS** id 5 len 4 *!--- CHAP authentication is successful. If authentication fails, check the !--- username and password on the LNS.* *Jun 6 04:02:08.018: Vi1 PPP: Phase is UP [0 sess, 0 load] *Jun 6 04:02:08.018: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10 *Jun 6 04:02:08.018: Vi1 IPCP: Address 1.1.1.1 (0x030601010101) *Jun 6 04:02:08.158: Vi1 CCP: I CONFREQ [Not negotiated] id 5 len 10 *Jun 6 04:02:08.158: Vi1 CCP: MS-PPC supported bits 0x01000001 (0x120601000001) *Jun 6 04:02:08.158: Vi1 LCP: O PROTREJ [Open] id 3 len 16 protocol CCP (0x80FD0105000A120601000001) *Jun 6 04:02:08.170: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34 *Jun 6 04:02:08.170: Vi1 IPCP: Address 0.0.0.0 (0x030600000000) *Jun 6 04:02:08.170: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000) *Jun 6 04:02:08.170: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000) *Jun 6 04:02:08.170: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000) *Jun 6 04:02:08.170: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) *Jun 6 04:02:08.170: Vi1 **IPCP: Pool returned 1.100.0.2** *!--- This is the new "Internal" IP address for the client returned by the !--- LNS IP address pool.* *Jun 6 04:02:08.170: Vi1 IPCP: O CONFREJ [REQsent] id 6 Len 28 *Jun 6 04:02:08.170: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000) *Jun 6 04:02:08.170: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000) *Jun 6 04:02:08.170: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000) *Jun 6 04:02:08.170: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) *Jun 6 04:02:08.174: Vi1 IPCP: I CONFACK [REQsent] id 1 Len 10 *Jun 6 04:02:08.174: Vi1 IPCP: Address 1.1.1.1 (0x030601010101) *Jun 6 04:02:08.326: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 Len 10 *Jun 6 04:02:08.326: Vi1 IPCP: Address 0.0.0.0 (0x030600000000) *Jun 6 04:02:08.326: Vi1 IPCP: O CONFNAK [ACKrcvd] id 7 Len 10 *Jun 6 04:02:08.330: Vi1 IPCP: Address 1.100.0.2 (0x030601640002) *Jun 6 04:02:08.486: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 Len 10 *Jun 6 04:02:08.486: Vi1 IPCP: Address 1.100.0.2 (0x030601640002) *Jun 6 04:02:08.486: Vi1 IPCP: O CONFACK [ACKrcvd] id 8 Len 10 *Jun 6 04:02:08.490: Vi1 IPCP: Address 1.100.0.2 (0x030601640002) *Jun 6 04:02:08.490: Vi1 IPCP: State is Open *Jun 6 04:02:08.490: Vi1 IPCP: Install route to 1.100.0.2 *Jun 6 04:02:09.018: **%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up** *!--- The interface is up.*

Эти выходные данные отладки на LNS показывают клиенту Windows 2000 разъединение вызова. Обратите внимание на различные сообщения, где LNS распознает разъединение и выполняет чистое завершение туннеля:

*Jun 6 04:03:25.174: **Vi1 LCP: I TERMREQ** [Open] id 9 Len 16 (0x21A20F49003CCD7400000000) *!--- This is the incoming session termination request. This means that the client !--- disconnected the call.* *Jun 6 04:03:25.174: Vi1 LCP: O TERMACK [Open] id 9 Len 4 *Jun 6 04:03:25.354: Vi1 Tnl/Cl 25924/2 L2TP: I CDN from JVEYNE-W2K1.cisco.com tnl 1, CL 1 *Jun 6 04:03:25.354: Vi1 Tnl/CL 25924/2 L2TP: Destroying session *Jun 6 04:03:25.358: Vi1 Tnl/CL 25924/2 L2TP: Session state change from established to idle *Jun 6 04:03:25.358: Vi1 Tnl/CL 25924/2 L2TP: Releasing idb for LAC/LNS tunnel 25924/1 session 2 state idle *Jun 6 04:03:25.358: Vi1 VPDN: Reset *Jun 6 04:03:25.358: Tnl 25924 L2TP: **Tunnel state change from established to no-sessions-left** *Jun 6 04:03:25.358: Tnl 25924 L2TP: **No more sessions in tunnel, shutdown (likely) in 10 seconds** *!--- Because there are no more calls in the tunnel, it will be shut down.* *Jun 6 04:03:25.362: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down *Jun 6 04:03:25.362: Vi1 LCP: State is Closed *Jun 6 04:03:25.362: Vi1 IPCP: State is Closed *Jun 6 04:03:25.362: Vi1 PPP: Phase is DOWN [0 sess, 0 load] *Jun 6 04:03:25.362: Vi1 VPDN: Cleanup *Jun 6 04:03:25.362: Vi1 VPDN:

```
Reset *Jun 6 04:03:25.362: Vi1 VPDN: Unbind interface *Jun 6 04:03:25.362: Vi1 VPDN: Unbind
interface *Jun 6 04:03:25.362: Vi1 VPDN: Reset *Jun 6 04:03:25.362: Vi1 VPDN: Unbind interface
*Jun 6 04:03:25.362: Vi1 IPCP: Remove route to 1.100.0.2 *Jun 6 04:03:25.514: Tnl 25924 L2TP: I
StopCCN from JVEYNE-W2K1.cisco.com tnl 1 *Jun 6 04:03:25.514: Tnl 25924 L2TP: Shutdown tunnel !-
-- The tunnel is shut down. *Jun 6 04:03:25.514: Tnl 25924 L2TP: Tunnel state change from no-
sessions-left to idle *Jun 6 04:03:26.362: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to down
```

Дополнительные сведения

- Настройка Cisco IOS и клиентов Windows 2000 для L2TP с использованием Microsoft IAS
- Общие сведения о VPDN (виртуальная частная коммутируемая сеть)
- Конфигурация VPDN без AAA
- Настройка аутентификации по протоколу L2TP с использованием RADIUS
- Настройка сервера Access с первичным интерфейсом обмена (PRI) на прием асинхронных вызовов и вызовов по каналам ISDN
- Страницы поддержки технологии коммутации
- Техническая поддержка - Cisco Systems