

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Pourquoi Authentification double ?](#)

[Termes et définitions](#)

[Configurer le NAS de Cisco IOS](#)

[Commandes de configuration principales](#)

[Profils TACACS+ pour l'Authentification double](#)

[Profil de matériel : nw76998-isdn](#)

[Profil utilisateur : nw76998](#)

[Session d'Authentification double d'échantillon](#)

[Capture d'authentification de matériel](#)

[Capture d'authentification de l'utilisateur](#)

[Actions de l'utilisateur](#)

[Debugs de Cisco IOS de l'authentification de l'utilisateur](#)

[Informations connexes](#)

[Introduction](#)

Cette étude de cas documente la conception, l'implémentation, et le dépannage de l'Authentification double de Cisco IOS®.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveurs d'accès de réseau Cisco IOS (NAS) Logiciel Cisco IOS version 11.3(3a)T de serveur exécutant d'accès de gamme AS5x00. L'accès au réseau est fourni par le réseau téléphonique public commuté (PSTN) utilisant des Modems et des ports d'Integrated Services Digital Network (le RNIS).
- CiscoSecure 2.2(2) pour Unix. Authentification, autorisation et comptabilité (AAA) de contrôle

de Cisco IOS sur les utilisateurs de connexion téléphonique, le matériel commuté, et les administrateurs de routeur.

- SecurID ACE/Server Mise en oeuvre de l'authentification poussée utilisant les jetons une fois du mot de passe (OTP).
- Base de données d'Oracle - Base de données SQL. Pour enregistrer la base de données d'AAA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Pourquoi Authentification double ?

Référez-vous aux [mots de passe une fois les prenant en charge sur le](#) pour en savoir plus de documentation [RNIS](#).

L'Authentification double est nécessaire pour prendre en charge l'implémentation d'une stratégie de sécurité que tout l'accès externe (tel que réseau téléphonique public commuté [POTS] /modem et RNIS) soit authentifié avec l'authentification (en deux parties) forte. Pour activer cette stratégie, OTP-générateur des jetons de SecurID sont fournies aux utilisateurs. L'utilisateur utilise alors typiquement un modem pour contrôler une session avec le réseau. Puisque l'utilisateur est au clavier contrôlant la session PPP, ils peuvent écrire le CODE DE PASSAGE de deux parts pour gagner l'accès au réseau comme nécessaire.

Cependant, quand le périphérique de l'utilisateur privé est un routeur à base LAN, typiquement il emploie un algorithme automatisé de Routage à établissement de connexion à la demande (DDR) pour déterminer quand établir et libérer les connexions à commutation de circuits (appels téléphoniques par le réseau téléphonique). En outre, le code DDR prévoit ajouter des appels supplémentaires si le chargement dicte.

Termes et définitions

Jeton

périphérique d'utilisateur final qui génère l'OTP pour chaque procédure de connexion distincte

OTP

mot de passe une fois

PIN

le code secret de l'utilisateur (deuxième partie d'en deux parties/d'authentification poussée)

CODE DE PASSAGE

mot de passe requis par le SecurID ACE/Server pour cette authentification

L'Authentification double est :

- L'authentification de matériel est authentification de routeur à routeur utilisant le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol).
- L'authentification de l'utilisateur est authentification de connexion par l'intermédiaire de telnet utilisant OTP et modifier la liste de contrôle d'accès virtuelle de profil (ACL) avec la commande d'Access-profil.

Les Profils virtuels utilisent les deux types d'interface suivants :

- Le modèle virtuel est utilisé pour copier les interfaces d'Access virtuelles.
- Access virtuel est utilisé par interfaces de PPP d'utilisateur (routeur).

Les Profils virtuels et l'Authentification double sont des caractéristiques de Cisco IOS version 11.3. Ce document comporte un ensemble de configurations et met au point les informations pour montrer le processus de conception et réalisation de ces caractéristiques.

Configurer le NAS de Cisco IOS

Par souci de concision, les informations de configuration fournies sont seulement la plupart d'informations pertinentes.

Commandes de configuration principales

Les interfaces RNIS sont empaquetées dans un groupe pour prendre en charge le PPP à liaisons multiples.

Les Profils virtuels et l'Authentification double exigent l'utilisation des modèles virtuels pour copier dans l'interface d'Access virtuelle. Le profil virtuel est une combinaison de la configuration de modèle virtuel et de l'AAA par attributs d'autorisation d'utilisateur dérivés du Terminal Access Controller Access Control System Plus (TACACS+).

Pour prendre en charge des groupes de recherche de multi-châssis, assurez-vous que la session de telnet d'authentification de l'utilisateur finit par sur le même NAS que la session PPP. Pour prendre en charge ceci, configurez la même adresse IP de bouclage sur le chaque NAS de sorte que les utilisateurs finaux veuillent toujours le telnet à la même adresse pour l'authentification de l'utilisateur.

En utilisant cette technique, assurez que votre ID de routeur de Protocole OSPF (Open Shortest Path First) est seul sur le chaque NAS (si en utilisant l'OSPF) et la propagation de cette route hôte devrait être désactivée puisque l'adresse est seulement appropriée aux clients directement connectés de PPP (c'est leur adresse IP d'authentification).

ACL 110 blocs accès à Internet et serveurs proxys d'Internet. Il est appliqué aux utilisateurs qui sont authentifiés avec un jeton OTP (SecurID).

L'ACL 120 est appliqué après que le matériel authentifie. Il bloque l'accès à n'importe quel périphérique excepté le telnet au routeur local.

Si la commande locale d'ip address-pool n'est pas configurée sur le NAS, le code d'AAA peut exiger du profil TACACS+ de contenir les informations d'adressage telles que le « adr-groupe = le par défaut » ou le « adr = 10.10.39.100". Cette paire de l'attribut-valeur (poids du commerce) sur le profil TACACS+ peut faire échouer l'Authentification double, et est plus compliquée pour configurer pour chaque profil. Appliquez cette commande une fois dans la configuration Cisco IOS, et l'utilisation TACACS+ pour par adresse IP d'utilisateur seulement (adresse = a.b.c.d).

Profils TACACS+ pour l'Authentification double

Les configurations suivantes sont utilisées sur CiscoSecure pour des profils d'Unix TACACS+.

Profil de matériel : 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 }
```

Profil utilisateur : 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 }
```

Session d'Authentification double d'échantillon

Capture d'authentification de matériel

D'abord, le routeur RNIS est authentifié utilisant le CHAP. Être suit la session de Cisco 700 installée comme passage manuellement à des fins d'illustration.

| | | | |
|-----------------------------|--------------------|--------------|------------------|
| user-isdn:u2> sh sec | Profile Parameters | PPP Security | PPP |
| Authentication OUT | NONE<*> | Client | User Name |
| isdn<*> | PAP Password | NONE | nw76998- |
| | | 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>

```

Remarque: Le Cisco 700 utilise le nom d'utilisateur nw76998-isdn de PPP. C'est l'user_id normal suffixé avec - le RNIS pour dénoter le matériel associé avec cet utilisateur.

La sortie suivante apparaît sur le Cisco IOS met au point (annoté à des fins d'illustration). Ce qui suit met au point s'exécute pour cette 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      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 vtemplatel 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

```

Après l'authentification de matériel, la session PPP pour l'utilisateur que nw76998-isdn est a maîtrisé par Virtual-Access2. L'interface Serial0:0 est un membre de l'ensemble Multilink PPP 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

```


Utilisez la commande de virX d'interface d'exposition de s'assurer que les protocoles de contrôle de réseau appropriés (NCPs) sont encore ouverts (par exemple, protocole de contrôle IP (IPCP)). Les pannes d'Authentification double peuvent faire arrêter NCPs.

```
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#
```

Ensuite, les telnets d'utilisateur de son PC à l'adresse IP de Pare-feu dans le NAS. Dans cette conception, l'adresse du bouclage 3 international est 10.10.20.1.

Capture d'authentification de l'utilisateur

Actions de l'utilisateur

L'utilisateur ouvre une session avec leur user-id et 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#
```

La commande de fusion d'Access-profil est utilisée de changer la configuration active. S'il y a une erreur avec l'Authentification double, elle apparaîtra avant que la prochaine demande de routeur.

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

Debugs de Cisco IOS de l'authentification de l'utilisateur

Cette deuxième authentification et la commande d'Access-profil est capturée dans le Cisco IOS annoté met au point. Une nouvelle session de telnet fait questionner l'AAA TACACS+ pour la demande de nom d'utilisateur.

```
rap523>access-profile merge      rap523>
TACACS+ authentifie l'utilisateur nw76998.
```

```
*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
```

TACACS+ autorise la paire AV de « service=shell » pour l'utilisateur nw76998.

```
*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
```

Quand l'utilisateur exécute la commande d'Access-profil en leur session de telnet, elle fait exécuter l'Authentification double de Cisco IOS associer le CHAP-utilisateur nw76998-isdn avec l'utilisateur de connexion nw76998.

```
*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 nouvelle configuration de la commande de l'interface virtual-access2 d'exposition est confirmée ci-dessous. Notez que la liste d'accès 110 n'était pas appliquée. Ceci doit toujours être résolu.

```
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 runts, 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>
```

[Informations connexes](#)

- [Prendre en charge les mots de passe une fois sur le RNIS](#)
- [Guide de conception et d'implémentation de la mise en cache de jetons \(TokenCaching\)](#)
- [Support et documentation techniques - Cisco Systems](#)