

配置 Cisco IOS 与 Windows 2000 客户端，使用 Microsoft IAS 实现 L2TP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[为 Microsoft IAS 配置 Windows 2000 Advanced Server](#)

[配置 RADIUS 客户端](#)

[配置 IAS 上的用户](#)

[将远程访问策略应用于 Windows 用户](#)

[为 L2TP 配置 Windows 2000 客户端](#)

[为 Windows 2000 客户端禁用 IPSec](#)

[为 L2TP 配置 Cisco IOS](#)

[启用加密](#)

[debug 和 show 命令](#)

[分割隧道](#)

[故障排除](#)

[问题 1：未禁用 IPSec](#)

[问题 2：错误 789](#)

[问题 3：隧道身份验证出现问题](#)

[相关信息](#)

简介

本文档介绍了如何使用 Microsoft Internet 身份验证服务器 (IAS) 为第二层隧道协议 (L2TP) 配置 Cisco IOS® 软件和 Windows 2000 客户端。

有关如何使用预共享密钥以及用于用户身份验证的 Microsoft Windows 2003 IAS RADIUS 服务器配置从远程 Microsoft Windows 2000/2003 和 XP 客户端到 PIX 安全设备企业办公室的 L2TP over IP Security (IPSec) 的详细信息，请参阅[使用预共享密钥在 Windows 2000/XP PC 和 PIX/ASA 7.2 之间进行的 L2TP Over IPsec 配置示例](#)。

有关如何使用加密方法配置从远程 Microsoft Windows 2000 和 XP 客户端到企业站点的 L2TP over IPSec 的详细信息，请参阅[使用预共享密钥配置从 Windows 2000 或 XP 客户端到 Cisco VPN 3000 系列集中器的 L2TP over IPSec](#)。

[先决条件](#)

[要求](#)

本文档没有任何特定的前提条件。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- 在具有 Active Directory 的 Microsoft 2000 Advanced Server 上安装的 Microsoft IAS 可选组件
- Cisco 3600 路由器
- Cisco IOS 软件版本 c3640-io3s56i-mz.121-5.T

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[配置](#)

本部分提供有关如何配置本文档所述功能的信息。

注意：有关本文档所用命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

[网络图](#)

本文档使用以下网络设置：

本文档将以下 IP 池用于拨号客户端：

- 网关路由器：192.168.1.2 | 192.168.1.254
- LNS：172.16.10.1 | 172.16.10.1

[为 Microsoft IAS 配置 Windows 2000 Advanced Server](#)

确保安装了 Microsoft IAS。要安装 Microsoft IAS，请以管理员身份登录并完成以下步骤：

1. 在**网络服务**下，确保清除所有复选框。
2. 选中 **Internet 身份验证服务器 (IAS)** 复选框，然后单击“确定”。
3. 在“Windows 组件向导”中，单击**下一步**。如果出现提示，请插入 Windows 2000 CD。
4. 复制完所需文件后，单击**完成**，然后关闭所有窗口。您不需要重新启动。

[配置 RADIUS 客户端](#)

完成这些步骤：

1. 从**管理工具**中，打开“Internet 身份验证服务器控制台”，然后单击“客户端”。
2. 在**友好名称**框中，输入网络访问服务器 (NAS) 的 IP 地址。
3. 单击**使用此 IP**。
4. 在**客户端供应商**下拉列表中，确保选中了“RADIUS 标准”。
5. 在**共享密钥**和“确认共享密钥”框中，输入密码，然后单击“完成”。
6. 在控制台树中，右键单击 **Internet 身份验证服务**，然后单击“启动”。
7. 关闭控制台。

[配置 IAS 上的用户](#)

与 CiscoSecure 不同，Windows 2000 远程身份验证拨入用户服务器 (RADIUS) 用户数据库紧密绑定到 Windows 用户数据库。

- 如果在 Windows 2000 Server 上安装了 Active Directory，请从 **Active Directory 用户和计算机** 中创建新的拨号用户。
- 如果未安装 Active Directory，您可以使用“管理工具”中的**本地用户和组**来创建新用户。

[在活动目录中配置用户](#)

完成以下步骤，以便使用 Active Directory 配置用户：

1. 在 **Active Directory 用户和计算机**控制台中，展开您的域。
2. 右键单击**用户滚动**以选择新用户。
3. 创建一个名为 tac 的新用户。
4. 在**密码和确认密码**对话框中输入您的密码。
5. 清除**用户下次登录时须更改密码**选项，然后单击“下一步”。
6. 打开用户 tac 的**属性**框。切换至**拨入**选项卡。
7. 在**远程访问权限 (拨入或 VPN)**下，单击“允许访问”，然后单击“确定”。

[在没有安装活动目录的情况下配置用户](#)

完成以下步骤，以便在未安装 Active Directory 的情况下配置用户：

1. 从**管理工具**中，单击“计算机管理”。
2. 展开**计算机管理控制台**，然后单击“本地用户和组”。
3. 右键单击**用户滚动**以选择新用户。
4. 在**密码和确认密码**对话框中输入密码。
5. 清除**用户下次登录时须更改密码**选项，然后单击“下一步”。
6. 打开新用户 tac 的**属性**框。切换至**拨入**选项卡。
7. 在**远程访问权限 (拨入或 VPN)**下，单击“允许访问”，然后单击“确定”。

[将远程访问策略应用于 Windows 用户](#)

完成以下步骤，以便应用远程访问策略：

1. 从**管理工具**中，打开“Internet 身份验证服务器控制台”，然后单击“远程访问策略”。
2. 单击“指定匹配条件”上的**添加**按钮，并添加服务类型。选择**成帧**作为可用类型。将此类型添加到所选类型，然后按**确定**。

3. 单击“指定匹配条件”上的**添加**按钮，然后添加“帧协议”。选择 **PPP** 作为可用类型。将此类型添加到所选类型，然后按**确定**。
4. 单击“指定匹配条件”上的**添加**按钮，然后添加“Windows 组”，以添加用户所属的 Windows 组。选择此组，然后将其添加到所选类型。按**确定**。
5. 对于在启用拨入权限的情况下允许访问属性，选择“授予远程访问权限”。
6. 关闭控制台。

为 L2TP 配置 Windows 2000 客户端

完成以下步骤，以便为 L2TP 配置 Windows 2000 客户端：

1. 从开始菜单中，选择“设置”，然后遵循以下路径之一：**控制面板 > 网络和拨号连接** 或者 **网络和拨号连接 > 新建连接**
2. 使用向导创建名为 **L2TP** 的连接。此连接通过 Internet 连接到专用网络。您还需要指定 L2TP 隧道网关的 IP 地址或名称。
3. 新连接显示在“控制面板”下的**网络和拨号连接**窗口中。从该窗口中，单击鼠标右键编辑属性。
4. 在**联网**选项卡下，确保“我呼叫的服务器类型”设置为“L2TP”。
5. 如果计划通过本地协议或 DHCP 从网关中向此客户端分配一个动态内部地址，请选择 **TCP/IP 协议**。确保将客户端配置为自动获取 IP 地址。您还可以自动发出 DNS 信息。**高级**按钮使您可以定义静态 WINS 和 DNS 信息。**选项**选项卡使您可以关闭 IPsec，或者为连接分配一个不同的策略。在**安全**选项卡下，您可以定义用户身份验证参数，例如 PAP、CHAP 或 MS-CHAP，或者 Windows 域登录。
6. 配置连接后，您可以双击此连接以启动登录屏幕，然后单击**连接**。

为 Windows 2000 客户端禁用 IPsec

1. 编辑刚刚创建的拨号连接 L2TP 的属性。右键单击新连接 **L2TP** 以获取“L2TP 属性”窗口。
2. 在**联网**选项卡下，单击“Internet 协议 (TCP/IP) 属性”。双击**高级**选项卡。转至**选项**选项卡，单击“IP 安全属性”，如果选择了“不使用 IPSEC”，请双击此选项。

注意： Microsoft Windows 2000 客户端有一个默认的远程访问和策略代理服务，默认情况下，这些服务可以为 L2TP 数据流创建一个策略。此默认策略不允许没有 IPsec 和加密的 L2TP 数据流。您可以通过编辑 Microsoft 客户端注册表编辑器禁用 Microsoft 默认行为。本部分介绍了编辑 Windows 注册表并对 L2TP 数据流禁用默认 IPsec 策略的过程。有关如何编辑 Windows 注册表，请参阅相关的 Windows 文档。

使用注册表编辑器 (Regedt32.exe) 添加新的注册表条目，以禁用 IPsec。有关详细信息，请参阅与 Regedt32.exe 相关的 Microsoft 文档或 Microsoft 帮助主题。

您必须将 ProhibitIpSec 注册表值添加到 L2TP 或 IPsec 连接的每台基于 Windows 2000 的终点计算机，以防创建针对 L2TP 和 IPsec 数据流的自动过滤器。如果 ProhibitIpSec 注册表值设置为“1”，基于 Windows 2000 的计算机将不会创建使用 CA 身份验证的自动过滤器，而是检查本地或 Active Directory IPsec 策略。要将 ProhibitIpSec 注册表值添加到基于 Windows 2000 的计算机，请使用 Regedt32.exe 在注册表中找到以下键：

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

将以下注册表值添加到此项：

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

注意： 您必须重新启动基于 Windows 2000 的计算机才能使更改生效。有关详细信息，请参阅以下 Microsoft 文章：

- Q258261 - 禁用用于 L2TP 的 IPSEC 策略
- Q240262- 使用预先共享密钥，如何配置L2TP/IPsec连接

为 L2TP 配置 Cisco IOS

以下配置简要列出了没有 IPsec 的 L2TP 所必需的命令。在此基本配置起作用后，您还可以配置 IPsec。

安格拉

```
Building configuration...
Current configuration : 1595 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname angela
!
logging rate-limit console 10 except errors
!--- Enable AAA services here. aaa new-model aaa
authentication login default group radius local aaa
authentication login console none aaa authentication ppp
default group radius local aaa authorization network
default group radius local enable password ww ! memory-
size iomem 30 ip subnet-zero ! ! no ip finger no ip
domain-lookup ip host rund 172.17.247.195 ! ip audit
notify log ip audit po max-events 100 ip address-pool
local ! ! !--- Enable VPN/VPDN services and define
groups and !--- specific variables required for the
group. vpdn enable no vpdn logging ! vpdn-group
L2TP_Windows 2000Client !--- Default L2TP VPDN group. !-
-- Allow the Router to accept incoming requests. accept-
dialin protocol L2TP virtual-template 1 no L2TP tunnel
authentication !--- Users are authenticated at the NAS
or LNS !--- before the tunnel is established. This is
not !--- required for client-initiated tunnels. ! ! call
rsvp-sync ! ! ! ! ! ! controller E1 2/0 ! ! interface
Loopback0 ip address 172.16.10.100 255.255.255.0 !
interface Ethernet0/0 ip address 10.200.20.2
255.255.255.0 half-duplex ! interface Virtual-Template1
ip unnumbered Loopback0 peer default ip address pool
default ppp authentication ms-chap ! ip local pool
default 172.16.10.1 172.16.10.10 ip classless ip route
0.0.0.0 0.0.0.0 10.200.20.1 ip route 192.168.1.0
255.255.255.0 10.200.20.250 no ip http server ! radius-
server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3 radius-server key cisco !
dial-peer cor custom ! ! ! ! ! line con 0 exec-timeout 0
0 login authentication console transport input none line
33 50 modem InOut line aux 0 line vty 0 4 exec-timeout 0
0 password ww ! end angela# *Mar 12 23:10:54.176: L2TP:
I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.176: Tnl 8663 L2TP: New tunnel created for
remote RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:10:54.176: Tnl 8663 L2TP: O SCCRQ to
```

```
RSHANMUG-W2K1.cisco.com tnlid 5 *Mar 12 23:10:54.180:
Tnl 8663 L2TP: Tunnel state change from idle to wait-
ctl-reply *Mar 12 23:10:54.352: Tnl 8663 L2TP: I SCCCN
from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12 23:10:54.352:
Tnl 8663 L2TP: Tunnel state change from wait-ctl-reply
to established *Mar 12 23:10:54.352: Tnl 8663 L2TP: SM
State established *Mar 12 23:10:54.356: Tnl 8663 L2TP: I
ICRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.356: Tnl/C1 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/C1 8663/44 L2TP: Session state
change from idle to wait-connect *Mar 12 23:10:54.356:
Tnl/C1 8663/44 L2TP: New session created *Mar 12
23:10:54.356: Tnl/C1 8663/44 L2TP: O ICRP to RSHANMUG-
W2K1.cisco.com 5/1 *Mar 12 23:10:54.544: Tnl/C1 8663/44
L2TP: I ICCN from RSHANMUG-W2K1.cisco.com tnl 5, cl 1
*Mar 12 23:10:54.544: Tnl/C1 8663/44 L2TP: Session state
change from wait-connect to established *Mar 12
23:10:54.544: Vi1 VPDN: Virtual interface created for
*Mar 12 23:10:54.544: Vi1 PPP: Phase is DOWN, Setup [0
sess, 0 load] *Mar 12 23:10:54.544: Vi1 VPDN: Clone from
Vtemplate 1 filterPPP=0 blocking *Mar 12 23:10:54.620:
Tnl/C1 8663/44 L2TP: Session with no hwidb *Mar 12
23:10:54.624: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up *Mar 12 23:10:54.624: Vi1 PPP: Using
set call direction *Mar 12 23:10:54.624: Vi1 PPP:
Treating connection as a callin *Mar 12 23:10:54.624:
Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0
load] *Mar 12 23:10:54.624: Vi1 LCP: State is Listen
*Mar 12 23:10:54.624: Vi1 VPDN: Bind interface
direction=2 *Mar 12 23:10:56.556: Vi1 LCP: I CONFREQ
[Listen] id 1 len 44 *Mar 12 23:10:56.556: Vi1 LCP:
MagicNumber 0x595E7636 (0x0506595E7636) *Mar 12
23:10:56.556: Vi1 LCP: PFC (0x0702) *Mar 12
23:10:56.556: Vi1 LCP: ACFC (0x0802) *Mar 12
23:10:56.556: Vi1 LCP: Callback 6 (0x0D0306) *Mar 12
23:10:56.556: Vi1 LCP: MRRU 1614 (0x1104064E) *Mar 12
23:10:56.556: Vi1 LCP: EndpointDisc 1 Local *Mar 12
23:10:56.556: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.556: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.556: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds
trivially *Mar 12 23:10:56.556: Vi1 LCP: O CONFREQ
[Listen] id 1 len 15 *Mar 12 23:10:56.556: Vi1 LCP:
AuthProto MS-CHAP (0x0305C22380) *Mar 12 23:10:56.556:
Vi1 LCP: MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.560: Vi1 LCP: O CONFREJ [Listen] id 1 len 34
*Mar 12 23:10:56.560: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:10:56.560: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:10:56.560: Vi1 LCP: EndpointDisc 1 Local *Mar
12 23:10:56.560: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.560: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.700: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:10:56.700: Vi1 LCP: AuthProto MS-CHAP
(0x0305C22380) *Mar 12 23:10:56.704: Vi1 LCP:
MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.704: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:10:56.704: Vi1 LCP: MagicNumber 0x595E7636
(0x0506595E7636) *Mar 12 23:10:56.704: Vi1 LCP: PFC
(0x0702) *Mar 12 23:10:56.704: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:10:56.704: Vi1 LCP: O CONFACK [ACKrcvd] id 2
len 14 *Mar 12 23:10:56.708: Vi1 LCP: MagicNumber
0x595E7636 (0x0506595E7636) *Mar 12 23:10:56.708: Vi1
LCP: PFC (0x0702) *Mar 12 23:10:56.708: Vi1 LCP: ACFC
```

```
(0x0802) *Mar 12 23:10:56.708: Vi1 LCP: State is Open
*Mar 12 23:10:56.708: Vi1 PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load] *Mar 12 23:10:56.708: Vi1
MS-CHAP: O CHALLENGE id 28 len 21 from angela *Mar 12
23:10:56.852: Vi1 LCP: I IDENTIFY [Open] id 3 len 18
magic 0x595E7636 MSRASV5.00 *Mar 12 23:10:56.872: Vi1
LCP: I IDENTIFY [Open] id 4 len 27 magic 0x595E7636
MSRAS-1- RSHANMUG-W2K1 *Mar 12 23:10:56.880: Vi1 MS-
CHAP: I RESPONSE id 28 len 57 from tac *Mar 12
23:10:56.880: AAA: parse name=Virtual-Access1 idb
type=21 tty=-1 *Mar 12 23:10:56.880: AAA: name=Virtual-
Access1 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=1 channel=0 *Mar 12 23:10:56.884: AAA/MEMORY:
create_user (0x6273D024) user='tac' ruser=''
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP
service=PPP priv=1 *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): port='Virtual-Access1'
list='' action=LOGIN service=PPP *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): using default list *Mar
12 23:10:56.884: AAA/AUTHEN/START (3634835145):
Method=radius (radius) *Mar 12 23:10:56.884: RADIUS:
ustruct sharecount=0 *Mar 12 23:10:56.884: RADIUS:
Initial Transmit Virtual-Access1 id 173
10.200.20.245:1645, Access-Request, len 129 *Mar 12
23:10:56.884: Attribute 4 6 0AC81402 *Mar 12
23:10:56.884: Attribute 5 6 00000001 *Mar 12
23:10:56.884: Attribute 61 6 00000001 *Mar 12
23:10:56.884: Attribute 1 5 7461631A *Mar 12
23:10:56.884: Attribute 26 16 000001370B0A0053 *Mar 12
23:10:56.884: Attribute 26 58 0000013701341C01 *Mar 12
23:10:56.884: Attribute 6 6 00000002 *Mar 12
23:10:56.884: Attribute 7 6 00000001 *Mar 12
23:10:56.900: RADIUS: Received from id 173
10.200.20.245:1645, Access-Accept, len 116 *Mar 12
23:10:56.900: Attribute 7 6 00000001 *Mar 12
23:10:56.900: Attribute 6 6 00000002 *Mar 12
23:10:56.900: Attribute 25 32 502605A6 *Mar 12
23:10:56.900: Attribute 26 40 000001370C22F6D5 *Mar 12
23:10:56.900: Attribute 26 12 000001370A061C4E *Mar 12
23:10:56.900: AAA/AUTHEN (3634835145): status = PASS
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
Port='Virtual-Access1' list='' service=NET *Mar 12
23:10:56.900: AAA/AUTHOR/LCP: Vi1 (1995716469)
user='tac' *Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP
(1995716469): send AV service=ppp *Mar 12 23:10:56.900:
Vi1 AAA/AUTHOR/LCP (1995716469): send AV protocol=lcp
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
found list default *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/LCP (1995716469): Method=radius (radius) *Mar
12 23:10:56.904: RADIUS: unrecognized Microsoft VSA type
10 *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR (1995716469):
Post authorization status = PASS_REPL *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/LCP: Processing AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP:
Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:56.904: Vi1 MS-CHAP: O SUCCESS id 28
len 4 *Mar 12 23:10:56.904: Vi1 PPP: Phase is UP [0
sess, 0 load] *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM:
(0): Can we start IPCP? *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/FSM (2094713042): Port='Virtual-Access1'
list='' service=NET *Mar 12 23:10:56.904:
AAA/AUTHOR/FSM: Vi1 (2094713042) user='tac' *Mar 12
```

```
23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): send AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM
(2094713042): send AV protocol=ip *Mar 12 23:10:56.904:
Vi1 AAA/AUTHOR/FSM (2094713042): found list default *Mar
12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042):
Method=radius (radius) *Mar 12 23:10:56.908: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:56.908:
Vi1 AAA/AUTHOR (2094713042): Post authorization status =
PASS_REPL *Mar 12 23:10:56.908: Vi1 AAA/AUTHOR/FSM: We
can start IPCP *Mar 12 23:10:56.908: Vi1 IPCP: O CONFREQ
[Closed] id 1 len 10 *Mar 12 23:10:56.908: Vi1 IPCP:
Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.040: Vi1 CCP: I CONFREQ [Not negotiated] id 5
len 10 *Mar 12 23:10:57.040: Vi1 CCP: MS-PPC supported
bits 0x01000001 (0x120601000001) *Mar 12 23:10:57.040:
Vi1 LCP: O PROTREJ [Open] id 2 len 16 protocol CCP
(0x80FD0105000A120601000001) *Mar 12 23:10:57.052: Vi1
IPCP: I CONFREQ [REQsent] id 6 len 34 *Mar 12
23:10:57.052: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:10:57.052: Vi1 IPCP: PrimaryDNS 0.0.0.0
(0x810600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
PrimaryWINS 0.0.0.0 (0x820600000000) *Mar 12
23:10:57.052: Vi1 IPCP: SecondaryDNS 0.0.0.0
(0x830600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
SecondaryWINS 0.0.0.0 (0x840600000000) *Mar 12
23:10:57.052: Vi1 AAA/AUTHOR/IPCP: Start. Her address
0.0.0.0, we want 0.0.0.0 *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 12
23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
0.0.0.0 *Mar 12 23:10:57.056: Vi1 IPCP: Pool returned
172.16.10.1 *Mar 12 23:10:57.056: Vi1 IPCP: O CONFREQ
[REQsent] id 6 len 28 *Mar 12 23:10:57.056: Vi1 IPCP:
PrimaryDNS 0.0.0.0 (0x810600000000) *Mar 12
23:10:57.056: Vi1 IPCP: PrimaryWINS 0.0.0.0
(0x820600000000) *Mar 12 23:10:57.056: Vi1 IPCP:
SecondaryDNS 0.0.0.0 (0x830600000000) *Mar 12
23:10:57.056: Vi1 IPCP: SecondaryWINS 0.0.0.0
(0x840600000000) *Mar 12 23:10:57.060: Vi1 IPCP: I
CONFACK [REQsent] id 1 len 10 *Mar 12 23:10:57.060: Vi1
IPCP: Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.192: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:10:57.192: Vi1 IPCP: Address 0.0.0.0
(0x030600000000) *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Processing AV service=ppp *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 IPCP: O CONFNAK
[ACKrcvd] id 7 len 10 *Mar 12 23:10:57.192: Vi1 IPCP:
Address 172.16.10.1 (0x0306AC100A01) *Mar 12
23:10:57.324: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:10:57.324: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1, we want
172.16.10.1 *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): Port='Virtual-Access1' list='' service=NET
```



```

*Mar 12 23:10:57.324: AAA/AUTHOR/IPCP: Vi1 (413757991)
user='tac' *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): send AV service=ppp *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR/IPCP (413757991): send AV protocol=ip
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
send AV addr*172.16.10.1 *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP (413757991): found list default *Mar 12
23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
Method=radius (radius) *Mar 12 23:10:57.324: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR (413757991): Post authorization status =
PASS_REPL *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP:
Reject 172.16.10.1, using 172.16.10.1 *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV addr*172.16.10.1 *Mar 12 23:10:57.328: Vi1
AAA/AUTHOR/IPCP: Authorization succeeded *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Done. Her address
172.16.10.1, we want 172.16.10.1 *Mar 12 23:10:57.328:
Vi1 IPCP: O CONFACK [ACKrcvd] id 8 len 10 *Mar 12
23:10:57.328: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.328: Vi1 IPCP: State
is Open *Mar 12 23:10:57.332: Vi1 IPCP: Install route to
172.16.10.1 *Mar 12 23:10:57.904: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Virtual-Access1, changed
state to up *Mar 12 23:11:06.324: Vi1 LCP: I ECHOREP
[Open] id 1 len 12 magic 0x595E7636 *Mar 12
23:11:06.324: Vi1 LCP: Received id 1, sent id 1, line up

```

```

angela#show vpdn L2TP Tunnel and Session Information Total tunnels 1 sessions 1 LocID RemID
Remote Name State Remote Address Port Sessions 8663 5 RSHANMUG-W2K1.c est 192.168.1.56 1701 1
LocID RemID TunID Intf Username State Last Chg Fastswitch 44 1 8663 Vi1 tac est 00:00:18 enabled
%No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnels *Mar 12 23:11:16.332:
Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic 0x595E7636 *Mar 12 23:11:16.332: Vi1 LCP: Received
id 2, sent id 2, line upsh caller ip Line User IP Address Local Number Remote Number <-> Vi1 tac
172.16.10.1 - - in angela#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA
external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external
type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic downloaded static route
Gateway of last resort is 10.200.20.1 to network 0.0.0.0 172.16.0.0/16 is variably subnetted, 2
subnets, 2 masks C 172.16.10.0/24 is directly connected, Loopback0 C 172.16.10.1/32 is directly
connected, Virtual-Access1 10.0.0.0/24 is subnetted, 1 subnets C 10.200.20.0 is directly
connected, Ethernet0/0 S 192.168.1.0/24 [1/0] via 10.200.20.250 S* 0.0.0.0/0 [1/0] via
10.200.20.1 *Mar 12 23:11:26.328: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x595E7636 *Mar 12
23:11:26.328: Vi1 LCP: Received id 3, sent id 3, line up172.16.10.1 angela#ping 172.16.10.1 Type
escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
!!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 156/160/168 ms

```

启用加密

在 interface virtual-template 1 下添加 **ppp encrypt mppe 40** 命令。确保同时在 Microsoft 客户端中选择了加密。

```

*Mar 12 23:27:36.608: L2TP: I SCCRP from RSHANMUG-W2K1.cisco.com tnl 13
*Mar 12 23:27:36.608: Tnl 31311 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:27:36.608: Tnl 31311 L2TP: O SCCRP to RSHANMUG-W2K1.cisco.com
tnlid 13
*Mar 12 23:27:36.612: Tnl 31311 L2TP: Tunnel state change from idle to
wait-ctl-reply

```

*Mar 12 23:27:36.772: Tnl 31311 L2TP: I SCCCN from RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.772: Tnl 31311 L2TP: Tunnel state change from
wait-ctl-reply to established
*Mar 12 23:27:36.776: Tnl 31311 L2TP: SM State established
*Mar 12 23:27:36.780: Tnl 31311 L2TP: I ICRQ from RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session FS enabled
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session state change from idle
to wait-connect
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: New session created
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: O ICRP to
RSHANMUG-W2K1.cisco.com 13/1
*Mar 12 23:27:36.924: Tnl/Cl 31311/52 L2TP: I ICCN from
RSHANMUG-W2K1.cisco.com tnl 13, cl 1
*Mar 12 23:27:36.928: Tnl/Cl 31311/52 L2TP: Session state change from
wait-connect to established
*Mar 12 23:27:36.928: Vi1 VPDN: Virtual interface created for
*Mar 12 23:27:36.928: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Mar 12 23:27:36.928: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Mar 12 23:27:36.972: Tnl/Cl 31311/52 L2TP: Session with no hwidb
*Mar 12 23:27:36.976: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Mar 12 23:27:36.976: Vi1 PPP: Using set call direction
*Mar 12 23:27:36.976: Vi1 PPP: Treating connection as a callin
*Mar 12 23:27:36.976: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess,
0 load]
*Mar 12 23:27:36.976: Vi1 LCP: State is Listen
*Mar 12 23:27:36.976: Vi1 VPDN: Bind interface direction=2
*Mar 12 23:27:38.976: Vi1 LCP: TIMEout: State Listen
*Mar 12 23:27:38.976: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar 12 23:27:38.976: Vi1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 12 23:27:38.976: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:38.976: Vi1 LCP: MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:38.984: Vi1 LCP: I CONFREQ [REQsent] id 1 len 44
*Mar 12 23:27:38.984: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:38.984: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:38.984: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:38.984: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP: EndpointDisc 1 Local
*Mar 12 23:27:38.984: Vi1 LCP: (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.984: Vi1 LCP: (0x10D0AC0000000A)
*Mar 12 23:27:38.984: Vi1 LCP: O CONFREQ [REQsent] id 1 len 34
*Mar 12 23:27:38.984: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP: EndpointDisc 1 Local
*Mar 12 23:27:38.988: Vi1 LCP: (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.988: Vi1 LCP: (0x10D0AC0000000A)
*Mar 12 23:27:39.096: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:27:39.096: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:39.096: Vi1 LCP: MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:39.128: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: O CONFACK [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: State is Open
*Mar 12 23:27:39.128: Vi1 PPP: Phase is AUTHENTICATING, by this end [0
sess, 0 load]
*Mar 12 23:27:39.128: Vi1 MS-CHAP: O CHALLENGE id 32 len 21 from angela

```
*Mar 12 23:27:39.260: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x4B4817ED MSRASV5.00
*Mar 12 23:27:39.288: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic
0x4B4817ED MSRAS-1- RSHANMUG-W2K1
*Mar 12 23:27:39.296: Vi1 MS-CHAP: I RESPONSE id 32 len 57 from tac
*Mar 12 23:27:39.296: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar 12 23:27:39.296: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar 12 23:27:39.296: AAA/MEMORY: create_user (0x6273D528) user='tac'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): using default list
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): Method=radius (radius)
*Mar 12 23:27:39.296: RADIUS: ustruct sharecount=0
*Mar 12 23:27:39.300: RADIUS: Initial Transmit Virtual-Access1 id 181
10.200.20.245:1645, Access-Request, len 129
*Mar 12 23:27:39.300:      Attribute 4 6 0AC81402
*Mar 12 23:27:39.300:      Attribute 5 6 00000001
*Mar 12 23:27:39.300:      Attribute 61 6 00000001
*Mar 12 23:27:39.300:      Attribute 1 5 7461631A
*Mar 12 23:27:39.300:      Attribute 26 16 000001370B0AFC72
*Mar 12 23:27:39.300:      Attribute 26 58 0000013701342001
*Mar 12 23:27:39.300:      Attribute 6 6 00000002
*Mar 12 23:27:39.300:      Attribute 7 6 00000001
*Mar 12 23:27:39.312: RADIUS: Received from id 181 10.200.20.245:1645,
Access-Accept, len 116
*Mar 12 23:27:39.312:      Attribute 7 6 00000001
*Mar 12 23:27:39.312:      Attribute 6 6 00000002
*Mar 12 23:27:39.312:      Attribute 25 32 502E05AE
*Mar 12 23:27:39.312:      Attribute 26 40 000001370C225042
*Mar 12 23:27:39.312:      Attribute 26 12 000001370A06204E
*Mar 12 23:27:39.312: AAA/AUTHEN (2410248116): status = PASS
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.316: AAA/AUTHOR/LCP: Vi1 (2365724222) user='tac'
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV protocol=lcp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): found list default
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): Method=radius
(radius)
*Mar 12 23:27:39.316: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR (2365724222): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.316: Vi1 MS-CHAP: O SUCCESS id 32 len 4
*Mar 12 23:27:39.316: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.320: AAA/AUTHOR/FSM: Vi1 (1499311111) user='tac'
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV service=ppp
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV protocol=ip
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): found list default
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): Method=radius
(radius)
*Mar 12 23:27:39.320: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR (1499311111): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: We can start IPCP
```

```
*Mar 12 23:27:39.320: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.320: Vi1 IPCP: Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (327346364):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.324: AAA/AUTHOR/FSM: Vi1 (327346364) user='tac'
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV service=ppp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV protocol=ccp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): found list default
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): Method=radius
(radius)
*Mar 12 23:27:39.324: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR (327346364): Post authorization status
= PASS_REPL
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM: We can start CCP
*Mar 12 23:27:39.324: Vi1 CCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.324: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.460: Vi1 CCP: I CONFREQ [REQsent] id 5 len 10
*Mar 12 23:27:39.460: Vi1 CCP: MS-PPC supported bits 0x01000001
(0x120601000001)
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.464: Vi1 CCP: O CONFNAK [REQsent] id 5 len 10
*Mar 12 23:27:39.464: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.472: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar 12 23:27:39.472: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 IPCP: Pool returned 172.16.10.1
*Mar 12 23:27:39.476: Vi1 IPCP: O CONFREQ [REQsent] id 6 len 28
*Mar 12 23:27:39.476: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.480: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.484: Vi1 IPCP: Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.488: Vi1 CCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.488: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Succeeded
```

```

*Mar 12 23:27:39.596: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: State is Open
*Mar 12 23:27:39.600: Vi1 MPPE: Generate keys using RADIUS data
*Mar 12 23:27:39.600: Vi1 MPPE: Initialize keys
*Mar 12 23:27:39.600: Vi1 MPPE: [40 bit encryption] [stateless mode]
*Mar 12 23:27:39.620: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.620: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.624: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.624: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.756: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.756: AAA/AUTHOR/IPCP: Vi1 (2840659706) user='tac'
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV service=ppp
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV protocol=ip
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV
addr*172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): found list
default
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): Method=radius
(radius)
*Mar 12 23:27:39.756: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR (2840659706): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Done. Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.760: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.760: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.760: Vi1 IPCP: State is Open
*Mar 12 23:27:39.764: Vi1 IPCP: Install route to 172.16.10.1
*Mar 12 23:27:40.316: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar 12 23:27:46.628: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x4B4817ED
*Mar 12 23:27:46.628: Vi1 LCP: Received id 1, sent id 1, line up
*Mar 12 23:27:56.636: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x4B4817ED
*Mar 12 23:27:56.636: Vi1 LCP: Received id 2, sent id 2, line upcaller ip
Line UserIP AddressLocal NumberRemote Number<->
Vi1 tac172.16.10.1--in

```

```

angela#show ppp mppe virtual-Access 1 Interface Virtual-Access1 (current connection) Software
encryption, 40 bit encryption, Stateless mode packets encrypted = 0 packets decrypted = 16 sent
CCP resets = 0 receive CCP resets = 0 next tx coherency = 0 next rx coherency = 16 tx key

```

```
changes = 0 rx key changes = 16 rx pkt dropped = 0 rx out of order pkt= 0 rx missed packets = 0
*Mar 12 23:28:06.604: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x4B4817ED *Mar 12
23:28:06.604: Vi1 LCP: Received id 3, sent id 3, line up angela#ping 172.16.10.1 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/196/204 ms angela#show ppp mppe
virtual-Access 1 Interface Virtual-Access1 (current connection) Software encryption, 40 bit
encryption, Stateless mode packets encrypted = 5 packets decrypted = 22 sent CCP resets = 0
receive CCP resets = 0 next tx coherency = 5 next rx coherency = 22 tx key changes = 5 rx key
changes = 22 rx pkt dropped = 0 rx out of order pkt= 0 rx missed packets = 0 angela#ping
172.16.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1,
timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =
184/200/232 ms angela#ping 172.16.10.1sh ppp mppe virtual-Access 1 Interface Virtual-Access1
(current connection) Software encryption, 40 bit encryption, Stateless mode packets encrypted =
10 packets decrypted = 28 sent CCP resets = 0 receive CCP resets = 0 next tx coherency = 10 next
rx coherency = 28 tx key changes = 10 rx key changes = 28 rx pkt dropped = 0 rx out of order
pkt= 0 rx missed packets = 0 angela#
```

debug 和 show 命令

使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

[命令输出解释程序 \(仅限注册用户\)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 **show** 命令输出的分析。

如果配置不起作用，最简单的 **debug** 将包括以下命令：

- **debug aaa authentication** —显示关于AAA/TACACS+验证的信息。
- **debug aaa authorization** - 显示有关 AAA/TACACS+ 授权的信息。
- **debug ppp negotiation** — 显示在 PPP 启动期间传输的 PPP 数据包，在此启动期间将协商 PPP 选项。
- **debug ppp authentication** —显示认证协议消息，包括质询验证协议(CHAP)信息包交换和密码认证协议交换。
- **debug radius** - 显示与 RADIUS 关联的详细调试信息。

如果身份验证起作用，但 Microsoft 点对点加密 (MPPE) 加密出现问题，请使用以下命令之一：

- **debug ppp mppe packet** —显示所有流入流出的MPPE流量。
- **debug ppp mppe event** —显示关键MPPE出现。
- **debug ppp mppe detailed** —显示冗长MPPE信息。
- **debug vpdn l2x-packets** —显示关于第2层转发(L2F)协议报头和状态的消息。
- **debug vpdn events** —显示关于正常隧道建立的一部分或关闭的事件的消息。
- **debug vpdn errors** —显示防止一个通道设立造成一个已建隧道关闭的错误或错误。
- **debug vpdn packets** —显示被交换的每个协议信息包。此选项可能会导致出现大量的调试消息，因此通常只应在具有单个活动会话的调试机箱中使用。
- **show vpdn** —显示关于活动L2F协议通道和消息标识符的信息在虚拟专用拨号网络(VPDN)。

您还可以使用 **show vpdn ?**命令查看其他特定于 vpdn 的 **show** 命令。

分割隧道

假设网关路由器是 Internet 服务提供商 (ISP) 路由器。当 PC 上显示点对点隧道协议 (PPTP) 隧道时，所安装的 PPTP 路由将比前一个默认值的度量高，从而导致断开了 Internet 连接。要解决此问题，请修改 Microsoft 路由以删除默认值并重新安装默认路由（这需要知道为 PPTP 客户端分配的 IP 地址；对于当前示例，IP 地址为 172.16.10.1）：

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

问题 1：未禁用 IPsec

症状

PC 用户看到以下消息：

```
Error connecting to L2TP:
Error 781: The encryption attempt failed because
no valid certificate was found.
```

解决方案

转至“虚拟专用连接”窗口的**属性**部分，然后单击“安全”选项卡。禁用**需要数据加密**选项。

问题 2：错误 789

症状

由于安全层在与远程计算机进行初始协商期间遇到处理错误，导致 L2TP 连接尝试失败。

由于 L2TP 不提供加密，因此 Microsoft 远程访问和策略代理服务创建了一个用于 L2TP 数据流的策略。这适用于 Microsoft Windows 2000 Advanced Server、Microsoft Windows 2000 Server 和 Microsoft Windows 2000 Professional。

解决方案

使用注册表编辑器 (Regedt32.exe) 添加新的注册表条目，以禁用 IPsec。请参阅与 Regedt32.exe 相关的 Microsoft 文档或 Microsoft 帮助主题。

您必须将 ProhibitIpSec 注册表值添加到 L2TP 或 IPsec 连接的每台基于 Windows 2000 的终点计算机，以防创建针对 L2TP 和 IPsec 数据流的自动过滤器。如果 ProhibitIpSec 注册表值设置为“1”，基于 Windows 2000 的计算机将不会创建使用 CA 身份验证的自动过滤器，而是检查本地或 Active Directory IPsec 策略。要将 ProhibitIpSec 注册表值添加到基于 Windows 2000 的计算机，请使用 Regedt32.exe 在注册表中找到以下键：

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

将以下注册表值添加到此项：

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

注意：您必须重新启动基于 Windows 2000 的计算机才能使更改生效。

问题 3：隧道身份验证出现问题

在建立隧道之前，用户在 NAS 或 LNS 中进行身份验证。对于客户端发起的隧道（例如从 Microsoft 客户端发起的 L2TP 隧道），不需要进行此类身份验证。

PC 用户看到以下消息：

```
Connecting to 10.200.20.2..
Error 651: The modem(or other connecting device) has reported an error.
Router debugs:

*Mar 12 23:03:47.124: L2TP: I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:03:47.124: Tnl 30107 L2TP: O SCCRP to RSHANMUG-W2K1.cisco.com
tnlid 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:03:47.308: Tnl 30107 L2TP: I SCCCN from RSHANMUG-W2K1.cisco.com
tnl 1
*Mar 12 23:03:47.308: Tnl 30107 L2TP: Got a Challenge Response in SCCCN
from RSHANMUG-W2K1.cisco.com
*Mar 12 23:03:47.308: AAA: parse name= idb type=-1 tty=-1
*Mar 12 23:03:47.308: AAA/MEMORY: create_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): port='' list='default'
action=SENDAUTH service=PPP
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): found list default
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=radius (radius)
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): no authenstruct
hwidb
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): Failed sendauthen
for angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = FAIL
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=LOCAL
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): SENDAUTH no password for
angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): no methods left to try
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): failed to authenticate
*Mar 12 23:03:47.308: VPDN: authentication failed, couldn't find user
information for angela
*Mar 12 23:03:47.308: AAA/MEMORY: free_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: O StopCCN to
RSHANMUG-W2K1.cisco.com tnlid 1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: Tunnel state change from
wait-ctl-reply to shutting-down
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Shutdown tunnel
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Tunnel state change from
shutting-down to idle
*Mar 12 23:03:47.324: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 1
*Mar 12 23:03:47.448: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 2
```

[相关信息](#)

- [第二层隧道协议 \(L2TP\)](#)
- [使用数字证书在 Windows 2000 和 VPN 3000 集中器之间进行的 L2TP Over IPsec 配置示例](#)
- [使用证书在 PIX 防火墙与 Windows 2000 PC 之间配置 IPsec 上的 L2TP](#)
- [第二层隧道协议](#)

- [配置虚拟专用网络](#)
- [配置使用 RADIUS 认证的第二层隧道协议](#)
- [技术支持和文档 - Cisco Systems](#)