Introduction

This case study documents the design, implementation, and troubleshooting of Cisco IOS® Double Authentication.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Network Access Servers (NAS)
  - AS5x00 series access server running Cisco IOS Software Release 11.3(3a)T.
  - Network access is provided through the Public Switched Telephone Network (PSTN) using modems and Integrated Services Digital Network (ISDN) ports.
- CiscoSecure 2.2(2) for Unix.
Controlling Cisco IOS Authentication, Authorization, and Accounting (AAA) on dialup users, dialup hardware, and router administrators.

- SecurID ACE/Server

- Implementing strong authentication using one−time password (OTP) tokens.
- Oracle Database – SQL Database.

- For storing the AAA database.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

Why Double Authentication?

Refer to the Supporting One−time Passwords on ISDN documentation for more information.

Double Authentication is necessary to support implementation of a security policy that all external access (such as plain old telephone service [POTS]/modem and ISDN) be authenticated with strong (two−part) authentication. To enable this policy, OTP−generating tokens from SecurID are provided to users. The user then typically uses a modem to control a session with the network. Since the user is at the keyboard controlling the PPP session, they can enter the two part PASSCODE to gain network access as needed.

However, when the home user's device is a LAN−based router, typically it uses an automated Dial−on−Demand Routing (DDR) algorithm to determine when to establish and release circuit−switched connections (phone calls through the phone network). Furthermore, the DDR code provides for adding additional calls if the load dictates.

Terms and Definitions

Token

end−user device that generates the OTP for each distinct login

OTP

one−time password

PIN

user's secret code (second part of two−part/strong authentication)

PASSCODE

password required by the SecurID ACE/Server for this authentication

Double Authentication is:
Hardware Authentication is router-to-router authentication using Challenge Handshake Authentication Protocol (CHAP).

User Authentication is login authentication via Telnet using OTP and modifying the Virtual Profile access control list (ACL) with the access-profile command.

Virtual Profiles use the following two interface types:

- Virtual Template is used to clone Virtual Access interfaces.
- Virtual Access is used per user (router) PPP interfaces.

Virtual Profiles and Double Authentication are features of Cisco IOS release 11.3. This document includes a set of configurations and debug information to illustrate the design and implementation process of these features.

**Configuring the Cisco IOS NAS**

For brevity, the configuration information provided is only the most relevant information.

```
CiscoIOS (tm) 5200 Software (C5200-LS-L), Version 11.3(3a)T,
RELEASE SOFTWARE (fc1)
System image file is "flash:c5200-1.113-3a.T.bin", booted via flash

Key Configuration Commands

```
```text
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 15 default tacacs+ if-authenticated
aaa authorization network default tacacs+ if-authenticated
```

The ISDN interfaces are bundled into a group to support Multilink PPP.

```
interface Serial0:23
dialer rotary-group 1
!
interface Serial1:23
dialer rotary-group 1
!
interface Dialer1
description - master for 'dialer rotary-group 1'
```

Virtual Profiles and Double Authentication require the use of Virtual Templates for cloning into the Virtual Access interface. The Virtual Profile is a combination of the Virtual Template configuration and the AAA per user authorization attributes derived from Terminal Access Controller Access Control System Plus (TACACS+).

```
virtual-profile virtual-template 1
virtual-profile aaa
!
interface Virtual-Template1
ip unnumbered Loopback3
no ip mroute-cache
ppp authentication chap pap
ppp multilink
```
To support multi-chassis hunt groups, ensure that the user authentication Telnet session ends up on the same NAS as the PPP session. To support this, configure the same loopback IP address on each NAS so that end users will always Telnet to the same address for user authentication.

When using this technique, ensure your Open Shortest Path First (OSPF) router ID is unique on each NAS (if using OSPF) and propagation of this host route should be disabled since the address is only relevant to directly connected PPP clients (it is their authentication IP address).

```
interface Loopback3
ip address 10.10.20.1 255.255.255.255
```

ACL 110 blocks access to the Internet and Internet proxy servers. It is applied to users who are authenticated with an OTP (SecurID) token.

```
access-list 110 deny ip any 10.25.16.0 0.0.15.255
access-list 110 permit ip any 10.0.0.0 0.255.255.255
access-list 110 deny ip any any
```

ACL 120 is applied after the hardware authenticates. It blocks access to any device except Telnet to the local router.

```
access-list 120 permit tcp any host 10.10.20.1 eq telnet
access-list 120 deny ip any any
```

If the `ip address-pool local` command is not configured on the NAS, the AAA code may require the TACACS+ profile to contain addressing information such as "addr-pool = default" or "addr = 10.10.39.100". This attribute-value (AV) pair on the TACACS+ profile can cause Double Authentication to fail, and is more complicated to configure for each profile. Apply this command once in the Cisco IOS configuration, and use TACACS+ for the per user IP address only (address = a.b.c.d).

```
ip address-pool local
ip local pool default 10.10.42.93 10.10.42.139
```

**TACACS+ Profiles for Double Authentication**

The following configurations are being used on CiscoSecure for Unix TACACS+ profiles.

**Hardware Profile: 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 set inacl = 120
Jun 19 21:00:05 rapcs02d } protocol = ip {
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 group = hardware {
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 } user = nw76998-isdn {
```
User Profile: nw76998

CiscoSecure: DEBUG - Profiles after Resolving Absolute Attributes:

Sample Double Authentication Session

Hardware Authentication Capture

First, the ISDN router is authenticated using CHAP. Following is the Cisco 700 session setup as run manually for illustrative purposes.

```
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
```
Note: The Cisco 700 is using the PPP user name nw76998-isdn. This is the normal user_id suffixed with -isdn to denote the hardware associated with this user.

The following output appears on the Cisco IOS debugs (annotated for illustrative purposes). The following debugs are running for this capture.

```
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
```

```
*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
*Mar 4 23:22:09.998 cst: Se0:0 LCP: MRRU 1524 (0x110405F4)
*Mar 4 23:22:09.998 cst: Se0:0 LCP: EndpointDisc 1 Local (0x130B017261705F64657631)
```

```
*Mar 4 23:22:09.998 cst: Se0:0 LCP: MagicNumber 0x760859AF
*Mar 4 23:22:09.998 cst: Se0:0 LCP: LinkDiscriminator 212 (0x170400D4)
*Mar 4 23:22:10.014 cst: Se0:0 LCP: AuthProto CHAP (0x0305C2232305)
*Mar 4 23:22:10.018 cst: Se0:0 LCP: MagicNumber 0x760859AF
```

```
*Mar 4 23:22:10.022 cst: Se0:0 LCP: MRRU 1800 (0x11040708)
*Mar 4 23:22:10.026 cst: Se0:0 LCP: EndpointDisc 3 0040.f911.4390
```

```
*Mar 4 23:22:10.030 cst: Se0:0 LCP: LinkDiscriminator 212 (0x170400D4)
*Mar 4 23:22:10.030 cst: Se0:0 LCP: O CONFREQ [Listen] id 1 len 34
```

```
*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:    MagicNumber 0x00100524
(0x050600100524)
*Mar  4 23:22:10.038 cst: Se0:0 LCP:    MRRU 1800 (0x11040708)
(0x1309030040F9114390)
*Mar  4 23:22:10.050 cst: Se0:0 LCP:    LinkDiscriminator 212 (0x170400D4)
*Mar  4 23:22:10.490 cst: Se0:0 LCP:    MagicNumber 0x760859AF
(0x0506760859AF)
*Mar  4 23:22:10.498 cst: Se0:0 LCP:    MRRU 1524 (0x110405F4)
*Mar  4 23:22:10.502 cst: Se0:0 LCP:    EndpointDisc 1 Local
(0x130B017261705F64657631)
*Mar  4 23:22:10.510 cst: Se0:0 LCP:    LinkDiscriminator 193 (0x170400C1)
*Mar  4 23:22:10.514 cst: Se0:0 LCP:    MagicNumber 0x760859AF
(0x0506760859AF)
*Mar  4 23:22:10.598 cst: Se0:0 LCP:    LinkDiscriminator 193 (0x170400C1)
*Mar  4 23:22:10.602 cst: Se0:0 LCP:    MagicNumber 0x760859AF
*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 23:22:10.616 cst: Se0:0 LCP:    State is Open
*Mar  4 23:22:10.618 cst: Se0:0 LCP:    PPP: Phase is AUTHENTICATING, by this end
"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 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
list='' ACTION=LOGIN service=PPP
*Mar  4 23:22:11.394 cst: TAC+: ver=193 id=286876619 received AUTHEN status = PASS
*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) send AV
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+
service=ppp
protocol=lcp
status = PASS_ADD
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
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+
service=ppp
protocol=multilink
*Mar 4 23:22:12.594 cst: Se0:0 IPCP: PPP phase is VIRTUALIZED, discarding
packet
status = PASS_ADD
status = PASS_ADD
*Mar 4 23:22:12.610 cst: Vi2 VTEMPLATE: Reuse Vi2, recycle queue size 1
address
*Mar 4 23:22:13.030 cst: Se0:0 CCP: PPP phase is VIRTUALIZED, discarding
packet
*Mar 4 23:22:13.038 cst: Se0:0 CCP: FavoredPeer 0xFFFFFFFF
(0x106FFFFFFFF)
*Mar 4 23:22:13.042 cst: Se0:0 CCP: Lower layer not up, discarding packet
Serial 0:0, changed state to up
it has vtemplate
 ****************
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 Serial10:0 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
(0x106FFFFFFFF)
*Mar 4 23:22:15.710 cst: Se0:0 BACP: Lower layer not up, discarding packet
*Mar 4 23:22:16.014 cst: Vi2 PPP: Phase is ESTABLISHING, Active Open
*Mar 4 23:22:16.026 cst: Vi2 LCP: AuthProto CHAP (0x0305C22305)
*Mar 4 23:22:16.026 cst: Vi2 LCP: MagicNumber 0x7608712A
*Mar 4 23:22:16.026 cst: Vi2 LCP: MagicNumber 0x0567608712A
*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)
user='nw76998−isdn' ruser='' port='Serial0:0'
rem_addr='5123678085/50050' authen_type=CHAP service=PPP
priv=1 source='AAA dup mlp'
*Mar 4 23:22:16.054 cst: AAA/AUTHOR/FSM Vi2: (0): Can we start IPCP?
list='' service=NET
*Mar 4 23:22:16.070 cst: AAA/AUTHOR/FSM (923557603) found list "default"
*Mar 4 23:22:16.314 cst: AAA/AUTHOR/FSM Vi2: We can start IPCP
*Mar 4 23:22:16.332 cst: V12 IPCP:  Address 10.10.20.1 (0x03060A1401)
list='' service=NET
*Mar 4 23:22:16.339 cst: AAA/AUTHOR/FSM (3515928500) found list "default"
*Mar 4 23:22:16.370 cst: Se0:0 IPCP: PPP phase is VIRTUALIZED, discarding packet
*Mar 4 23:22:16.590 cst: AAA/AUTHOR/FSM Vi2: We cannot start CCP
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
user="nw76998-isdn"
protocol=ip
addr=172.20.1.1
protocol=ip
addr=172.20.1.1
protocol=ip
Mar  4 23:22:19.362 cst: Vi2 IPCP: TIMEout: Time 0x15C08D5C State REQsent
Mar  4 23:22:19.370 cst: Vi2 IPCP: Address 10.10.20.1 (0x03060A0A1401)
Mar  4 23:22:19.762 cst: AAA/AUTHOR/IPCP Vi2: Reject 172.20.1.1, using 0.0.0.0
Mar  4 23:22:19.774 cst: Vi2 VTEMPLATE: Has a new cloneblk AAA, now it has vtem plate/AAA
IP access-group 120 in
end
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 23:22:20.078 cst: AAA/AUTHOR/IPCP Vi2: Done. Her address 172.20.1.1, we want 0.0.0.0
Mar  4 23:22:20.086 cst: set_ip_peer_addr: Vi2: address = 10.10.42.132 (3) is redundant
Mar  4 23:22:20.094 cst: Vi2 IPCP: Address 10.10.42.132
(0x03060A0A2A84)
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
    (0x0106FFFFFFFF)
*Mar 4 23:22:20.118 cst: Vi2 LCP: O PROTREJ [Open] id 2 len 16 protocol BACP (0x0C02B010300A0106FFFFFFFF)
*Mar 4 23:22:20.126 cst: Vi2 IPCP: Address 10.10.20.1 (0x03060A0A1401)
*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 23:22:21.190 cst: AAA/AUTHOR/IPCP (2513491870) found list "default"
*Mar 4 23:22:21.566 cst: Vi2 VTEMPLATE: Has a new cloneblk AAA, now it has vtem plate/AAA
*Mar 4 23:22:21.866 cst: Vi2 AAA/AUTHOR: Vaccess parse 'interface Virtual−Access 2 IP access−group 120 in ' ok (0)
*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 23:22:21.886 cst: set_ip_peer_addr: Vi2: address = 10.10.42.132 (3) is redundant
*Mar 4 23:22:21.894 cst: Vi2 IPCP: Address 10.10.42.132 (0x03060A0A2A84)
After the hardware authentication, the PPP session for user nw76998-isdn is being mastered by Virtual–Access2. Interface Serial0:0 is a member of the Virtual–Access2 Multilink PPP bundle.

Use the show interface virX command to ensure the proper Network Control Protocols (NCPs) are still open (for example, IP Control Protocol (IPCP)). Double Authentication failures can cause NCPs to shut down.

Next, the user Telnets from his PC to the firewall IP address in the NAS. In this design, the int loopback 3 address is 10.10.20.1.
User Authentication Capture

User Actions

The user logs on with their user ID and OTP.

User Access Verification

Username: nw76998
Enter PASSCODE:

The access−profile merge command is used to change the active configuration. If there is an error with Double Authentication, it will appear before the next router prompt.

\texttt{rap523>access-profile merge}
\texttt{rap523>}

Cisco IOS Debugs of User Authentication

This second authentication and the access−profile command is captured in the annotated Cisco IOS debugs. A new Telnet session causes AAA to query TACACS+ for the user name prompt.

*Mar 4 23:39:01.480 cst: AAA/AUTHEN: create_user (0x510FFC) user='' ruser='' port='tty51' rem_addr='10.10.42.132' authen_type=ASCII service=LOGIN priv=1
*Mar 4 23:39:01.484 cst: AAA/AUTHEN/START (2461152058): port='tty51' list='' ACTION=LOGIN service=LOGIN

TACACS+ authenticates the user nw76998.

*Mar 4 23:39:01.716 cst: AAA/AUTHEN: create_user (0x510FFC) user='' ruser='' port='tty51' rem_addr='10.10.42.132' authen_type=ASCII service=LOGIN priv=1
*Mar 4 23:39:05.596 cst: AAA/AUTHEN/CONT (2461152058): continue_login (user=('(undef)'))
*Mar 4 23:39:05.808 cst: TAC+: send AUTHEN/CONT packet ver=192 id=2461152058 received AUTHEN status = GETPASS
*Mar 4 23:39:15.316 cst: AAA/AUTHEN/CONT (2461152058): continue_login (user='nw76998')

TACACS+ authorizes the "service=shell" AV pair for the user nw76998.

*Mar 4 23:39:16.644 cst: AAA/AUTHOR/EXEC: (2900386803) user='nw76998'
*Mar 4 23:39:16.648 cst: AAA/AUTHOR/EXEC: (2900386803) send AV cmd*
*Mar 4 23:39:16.652 cst: AAA/AUTHOR/EXEC (2900386803) found list "default"
When the user executes the access−profile command in their Telnet session, it causes the Cisco IOS Double Authentication to execute associating the CHAP−user nw76998−isdn with the login−user nw76998.

```
*Mar 4 23:39:26.568 cst: Vi2 ACCESS−PROFILE:
  Chap-user nw76998−isdn login-user nw76998 src-addr 10.10.42.132
  Attempting to re-authorize. user nw76998 src-addr 10.10.42.132
```

```
  "" service=NET
*Mar 4 23:39:26.584 cst: AAA/AUTHOR/FSM: Vi2 (2696786804) user='nw76998'
*Mar 4 23:39:26.592 cst: AAA/AUTHOR/FSM (2696786804) found list "default"
```

```
*Mar 4 23:39:26.832 cst: AAA/AUTHOR/FSM Vi2: We can start IPCP
*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
```

```
  no ip access−group 120 in
```

```
*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 23:39:27.224 cst: AAA/AUTHOR/FSM (107142084) found list "default"
```

```
*Mar 4 23:39:27.228 cst: AAA/AUTHOR/TAC+: (107142084) user=nw76998
```
The new configuration of the show interface virtual-access2 command is confirmed below. Notice the access-list 110 was not applied. This still needs to be resolved.

```
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
```

Related Information

- Supporting One-time Passwords on ISDN
- TokenCaching Design and Implementation Guide
- Double Authentication Feature Guide
- CiscoSecure Server Manuals
- Technical Support & Documentation – Cisco Systems