Konfigurieren von CiscoSecure ACS für PPTP-Authentifizierung des Windows-Routers

Inhalt

Einführung

Die Unterstützung für Point-to-Point Tunnel Protocol (PPTP) wurde der Cisco IOS® Softwareversion 12.0.5.XE5 auf den Cisco 7100- und 7200-Plattformen hinzugefügt (siehe PPTP mit Microsoft Point-to-Point Encryption (MPPE) [Cisco IOS Softwareversion 12.0]). Die Unterstützung für weitere Plattformen wurde in Version 12.1.5.T der Cisco IOS-Software hinzugefügt (siehe MSCHAP Version 2).

RFC 2637 beschreibt PPTP. In PPTP-Hinsicht ist laut RFC der PPTP Access Concentrator (PAC) der Client (der PC, d. h. der Anrufer), und der PPTP Network Server (PNS) ist der Server (der Router, der Angerufene).

In diesem Dokument wird davon ausgegangen, dass PPTP-Verbindungen zum Router mit der lokalen Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) V1-Authentifizierung (und optional MPPE, das MS-CHAP V1 erfordert) unter Verwendung dieser Dokumente erstellt wurden und bereits betriebsbereit sind. Für die MPPE-Verschlüsselungsunterstützung ist RADIUS erforderlich. TACACS+ funktioniert für die Authentifizierung, jedoch nicht für die MPPE-Keying.

Die MS-CHAP V2-Unterstützung wurde der Cisco IOS Software-Version 12.2(2)XB5 hinzugefügt und in die Cisco IOS-Softwareversion 12.2(13)T integriert (siehe MSCHAP-Version 2). MPPE wird jedoch von MS-CHAP V2 noch nicht unterstützt.

Diese Beispielkonfiguration veranschaulicht das Einrichten einer PC-Verbindung mit dem Router (unter 10.66.79.99), die dann eine Benutzerauthentifizierung für das Cisco Secure Access Control System (ACS) 4.2 für Windows-Server (unter 10.66.79.120) bereitstellt, bevor Sie den Benutzer in das Netzwerk einbinden.

Hinweis: Der RADIUS-Server befindet sich normalerweise nicht außerhalb des Routers, außer in einer Laborumgebung.

Die PPTP-Unterstützung wurde Cisco Secure ACS 2.5 hinzugefügt, funktioniert aber aufgrund der Cisco Bug-ID CSCds92266 möglicherweise nicht mit dem Router (nur registrierte Kunden). ACS 2.6 und höher haben dieses Problem nicht.

MPPE wird von Cisco Secure UNIX nicht unterstützt. Zwei weitere RADIUS-Anwendungen mit MPPE-Unterstützung sind Microsoft RADIUS und Funk RADIUS.

Weitere Informationen zur Konfiguration von PPTP und MPPE mit einem Router finden Sie unter Konfigurieren des Cisco Routers und der VPN-Clients mithilfe von PPTP und MPPE.

Weitere Informationen zur Konfiguration von PPTP auf einem VPN 3000-Konzentrator mit Cisco Secure ACS für Windows RADIUS-Authentifizierung mit einem VPN 3000-Concentrator mit Cisco Secure ACS für Windows für RADIUS-Authentifizierung finden Sie unter Konfigurieren des VPN 3000-Concentrators und PPTP-Konfiguration.

Siehe PIX 6.x: PPTP mit Radius-Authentifizierungskonfigurationsbeispiel zum Konfigurieren von PPTP-Verbindungen zum PIX.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS 4.2 für Windows
- Cisco Router der Serie 3600
- Cisco IOS Softwareversion 12.4(3)

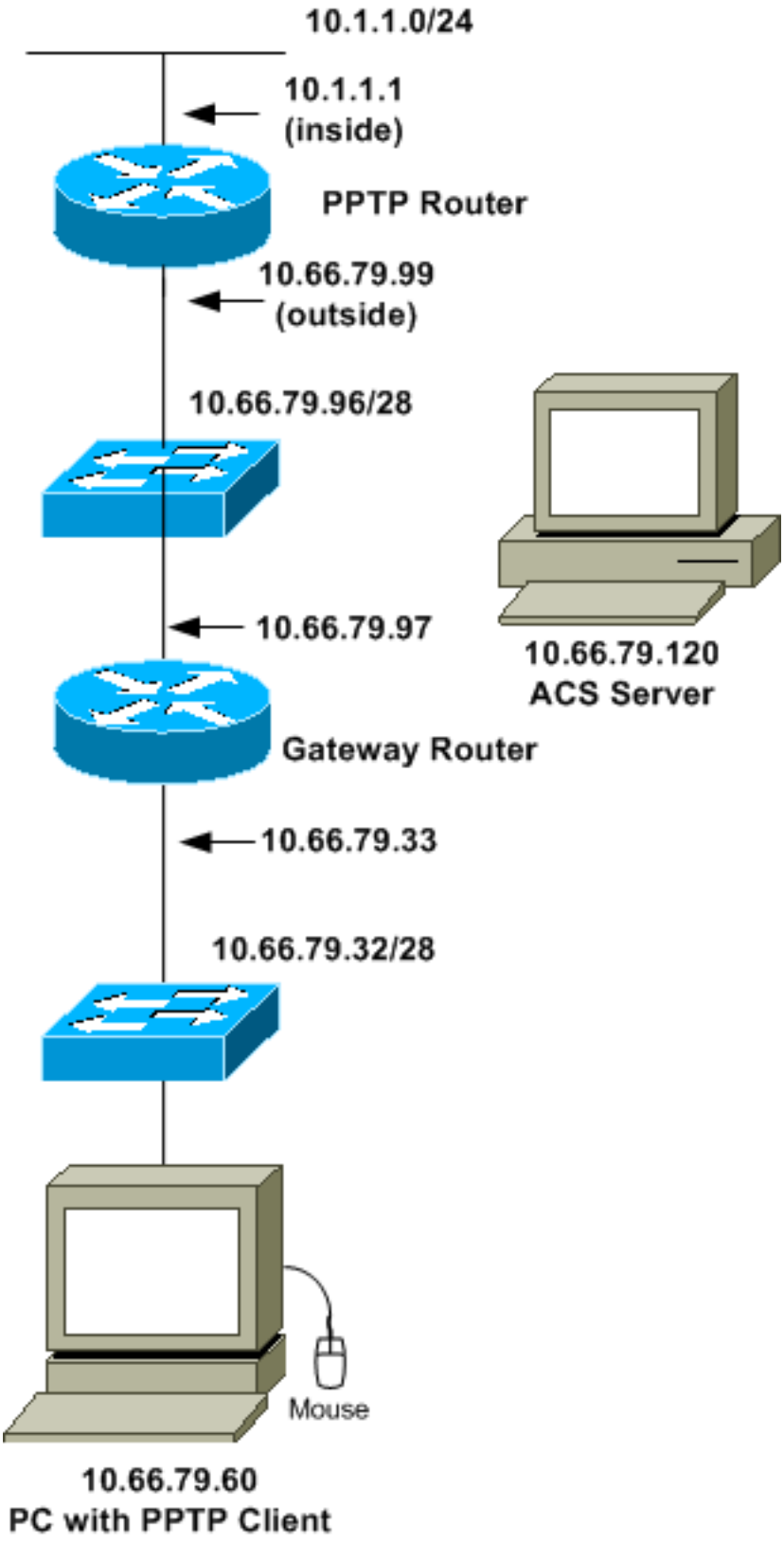
Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie sich in einem Live-Netzwerk befinden, stellen Sie sicher, dass Sie die potenziellen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

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Routerkonfiguration

Verwenden Sie diese Router-Konfiguration. Der Benutzer sollte eine Verbindung mit "**username john password doe**" herstellen können, auch wenn der RADIUS-Server nicht erreichbar ist (dies ist möglich, wenn der Server noch nicht mit Cisco Secure ACS konfiguriert wurde). In diesem Beispiel wird davon ausgegangen, dass die lokale Authentifizierung (und optional die Verschlüsselung) bereits aktiv ist.

Cisco Router der Serie 3600

```
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-Serverfallback-Funktion

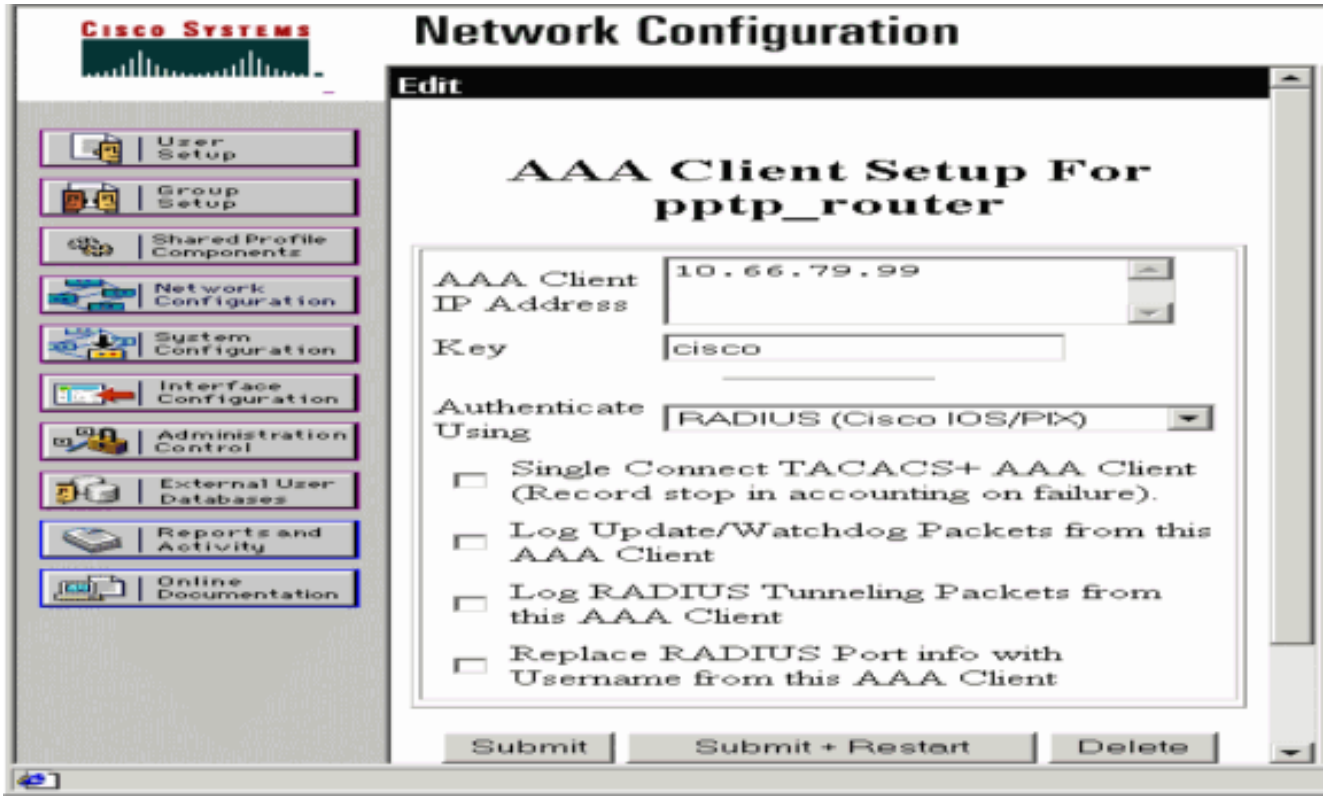
Wenn der primäre RADIUS-Server nicht mehr verfügbar ist, führt der Router ein Failover zum nächsten aktiven Backup-RADIUS-Server durch. Der Router verwendet weiterhin den sekundären RADIUS-Server für immer, selbst wenn der primäre Server verfügbar ist. In der Regel ist der primäre Server eine hohe Leistung und der bevorzugte Server.

Um die Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA) bei der Anmeldung festzulegen, verwenden Sie den Befehl **aaa authentication login** im globalen Konfigurationsmodus.

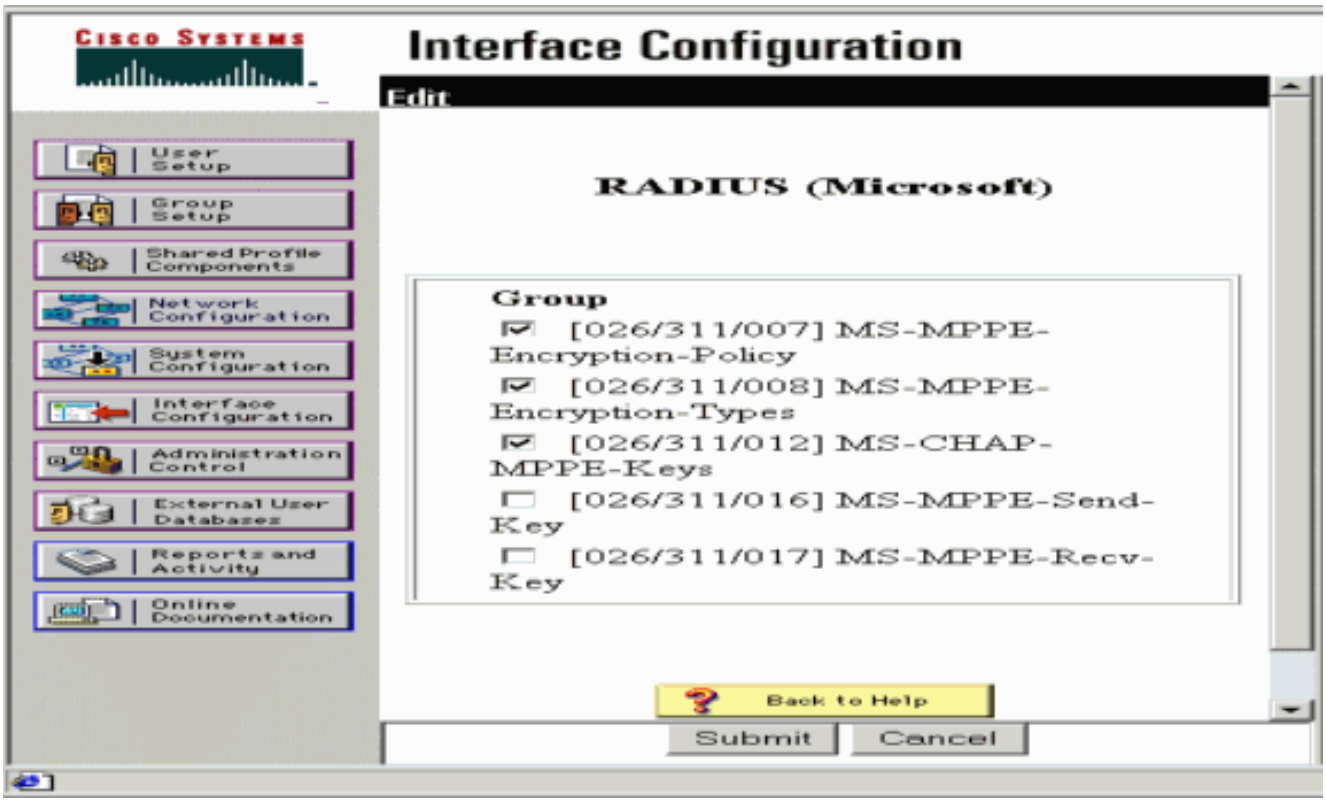
Cisco Secure ACS für Windows-Konfiguration

Gehen Sie folgendermaßen vor, um Cisco Secure ACS zu konfigurieren:

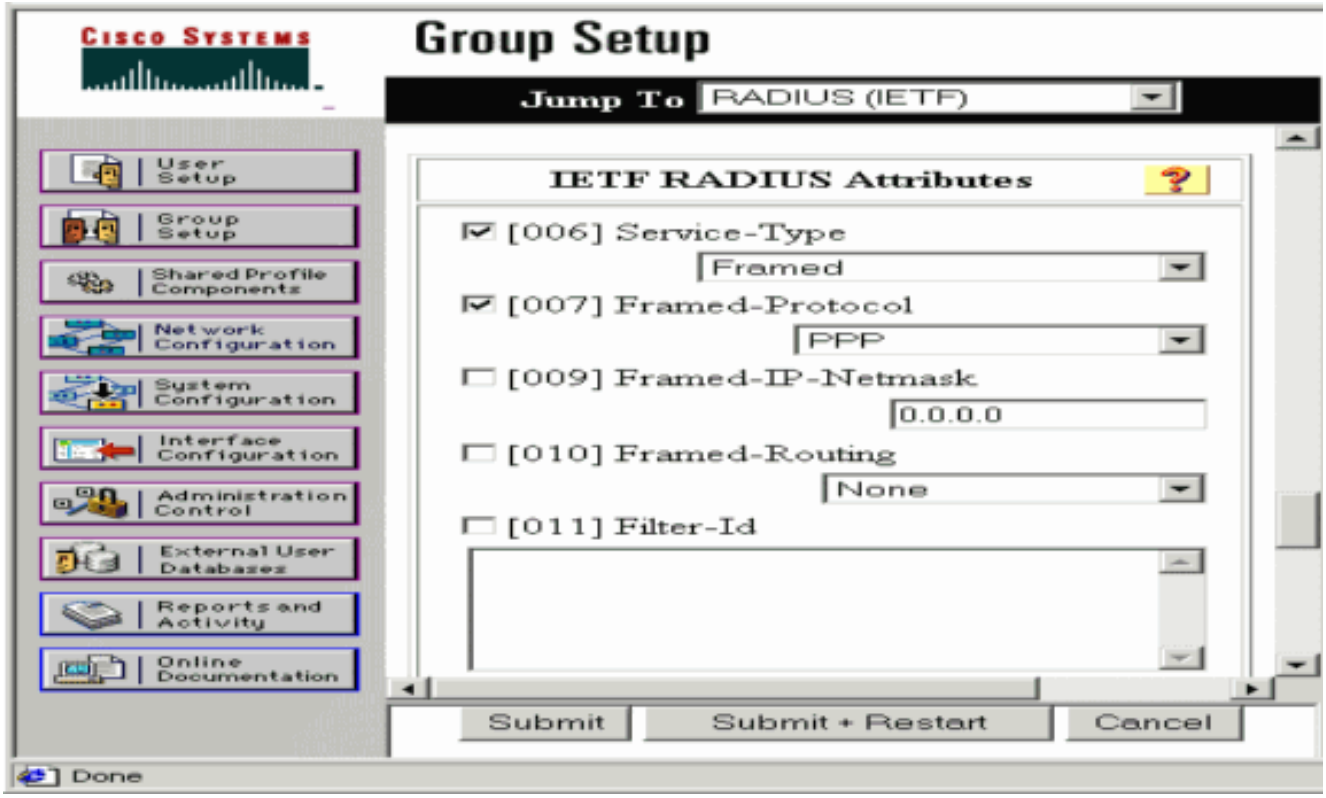
1. Klicken Sie auf **Netzwerkkonfiguration**, fügen Sie einen Eintrag für den Router hinzu, und klicken Sie auf **Senden + Neu starten**, wenn Sie fertig sind.



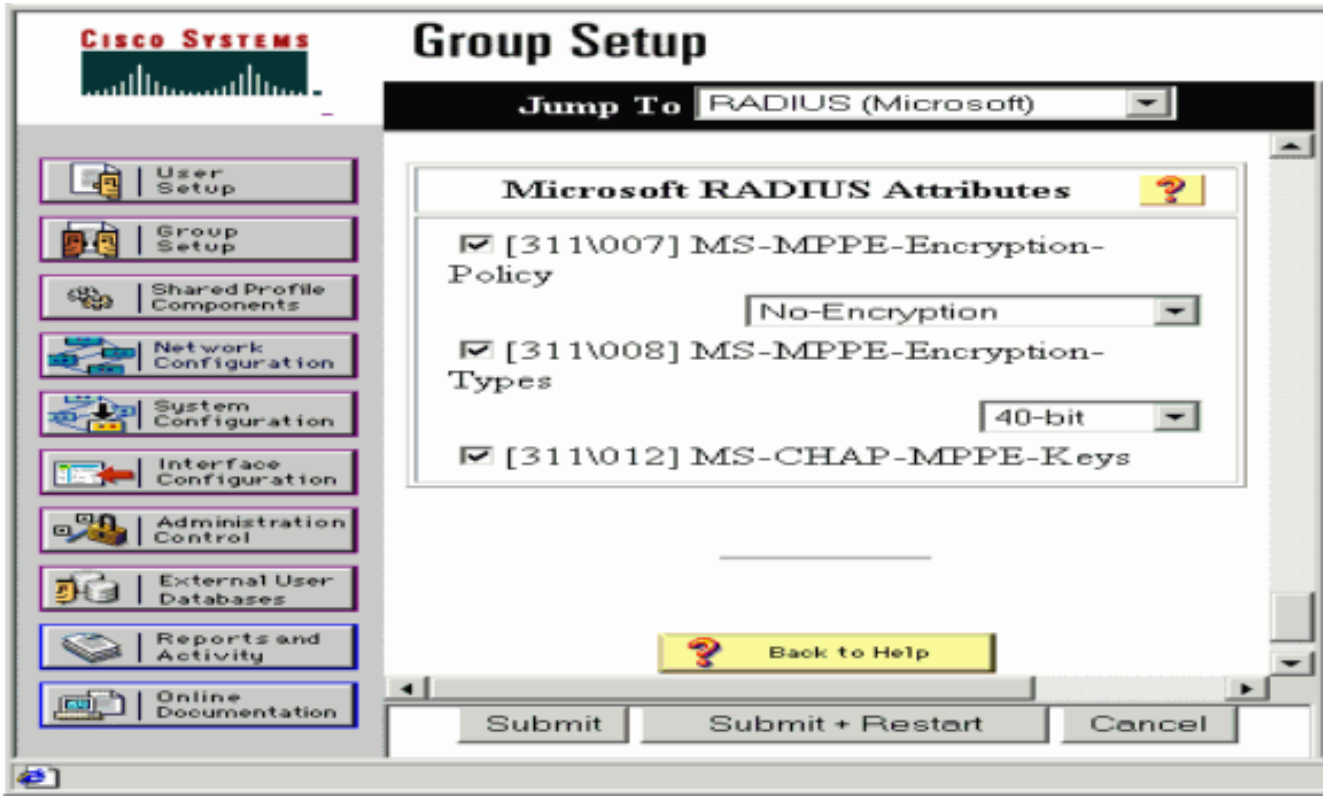
2. Wählen Sie **Schnittstellenkonfiguration > RADIUS (Microsoft)**, überprüfen Sie dann Ihre MPPE-Attribute, und klicken Sie auf **Senden**.



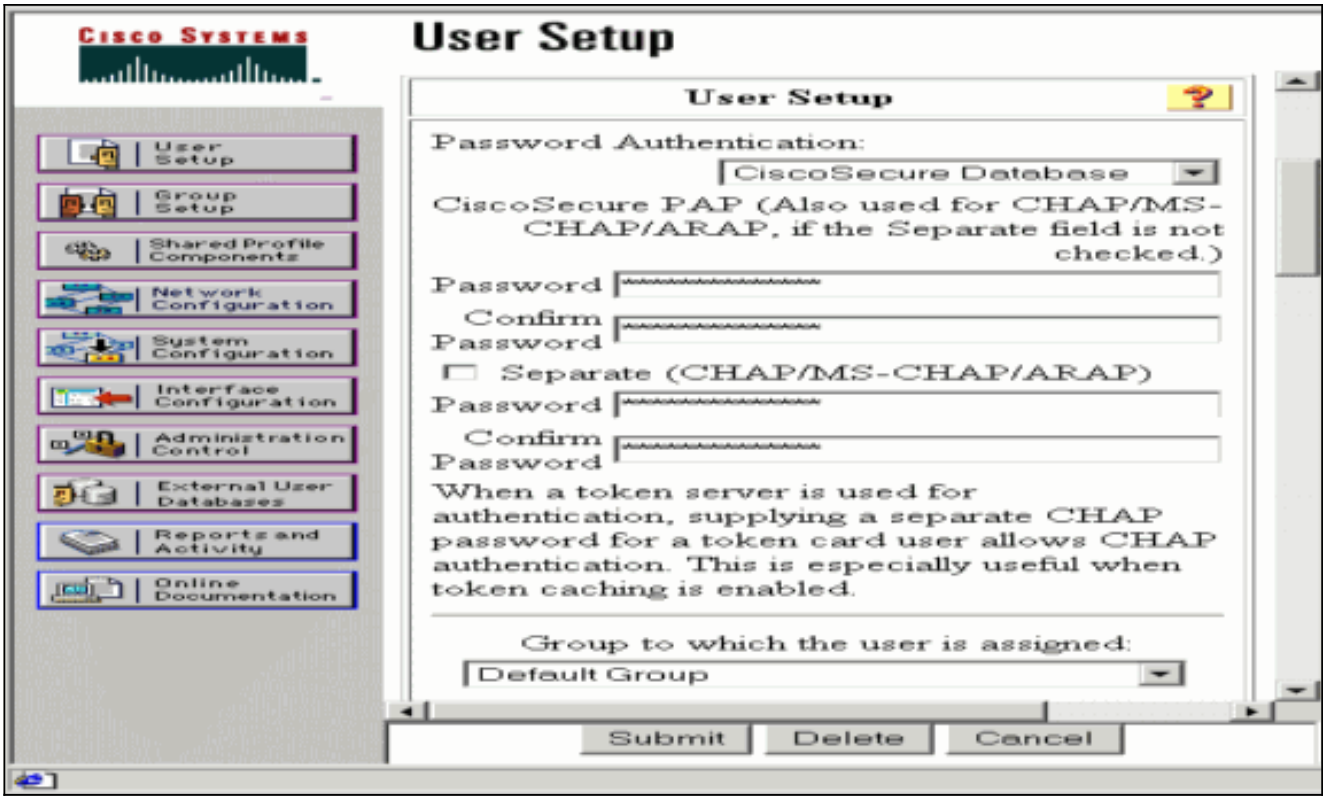
3. Klicken Sie auf **Gruppeneinrichtung**, und wählen Sie als Servicetyp **Framed aus**. Wählen Sie als Framed-Protokoll **PPP** aus, und klicken Sie auf **Submit (Senden)**.



4. Aktivieren Sie im **Gruppensetup** die MS-MPPE RADIUS-Informationen, und klicken Sie abschließend auf **Senden + Neu starten**.



5. Klicken Sie auf **Benutzereinrichtung**, fügen Sie ein Kennwort hinzu, weisen Sie den Benutzer der Gruppe zu, und klicken Sie auf **Senden**.



6. Testen Sie die Authentifizierung des Routers, bevor Sie die Verschlüsselung hinzufügen. Wenn die Authentifizierung nicht funktioniert, lesen Sie den Abschnitt Fehlerbehebung in diesem Dokument.

Hinzufügen zur Konfiguration

Verschlüsselung hinzufügen

Mit dem folgenden Befehl können Sie die MPPE-Verschlüsselung hinzufügen:

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

Da im Beispiel davon ausgegangen wird, dass die Verschlüsselung mit der lokalen Authentifizierung (Benutzername und Kennwort auf dem Router) funktioniert, ist der PC korrekt konfiguriert. Sie können diesen Befehl jetzt hinzufügen, um eine maximale Flexibilität zu ermöglichen:

```
ppp encrypt mppe auto
```

Statische IP-Adressenzuweisung vom Server

Wenn Sie dem Benutzer eine bestimmte IP-Adresse zuweisen müssen, wählen Sie im ACS User Setup (ACS-Benutzereinrichtung) die Option **Assign static IP Address (Statische IP-Adresse zuweisen) aus,** und füllen Sie die IP-Adresse aus.

Hinzufügen von Zugriffslisten zum Server

Um zu steuern, auf was der PPTP-Benutzer zugreifen kann, wenn der Benutzer mit dem Router verbunden ist, können Sie eine Zugriffsliste auf dem Router konfigurieren. Wenn Sie z. B. den folgenden Befehl ausgeben:

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

und wählen Sie **Filter-ID (Attribut 11)** in ACS aus, und geben Sie **101** in das Feld ein. Der PPTP-Benutzer kann auf den 10.1.1.2-Host zugreifen, aber nicht auf andere. Wenn Sie einen **Befehl show ip interface virtual-access *x*** ausgeben, wobei x eine Zahl ist, die Sie aus dem Befehl **show user** ermitteln können, sollte die Zugriffsliste wie folgt angezeigt werden:

```
Inbound access list is 101
```

Accounting hinzufügen

Sie können mit dem folgenden Befehl Accounting für Sitzungen hinzufügen:

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

Die Accounting-Datensätze in Cisco Secure ACS werden angezeigt, wie in der folgenden Ausgabe gezeigt:

```
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
```

Hinweis: Zur Anzeige wurden dem Beispiel Zeilenumbrüche hinzugefügt. Die Zeilenumbrüche in der tatsächlichen Ausgabe unterscheiden sich von den hier gezeigten.

Split Tunneling

Wenn der PPTP-Tunnel auf dem PC hochgefahren wird, wird der PPTP-Router mit einer höheren Metrik als der vorherige Standard installiert, sodass Sie die Internetverbindung verlieren. Um dies zu beheben, müssen Sie, da das Netzwerk im Router 10.1.1.X ist, eine Batch-Datei (Batch.bat) ausführen, um das Microsoft-Routing so zu ändern, dass die Standardroute gelöscht und die Standardroute neu installiert wird (hierfür ist die IP-Adresse erforderlich, der der PPTP-Client zugewiesen ist). Beispiel: 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
```

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass 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 session**: Zeigt Informationen über den L2F-Protokolltunnel (Active Level 2 Forwarding) und die Meldungskennung in einem Virtual Private Dialup Network (VPDN) an.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

1. **Der PC legt die Verschlüsselung fest, der Router jedoch nicht.**Der PC-Benutzer sieht Folgendes:
   ```
   The remote computer does not support the required data encryption type.
   ```
2. **Sowohl der PC als auch der Router geben die Verschlüsselung an, der RADIUS-Server ist jedoch nicht so konfiguriert, dass er die MPPE-Schlüssel absendet (diese werden normalerweise als Attribut 26 angezeigt).**Der PC-Benutzer sieht Folgendes:
   ```
   The remote computer does not support the required
   data encryption type.
   ```
3. **Der Router gibt die Verschlüsselung an (erforderlich), der PC jedoch nicht (nicht zulässig).**Der PC-Benutzer sieht Folgendes:
   ```
   The specified port is not connected.
   ```
4. **Der Benutzer gibt den falschen Benutzernamen oder das falsche Kennwort ein.**Der PC-Benutzer sieht Folgendes:
   ```
   Access was denied because the username and/or
   password was invalid on the domain.
   ```
   Das Router-**Debugging** zeigt Folgendes an:**Hinweis:** In diesem Beispiel wurden Zeilenumbrüche zu Anzeigezwecken hinzugefügt. Die Zeilenumbrüche in der tatsächlichen Ausgabe unterscheiden sich von den hier gezeigten.
   ```
   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. **Der RADIUS-Server ist nicht kommunikativ.**Der PC-Benutzer sieht Folgendes:
   ```
   Access was denied because the username and/or password
   was invalid on the domain.
   ```
   Das Router-**Debugging** zeigt Folgendes an:**Hinweis:** In diesem Beispiel wurden Zeilenumbrüche zu Anzeigezwecken hinzugefügt. Die Zeilenumbrüche in der tatsächlichen Ausgabe unterscheiden sich von den hier gezeigten.
   ```
   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
   ```

Befehle zur Fehlerbehebung

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**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Wenn Dinge nicht funktionieren, umfassen die minimalen **Debugbefehle** Folgendes:

- **debug aaa authentication**: Zeigt Informationen über die AAA/TACACS+-Authentifizierung an.
- **debug aaa autorization**: Zeigt Informationen zur AAA/TACACS+-Autorisierung an.
- **debug ppp negotiation**: Zeigt PPP-Pakete an, die während des PPP-Starts übertragen werden und über die PPP-Optionen ausgehandelt werden.
- **debug ppp authentication**: Zeigt Authentifizierungsprotokollmeldungen an, die den Austausch von CHAP-Paketen und das Passwort Authentication Protocol (PAP) beinhalten.
- **debug radius**: Zeigt detaillierte Debuginformationen an, die dem RADIUS zugeordnet sind.

Wenn die Authentifizierung funktioniert, aber Probleme mit der MPPE-Verschlüsselung auftreten, verwenden Sie die folgenden Befehle:

- **debug ppp mppe packet**: Zeigt den gesamten ein- und ausgehenden MPPE-Datenverkehr an.
- **debug ppp mppe event**: Zeigt die wichtigsten MPPE-Ereignisse an.
- **debug ppp mppe detail**: Zeigt ausführliche MPPE-Informationen an.
- **debug vpdn l2x-pakete**: Zeigt Meldungen über L2F-Protokollheader und den Status an.
- **debug vpdn events**: Zeigt Meldungen über Ereignisse an, die zum normalen Tunnelaufbau oder -abbruch gehören.
- **debug vpdn errors** (**vpdn-Fehler debuggen**): Zeigt Fehler an, die verhindern, dass ein Tunnel erstellt wird, oder Fehler, die das Schließen eines etablierten Tunnels verursachen.

- **debug vpdn pakete**: Zeigt jedes ausgetauschte Protokollpaket an. Diese Option kann zu einer großen Anzahl von Debug-Meldungen führen, und Sie sollten diesen Befehl in der Regel nur in einem Debuggehäuse mit einer einzigen aktiven Sitzung verwenden.

Sie können diese Befehle auch zur Fehlerbehebung verwenden:

- **clear interface virtual-access *x*** - Schließt einen angegebenen Tunnel und alle Sitzungen im Tunnel.

Beispiel für gute Debugausgabe

Dieses Debuggen zeigt wichtige Ereignisse aus der RFC:

- **SCCRQ** = Start-Control-Connection-Request - Nachrichtencode Bytes 9 und 10 = 0001
- **SCCRP** = Start-Control-Connection-Reply
- **OCRQ** = Outgoing-Call-Request - Nachrichtencode Bytes 9 und 10 = 0007
- **OCRP** = Outgoing Call - Reply

Hinweis: In diesem Beispiel wurden Zeilenumbrüche zu Anzeigezwecken hinzugefügt. Die Zeilenumbrüche in der tatsächlichen Ausgabe unterscheiden sich von den hier gezeigten.

```
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 009C00011A2B3C4D000100000100000000000010000...
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
```

Zugehörige Informationen

- Support-Seite für Cisco Secure ACS für Windows
- Technischer Support und Dokumentation - Cisco Systems