

Configuring Cisco Secure ACS for Windows Router PPTP Authentication

Document ID: 5433

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions
- Network Diagram

Router Configuration

RADIUS Server Fallback Feature

Cisco Secure ACS for Windows Configuration

Adding to the Configuration

- Adding Encryption
- Static IP Address Assignment from Server
- Add Access Lists to the Server
- Add Accounting
- Split Tunneling

Verify

Troubleshoot

- Troubleshooting Commands
- Good debug Output Example

Related Information

Introduction

Point-to-Point Tunnel Protocol (PPTP) support was added to Cisco IOS® Software Release 12.0.5.XE5 on the Cisco 7100 and 7200 platforms (refer to PPTP with Microsoft Point-to-Point Encryption (MPPE) [Cisco IOS Software Release 12.0]). Support for more platforms was added in Cisco IOS Software Release 12.1.5.T (refer to MSCHAP Version 2).

RFC 2637 describes PPTP. In PPTP terms, according to the RFC, the PPTP Access Concentrator (PAC) is the client (the PC, that is, the caller) and the PPTP Network Server (PNS) is the server (the router, the callee).

This document assumes that PPTP connections to the router with local Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) V1 authentication (and optionally MPPE, which requires MS-CHAP V1) have been created with the use of these documents and are already operational. RADIUS is required for MPPE encryption support. TACACS+ works for authentication, but not MPPE keying. MS-CHAP V2 support was added to Cisco IOS Software Release 12.2(2)XB5 and was integrated into Cisco IOS Software Release 12.2(13)T (refer to MSCHAP Version 2), however, MPPE is not supported with MS-CHAP V2 as of yet.

This sample configuration demonstrates how to set up a PC connection to the router (at 10.66.79.99), which then provides user authentication to the Cisco Secure Access Control System (ACS) 4.2 for Windows server (at 10.66.79.120), before you allow the user into the network.

Note: The RADIUS server is not usually outside the router except in a lab environment.

PPTP support was added to Cisco Secure ACS 2.5, but may not work with the router due to Cisco bug ID

CSCds92266 (registered customers only) . ACS 2.6 and later do not have this problem.

Cisco Secure UNIX does not support MPPE. Two other RADIUS applications with MPPE support include Microsoft RADIUS and Funk RADIUS.

Refer to [Configuring the Cisco Router and VPN Clients Using PPTP and MPPE](#) for more information on how to configure PPTP and MPPE with a router.

Refer to [Configuring the VPN 3000 Concentrator and PPTP with Cisco Secure ACS for Windows RADIUS Authentication](#) for more information on how to configure PPTP on a VPN 3000 Concentrator with Cisco Secure ACS for Windows for RADIUS authentication.

Refer to [PIX 6.x: PPTP with Radius Authentication Configuration Example](#) in order to configure PPTP connections to the PIX.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure ACS 4.2 for Windows
- Cisco 3600 router
- Cisco IOS Software Release 12.4(3)

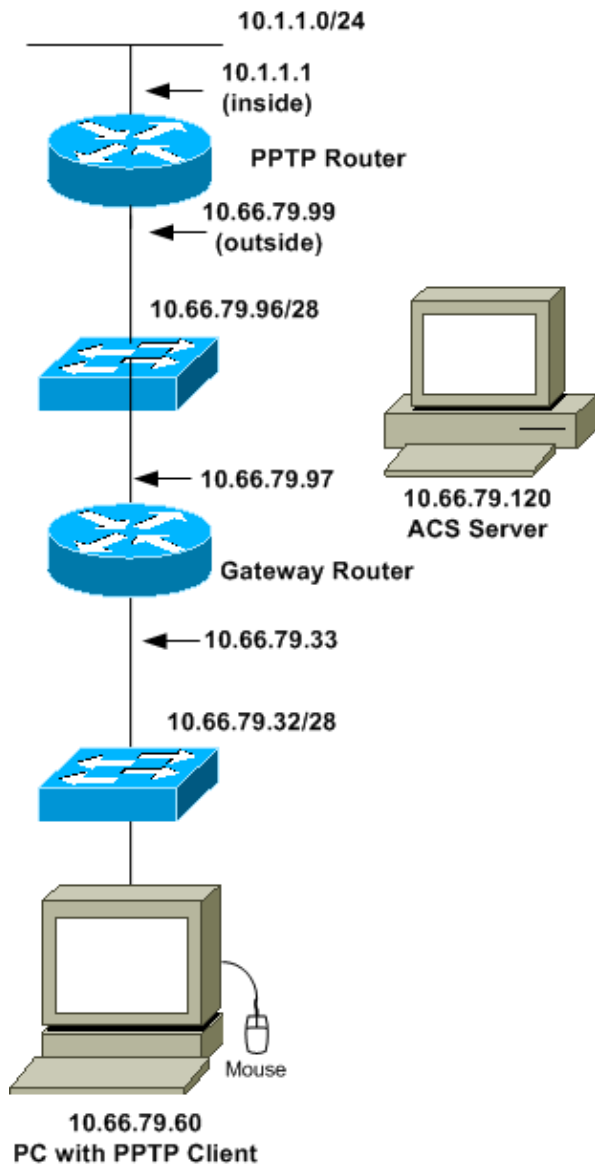
The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are in a live network, ensure that you understand the potential impact of any command before you use it.

Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

Network Diagram

This document uses this network setup:



Router Configuration

Use this router configuration. The user should be able to connect with "**username john password doe**" even if the RADIUS server is unreachable (which is possible if the server was not configured with Cisco Secure ACS yet). This example assumes that local authentication (and, optionally, encryption) is already operational.

Cisco 3600 Router

```
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 Server Fallback Feature

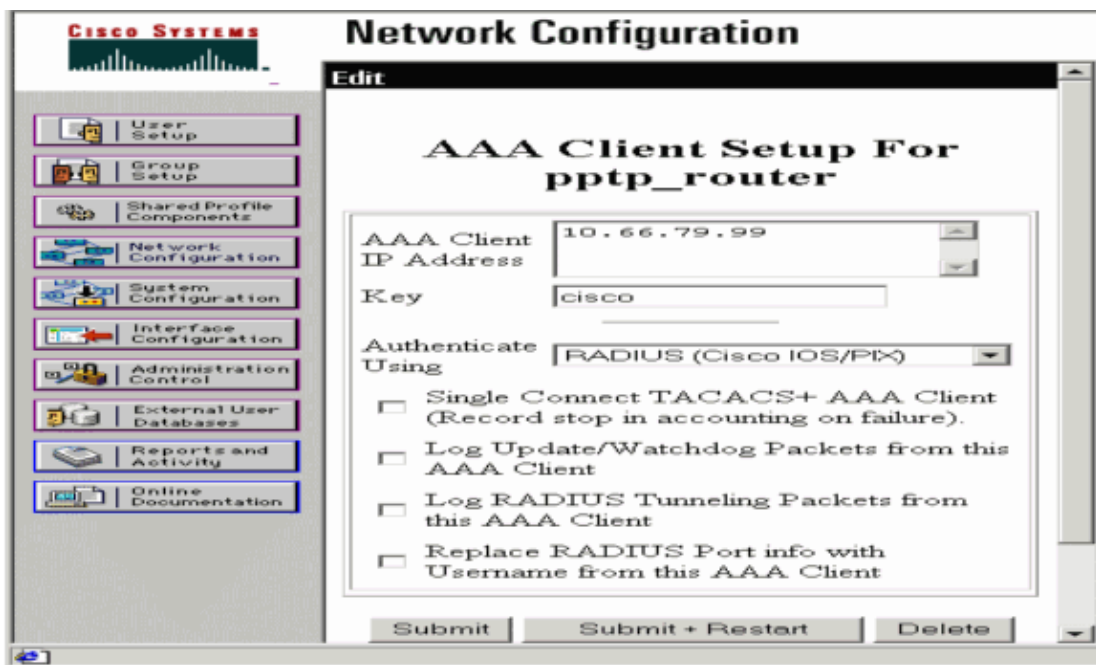
When the primary RADIUS server becomes unavailable, the router will failover to the next active backup RADIUS server. The router will continue to use the secondary RADIUS server forever even if the primary server is available. Usually the primary server is high performance and the preferred server.

In order to set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode.

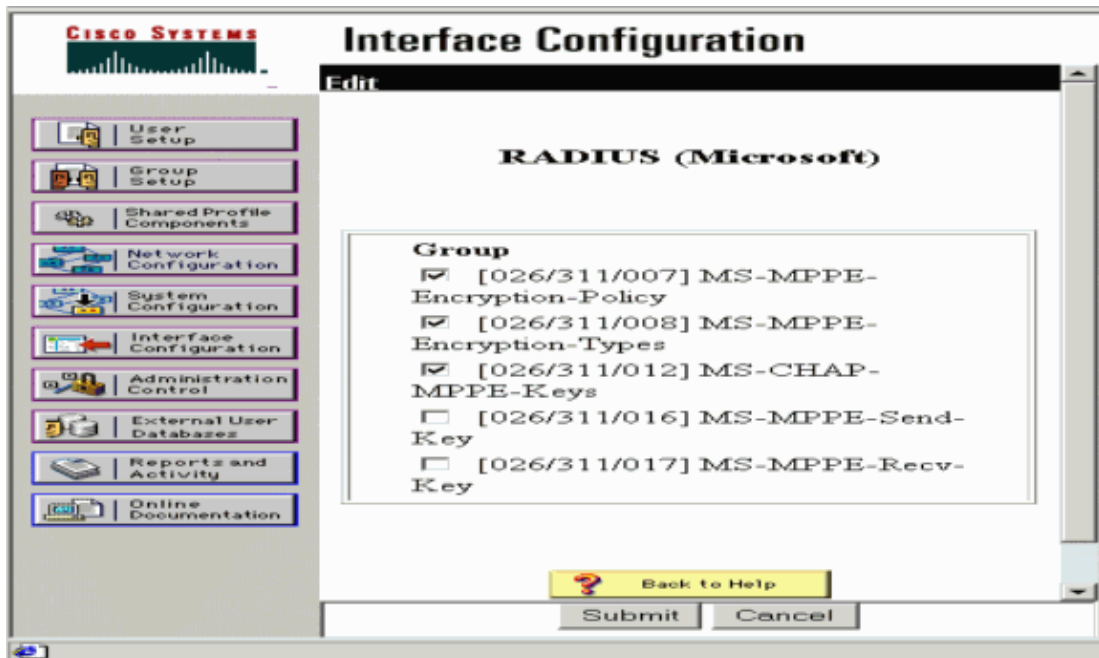
Cisco Secure ACS for Windows Configuration

Use this procedure to configure Cisco Secure ACS:

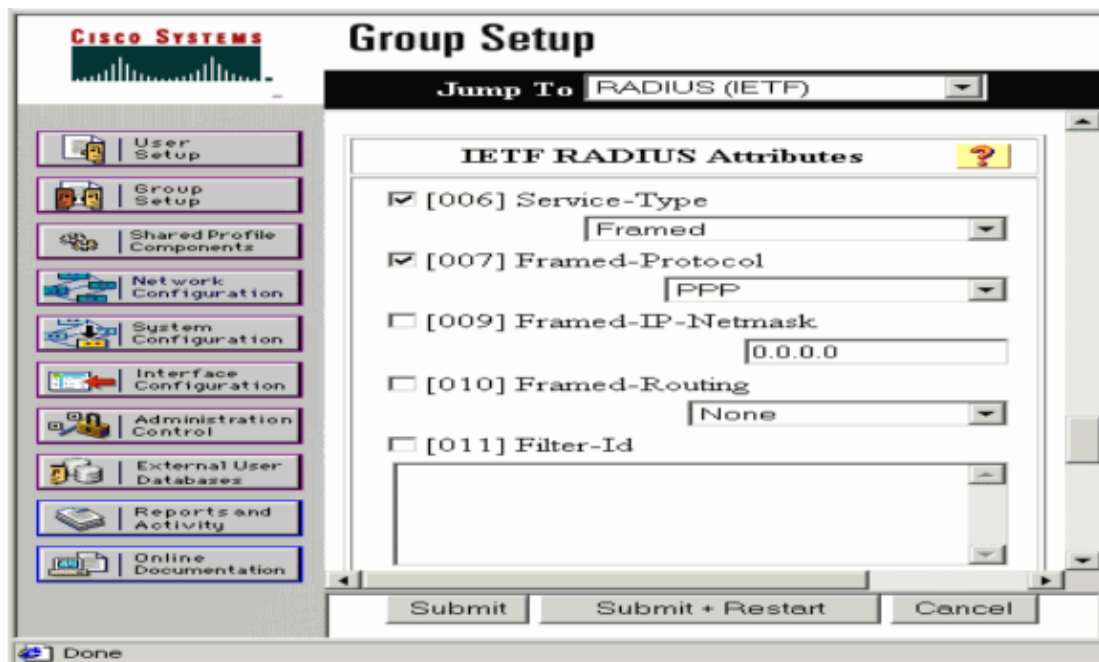
1. Click **Network Configuration**, add an entry for the router, and click **Submit + Restart** when you are finished.



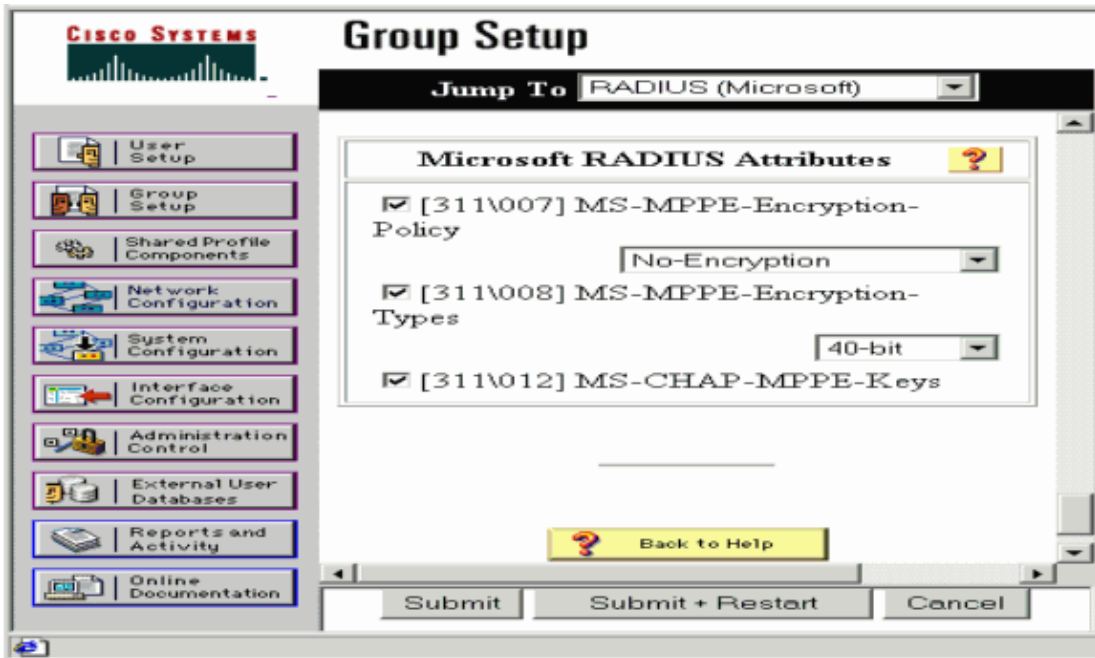
2. Select **Interface Configuration > RADIUS (Microsoft)**, then check your MPPE attributes and click **Submit**.



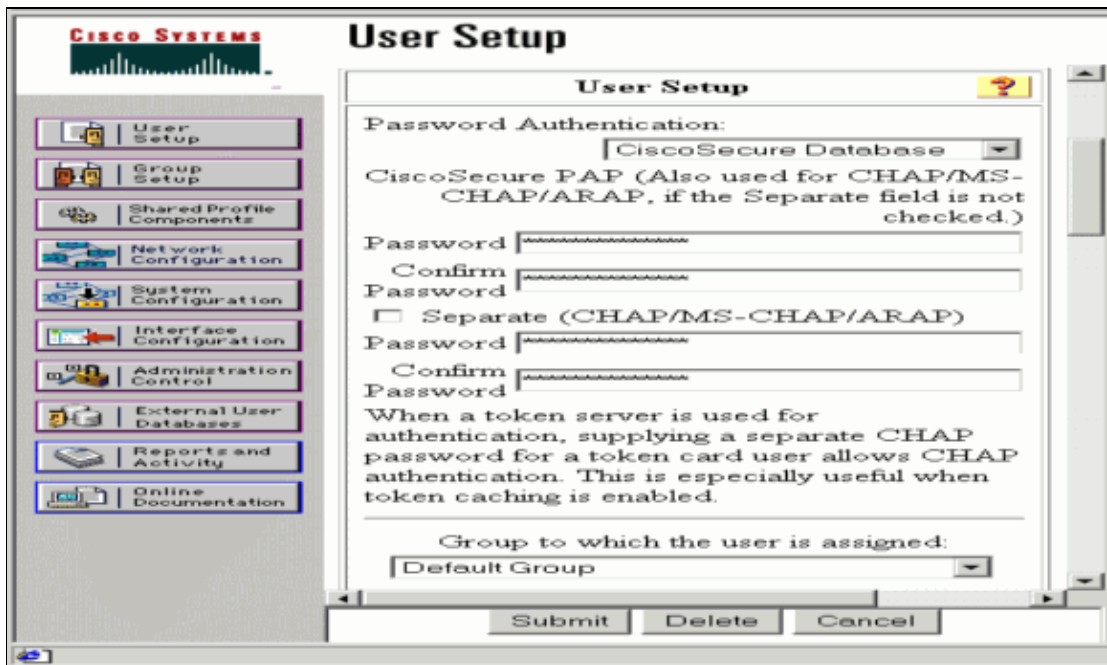
3. Click **Group Setup** and for Service-Type, select **Framed**. For Framed-Protocol, select **PPP** and click **Submit**.



4. In **Group Setup**, check the MS-MPPE RADIUS information and when you are done, click **Submit + Restart**.



5. Click **User Setup**, add a Password, assign the User to the Group and click **Submit**.



6. Test authentication to the router before you add encryption. If authentication does not work, see the Troubleshoot section of this document.

Adding to the Configuration

Adding Encryption

You can add MPPE encryption with this command:

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

Because the example assumes that encryption works with local authentication (username and password on the router), the PC is configured properly. You can now add this command to allow maximum flexibility:

```
ppp encrypt mppe auto
```

Static IP Address Assignment from Server

If you need to assign a particular IP address to the user, in ACS User Setup, select **Assign static IP Address** and fill in the IP address.

Add Access Lists to the Server

In order to control what the PPTP user can access once the user is connected to the router, you can configure an access list on the router. For example, if you issue this command:

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

and choose **Filter-Id (attribute 11)** in ACS and enter **101** in the box, the PPTP user can access the 10.1.1.2 host but not others. When you issue a **show ip interface virtual-access x** command, where *x* is a number that you are able to determine from a **show user** command, the access list should show as applied:

```
Inbound access list is 101
```

Add Accounting

You can add accounting for sessions with this command:

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

Accounting records in Cisco Secure ACS appear as this output shows:

```
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
```

Note: Line breaks were added to the example for display purposes. The line breaks in your actual output are different from those shown here.

Split Tunneling

When the PPTP tunnel comes up on the PC, the PPTP router is installed with a higher metric than the previous default, so you lose Internet connectivity. In order to remedy this, given that the network inside the router is 10.1.1.X, run a batch file (batch.bat) to modify the Microsoft routing to delete the default and reinstall the default route (this requires the IP address the PPTP client is assigned; for the example, that is 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
```

Verify

This section provides information you can use to confirm your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show vpdn session** Displays information about active Level 2 Forwarding (L2F) protocol tunnel and message identifiers in a Virtual Private Dialup Network (VPDN).

```
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
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

1. The PC specifies encryption, but the router does not.

The PC user sees:

```
The remote computer does not support the required data encryption type.
```

2. Both the PC and the router specify encryption, but the RADIUS server is not configured to send down the MPPE keys (these normally appear as attribute 26).

The PC user sees:

```
The remote computer does not support the required
data encryption type.
```

3. The router specifies encryption (required), but the PC does not (not allowed).

The PC user sees:

```
The specified port is not connected.
```

4. The user enters the incorrect username or password.

The PC user sees:

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

The router **debug** shows:

Note: Line breaks were added to this example for display purposes. The line breaks in your actual output are different from those shown here.

```
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. The RADIUS server is uncommunicative.

The PC user sees:

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

The router **debug** shows:

Note: Line breaks were added to this example for display purposes. The line breaks in your actual output are different from those shown here.

```
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
```

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

If things do not work, minimal **debug** commands include:

- **debug aaa authentication** Displays information about AAA/TACACS+ authentication.
- **debug aaa authorization** Displays information on AAA/TACACS+ authorization.
- **debug ppp negotiation** Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.
- **debug ppp authentication** Displays authentication protocol messages, which include CHAP packet exchanges and Password Authentication Protocol (PAP) exchanges.
- **debug radius** Displays detailed debugging information associated with the RADIUS.

If authentication works, but there are problems with MPPE encryption, use these commands:

- **debug ppp mppe packet** Displays all incoming and outgoing MPPE traffic.
- **debug ppp mppe event** Displays key MPPE occurrences.

- **debug ppp mppe detailed** Displays verbose MPPE information.
- **debug vpdn l2x-packets** Displays messages about L2F protocol headers and status.
- **debug vpdn events** Displays messages about events that are part of normal tunnel establishment or shutdown.
- **debug vpdn errors** Displays errors that prevent a tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn packets** Displays each protocol packet exchanged. This option may result in a large number of debug messages, and you should generally only use this command on a debug chassis with a single active session.

You can also use these commands for troubleshooting purposes:

- **clear interface virtual-access x** Shuts down a specified tunnel and all sessions within the tunnel.

Good debug Output Example

This debug shows significant events from the RFC:

- **SCCRQ** = Start-Control-Connection-Request – message code bytes 9 and 10 = 0001
- **SCCRP** = Start-Control-Connection-Reply
- **OCRQ** = Outgoing-Call-Request – message code bytes 9 and 10 = 0007
- **OCRP** = Outgoing-Call-Reply

Note: Line breaks were added to this example for display purposes. The line breaks in your actual output are different from those shown here.

```

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-Templatel
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 CONFREQ [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 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
```

Related Information

- [Cisco Secure ACS for Windows Support Page](#)
 - [Documentation for Cisco Secure ACS for Windows](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 26, 2007

Document ID: 5433
