

CiscoSecure ACS for Windows とルータの PPTP 認証の設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ネットワーク図](#)

[ルータの設定](#)

[RADIUS サーバ フォールバック機能](#)

[Cisco Secure ACS for Windows の設定](#)

[設定への追加](#)

[暗号化の追加](#)

[サーバからの固定 IP アドレスの割り当て](#)

[サーバへのアクセスリストの追加](#)

[アカウントिंगの追加](#)

[スプリット トンネリング](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[debug の正常な出力例](#)

[関連情報](#)

概要

[Point-to-Point Tunnel Protocol \(PPTP \) のサポートは、Cisco 7100 および 7200 プラットフォーム用の Cisco IOS® ソフトウェア リリース 12.0.5.XE5 で追加されました \(『PPTP with Microsoft Point-to-Point Encryption \(MPPE\)』 \(Cisco IOS ソフトウェア リリース 12.0 \) を参照してください \)](#)。他のプラットフォームでのサポートは、Cisco IOS ソフトウェア リリース 12.1.5.T で追加されました (『[MSCHAP バージョン 2](#)』 を参照してください)。

PPTP については、[RFC 2637](#) を参照してください。RFC によれば、PPTP の用語では、PPTP Access Concentrator (PAC) がクライアント (PC、つまり発信者) で、PPTP Network Server (PNS) がサーバ (ルータ、つまり受信者) です。

このドキュメントでは、ルータへの PPTP 接続がこれらのドキュメントを使用して確立され、すでに動作していることを前提としています。この PPTP 接続には、ローカルの Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP; マイクロソフト チャレンジ ハンドシェイク認証プロトコル) の V1 認証 (およびオプションで MPPE、これには MS-CHAP V1 が必要) が使用されます。MPPE 暗号化サポートには、RADIUS が必要です。TACACS+ は認証用に

動作しますが、MPPE 鍵が動作しません。MS-CHAP V2 サポートは Cisco IOS ソフトウェア リリース 12.2(2)XB5 に追加され、Cisco IOS ソフトウェア リリース 12.2(13)T に統合されました (『[MSCHAP バージョン 2](#)』を参照)。一方、現時点では MS-CHAP V2 ではまだ MPPE はサポートされていません。

この設定例では、ルータ (10.66.79.99) への PC 接続を確立し、Cisco Secure Access Control System (ACS) 4.2 for Windows サーバ (10.66.79.120) に対してユーザを認証してから、ユーザにネットワークへの参加を許可します。

注: RADIUS サーバは通常、ラボ環境を除いては、ルータの Outside にあることはありません。

PPTP のサポートは、Cisco Secure ACS 2.5 に追加されましたが、Cisco bug ID [CSCds92266](#) の問題が原因でルータと連携して動作しないことがあります ([登録ユーザ専用](#))。ACS 2.6 以降ではこの問題は発生しません。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。

Cisco Secure UNIX では MPPE をサポートしていません。MPPE をサポートする他の 2 つの RADIUS アプリケーションには、Microsoft RADIUS と Funk RADIUS があります。

ルータで PPTP および MPPE を設定する方法についての詳細は、『[PPTP および MPPE を使用した Cisco ルータおよび VPN クライアントの設定](#)』を参照してください。

Cisco Secure ACS for Windows を使用する VPN 3000 コンセントレータの PPTP を RADIUS 認証用に設定する方法についての詳細は、『[Cisco Secure ACS for Windows の RADIUS 認証を使用した VPN 3000 コンセントレータの PPTP の設定](#)』を参照してください。

PIX がルータからのダイナミック IPsec 接続を受け入れるシナリオの詳細については、『[ACS 6.x : RADIUS認証 設定例の PPTP](#)』PIX への PPTP 接続を設定するため。

[前提条件](#)

[要件](#)

このドキュメントに関する固有の要件はありません。

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure ACS 4.2 for Windows
- Cisco 3600 ルータ
- Cisco IOS ソフトウェア リリース 12.4(3)

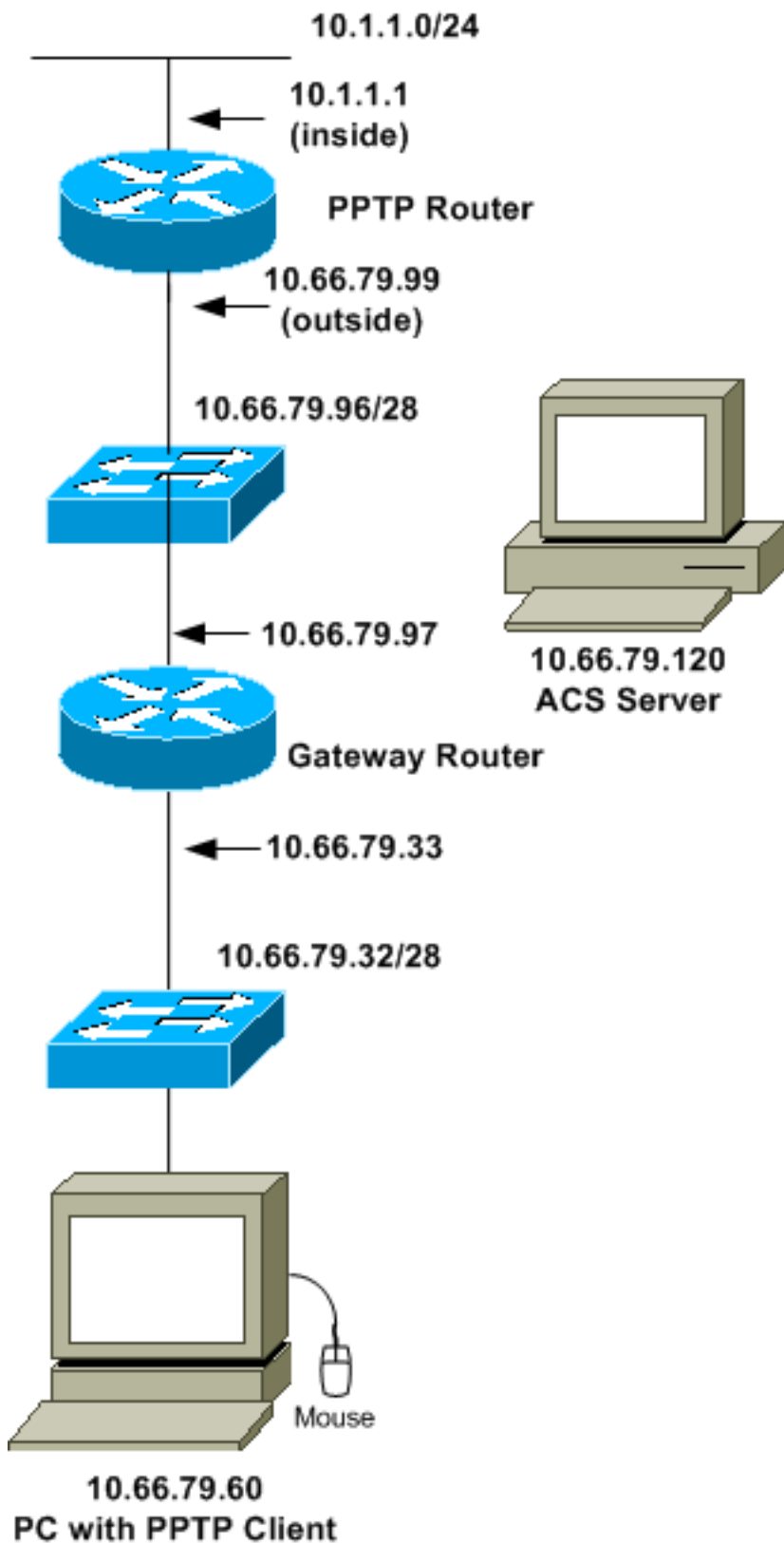
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

[表記法](#)

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



ルータの設定

次のルータ設定を使用します。RADIUS サーバに到達できない場合でも (サーバに Cisco Secure ACS がまだ設定されていないと到達できないことがあります)、ユーザは「ユーザ名 john、パス

ワード `doe`」を使用して接続できる必要があります。この例では、ローカル認証 (およびオプションで暗号化) がすでに動作していることを前提としています。

Cisco 3600 ルータ

```
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 サーバ フォールバック機能

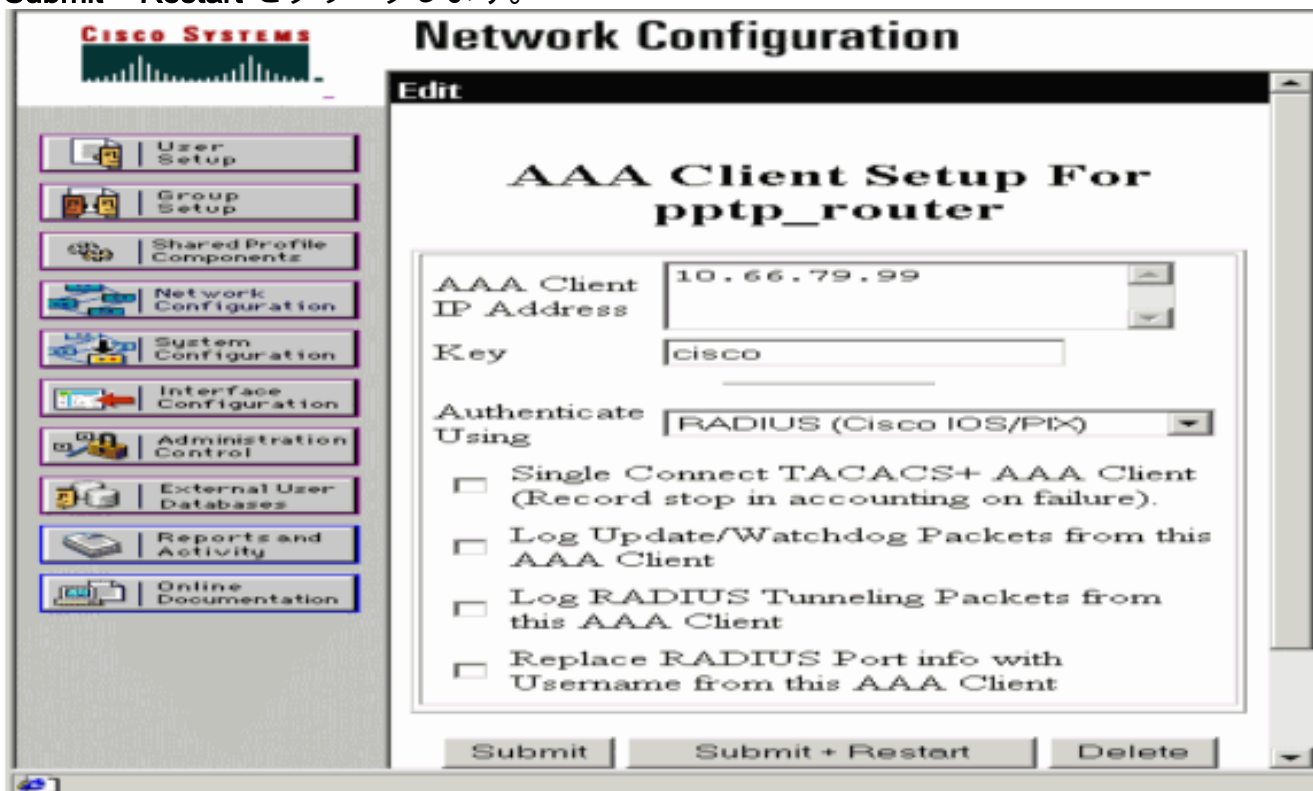
プライマリ RADIUS サーバが使用不能になると、ルータは次にアクティブなバックアップ RADIUS サーバにフェールオーバーします。ルータは、プライマリ サーバが使用可能になっても、永続的にセカンダリ RADIUS サーバを使用し続けます。通常、プライマリ サーバはパフォーマンスが高く、優先サーバとなっています。

ログイン時に Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントイング) 認証を設定するには、グローバル コンフィギュレーション モードで [aaa authentication login](#) コマンドを使用します。

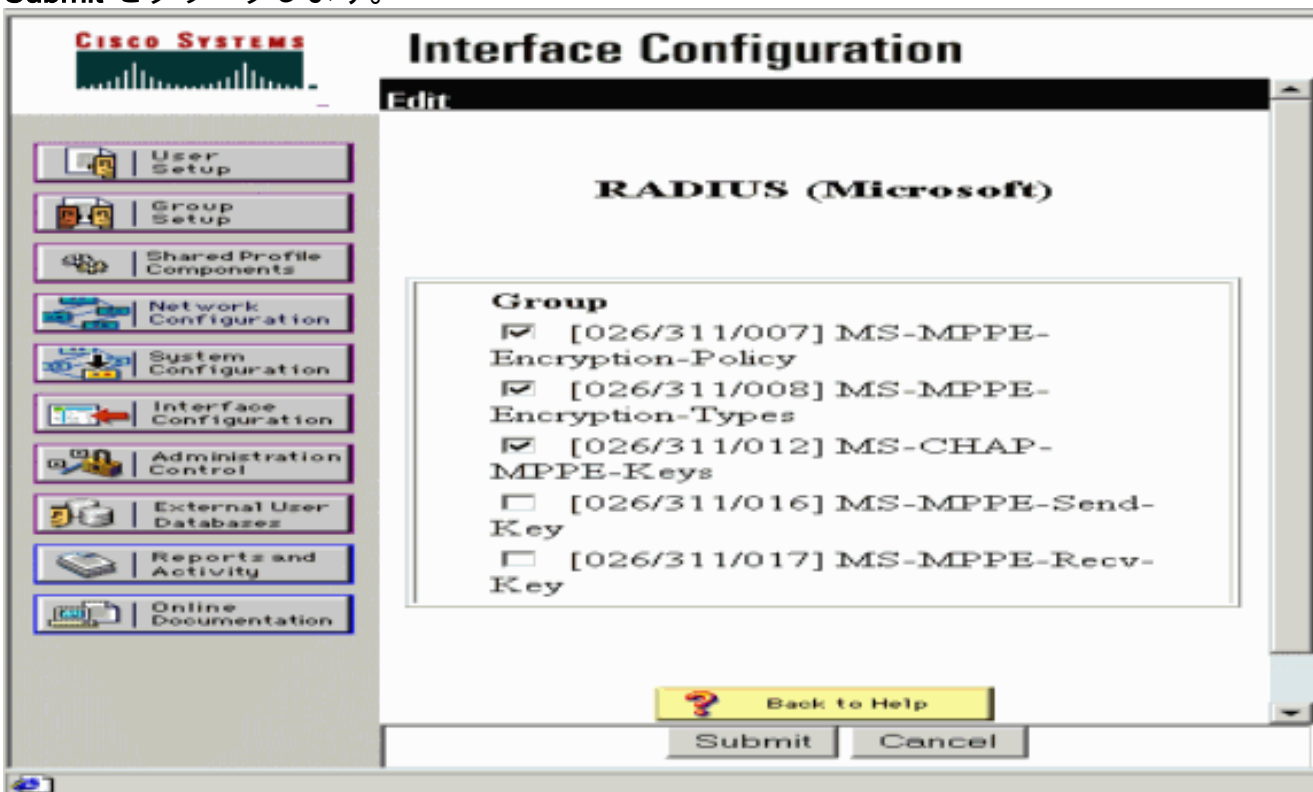
Cisco Secure ACS for Windows の設定

Cisco Secure ACS を設定するには、次の手順に従います。

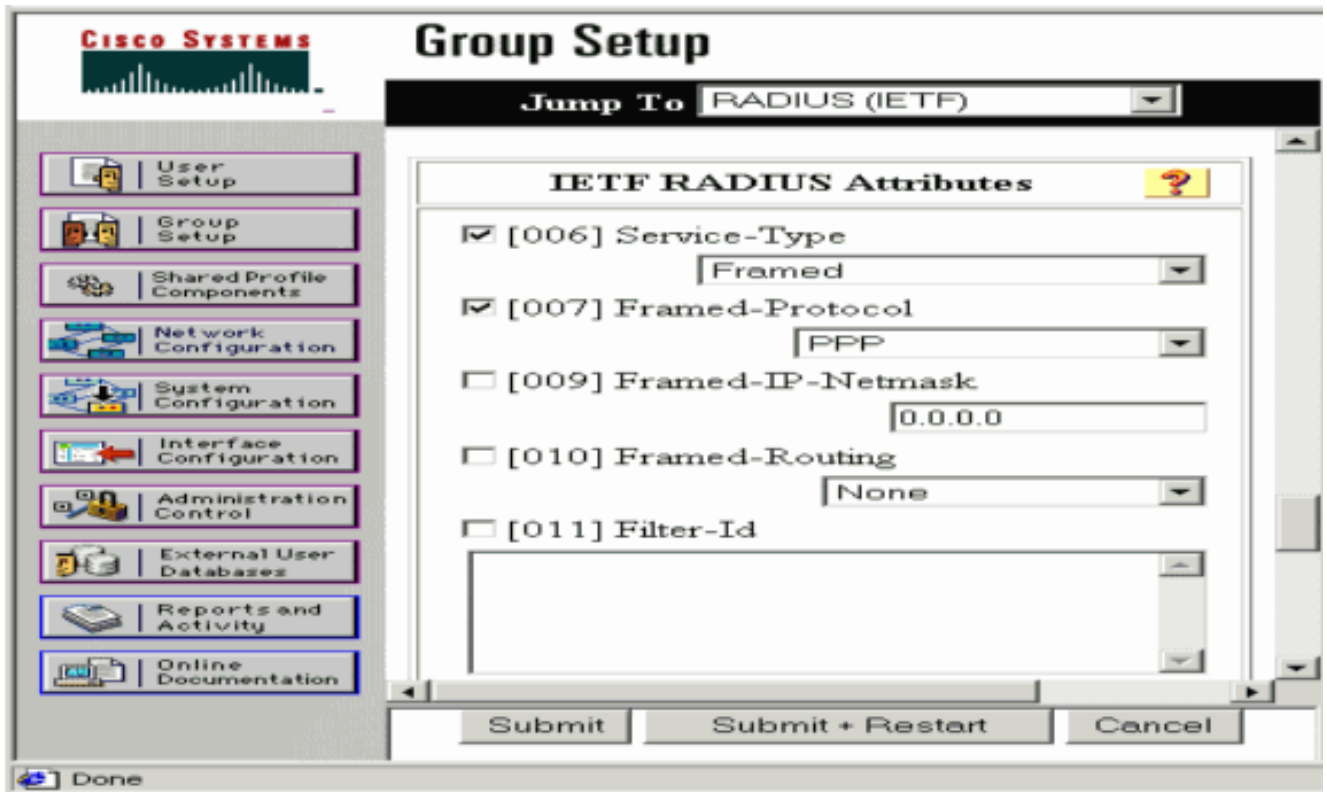
1. Network Configuration をクリックし、ルータのエントリを追加し、作業が終了したら Submit + Restart をクリックします。



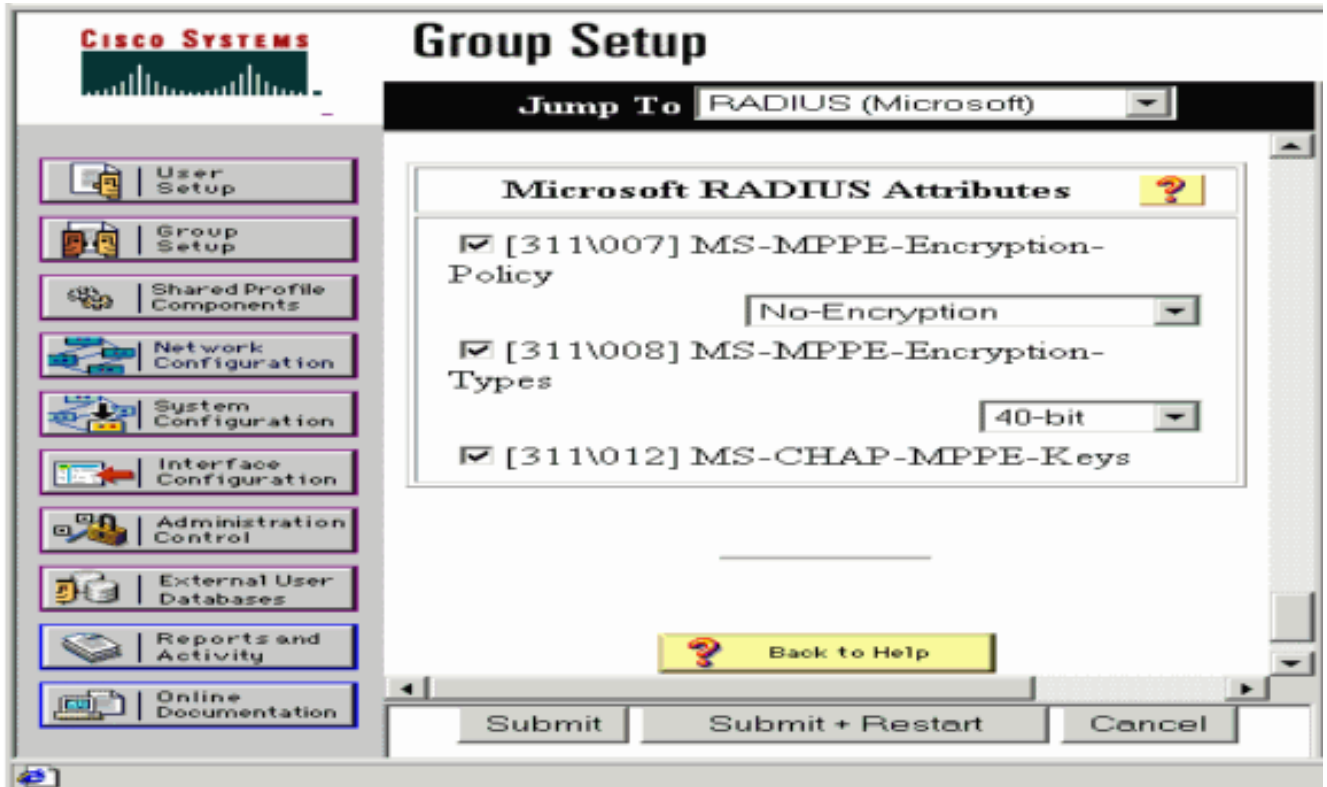
2. Interface Configuration > RADIUS (Microsoft) を選択し、MPPE アトリビュートを確認し、Submit をクリックします。



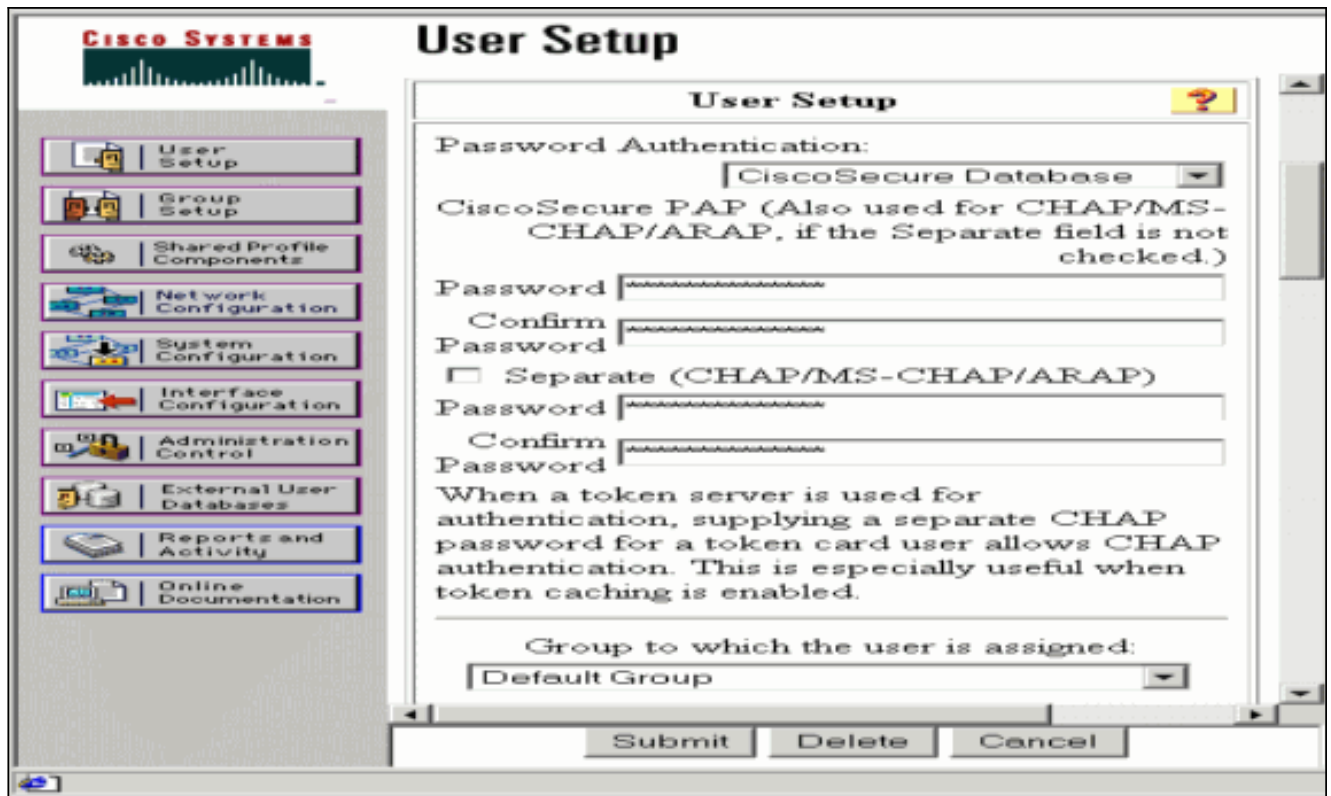
3. Group Setup をクリックし、Service-Type には Framed を選択します。Framed-Protocol には、PPP を選択し、Submit をクリックします。



4. Group Setup で、MS-MPPE RADIUS 情報を確認し、作業が終了したら Submit + Restart をクリックします。



5. User Setup をクリックし、パスワードを追加し、ユーザをグループに割り当ててから、Submit をクリックします。



6. 暗号化を追加する前に、ルータに対する認証をテストします。認証が機能しない場合は、このドキュメント内の「[トラブルシューティング](#)」セクションを参照してください。

設定への追加

暗号化の追加

次のコマンドを使用して、MPPE 暗号化を追加できます。

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

この例では暗号化とローカル認証（ルータでのユーザ名とパスワード）を併用することを想定しているため、PC は正しく設定されています。ここで次のコマンドを追加して、柔軟性を最大限に高めます。

```
ppp encrypt mppe auto
```

サーバからの固定 IP アドレスの割り当て

ユーザに対して特定の IP アドレスを割り当てる必要がある場合は、ACS User Setup で **Assign static IP Address** を選択し、IP アドレスを入力します。

サーバへのアクセス リストの追加

ルータに接続した後に PPTP ユーザがアクセス可能なものを制御するには、ルータにアクセス リストを設定します。たとえば、次のコマンドを実行したとします。

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

この場合、ACS で **Filter-Id (attribute 11)** を選択し、対応するボックスに **101** と入力すると、その

PPTP ユーザは 10.1.1.2 ホストにアクセスできますが、他のホストにはアクセスできなくなります。 `show ip interface virtual-access x` コマンド (`x` は `show user` コマンドで識別できる数値) を発行すると、該当するアクセスリストが表示されます。

```
Inbound access list is 101
```

[アカウントिंगの追加](#)

次のコマンドを使用して、セッションのアカウントングを追加できます。

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

Cisco Secure ACS のアカウントングレコードが次の出力のように表示されます。

```
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
```

注: この例では、表示用に改行が付加されています。実際の出力での改行位置は、この例とは異なります。

[スプリットトンネリング](#)

PPTP トンネルが PC にまで達する場合、PPTP ルータが以前のデフォルトよりも高いメトリックでインストールされます。そのため、インターネットへの接続が失われます。ルータの中のネットワークが 10.1.1.X であることこれを直すことは、与えられて、デフォルトを削除し、デフォルトルートを再インストールするために Microsoft のルーティングを修正するようにバッチファイル (`batch.bat`) を実行します (これは PPTP クライアントが割り当てられる IP アドレスを要求します; 例のために、それは 192.168.1.1) あります:

```
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
```

[確認](#)

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

[Output Interpreter Tool](#) (OIT) ([登録](#) ユーザ専用) では、特定の `show` コマンドがサポートされています。OIT を使用して、`show` コマンド出力の解析を表示できます。

- `show vpdn session` : アクティブな Level 2 Forwarding (L2F; レベル 2 フォワーディング) プロトコル トンネルに関する情報と、Virtual Private Dialup Network (VPDN; バーチャルプライベートダイヤルアップネットワーク) のメッセージ識別子を表示します。

```
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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

1. PC では暗号化が指定されているが、ルータでは指定されていない。PC ユーザには次のように表示されます。The remote computer does not support the required data encryption type.
2. PC とルータでは暗号化が指定されているが、RADIUS サーバでは MPPE 鍵を送信するように設定されていない (通常はアトリビュート 26 として表示される)。PC ユーザには次のように表示されます。The remote computer does not support the required data encryption type.
3. ルータでは暗号化が指定されている (必須) が、PC では指定されていない (許可されていない)。PC ユーザには次のように表示されます。The specified port is not connected.
4. ユーザが誤ったユーザ名またはパスワードを入力した。PC ユーザには次のように表示されます。Access was denied because the username and/or

password was invalid on the domain.ルータの **debug** の出力は次のように表示されます。注: この例では、表示用に改行が付加されています。実際の出力での改行位置は、この例とは異なります。

```
Sep 28 21:34:16.299: RADIUS: Received fromid 21645/13 10.66.79.120:1645,
Access-Reject, len 54
```

```
Sep 28 21:34:16.299: RADIUS: authenticator 37 BA 2B 4F 23 02 44 4D - D4
A0 41 3B 61 2D 5E 0C
```

```
Sep 28 21:34:16.299: RADIUS: Vendor, Microsoft [26] 22
```

```
Sep 28 21:34:16.299: RADIUS: MS-CHAP-ERROR [2] 16
```

```
Sep 28 21:34:16.299: RADIUS: 01 45 3D 36 39 31 20 52 3D 30 20 56 3D
[?E=691 R=0 V=]
```

```
Sep 28 21:34:16.299: RADIUS: Reply-Message [18] 12
```

```
Sep 28 21:34:16.299: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
```

5. RADIUS サーバと通信できない。PC ユーザには次のように表示されます。Access was denied because the username and/or password

was invalid on the domain.ルータの **debug** の出力は次のように表示されます。注: この例では、表示用に改行が付加されています。実際の出力での改行位置は、この例とは異なります。

```
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
```

トラブルシューティングのためのコマンド

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

動作しない場合、**debug** コマンドには、少なくとも次のものがあります。

- **debug aaa authentication** : AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization** : AAA/TACACS+ 許可に関する情報を表示します。
- **debug ppp negotiation** - PPP の開始時に送信される PPP パケットを表示します。PPP の開始時には PPP オプションがネゴシエートされます。
- **debug ppp authentication** : CHAP パケット交換や Password Authentication Protocol (PAP; パスワード認証プロトコル) 交換などの認証プロトコル メッセージを表示します。
- **debug radius** : RADIUS に関連するデバッグの詳細情報を表示します。

認証が動作するものの、MPPE 暗号化に関係する問題がある場合は、次のコマンドを使用します。

- **debug ppp mppe packet** : 着信および発信の MPPE トラフィックを表示します。
- **debug ppp mppe event** : キーとなる MPPE の発生を表示します。
- **debug ppp mppe detailed** : 詳細な MPPE 情報を表示します。
- **debug vpdn l2x-packets** : L2F プロトコル ヘッダーとステータスに関するメッセージを表示します。
- **debug vpdn events** : 通常のトンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。
- **debug vpdn errors** : トンネルの確立を阻害するエラー、または確立されたトンネルをクローズするエラーを表示します。
- **debug vpdn packets** : 交換される各プロトコル パケットを表示します。このオプションにより、大量のデバッグ メッセージが生成される場合があるため、通常はアクティブなセッションが 1 つのみの状態のデバッグ シャーシに対してこのコマンドを実行してください。

また、次のコマンドもトラブルシューティングに使用できます。

- **clear interface virtual-access x** : 指定したトンネルおよびトンネル内のすべてのセッションをシャットダウンします。

[debug の正常な出力例](#)

次に示すデバッグは、RFC からの重要なイベントを表示しています。

- **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

注: この例では、表示用に改行が付加されています。実際の出力での改行位置は、この例とは異なります。

```

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: rcv 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 36 [CISCOACS:00000006] 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 (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 secondary dns Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for secondary wins Sep 28 21:53:22.555: Vi3 IPCP: O CONFREQ [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 (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
```

関連情報

- [Cisco Secure ACS for Windows に関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)