為Windows路由器PPTP身份驗證配置CiscoSecure ACS

目錄

簡介

點對點通道通訊協定(PPTP)支援新增到思科7100和7200平台上的Cisco IOS®軟體版本12.0.5.XE5中(請參閱使用Microsoft點對點加密(MPPE)的PPTP[Cisco IOS軟體版本12.0])。 Cisco IOS軟體版本12.1.5.T新增了對更多平台的支援(請參閱MSCHAP版本2)。

RFC 2637 描述了PPTP。在PPTP術語中,根據RFC,PPTP訪問集中器(PAC)是客戶端(即PC,即呼叫者),而PPTP網路伺服器(PNS)是伺服器(路由器,被叫者)。

本文假設已使用這些文檔建立了使用本地Microsoft-Challenge Handshake身份驗證協定(MS-CHAP)V1身份驗證(以及需要MS-CHAP V1的MPPE)的PPTP連線,並且這些連線已可以運行。MPPE加密支援需要RADIUS。TACACS+適用於驗證,但不適用於MPPE金鑰。MS-CHAP V2支援已新增到Cisco IOS軟體版本12.2(2)XB5中,並已整合到Cisco IOS軟體版本12.2(13)T中(請參閱MSCHAP版本2),但是MS-CHAP V2目前尚不支援MPPE。

此示例配置演示了如何設定與路由器(10.66.79.99)的PC連線,該路由器隨後會在允許使用者進入網路之前,向Windows伺服器的Cisco安全訪問控制系統(ACS)4.2(10.66.79.120)提供使用者身份驗證

。

注意：RADIUS伺服器通常不在路由器外部，除非在實驗環境中。

已將PPTP支援新增到Cisco Secure ACS 2.5，但由於Cisco錯誤ID [CSCds9266](僅限[註冊]客戶)，可能無法與路由器一起工作。ACS 2.6及更高版本沒有此問題。

Cisco Secure UNIX不支援MPPE。另外兩個支援MPPE的RADIUS應用程式包括Microsoft RADIUS和Funk RADIUS。

有關如何使用路由器配置PPTP和MPPE的詳細資訊，請參閱[使用PPTP和MPPE配置Cisco路由器和VPN客戶端]。

有關如何在VPN 3000集中器上配置用於RADIUS身份驗證的Cisco Secure ACS，請參閱[使用用於Windows RADIUS身份驗證的Cisco Secure ACS配置VPN 3000集中器和PPTP]，瞭解詳細資訊。

請參閱[PIX 6.x:使用Radius身份驗證的PPTP]配置示例，以便配置與PIX的PPTP連線。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

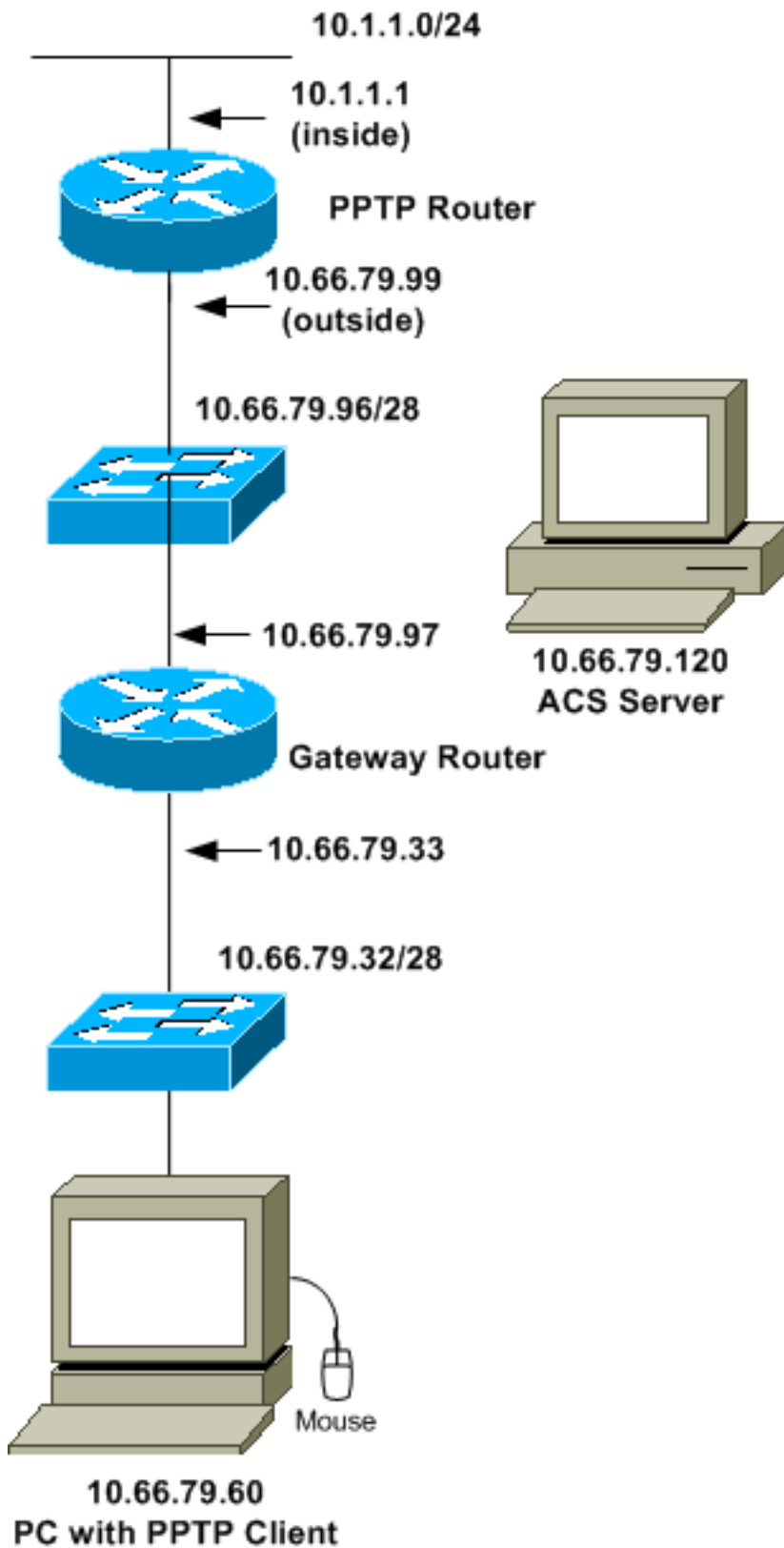- 適用於Windows的Cisco安全ACS 4.2
- 思科3600路由器
- Cisco IOS 軟體版本 12.4(3)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您處於使用中的網路中，請確保您在使用任何指令之前瞭解其潛在影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。]

網路圖表

本檔案會使用以下網路設定：

10.1.1.0/24

10.1.1.1
(inside)

PPTP Router

10.66.79.99
(outside)

10.66.79.96/28

10.66.79.97

10.66.79.120
ACS Server

Gateway Router

10.66.79.33

10.66.79.32/28

Mouse

10.66.79.60
PC with PPTP Client

路由器配置

使用此路由器配置。即使RADIUS伺服器無法連線（如果伺服器尚未設定Cisco Secure ACS，則可能連線），使用者也應能使用「username john password doe」連線。 此示例假設本地身份驗證（以及可選的加密）已可操作。

思科3600路由器

```
Current configuration : 1729 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname moss
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username john password 0 doe
aaa new-model
!


aaa authentication ppp default group radius local

aaa authentication login default local

!--- In order to set authentication, authorization, and
accounting (AAA) authentication !--- at login, use the
aaa authentication login command in global !---
configuration mode as shown above.


aaa authorization network default group radius if-
authenticated
aaa session-id common
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
!--- Default PPTP VPDN group. accept-dialin
protocol pptp
virtual-template 1
!
no ftp-server write-enable
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
half-duplex
!
interface Ethernet0/1
ip address 10.66.79.99 255.255.255.224
half-duplex
!
interface Virtual-Template1
ip unnumbered Ethernet0/1
peer default ip address pool testpool
ppp authentication ms-chap
!
ip local pool testpool 192.168.1.1 192.168.1.254
ip http server
no ip http secure-server
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.66.79.97
!
radius-server host 10.66.79.120 auth-port 1645 acct-port
1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
line aux 0
line vty 0 4
password cisco
!
end
```
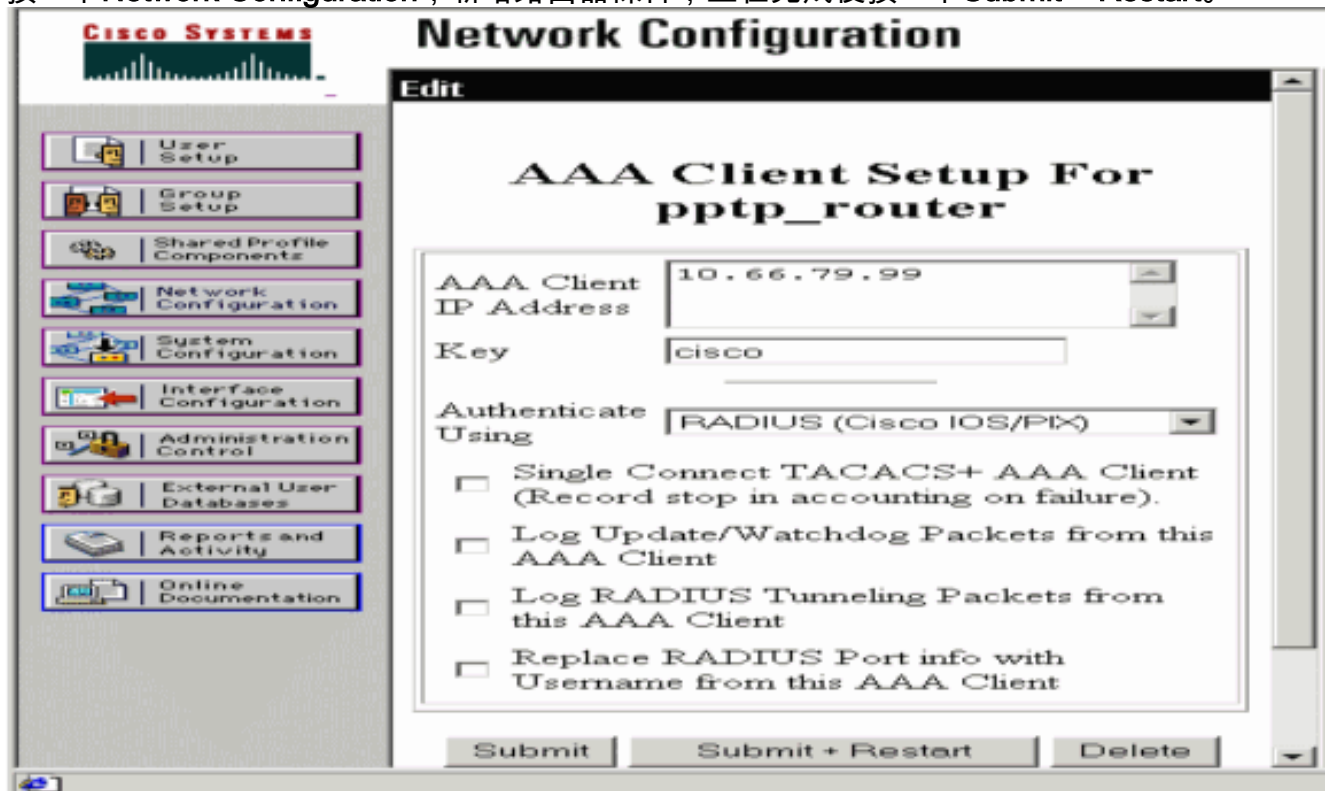
RADIUS伺服器回退功能

當主RADIUS伺服器不可用時，路由器將故障切換到下一個活動備份RADIUS伺服器。即使主伺服器可用，路由器也會一直使用輔助RADIUS伺服器。通常，主伺服器是高效能，是首選伺服器。

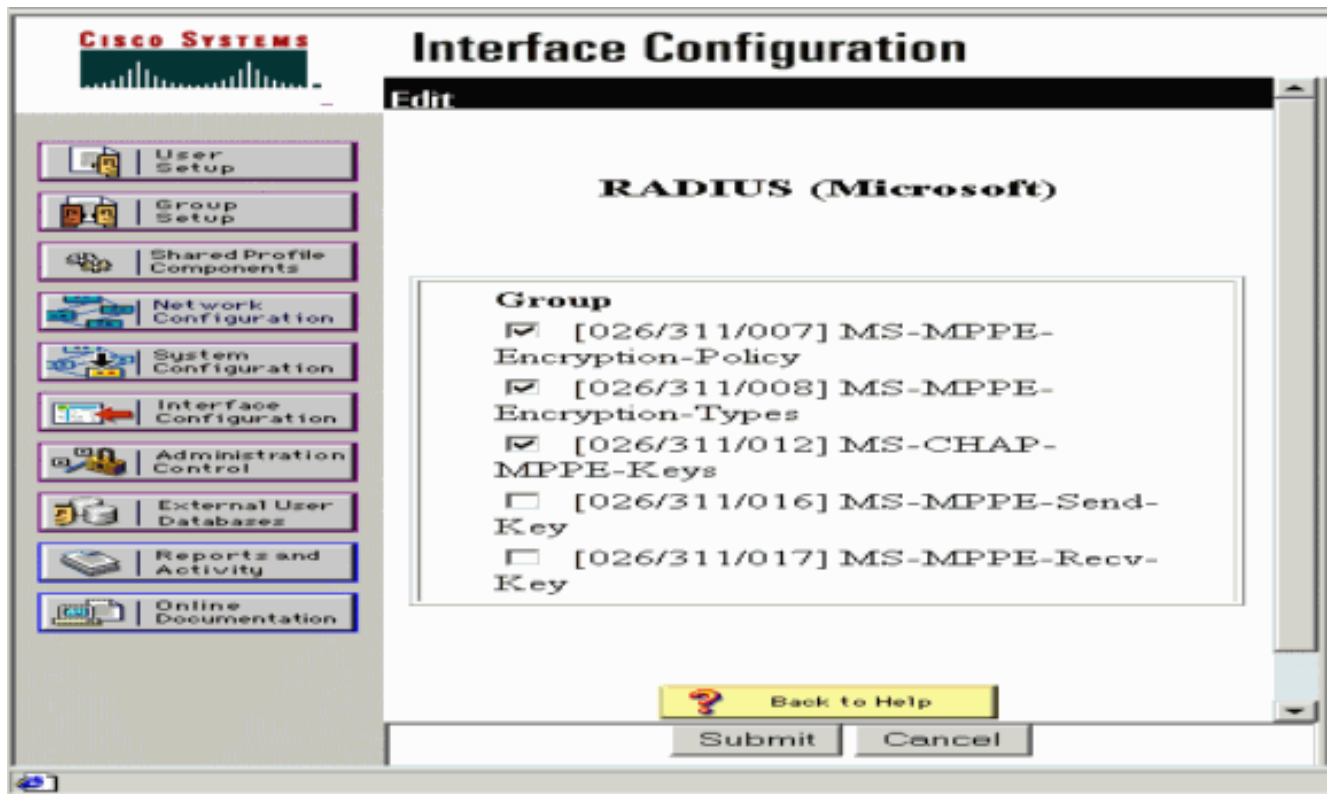要在登入時設定身份驗證、授權和記帳(AAA)身份驗證，請在全域性配置模式下使用aaa authentication login命令。

Cisco Secure ACS for Windows配置

使用以下過程配置Cisco Secure ACS:

1. 按一下**Network Configuration**，新增路由器條目，並在完成後按一下**Submit + Restart**。
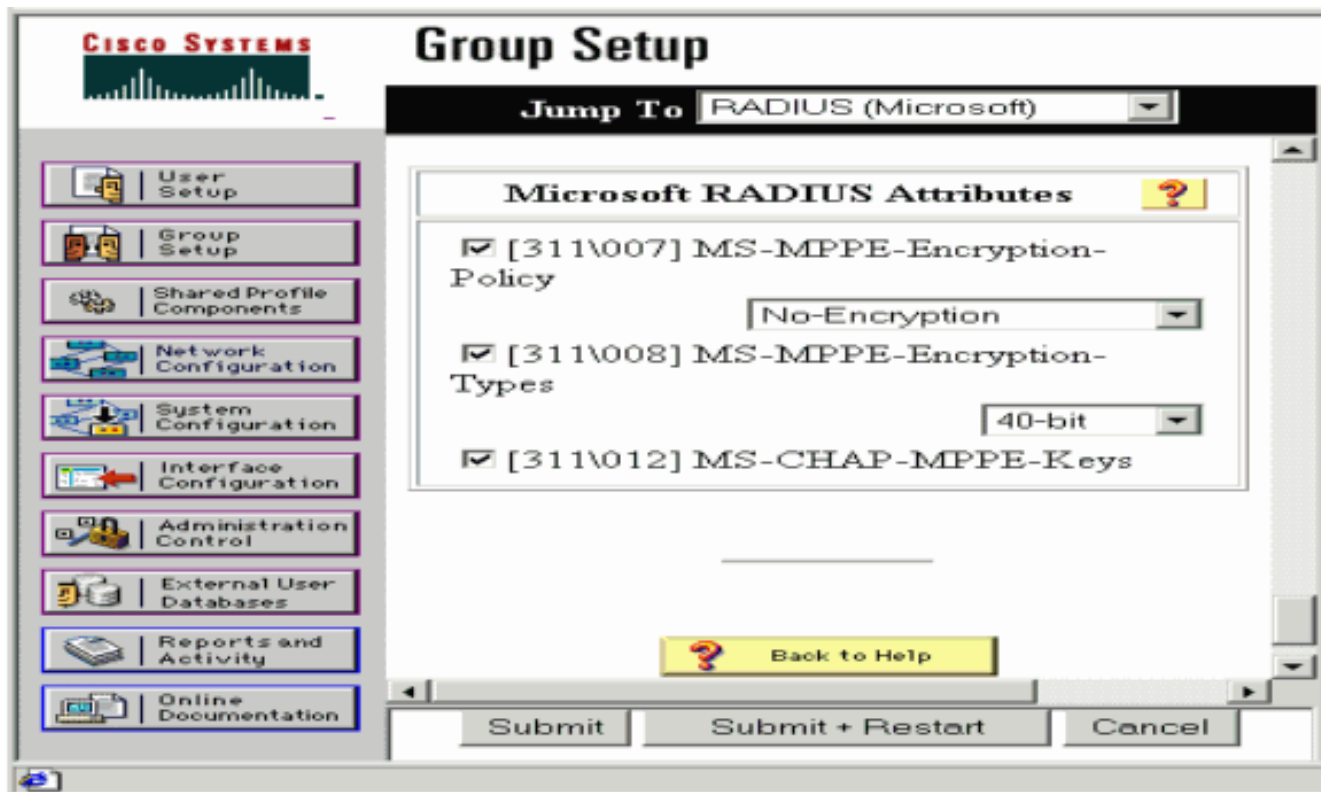

2. 選擇**Interface Configuration > RADIUS(Microsoft)**，然後檢查MPPE屬性並按一下**Submit**。
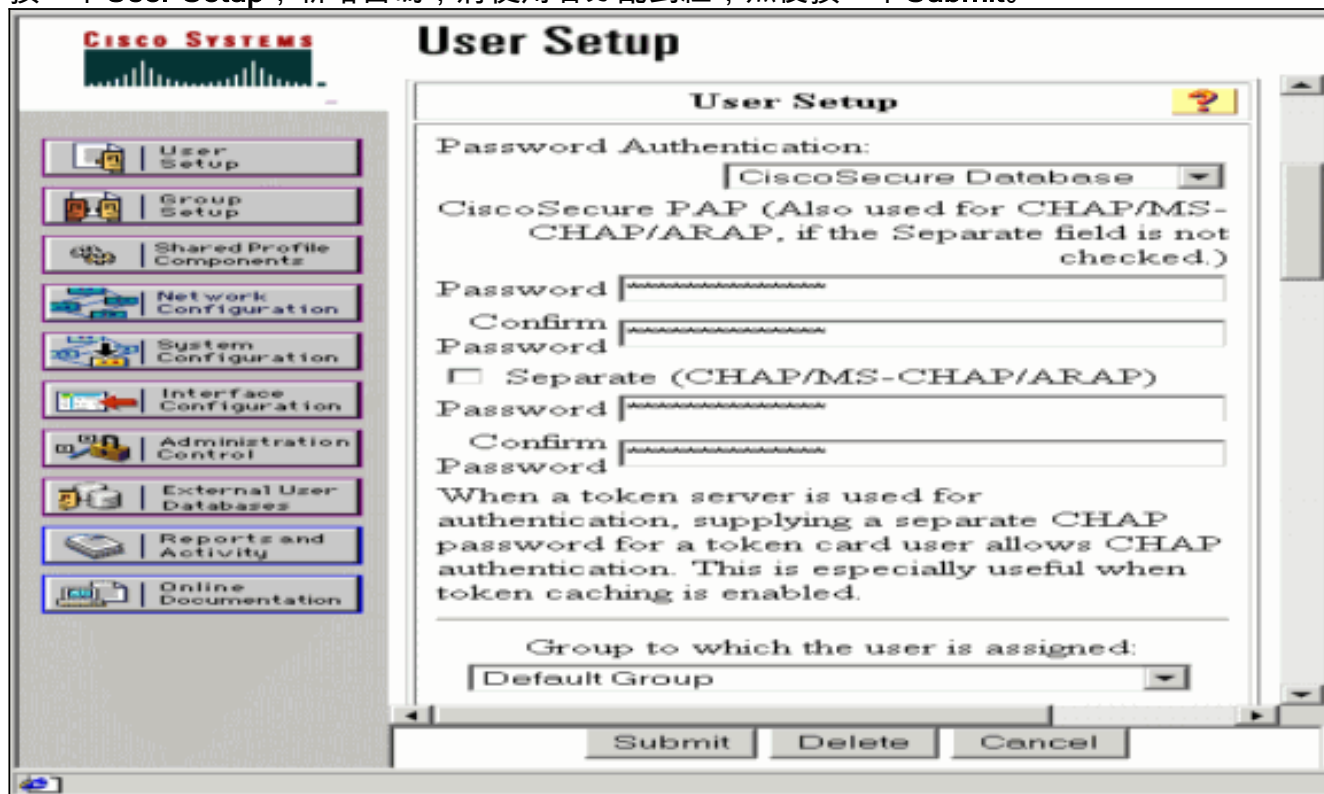
3. 按一下**Group Setup**，對於Service-Type，選擇**Framed**。對於Framed-Protocol，選擇
   PPP，然後按一下**Submit**。
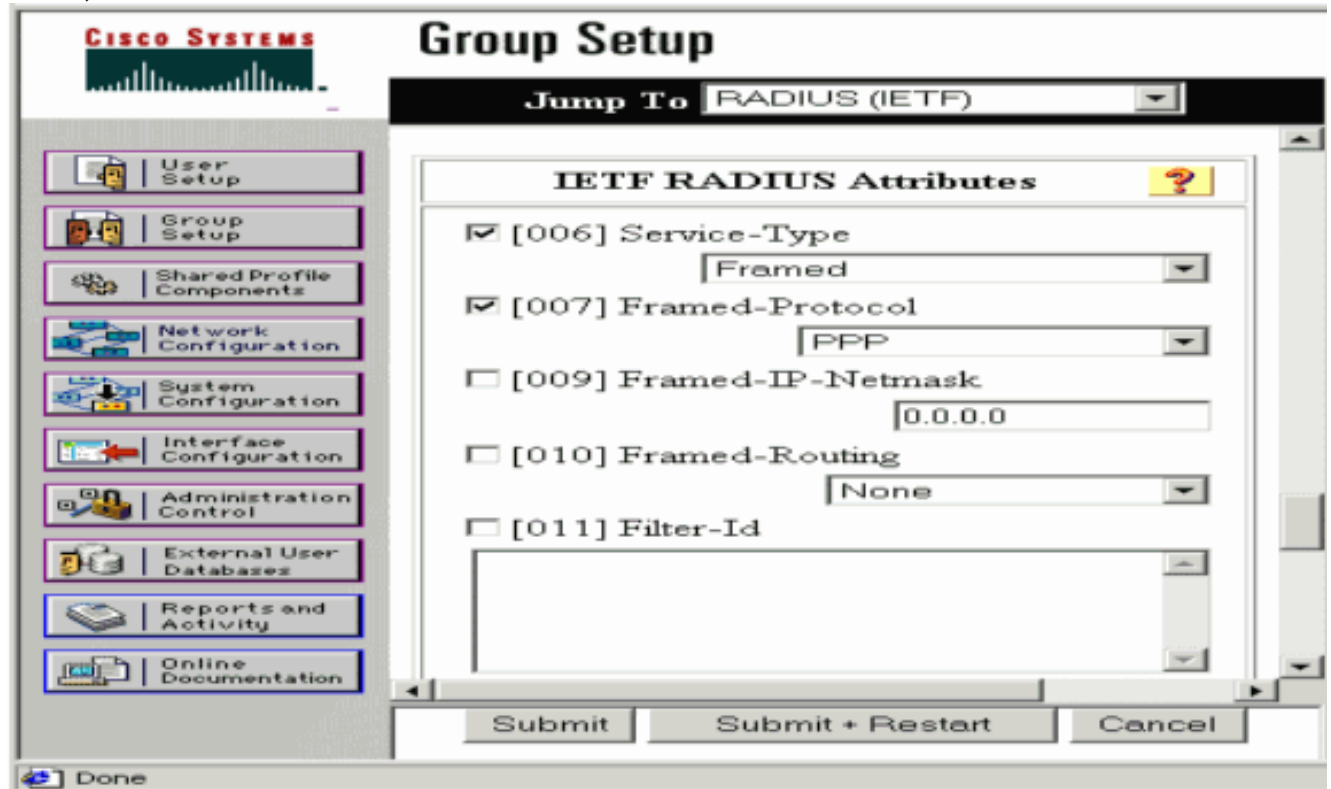
4. 在**Group Setup**中，檢查MS-MPPE RADIUS資訊，完成後，按一下**Submit + Restart**。

5. 按一下User Setup，新增密碼，將使用者分配到組，然後按一下Submit。

6. 在新增加密之前測試對路由器的身份驗證。如果驗證無效，請參閱本文檔的疑難解答部分。

新增到配置

新增加密

您可以使用以下命令新增MPPE加密：

```
interface virtual-template 1
(config-if)#ppp encrypt mppe 40|128|auto passive|required|stateful
```

由於該示例假定加密與本地身份驗證（路由器上的使用者名稱和密碼）配合使用，因此PC配置正確。現在，您可以新增以下命令來獲得最大的靈活性：

```
ppp encrypt mppe auto
```

從伺服器分配靜態IP地址

如果需要為使用者分配特定IP地址，請在ACS使用者設定中選擇**分配靜態IP地址**，然後填寫IP地址。

向伺服器新增訪問清單

為了控制使用者連線到路由器後PPTP使用者可以訪問的內容，您可以在路由器上配置訪問清單。例如，如果您發出以下命令：

```
access-list 101 permit ip any host 10.1.1.2 log
```

然後在ACS中選擇**Filter-Id(attribute 11)**，並在框中輸入**101**,PPTP使用者可以訪問10.1.1.2主機，但不能訪問其他主機。當您發出**show ip interface virtual-access *x***命令時，其中*x*是您可以通過**show user**命令確定的數字，訪問清單應顯示為已應用：

```
Inbound access list is 101
```

新增記帳

您可以使用以下命令新增會話記帳：

```
aaa accounting network default start-stop radius
```

Cisco Secure ACS中的記帳記錄如下輸出所示：

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,
Acct-Status-Type,Acct-Session-Id,Acct-Session-Time,
Service-Type,Framed-Protocol,Acct-Input-Octets,
Acct-Output-Octets,Acct-Input-Packets,Acct-Output-Packets,
Framed-IP-Address,NAS-Port,NAS-IP-Address
09/28/2003,20:58:37,georgia,Default Group,,Start,00000005,,
Framed,PPP,,,,,,5,10.66.79.99
09/28/2000,21:00:38,georgia,Default Group,,Stop,00000005,121,
Framed,PPP,3696,1562,49,
38,192.168.1.1,5,10.66.79.99
```

附註： 為便於顯示，已將換行符新增到示例。實際輸出中的換行符與此處顯示的不同。

分割通道

當PC上出現PPTP隧道時，PPTP路由器的安裝度量高於以前的預設值，因此會丟失Internet連線。為了解決此問題，假設路由器內部的網路為10.1.1.X，請運行批處理檔案(batch.bat)來修改Microsoft路由以刪除預設路由並重新安裝預設路由（這需要分配PPTP客戶端的IP地址）；例如，192.168.1.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 10.66.79.33 metric 1
route add 10.1.1.0 mask 255.255.255.0 192.168.1.1 metric 1
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](僅供[已註冊](客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- **show vpdn session** — 顯示有關虛擬專用撥接網路(VPDN)中作用中第2層轉送(L2F)通訊協定通道和訊息識別符號的資訊。

```
moss#show vpdn session
%No active L2TP tunnels
%No active L2F tunnels

PPTP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf    Username      State   Last Chg Uniq ID
7     32768 7     Vi3     georgia       estabd  00:00:25 6
moss#show vpdn
%No active L2TP tunnels
%No active L2F tunnels

PPTP Tunnel and Session Information Total tunnels 1 sessions 1
LocID Remote Name     State    Remote Address   Port   Sessions VPDN Group
7                     estabd   10.66.79.60      3454   1        1

LocID RemID TunID Intf    Username      State   Last Chg Uniq ID
7     32768 7     Vi3     georgia       estabd  00:00:51 6
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. **PC指定加密，但路由器不指定。** PC使用者可看到：
   `The remote computer does not support the required data encryption type.`
2. **PC和路由器都指定加密，但RADIUS伺服器未配置為向下傳送MPPE金鑰（通常顯示為屬性26）。** PC使用者可看到：
   `The remote computer does not support the required`
   `data encryption type.`
3. **路由器指定加密（必需），但PC不指定（不允許）。** PC使用者可看到：
   `The specified port is not connected.`
4. **使用者輸入的使用者名稱或密碼不正確。** PC使用者可看到：
   `Access was denied because the username and/or`
   `password was invalid on the domain.`

路由器debug顯示：**注意**：為了顯示目的，在此示例中新增了換行符。實際輸出中的換行符與此處顯示的不同。

```
Sep 28 21:34:16.299: RADIUS: Received from id 21645/13 10.66.79.120:1645,
Access-Reject, len 54
Sep 28 21:34:16.299: RADIUS: authenticator 37 BA 2B 4F 23 02 44 4D - D4
A0 41 3B 61 2D 5E 0C
Sep 28 21:34:16.299: RADIUS:  Vendor, Microsoft    [26]  22
Sep 28 21:34:16.299: RADIUS:   MS-CHAP-ERROR       [2]   16
Sep 28 21:34:16.299: RADIUS:   01 45 3D 36 39 31 20 52 3D 30 20 56 3D
[?E=691 R=0 V=]
Sep 28 21:34:16.299: RADIUS:  Reply-Message        [18]  12
Sep 28 21:34:16.299: RADIUS:   52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
```

5. **RADIUS伺服器無法通訊。**PC使用者可看到：

```
Access was denied because the username and/or password
was invalid on the domain.
```

路由器debug顯示：**注意**：為了顯示目的，在此示例中新增了換行符。實際輸出中的換行符與此處顯示的不同。

```
Sep 28 21:46:56.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)
for id 21645/43
Sep 28 21:47:01.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)
for id 21645/43
Sep 28 21:47:06.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)
for id 21645/43
Sep 28 21:47:11.135: RADIUS: No response from (10.66.79.120:1645,1646)
for id 21645/43
Sep 28 21:47:11.135: RADIUS/DECODE: parse response no app start; FAIL
Sep 28 21:47:11.135: RADIUS/DECODE: parse response; FAIL
```

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

如果不起作用，則最少的debug命令包括：

- debug aaa authentication — 顯示有關AAA/TACACS+身份驗證的資訊。
- debug aaa authorization — 顯示有關AAA/TACACS+授權的資訊。
- debug ppp negotiation — 顯示在PPP啟動期間傳輸的PPP資料包，其中協商了PPP選項。
- debug ppp authentication — 顯示身份驗證協定消息，包括CHAP資料包交換和密碼身份驗證協定(PAP)交換。
- debug radius — 顯示與RADIUS關聯的詳細調試資訊。

如果身份驗證有效，但MPPE加密出現問題，請使用以下命令：

- debug ppp mppe packet — 顯示所有傳入和傳出MPPE流量。
- debug ppp mppe event — 顯示關鍵MPPE事件。
- debug ppp mppe detailed — 顯示詳細的MPPE資訊。
- debug vpdn l2x-packets — 顯示有關L2F協定標頭和狀態的消息。
- debug vpdn events — 顯示有關屬於正常隧道建立或關閉一部分的事件的消息。
- debug vpdn errors — 顯示阻止隧道建立的錯誤或導致已建立的隧道關閉的錯誤。
- debug vpdn packets — 顯示交換的每個協定資料包。此選項可能導致大量調試消息，並且通常只能在具有單個活動會話的debug機箱上使用此命令。

您也可以使用以下命令進行疑難排解：

- clear interface virtual-access *x* — **關閉指定通道和通道中的所有會話。**

良好調試輸出示例

此偵錯會顯示RFC中的重要事件：

- **SCCRQ** = Start-Control-Connection-Request — 消息代碼位元組9和10 = 0001
- **SCCRP** = Start-Control-Connection-Reply
- **OCRQ** = Outgoing-Call-Request — 消息代碼位元組9和10 = 0007
- **OCRP** = Outgoing-Call-Reply

注意：為了顯示目的，在此示例中新增了換行符。實際輸出中的換行符與此處顯示的不同。

```
moss#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
PPP:
  PPP protocol negotiation debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on
VPN:
  L2X control packets debugging is on
Sep 28 21:53:22.403:  Tnl 23 PPTP:
I 009C00011A2B3C4D0001000001000000000000010000...
Sep 28 21:53:22.403:  Tnl 23 PPTP: I SCCRQ
Sep 28 21:53:22.403:  Tnl 23 PPTP: protocol version 100
Sep 28 21:53:22.403:  Tnl 23 PPTP: framing caps 1
Sep 28 21:53:22.403:  Tnl 23 PPTP: bearer caps 1
Sep 28 21:53:22.403:  Tnl 23 PPTP: max channels 0
Sep 28 21:53:22.403:  Tnl 23 PPTP: firmware rev 893
Sep 28 21:53:22.403:  Tnl 23 PPTP: hostname ""
Sep 28 21:53:22.403:  Tnl 23 PPTP: vendor "Microsoft Windows NT"
Sep 28 21:53:22.403:  Tnl 23 PPTP: O SCCRP
Sep 28 21:53:22.407:  Tnl 23 PPTP: I
00A800011A2B3C4D0007000080007C0E0000012C05F5...
Sep 28 21:53:22.407:  Tnl 23 PPTP: CC I OCRQ
Sep 28 21:53:22.407:  Tnl 23 PPTP: call id 32768
Sep 28 21:53:22.411:  Tnl 23 PPTP: serial num 31758
Sep 28 21:53:22.411:  Tnl 23 PPTP: min bps 300
Sep 28 21:53:22.411:  Tnl 23 PPTP: max bps 100000000
Sep 28 21:53:22.411:  Tnl 23 PPTP: bearer type 3
Sep 28 21:53:22.411:  Tnl 23 PPTP: framing type 3
Sep 28 21:53:22.411:  Tnl 23 PPTP: recv win size 64
Sep 28 21:53:22.411:  Tnl 23 PPTP: ppd 0
Sep 28 21:53:22.411:  Tnl 23 PPTP: phone num len 0
Sep 28 21:53:22.411:  Tnl 23 PPTP: phone num ""
Sep 28 21:53:22.411: AAA/BIND(0000001C): Bind i/f Virtual-Template1
Sep 28 21:53:22.415:  Tnl/Sn 23/23 PPTP: CC O OCRP
Sep 28 21:53:22.415: ppp27 PPP: Using vpn set call direction
Sep 28 21:53:22.415: ppp27 PPP: Treating connection as a callin
Sep 28 21:53:22.415: ppp27 PPP: Phase is ESTABLISHING, Passive Open
Sep 28 21:53:22.415: ppp27 LCP: State is Listen
Sep 28 21:53:22.459:  Tnl 23 PPTP: I
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFFF
Sep 28 21:53:22.459:  Tnl/Sn 23/23 PPTP: CC I SLI
Sep 28 21:53:22.459: ppp27 LCP: I CONFREQ [Listen] id 0 len 44
```

```
Sep 28 21:53:22.459: ppp27 LCP:    MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.459: ppp27 LCP:    PFC (0x0702)
Sep 28 21:53:22.459: ppp27 LCP:    ACFC (0x0802)
Sep 28 21:53:22.459: ppp27 LCP:    Callback 6  (0x0D0306)
Sep 28 21:53:22.459: ppp27 LCP:    MRRU 1614 (0x1104064E)
Sep 28 21:53:22.459: ppp27 LCP:    EndpointDisc 1 Local
Sep 28 21:53:22.459: ppp27 LCP:     (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.463: ppp27 LCP:     (0x2D0E8100000016)
Sep 28 21:53:22.463: ppp27 LCP: O CONFREQ [Listen] id 1 len 15
Sep 28 21:53:22.463: ppp27 LCP:    AuthProto MS-CHAP (0x0305C22380)
Sep 28 21:53:22.463: ppp27 LCP:    MagicNumber 0xD0B06B2C (0x0506D0B06B2C)
Sep 28 21:53:22.463: ppp27 LCP: O CONFREJ [Listen] id 0 len 11
Sep 28 21:53:22.463: ppp27 LCP:    Callback 6  (0x0D0306)
Sep 28 21:53:22.463: ppp27 LCP:    MRRU 1614 (0x1104064E)
Sep 28 21:53:22.467: ppp27 LCP: I CONFACK [REQsent] id 1 len 15
Sep 28 21:53:22.467: ppp27 LCP:    AuthProto MS-CHAP (0x0305C22380)
Sep 28 21:53:22.467: ppp27 LCP:    MagicNumber 0xD0B06B2C (0x0506D0B06B2C)
Sep 28 21:53:22.467: ppp27 LCP: I CONFREQ [ACKrcvd] id 1 len 37
Sep 28 21:53:22.467: ppp27 LCP:    MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.467: ppp27 LCP:    PFC (0x0702)
Sep 28 21:53:22.467: ppp27 LCP:    ACFC (0x0802)
Sep 28 21:53:22.471: ppp27 LCP:    EndpointDisc 1 Local
Sep 28 21:53:22.471: ppp27 LCP:     (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.471: ppp27 LCP:     (0x2D0E8100000016)
Sep 28 21:53:22.471: ppp27 LCP: O CONFACK [ACKrcvd] id 1 len 37
Sep 28 21:53:22.471: ppp27 LCP:    MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.471: ppp27 LCP:    PFC (0x0702)
Sep 28 21:53:22.471: ppp27 LCP:    ACFC (0x0802)
Sep 28 21:53:22.471: ppp27 LCP:    EndpointDisc 1 Local
Sep 28 21:53:22.471: ppp27 LCP:     (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.471: ppp27 LCP:     (0x2D0E8100000016)
Sep 28 21:53:22.471: ppp27 LCP: State is Open
Sep 28 21:53:22.471: ppp27 PPP: Phase is AUTHENTICATING, by this end
Sep 28 21:53:22.475: ppp27 MS-CHAP: O CHALLENGE id 1 len 21 from "SV3-2   "
Sep 28 21:53:22.475:   Tnl 23 PPTP: I
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFFF
Sep 28 21:53:22.475:   Tnl/Sn 23/23 PPTP: CC I SLI
Sep 28 21:53:22.479: ppp27 LCP: I IDENTIFY [Open] id 2 len
18 magic 0x377413E2 MSRASV5.00
Sep 28 21:53:22.479: ppp27 LCP: I IDENTIFY [Open] id 3 len
30 magic 0x377413E2 MSRAS-0-CSCOAPACD12364
Sep 28 21:53:22.479: ppp27 MS-CHAP: I RESPONSE id 1 len 61 from "georgia"
Sep 28 21:53:22.483: ppp27 PPP: Phase is FORWARDING, Attempting Forward
Sep 28 21:53:22.483: ppp27 PPP: Phase is AUTHENTICATING, Unauthenticated User
Sep 28 21:53:22.483: AAA/AUTHEN/PPP (0000001C): Pick method list 'default'
Sep 28 21:53:22.483: RADIUS:  AAA Unsupported    [152] 14
Sep 28 21:53:22.483: RADIUS:   55 6E 69 71 2D 53 65 73 73 2D 49 44
[Uniq-Sess-ID]
Sep 28 21:53:22.483: RADIUS(0000001C): Storing nasport 27 in rad_db
Sep 28 21:53:22.483: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Sep 28 21:53:22.483: RADIUS/ENCODE(0000001C): acct_session_id: 38
Sep 28 21:53:22.487: RADIUS(0000001C): sending
Sep 28 21:53:22.487: RADIUS/ENCODE: Best Local IP-Address 10.66.79.99
for Radius-Server 10.66.79.120
Sep 28 21:53:22.487: RADIUS(0000001C): Send Access-Request to
10.66.79.120:1645 id 21645/44, len 133
Sep 28 21:53:22.487: RADIUS:  authenticator 15 8A 3B EE 03 24
0C F0 - 00 00 00 00 00 00 00 00
Sep 28 21:53:22.487: RADIUS:  Framed-Protocol     [7]   6    PPP                        [1]
Sep 28 21:53:22.487: RADIUS:  User-Name           [1]   9    "georgia"
Sep 28 21:53:22.487: RADIUS:  Vendor, Microsoft   [26]  16
Sep 28 21:53:22.487: RADIUS:   MSCHAP_Challenge   [11]  10
Sep 28 21:53:22.487: RADIUS:    15 8A 3B EE 03 24 0C  [??;??$?]
Sep 28 21:53:22.487: RADIUS:  Vendor, Microsoft   [26]  58
```

```
Sep 28 21:53:22.487: RADIUS:    MS-CHAP-Response   [1]   52   *
Sep 28 21:53:22.487: RADIUS: NAS-Port-Type         [61]  6    Virtual                    [5]
Sep 28 21:53:22.487: RADIUS: NAS-Port              [5]   6    27
Sep 28 21:53:22.487: RADIUS: Service-Type          [6]   6    Framed                     [2]
Sep 28 21:53:22.491: RADIUS: NAS-IP-Address        [4]   6    10.66.79.99
Sep 28 21:53:22.515: RADIUS: Received from id 21645/44 10.66.79.120:1645,
Access-Accept, len 141
Sep 28 21:53:22.515: RADIUS: authenticator ED 3F 8A 08 2D A2 EB 4F - 78
3F 5D 80 58 7B B5 3E
Sep 28 21:53:22.515: RADIUS: Service-Type          [6]   6    Framed                     [2]
Sep 28 21:53:22.515: RADIUS: Framed-Protocol       [7]   6    PPP                        [1]
Sep 28 21:53:22.515: RADIUS: Filter-Id             [11]  8
Sep 28 21:53:22.515: RADIUS:    31 30 31 2E 69 6E      [101.in]
Sep 28 21:53:22.515: RADIUS: Vendor, Microsoft     [26]  12
Sep 28 21:53:22.515: RADIUS:    MS-MPPE-Enc-Policy [7]   6
Sep 28 21:53:22.515: RADIUS:    00 00 00              [???]
Sep 28 21:53:22.515: RADIUS: Vendor, Microsoft     [26]  12
Sep 28 21:53:22.515: RADIUS:    MS-MPPE-Enc-Type   [8]   6
Sep 28 21:53:22.515: RADIUS:    00 00 00              [???]
Sep 28 21:53:22.515: RADIUS: Vendor, Microsoft     [26]  40
Sep 28 21:53:22.515: RADIUS:    MS-CHAP-MPPE-Keys  [12]  34   *
Sep 28 21:53:22.519: RADIUS: Framed-IP-Address     [8]   6    192.168.1.1
Sep 28 21:53:22.519: RADIUS: Class                 [25]  31
Sep 28 21:53:22.519: RADIUS:
43 49 53 43 4F 41 43 53 3A 30 30 30 30 30 30 36  [CISCOACS:0000006]
Sep 28 21:53:22.519: RADIUS:
33 2F 30 61 34 32 34 66 36 33 2F 32 37           [3/0a424f63/27]
Sep 28 21:53:22.519: RADIUS(0000001C): Received from id 21645/44
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: service-type
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: Framed-Protocol
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: inacl: Peruser
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: MS-CHAP-MPPE-Keys
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: addr
Sep 28 21:53:22.523: ppp27 PPP: Phase is FORWARDING, Attempting Forward
Sep 28 21:53:22.523: Vi3 PPP: Phase is DOWN, Setup
Sep 28 21:53:22.527: AAA/BIND(0000001C): Bind i/f Virtual-Access3
Sep 28 21:53:22.531: %LINK-3-UPDOWN: Interface Virtual-Access3,
changed state to up
Sep 28 21:53:22.531: Vi3 PPP: Phase is AUTHENTICATING, Authenticated User
Sep 28 21:53:22.531: Vi3 AAA/AUTHOR/LCP: Process Author
Sep 28 21:53:22.531: Vi3 AAA/AUTHOR/LCP: Process Attr: service-type
Sep 28 21:53:22.531: Vi3 MS-CHAP: O SUCCESS id 1 len 4
Sep 28 21:53:22.535: Vi3 PPP: Phase is UP
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/IPCP: FSM authorization not needed
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/FSM: We can start IPCP
Sep 28 21:53:22.535: Vi3 IPCP: O CONFREQ [Closed] id 1 len 10
Sep 28 21:53:22.535: Vi3 IPCP:    Address 10.66.79.99 (0x03060A424F63)
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/CCP: FSM authorization not needed
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/FSM: We can start CCP
Sep 28 21:53:22.535: Vi3 CCP: O CONFREQ [Closed] id 1 len 10
Sep 28 21:53:22.535: Vi3 CCP: MS-PPC supported bits 0x01000060 (0x120601000060)
Sep 28 21:53:22.535: Vi3 PPP: Process pending packets
Sep 28 21:53:22.539: RADIUS(0000001C): Using existing nas_port 27
Sep 28 21:53:22.539: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Sep 28 21:53:22.539: RADIUS(0000001C): sending
Sep 28 21:53:22.539: RADIUS/ENCODE: Best Local IP-Address
10.66.79.99 for Radius-Server 10.66.79.120
Sep 28 21:53:22.539: RADIUS(0000001C): Send Accounting-Request
to 10.66.79.120:1646 id 21645/45, len 147
Sep 28 21:53:22.539: RADIUS: authenticator 1A 76 20 95 95 F8
81 42 - 1F E8 E7 C1 8F 10 BA 94
Sep 28 21:53:22.539: RADIUS: Acct-Session-Id     [44]  10   "00000026"
Sep 28 21:53:22.539: RADIUS: Tunnel-Server-Endpoi[67]  13   "10.66.79.99"
Sep 28 21:53:22.539: RADIUS: Tunnel-Client-Endpoi[66]  13   "10.66.79.60"
```

```
Sep 28 21:53:22.543: RADIUS:  Tunnel-Assignment-Id[82]  3   "1"
Sep 28 21:53:22.543: RADIUS:  Framed-Protocol    [7]   6   PPP                       [1]
Sep 28 21:53:22.543: RADIUS:  Acct-Authentic     [45]  6   RADIUS                    [1]
Sep 28 21:53:22.543: RADIUS:  User-Name          [1]   9   "georgia"
Sep 28 21:53:22.543: RADIUS:  Acct-Status-Type   [40]  6   Start                     [1]
Sep 28 21:53:22.543: RADIUS:  NAS-Port-Type      [61]  6   Virtual                   [5]
Sep 28 21:53:22.543: RADIUS:  NAS-Port           [5]   6   27
Sep 28 21:53:22.543: RADIUS:  Class              [25]  31
Sep 28 21:53:22.543: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30
30 30 36  [CISCOACS:0000006]
Sep 28 21:53:22.543: RADIUS:   33 2F 30 61 34 32 34 66 36 33 2F 32 37
          [3/0a424f63/27]
Sep 28 21:53:22.547: RADIUS:  Service-Type       [6]   6   Framed                    [2]
Sep 28 21:53:22.547: RADIUS:  NAS-IP-Address     [4]   6   10.66.79.99
Sep 28 21:53:22.547: RADIUS:  Acct-Delay-Time    [41]  6   0
Sep 28 21:53:22.547: Vi3 CCP: I CONFREQ [REQsent] id 4 len 10
Sep 28 21:53:22.547: Vi3 CCP:    MS-PPC supported bits 0x010000F1
(0x1206010000F1)
Sep 28 21:53:22.547: Vi3 CCP: O CONFNAK [REQsent] id 4 len 10
Sep 28 21:53:22.551: Vi3 CCP:    MS-PPC supported bits 0x01000060
(0x120601000060)
Sep 28 21:53:22.551: Vi3 CCP: I CONFNAK [REQsent] id 1 len 10
Sep 28 21:53:22.551: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.551: Vi3 CCP: O CONFREQ [REQsent] id 2 len 10
Sep 28 21:53:22.551: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.551: Vi3 IPCP: I CONFREQ [REQsent] id 5 len 34
Sep 28 21:53:22.551: Vi3 IPCP:    Address 0.0.0.0 (0x030600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Sep 28 21:53:22.551: Vi3 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0,
we want 0.0.0.0
Sep 28 21:53:22.551: Vi3 AAA/AUTHOR/IPCP: Processing AV inacl
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Processing AV addr
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Authorization succeeded
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0,
we want 192.168.1.1
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for primary dns
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for primary wins
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for seconday dns
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for seconday wins
Sep 28 21:53:22.555: Vi3 IPCP: O CONFREJ [REQsent] id 5 len 28
Sep 28 21:53:22.555: Vi3 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Sep 28 21:53:22.555: Vi3 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Sep 28 21:53:22.555: Vi3 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Sep 28 21:53:22.555: Vi3 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Sep 28 21:53:22.555: Vi3 IPCP: I CONFACK [REQsent] id 1 len 10
Sep 28 21:53:22.555: Vi3 IPCP:    Address 10.66.79.99 (0x03060A424F63)
Sep 28 21:53:22.563: Vi3 CCP: I CONFREQ [REQsent] id 6 len 10
Sep 28 21:53:22.563: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.563: Vi3 CCP: O CONFACK [REQsent] id 6 len 10
Sep 28 21:53:22.563: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.567: Vi3 CCP: I CONFACK [ACKsent] id 2 len 10
Sep 28 21:53:22.567: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.567: Vi3 CCP: State is Open
Sep 28 21:53:22.567: Vi3 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
Sep 28 21:53:22.567: Vi3 IPCP:    Address 0.0.0.0 (0x030600000000)
Sep 28 21:53:22.567: Vi3 IPCP: O CONFNAK [ACKrcvd] id 7 len 10
```

```
Sep 28 21:53:22.571: Vi3 IPCP:    Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
Sep 28 21:53:22.575: Vi3 IPCP:    Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: O CONFACK [ACKrcvd] id 8 len 10
Sep 28 21:53:22.575: Vi3 IPCP:    Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: State is Open
Sep 28 21:53:22.575: AAA/AUTHOR: Processing PerUser AV inacl
Sep 28 21:53:22.583: Vi3 IPCP: Install route to 192.168.1.1
Sep 28 21:53:22.583: Vi3 IPCP: Add link info for cef entry 192.168.1.1
Sep 28 21:53:22.603: RADIUS: Received from id 21645/45 10.66.79.120:1646,
Accounting-response, len 20
Sep 28 21:53:22.603: RADIUS:  authenticator A6 B3 4C 4C 04 1B BE 8E - 6A
BF 91 E2 3C 01 3E CA
Sep 28 21:53:23.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 Virtual-Access3, changed state to up
```

相關資訊

- [Cisco Secure ACS for Windows支援頁](#)
- [技術支援與文件 - Cisco Systems](#)