Comment appliquer des listes d'accès pour les interfaces de numérotation avec un serveur TACACS+

Contenu

Introduction

Ce document explique comment appliquer des listes d'accès aux interfaces de numérotation avec un serveur TACACS+. Il existe deux méthodes possibles :

- Définissez la liste d’accès numérotée sur le routeur et référencez la liste d’accès numérotée sur le serveur. Ceci est pris en charge dans la plupart des versions du logiciel Cisco IOS®.
- Définissez l'intégralité de la liste d'accès sur le serveur. La version 11.3 ou ultérieure du logiciel Cisco IOS est requise pour cette méthode **par utilisateur**.

Remarque : Pour RNIS, vous devez utiliser la méthode **par utilisateur** et vous devez avoir des profils virtuels configurés sur le routeur.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Logiciel Cisco IOS Version 11.1 ou ultérieure (définition des listes d’accès sur le routeur)Logiciel Cisco IOS Version 11.3 ou ultérieure (définition des listes d'accès sur le serveur)
- Cisco Secure ACS pour UNIXCisco Secure ACS pour Windows 2.x et versions ultérieuresfreeware TACACS+

Remarque : Ce document suppose que l'accès à la numérotation a été précédemment configuré. Ce document ne traite pas des détails de la configuration de numérotation. Référez-vous à Configuration du NAS pour l'accès commuté de base pour plus d'informations sur la configuration d'un serveur d'accès réseau (NAS) pour la numérotation.

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

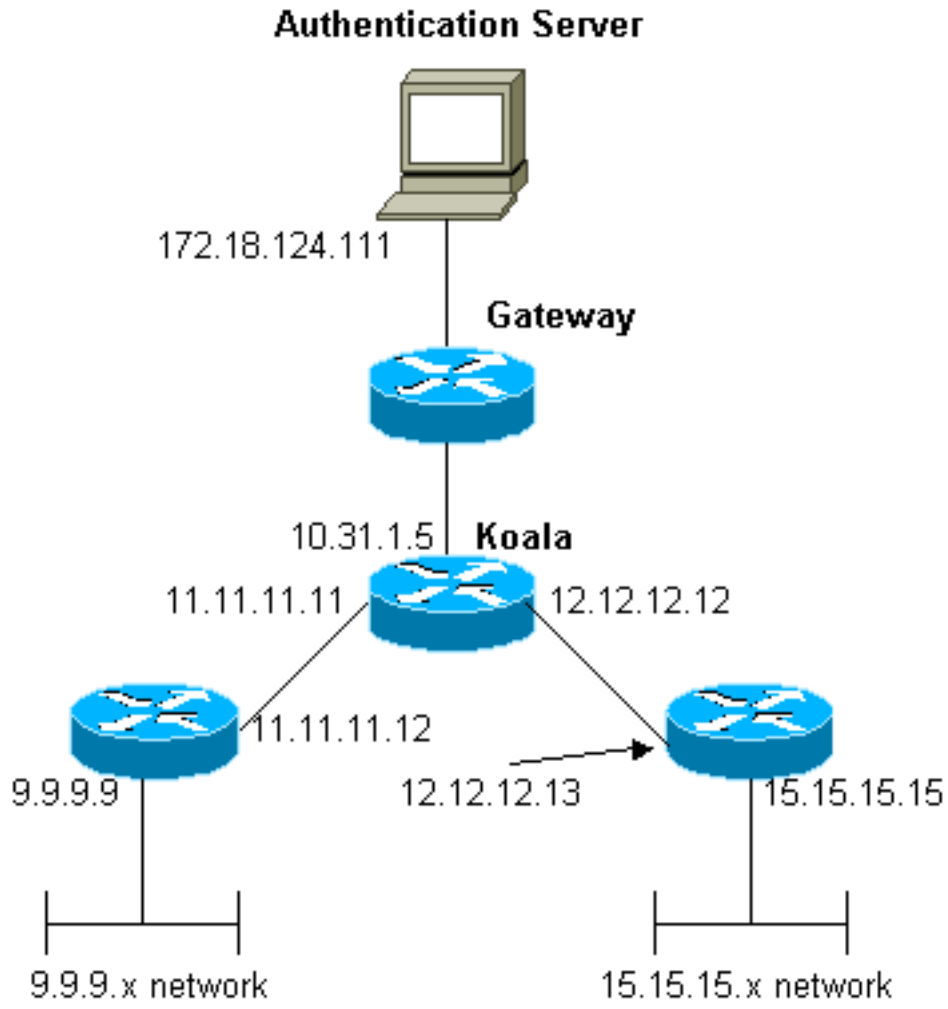
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez l’outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque : les configurations permettent à l'utilisateur qui reçoit une adresse 1.1.1.x de "'mypool » à ping (trafic ICMP) sur le réseau 9.9.9.x et Telnet (trafic TCP) vers le réseau 15.15.15.x. Il ne permet pas à l'utilisateur d'envoyer une requête ping au réseau 15.15.15.x ou Telnet vers le réseau 9.9.9.x.

Configurations

Ce document utilise les configurations suivantes.

- Routeur de la gamme Cisco 2500 exécutant le logiciel Cisco IOS Version 12.0(5)T
- Cisco Secure ACS pour UNIX 2.3
- Cisco Secure ACS pour Windows 3.2

Définir des listes d'accès numérotées sur le routeur

Routeur de la gamme Cisco 2500 qui exécute le logiciel Cisco IOS Version 12.0(5)T

`Current configuration:`
`!`
`version 12.0`
`service timestamps debug uptime`
`service timestamps log uptime`
`no service password-encryption`

```
!
hostname koala
!
aaa new-model
!
!--- These three lines of the configuration !--- are
specific to Cisco IOS Software Release 12.0.5.T and
later. !--- See the Commands for Other Cisco IOS
Releases section for commands !--- for other Cisco IOS
releases. ! aaa authentication login default local group
tacacs+
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable secret 5 $1$mnZQ$g6XdsgVnnYjEa.l7v.Pij1
enable password ww
!
username john password 0 doe
!
ip subnet-zero
!
cns event-service server
!
interface Ethernet0
ip address 10.31.1.5 255.255.255.0
no ip directed-broadcast
no mop enabled
!
interface Serial0
ip address 11.11.11.11 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface Serial1
ip address 12.12.12.12 255.255.255.0
no ip directed-broadcast
!
interface Async1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
async mode dedicated
peer default ip address pool mypool
fair-queue 64 16 0
no cdp enable
ppp authentication chap
!
ip local pool mypool 1.1.1.1 1.1.1.5
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
ip route 9.9.9.0 255.255.255.0 11.11.11.12
ip route 15.15.15.0 255.255.255.0 12.12.12.13
no ip http server
!
!--- Access list 101 is defined on the NAS. access-list
101 permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255
access-list 101 permit tcp 1.1.1.0 0.0.0.255 15.15.15.0
0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!--- Specify TACACS+ server host and key. tacacs-server
```

```
host 172.18.124.111
tacacs-server key cisco
!
line con 0
transport input none
line 1
modem InOut
transport input all
stopbits 1
speed 115200
flowcontrol hardware
line 2 16
line aux 0
line vty 0 4
password ww
!
end
```

Commandes pour d'autres versions de Cisco IOS

Remarque : afin d'utiliser ces commandes, supprimez les commandes en gras de la configuration du routeur de la gamme Cisco 2500 et collez ces commandes dans, comme indiqué dans votre version du logiciel Cisco IOS.

Logiciel Cisco IOS versions 11.3.3.T à 12.0.5.T

```
aaa authentication login default tacacs+ local
aaa authentication ppp default if-needed tacacs+ local
aaa authorization network default tacacs+
```

Logiciel Cisco IOS versions 11.1 à 11.3.3.T

```
aaa authentication login default tacacs+
aaa authentication ppp default if-needed tacacs+
aaa authorization network tacacs+
```

Configuration du serveur - logiciel gratuit TACACS+

```
user = chaprtr {
chap = cleartext chaprtr
service = ppp protocol = ip {
inacl=101
}
}
```

Configuration du serveur - Cisco Secure UNIX - TACACS+

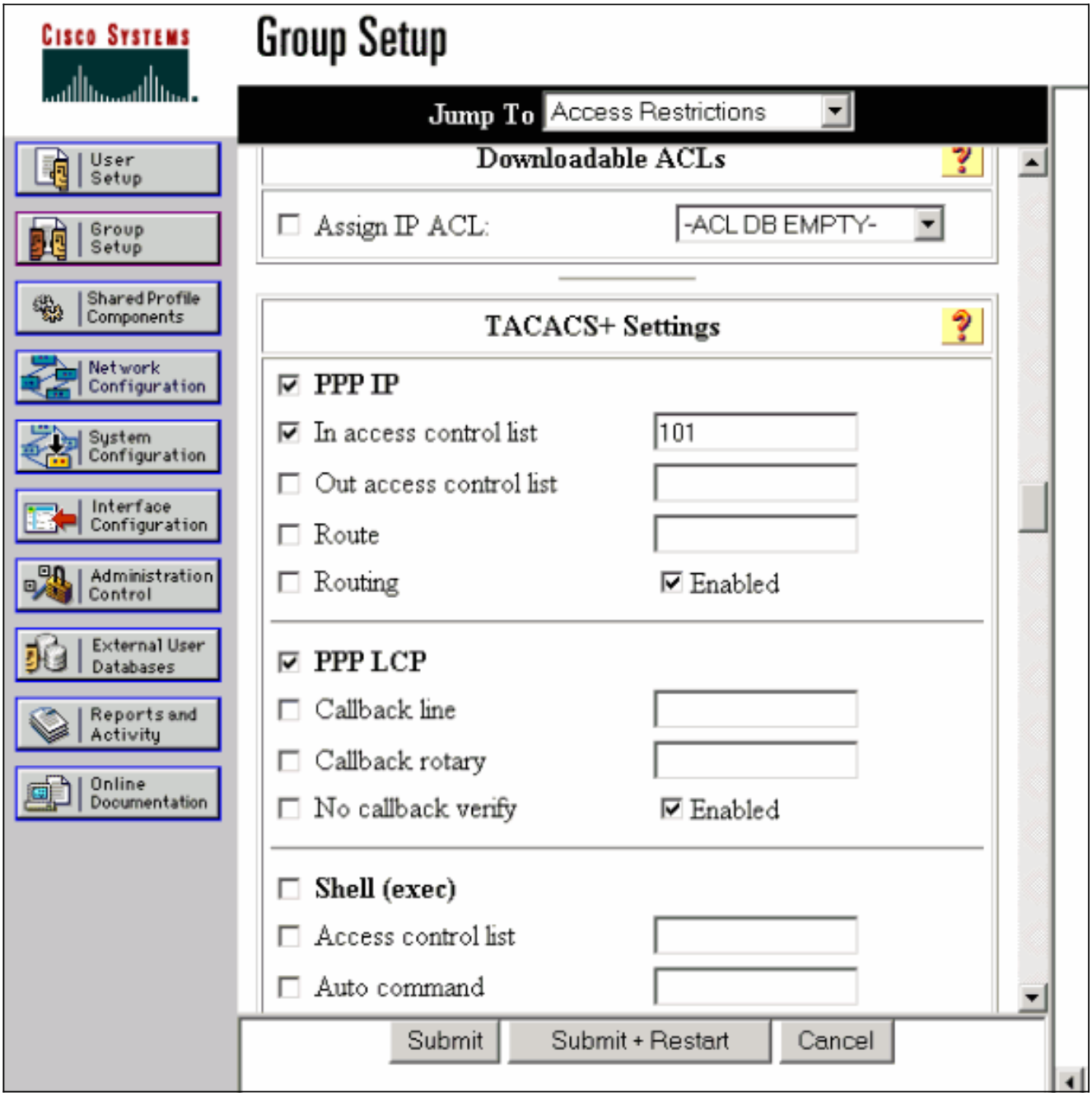
```
rtp-berry# ./ViewProfile -p 9900 -u chaprtr
User Profile Information
user = chaprtr{
profile_id = 182
set server current-failed-logins = 1
profile_cycle = 2
service=ppp {
protocol=lcp {
}
protocol=ip {
```

```
set inacl=101
}
}
password = chap "chaprtr"
}
```

Configuration du serveur - Cisco Secure ACS pour Windows 2.x et versions ultérieures - TACACS+

Complétez ces étapes afin de configurer Cisco Secure ACS pour Windows pour spécifier les listes de contrôle d'accès que le NAS doit appliquer.

1. Cliquez sur **Configuration du groupe**, sélectionnez le groupe auquel appartient l'utilisateur et cliquez sur **Modifier les paramètres**.
2. Cochez les cases **PPP IP**, **In access control list** et **PPP LCP** dans la section TACACS+ Settings.Spécifiez le numéro de la liste de contrôle d'accès à appliquer (dans ce cas, 101) dans la zone 'Dans la liste de contrôle d'accès'.
3. Cochez **Enabled** afin d'activer les options **PPP IP** et **PPP LCP**.



Exemple de débogage de routeur

```
koala#show debug
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
koala#show ip access-lists
Extended IP access list 101
permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log (2 matches)
permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255 log (11 matches)
koala#
4d05h: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
4d05h: %LINK-3-UPDOWN: Interface Async1, changed state to up
4d05h: AAA: parse name=Async1 idb type=10 tty=1
4d05h: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=1 channel=0
4d05h: AAA/MEMORY: create_user (0x54F934) user='chaprtr'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP
service=PPP priv=1
4d05h: AAA/AUTHEN/START (1203050692): port='Async1' list=''
action=LOGIN service=PPP
4d05h: AAA/AUTHEN/START (1203050692): using "default" list
4d05h: AAA/AUTHEN (1203050692): status = UNKNOWN
4d05h: AAA/AUTHEN/START (1203050692): Method=tacacs+ (tacacs+)
4d05h: TAC+: send AUTHEN/START packet ver=193 id=1203050692
4d05h: TAC+: Using default tacacs server-group "tacacs+" list.
4d05h: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
4d05h: TAC+: Opened TCP/IP handle 0x538778 to 172.18.124.111/49
4d05h: TAC+: 172.18.124.111 (1203050692) AUTHEN/START/LOGIN/CHAP queued
4d05h: TAC+: (1203050692) AUTHEN/START/LOGIN/CHAP processed
4d05h: TAC+: ver=192 id=1203050692 received AUTHEN status = GETPASS
4d05h: TAC+: Closing TCP/IP 0x538778 connection to 172.18.124.111/49
4d05h: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
4d05h: TAC+: Opened TCP/IP handle 0x538BBC to 172.18.124.111/49
4d05h: TAC+: Opened 172.18.124.111 index=1
4d05h: AAA: parse name=Async1 idb type=-1 tty=-1
4d05h: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
4d05h: AAA/MEMORY: create_user (0x19FCF8) user='chaprtr' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
4d05h: TAC+: rev0 inbound chap for id=1203050692 using id=2966879003
4d05h: TAC+: 172.18.124.111 (2966879003) AUTHEN/START/SENDPASS/CHAP queued
4d05h: TAC+: (2966879003) AUTHEN/START/SENDPASS/CHAP processed
4d05h: TAC+: ver=192 id=2966879003 received AUTHEN status = PASS
4d05h: TAC+: rev0 inbound chap SENDPASS status=PASS for id=1203050692
4d05h: TAC+: rev0 inbound chap MD5 compare OK
4d05h: AAA/MEMORY: free_user (0x19FCF8) user='chaprtr' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
4d05h: TAC+: Closing TCP/IP 0x538BBC connection to 172.18.124.111/49
4d05h: AAA/AUTHEN (1203050692): status = PASS
4d05h: As1 AAA/AUTHOR/LCP: Authorize LCP
4d05h: As1 AAA/AUTHOR/LCP (3002156107): Port='Async1' list='' service=NET
4d05h: AAA/AUTHOR/LCP: As1 (3002156107) user='chaprtr'
4d05h: As1 AAA/AUTHOR/LCP (3002156107): send AV service=ppp
4d05h: As1 AAA/AUTHOR/LCP (3002156107): send AV protocol=lcp
4d05h: As1 AAA/AUTHOR/LCP (3002156107): found list "default"
4d05h: As1 AAA/AUTHOR/LCP (3002156107): Method=tacacs+ (tacacs+)
4d05h: AAA/AUTHOR/TAC+: (3002156107): user=chaprtr
4d05h: AAA/AUTHOR/TAC+: (3002156107): send AV service=ppp
4d05h: AAA/AUTHOR/TAC+: (3002156107): send AV protocol=lcp
4d05h: TAC+: using previously set server 172.18.124.111 from group tacacs+
```

```
4d05h: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
4d05h: TAC+: Opened TCP/IP handle 0x539000 to 172.18.124.111/49
4d05h: TAC+: Opened 172.18.124.111 index=1
4d05h: TAC+: 172.18.124.111 (3002156107) AUTHOR/START queued
4d05h: TAC+: (3002156107) AUTHOR/START processed
4d05h: TAC+: (3002156107): received author response status = PASS_ADD
4d05h: TAC+: Closing TCP/IP 0x539000 connection to 172.18.124.111/49
4d05h: As1 AAA/AUTHOR (3002156107): Post authorization status = PASS_ADD
4d05h: As1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
4d05h: As1 AAA/AUTHOR/FSM (1577158668): Port='Async1' list='' service=NET
4d05h: AAA/AUTHOR/FSM: As1 (1577158668) user='chaprtr'
4d05h: As1 AAA/AUTHOR/FSM (1577158668): send AV service=ppp
4d05h: As1 AAA/AUTHOR/FSM (1577158668): send AV protocol=ip
4d05h: As1 AAA/AUTHOR/FSM (1577158668): found list "default"
4d05h: As1 AAA/AUTHOR/FSM (1577158668): Method=tacacs+ (tacacs+)
4d05h: AAA/AUTHOR/TAC+: (1577158668): user=chaprtr
4d05h: AAA/AUTHOR/TAC+: (1577158668): send AV service=ppp
4d05h: AAA/AUTHOR/TAC+: (1577158668): send AV protocol=ip
4d05h: TAC+: using previously set server 172.18.124.111 from group tacacs+
4d05h: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
4d05h: TAC+: Opened TCP/IP handle 0x539444 to 172.18.124.111/49
4d05h: TAC+: Opened 172.18.124.111 index=1
4d05h: TAC+: 172.18.124.111 (1577158668) AUTHOR/START queued
4d05h: TAC+: (1577158668) AUTHOR/START processed
4d05h: TAC+: (1577158668): received author response status = PASS_ADD
4d05h: TAC+: Closing TCP/IP 0x539444 connection to 172.18.124.111/49
4d05h: As1 AAA/AUTHOR (1577158668): Post authorization status = PASS_ADD
4d05h: As1 AAA/AUTHOR/FSM: We can start IPCP
4d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to up
4d05h: As1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 0.0.0.0
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV inacl=101
4d05h: As1 AAA/AUTHOR/IPCP: Authorization succeeded
4d05h: As1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 0.0.0.0
4d05h: As1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 1.1.1.2
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
 !--- Apply ACL 101 in the inbound direction. 4d05h: As1 AAA/AUTHOR/IPCP: Processing AV
inacl=101
4d05h: As1 AAA/AUTHOR/IPCP: Authorization succeeded
4d05h: As1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 1.1.1.2
4d05h: As1 AAA/AUTHOR/IPCP: Start. Her address 1.1.1.2, we want 1.1.1.2
4d05h: As1 AAA/AUTHOR/IPCP (1659098608): Port='Async1' list=''
service=NET
4d05h: AAA/AUTHOR/IPCP: As1 (1659098608) user='chaprtr'
4d05h: As1 AAA/AUTHOR/IPCP (1659098608): send AV service=ppp
4d05h: As1 AAA/AUTHOR/IPCP (1659098608): send AV protocol=ip
4d05h: As1 AAA/AUTHOR/IPCP (1659098608): send AV addr*1.1.1.2
4d05h: As1 AAA/AUTHOR/IPCP (1659098608): found list "default"
4d05h: As1 AAA/AUTHOR/IPCP (1659098608): Method=tacacs+ (tacacs+)
4d05h: AAA/AUTHOR/TAC+: (1659098608): user=chaprtr
4d05h: AAA/AUTHOR/TAC+: (1659098608): send AV service=ppp
4d05h: AAA/AUTHOR/TAC+: (1659098608): send AV protocol=ip
4d05h: AAA/AUTHOR/TAC+: (1659098608): send AV addr*1.1.1.2
4d05h: TAC+: using previously set server 172.18.124.111 from
group tacacs+
4d05h: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
4d05h: TAC+: Opened TCP/IP handle 0x538BBC to 172.18.124.111/49
4d05h: TAC+: Opened 172.18.124.111 index=1
4d05h: TAC+: 172.18.124.111 (1659098608) AUTHOR/START queued
4d05h: TAC+: (1659098608) AUTHOR/START processed
4d05h: TAC+: (1659098608): received author response status = PASS_REPL
```

```
4d05h: TAC+: Closing TCP/IP 0x538BBC connection to 172.18.124.111/49
4d05h: As1 AAA/AUTHOR (1659098608): Post authorization status = PASS_REPL
4d05h: As1 AAA/AUTHOR/IPCP: Reject 1.1.1.2, using 1.1.1.2
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV inacl=101
4d05h: As1 AAA/AUTHOR/IPCP: Processing AV addr*1.1.1.2
4d05h: As1 AAA/AUTHOR/IPCP: Authorization succeeded
4d05h: As1 AAA/AUTHOR/IPCP: Done. Her address 1.1.1.2, we want 1.1.1.2
4d05h: %SEC-6-IPACCESSLOGDP: list 101 permitted icmp 1.1.1.2 ->
9.9.9.9 (0/0), 3 packets
koala#show ip access-lists
Extended IP access list 101
permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255 log (5 matches)
permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255 log (11 matches)
koala#
```

Définir des listes d'accès sur le serveur

Remarque : les instructions de route ne doivent pas être transmises du serveur au routeur. L'utilisateur de la numérotation choisit normalement les routes à partir du routeur. La présence des instructions de route sur le routeur dépend du fait que les routes sont transmises à partir du serveur ou récupérées à partir du routeur :

```
ip route 9.9.9.0 255.255.255.0 11.11.11.12
ip route 15.15.15.0 255.255.255.0 12.12.12.13
```

Dans cet exemple de configuration, le fait de transmettre les routes à partir du serveur est uniquement utilisé à titre d'illustration.

Configuration du routeur

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname koala
!
aaa new-model
!
!--- These three lines of the configuration !--- are
specific to Cisco IOS Software Release 12.0.5.T and
later. !--- See the Commands for Other IOS Releases
section for !--- commands for other Cisco IOS Software
releases. ! aaa authentication login default group
tacacs+ none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable secret 5 $1$mnZQ$g6XdsgVnnYjEa.l7v.Pij1
enable password ww
!
username john password 0 doe
!
ip subnet-zero
!
cns event-service server
!
interface Ethernet0
```

```
ip address 10.31.1.5 255.255.255.0
no ip directed-broadcast
no mop enabled
!
interface Serial0
ip address 11.11.11.11 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface Serial1
ip address 12.12.12.12 255.255.255.0
no ip directed-broadcast
!
interface Async1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
async mode dedicated
peer default ip address pool mypool
fair-queue 64 16 0
no cdp enable
ppp authentication chap
!
ip local pool mypool 1.1.1.1 1.1.1.5
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
ip route 172.17.192.0 255.255.255.0 10.31.1.1
ip route 172.18.124.0 255.255.255.0 10.31.1.1
ip route 172.18.125.0 255.255.255.0 10.31.1.1
no ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 172.18.124.111
tacacs-server key cisco
!
line con 0
transport input none
line 1
autoselect during-login
autoselect ppp
modem InOut
transport input all
stopbits 1
speed 115200
flowcontrol hardware
line 2 16
line aux 0
line vty 0 4
password ww
!
end
```

Commandes pour d'autres versions de Cisco IOS

Remarque : afin d'utiliser ces commandes, supprimez les commandes en gras de la configuration du routeur et collez ces commandes dans, comme le dicte votre version du logiciel Cisco IOS.

Logiciel Cisco IOS versions 11.3.3.T à 12.0.5.T

```
aaa authentication login default tacacs+ local
aaa authentication ppp default if-needed tacacs+ local
aaa authorization network default tacacs+
```

Logiciel Cisco IOS versions 11.3 à 11.3.3.T

```
aaa authentication login default tacacs+
aaa authentication ppp default if-needed tacacs+
aaa authorization network tacacs+
```

Configuration du serveur - logiciel gratuit TACACS+

```
user = chaprtr {
chap = cleartext chaprtr
service = ppp protocol = ip {
route#1 = "9.9.9.9 255.255.255.255 11.11.11.12"
route#2 = "15.15.15.15 255.255.255.255 12.12.12.13"
route#3 = "15.15.15.16 255.255.255.255 12.12.12.13"
inacl#1 = "permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255"
inacl#2 = "permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255"
}
}
```

Configuration du serveur - Cisco Secure UNIX - TACACS+

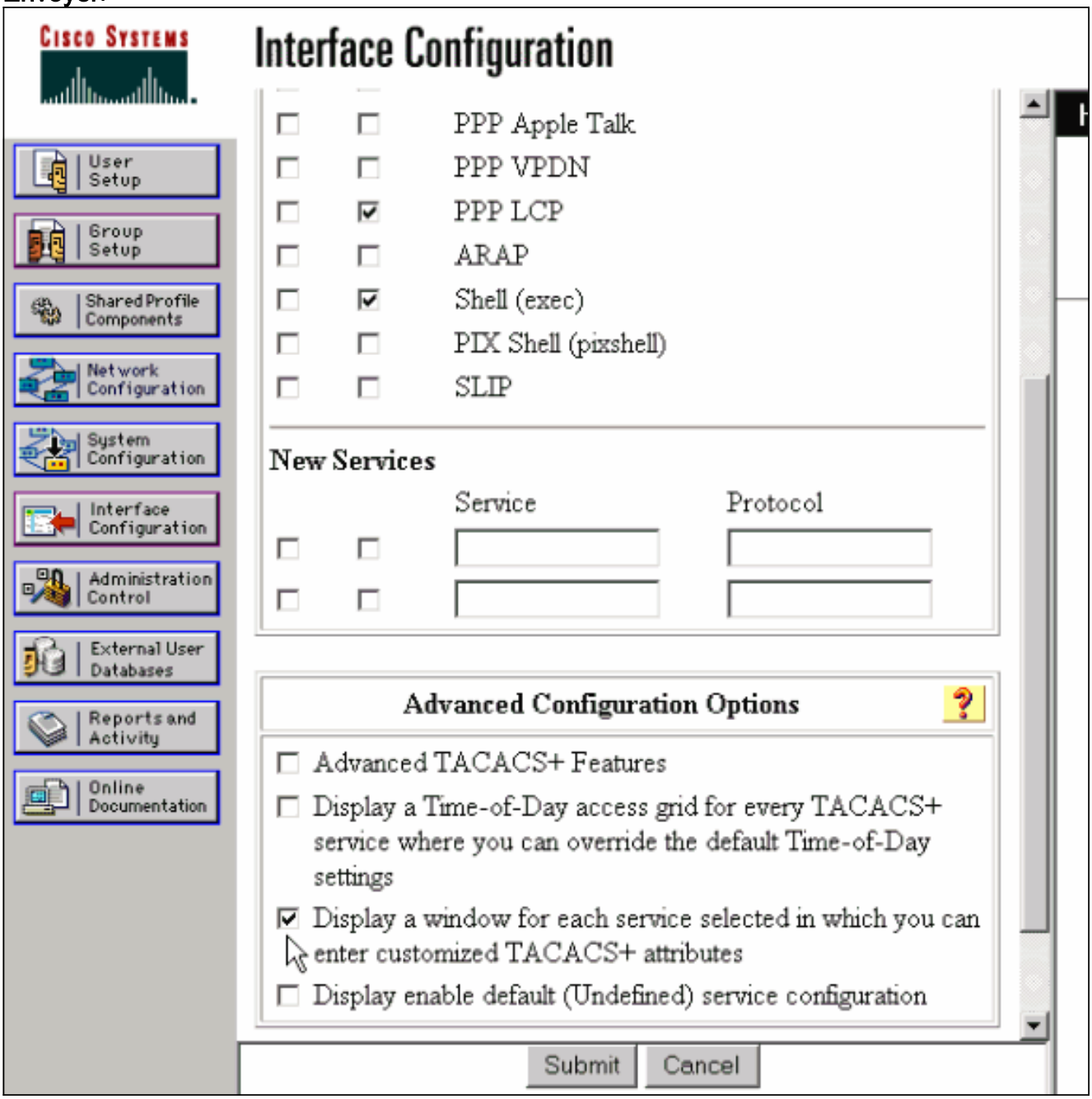
```
rtp-berry# ./ViewProfile -p 9900 -u chaprtr
User Profile Information
user = chaprtr{
profile_id = 183
set server current-failed-logins = 1
profile_cycle = 4
service=ppp {
protocol=lcp {
}
protocol=ip {
set route#1="9.9.9.9 255.255.255.255 11.11.11.12"
set route#2="15.15.15.15 255.255.255.255 12.12.12.13"
set route#3="15.15.15.16 255.255.255.255 12.12.12.13"
set inacl#1="permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255"
set inacl#2="permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255"
}
}

password = chap "chaprtr"
}
```

Configuration du serveur - Cisco Secure Windows 2.x - TACACS+

Complétez ces étapes afin de configurer Cisco Secure pour Windows pour qu'il transfère les listes de contrôle d'accès au NAS.

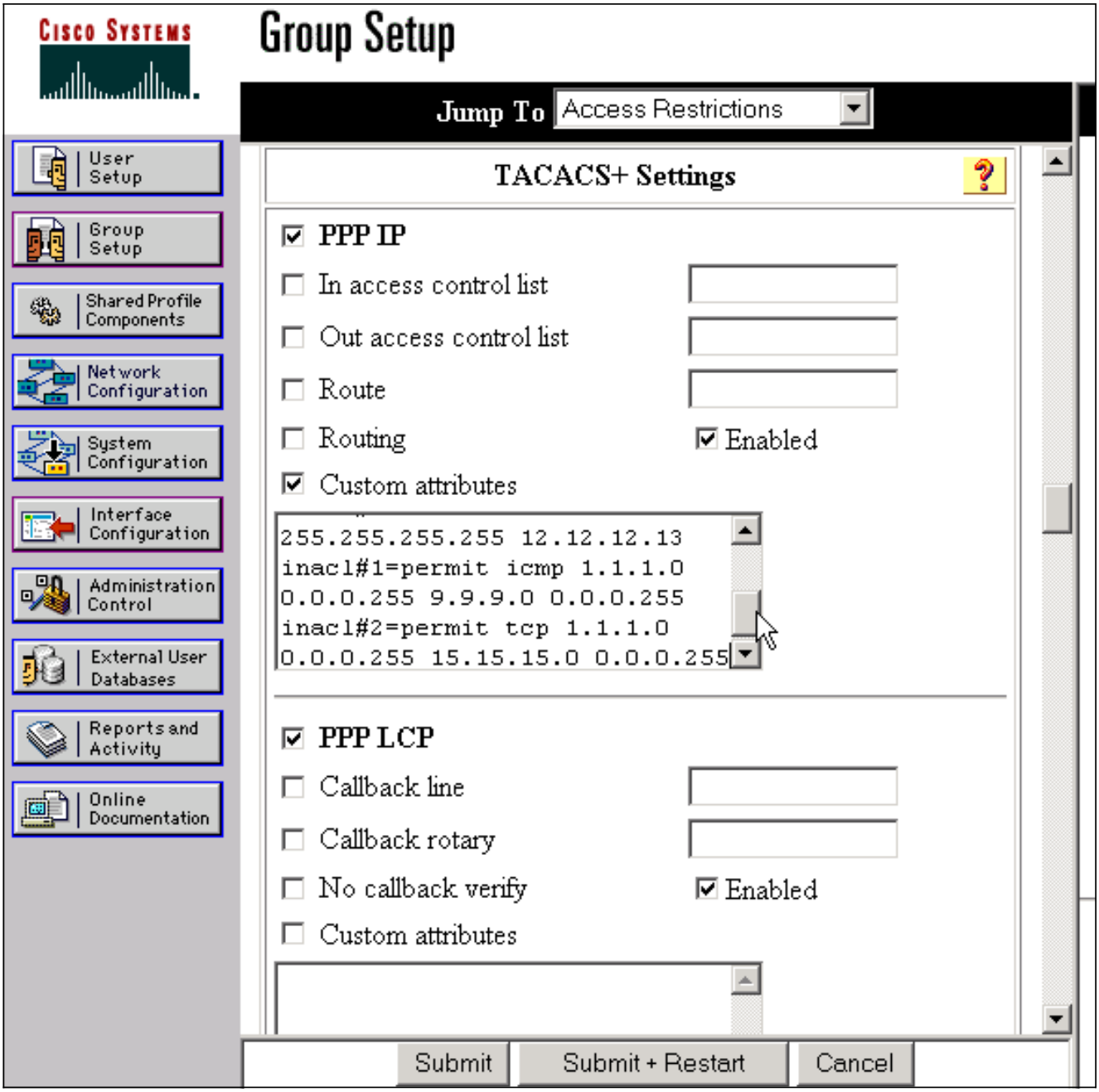
1. Cliquez sur **Interface Configuration** et sélectionnez **TACACS+ Cisco**.
2. Cochez la case **Afficher une fenêtre pour chaque service sélectionné dans laquelle vous pouvez saisir des attributs TACACS+ personnalisés** dans la section Options de configuration

avancées, puis cliquez sur **Envoyer**.



3. Cliquez sur **Configuration du groupe**, sélectionnez le groupe auquel appartient l'utilisateur et cliquez sur **Modifier les paramètres**.
4. Accédez à la section PPP IP et cochez les cases **PPP IP**, **Custom Attributes** et **Enable** de TACACS+ Settings.Entrez le texte affiché ici dans la zone Attributs personnalisés et cliquez sur **Soumettre**.

```
route#1=9.9.9.9 255.255.255.255 11.11.11.12
route#2=15.15.15.15 255.255.255.255 12.12.12.13
route#3=15.15.15.16 255.255.255.255 12.12.12.13
inacl#1=permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255
inacl#2=permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255
```



[Exemple de débogage de routeur]

Ce profil utilisateur a été utilisé pour créer cette sortie de débogage.

```
chaprtr
{
login = cleartext cisco
chap = cleartext
chaprtr service = ppp
protocol = ip
{
route#1 = "9.9.9.9 255.255.255.255 11.11.11.12"
route#2 = "15.15.15.15 255.255.255.255 12.12.12.13"
route#3 = "15.15.15.16 255.255.255.255 12.12.12.13"
inacl#1 = "permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255"
inacl#2 = "permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255"
}
}
```

```
koala#
*Mar  1 01:22:39.963: As1 LCP: I CONFREQ [Closed] id 0 len 23
*Mar  1 01:22:39.967: As1 LCP:    ACCM 0x00000000 (0x020600000000)
*Mar  1 01:22:39.971: As1 LCP:    MagicNumber 0x000034BD (0x0506000034BD)
*Mar  1 01:22:39.971: As1 LCP:    PFC (0x0702)
*Mar  1 01:22:39.975: As1 LCP:    ACFC (0x0802)
*Mar  1 01:22:39.975: As1 LCP:    Callback 6  (0x0D0306)
*Mar  1 01:22:39.979: As1 LCP: Lower layer not up, Fast Starting
*Mar  1 01:22:39.983: As1 PPP: Treating connection as a dedicated line
*Mar  1 01:22:39.983: As1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load]
*Mar  1 01:22:39.987: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar  1 01:22:39.991: As1 LCP: O CONFREQ [Closed] id 30 len 25
*Mar  1 01:22:39.995: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Mar  1 01:22:39.999: As1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 01:22:40.003: As1 LCP:    MagicNumber 0xE069F1B8 (0x0506E069F1B8)
*Mar  1 01:22:40.003: As1 LCP:    PFC (0x0702)
*Mar  1 01:22:40.007: As1 LCP:    ACFC (0x0802)
*Mar  1 01:22:40.011: As1 LCP: O CONFREJ [REQsent] id 0 len 7
*Mar  1 01:22:40.011: As1 LCP:    Callback 6  (0x0D0306)
01:22:40: %LINK-3-UPDOWN: Interface Async1, changed state to up
*Mar  1 01:22:40.139: As1 LCP: I CONFACK [REQsent] id 30 len 25
*Mar  1 01:22:40.143: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Mar  1 01:22:40.143: As1 LCP:    AuthProto CHAP (0x0305C22305)
*Mar  1 01:22:40.147: As1 LCP:    MagicNumber 0xE069F1B8 (0x0506E069F1B8)
*Mar  1 01:22:40.151: As1 LCP:    PFC (0x0702)
*Mar  1 01:22:40.151: As1 LCP:    ACFC (0x0802)
*Mar  1 01:22:40.155: As1 LCP: I CONFREQ [ACKrcvd] id 1 len 20
*Mar  1 01:22:40.159: As1 LCP:    ACCM 0x00000000 (0x020600000000)
*Mar  1 01:22:40.163: As1 LCP:    MagicNumber 0x000034BD (0x0506000034BD)
*Mar  1 01:22:40.163: As1 LCP:    PFC (0x0702)
*Mar  1 01:22:40.167: As1 LCP:    ACFC (0x0802)
*Mar  1 01:22:40.171: As1 LCP: O CONFACK [ACKrcvd] id 1 len 20
*Mar  1 01:22:40.171: As1 LCP:    ACCM 0x00000000 (0x020600000000)
*Mar  1 01:22:40.175: As1 LCP:    MagicNumber 0x000034BD (0x0506000034BD)
*Mar  1 01:22:40.179: As1 LCP:    PFC (0x0702)
*Mar  1 01:22:40.179: As1 LCP:    ACFC (0x0802)
*Mar  1 01:22:40.183: As1 LCP: State is Open
*Mar  1 01:22:40.183: As1 PPP: Phase is AUTHENTICATING, by this end
[0 sess, 1 load]
*Mar  1 01:22:40.187: As1 CHAP: O CHALLENGE id 10 len 26 from "koala"
*Mar  1 01:22:40.295: As1 LCP: I IDENTIFY [Open] id 2 len 18 magic
0x000034BD MSRASV4.00
*Mar  1 01:22:40.307: As1 LCP: I IDENTIFY [Open] id 3 len 21 magic
0x000034BD MSRAS-1-ZEKIE
*Mar  1 01:22:40.315: As1 CHAP: I RESPONSE id 10 len 28 from "chaprtr"
*Mar  1 01:22:40.323: AAA: parse name=Async1 idb type=10 tty=1
*Mar  1 01:22:40.323: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=1 channel=0
*Mar  1 01:22:40.327: AAA/MEMORY: create_user (0x4ED58C) user='chaprtr'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP service=PPP
priv=1
*Mar  1 01:22:40.331: AAA/AUTHEN/START (2439833946): port='Async1'
list='' action=LOGIN service=PPP
*Mar  1 01:22:40.335: AAA/AUTHEN/START (2439833946): using "default" list
*Mar  1 01:22:40.339: AAA/AUTHEN (2439833946): status = UNKNOWN
*Mar  1 01:22:40.339: AAA/AUTHEN/START (2439833946): Method=tacacs+ (tacacs+)
*Mar  1 01:22:40.343: TAC+: send AUTHEN/START packet ver=193 id=2439833946
*Mar  1 01:22:40.347: TAC+: Using default tacacs server-group "tacacs+" list.
*Mar  1 01:22:40.347: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
*Mar  1 01:22:40.359: TAC+: Opened TCP/IP handle 0x4EDDF8 to 172.18.124.111/49
*Mar  1 01:22:40.367: TAC+: 172.18.124.111 (2439833946)
AUTHEN/START/LOGIN/CHAP queued
*Mar  1 01:22:40.667: TAC+: (2439833946) AUTHEN/START/LOGIN/CHAP processed
*Mar  1 01:22:40.671: TAC+: ver=192 id=2439833946 received AUTHEN
```

```
status = GETPASS
*Mar  1 01:22:40.675: TAC+: Closing TCP/IP 0x4EDDF8 connection to
172.18.124.111/49
*Mar  1 01:22:40.679: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
*Mar  1 01:22:40.695: TAC+: Opened TCP/IP handle 0x4EE23C to 172.18.124.111/49
*Mar  1 01:22:40.695: TAC+: Opened 172.18.124.111 index=1
*Mar  1 01:22:40.699: AAA: parse name=Async1 idb type=-1 tty=-1
*Mar  1 01:22:40.703: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=1 channel=0
*Mar  1 01:22:40.707: AAA/MEMORY: create_user (0x4EC300) user='chaprtr'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
*Mar  1 01:22:40.711: TAC+: rev0 inbound chap for id=2439833946 using
id=1730351499
*Mar  1 01:22:40.715: TAC+: 172.18.124.111 (1730351499)
AUTHEN/START/SENDPASS/CHAP queued
*Mar  1 01:22:40.915: TAC+: (1730351499) AUTHEN/START/SENDPASS/CHAP processed
*Mar  1 01:22:40.919: TAC+: ver=192 id=1730351499 received AUTHEN
status = PASS
*Mar  1 01:22:40.923: TAC+: rev0 inbound chap SENDPASS status=PASS
for id=2439833946
*Mar  1 01:22:40.927: TAC+: rev0 inbound chap MD5 compare OK
*Mar  1 01:22:40.927: AAA/MEMORY: free_user (0x4EC300) user='chaprtr'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP service=PPP
priv=1
*Mar  1 01:22:40.935: TAC+: Closing TCP/IP 0x4EE23C connection to
172.18.124.111/49
*Mar  1 01:22:40.939: AAA/AUTHEN (2439833946): status = PASS
*Mar  1 01:22:40.943: As1 AAA/AUTHOR/LCP: Authorize LCP
*Mar  1 01:22:40.947: As1 AAA/AUTHOR/LCP (4250537500): Port='Async1'
list='' service=NET
*Mar  1 01:22:40.947: AAA/AUTHOR/LCP: As1 (4250537500) user='chaprtr'
*Mar  1 01:22:40.951: As1 AAA/AUTHOR/LCP (4250537500): send AV service=ppp
*Mar  1 01:22:40.955: As1 AAA/AUTHOR/LCP (4250537500): send AV protocol=lcp
*Mar  1 01:22:40.955: As1 AAA/AUTHOR/LCP (4250537500): found list "default"
*Mar  1 01:22:40.959: As1 AAA/AUTHOR/LCP (4250537500):
Method=tacacs+ (tacacs+)
*Mar  1 01:22:40.963: AAA/AUTHOR/TAC+: (4250537500): user=chaprtr
*Mar  1 01:22:40.963: AAA/AUTHOR/TAC+: (4250537500): send AV service=ppp
*Mar  1 01:22:40.967: AAA/AUTHOR/TAC+: (4250537500): send AV protocol=lcp
*Mar  1 01:22:40.971: TAC+: using previously set server 172.18.124.111
from group tacacs+
*Mar  1 01:22:40.971: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
*Mar  1 01:22:40.987: TAC+: Opened TCP/IP handle 0x4EE680 to 172.18.124.111/49
*Mar  1 01:22:40.991: TAC+: Opened 172.18.124.111 index=1
*Mar  1 01:22:40.999: TAC+: 172.18.124.111 (4250537500) AUTHOR/START queued
*Mar  1 01:22:41.195: TAC+: (4250537500) AUTHOR/START processed
*Mar  1 01:22:41.199: TAC+: (4250537500): received author response
status = PASS_ADD
*Mar  1 01:22:41.203: TAC+: Closing TCP/IP 0x4EE680 connection to
172.18.124.111/49
*Mar  1 01:22:41.207: As1 AAA/AUTHOR (4250537500): Post authorization
status = PASS_ADD
*Mar  1 01:22:41.215: As1 CHAP: O SUCCESS id 10 len 4
*Mar  1 01:22:41.219: As1 PPP: Phase is UP [0 sess, 0 load]
*Mar  1 01:22:41.223: As1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar  1 01:22:41.223: As1 AAA/AUTHOR/FSM (2403262371): Port='Async1'
list='' service=NET
*Mar  1 01:22:41.227: AAA/AUTHOR/FSM: As1 (2403262371) user='chaprtr'
*Mar  1 01:22:41.231: As1 AAA/AUTHOR/FSM (2403262371): send AV service=ppp
*Mar  1 01:22:41.231: As1 AAA/AUTHOR/FSM (2403262371): send AV protocol=ip
*Mar  1 01:22:41.235: As1 AAA/AUTHOR/FSM (2403262371): found list "default"
*Mar  1 01:22:41.239: As1 AAA/AUTHOR/FSM (2403262371):
Method=tacacs+ (tacacs+)
*Mar  1 01:22:41.239: AAA/AUTHOR/TAC+: (2403262371): user=chaprtr
```

```
*Mar  1 01:22:41.243: AAA/AUTHOR/TAC+: (2403262371): send AV service=ppp
*Mar  1 01:22:41.243: AAA/AUTHOR/TAC+: (2403262371): send AV protocol=ip
*Mar  1 01:22:41.247: TAC+: using previously set server 172.18.124.111
from group tacacs+
*Mar  1 01:22:41.251: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
*Mar  1 01:22:41.263: TAC+: Opened TCP/IP handle 0x4EEAC4 to
172.18.124.111/49
*Mar  1 01:22:41.267: TAC+: Opened 172.18.124.111 index=1
*Mar  1 01:22:41.275: TAC+: 172.18.124.111 (2403262371) AUTHOR/START queued
*Mar  1 01:22:41.323: As1 CCP: I CONFREQ [Not negotiated] id 4 len 12
*Mar  1 01:22:41.327: As1 CCP:    OUI  (0x0002)
*Mar  1 01:22:41.327: As1 CCP:    MS-PPC supported bits 0x00007080
(0x120600007080)
*Mar  1 01:22:41.335: As1 LCP: O PROTREJ [Open] id 31 len 18 protocol CCP
(0x80FD0104000C0002120600007080)
*Mar  1 01:22:41.339: As1 IPCP: I CONFREQ [Closed] id 5 len 40
*Mar  1 01:22:41.343: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
(0x0206002D0F01)
*Mar  1 01:22:41.347: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 01:22:41.351: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 01:22:41.355: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  1 01:22:41.359: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 01:22:41.363: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  1 01:22:41.607: TAC+: (2403262371) AUTHOR/START processed
*Mar  1 01:22:41.623: TAC+: (2403262371): received author response
status = PASS_ADD
*Mar  1 01:22:41.627: TAC+: Closing TCP/IP 0x4EEAC4 connection to
172.18.124.111/49
*Mar  1 01:22:41.635: As1 AAA/AUTHOR (2403262371): Post authorization
status = PASS_ADD
*Mar  1 01:22:41.647: As1 AAA/AUTHOR/FSM: We can start IPCP
*Mar  1 01:22:41.651: As1 IPCP: O CONFREQ [Closed] id 7 len 10
*Mar  1 01:22:41.655: As1 IPCP:    Address 10.31.1.5 (0x03060A1F0105)
*Mar  1 01:22:41.659: As1 AAA/AUTHOR/FSM: (0): Can we start CDPCP?
*Mar  1 01:22:41.663: As1 AAA/AUTHOR/FSM (840307497): Port='Async1'
list='' service=NET
*Mar  1 01:22:41.667: AAA/AUTHOR/FSM: As1 (840307497) user='chaprtr'
*Mar  1 01:22:41.671: As1 AAA/AUTHOR/FSM (840307497): send AV service=ppp
*Mar  1 01:22:41.671: As1 AAA/AUTHOR/FSM (840307497): send AV protocol=cdp
*Mar  1 01:22:41.675: As1 AAA/AUTHOR/FSM (840307497): found list "default"
*Mar  1 01:22:41.675: As1 AAA/AUTHOR/FSM (840307497): Method=tacacs+
(tacacs+)
*Mar  1 01:22:41.679: AAA/AUTHOR/TAC+: (840307497): user=chaprtr
*Mar  1 01:22:41.683: AAA/AUTHOR/TAC+: (840307497): send AV service=ppp
*Mar  1 01:22:41.683: AAA/AUTHOR/TAC+: (840307497): send AV protocol=cdp
*Mar  1 01:22:41.687: TAC+: using previously set server 172.18.124.111
from group tacacs+
*Mar  1 01:22:41.691: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
*Mar  1 01:22:41.703: TAC+: Opened TCP/IP handle 0x4EE23C to
172.18.124.111/49
*Mar  1 01:22:41.707: TAC+: Opened 172.18.124.111 index=1
*Mar  1 01:22:41.715: TAC+: 172.18.124.111 (840307497) AUTHOR/START queued
*Mar  1 01:22:41.759: As1 IPCP: I CONFACK [REQsent] id 7 len 10
*Mar  1 01:22:41.763: As1 IPCP:    Address 10.31.1.5 (0x03060A1F0105)
*Mar  1 01:22:41.915: TAC+: (840307497) AUTHOR/START processed
*Mar  1 01:22:41.923: TAC+: (840307497): received author response
status = FAIL
*Mar  1 01:22:41.927: TAC+: Closing TCP/IP 0x4EE23C connection to
172.18.124.111/49
*Mar  1 01:22:41.931: As1 AAA/AUTHOR (840307497): Post authorization
status = FAIL
*Mar  1 01:22:41.935: As1 AAA/AUTHOR/FSM: We cannot start CDPCP
*Mar  1 01:22:41.935: As1 CDPCP: State is Closed
01:22:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
```

```
changed state to up
*Mar  1 01:22:42.359: As1 PPP: Outbound cdp packet dropped,
CDPCP is Closed [starting negotiations]
*Mar  1 01:22:42.359: As1 CDPCP: State is Closed
*Mar  1 01:22:42.499: As1 PPP: Outbound cdp packet dropped,
CDPCP is Closed [starting negotiations]
*Mar  1 01:22:42.503: As1 CDPCP: State is Closed
*Mar  1 01:22:42.639: As1 PPP: Outbound cdp packet dropped,
CDPCP is Closed [starting negotiations]
*Mar  1 01:22:42.643: As1 CDPCP: State is Closed
*Mar  1 01:22:42.795: As1 PPP: Outbound cdp packet dropped,
CDPCP is Closed [starting negotiations]
*Mar  1 01:22:42.799: As1 CDPCP: State is Closed
*Mar  1 01:22:43.147: As1 CDPCP: TIMEout: State Closed
*Mar  1 01:22:43.151: As1 CDPCP: State is Listen
*Mar  1 01:22:43.155: As1 IPCP: I CONFREQ [ACKrcvd] id 5 len 40
*Mar  1 01:22:43.159: As1 IPCP:    CompressType VJ 15 slots
CompressSlotID (0x0206002D0F01)
*Mar  1 01:22:43.163: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 01:22:43.167: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 01:22:43.171: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  1 01:22:43.171: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 01:22:43.175: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  1 01:22:43.179: As1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0,
we want 0.0.0.0
*Mar  1 01:22:43.183: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  1 01:22:43.187: As1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
 !--- The NAS received the route statements and ACLs !--- from the ACS device. *Mar  1
01:22:43.187: As1 AAA/AUTHOR/IPCP: Processing AV route#1=
9.9.9.9 255.255.255.255 11.11.11.12
*Mar  1 01:22:43.191: As1 AAA/AUTHOR/IPCP: Processing AV route#2=
15.15.15.15 255.255.255.255 12.12.12.13
*Mar  1 01:22:43.195: As1 AAA/AUTHOR/IPCP: Processing AV route#3=
15.15.15.16 255.255.255.255 12.12.12.13
*Mar  1 01:22:43.199: As1 AAA/AUTHOR/IPCP: Processing AV inacl#1=
permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255
*Mar  1 01:22:43.199: As1 AAA/AUTHOR/IPCP: Processing AV inacl#2=
permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255
*Mar  1 01:22:43.203: As1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  1 01:22:43.207: As1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0,
we want 0.0.0.0
*Mar  1 01:22:43.211: As1 IPCP: Pool returned 1.1.1.1
*Mar  1 01:22:43.215: As1 IPCP: O CONFREJ [ACKrcvd] id 5 len 28
*Mar  1 01:22:43.219: As1 IPCP:    CompressType VJ 15 slots
CompressSlotID (0x0206002D0F01)
*Mar  1 01:22:43.223: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  1 01:22:43.227: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 01:22:43.231: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  1 01:22:43.339: As1 IPCP: I CONFREQ [ACKrcvd] id 6 len 16
*Mar  1 01:22:43.343: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 01:22:43.347: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 01:22:43.351: As1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0,
we want 1.1.1.1
*Mar  1 01:22:43.355: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  1 01:22:43.355: As1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
!--- The NAS applies the route statements and ACLs. *Mar  1 01:22:43.359: As1 AAA/AUTHOR/IPCP:
Processing AV route#1=
9.9.9.9 255.255.255.255 11.11.11.12
*Mar  1 01:22:43.363: As1 AAA/AUTHOR/IPCP: Processing AV route#2=
15.15.15.15 255.255.255.255 12.12.12.13
*Mar  1 01:22:43.363: As1 AAA/AUTHOR/IPCP: Processing AV route#3=
15.15.15.16 255.255.255.255 12.12.12.13
*Mar  1 01:22:43.367: As1 AAA/AUTHOR/IPCP: Processing AV inacl#1=
permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255
```

```
*Mar  1 01:22:43.371: As1 AAA/AUTHOR/IPCP: Processing AV inacl#2=
permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255
*Mar  1 01:22:43.375: As1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  1 01:22:43.375: As1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0,
we want 1.1.1.1
*Mar  1 01:22:43.383: As1 IPCP: O CONFNAK [ACKrcvd] id 6 len 16
*Mar  1 01:22:43.387: As1 IPCP:    Address 1.1.1.1 (0x030601010101)
*Mar  1 01:22:43.391: As1 IPCP:    PrimaryDNS 172.18.125.3 (0x8106AC127D03)
*Mar  1 01:22:43.499: As1 IPCP: I CONFREQ [ACKrcvd] id 7 len 16
*Mar  1 01:22:43.503: As1 IPCP:    Address 1.1.1.1 (0x030601010101)
*Mar  1 01:22:43.507: As1 IPCP:    PrimaryDNS 172.18.125.3 (0x8106AC127D03)
*Mar  1 01:22:43.511: As1 AAA/AUTHOR/IPCP: Start.  Her address 1.1.1.1,
we want 1.1.1.1
*Mar  1 01:22:43.519: As1 AAA/AUTHOR/IPCP (2646570182): Port='Async1'
list='' service=NET
*Mar  1 01:22:43.519: AAA/AUTHOR/IPCP: As1 (2646570182) user='chaprtr'
*Mar  1 01:22:43.523: As1 AAA/AUTHOR/IPCP (2646570182): send AV service=ppp
*Mar  1 01:22:43.523: As1 AAA/AUTHOR/IPCP (2646570182): send AV protocol=ip
*Mar  1 01:22:43.527: As1 AAA/AUTHOR/IPCP (2646570182): send AV addr*1.1.1.1
*Mar  1 01:22:43.531: As1 AAA/AUTHOR/IPCP (2646570182): found list "default"
*Mar  1 01:22:43.535: As1 AAA/AUTHOR/IPCP (2646570182): Method=tacacs+ (tacacs+)
*Mar  1 01:22:43.539: AAA/AUTHOR/TAC+: (2646570182): user=chaprtr
*Mar  1 01:22:43.539: AAA/AUTHOR/TAC+: (2646570182): send AV service=ppp
*Mar  1 01:22:43.543: AAA/AUTHOR/TAC+: (2646570182): send AV protocol=ip
*Mar  1 01:22:43.543: AAA/AUTHOR/TAC+: (2646570182): send AV addr*1.1.1.1
*Mar  1 01:22:43.547: TAC+: using previously set server 172.18.124.111 from
group tacacs+
*Mar  1 01:22:43.551: TAC+: Opening TCP/IP to 172.18.124.111/49 timeout=5
*Mar  1 01:22:43.563: TAC+: Opened TCP/IP handle 0x4EE23C to 172.18.124.111/49
*Mar  1 01:22:43.567: TAC+: Opened 172.18.124.111 index=1
*Mar  1 01:22:43.575: TAC+: 172.18.124.111 (2646570182) AUTHOR/START queued
*Mar  1 01:22:43.875: TAC+: (2646570182) AUTHOR/START processed
*Mar  1 01:22:43.887: TAC+: (2646570182): received author response
status = PASS_REPL
*Mar  1 01:22:43.891: TAC+: Closing TCP/IP 0x4EE23C connection to
172.18.124.111/49
*Mar  1 01:22:43.899: As1 AAA/AUTHOR (2646570182): Post authorization
status = PASS_REPL
*Mar  1 01:22:43.911: As1 AAA/AUTHOR/IPCP: Reject 1.1.1.1, using 1.1.1.1
*Mar  1 01:22:43.915: As1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  1 01:22:43.919: As1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
*Mar  1 01:22:43.923: As1 AAA/AUTHOR/IPCP: Processing AV route#1=
9.9.9.9 255.255.255.255 11.11.11.12
*Mar  1 01:22:43.923: As1 AAA/AUTHOR/IPCP: Processing AV route#2=
15.15.15.15 255.255.255.255 12.12.12.13
*Mar  1 01:22:43.927: As1 AAA/AUTHOR/IPCP: Processing AV route#3=
15.15.15.16 255.255.255.255 12.12.12.13
*Mar  1 01:22:43.931: As1 AAA/AUTHOR/IPCP: Processing AV inacl#1=
permit icmp 1.1.1.0 0.0.0.255 9.9.9.0 0.0.0.255
*Mar  1 01:22:43.935: As1 AAA/AUTHOR/IPCP: Processing AV inacl#2=
permit tcp 1.1.1.0 0.0.0.255 15.15.15.0 0.0.0.255
*Mar  1 01:22:43.939: As1 AAA/AUTHOR/IPCP: Processing AV addr*1.1.1.1
*Mar  1 01:22:43.939: As1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  1 01:22:43.943: As1 AAA/AUTHOR/IPCP: Done.  Her address 1.1.1.1,
we want 1.1.1.1
*Mar  1 01:22:43.947: As1 IPCP: O CONFACK [ACKrcvd] id 7 len 16
*Mar  1 01:22:43.951: As1 IPCP:    Address 1.1.1.1 (0x030601010101)
*Mar  1 01:22:43.955: As1 IPCP:    PrimaryDNS 172.18.125.3
(0x8106AC127D03)
*Mar  1 01:22:43.959: As1 IPCP: State is Open
*Mar  1 01:22:44.483: As1 IPCP: Install route to 1.1.1.1
koala#
koala#
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug aaa authentication** - Affiche des informations sur l'authentification AAA/TACACS+.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/TACACS+.
- **debug aaa per-user** - Affiche des informations sur les paramètres de configuration par utilisateur sur le routeur ou les serveurs d'accès envoyés depuis un serveur AAA.
- **debug tacacs+** : affiche les informations de débogage détaillées associées à TACACS+.
- **debug ppp negotiation** - Affiche les paquets PPP transmis lors du démarrage PPP, où les options PPP sont négociées.

Référez-vous à Dépannage des listes d'accès sur les interfaces de numérotation pour des informations de dépannage.

Informations connexes

- Cisco Secure Access Control Server pour UNIX
- Cisco Secure Access Control Server pour Windows