Contenido

Introducción

Este caso práctico documenta el diseño, la implementación, y el troubleshooting de la Autenticación doble de Cisco IOS®.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Access Servers del Cisco IOS Network (NAS)Cisco IOS Software Release 11.3(3a)T corriente del servidor de acceso de las AS5x00 Series.El acceso a la red se proporciona con el Public Switched Telephone Network (PSTN) usando los módems y los puertos del Integrated Services Digital Network (ISDN).
- CiscoSecure 2.2(2) para Unix.Authentication, Authorization, and Accounting (AAA) del Cisco

IOS que controla en los usuarios de marcación manual, hardware de acceso a través de marcado telefónico, y administradores de router.
- SecurID ACE/ServerImplementar la autenticación robusta usando los tokens del contraseña que se puede utilizar una sola vez (OTP).
- Base de datos Oracle - Base de datos SQL.Para salvar la base de datos de AAA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Antecedentes

¿Por qué la autenticación doble?

Refiera a la documentación de las contraseñas de uso único en ISDN que soporta para más información.

La Autenticación doble es necesaria soportar la implementación de una política de seguridad que todo el acceso externo (tal como viejo servicio de telefonía llano [POTS] /modem y ISDN) esté autenticado con la autenticación (bipartita) fuerte. Para habilitar esta directiva, OTP-generando los tokens del SecurID se proporciona a los usuarios. El usuario entonces utiliza típicamente un módem para controlar una sesión con la red. Puesto que el usuario está en el teclado que controla a la sesión PPP, pueden ingresar la CONTRASEÑA de dos porciones para tener el acceso a la red según lo necesitado.

Sin embargo, cuando el dispositivo del usuario casero es un router basado en LAN, utiliza típicamente un algoritmo automatizado del Dial-on-Demand Routing (DDR) para determinar cuando establecer y liberar las conexiones conmutadas de circuitos (llamadas telefónicas a través de la red telefónica). Además, el código DDR prevé agregar las llamadas adicionales si la carga dicta.

Términos y definiciones

Token

dispositivo del usuario final que genera el OTP para cada login distinto

OTP

contraseña de USO único

PIN

el código secreto del usuario (segunda parte de bipartita/autenticación robusta)

CONTRASEÑA

contraseña requerida por el SecurID ACE/Server para esta autenticación

La Autenticación doble es:

- La autenticación mediante hardware es autenticación del router a router usando el Challenge Handshake Authentication Protocol (CHAP).
- La autenticación de usuario es autenticación de inicio de sesión vía Telnet usando el OTP y la modificación del Access Control List del perfil virtual (ACL) con el comando access-profile.

Los Perfiles virtuales utilizan los dos tipos de interfaz siguientes:

- La plantilla virtual se utiliza para reproducir las interfaces de acceso virtual.
- El acceso virtual se utiliza por las interfaces del usuario (router) PPP.

Los Perfiles virtuales y la Autenticación doble son características del Cisco IOS Release 11.3. Este documento incluye un conjunto de las configuraciones y de información del debug para ilustrar el diseño y el proceso de instrumentación de estas características.

Configuración de NAS en Cisco IOS

Para la brevedad, la información de la configuración proporcionada es solamente la mayoría de la información pertinente.

Comandos de configuración clave

Las interfaces de ISDN se lían en un grupo para soportar el Multilink PPP.

Los Perfiles virtuales y la Autenticación doble requieren el uso de las plantillas virtuales para reproducirse en la interfaz de acceso virtual. El perfil virtual es una combinación de la configuración de plantilla virtual y del AAA por los atributos de la autorización de usuario derivados del Terminal Access Controller Access Control System más (TACACS+).

Para soportar los grupos Hunt del multi-chasis, asegúrese de que la sesión telnet de la autenticación de usuario termina para arriba en el mismo NAS que la sesión PPP. Para soportar esto, configure el mismo Loopback IP Address en cada NAS de modo que los usuarios finales quieran siempre Telnet al mismo direccionamiento para la autenticación de usuario.

Al usar esta técnica, asegúrese que su Router ID del Open Shortest Path First (OSPF) es único en cada NAS (si usa el OSPF) y la propagación de esta ruta del host debe ser inhabilitada puesto que el direccionamiento es solamente relevante a los clientes PPP directamente conectados (es su dirección IP de la autenticación).

El ACL 110 bloquea el acceso a los servidores proxy de Internet y de Internet. Se aplica a los usuarios que se autentican con un token OTP (SecurID).

El ACL 120 es aplicado después de que el hardware autentique. Bloquea el acceso a cualquier dispositivo excepto Telnet al router local.

Si no configuran al **comando ip address-pool local** en el NAS, el código AAA puede requerir el perfil TACACS+ contener la información de direccionamiento tal como “addr-pool = valor por

defecto” o “addr el = 10.10.39.100". Este par del valor de atributo (AV) en el perfil TACACS+ puede hacer la Autenticación doble fallar, y es complicado para configurar para cada perfil. Aplique este comando una vez en la configuración del Cisco IOS, y el uso TACACS+ para por la dirección IP del usuario solamente (direccionamiento = a.b.c.d).

TACACS+ Perfiles para autenticación doble

Las configuraciones siguientes se están utilizando en el CiscoSecure para los perfiles de Unix TACACS+.

Perfil del hardware: nw76998-isdn

```
CiscoSecure: DEBUG - Profiles after Resolving Absolute Attributes: Jun 19 21:00:04 rapcs02d
group = hardware { Jun 19 21:00:04 rapcs02d        profile_id = 2850 Jun 19 21:00:04 rapcs02d
profile_cycle = 5 Jun 19 21:00:05 rapcs02d } Jun 19 21:00:05 rapcs02d group = isdn_rtr_blocked {
Jun 19 21:00:05 rapcs02d        service = ppp { Jun 19 21:00:05 rapcs02d                protocol
= lcp { Jun 19 21:00:05 rapcs02d                } Jun 19 21:00:05 rapcs02d
protocol = ip { Jun 19 21:00:05 rapcs02d                          set inacl = 120 Jun 19 21:00:05
rapcs02d                } Jun 19 21:00:05 rapcs02d                protocol = multilink { Jun 19
21:00:05 rapcs02d                } Jun 19 21:00:05 rapcs02d        } Jun 19 21:00:05 rapcs02d
profile_id = 2874 Jun 19 21:00:05 rapcs02d        profile_cycle = 6 Jun 19 21:00:05 rapcs02d
member = hardware Jun 19 21:00:05 rapcs02d } Jun 19 21:00:05 rapcs02d user = nw76998-isdn { Jun
19 21:00:05 rapcs02d        profile_id = 1284 Jun 19 21:00:05 rapcs02d        profile_cycle =
122 Jun 19 21:00:05 rapcs02d        member = isdn_rtr_blocked Jun 19 21:00:05 rapcs02d
password = chap "********" Jun 19 21:00:05 rapcs02d }
```

Perfil del usuario: nw76998

```
CiscoSecure: DEBUG - Profiles after Resolving Absolute Attributes: Jun 19 21:47:33 rapcs02d
group = dialup_users { Jun 19 21:47:33 rapcs02d        profile_id = 2875 Jun 19 21:47:33
rapcs02d        profile_cycle = 3 Jun 19 21:47:33 rapcs02d        password = pap "********" Jun
19 21:47:33 rapcs02d        password = sdi Jun 19 21:47:33 rapcs02d } Jun 19 21:47:33 rapcs02d
group = class110 { Jun 19 21:47:33 rapcs02d        service = ppp { Jun 19 21:47:33 rapcs02d
protocol = multilink { Jun 19 21:47:33 rapcs02d                } Jun 19 21:47:33 rapcs02d
protocol = lcp { Jun 19 21:47:33 rapcs02d                } Jun 19 21:47:33 rapcs02d
protocol = ip { Jun 19 21:47:33 rapcs02d                          set inacl = 110 Jun 19 21:47:34
rapcs02d                } Jun 19 21:47:34 rapcs02d                protocol = ccp { Jun 19
21:47:34 rapcs02d                } Jun 19 21:47:34 rapcs02d        } Jun 19 21:47:34 rapcs02d
service = shell { Jun 19 21:47:34 rapcs02d        } Jun 19 21:47:34 rapcs02d        profile_id =
2584 Jun 19 21:47:34 rapcs02d        profile_cycle = 3 Jun 19 21:47:34 rapcs02d        member =
dialup_users Jun 19 21:47:34 rapcs02d } Jun 19 21:47:34 rapcs02d user = nw76998 { Jun 19
21:47:34 rapcs02d        service = shell { Jun 19 21:47:34 rapcs02d        } Jun 19 21:47:34
rapcs02d        profile_id = 614 Jun 19 21:47:34 rapcs02d        set server current-failed-
logins = 0 Jun 19 21:47:34 rapcs02d        profile_cycle = 121 Jun 19 21:47:34 rapcs02d
member = class110 Jun 19 21:47:34 rapcs02d }
```

Sesión de autenticación doble de ejemplo

Captura de autenticación de hardware

Primero, autentican al router ISDN usando la GRIETA. Lo que sigue es la sesión del Cisco 700 puesta según lo ejecutado manualmente con fines ilustrativos.

```
    user-isdn:u2> sh sec     Profile Parameters          PPP Security            PPP
Authentication OUT   NONE<*>            Client              User Name              nw76998-
isdn<*>              PAP Password           NONE              CHAP Secret           EXISTS
Host             PAP Password           NONE              CHAP Secret           EXISTS
Callback             Request                OFF               Reply                 OFF
```

```
user-isdn:u2>      user-isdn:u2>      user-isdn:u2> sh conn      Connections    01/01/1995
21:55:26          Start Date & Time   #  Name      #     Ethernet        1 01/01/1995 00:00:00 #
# 00 00 00 00 00 00        3 01/01/1995 10:20:20 # u2         #        8 01/01/1995 21:47:09 #
access-gw1 #                  Link: 1 Channel:  1 Phone: 18007735048      user-isdn:u2>
user-isdn:u2> call ch2       L05  0  12105950050  Outgoing Call Initiated      user-isdn:u2>
user-isdn:u2>  L08  2  12105950050  Call Connected      user-isdn:u2>  Connection 3 Add     Link
1 Channel 2      user-isdn:u2>
```

Nota: El Cisco 700 está utilizando el nombre de usuario PPP nw76998-isdn. Éste es el user_id normal añadido como sufijo con - el isdn para denotar el hardware asociado a este usuario.

El producto siguiente aparece en los debugs del Cisco IOS (anotados con fines ilustrativos). Los debugs siguientes se están ejecutando para esta captura.

```
    rap523#sh debug      General OS:        AAA Authentication debugging is on        AAA
Authorization debugging is on        AAA Per-user attributes debugging is on      Generic IP:
IP peer address activity debugging is on      PPP:        PPP authentication debugging is on
PPP protocol negotiation debugging is on      VTEMPLATE:        Virtual Template debugging is on
rap523#sh user          Line     User      Host(s)                  Idle Location      * 50 vty
0   nw76998r  idle                 00:00:00 10.10.34.7                  rap523#          *Mar
4 23:22:08.910 cst: %LINK-3-UPDOWN: Interface Serial0:0, changed          state to up
*Mar  4 23:22:08.954 cst: Se0:0 PPP: Treating connection as a callin          *Mar  4
23:22:08.954 cst: Se0:0 PPP: Phase is ESTABLISHING, Passive Open          *Mar  4 23:22:08.958
cst: Se0:0 LCP: State is Listen          *Mar  4 23:22:09.990 cst: Se0:0 LCP: I CONFREQ
[Listen] id 1 len 31          *Mar  4 23:22:09.990 cst: Se0:0 LCP:    MRU 1522 (0x010405F2)
*Mar  4 23:22:09.994 cst: Se0:0 LCP:    MagicNumber 0x00100524          (0x050600100524)
*Mar  4 23:22:09.998 cst: Se0:0 LCP:    MRRU 1800 (0x11040708)          *Mar  4 23:22:10.002
cst: Se0:0 LCP:    EndpointDisc 3 0040.f911.4390          (0x1309030040F9114390)          *Mar
4 23:22:10.006 cst: Se0:0 LCP:    LinkDiscriminator 212 (0x170400D4)          *Mar  4
23:22:10.010 cst: Se0:0 LCP: O CONFREQ [Listen] id 81 len 34          *Mar  4 23:22:10.014 cst:
Se0:0 LCP:    AuthProto CHAP (0x0305C22305)          *Mar  4 23:22:10.018 cst: Se0:0 LCP:
MagicNumber 0x760859AF          (0x0506760859AF)          *Mar  4 23:22:10.022 cst: Se0:0 LCP:
MRRU 1524 (0x110405F4)          *Mar  4 23:22:10.026 cst: Se0:0 LCP:    EndpointDisc 1 Local
(0x130B017261705F64657631)          *Mar  4 23:22:10.026 cst: Se0:0 LCP:    LinkDiscriminator
193 (0x170400C1)          value = 0xD4          *Mar  4 23:22:10.034 cst: Se0:0 LCP: O CONFACK
[Listen] id 1 len 31          *Mar  4 23:22:10.038 cst: Se0:0 LCP:    MRU 1522 (0x010405F2)
*Mar  4 23:22:10.038 cst: Se0:0 LCP:    MagicNumber 0x00100524          (0x050600100524)
*Mar  4 23:22:10.042 cst: Se0:0 LCP:    MRRU 1800 (0x11040708)          *Mar  4 23:22:10.046
cst: Se0:0 LCP:    EndpointDisc 3 0040.f911.4390          (0x1309030040F9114390)          *Mar
4 23:22:10.050 cst: Se0:0 LCP:    LinkDiscriminator 212 (0x170400D4)          *Mar  4
23:22:10.490 cst: Se0:0 LCP: I CONFNAK [ACKsent] id 81 len 8          *Mar  4 23:22:10.494 cst:
Se0:0 LCP:    MRU 1522 (0x010405F2)          *Mar  4 23:22:10.498 cst: Se0:0 LCP: O CONFREQ
[ACKsent] id 82 len 34          *Mar  4 23:22:10.498 cst: Se0:0 LCP:    AuthProto CHAP
(0x0305C22305)          *Mar  4 23:22:10.502 cst: Se0:0 LCP:    MagicNumber 0x760859AF
(0x0506760859AF)          *Mar  4 23:22:10.506 cst: Se0:0 LCP:    MRRU 1524 (0x110405F4)
*Mar  4 23:22:10.510 cst: Se0:0 LCP:    EndpointDisc 1 Local          (0x130B017261705F64657631)
*Mar  4 23:22:10.514 cst: Se0:0 LCP:    LinkDiscriminator 193 (0x170400C1)          *Mar  4
23:22:10.594 cst: Se0:0 LCP: I CONFACK [ACKsent] id 82 len 34          *Mar  4 23:22:10.598
cst: Se0:0 LCP:    AuthProto CHAP (0x0305C22305)          *Mar  4 23:22:10.602 cst: Se0:0 LCP:
MagicNumber 0x760859AF          (0x0506760859AF)          *Mar  4 23:22:10.606 cst: Se0:0 LCP:
MRRU 1524 (0x110405F4)          *Mar  4 23:22:10.610 cst: Se0:0 LCP:    EndpointDisc 1 Local
(0x130B017261705F64657631)          *Mar  4 23:22:10.614 cst: Se0:0 LCP:    LinkDiscriminator
193 (0x170400C1)          *Mar  4 23:22:10.614 cst: Se0:0 LCP: State is Open          *Mar  4
23:22:10.618 cst: Se0:0 PPP: Phase is AUTHENTICATING, by this end          *Mar  4 23:22:10.622
cst: Se0:0 CHAP: O CHALLENGE id 38 len 29 from          "rap_dev1"          *Mar  4
23:22:10.906 cst: Se0:0 CHAP: I RESPONSE id 38 len 33 from          "nw76998-isdn"
*Mar  4 23:22:10.910 cst: Se0:0 PPP: Phase is FORWARDING          *Mar  4 23:22:11.142 cst:
Se0:0 PPP: Phase is AUTHENTICATING          *Mar  4 23:22:11.142 cst: Se0:0 CHAP: I RESPONSE id
38 len 33 from          "nw76998-isdn"          *Mar  4 23:22:11.150 cst: AAA/AUTHEN:
create_user (0x50928C)          user='nw76998-isdn'          ruser='' port='Serial0:0'
rem_addr='5123678085/50050' authen_type=CHAP          service=PPP priv=1          *Mar  4
23:22:11.158 cst: AAA/AUTHEN/START (286876619): port='Serial0:0'          list='' ACTION=LOGIN
service=PPP          *Mar  4 23:22:11.158 cst: AAA/AUTHEN/START (286876619): using "default"
```

```
list           *Mar  4 23:22:11.162 cst: AAA/AUTHEN (286876619): status = UNKNOWN           *Mar
4 23:22:11.166 cst: AAA/AUTHEN/START (286876619): METHOD=TACACS+           *Mar  4 23:22:11.166
cst: TAC+: send AUTHEN/START packet ver=193          id=286876619           *Mar  4 23:22:11.394
cst: TAC+: ver=193 id=286876619 received AUTHEN status          = PASS           *Mar  4
23:22:11.398 cst: AAA/AUTHEN (286876619): status = PASS           *Mar  4 23:22:11.406 cst:
AAA/AUTHOR/LCP Se0:0: Authorize LCP           *Mar  4 23:22:11.410 cst: AAA/AUTHOR/LCP Se0:0
(1891051227):          Port='Serial0:0' list='' service=NET           *Mar  4 23:22:11.410 cst:
AAA/AUTHOR/LCP: Se0:0 (1891051227)          user='nw76998-isdn'           *Mar  4 23:22:11.414
cst: AAA/AUTHOR/LCP: Se0:0 (1891051227) send AV          service=ppp           *Mar  4
23:22:11.418 cst: AAA/AUTHOR/LCP: Se0:0 (1891051227) send AV          protocol=lcp
*Mar  4 23:22:11.418 cst: AAA/AUTHOR/LCP (1891051227) found list "default"           *Mar  4
23:22:11.422 cst: AAA/AUTHOR/LCP: Se0:0 (1891051227) METHOD=TACACS+           *Mar  4
23:22:11.426 cst: AAA/AUTHOR/TAC+: (1891051227): user=nw76998-isdn           *Mar  4
23:22:11.430 cst: AAA/AUTHOR/TAC+: (1891051227): send AV          service=ppp           *Mar  4
23:22:11.430 cst: AAA/AUTHOR/TAC+: (1891051227): send AV          protocol=lcp           *Mar  4
23:22:12.326 cst: TAC+: (1891051227): received author response          status = PASS_ADD
*Mar  4 23:22:12.330 cst: AAA/AUTHOR (1891051227): Post authorization          status = PASS_ADD
*Mar  4 23:22:12.334 cst: Se0:0 CHAP: O SUCCESS id 38 len 4           *Mar  4 23:22:12.342 cst:
Se0:0 PPP: Phase is VIRTUALIZED           *Mar  4 23:22:12.370 cst: AAA/AUTHOR/MLP Se0:0
(3969993324):          Port='Serial0:0' list='' service=NET           *Mar  4 23:22:12.370 cst:
AAA/AUTHOR/MLP: Se0:0 (3969993324)          user='nw76998-isdn'           *Mar  4 23:22:12.374
cst: AAA/AUTHOR/MLP: Se0:0 (3969993324) send AV          service=ppp           *Mar  4
23:22:12.378 cst: AAA/AUTHOR/MLP: Se0:0 (3969993324) send AV          protocol=multilink
*Mar  4 23:22:12.378 cst: AAA/AUTHOR/MLP (3969993324) found list "default"           *Mar  4
23:22:12.382 cst: AAA/AUTHOR/MLP: Se0:0 (3969993324) METHOD=TACACS+           *Mar  4
23:22:12.386 cst: AAA/AUTHOR/TAC+: (3969993324): user=nw76998-isdn           *Mar  4
23:22:12.390 cst: AAA/AUTHOR/TAC+: (3969993324): send AV          service=ppp           *Mar  4
23:22:12.390 cst: AAA/AUTHOR/TAC+: (3969993324): send AV          protocol=multilink
*Mar  4 23:22:12.594 cst: Se0:0 IPCP: PPP phase is VIRTUALIZED, discarding          packet
*Mar  4 23:22:12.598 cst: TAC+: (3969993324): received author response          status =
PASS_ADD           *Mar  4 23:22:12.606 cst: AAA/AUTHOR (3969993324): Post authorization
status = PASS_ADD           *Mar  4 23:22:12.610 cst: Vi2 VTEMPLATE: Reuse Vi2, recycle queue
size 1           *Mar  4 23:22:12.614 cst: Vi2 VTEMPLATE: Set default settings with no ip
address           *Mar  4 23:22:13.030 cst: Se0:0 CCP: PPP phase is VIRTUALIZED, discarding
packet           *Mar  4 23:22:13.034 cst: Se0:0 BACP: I CONFREQ [Closed] id 1 len 10
*Mar  4 23:22:13.038 cst: Se0:0 BACP:    FavoredPeer 0xFFFFFFFF          (0x0106FFFFFFFF)
*Mar  4 23:22:13.042 cst: Se0:0 BACP: Lower layer not up, discarding packet           *Mar  4
23:22:13.074 cst: %LINEPROTO-5-UPDOWN: Line protocol on Interface          Serial 0:0, changed
state to up           *Mar  4 23:22:13.222 cst: Vi2 VTEMPLATE: Hardware address 0060.4780.b3c2
*Mar  4 23:22:13.226 cst: Vi2 PPP: Phase is DOWN, Setup           *Mar  4 23:22:13.230 cst: Vi2
VTEMPLATE: Has a new cloneblk vtemplate, now          it has vtemplate           *Mar  4
23:22:13.234 cst: Vi2 VTEMPLATE: Undo default settings           *Mar  4 23:22:14.610 cst: Vi2
VTEMPLATE: ************* CLONE VACCESS2          *****************           *Mar  4
23:22:14.610 cst: Vi2 VTEMPLATE: Clone from vtemplate1           interface Virtual-Access2
no ip address           encap ppp           ip unnumb loop 3           ppp authen chap pap
ppp multi           compress stac           end           *Mar  4 23:22:14.994 cst: %ISDN-6-
CONNECT: Interface Serial0:0 is now          connected to 5123678085 nw76998-isdn           *Mar
4 23:22:15.698 cst: Se0:0 IPCP: PPP phase is VIRTUALIZED, discarding          packet
*Mar  4 23:22:15.702 cst: Se0:0 CCP: PPP phase is VIRTUALIZED, discarding          packet
*Mar  4 23:22:15.706 cst: Se0:0 BACP: I CONFREQ [Closed] id 2 len 10           *Mar  4
23:22:15.710 cst: Se0:0 BACP:    FavoredPeer 0xFFFFFFFF          (0x0106FFFFFFFF)           *Mar
4 23:22:15.710 cst: Se0:0 BACP: Lower layer not up, discarding packet           *Mar  4
23:22:16.006 cst: %LINK-3-UPDOWN: Interface Virtual-Access2,          changed state to up
*Mar  4 23:22:16.014 cst: Vi2 PPP: Treating connection as a dedicated line           *Mar  4
23:22:16.014 cst: Vi2 PPP: Phase is ESTABLISHING, Active Open           *Mar  4 23:22:16.022
cst: Vi2 LCP: O CONFREQ [Closed] id 1 len 30           *Mar  4 23:22:16.026 cst: Vi2 LCP:
AuthProto CHAP (0x0305C22305)           *Mar  4 23:22:16.026 cst: Vi2 LCP:    MagicNumber
0x7608712A          (0x05067608712A)           *Mar  4 23:22:16.030 cst: Vi2 LCP:    MRRU 1524
(0x110405F4)           *Mar  4 23:22:16.034 cst: Vi2 LCP:    EndpointDisc 1 Local
(0x130B017261705F64657631)           *Mar  4 23:22:16.042 cst: AAA/AUTHEN: dup_user (0x41E248)
user='nw76998-isdn' ruser='' port='Serial0:0'           rem_addr='5123678085/50050'
authen_type=CHAP service=PPP           priv=1 source='AAA dup mlp'           *Mar  4
23:22:16.046 cst: AAA/AUTHOR/MLP Vi2: Processing AV service=ppp           *Mar  4 23:22:16.046
cst: AAA/AUTHOR/MLP Vi2: Processing AV          protocol=multilink           *Mar  4
```

```
23:22:16.050 cst: Vi2 PPP: Phase is UP          *Mar  4 23:22:16.054 cst: AAA/AUTHOR/FSM Vi2:
(0): Can we start IPCP?          *Mar  4 23:22:16.058 cst: AAA/AUTHOR/FSM Vi2 (923557603):
Port='Serial0:0'          list='' service=NET          *Mar  4 23:22:16.062 cst:
AAA/AUTHOR/FSM: Vi2 (923557603)          user='nw76998-isdn'          *Mar  4 23:22:16.062 cst:
AAA/AUTHOR/FSM: Vi2 (923557603) send AV          service=ppp          *Mar  4 23:22:16.066 cst:
AAA/AUTHOR/FSM: Vi2 (923557603) send AV          protocol=ip          *Mar  4 23:22:16.070 cst:
AAA/AUTHOR/FSM (923557603) found list "default"          *Mar  4 23:22:16.070 cst:
AAA/AUTHOR/FSM: Vi2 (923557603) METHOD=TACACS+          *Mar  4 23:22:16.074 cst:
AAA/AUTHOR/TAC+: (923557603): user=nw76998-isdn          *Mar  4 23:22:16.078 cst:
AAA/AUTHOR/TAC+: (923557603): send AV service=ppp          *Mar  4 23:22:16.078 cst:
AAA/AUTHOR/TAC+: (923557603): send AV protocol=ip          *Mar  4 23:22:16.298 cst: TAC+:
(923557603): received author response          status = PASS_ADD          *Mar  4 23:22:16.306
cst: AAA/AUTHOR (923557603): Post authorization status          = PASS_ADD          *Mar  4
23:22:16.314 cst: AAA/AUTHOR/FSM Vi2: We can start IPCP          *Mar  4 23:22:16.318 cst: Vi2
IPCP: O CONFREQ [Closed] id 1 len 10          *Mar  4 23:22:16.322 cst: Vi2 IPCP:    Address
10.10.20.1 (0x03060A0A1401)          *Mar  4 23:22:16.326 cst: AAA/AUTHOR/FSM Vi2: (0): Can we
start CCP?          *Mar  4 23:22:16.330 cst: AAA/AUTHOR/FSM Vi2 (3515928500): Port='Serial0:0'
list='' service=NET          *Mar  4 23:22:16.330 cst: AAA/AUTHOR/FSM: Vi2 (3515928500)
user='nw76998-isdn'          *Mar  4 23:22:16.334 cst: AAA/AUTHOR/FSM: Vi2 (3515928500) send AV
service=ppp          *Mar  4 23:22:16.338 cst: AAA/AUTHOR/FSM: Vi2 (3515928500) send AV
protocol=ccp          *Mar  4 23:22:16.338 cst: AAA/AUTHOR/FSM (3515928500) found list
"default"          *Mar  4 23:22:16.342 cst: AAA/AUTHOR/FSM: Vi2 (3515928500) METHOD=TACACS+
*Mar  4 23:22:16.346 cst: AAA/AUTHOR/TAC+: (3515928500): user=nw76998-isdn          *Mar  4
23:22:16.346 cst: AAA/AUTHOR/TAC+: (3515928500): send AV          service=ppp          *Mar  4
23:22:16.350 cst: AAA/AUTHOR/TAC+: (3515928500): send AV          protocol=ccp          *Mar  4
23:22:16.370 cst: Se0:0 IPCP: PPP phase is VIRTUALIZED, discarding          packet
*Mar  4 23:22:16.582 cst: TAC+: (3515928500): received author response          status = FAIL
*Mar  4 23:22:16.586 cst: AAA/AUTHOR (3515928500): Post authorization          status = FAIL
*Mar  4 23:22:16.590 cst: AAA/AUTHOR/FSM Vi2: We cannot start CCP          *Mar  4 23:22:16.594
cst: Vi2 CCP: State is Closed          *Mar  4 23:22:17.518 cst: %LINEPROTO-5-UPDOWN: Line
protocol on Interface          Virtual-Access2, changed state to up          *Mar  4
23:22:19.266 cst: Vi2 IPCP: I CONFREQ [REQsent] id 3 len 10          *Mar  4 23:22:19.270 cst:
Vi2 IPCP:    Address 172.20.1.1 (0x0306AC140101)          *Mar  4 23:22:19.274 cst:
AAA/AUTHOR/IPCP Vi2: Start.  Her address          172.20.1.1, we want 0.0.0.0          *Mar  4
23:22:19.278 cst: AAA/AUTHOR/IPCP Vi2 (3421422059):          Port='Serial0:0' list=''
service=NET          *Mar  4 23:22:19.282 cst: AAA/AUTHOR/IPCP: Vi2 (3421422059)
user='nw76998-isdn'          *Mar  4 23:22:19.286 cst: AAA/AUTHOR/IPCP: Vi2 (3421422059) send
AV          service=ppp          *Mar  4 23:22:19.286 cst: AAA/AUTHOR/IPCP: Vi2 (3421422059)
send AV          protocol=ip          *Mar  4 23:22:19.290 cst: AAA/AUTHOR/IPCP: Vi2
(3421422059) send AV          addr*172.20.1.1          *Mar  4 23:22:19.294 cst:
AAA/AUTHOR/IPCP (3421422059) found list "default"          *Mar  4 23:22:19.294 cst:
AAA/AUTHOR/IPCP: Vi2 (3421422059) METHOD=TACACS+          *Mar  4 23:22:19.298 cst:
AAA/AUTHOR/TAC+: (3421422059): user=nw76998-isdn          *Mar  4 23:22:19.302 cst:
AAA/AUTHOR/TAC+: (3421422059): send AV          service=ppp          *Mar  4 23:22:19.302 cst:
AAA/AUTHOR/TAC+: (3421422059): send AV          protocol=ip          *Mar  4 23:22:19.306 cst:
AAA/AUTHOR/TAC+: (3421422059): send AV          addr*172.20.1.1          *Mar  4 23:22:19.362
cst: Vi2 IPCP: TIMEout: Time 0x15C08D5C State REQsent          *Mar  4 23:22:19.366 cst: Vi2
IPCP: O CONFREQ [REQsent] id 2 len 10          *Mar  4 23:22:19.370 cst: Vi2 IPCP:    Address
10.10.20.1 (0x03060A0A1401)          *Mar  4 23:22:19.550 cst: Vi2 PPP: Unsupported or un-
negotiated protocol.          Link ip          *Mar  4 23:22:19.746 cst: TAC+: (3421422059):
received author response          status = PASS_REPL          *Mar  4 23:22:19.754 cst:
AAA/AUTHOR (3421422059): Post authorization          status = PASS_REPL          *Mar  4
23:22:19.762 cst: AAA/AUTHOR/IPCP Vi2: Reject 172.20.1.1, using          0.0.0.0          *Mar
4 23:22:19.766 cst: AAA/AUTHOR/IPCP Vi2: Processing AV service=ppp          *Mar  4
23:22:19.766 cst: AAA/AUTHOR/IPCP Vi2: Processing AV protocol=ip          *Mar  4 23:22:19.770
cst: AAA/AUTHOR/IPCP Vi2: Processing AV inacl=120          *Mar  4 23:22:19.774 cst: Vi2
VTEMPLATE: Has a new cloneblk AAA, now it has          vtem plate/AAA          *Mar  4
23:22:19.778 cst: Vi2 VTEMPLATE: ************ CLONE VACCESS2          ****************
*Mar  4 23:22:19.782 cst: Vi2 VTEMPLATE: Clone from AAA          interface Virtual-Access2
IP access-group 120 in          end          *Mar  4 23:22:20.070 cst: Vi2 AAA/AUTHOR: Vaccess
parse 'interface          Virtual-Access2          IP access-group 120 in          ' ok (0)
*Mar  4 23:22:20.074 cst: AAA/AUTHOR/IPCP Vi2: Processing AV addr*0.0.0.0          *Mar  4
23:22:20.074 cst: AAA/AUTHOR/IPCP Vi2: Authorization succeeded          *Mar  4 23:22:20.078
cst: AAA/AUTHOR/IPCP Vi2: Done.  Her address          172.20.1.1, we want 0.0.0.0          *Mar
```

```
4 23:22:20.082 cst: ip_get_pool: Vi2: validate address = 172.20.1.1           *Mar  4
23:22:20.086 cst: ip_get_pool: Vi2: returning address =          10.10.42.132           *Mar  4
23:22:20.086 cst: set_ip_peer_addr: Vi2: address = 10.10.42.132 (3)          is redundant
*Mar  4 23:22:20.090 cst: Vi2 IPCP: O CONFNAK [REQsent] id 3 len 10           *Mar  4
23:22:20.094 cst: Vi2 IPCP:    Address 10.10.42.132          (0x03060A0A2A84)           *Mar  4
23:22:20.098 cst: Vi2 CCP: I CONFREQ [Closed] id 3 len 9           *Mar  4 23:22:20.102 cst: Vi2
CCP:    Stacker history 1 check mode LCB          (0x1105000101)           *Mar  4 23:22:20.106
cst: Vi2 CCP: Lower layer not up, discarding packet           *Mar  4 23:22:20.110 cst: Vi2
BACP: I CONFREQ [Not negotiated] id 3 len 10           *Mar  4 23:22:20.114 cst: Vi2 BACP:
FavoredPeer 0xFFFFFFFF          (0x0106FFFFFFFF)           *Mar  4 23:22:20.118 cst: Vi2 LCP: O
PROTREJ [Open] id 2 len 16 protocol          BACP (0xC02B0103000A0106FFFFFFFF)           *Mar  4
23:22:20.122 cst: Vi2 IPCP: I CONFACK [REQsent] id 2 len 10           *Mar  4 23:22:20.126 cst:
Vi2 IPCP:    Address 10.10.20.1 (0x03060A0A1401)           *Mar  4 23:22:20.318 cst: Vi2 IPCP: I
CONFREQ [ACKrcvd] id 4 len 10           *Mar  4 23:22:20.322 cst: Vi2 IPCP:    Address
10.10.42.132          (0x03060A0A2A84)           *Mar  4 23:22:20.326 cst: AAA/AUTHOR/IPCP Vi2:
Start.  Her address          10.10.42.132, we want 10.10.42.132           *Mar  4 23:22:21.174
cst: AAA/AUTHOR/IPCP Vi2 (2513491870):          Port='Serial0:0' list='' service=NET
*Mar  4 23:22:21.178 cst: AAA/AUTHOR/IPCP: Vi2 (2513491870)          user='nw76998-isdn'
*Mar  4 23:22:21.182 cst: AAA/AUTHOR/IPCP: Vi2 (2513491870) send AV          service=ppp
*Mar  4 23:22:21.182 cst: AAA/AUTHOR/IPCP: Vi2 (2513491870) send AV          protocol=ip
*Mar  4 23:22:21.186 cst: AAA/AUTHOR/IPCP: Vi2 (2513491870) send AV          addr*10.10.42.132
*Mar  4 23:22:21.190 cst: AAA/AUTHOR/IPCP (2513491870) found list "default"           *Mar  4
23:22:21.190 cst: AAA/AUTHOR/IPCP: Vi2 (2513491870) METHOD=TACACS+           *Mar  4
23:22:21.194 cst: AAA/AUTHOR/TAC+: (2513491870): user=nw76998-isdn           *Mar  4
23:22:21.198 cst: AAA/AUTHOR/TAC+: (2513491870): send AV          service=ppp           *Mar  4
23:22:21.198 cst: AAA/AUTHOR/TAC+: (2513491870): send AV          protocol=ip           *Mar  4
23:22:21.202 cst: AAA/AUTHOR/TAC+: (2513491870): send AV          addr*10.10.42.132
*Mar  4 23:22:21.538 cst: TAC+: (2513491870): received author response          status =
PASS_REPL           *Mar  4 23:22:21.546 cst: AAA/AUTHOR (2513491870): Post authorization
status = PASS_REPL           *Mar  4 23:22:21.554 cst: AAA/AUTHOR/IPCP Vi2: Reject 10.10.42.132,
using          10.10.42.132           *Mar  4 23:22:21.558 cst: AAA/AUTHOR/IPCP Vi2: Processing
AV service=ppp           *Mar  4 23:22:21.562 cst: AAA/AUTHOR/IPCP Vi2: Processing AV
protocol=ip           *Mar  4 23:22:21.562 cst: AAA/AUTHOR/IPCP Vi2: Processing AV inacl=120
*Mar  4 23:22:21.566 cst: Vi2 VTEMPLATE: Has a new cloneblk AAA, now it has          vtem
plate/AAA           *Mar  4 23:22:21.570 cst: Vi2 VTEMPLATE: ************* CLONE VACCESS2
*****************           *Mar  4 23:22:21.574 cst: Vi2 VTEMPLATE: Clone from AAA
interface Virtual-Access2           IP access-group 120 in           end           *Mar  4
23:22:21.866 cst: Vi2 AAA/AUTHOR: Vaccess parse 'interface          Virtual-Access 2 IP access-
group 120 in ' ok (0)           *Mar  4 23:22:21.870 cst: AAA/AUTHOR/IPCP Vi2: Processing AV
addr*10.10.42.132           *Mar  4 23:22:21.874 cst: AAA/AUTHOR/IPCP Vi2: Authorization
succeeded           *Mar  4 23:22:21.878 cst: AAA/AUTHOR/IPCP Vi2: Done.  Her address
10.10.42.132, we want 10.10.42.132           *Mar  4 23:22:21.878 cst: ip_get_pool: Vi2:
validate address = 10.10.42.132           *Mar  4 23:22:21.882 cst: ip_get_pool: Vi2: returning
address =          10.10.42.132           *Mar  4 23:22:21.886 cst: set_ip_peer_addr: Vi2:
address = 10.10.42.132 (3)          is redundant           *Mar  4 23:22:21.890 cst: Vi2 IPCP: O
CONFACK [ACKrcvd] id 4 len 10           *Mar  4 23:22:21.894 cst: Vi2 IPCP:    Address
10.10.42.132          (0x03060A0A2A84)           *Mar  4 23:22:21.894 cst: Vi2 IPCP: State is
Open           *Mar  4 23:22:21.902 cst: Vi2 CCP: I CONFREQ [Closed] id 4 len 9           *Mar
4 23:22:21.906 cst: Vi2 CCP:    Stacker history 1 check mode LCB          (0x1105000101)
*Mar  4 23:22:21.906 cst: Vi2 CCP: Lower layer not up, discarding packet           *Mar  4
23:22:21.914 cst: Vi2 AAA/AUTHOR: IP_UP           *Mar  4 23:22:21.914 cst: Vi2 AAA/PER-USER:
processing author params.           *Mar  4 23:22:21.922 cst: Vi2 IPCP: Install route to
10.10.42.132
```

Después de la autenticación mediante hardware, las sesiones PPP para usuario nw76998-isdn están estando dominaron por Virtual-Access2. La interfaz Serial0:0 es un miembro del agrupamiento de PPP de links múltiples Virtual-Access2.

```
    rap523#sh user          Line     User      Host(s)                  Idle Location      * 50
vty 0   nw76998r  idle                 00:00:00 10.10.34.7        Vi2        nw76998-i Virtual
PPP (Bundle) 00:02:13        Se0:0      nw76998-i Sync PPP             00:00:01
```

Utilice el comando show interface virx de asegurarse que los protocolos de control de red adecuada (NCP) están todavía abiertos (por ejemplo, el IP Control Protocol (IPCP)). Los

incidentes de la Autenticación doble pueden hacer los NCP apagar.

```
rap523#sh int vir2      Virtual-Access2 is up, line protocol is up        Hardware is Virtual
Access interface        Interface is unnumbered.  Using address of Loopback3 (10.10.20.1)
LCP Open, multilink Open        Closed: CCP        Open: IPCP     rap523#sh int vi2 conf
Virtual-Access2 is a MLP bundle interface      Building configuration...      interface Virtual-
Access2 configuration...      ip unnumbered Loopback3      ip access-group 120 in      no ip
mroute-cache      no fair-queue      compress stac      ppp max-bad-auth 3      ppp
authentication chap pap      ppp multilink      rap523#sh access-list      Extended IP access
list 100       deny ip any 10.25.16.0 0.0.15.255       deny ip any host 10.25.2.4       permit
ip any 10.0.0.0 0.255.255.255       deny ip any any      Extended IP access list 110       deny
ip any 10.25.16.0 0.0.15.255       permit ip any 10.0.0.0 0.255.255.255 (9503 matches)
deny ip any any (43 matches)      Extended IP access list 120       permit tcp any host
10.10.20.1 eq telnet (427 matches)       deny ip any any (16 matches)      rap523#
```

Después, las telnets del usuario de su PC a la dirección IP del Firewall en el NAS. En este diseño, el direccionamiento del Int Loopback 3 es 10.10.20.1.

Captura de autenticación de usuario

Acciones del usuario

El usuario abre una sesión con su identificación del usuario y OTP.

```
     rap523#sh int vi2 conf      Virtual-Access2 is a MLP bundle interface      Building
configuration...      interface Virtual-Access2 configuration...      ip unnumbered Loopback3
ip access-group 120 in      no ip mroute-cache      no fair-queue      compress stac      ppp
max-bad-auth 3      ppp authentication chap pap      ppp multilink      rap523#sh access-list
Extended IP access list 100       deny ip any 10.25.16.0 0.0.15.255       deny ip any host
10.25.2.4       permit ip any 10.0.0.0 0.255.255.255       deny ip any any      Extended IP
access list 110       deny ip any 10.25.16.0 0.0.15.255       permit ip any 10.0.0.0
0.255.255.255 (9503 matches)       deny ip any any (43 matches)      Extended IP access list 120
permit tcp any host 10.10.20.1 eq telnet (427 matches)       deny ip any any (16 matches)
rap523#
```

Utilizan al **comando access-profile merge** de cambiar la configuración activa. Si hay un error con la Autenticación doble, aparecerá antes del prompt de router siguiente.

```
rap523>access-profile merge      rap523>
```

Debugs del Cisco IOS de la autenticación de usuario

Capturan esta segunda autenticación y al **comando access-profile** en los debugs anotados del Cisco IOS. Una nueva sesión telnet hace el AAA preguntar el TACACS+ para el prompt del Nombre de usuario.

```
rap523>access-profile merge      rap523>
```

El TACACS+ autentica el nw76998 del usuario.

```
     *Mar  4 23:39:01.716 cst: TAC+: ver=192 id=2461152058 received AUTHEN status =     GETUSER
*Mar  4 23:39:01.720 cst: AAA/AUTHEN (2461152058): status = GETUSER      *Mar  4 23:39:05.596
cst: AAA/AUTHEN/CONT (2461152058): continue_login     (user='(undef)')      *Mar  4 23:39:05.600
cst: AAA/AUTHEN (2461152058): status = GETUSER      *Mar  4 23:39:05.600 cst: AAA/AUTHEN
(2461152058): METHOD=TACACS+      *Mar  4 23:39:05.604 cst: TAC+: send AUTHEN/CONT packet
id=2461152058      *Mar  4 23:39:05.808 cst: TAC+: ver=192 id=2461152058 received AUTHEN status
=     GETPASS      *Mar  4 23:39:05.812 cst: AAA/AUTHEN (2461152058): status = GETPASS      *Mar
4 23:39:15.316 cst: AAA/AUTHEN/CONT (2461152058): continue_login     (user='nw76998')      *Mar
4 23:39:15.320 cst: AAA/AUTHEN (2461152058): status = GETPASS      *Mar  4 23:39:15.320 cst:
AAA/AUTHEN (2461152058): METHOD=TACACS+      *Mar  4 23:39:15.324 cst: TAC+: send AUTHEN/CONT
packet id=2461152058      *Mar  4 23:39:16.632 cst: TAC+: ver=192 id=2461152058 received AUTHEN
```

status = PASS *Mar 4 23:39:16.632 cst: AAA/AUTHEN (2461152058): status = PASS

El TACACS+ autoriza el par AV del “service=shell” para el nw76998 del usuario.

*Mar 4 23:39:01.716 cst: TAC+: ver=192 id=2461152058 received AUTHEN status = GETUSER *Mar 4 23:39:01.720 cst: AAA/AUTHEN (2461152058): status = GETUSER *Mar 4 23:39:05.596 cst: AAA/AUTHEN/CONT (2461152058): continue_login (user='(undef)') *Mar 4 23:39:05.600 cst: AAA/AUTHEN (2461152058): status = GETUSER *Mar 4 23:39:05.600 cst: AAA/AUTHEN (2461152058): METHOD=TACACS+ *Mar 4 23:39:05.604 cst: TAC+: send AUTHEN/CONT packet id=2461152058 *Mar 4 23:39:05.808 cst: TAC+: ver=192 id=2461152058 received AUTHEN status = GETPASS *Mar 4 23:39:05.812 cst: AAA/AUTHEN (2461152058): status = GETPASS *Mar 4 23:39:15.316 cst: AAA/AUTHEN/CONT (2461152058): continue_login (user='nw76998') *Mar 4 23:39:15.320 cst: AAA/AUTHEN (2461152058): status = GETPASS *Mar 4 23:39:15.320 cst: AAA/AUTHEN (2461152058): METHOD=TACACS+ *Mar 4 23:39:15.324 cst: TAC+: send AUTHEN/CONT packet id=2461152058 ***Mar 4 23:39:16.632 cst: TAC+: ver=192 id=2461152058 received AUTHEN status = PASS** *Mar 4 23:39:16.632 cst: AAA/AUTHEN (2461152058): status = PASS

Cuando el usuario ejecuta el comando access-profile en su sesión telnet, hace la Autenticación doble del Cisco IOS ejecutar la asociación del Grieta-usuario nw76998-isdn al nw76998 del usuario que ingresa al sistema.

Mar 4 23:39:26.568 cst: ACCESS-PROFILE/10.10.42.132: Started *Mar 4 23:39:26.568 cst: Vi2 ACCESS-PROFILE: Chap-user nw76998-isdn login-user nw76998 src-addr 10.10.42.132 *Mar 4 23:39:26.576 cst: Vi2 ACCESS-PROFILE/IPCP: Attempting to re-authorize. user nw76998 src-addr 10.10.42.132** *Mar 4 23:39:26.580 cst: AAA/AUTHOR/FSM Vi2: (0): Can we start IPCP? *Mar 4 23:39:26.580 cst: AAA/AUTHOR/FSM Vi2 (2696786804): Port='Serial0:0' list ='' service=NET *Mar 4 23:39:26.584 cst: AAA/AUTHOR/FSM: Vi2 (2696786804) user='nw76998' *Mar 4 23:39:26.588 cst: AAA/AUTHOR/FSM: Vi2 (2696786804) send AV service=ppp *Mar 4 23:39:26.588 cst: AAA/AUTHOR/FSM: Vi2 (2696786804) send AV protocol=ip *Mar 4 23:39:26.592 cst: AAA/AUTHOR/FSM (2696786804) found list "default" *Mar 4 23:39:26.596 cst: AAA/AUTHOR/FSM: Vi2 (2696786804) METHOD=TACACS+ *Mar 4 23:39:26.600 cst: AAA/AUTHOR/TAC+: (2696786804): user=nw76998 *Mar 4 23:39:26.600 cst: AAA/AUTHOR/TAC+: (2696786804): send AV service=ppp *Mar 4 23:39:26.604 cst: AAA/AUTHOR/TAC+: (2696786804): send AV protocol=ip *Mar 4 23:39:26.816 cst: TAC+: (2696786804): received author response status = PASS_ADD *Mar 4 23:39:26.824 cst: AAA/AUTHOR (2696786804): Post authorization status = PASS_ADD ***Mar 4 23:39:26.832 cst: AAA/AUTHOR/FSM Vi2: We can start IPCP *Mar 4 23:39:26.836 cst: Vi2 ACCESS-PROFILE/IPCP: AV: service=ppp *Mar 4 23:39:26.836 cst: Vi2 ACCESS-PROFILE/IPCP: AV: protocol=ip *Mar 4 23:39:26.840 cst: Vi2 ACCESS-PROFILE/IPCP: AV: inacl=110 *Mar 4 23:39:26.844 cst: Vi2 ACCESS-PROFILE/ACL: Interface has input access list: 120 *Mar 4 23:39:26.848 cst: Vi2 VTEMPLATE: Has a new cloneblk AAA, now it has vtem plate/AAA *Mar 4 23:39:26.852 cst: Vi2 VTEMPLATE: ******* CLONE VACCESS2 ******** *Mar 4 23:39:26.856 cst: Vi2 VTEMPLATE: Clone from AAA interface Virtual-Access2 no ip access-group 120 in end** *Mar 4 23:39:27.196 cst: Vi2 AAA/AUTHOR: Vaccess parse 'interface Virtual-Access2 no ip access-group 120 in' ok (0) *Mar 4 23:39:27.200 cst: Vi2 ACCESS-PROFILE/IPCP: Reauthorization success! user nw76998 src-addr 10.10.42.132 *Mar 4 23:39:27.204 cst: Vi2 ACCESS-PROFILE/CCP: Attempting to re-authorize. user nw76998 src-addr 10.10.42.132 *Mar 4 23:39:27.208 cst: AAA/AUTHOR/FSM Vi2: (0): Can we start CCP? *Mar 4 23:39:27.212 cst: AAA/AUTHOR/FSM Vi2 (107142084): Port='Serial0:0' list= '' service=NET *Mar 4 23:39:27.216 cst: AAA/AUTHOR/FSM: Vi2 (107142084) user='nw76998' *Mar 4 23:39:27.216 cst: AAA/AUTHOR/FSM: Vi2 (107142084) send AV service=ppp *Mar 4 23:39:27.220 cst: AAA/AUTHOR/FSM: Vi2 (107142084) send AV protocol=ccp *Mar 4 23:39:27.224 cst: AAA/AUTHOR/FSM (107142084) found list "default" *Mar 4 23:39:27.224 cst: AAA/AUTHOR/FSM: Vi2 (107142084) METHOD=TACACS+ *Mar 4 23:39:27.228 cst: AAA/AUTHOR/TAC+: (107142084): user=nw76998 *Mar 4 23:39:27.232 cst: AAA/AUTHOR/TAC+: (107142084): send AV service=ppp *Mar 4 23:39:27.232 cst: AAA/AUTHOR/TAC+: (107142084): send AV protocol=ccp *Mar 4 23:39:28.140 cst: TAC+: (107142084): received author response status = PASS_ADD *Mar 4 23:39:28.148 cst: AAA/AUTHOR (107142084): Post authorization status = PASS_ADD *Mar 4 23:39:28.152 cst: AAA/AUTHOR/FSM Vi2: We can start CCP *Mar 4 23:39:28.156 cst: Vi2 ACCESS-PROFILE/CCP: AV: service=ppp *Mar 4 23:39:28.156 cst: Vi2 ACCESS-PROFILE/CCP: AV: protocol=ccp *Mar 4 23:39:28.160 cst: Vi2 ACCESS-PROFILE/CCP: Protocol not yet implemented. user nw76998 src-addr 10.10.42.132 *Mar 4 23:39:28.164 cst: Vi2 ACCESS-PROFILE/CCP: Reauthorization success! user nw76998 src-addr 10.10.42.132 *Mar 4 23:39:28.168 cst: Vi2 ACCESS-PROFILE: Done

La nueva configuración del comando show interface virtual-access2 se confirma abajo. Note que la lista de acceso 110 no era aplicada. Esto todavía necesita ser resuelta.

```
rap523>sh int virtual-access 2 conf      Virtual-Access2 is a MLP bundle interface      Building
configuration...      interface Virtual-Access2 configuration...      ip unnumbered Loopback3
no ip mroute-cache      no fair-queue      compress stac      ppp max-bad-auth 3      ppp
authentication chap pap      ppp multilink      rap523>sh int virtual-access2      Virtual-
Access2 is up, line protocol is up        Hardware is Virtual Access interface        Interface
is unnumbered.  Using address of Loopback3 (10.10.20.1)        MTU 1500 bytes, BW 56 Kbit, DLY
100000 usec, rely 255/255, load 4/255        Encapsulation PPP, loopback not set, keepalive set
(10 sec)        DTR is pulsed for 5 seconds on reset        LCP Open, multilink Open
Closed: CCP        Open: IPCP        Last input 00:00:00, output never, output hang never
Last clearing of "show interface" counters 00:32:14        Queueing strategy: fifo        Output
queue 0/40, 0 drops; input queue 1/75, 0 drops        5 minute input rate 1000 bits/sec, 4
packets/sec        5 minute output rate 1000 bits/sec, 3 packets/sec           153 packets
input, 6508 bytes, 0 no buffer           Received 141 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort           129 packets output,
10336 bytes, 0 underruns           0 output errors, 0 collisions, 0 interface resets           0
output buffer failures, 0 output buffers swapped out           0 carrier transitions
rap523>
```

Información Relacionada

- Soportar las contraseñas de uso único en ISDN
- Diseño TokenCaching y Guía de instalación
- Soporte Técnico y Documentación - Cisco Systems