# Configurazione di Cisco Secure ACS per l'autenticazione PPTP del router Windows

## Sommario



## Introduzione

Il supporto PPTP (Point-to-Point Tunnel Protocol) è stato aggiunto al software Cisco IOS® versione 12.0.5.XE5 sulle piattaforme Cisco 7100 e 7200 (fare riferimento a PPTP con Microsoft Point-to-Point Encryption (MPPE) [software Cisco IOS versione 12.0]). Il supporto per più piattaforme è stato aggiunto nel software Cisco IOS versione 12.1.5.T (fare riferimento alla versione 2 di MSCHAP).

La RFC 2637 descrive PPTP. In termini PPTP, secondo l'RFC, il PPTP Access Concentrator (PAC) è il client (il PC, ovvero il chiamante) e il PPTP Network Server (PNS) è il server (il router, il chiamato).

In questo documento si presume che le connessioni PPTP al router con autenticazione V1 Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) locale (e facoltativamente MPPE, che richiede MS-CHAP V1) siano state create con l'uso di questi documenti e siano già operative. RADIUS è richiesto per il supporto della crittografia MPPE. TACACS+ funziona per l'autenticazione, ma non per la generazione di chiavi MPPE. Il supporto MS-CHAP V2 è stato

aggiunto al software Cisco IOS versione 12.2(2)XB5 ed è stato integrato nel software Cisco IOS versione 12.2(13)T (fare riferimento alla versione 2 di MSCHAP). Tuttavia, MPPE non è ancora supportato con MS-CHAP V2.

In questa configurazione di esempio viene illustrato come configurare una connessione PC al router (versione 10.66.79.99), che quindi fornisce l'autenticazione utente a Cisco Secure Access Control System (ACS) 4.2 per il server Windows (versione 10.66.79.120), prima di consentire l'accesso dell'utente alla rete.

**Nota:** il server RADIUS in genere non si trova all'esterno del router, ad eccezione degli ambienti lab.

Il supporto PPTP è stato aggiunto a Cisco Secure ACS 2.5, ma potrebbe non funzionare con il router a causa dell'ID bug Cisco CSCds92266 (solo utenti registrati). ACS 2.6 e versioni successive non presentano questo problema.

Cisco Secure UNIX non supporta MPPE. Altre due applicazioni RADIUS con supporto MPPE includono Microsoft RADIUS e Funk RADIUS.

Per ulteriori informazioni su come configurare i protocolli PPTP e MPPE con un router, consultare il documento sulla configurazione del router e dei client VPN Cisco con i protocolli PPTP e MPPE.

Per ulteriori informazioni su come configurare PPTP su VPN 3000 Concentrator con Cisco Secure ACS per autenticazione Windows RADIUS, fare riferimento a Configurazione di VPN 3000 Concentrator e PPTP con Cisco Secure ACS per Windows per autenticazione RADIUS.

Per ulteriori informazioni, fare riferimento al documento PIX 6.x: Esempio di configurazione di PPTP con autenticazione Radius per configurare le connessioni PPTP al PIX.

# Prerequisiti

## Requisiti

Non sono previsti prerequisiti specifici per questo documento.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

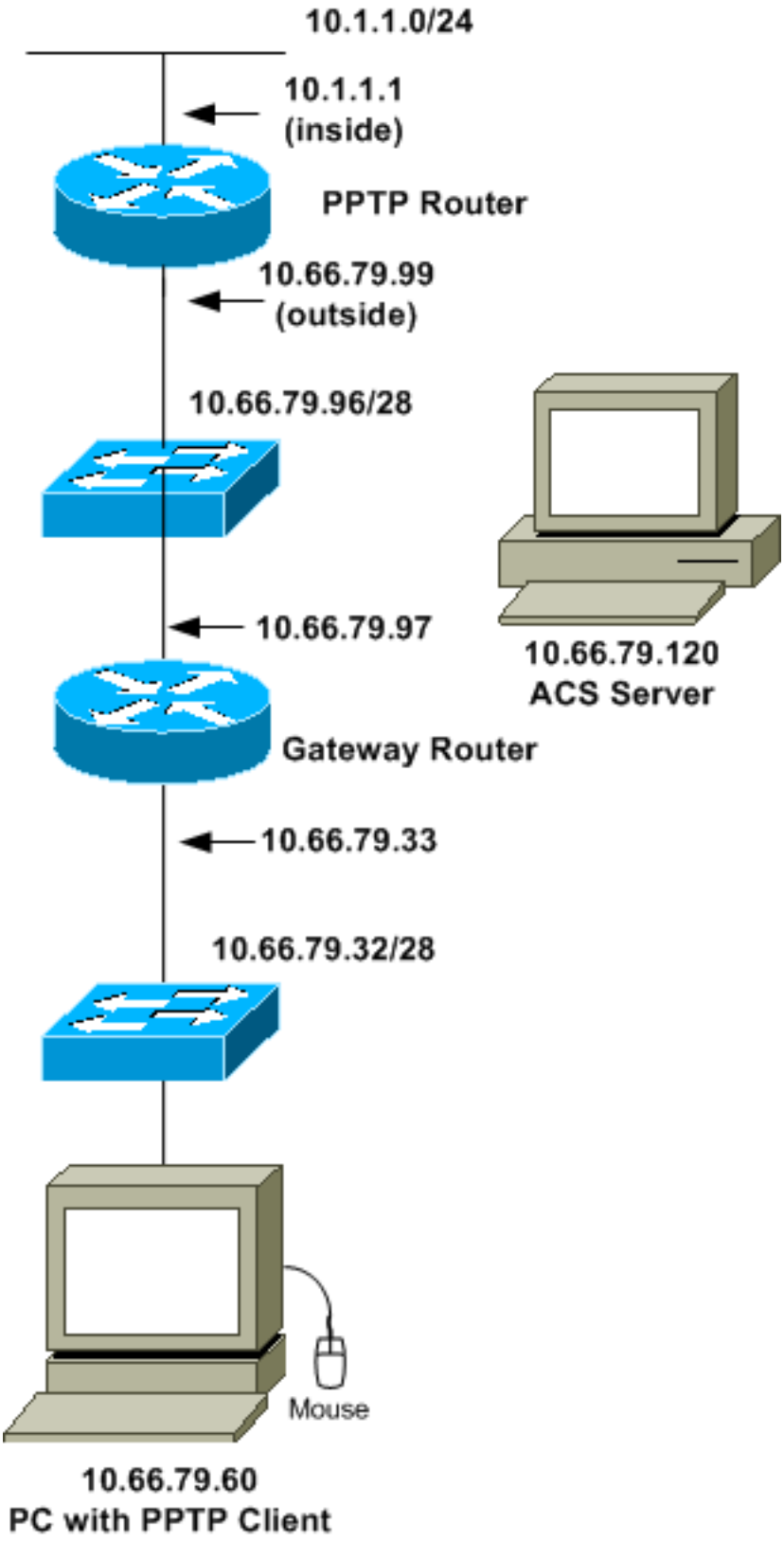
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

## Esempio di rete

Nel documento viene usata questa impostazione di rete:




# Configurazione router

Utilizzare questa configurazione del router. L'utente deve essere in grado di connettersi con "**username john password do**" anche se il server RADIUS non è raggiungibile (ciò è possibile se il server non è stato ancora configurato con Cisco Secure ACS). L'esempio presuppone che l'autenticazione locale (e, facoltativamente, la crittografia) sia già operativa.

**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
```

## Funzione di fallback del server RADIUS

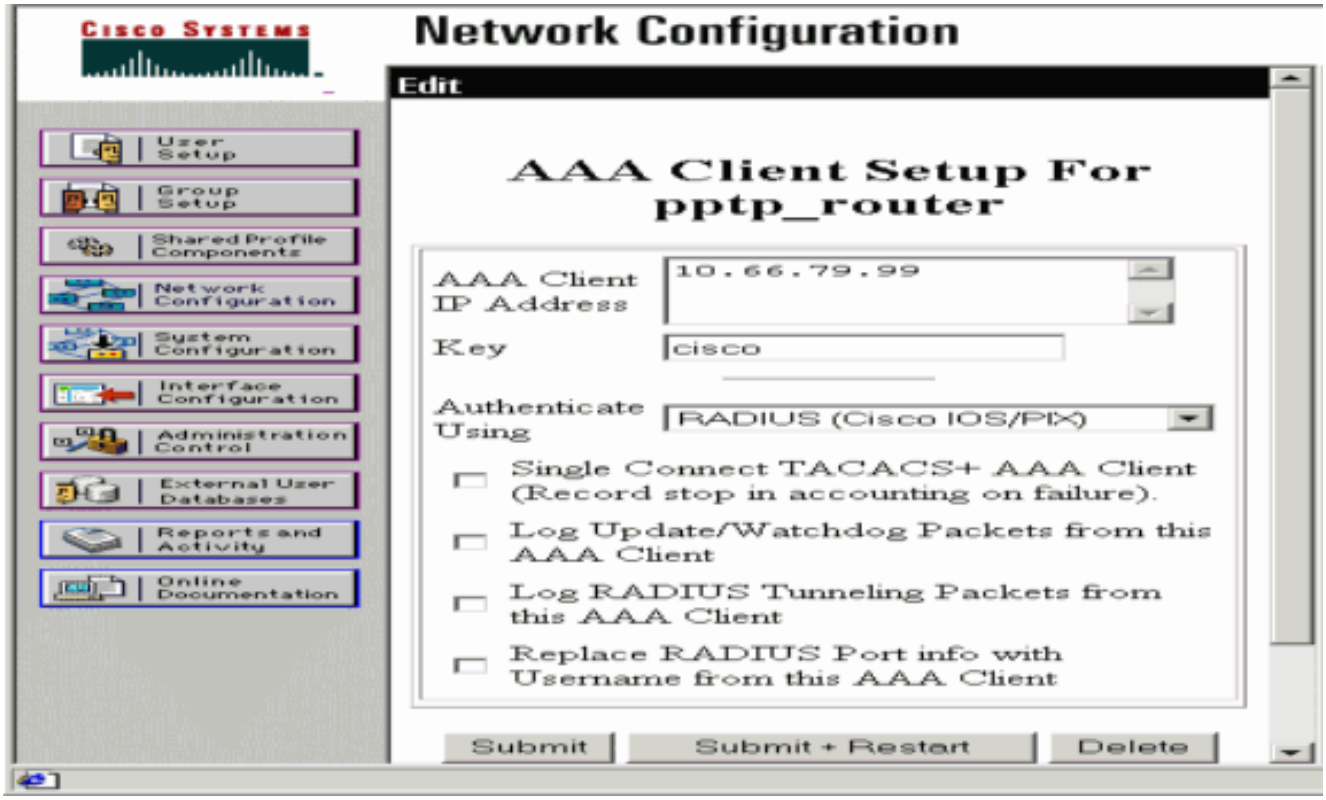
Quando il server RADIUS primario diventa non disponibile, il router eseguirà il failover sul successivo server RADIUS di backup attivo. Il router continuerà a utilizzare il server RADIUS secondario per sempre anche se il server primario è disponibile. In genere, il server principale è il server preferito e offre prestazioni elevate.

Per impostare l'autenticazione di autenticazione, autorizzazione e accounting (AAA) al momento dell'accesso, utilizzare il comando aaa authentication login in modalità di configurazione globale.

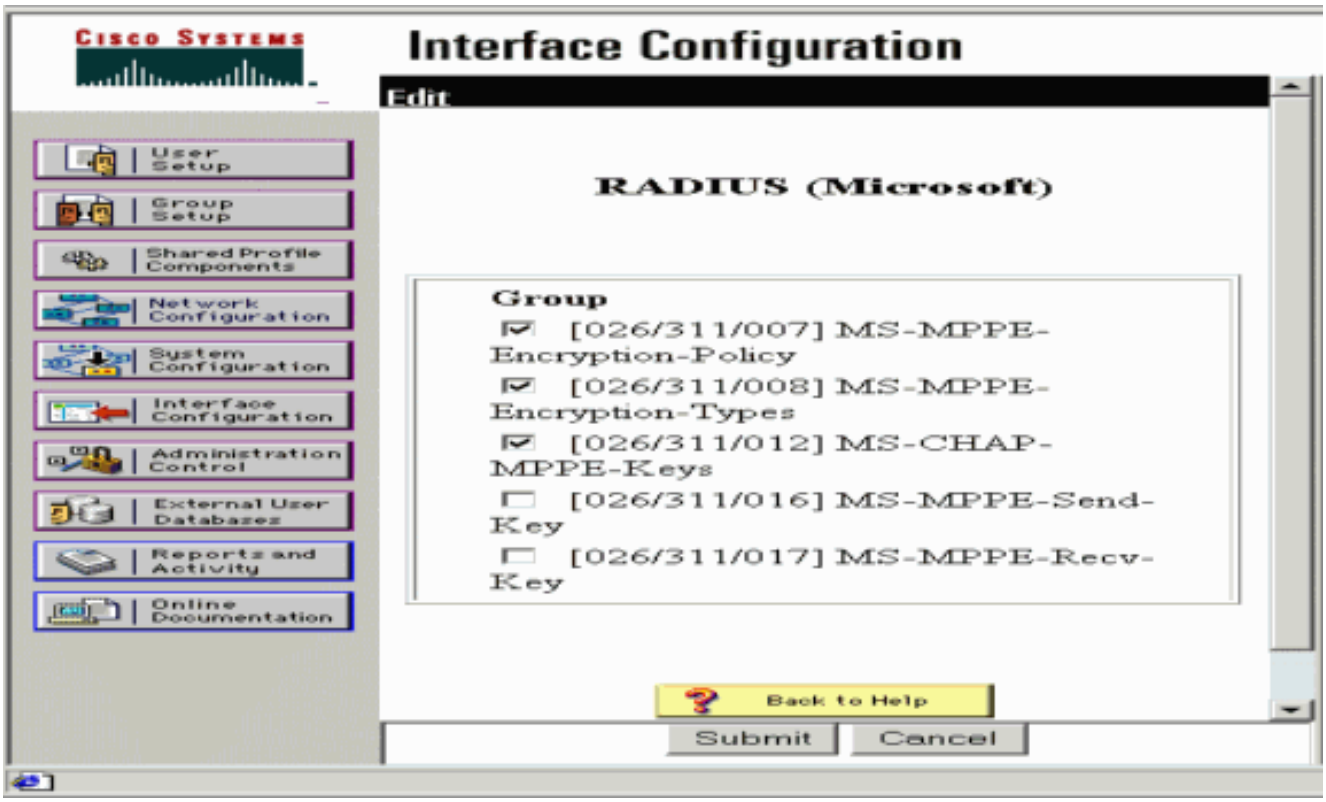
## Configurazione Cisco Secure ACS per Windows

Utilizzare questa procedura per configurare Cisco Secure ACS:

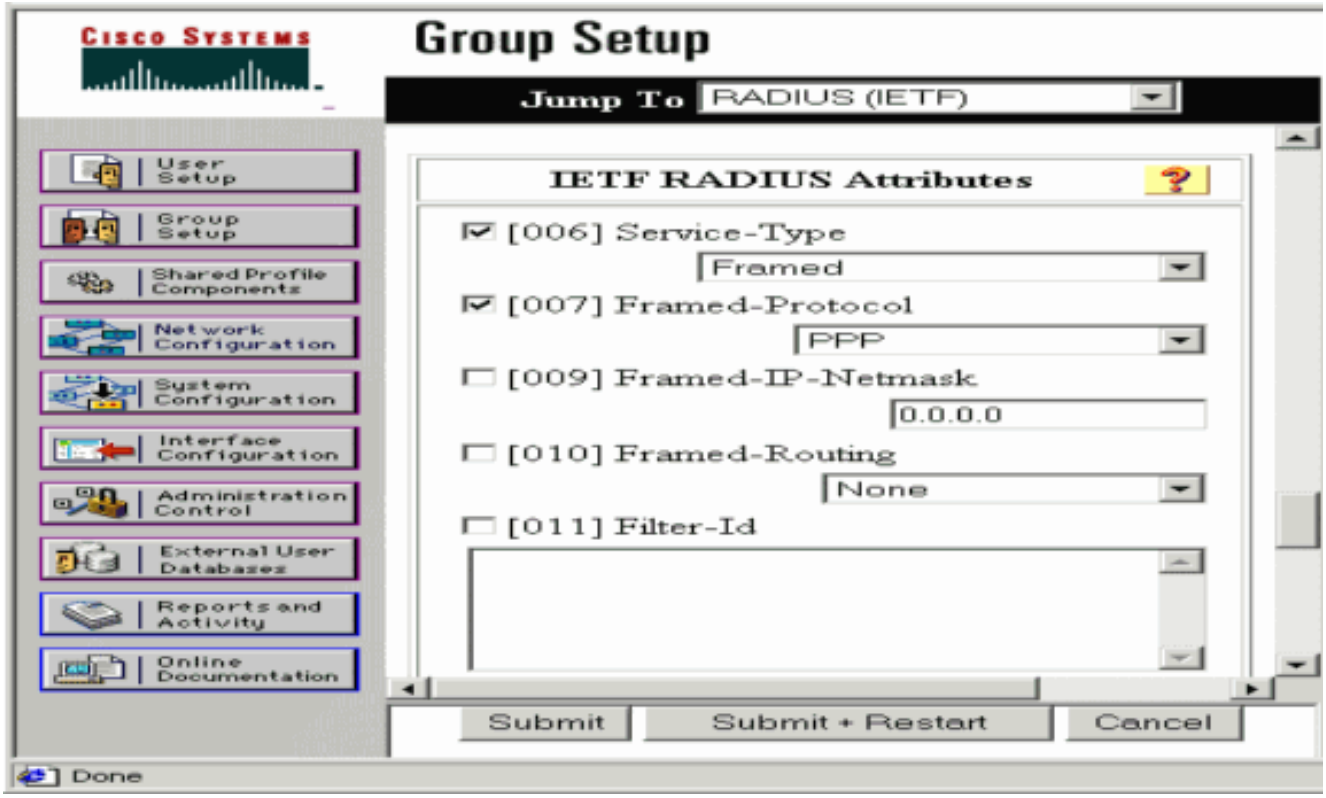
1. Fare clic su **Configurazione di rete**, aggiungere una voce per il router e al termine fare clic su **Invia +**
   **Riavvia**.



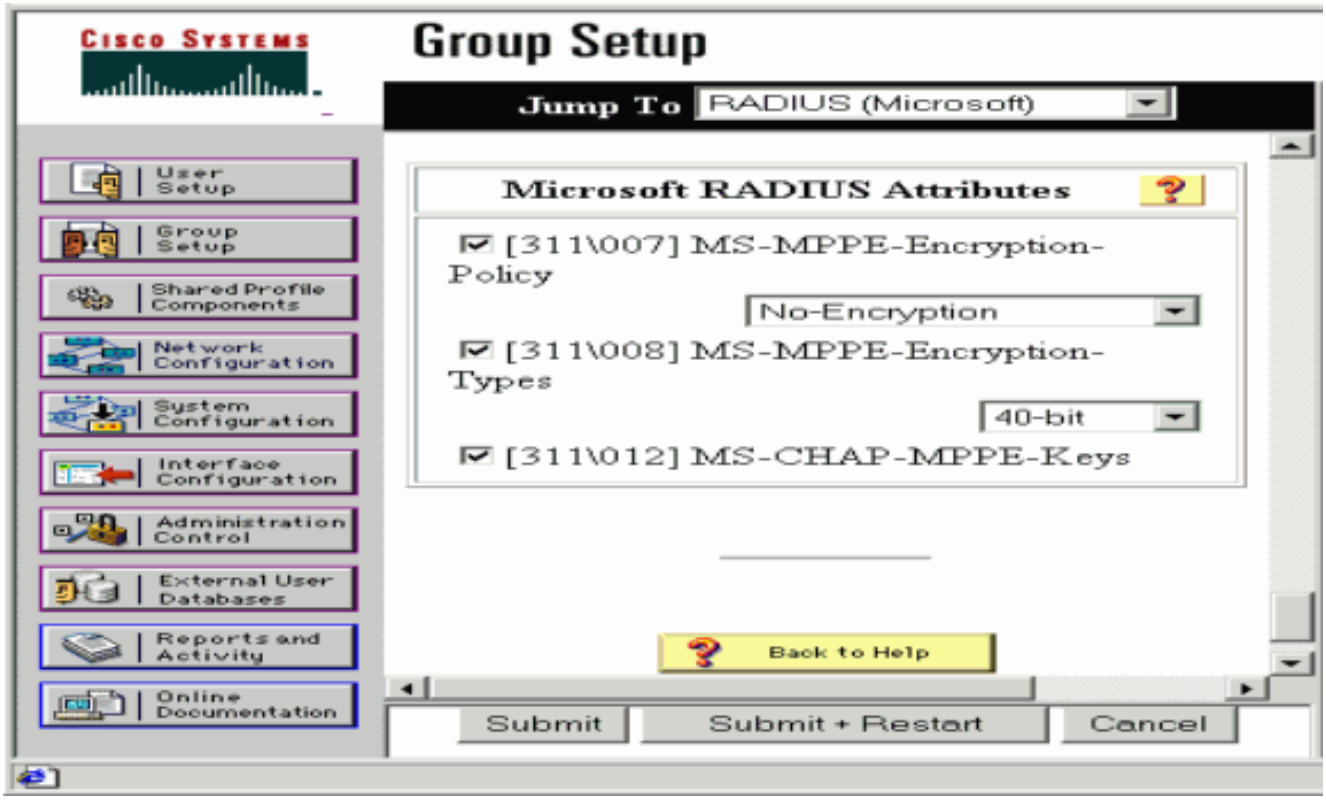

2. Selezionare **Configurazione interfaccia > RADIUS (Microsoft)**, quindi controllare gli attributi MPPE e fare clic su
**Invia**.



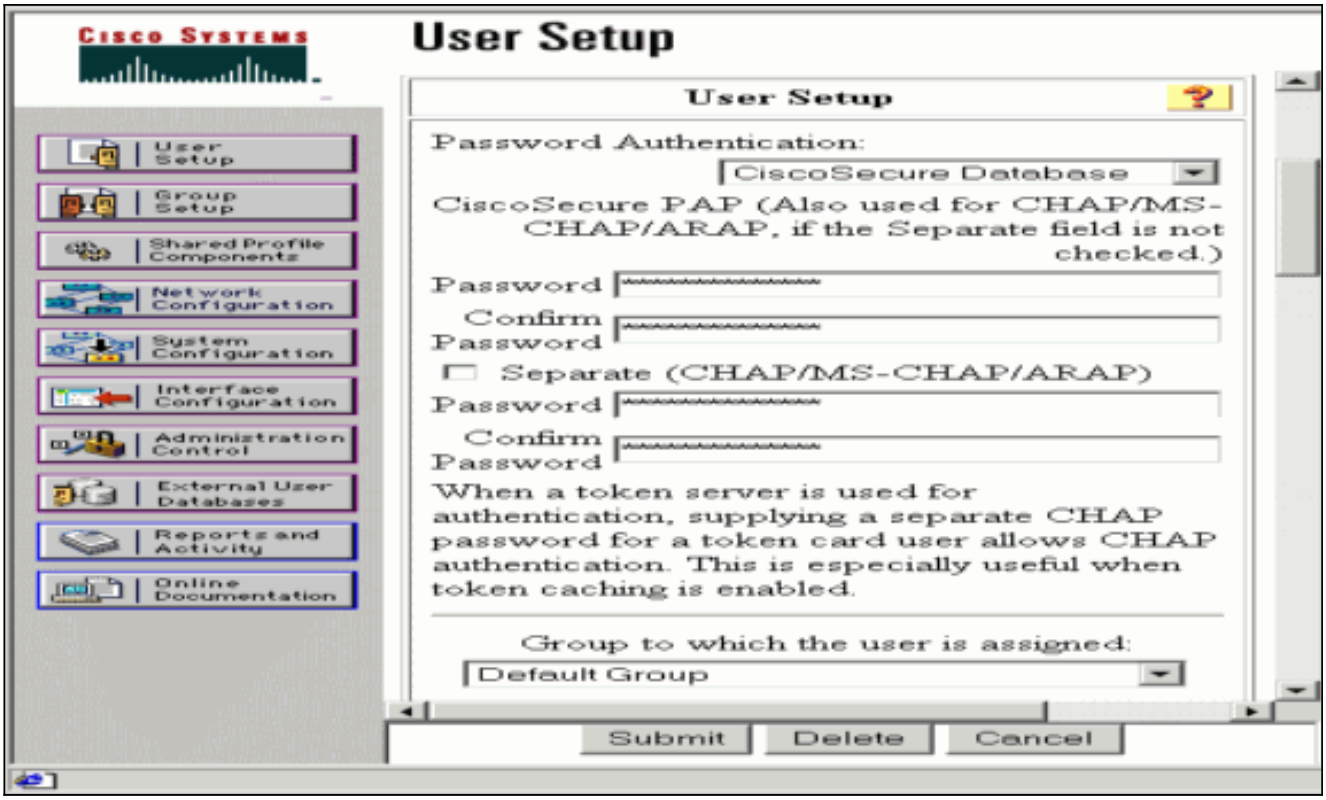

3. Fare clic su **Group Setup** e per Service-Type selezionare **Framed**. Per Protocollo con frame, selezionare **PPP** e fare clic su
**Invia**.




4. In **Configurazione gruppo**, controllare le informazioni MS-MPPE RADIUS e al termine fare clic su **Invia + Riavvia**.




5. Fare clic su **Configurazione utente**, aggiungere una password, assegnare l'utente al gruppo e fare clic su **Invia**.




6. Eseguire il test di autenticazione sul router prima di aggiungere la crittografia. Se l'autenticazione non funziona, consultare la sezione Risoluzione dei problemi in questo documento.

# Aggiunta alla configurazione

## Aggiunta della crittografia

Èpossibile aggiungere la crittografia MPPE con questo comando:

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

Poiché nell'esempio si presume che la crittografia funzioni con l'autenticazione locale (nome utente e password sul router), il PC è configurato correttamente. È ora possibile aggiungere questo comando per consentire la massima flessibilità:

```
ppp encrypt mppe auto
```

## Assegnazione indirizzo IP statico dal server

Se è necessario assegnare un particolare indirizzo IP all'utente, in Configurazione utente ACS selezionare **Assegna indirizzo IP statico** e specificare l'indirizzo IP.

## Aggiungi elenchi di accesso al server

Per controllare gli elementi a cui l'utente PPTP può accedere una volta connesso al router, è possibile configurare un elenco degli accessi sul router. Ad esempio, se si usa questo comando:

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

e scegliere **Filter-Id (attributo 11)** in ACS e immettere **101** nella casella, l'utente PPTP può accedere all'host 10.1.1.2 ma non ad altri. Quando si esegue un comando **show ip interface virtual-access**x, dove *x* è un numero che è possibile determinare da un comando **show user**, l'elenco degli accessi deve essere visualizzato come applicato:

```
Inbound access list is 101
```

## Aggiungi accounting

Èpossibile aggiungere l'accounting per le sessioni con questo comando:

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

I record di accounting in Cisco Secure ACS vengono visualizzati come mostrato nell'output:

```
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
```

**Nota:** Le interruzioni di riga sono state aggiunte all'esempio a scopo di visualizzazione. Le interruzioni di riga nell'output effettivo sono diverse da quelle mostrate di seguito.

## Tunneling ripartito

Quando sul PC viene visualizzato il tunnel PPTP, il router PPTP viene installato con una metrica superiore a quella predefinita, pertanto la connettività Internet viene interrotta. Per risolvere questo problema, poiché la rete all'interno del router è 10.1.1.X, eseguire un file batch (batch.bat) per modificare il routing Microsoft in modo da eliminare il percorso predefinito e reinstallare quello predefinito (è necessario l'indirizzo IP assegnato al client PPTP; ad esempio, 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
```

# Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione

funzioni correttamente.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show vpdn session**: visualizza informazioni sul tunnel del protocollo L2F (Level 2 Forwarding) attivo e sugli identificatori di messaggio in una VPDN (Virtual Private Dialup Network).

```
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
```

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. **Il PC specifica la crittografia, ma il router no.**L'utente del PC vede:
   ```
   The remote computer does not support the required data encryption type.
   ```
2. **Sia il PC che il router specificano la crittografia, ma il server RADIUS non è configurato per l'invio delle chiavi MPPE (normalmente visualizzate come attributo 26).**L'utente del PC vede:
   ```
   The remote computer does not support the required
   data encryption type.
   ```
3. **Il router specifica la crittografia (obbligatoria), ma il PC no (non consentita).**L'utente del PC vede:
   ```
   The specified port is not connected.
   ```
4. **Il nome utente o la password immessi non sono corretti.**L'utente del PC vede:
   ```
   Access was denied because the username and/or
   password was invalid on the domain.
   ```
   Il **debug** del router mostra:**Nota:** sono state aggiunte interruzioni di riga a questo esempio per la visualizzazione. Le interruzioni di riga nell'output effettivo sono diverse da quelle mostrate di seguito.
   ```
   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. **Il server RADIUS non è in grado di comunicare.**L'utente del PC vede:
   ```
   Access was denied because the username and/or password
   was invalid on the domain.
   ```
   Il **debug** del router mostra:**Nota:** sono state aggiunte interruzioni di riga a questo esempio per la visualizzazione. Le interruzioni di riga nell'output effettivo sono diverse da quelle mostrate di seguito.
   ```
   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
   ```

## Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

**Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Se l'operazione non riesce, i comandi di **debug** minimi includono:

- **debug aaa authentication**: visualizza le informazioni sull'autenticazione AAA/TACACS+.
- **debug aaa authorization**: visualizza le informazioni sull'autorizzazione AAA/TACACS+.
- **debug ppp negotiation**: visualizza i pacchetti PPP trasmessi durante l'avvio del protocollo PPP, in cui le opzioni PPP vengono negoziate.
- **debug ppp authentication**: visualizza i messaggi del protocollo di autenticazione, che includono gli scambi di pacchetti CHAP e gli scambi PAP (Password Authentication Protocol).
- **debug radius**: visualizza informazioni di debug dettagliate associate a RADIUS.

Se l'autenticazione funziona ma si verificano problemi con la crittografia MPPE, utilizzare i seguenti comandi:

- **debug ppp mppe packet**: visualizza tutto il traffico MPPE in entrata e in uscita.
- **debug ppp mppe event**: visualizza le occorrenze principali di MPPE.
- **debug ppp mppe detailed**: visualizza informazioni MPPE dettagliate.
- **debug vpdn l2x-packets**: visualizza i messaggi relativi alle intestazioni e allo stato del protocollo L2F.
- **debug vpdn events**: visualizza i messaggi relativi agli eventi che fanno parte della normale creazione del tunnel o del normale arresto.
- **debug vpdn errors**: visualizza gli errori che impediscono di stabilire un tunnel o gli errori che provocano la chiusura di un tunnel stabilito.
- **debug vpdn packets**: visualizza tutti i pacchetti del protocollo scambiati. Questa opzione può generare un numero elevato di messaggi di debug e in genere è consigliabile utilizzare questo comando solo su uno chassis di debug con una singola sessione attiva.

Per la risoluzione dei problemi è inoltre possibile utilizzare i seguenti comandi:

- **clear interface virtual-access *x*: chiude un tunnel specificato e tutte le sessioni all'interno del tunnel.**

## Esempio di output di debug valido

Questo debug mostra gli eventi significativi della RFC:

- **SCCRQ** = Start-Control-Connection-Request - byte del codice messaggio 9 e 10 = 0001
- **SCCRP** = Start-Control-Connection-Reply
- **OCRQ** = Outgoing-Call-Request - byte del codice messaggio 9 e 10 = 0007
- **OCRP** = In uscita-Chiamata-Risposta

**Nota:** sono state aggiunte interruzioni di riga a questo esempio per la visualizzazione. Le interruzioni di riga nell'output effettivo sono diverse da quelle mostrate di seguito.

```
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
00A800011A2B3C4D00070000080007C0E0000012C05F5...
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
```

# Informazioni correlate

- Pagina di supporto di Cisco Secure ACS per Windows
- Documentazione e supporto tecnico – Cisco Systems