Настройка Cisco IOS и Windows 2000 для PPTP с использованием Microsoft IAS

Содержание

Введение

Поддержка протокола туннелирования PPTP была добавлена в выпуске ПО Cisco IOS® 12.0.5. XE5 на платформах маршрутизаторов Cisco 7100 и 7200. В выпуске ПО Cisco IOS 12.1.5.T добавлена поддержка ряда дополнительных платформ. Т.

Запрос на комментарий (RFC) 2637 описывает PPTP. Согласно этому RFC, концентратор доступа PPTP (PAC) является клиентом (т. е. ПК или вызывающим устройством), а сетевой сервер PPTP (PNS) является сервером (т. е. маршрутизатором или вызываемым устройством).

Предварительные условия

Требования

В этом документе предполагается, что вы установили подключения PPTP к маршрутизатору с локальным протоколом квитирования с аутентификацией Microsoft (MS-CHAP) V1 (и дополнительно протокол шифрования соединений типа точка-точка корпорации Microsoft (MPPE) [MPPE], который требует MS-CHAP V1), с помощью этих документов, и что они уже работают. Служба удаленной аутентификации пользователей по коммутируемым линиям (RADIUS) требуется для поддержки шифрования по протоколу MPPE; TACACS + работает для аутентификации, но не для кодирования MPPE.

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Дополнительный компонент Microsoft IAS устанавливается на расширенной версии сервера Microsoft 2000 с Active Directory.
- Маршрутизатор Cisco 3600.
- ПО Cisco IOS версии c3640-io3s56i-mz.121-5. T.

В этой конфигурации используется Microsoft IAS, установленный на расширенной версии сервера Windows 2000, как сервер RADIUS.

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. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Теоретические сведения

Этот пример конфигурации демонстрирует, как настроить ПК для соединения с маршрутизатором (по адресу 10.200.20.2), который затем подтверждает подлинность пользователя Internet Authentication Server (IAS) Microsoft (по адресу 10.200.20.245), после чего позволяет пользователю войти в сеть. Поддержка PPTP доступна в Cisco Secure Access Control Server (ACS) версии 2.5 для Windows. Однако, это не может работать с маршрутизатором из-за проблемы Cisco Bug ID CSCds92266. При использовании Cisco Secure рекомендуется применять версию 2.6 Cisco Secure или выше. Cisco Secure UNIX не поддерживает MPPE. Два других приложения RADIUS с поддержкой MPPE: Microsoft RADIUS и Funk RADIUS.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Для получения дополнительной информации о командах, встречающихся в

этом документе, используйте средство поиска команд

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.

Пул IP для клиентов удаленного доступа:

- Маршрутизатор/шлюз: 192.168.1.2 ~ 192.168.1.254
- LNS: 172.16.10.1 ~ 172.16.10.10

Несмотря на то что в вышеупомянутой настройке используется клиент удаленного доступа для соединения с маршрутизатором интернет-провайдера (ISP) через модемную связь, можно подключить ПК и маршрутизатор/шлюз через любые среды, такие как LAN.

Настройка сервера Windows 2000 Advanced Server для Microsoft IAS

В этом разделе показано, как настроить расширенную версию сервера Windows 2000 для Microsoft IAS:

1. Убедитесь, что установлен Microsoft IAS. Для установки Microsoft IAS войдите в систему как администратор. **В разеделе Network Services убедитесь, что сняты все флажки. Установите флажок Internet Authentication Server, затем нажмите "OK".**
2. **В мастере компонентов Windows нажмите Next.** В случае появления запроса, вставьте CD-диск Windows 2000.
3. **После того как необходимые файлы будут скопированы, нажмите Finish, а затем закройте все окна.** Выполнять перезагрузку не нужно.

Настройка клиентов RADIUS

В этом разделе представлены этапы настройки клиентов RADIUS:

1. **В разделе Administrative Tools, откройте консоль Internet Authentication Server ии нажмите Clients.**
2. **В окне Friendly Name введите IP-адрес сервера доступа к сети (NAS).**
3. **Щелкните вариант Use this IP.**
4. **В поле выпадающего списка Client-Vendor убедитесь, что выбран вариант RADIUS Standard.**
5. **В полях Shared Secret и Confirm Shared Secret, введите пароль, затем нажмите Finish.**
6. **В дереве консоли щелкните правой кнопкой мыши Internet Authentication Service, затем нажмите Start.**
7. Закройте консоль.

Настройка пользователей в IAS

В отличие от Cisco Secure, база данных пользователей RADIUS в Windows 2000 плотно связана с базой данных пользователей Windows. **В случае если Active Directory установлен на вашем сервере Windows 2000, создавайте своих новых пользователей с удаленным доступом из пользователей и компьютеров Active Directory. Если Active Directory не установлен, используйте локальных пользователей и группы из средств администрирования**

для создания новых пользователей.

Настройка пользователей в Active Directory

В этом разделе представлены этапы настройки пользователей в Active Directory:

1. На консоли пользователей и компьютеров Active Directory разверните свой домен. Щелкните правой кнопкой мыши Users. Прокрутите список и перейдите к пункту New User. Создайте нового пользователя с именем tac.
2. Введите пароль в диалоговых окнахPassword и Confirm Password.
3. Очистите поле User Must Change Password at Next Logon и нажмите Next.
4. Откройте окно User tac Properties. Перейдите на вкладку Dial-In. В разделе Remote Access Permission (Dial-in or VPN), нажмите Allow Access, затем нажмите "OK".

Настройка пользователей, если не установлен Active Directory

Если Active Directory не установлен, в этом разделе представлены этапы настройки пользователей:

1. В разделе Administrative Tools щелкните Computer Management. Разверните консоль Computer Management и щелкните Local Users and Groups. Щелкните правой кнопкой мыши полосу прокрутки Users для выбора New User. Создайте нового пользователя с именем tac.
2. Введите пароль в диалоговых окнахPassword и Confirm Password.
3. Очистите опцию User Must Change Password at Next Logon и нажмите Next.
4. Откройте окно свойств нового пользователя с именем tac. Перейдите на вкладку Dial-In. В разделе Remote Access Permission (Dial-in or VPN), нажмите Allow Access, затем нажмите "OK".

Применение политики удаленного доступа к пользователю Windows

В этом разделе представлены этапы применения политики удаленного доступа к пользователю Windows:

1. В разделе Administrative Tools откройте консоль Internet Authentication Server и нажмите Remote Access Policies.
2. Нажмите кнопку Add в Specify the Conditions to Match и добавьте Service-Type. Выберите доступный тип как Framed и добавьте его в списокSelected Types. Нажмите OK.
3. Нажмите кнопку Add в Specify the Conditions to Match и добавьте Framed Protocol. Выберите доступный тип как ppp и добавьте его в список Selected Types. Нажмите OK.
4. Нажмите кнопку Add в Specify the Conditions to Match и добавьте Windows-Groups, чтобы добавить группу пользователей Windows, к которой принадлежит пользователь. Выберите группу и добавьте ее в список Selected Types, затем нажмите OK.
5. В свойствах Allow Access if Dial-in Permission is Enabled выберите Grant remote Access permission.
6. Закройте консоль.

Настройка клиента Windows 2000 для PPTP

В следующем далее разделе представлены этапынастройки клиента Windows 2000 для PPTP:

1. **В меню Start выберите Settings, затем или:Control Panel и Network and Dial-up Connections, илиNetwork and Dial-up Connections, затем Make New Connection.Используйте программу-мастер для создания подключения с именем PPTP.** Это подключение соединяется с частной сетью через Интернет. Также необходимо задать IP-адрес или имя для PPTP Network Server (PNS).
2. **Новое подключение появляется в окне Network и Dial-up Connections в Control Panel.**Здесь щелкните правой кнопкой мыши для редактирования свойств подключения. **На вкладкеNetworking удостоверьтесь, что поле Type of Server I Am Calling установлено в PPTP. Если планируется выделить динамический внутренний адрес этому клиенту от шлюза, или через локальный пул, или через протокол DHCP (динамического конфигурирования узла), выберите протокол TCP/IP и удостоверьтесь, что клиент настроен для получения IP-адреса автоматически.** Можно также выдавать информацию DNS автоматически.**Кнопка Advanced позволяет определять статический сервис Windows назначения имен в Интернете (WINS) и информацию DNS.Вкладка Options позволяет выключать IPSec или назначать другую политику для подключения.**
3. **На вкладке Security можно определить параметры аутентификации пользователя.** Например, PAP, CHAP или MS-CHAP, а также вход в систему домена Windows. Как только поключение настроено, можно дважды щелкнуть по нему, чтобы отобразить экран входа в систему, а затем установить соединение.

Конфигурации

С помощью приведенной ниже конфигурации маршрутизатора пользователь может соединиться с именем пользователя tac и паролем admin, даже если сервер RADIUS недоступен (это возможно, когда необходимо еще настроить Microsoft IAS). В следующем ниже примере конфигурации описаны команды, необходимые для L2tp без IPSec.

angela

```
angela#show running-config Building configuration...
Current configuration : 1606 bytes ! version 12.1 no
service single-slot-reload-enable service timestamps
debug datetime msec service timestamps log datetime msec
no service password-encryption ! hostname angela !
logging rate-limit console 10 except errors !---Enable
AAA services here aaa new-model aaa authentication login
default group radius local aaa authentication login
console none aaa authentication ppp default group radius
local aaa authorization network default group radius
local enable password ! username tac password 0 admin
memory-size iomem 30 ip subnet-zero ! ! no ip finger no
ip domain-lookup ip host rund 172.17.247.195 ! ip audit
notify log ip audit po max-events 100 ip address-pool
local !---Enable VPN/Virtual Private Dialup Network
(VPDN) services !---and define groups and their
respective parameters. vpdn enable no vpdn logging ! !
vpdn-group PPTP_WIN2KClient !---Default PPTP VPDN group
!---Allow the router to accept incoming Requests accept-
dialin protocol pptp virtual-template 1 ! ! ! call rsvp-
```

```
sync ! ! ! ! ! ! ! controller E1 2/0 ! ! interface
Loopback0 ip address 172.16.10.100 255.255.255.0 !
interface Ethernet0/0 ip address 10.200.20.2
255.255.255.0 half-duplex ! interface Virtual-Template1
ip unnumbered Loopback0 peer default ip address pool
default !--- The following encryption command is
optional !--- and could be added later. ppp encrypt mppe
40 ppp authentication ms-chap ! ip local pool default
172.16.10.1 172.16.10.10 ip classless ip route 0.0.0.0
0.0.0.0 10.200.20.1 ip route 192.168.1.0 255.255.255.0
10.200.20.250 no ip http server ! radius-server host
10.200.20.245 auth-port 1645 acct-port 1646 radius-
server retransmit 3 radius-server key cisco ! dial-peer
cor custom ! ! ! ! ! line con 0 exec-timeout 0 0 login
authentication console transport input none line 33 50
modem InOut line aux 0 line vty 0 4 exec-timeout 0 0
password ! end angela#show debug General OS: AAA
Authentication debugging is on AAA Authorization
debugging is on PPP: MPPE Events debugging is on PPP
protocol negotiation debugging is on VPN: L2X protocol
events debugging is on L2X protocol errors debugging is
on VPDN events debugging is on VPDN errors debugging is
on Radius protocol debugging is on angela# *Mar 7
04:21:07.719: L2X: TCP connect reqd from 0.0.0.0:2000
*Mar 7 04:21:07.991: Tnl 29 PPTP: Tunnel created; peer
initiated *Mar 7 04:21:08.207: Tnl 29 PPTP: SCCRQ-ok ->
state change wt-sccrq to estabd *Mar 7 04:21:09.267:
VPDN: Session vaccess task running *Mar 7 04:21:09.267:
Vi1 VPDN: Virtual interface created *Mar 7 04:21:09.267:
Vi1 VPDN: Clone from Vtemplate 1 *Mar 7 04:21:09.343:
Tnl/Cl 29/29 PPTP: VAccess created *Mar 7 04:21:09.343:
Vi1 Tnl/Cl 29/29 PPTP: vacc-ok -> #state change wt-vacc
to estabd *Mar 7 04:21:09.343: Vi1 VPDN: Bind interface
direction=2 *Mar 7 04:21:09.347: %LINK-3-UPDOWN:
Interface Virtual-Access1, changed state to up *Mar 7
04:21:09.347: Vi1 PPP: Using set call direction *Mar 7
04:21:09.347: Vi1 PPP: Treating connection as a callin
*Mar 7 04:21:09.347: Vi1 PPP: Phase is ESTABLISHING,
Passive Open [0 sess, 0 load] *Mar 7 04:21:09.347: Vi1
LCP: State is Listen *Mar 7 04:21:10.347: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up *Mar 7 04:21:11.347: Vi1 LCP:
TIMEout: State Listen *Mar 7 04:21:11.347: Vi1
AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Mar 7
04:21:11.347: Vi1 LCP: O CONFREQ [Listen] id 7 len 15
*Mar 7 04:21:11.347: Vi1 LCP: AuthProto MS-CHAP
(0x0305C22380) *Mar 7 04:21:11.347: Vi1 LCP: MagicNumber
0x3050EB1F (0x05063050EB1F) *Mar 7 04:21:11.635: Vi1
LCP: I CONFACK [REQsent] id 7 len 15 *Mar 7
04:21:11.635: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 7 04:21:11.635: Vi1 LCP: MagicNumber 0x3050EB1F
(0x05063050EB1F) *Mar 7 04:21:13.327: Vi1 LCP: I CONFREQ
[ACKrcvd] id 1 len 44 *Mar 7 04:21:13.327: Vi1 LCP:
MagicNumber 0x35BE1CB0 (0x050635BE1CB0) *Mar 7
04:21:13.327: Vi1 LCP: PFC (0x0702) *Mar 7 04:21:13.327:
Vi1 LCP: ACFC (0x0802) *Mar 7 04:21:13.327: Vi1 LCP:
Callback 6 (0x0D0306) *Mar 7 04:21:13.327: Vi1 LCP: MRRU
1614 (0x1104064E) *Mar 7 04:21:13.327: Vi1 LCP:
EndpointDisc 1 Local *Mar 7 04:21:13.327: Vi1 LCP:
(0x1317016AC616B006CC4281A1CA941E39) *Mar 7
04:21:13.331: Vi1 LCP: (0xB9182600000008) *Mar 7
04:21:13.331: Vi1 LCP: O CONFREJ [ACKrcvd] id 1 len 34
*Mar 7 04:21:13.331: Vi1 LCP: Callback 6 (0x0D0306) *Mar
7 04:21:13.331: Vi1 LCP: MRRU 1614 (0x1104064E) *Mar 7
```

```
04:21:13.331: Vi1 LCP: EndpointDisc 1 Local *Mar 7
04:21:13.331: Vi1 LCP:
(0x1317016AC616B006CC4281A1CA941E39) *Mar 7
04:21:13.331: Vi1 LCP: (0xB9182600000008) *Mar 7
04:21:13.347: Vi1 LCP: TIMEout: State ACKrcvd *Mar 7
04:21:13.347: Vi1 LCP: O CONFREQ [ACKrcvd] id 8 len 15
*Mar 7 04:21:13.347: Vi1 LCP: AuthProto MS-CHAP
(0x0305C22380) *Mar 7 04:21:13.347: Vi1 LCP: MagicNumber
0x3050EB1F (0x05063050EB1F) *Mar 7 04:21:13.647: Vi1
LCP: I CONFREQ [REQsent] id 2 len 14 *Mar 7
04:21:13.651: Vi1 LCP: MagicNumber 0x35BE1CB0
(0x050635BE1CB0) *Mar 7 04:21:13.651: Vi1 LCP: PFC
(0x0702) *Mar 7 04:21:13.651: Vi1 LCP: ACFC (0x0802)
*Mar 7 04:21:13.651: Vi1 LCP: O CONFACK [REQsent] id 2
len 14 *Mar 7 04:21:13.651: Vi1 LCP: MagicNumber
0x35BE1CB0 (0x050635BE1CB0) *Mar 7 04:21:13.651: Vi1
LCP: PFC (0x0702) *Mar 7 04:21:13.651: Vi1 LCP: ACFC
(0x0802) *Mar 7 04:21:13.723: Vi1 LCP: I CONFACK
[ACKsent] id 8 len 15 *Mar 7 04:21:13.723: Vi1 LCP:
AuthProto MS-CHAP (0x0305C22380) *Mar 7 04:21:13.723:
Vi1 LCP: MagicNumber 0x3050EB1F (0x05063050EB1F) *Mar 7
04:21:13.723: Vi1 LCP: State is Open *Mar 7
04:21:13.723: Vi1 PPP: Phase is AUTHENTICATING, by this
end [0 sess, 0 load] *Mar 7 04:21:13.723: Vi1 MS-CHAP: O
CHALLENGE id 20 len 21 from "angela " *Mar 7
04:21:14.035: Vi1 LCP: I IDENTIFY [Open] id 3 len 18
magic 0x35BE1CB0 MSRASV5.00 *Mar 7 04:21:14.099: Vi1
LCP: I IDENTIFY [Open] id 4 len 24 magic 0x35BE1CB0
MSRAS-1-RSHANMUG *Mar 7 04:21:14.223: Vi1 MS-CHAP: I
RESPONSE id 20 len 57 from "tac" *Mar 7 04:21:14.223:
AAA: parse name=Virtual-Access1 idb type=21 tty=-1 *Mar
7 04:21:14.223: AAA: name=Virtual-Access1 flags=0x11
type=5 shelf=0 slot=0 adapter=0 port=1 channel=0 *Mar 7
04:21:14.223: AAA/MEMORY: create_user (0x62740E7C)
user='tac' ruser='' port='Virtual-Access1' rem_addr=''
authen_type=MSCHAP service=PPP priv=1 *Mar 7
04:21:14.223: AAA/AUTHEN/START (2474402925):
port='Virtual-Access1' list='' action=LOGIN service=PPP
*Mar 7 04:21:14.223: AAA/AUTHEN/START (2474402925):
using "default" list *Mar 7 04:21:14.223:
AAA/AUTHEN/START (2474402925): Method=radius (radius)
*Mar 7 04:21:14.223: RADIUS: ustruct sharecount=0 *Mar 7
04:21:14.223: RADIUS: Initial Transmit Virtual-Access1
id 116 10.200.20.245:1645, Access-Request, len 129 *Mar
7 04:21:14.227: Attribute 4 6 0AC81402 *Mar 7
04:21:14.227: Attribute 5 6 00000001 *Mar 7
04:21:14.227: Attribute 61 6 00000005 *Mar 7
04:21:14.227: Attribute 1 5 7461631A *Mar 7
04:21:14.227: Attribute 26 16 000001370B0AFD11 *Mar 7
04:21:14.227: Attribute 26 58 0000013701341401 *Mar 7
04:21:14.227: Attribute 6 6 00000002 *Mar 7
04:21:14.227: Attribute 7 6 00000001 *Mar 7
04:21:14.239: RADIUS: Received from id 116
10.200.20.245:1645, Access-Accept, len 116 *Mar 7
04:21:14.239: Attribute 7 6 00000001 *Mar 7
04:21:14.239: Attribute 6 6 00000002 *Mar 7
04:21:14.239: Attribute 25 32 64080750 *Mar 7
04:21:14.239: Attribute 26 40 000001370C223440 *Mar 7
04:21:14.239: Attribute 26 12 000001370A06144E *Mar 7
04:21:14.239: AAA/AUTHEN (2474402925): status = PASS
*Mar 7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
Port='Virtual-Access1' list='' service=NET *Mar 7
04:21:14.243: AAA/AUTHOR/LCP: Vi1 (2434357606)
```

```
user='tac' *Mar 7 04:21:14.243: Vi1 AAA/AUTHOR/LCP
(2434357606): send AV service=ppp *Mar 7 04:21:14.243:
Vi1 AAA/AUTHOR/LCP (2434357606): send AV protocol=lcp
*Mar 7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
found list "default" *Mar 7 04:21:14.243: Vi1
AAA/AUTHOR/LCP (2434357606): Method=radius (radius) *Mar
7 04:21:14.243: RADIUS: unrecognized Microsoft VSA type
10 *Mar 7 04:21:14.243: Vi1 AAA/AUTHOR (2434357606):
Post authorization status = PASS_REPL *Mar 7
04:21:14.243: Vi1 AAA/AUTHOR/LCP: Processing AV
service=ppp *Mar 7 04:21:14.243: Vi1 AAA/AUTHOR/LCP:
Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 7 04:21:14.243: Vi1 MS-CHAP: O SUCCESS id 20
len 4 *Mar 7 04:21:14.243: Vi1 PPP: Phase is UP [0 sess,
0 load] *Mar 7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: (0):
Can we start IPCP? *Mar 7 04:21:14.247: Vi1
AAA/AUTHOR/FSM (1553311212): Port='Virtual-Access1'
list='' service=NET *Mar 7 04:21:14.247: AAA/AUTHOR/FSM:
Vi1 (1553311212) user='tac' *Mar 7 04:21:14.247: Vi1
AAA/AUTHOR/FSM (1553311212): send AV service=ppp *Mar 7
04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212): send AV
protocol=ip *Mar 7 04:21:14.247: Vi1 AAA/AUTHOR/FSM
(1553311212): found list "default" *Mar 7 04:21:14.247:
Vi1 AAA/AUTHOR/FSM (1553311212): Method=radius (radius)
*Mar 7 04:21:14.247: RADIUS: unrecognized Microsoft VSA
type 10 *Mar 7 04:21:14.247: Vi1 AAA/AUTHOR
(1553311212): Post authorization status = PASS_REPL *Mar
7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar 7 04:21:14.247: Vi1 IPCP: O CONFREQ [Not
negotiated] id 4 len 10 *Mar 7 04:21:14.247: Vi1 IPCP:
Address 172.16.10.100 (0x0306AC100A64) *Mar 7
04:21:14.247: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
*Mar 7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (3663845178):
Port='Virtual-Access1' list='' service=NET *Mar 7
04:21:14.251: AAA/AUTHOR/FSM: Vi1 (3663845178)
user='tac' *Mar 7 04:21:14.251: Vi1 AAA/AUTHOR/FSM
(3663845178): send AV service=ppp *Mar 7 04:21:14.251:
Vi1 AAA/AUTHOR/FSM (3663845178): send AV protocol=ccp
*Mar 7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178):
found list "default" *Mar 7 04:21:14.251: Vi1
AAA/AUTHOR/FSM (3663845178): Method=radius (radius) *Mar
7 04:21:14.251: RADIUS: unrecognized Microsoft VSA type
10 *Mar 7 04:21:14.251: Vi1 AAA/AUTHOR (3663845178):
Post authorization status = PASS_REPL *Mar 7
04:21:14.251: Vi1 AAA/AUTHOR/FSM: We can start CCP *Mar
7 04:21:14.251: Vi1 CCP: O CONFREQ [Closed] id 3 len 10
*Mar 7 04:21:14.251: Vi1 CCP: MS-PPC supported bits
0x01000020 (0x120601000020) *Mar 7 04:21:14.523: Vi1
CCP: I CONFREQ [REQsent] id 5 len 10 *Mar 7
04:21:14.523: Vi1 CCP: MS-PPC supported bits 0x010000F1
(0x1206010000F1) *Mar 7 04:21:14.523: Vi1 MPPE: don't
understand all options, NAK *Mar 7 04:21:14.523: Vi1
AAA/AUTHOR/FSM: Check for unauthorized mandatory AV's
*Mar 7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Processing AV
service=ppp *Mar 7 04:21:14.523: Vi1 AAA/AUTHOR/FSM:
Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 7 04:21:14.523: Vi1 CCP: O CONFNAK [REQsent] id 5
len 10 *Mar 7 04:21:14.523: Vi1 CCP: MS-PPC supported
bits 0x01000020 (0x120601000020) *Mar 7 04:21:14.607:
Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34 *Mar 7
04:21:14.607: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
```

```
*Mar 7 04:21:14.607: Vi1 IPCP: PrimaryDNS 0.0.0.0
(0x810600000000) *Mar 7 04:21:14.607: Vi1 IPCP:
PrimaryWINS 0.0.0.0 (0x820600000000) *Mar 7
04:21:14.607: Vi1 IPCP: SecondaryDNS 0.0.0.0
(0x830600000000) *Mar 7 04:21:14.607: Vi1 IPCP:
SecondaryWINS 0.0.0.0 (0x840600000000) *Mar 7
04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Start. Her address
0.0.0.0, we want 0.0.0.0 *Mar 7 04:21:14.607: Vi1
AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 7
04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 7 04:21:14.607: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
0.0.0.0 *Mar 7 04:21:14.607: Vi1 IPCP: Pool returned
172.16.10.1 *Mar 7 04:21:14.607: Vi1 IPCP: O CONFREJ
[REQsent] id 6 len 28 *Mar 7 04:21:14.607: Vi1 IPCP:
PrimaryDNS 0.0.0.0 (0x810600000000) *Mar 7 04:21:14.611:
Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000) *Mar 7
04:21:14.611: Vi1 IPCP: SecondaryDNS 0.0.0.0
(0x830600000000) *Mar 7 04:21:14.611: Vi1 IPCP:
SecondaryWINS 0.0.0.0 (0x840600000000) *Mar 7
04:21:14.675: Vi1 IPCP: I CONFACK [REQsent] id 4 len 10
*Mar 7 04:21:14.675: Vi1 IPCP: Address 172.16.10.100
(0x0306AC100A64) *Mar 7 04:21:14.731: Vi1 CCP: I CONFACK
[REQsent] id 3 len 10 *Mar 7 04:21:14.731: Vi1 CCP: MS-
PPC supported bits 0x01000020 (0x120601000020) *Mar 7
04:21:14.939: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 7 04:21:14.939: Vi1 CCP: MS-PPC supported bits
0x01000020 (0x120601000020) *Mar 7 04:21:14.939: Vi1
AAA/AUTHOR/FSM: Check for unauthorized mandatory AV's
*Mar 7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Processing AV
service=ppp *Mar 7 04:21:14.939: Vi1 AAA/AUTHOR/FSM:
Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 7 04:21:14.939: Vi1 CCP: O CONFACK [ACKrcvd] id 7
len 10 *Mar 7 04:21:14.939: Vi1 CCP: MS-PPC supported
bits 0x01000020 (0x120601000020) *Mar 7 04:21:14.943:
Vi1 CCP: State is Open *Mar 7 04:21:14.943: Vi1 MPPE:
Generate keys using RADIUS data *Mar 7 04:21:14.943: Vi1
MPPE: Initialize keys *Mar 7 04:21:14.943: Vi1 MPPE: [40
bit encryption] [stateless mode] *Mar 7 04:21:14.991:
Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10 *Mar 7
04:21:14.991: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 7 04:21:14.991: Vi1 AAA/AUTHOR/IPCP: Start. Her
address 0.0.0.0, we want 172.16.10.1 *Mar 7
04:21:14.991: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp *Mar 7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP:
Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 7 04:21:14.995: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
172.16.10.1 *Mar 7 04:21:14.995: Vi1 IPCP: O CONFNAK
[ACKrcvd] id 8 len 10 *Mar 7 04:21:14.995: Vi1 IPCP:
Address 172.16.10.1 (0x0306AC100A01) *Mar 7
04:21:15.263: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 7 04:21:15.263: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 7 04:21:15.263: Vi1
AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1, we want
172.16.10.1 *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP
(2052567766): Port='Virtual-Access1' list='' service=NET
*Mar 7 04:21:15.267: AAA/AUTHOR/IPCP: Vi1 (2052567766)
```

user='tac' *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): send AV service=ppp *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): send AV protocol=ip *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): send AV addr*172.16.10.1 *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): found list "default" *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): Method=radius (radius) *Mar 7 04:21:15.267: RADIUS: unrecognized Microsoft VSA type 10 *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR (2052567766): Post authorization status = PASS_REPL *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using 172.16.10.1 *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111 *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1 *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded *Mar 7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Done. Her address 172.16.10.1, we want 172.16.10.1 *Mar 7 04:21:15.271: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10 *Mar 7 04:21:15.271: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01) *Mar 7 04:21:15.271: Vi1 IPCP: State is Open *Mar 7 04:21:15.271: Vi1 IPCP: Install route to 172.16.10.1 *Mar 7 04:21:22.571: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic 0x35BE1CB0 *Mar 7 04:21:22.571: Vi1 LCP: Received id 1, sent id 1, line up *Mar 7 04:21:30.387: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic 0x35BE1CB0 *Mar 7 04:21:30.387: Vi1 LCP: Received id 2, sent id 2, line up angela#**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 29 estabd 192.168.1.47 2000 1 LocID RemID TunID Intf Username State Last Chg 29 32768 29 Vi1 tac estabd 00:00:31 %No active PPPoE tunnels angela# *Mar 7 04:21:40.471: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x35BE1CB0 *Mar 7 04:21:40.471: Vi1 LCP: Received id 3, sent id 3, line up *Mar 7 04:21:49.887: Vi1 LCP: I ECHOREP [Open] id 4 len 12 magic 0x35BE1CB0 *Mar 7 04:21:49.887: Vi1 LCP: Received id 4, sent id 4, line up angela#**ping 192.168.1.47** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.47, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 484/584/732 ms *Mar 7 04:21:59.855: Vi1 LCP: I ECHOREP [Open] id 5 len 12 magic 0x35BE1CB0 *Mar 7 04:21:59.859: Vi1 LCP: Received id 5, sent id 5, line up *Mar 7 04:22:06.323: Tnl 29 PPTP: timeout -> state change estabd to estabd *Mar 7 04:22:08.111: Tnl 29 PPTP: EchoRQ -> state change estabd to estabd *Mar 7 04:22:08.111: Tnl 29 PPTP: EchoRQ -> echo state change Idle to Idle *Mar 7 04:22:09.879: Vi1 LCP: I ECHOREP [Open] id 6 len 12 magic 0x35BE1CB0 *Mar 7 04:22:09.879: Vi1 LCP: Received id 6, sent id 6, line up angela#**ping 172.16.10.1** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 584/707/1084 ms *Mar 7 04:22:39.863: Vi1 LCP: I ECHOREP [Open] id 7 len 12 magic 0x35BE1CB0 *Mar 7 04:22:39.863: Vi1 LCP: Received id 7, sent id 7, line up angela#**clear vpdn tunnel pptp tac** Could not find specified tunnel angela#**show vpdn tunnel** %No active L2TP tunnels %No active L2F tunnels PPTP Tunnel Information

```
Total tunnels 1 sessions 1 LocID Remote Name State
Remote Address Port Sessions 29 estabd 192.168.1.47 2000
1 %No active PPPoE tunnels angela# *Mar 7 04:23:05.347:
Tnl 29 PPTP: timeout -> state change estabd to estabd
angela# *Mar 7 04:23:08.019: Tnl 29 PPTP: EchoRQ ->
state change estabd to estabd *Mar 7 04:23:08.019: Tnl
29 PPTP: EchoRQ -> echo state change Idle to Idle
angela# *Mar 7 04:23:09.887: Vi1 LCP: I ECHOREP [Open]
id 10 len 12 magic 0x35BE1CB0 *Mar 7 04:23:09.887: Vi1
LCP: Received id 10, sent id 10, line up
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Интерпретатором выходных данных; это позволяет выполнять анализ выходных данных команды show.

- **show vpdn -** Отображает информацию об активном туннеле протокола Level 2 Forwarding (L2F) и идентификаторах сообщений в VPDN.

Можно также использовать show vpdn? чтобы увидеть другие специфичные для VPDN команды show.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Некоторые команды show поддерживаются Интерпретатором выходных данных; это позволяет выполнять анализ выходных данных команды show.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- **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.**
- **команда "debug ppp authentication" отображает сообщения протокола проверки подлинности, включая информацию об обмене пакетами протокола проверки подлинности запроса CHAP и обмене по протоколу проверки подлинности по паролю (PAP).**
- **debug radius– выводит подробные данные об отладке сервера RADIUS.** Если аутентификация работает, но существуют проблемы с шифрованием MPPE, используют одну из команд отладки, приведенных ниже.
- **debug ppp mppe packet - Отображает весь входящий 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 вЂ” 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.** Этот параметр может вызвать существенное увеличение числа отладочных сообщений, поэтому его следует использовать только в конфигурации отладки с одним активным сеансом.

Раздельное туннелирование

Предположим, что маршрутизатор/шлюзом является маршрутизатором ISP. Когда туннель PPTP доходит до ПК, маршрут PPTP устанавливается с более высокой метрикой, чем предыдущий по умолчанию, и, как следствие, мы теряем интернет-подключение. Для исправления этого модифицируйте организацию маршрутизации Microsoft, чтобы удалить и повторно установить маршрут по умолчанию (это требует знания IP-адреса, назначенного клиенту PPTP; для текущего примера это адрес 172.16.10.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

Если не сделана настройка клиента для шифрования

На вкладке Security подключения удаленного доступа, используемого для сеанса PPTP, можно определить параметры аутентификации пользователя. Например, это может быть PAP, CHAP, MS-CHAP или вход в систему домена Windows. **При выборе варианта No Encryption Allowed (сервер отключается, если это требует шифрования) в разделе Properties VPN-подключения можно видеть сообщение об ошибке PPTP у на стороне клиента:**

```
Registering your computer on the network..
Error 734:  The PPP link control protocol was terminated.
Debugs on the  router:
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Processing AV protocol=ccp
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  8 22:38:52.500: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar  8 22:38:52.500: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  8 22:38:52.500: Vi1 CCP: State is Open
*Mar  8 22:38:52.500: Vi1 MPPE: RADIUS keying material missing
*Mar  8 22:38:52.500: Vi1 CCP: O TERMREQ [Open] id 5 len 4
*Mar  8 22:38:52.524: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar  8 22:38:52.524: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  8 22:38:52.524: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
```

```
*Mar  8 22:38:52.524: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar  8 22:38:52.640: Vi1 CCP: I TERMACK [TERMsent] id 5 len 4
*Mar  8 22:38:52.640: Vi1 CCP: State is Closed
*Mar  8 22:38:52.640: Vi1 MPPE: Required encryption not negotiated
*Mar  8 22:38:52.640: Vi1 IPCP: State is Closed
*Mar  8 22:38:52.640: Vi1 PPP: Phase is TERMINATING [0 sess, 0 load]
*Mar  8 22:38:52.640: Vi1 LCP: O TERMREQ [Open] id 13 len 4
*Mar  8 22:38:52.660: Vi1 IPCP: LCP not open, discarding packet
*Mar  8 22:38:52.776: Vi1 LCP: I TERMACK [TERMsent] id 13 len 4
*Mar  8 22:38:52.776: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar  8 22:38:52.780: Vi1 LCP: State is Closed
*Mar  8 22:38:52.780: Vi1 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  8 22:38:52.780: Vi1 VPDN: Cleanup
*Mar  8 22:38:52.780: Vi1 VPDN: Reset
*Mar  8 22:38:52.780: Vi1
Tnl/Cl 33/33 PPTP: close -> state change estabd to terminal
*Mar  8 22:38:52.780: Vi1 Tnl/Cl 33/33 PPTP:
Destroying session, trace follows:
*Mar  8 22:38:52.780: -Traceback= 60C4A150 60C4AE48 60C49F68 60C4B5AC
60C30450 60C18B10 60C19238 60602CC4 605FC380 605FB730 605FD614 605F72A8
6040DE0C 6040DDF8
*Mar  8 22:38:52.784: Vi1 Tnl/Cl 33/33 PPTP:
Releasing idb for tunnel 33 session 33
*Mar  8 22:38:52.784: Vi1 VPDN: Reset
*Mar  8 22:38:52.784: Tnl 33 PPTP:
no-sess -> state change estabd to wt-stprp
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
*Mar  8 22:38:52.784: Vi1 VPDN: Reset
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
```

Если клиент настроен для шифрования, а маршрутизатор – нет

Можно видеть следующее сообщение на ПК:

```
Registering your computer on the network..
Errror 742: The remote computer doesnot support the required data
encryption type.
On the Router:
*Mar  9 01:06:00.868: Vi2 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Mar  9 01:06:00.868: Vi2 CCP:    MS-PPC supported bits 0x010000B1
(0x1206010000B1)
*Mar  9 01:06:00.868: Vi2 LCP: O PROTREJ [Open] id 18 len 16 protocol CCP
(0x80FD0105000A1206010000B1)
*Mar  9 01:06:00.876: Vi2 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar  9 01:06:00.876: Vi2 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#1
1Z1`1k1}111
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 IPCP: Pool returned 172.16.10.1
*Mar  9 01:06:00.880: Vi2 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
```

```
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.884: Vi2 IPCP: I CONFACK [REQsent] id 8 len 10
*Mar  9 01:06:00.884: Vi2 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar  9 01:06:01.024: Vi2 LCP: I TERMREQ [Open] id 7 len 16
(0x79127FBE003CCD74000002E6)
*Mar  9 01:06:01.024: Vi2 LCP: O TERMACK [Open] id 7 len 4
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: ClearReq -> state change
estabd to terminal
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: Destroying session, trace
follows:
*Mar  9 01:06:01.152: -Traceback= 60C4A150 60C4AE48 60C49F68 60C4B2CC
60C4B558 60C485E0 60C486E0 60C48AB8 6040DE0C 6040DDF8
*Mar  9 01:06:01.156: Vi2 Tnl/Cl 38/38 PPTP: Releasing idb for tunnel 38
session 38
*Mar  9 01:06:01.156: Vi2 VPDN: Reset
*Mar  9 01:06:01.156: Tnl 38 PPTP: no-sess -> state change estabd to
wt-stprp
*Mar  9 01:06:01.160: %LINK-3-UPDOWN: Interface Virtual-Access2, changed
state to down
*Mar  9 01:06:01.160: Vi2 LCP: State is Closed
*Mar  9 01:06:01.160: Vi2 IPCP: State is Closed
*Mar  9 01:06:01.160: Vi2 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  9 01:06:01.160: Vi2 VPDN: Cleanup
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: AAA/MEMORY: free_user (0x6273D528) user='tac' ruser=''
port='Virtual-Access2' rem_addr='' authen_type=MSCHAP service=PPP priv=1
*Mar  9 01:06:01.324: Tnl 38 PPTP: StopCCRQ -> state change wt-stprp to wt-stprp
*Mar  9 01:06:01.324: Tnl 38 PPTP: Destroy tunnel
*Mar  9 01:06:02.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to down
```

Отключение MS-CHAP при настройке компьютера для шифрования

Можно видеть следующее сообщение на ПК:

```
The current encryption selection requires EAP or some version of
MS-CHAP logon security methods.
```

Если пользователь задает неверное имя пользователя или пароль, можно видеть следующий результат.

На ПК:

```
Verifying Username and Password..
Error 691: Access was denied because the username and/or password
was invalid on the domain.
```

На маршрутизаторе:

```
*Mar  9 01:13:43.192: RADIUS: Received from id 139 10.200.20.245:1645,
Access-Reject, len 42
*Mar  9 01:13:43.192: Attribute 26 22 0000013702101545
*Mar  9 01:13:43.192: AAA/AUTHEN (608505327): status = FAIL
*Mar  9 01:13:43.192: Vi2 CHAP: Unable to validate Response. Username tac:
Authentication failure
*Mar  9 01:13:43.192: Vi2 MS-CHAP: O FAILURE id 21 len 13 msg is "E=691 R=0"
*Mar  9 01:13:43.192: Vi2 PPP: Phase is TERMINATING [0 sess, 0 load]
*Mar  9 01:13:43.192: Vi2 LCP: O TERMREQ [Open] id 20 len 4
```

```
*Mar  9 01:13:43.196: AAA/MEMORY: free_user (0x62740E7C) user='tac'
ruser='' port='Virtual-Access2' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
```

Когда сервер Radius недоступен

Можно видеть следующий результат на маршрутизаторе:

```
*Mar  9 01:18:32.944: RADIUS: Retransmit id 141
*Mar  9 01:18:42.944: RADIUS: Tried all servers.
*Mar  9 01:18:42.944: RADIUS: No valid server found. Trying any viable server
*Mar  9 01:18:42.944: RADIUS: Tried all servers.
*Mar  9 01:18:42.944: RADIUS: No response for id 141
*Mar  9 01:18:42.944: Radius: No response from server
*Mar  9 01:18:42.944: AAA/AUTHEN (374484072): status = ERROR
```

Дополнительные сведения

- PPTP с MPPE
- Страница технологии PPTP
- Общие сведения о VPDN (виртуальная частная коммутируемая сеть)
- Общие сведения о Radius
- Настройка конфигурации CiscoSecure ACS для аутентификации протокола PPTP маршрутизатора Windows
- Cisco Systems – техническая поддержка и документация