

Настройка конфигурации CiscoSecure ACS для аутентификации протокола PPTP маршрутизатора Windows

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Схема сети](#)

[Настройка маршрутизатора](#)

[Функция нейтрализации сервера RADIUS](#)

[Конфигурация CiscoSecure ACS для Windows](#)

[Добавление к конфигурации](#)

[Добавление шифрования](#)

[Назначение статического IP-адреса с сервера](#)

[Добавьте списки доступа к серверу](#)

[Добавление учета](#)

[Раздельное туннелирование](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Пример выходных данных хорошей отладки](#)

[Дополнительные сведения](#)

Введение

Поддержка протокола туннелирования PPTP была добавлена в выпуске ПО Cisco IOS® 12.0.5. [XE5 на платформах Cisco 7100 и 7200 \(см. описание применения PPTP с средствами шифрования Microsoft для двухточечного соединения \(MPPE\) \[Cisco IOS Software Release 12.0\]\)](#). В выпуске ПО Cisco IOS 12.1.5.T добавлена поддержка ряда дополнительных платформ. ([см. описание версии 2 MSCHAP](#)).

[RFC 2637](#) описывает PPTP. В терминологии PPTP, согласно RFC, концентратор доступа PPTP (PAC) является клиентом (компьютер, то есть вызывающий), а сетевой сервер PPTP (PNS) – сервером (маршрутизатор, вызываемый).

Этот документ предполагает, что подключения PPTP к маршрутизатору с локальным Протоколом Квитирования с аутентификацией Microsoft (MS-CHAP) аутентификация V1 (и дополнительно MPPE, который требует V1 MS-CHAP) была создана с использованием этих

документов и уже в рабочем состоянии. RADIUS требуется для Поддержки шифрования по протоколу MPPE. TACACS + работает для аутентификации, но не кодирования MPPE. Поддержка MS-CHAP V2 была добавлена к Cisco IOS Software Release 12.2 (2) XБ5 и была интегрирована в программное обеспечение Cisco IOS версии 12.2(13)Т (обратитесь к [Версии 2 MSCHAP](#)), однако, MPPE не поддерживается с MS-CHAP V2 на данный момент.

Этот пример конфигурации демонстрирует, как установить Подключение ПК к маршрутизатору (в 10.66.79.99), который тогда предоставляет проверку подлинности пользователя системе управления доступом Cisco Secure Access Control System (ACS) 4.2 для Windows Server (в 10.66.79.120), прежде чем вы позволите пользователю в сеть.

Примечание: Сервер RADIUS обычно не вне маршрутизатора кроме лабораторной среды.

Поддержка PPTP была добавлена к Cisco Secure ACS 2.5, но может не работать с маршрутизатором вследствие к идентификатору ошибки Cisco [CSCds92266 \(только зарегистрированные клиенты\)](#). ACS 2.6 и позже не имеет этой проблемы.

Cisco Secure UNIX не поддерживает MPPE. Два других Приложения RADIUS с Поддержкой MPPE включают Microsoft RADIUS и Funk RADIUS.

См. [Настройку маршрутизатор Cisco и Клиенты VPN Использование PPTP и MPPE](#) для получения дополнительной информации о том, как настроить PPTP и MPPE с маршрутизатором.

См. [Настройку VPN 3000 Concentrator и PPTP с Cisco Secure ACS для Аутентификации Windows RADIUS](#) для получения дополнительной информации о том, как настроить PPTP на VPN 3000 Concentrator с Cisco Secure ACS для Windows для Проверки подлинности RADIUS.

[См. документ PIX 6.x: PPTP с Примером настройки аутентификации RADIUS](#) для настройки подключений PPTP к PIX.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Secure ACS 4.2 для Windows
- Маршрутизатор Cisco 3600
- ПО Cisco IOS версии 12.4.3

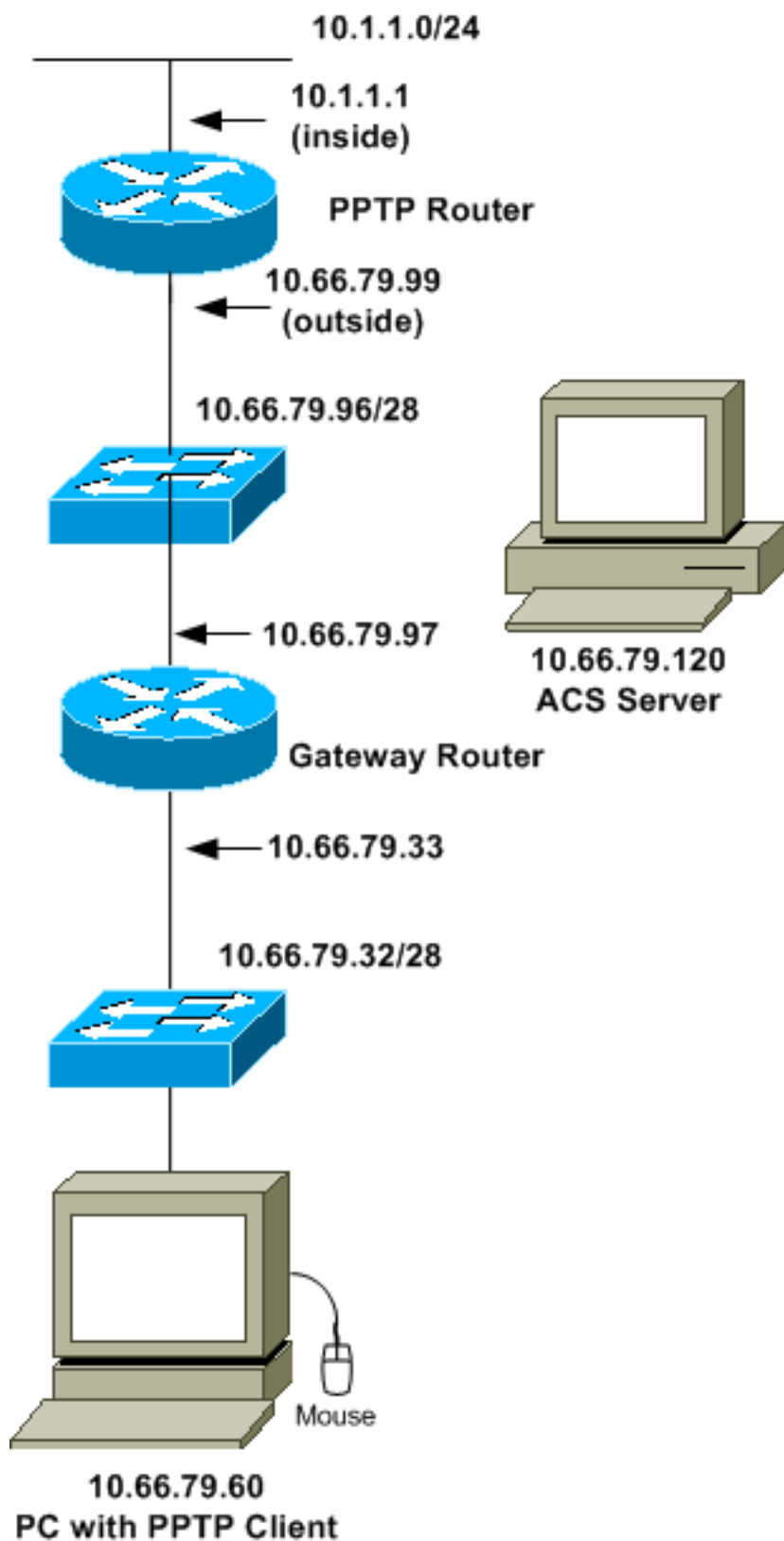
Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если вы находитесь в действующей сети, гарантируете понимание потенциального воздействия любой команды перед использованием его.

Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

Схема сети

В настоящем документе используется следующая схема сети:



Настройка маршрутизатора

Используйте эту конфигурацию маршрутизатора. Пользователь должен быть в состоянии соединиться с "самкой пароля пользователя John", даже если сервер RADIUS недостижим (который возможен, если сервер еще не был настроен с Cisco Secure ACS). Данный пример предполагает, что локальная проверка подлинности (и, дополнительно, шифрование) уже в рабочем состоянии.

Маршрутизатор Cisco 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
```

Функция нейтрализации сервера RADIUS

Если основной сервер RADIUS станет недоступным, маршрутизатор произведет аварийное переключение на следующий активный резервный сервер RADIUS. Маршрутизатор продолжит использовать вторичный сервер RADIUS и далее, даже если первичный сервер вновь станет доступен. Обычно в качестве первичного выбирается мощный и наиболее предпочтительный сервер.

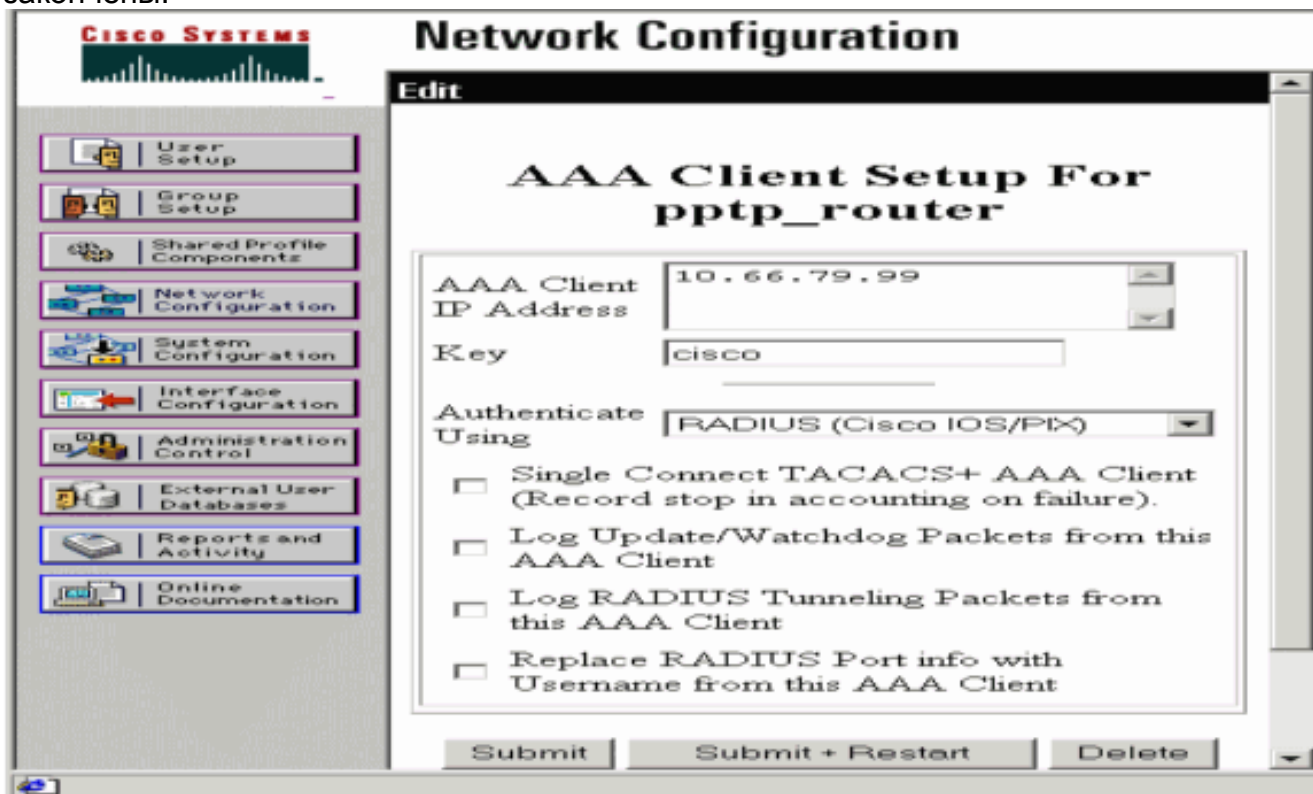
Для установки аутентификации аутентификации, авторизации и учета (AAA) при входе в

систему используйте [команду aaa authentication login](#) в режиме глобальной конфигурации.

Конфигурация CiscoSecure ACS для Windows

Используйте эту процедуру для настройки Cisco Secure ACS:

1. Нажмите **Network Configuration**, добавьте запись для маршрутизатора и нажмите **Submit + Перезапуск**, когда вы будете закончены.

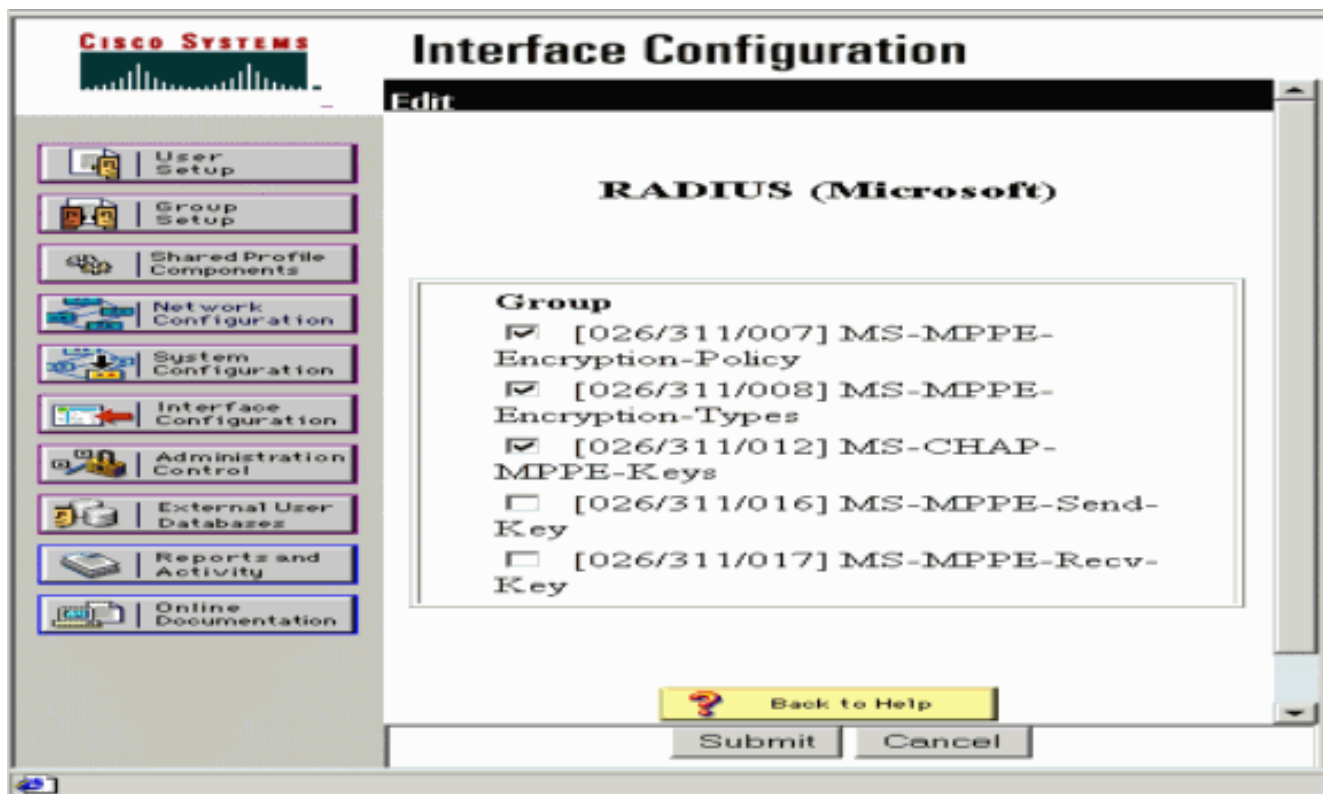


The screenshot shows the Cisco Secure ACS web interface. The main title is "Network Configuration" and the sub-title is "AAA Client Setup For ptp_router". The interface includes a left-hand navigation menu with options like "User Setup", "Group Setup", "Shared Profile Components", "Network Configuration", "System Configuration", "Interface Configuration", "Administration Control", "External User Databases", "Reports and Activity", and "Online Documentation". The main content area contains the following fields and options:

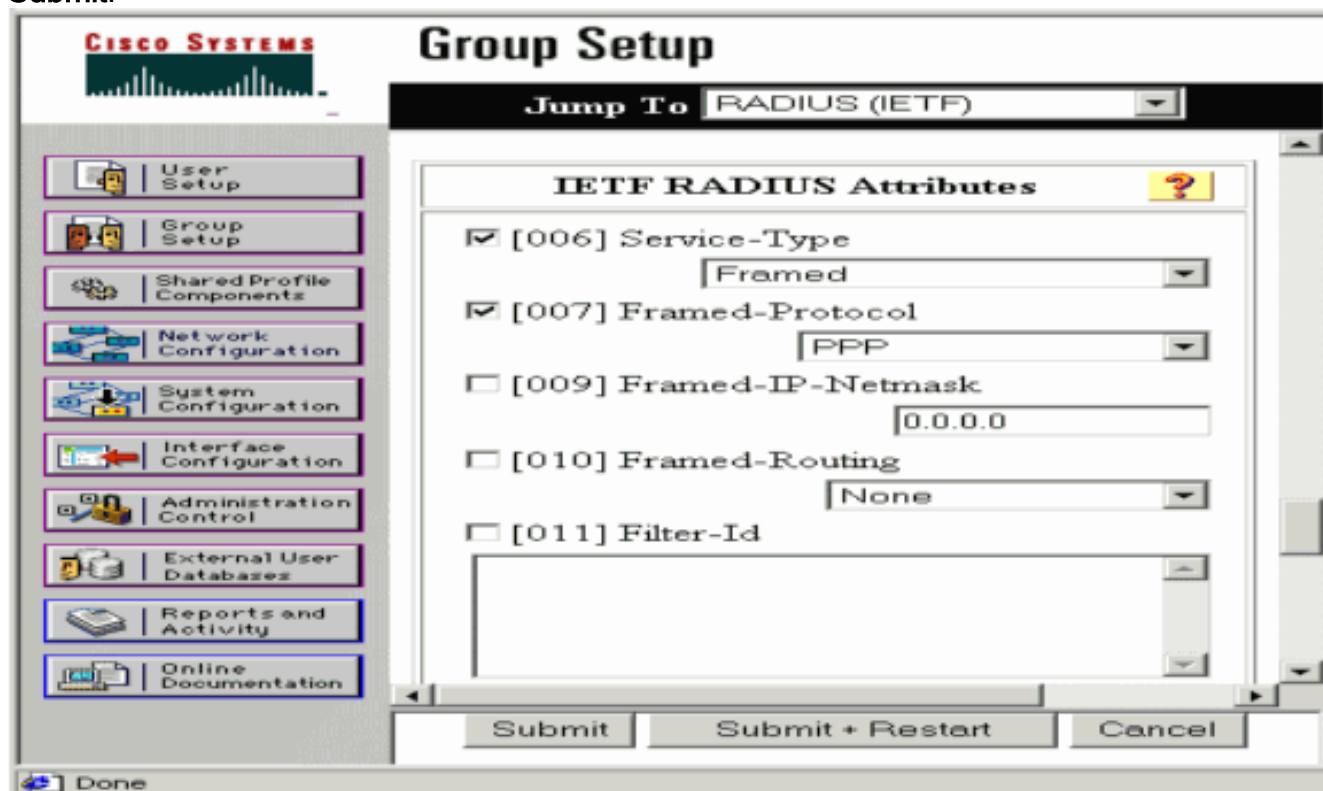
- AAA Client IP Address: 10.66.79.99
- Key: cisco
- Authenticate Using: RADIUS (Cisco IOS/PK)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

At the bottom of the form are three buttons: "Submit", "Submit + Restart", and "Delete".

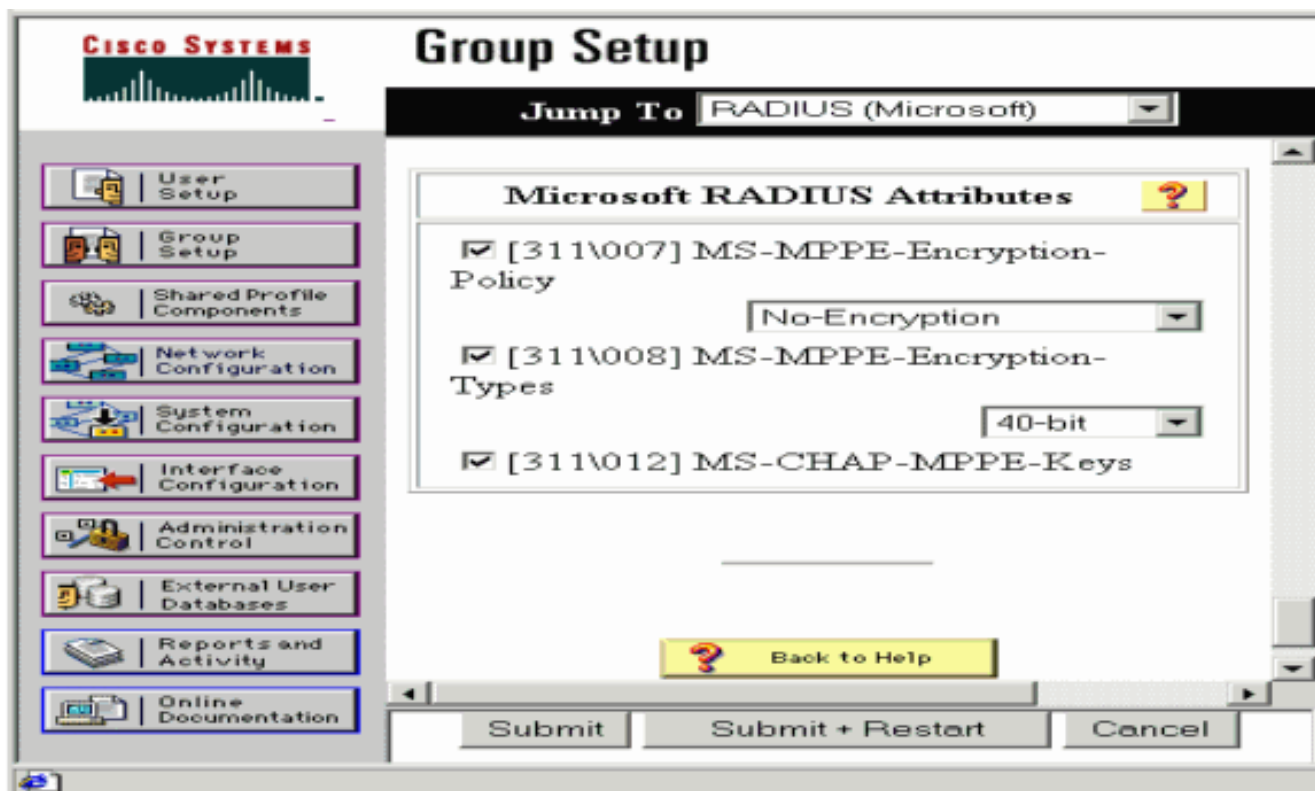
2. Выберите **Interface Configuration > RADIUS (Microsoft)**, затем проверьте свои Атрибуты MPPE и нажмите **Submit**.



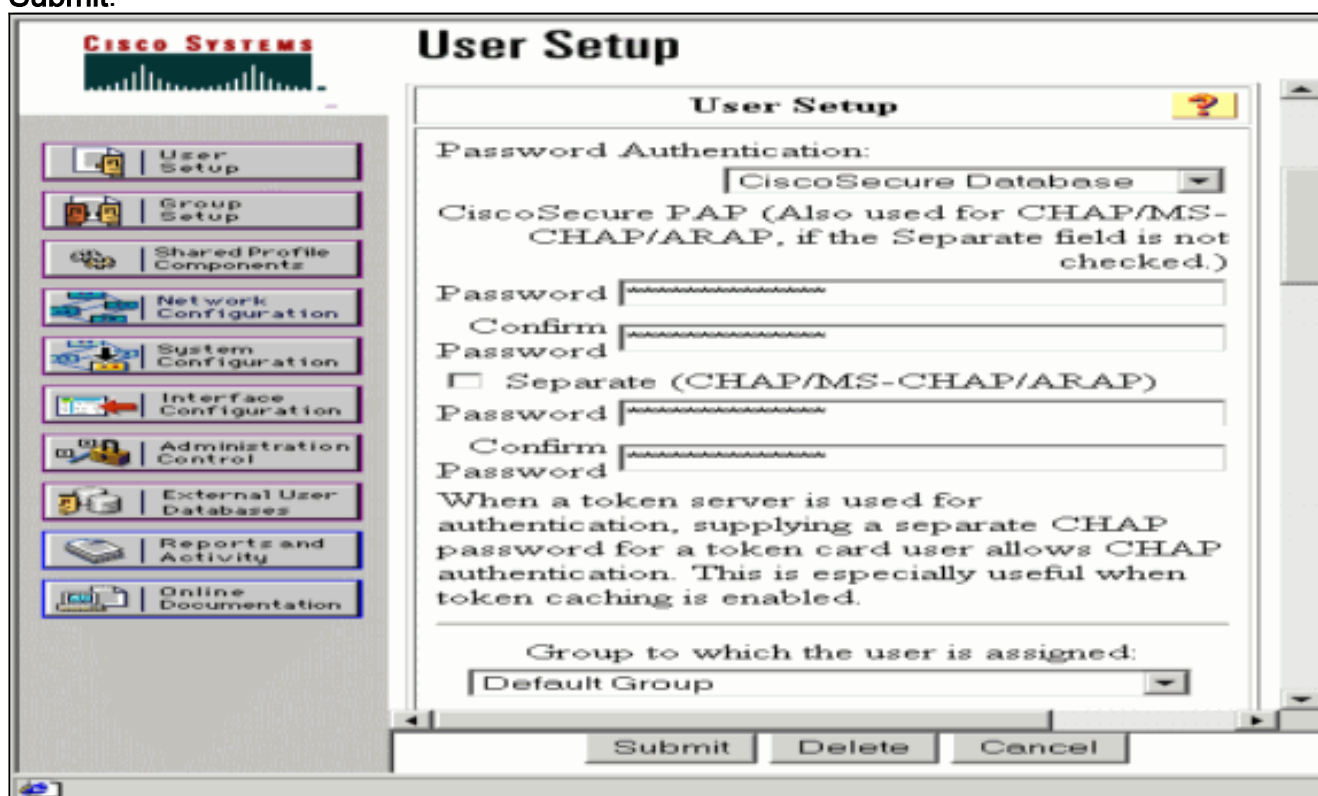
3. Нажмите **Group Setup** и для Service-Type, выберите **Framed**. Для кадрованного протокола выберите **PPP** и нажмите **Submit**.



4. В **Настройке групп** проверьте Данные RADIUS MS-MPPE и когда вы сделаны, нажмите **Submit + Перезапуск**.



5. Нажмите **User Setup**, добавьте Пароль, назначьте Пользователя на Группу и нажмите **Submit**.



6. Тестовая аутентификация к маршрутизатору перед добавлением шифрования. Если аутентификация не работает, посмотрите раздел [Устранения неполадок](#) этого документа.

[Добавление к конфигурации](#)

[Добавление шифрования](#)

Можно добавить шифрование MPPE с этой командой:

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

Поскольку пример предполагает, что шифрование работает с локальной проверкой подлинности (имя пользователя и пароль на маршрутизаторе), ПК настроен должным образом. Можно теперь добавить эту команду для разрешения максимальной гибкости:

```
ppp encrypt mppe auto
```

[Назначение статического IP-адреса с сервера](#)

Если необходимо назначить определенный IP - адрес на пользователя в Настройке Пользователя ACS, выберите **статический IP - адрес Assign** и заполните IP-адрес.

[Добавьте списки доступа к серверу](#)

Для управления тем, к чему пользователь PPTP может обратиться, как только пользователь связан с маршрутизатором, можно настроить список доступа на маршрутизаторе. Например, если вы выполняете эту команду:

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

и выберите, **Filter-Id (припишите 11)** в ACS, и войдите **101** в коробке, пользователь PPTP может обратиться к этим 10.1.1.2 хостам, но не другим. При запуске **show ip interface virtual-access x** команда где x является номером, который вы в состоянии определить от команды **show user**, список доступа должен показать, как применено:

```
Inbound access list is 101
```

[Добавление учета](#)

Можно добавить составление сеансов с этой командой:

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

Учетные записи в Cisco Secure ACS появляются как показано в выходных данных ниже:

```
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
```

Примечание: Разрывы строки были добавлены к примеру в целях показа. Разрывы строки в вашей эффективной выходной мощности отличаются от показанных здесь.

[Раздельное туннелирование](#)

Когда туннель PPTP подходит на ПК, маршрутизатор PPTP установлен с более высокой метрикой, чем предыдущий по умолчанию, таким образом, вы теряете интернет-

соединение. Для исправления этого, учитывая, что сеть в маршрутизаторе 10.1.1. X, выполните пакетный файл (batch.bat) для изменения Организации маршрутизации Microsoft, чтобы удалить по умолчанию и повторно установить маршрут по умолчанию (это требует IP-адреса, клиенту PPTP назначают; для примера, который является 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
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

- **show vpdn session** — Отображает информацию об активном протоколе туннеля Level 2 Forwarding (L2F) и идентификаторах сообщения в Виртуальной частной коммутируемой сети (VPDN).

```
mos#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 mos#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
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

1. **ПК задает шифрование, но маршрутизатор не делает.** Пользователь ПК видит: The remote computer does not support the required data encryption type.
2. **И ПК и маршрутизатор задают шифрование, но сервер RADIUS не настроен для передачи вниз ключей MPPE (они обычно появляются как атрибут 26).** Пользователь ПК видит: The remote computer does not support the required data encryption type.
3. **Маршрутизатор задает (требуемое) шифрование, но ПК не делает (не позволенный).** Пользователь ПК видит: The specified port is not connected.
4. **Пользователь вводит неверное имя пользователя или пароль.** Пользователь ПК видит: Access was denied because the username and/or password was invalid on the domain. **Отладка маршрутизатора** показывает: **Примечание:** Разрывы строки были добавлены к данному примеру в целях показа. Разрывы строки в вашей эффективной выходной мощности отличаются от показанных здесь.
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. **Сервер RADIUS необщителен.** Пользователь ПК видит: Access was denied because the username and/or password was invalid on the domain. **Отладка маршрутизатора** показывает: **Примечание:** Разрывы строки были добавлены к данному примеру в целях показа. Разрывы строки в вашей эффективной выходной мощности отличаются от показанных здесь.

```
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
```

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

Примечание: Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки".

Если вещи не работают, минимальные команды отладки включают:

- **debug aaa authentication** - Вывод сведений об аутентификации AAA/TACACS+.
- **debug aaa authorization** — отображаются данные авторизации AAA/TACACS+.
- **"debug ppp negotiation"** – отображаются PPP-пакеты, передаваемые при запуске PPP с согласованием параметров.
- **debug ppp authenticaion** — Отображает сообщения протокола аутентификации, которые включают обмены пакетами CHAP и обмены Протокола аутентификации пароля (PAP).
- **debug radius**– выводит подробные данные об отладке сервера RADIUS.

Если аутентификация работает, но существуют проблемы с шифрованием MPPE, используют эти команды:

- **debug ppp mppe packet** — Отображает все поступление и исходящий трафик MPPE.
- **debug ppp mppe event** – отображаются основные события MPPE.
- **debug ppp mppe detailed** - отображает подробные сведения об MPPE.
- **debug vpdn l2x-packets в Ё**” служит для отображения сообщений о заголовках и статусе протокола L2F.
- **debug vpdn events** –отображает сообщения о событиях, являющихся частью нормального туннельного открытия или закрытия.
- **debug vpdn errors** – отображает ошибки, которые мешают установке туннеля, или ошибки, которые вызывают закрытие установленного туннеля.
- команда **debug vpdn packets** отображает замененные пакеты данных для всех протоколов. Эта опция может привести к большому числу сообщений отладки, и необходимо обычно только использовать эту команду на шасси отладки с одиночным активным сеансом.

Можно также использовать эти команды для целей устранения проблем:

- **clear interface virtual-access x** — Завершает работу указанного туннеля и всех сеансов в туннеле.

Пример выходных данных хорошей отладки

Эта отладка показывает важные события от RFC:

- **SCCRQ = Start-Control-Connection-Request** – байты кода сообщения 9 и 10 = 0001
- **SCCRP = Начало-Управление-Подключение-Отклик**
- **OCRQ = Outgoing Call ReQuest** - байты кода сообщения 9 и 10 = 0007
- **OCRP = исходящий вызов-ответ**

Примечание: Разрывы строки были добавлены к данному примеру в целях показа. Разрывы строки в вашей эффективной выходной мощности отличаются от показанных здесь.

```
mos#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 009C00011A2B3C4D000100000100000000000000010000... 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: ppp 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 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 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 (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

[Дополнительные сведения](#)

- [Страница поддержки Cisco Secure ACS для Windows](#)
- [Cisco Systems – техническая поддержка и документация](#)