Contents

CAPITOLUL 5. ASSIGNING ADMINISTRATIVE ROLES

5.0 Introduction

5.0.1 - Scope

Configurarea nivelurilor de privilegii administrative și CLI bazat pe roluri. Acești pași sunt critici pentru limitarea accesului la dispozitivele de rețea pe baza rolului de serviciu al utilizatorilor administrativi.

5.0.2 - Obiective

Topic Title	Topic Objective
Configure Privilege Levels	Utilizarea comenzilor corecte pentru a configura nivelurile de privilegii administrative pentru a controla disponibilitatea comenzilor.
Configure Role-Based CLI	Utilizarea comenzilor corecte pentru a configura accesul CLI bazat pe roluri pentru a controla disponibilitatea comenzilor.

5.1 Configure Privilege Levels

5.1.1 - Limiting Command Availability

Organizațiile mari au multe funcții variate în cadrul unui departament IT. Nu toate funcțiile postului ar trebui să aibă același nivel de acces la dispozitivele de infrastructură.

Software-ul Cisco IOS are două metode de furnizare a accesului la infrastructură:

1. *nivel de privilegii,*
2. *CLI bazat pe roluri.*

Ambele metode ajută la determinarea cui ar trebui să se permită să se conecteze la dispozitiv și ce ar trebui să poată face persoana respectivă cu el. Accesul CLI bazat pe roluri oferă mai multă granularitate și control.

În mod implicit, CLI-ul software Cisco IOS are două niveluri de acces la comenzi:

1) Modul EXEC utilizator (nivel de privilegiu 1) - Acesta oferă cele mai mici privilegii de utilizator în modul EXEC și permite numai comenzile la nivel de utilizator disponibile la promptul Router>.
2) Mod EXEC privilegiat (nivel de privilegiu 15) - Acesta include toate comenzile la nivel de activare la promptul Router#.

Există 16 niveluri de privilegii în total, după cum sunt enumerate mai jos. Cu cât este mai mare nivelul de privilegii, cu atât mai mult acces la router are un utilizator. Comenzile care sunt disponibile la niveluri de privilegii inferioare sunt, de asemenea, executabile la niveluri superioare.

Nivelul 0: Predefinit pentru privilegii de acces la nivel de utilizator. Folosit rar, dar include cinci comenzi: dezactivare, activare, ieșire, ajutor și deconectare.

Nivelul 1: Nivelul implicit pentru autentificare cu promptul routerului Router >. Un utilizator nu poate face modificări sau nu poate vizualiza fișierul de configurare care rulează.

Nivelurile 2 -14: poate fi personalizat pentru privilegii la nivel de utilizator. Comenzile de la nivelurile inferioare pot fi mutate la un alt nivel superior, sau comenzile de la nivelurile superioare pot fi mutate la un nivel inferior.

Nivelul 15: Rezervat pentru privilegiile modului de activare (comandă de activare). Utilizatorii pot modifica configurațiile și pot vizualiza fișierele de configurare.

Pentru a atribui comenzi unui nivel de privilegiu personalizat, se utilizeaza comanda modului de configurare globală a privilegiilor prezentată mai jos.

```
Router(config)# privilege mode {level level|reset} command
```

Command	Description
mode	Specifică modul de configurare. Folosește privilegiul ? comandă pentru a vedea o listă completă a modurilor de configurare a routerului disponibile pe router.
level	(Opțional) Permite setarea unui nivel de privilegii cu o comandă specificată.
level	(Opțional) Nivelul de privilegii care este asociat cu o comandă. Se pot specifica până la 16 niveluri de privilegii, folosind numerele de la 0 la 15.
reset	(Opțional) Resetează nivelul de privilegii al unei comenzi.
command	(Opțional) Argument de utilizat când se doreste resetarea nivelului de privilegii.

5.1.2 - Configuring and Assigning Privilege Levels

Pentru a configura un nivel de privilegii cu anumite comenzi, se utilizeaza nivelul de privilegiu exec [comandă]. Exemplul prezintă exemple pentru trei niveluri de privilegii diferite.

- *Nivelul de privilegiu 5 are acces la toate comenzile disponibile pentru nivelul predefinit 1 și comanda ping.*

- *Nivelul de privilegii 10 are acces la toate comenzile disponibile pentru nivelul 5, precum și la comanda de reîncărcare.*
- *Nivelul de privilegii 15 este predefinit și nu trebuie configurat în mod explicit. Acest nivel de privilegii are acces la toate comenzile, inclusiv vizualizarea și modificarea configurației.*

```
R1#                                conf                                t
 R1(config)#    !Level    5    and    SUPPORT    user    configuration
 R1(config)#       privilege       exec       level       5       ping
 R1(config)#  enable algorithm-type scrypt secret level 5 cisco5
 R1(config)#  username SUPPORT privilege 5 algorithm-type scrypt
secret                                                          cisco5
 R1(config)#    !Level    10    and    JR-ADMIN    user    configuration
 R1(config)#       privilege       exec       level       10       reload
 R1(config)#  enable algorithm-type scrypt secret level 10 cisco10
 R1(config)#  username JR-ADMIN privilege 10 algorithm-type scrypt
secret                                                        cisco10
 R1(config)#    !Level    15    and    ADMIN    user    configuration
 R1(config)#  enable algorithm-type scrypt secret level 15 cisco123
 R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret
cisco123
```

Există două metode de atribuire a parolelor diferitelor niveluri de privilegii:

1. *Pentru un utilizator căruia i se acordă un anumit nivel de privilegii, prin comanda nume de utilizator, nivel de privilegii, parolă secretă, modul de configurare globală*
2. *La nivelul de privilegii, prin comanda enable secret level password global configuration mode*

Notă: Atât comenzile secrete pentru numele de utilizator, cât și pentru activare secrete sunt configurate pentru criptarea de tip 9.

Se utilizeaza comanda nume de utilizator pentru a atribui un nivel de privilegii unui anumit utilizator. Se utilizeaza comanda enable secret pentru a atribui un nivel de privilegii unei anumite parole pentru modul EXEC. De exemplu, utilizatorului SUPPORT îi este atribuit nivelul de privilegiu 5 cu parola cisco5. Cu toate acestea, așa cum se arată în exemplul de mai jos, orice utilizator poate accesa nivelul de privilegiu 5 dacă acel utilizator știe că parola secretă de activare este cisco5. Exemplul demonstrează, de asemenea, că nivelul de privilegiu 5 nu poate reîncărca routerul.

```
R1> enable 5
Password: <cisco5>
R1# show privilege  Current privilege level is 5
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
R1# reload
Translating "reload"  % Bad IP address or host name
Translating "reload"
 % Unknown command or computer name, or unable to find computer address
R1#
```

În exemplul de mai jos, utilizatorul activează nivelul de privilegiu 10 care are acces la comanda reload. Cu toate acestea, utilizatorii la nivelul de privilegii 10 nu pot vizualiza configurația în execuție.

```
R1# enable 10
Password: <cisco10>
R1# show privilege
Current privilege level is 10
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1# reload

System configuration has been modified. Save? [yes/no]: ^C

R1# show running-config
^
% Invalid input detected at '^' marker.
R1#
```

În exemplul următor, utilizatorul activează nivelul de privilegiu 15, care are acces deplin pentru a vizualiza și modifica configurația, inclusiv vizualizarea configurației care rulează.

```
R1# enable 15
Password:
R1# show privilege
Current privilege level is 15
R1# show running-config Building configuration...
 Current configuration : 1979 bytes
!
! Last configuration change at 15:30:07 UTC Tue Feb 17 2015
!
version 15.4
R1#
```

5.1.3 - Limitations of Privilege Levels

Utilizarea nivelurilor de privilegii are limitările sale:

Nu există control de acces la anumite interfețe, porturi, interfețe logice și sloturi pe un router.

Comenzile disponibile la niveluri de privilegii inferioare sunt întotdeauna executabile la niveluri superioare.

Comenzile setate special la un nivel de privilegii mai înalt nu sunt disponibile pentru utilizatorii cu privilegii mai mici.

Atribuirea unei comenzi cu mai multe cuvinte cheie permite accesul la toate comenzile care folosesc acele cuvinte cheie. De exemplu, permiterea accesului la show ip route permite utilizatorului accesul la toate comenzile show și show ip.

Notă: Dacă un administrator trebuie să creeze un cont de utilizator care să aibă acces la majoritatea, dar nu la toate comenzile, instrucțiunile de privilegiu exec trebuie să fie configurate pentru fiecare comandă care trebuie executată la un nivel de privilegii mai mic de valoarea 15.

5.2 Configure Role-Based CLI

5.2.1 - Role-Based CLI Access

Într-un efort de a oferi mai multă flexibilitate decât permit nivelurile de privilegii, Cisco a introdus caracteristica de acces CLI bazată pe roluri începand cu Cisco IOS Release 12.3(11)T. Această caracteristică oferă un acces mai fin și mai granular, controlând ce comenzi sunt disponibile pentru anumite roluri. Accesul CLI bazat pe roluri permite administratorului de rețea să creeze diferite vederi ale configurațiilor routerului pentru diferiți utilizatori. Fiecare vizualizare definește comenzile CLI pe care le poate accesa fiecare utilizator.

Securitate - Accesul CLI bazat pe roluri îmbunătățește securitatea dispozitivului prin definirea setului de comenzi CLI care sunt accesibile de către un anumit utilizator. În plus, administratorii pot controla accesul utilizatorilor la anumite porturi, interfețe logice și sloturi de pe un router. Acest lucru împiedică un utilizator să modifice accidental sau intenționat o configurație sau să colecteze informații la care nu ar trebui să aibă acces.

Disponibilitate - Accesul CLI bazat pe roluri previne executarea neintenționată a comenzilor CLI de către personalul neautorizat și minimizează timpul de nefuncționare.

Eficienta operationala - Utilizatorii văd doar comenzile CLI aplicabile porturilor și CLI la care au acces. Prin urmare, routerul pare a fi mai puțin complex, iar comenzile sunt mai ușor de identificat atunci când se utilizeaza funcția de ajutor de pe dispozitiv.

5.2.2 - Role-Based Views

CLI bazat pe roluri oferă trei tipuri de vederi care dictează ce comenzi sunt disponibile:

Vedere rădăcină - Pentru a configura orice vizualizare pentru sistem, administratorul trebuie să fie în vizualizarea rădăcină. Vizualizarea rădăcină are aceleași privilegii de acces ca un utilizator care are privilegii de nivel 15. Cu toate acestea, o vizualizare rădăcină nu este

același lucru cu un utilizator de nivel 15. Doar un utilizator de vizualizare root poate configura o nouă vizualizare și poate adăuga sau elimina comenzi din vizualizările existente.

Vizualizare CLI - Un set specific de comenzi poate fi grupat într-o vizualizare CLI. Spre deosebire de nivelurile de privilegii, o vizualizare CLI nu are ierarhie de comandă și nici vizualizări superioare sau inferioare. Fiecărei vizualizări trebuie alocate toate comenzile asociate cu acea vedere. O vizualizare nu moștenește comenzi de la nicio altă vizualizare. În plus, aceleași comenzi pot fi utilizate în mai multe vizualizări.

Supervizualizare - O supervizualizare constă dintr-una sau mai multe vizualizări CLI. Administratorii pot defini ce comenzi sunt acceptate și ce informații de configurare sunt vizibile. Superview-urile permit unui administrator de rețea să atribuie utilizatorilor și grupurilor de utilizatori mai multe vizualizări CLI simultan, în loc să fie nevoit să atribuie o singură vizualizare CLI pentru fiecare utilizator cu toate comenzile asociate cu acea singură vizualizare CLI.

Superviziunile au mai multe caracteristici specifice:

- *O singură vizualizare CLI poate fi partajată în mai multe supervizualizări.*
- *Comenzile nu pot fi configurate pentru o supraveghere. Un administrator trebuie să adauge comenzi la vizualizarea CLI și să adauge acea vizualizare CLI la supervizualizare.*
- *Utilizatorii care sunt conectați la o supervizualizare pot accesa toate comenzile care sunt configurate pentru oricare dintre vizualizările CLI care fac parte din supervizualizare.*
- *Fiecare supervizualizare are o parolă care este utilizată pentru a comuta între supervizualizări sau de la o vizualizare CLI la o vizualizare.*
- *Ștergerea unei supervizualizări nu șterge vizualizările CLI asociate. Vizualizările CLI rămân disponibile pentru a fi atribuite unei alte supervizualizări.*

5.2.3 - Configure Role-Based Views

Înainte ca un administrator să poată crea o vizualizare, cei 3 AAA trebuie să fie activat folosind comanda aaa new-model. Pentru a configura și edita vizualizări, un administrator trebuie să se conecteze ca vizualizare rădăcină utilizând comanda EXEC cu privilegii de vizualizare activată. Se poate folosi și comanda enable view root. Când vi se solicită, introduceți parola secretă de activare.

Există cinci pași pentru a crea și gestiona o anumită vizualizare.

Pasul 1. Activarea celor 3 AAA cu comanda modului de configurare globală ***aaa new-model***. Se iese și se intra în vizualizarea rădăcină cu comanda ***enable view***.

Parameter	Description
view	Acest parametru intră în vizualizarea rădăcină dacă nu este specificat niciun nume de vizualizare, ceea ce permite unui administrator să configureze vizualizările CLI. Parametrul de vizualizare este necesar pentru a configura o vizualizare CLI.
view-name	(Opțional) Acest parametru intră sau iese dintr-o vizualizare CLI specificată. Acest parametru poate fi utilizat pentru a comuta de la o vizualizare CLI la alta vizualizare CLI.

Pasul 2. Creare vizualizare folosind comanda modului de configurare globală vizualizare-nume vizualizare. Aceasta activează modul de configurare a vizualizării. Excluzând vizualizarea rădăcină, există o limită maximă de 15 vizualizări în total.

```
Router(config)# parser view view-name
```

Pasul 3. Atribuirea unei parole secrete vizualizării utilizând comanda modului de configurare a vizualizarii parolei secrete.

Aceasta setează o parolă pentru a proteja accesul la vizualizare. Parola trebuie creată imediat după crearea unei vizualizări, în caz contrar, va apărea un mesaj de eroare.

```
Router(config-view)# secret password
```

Pasul 4. Atribuirea de comenzi la vizualizarea selectată utilizând comanda commands parser-mode în modul de configurare a vizualizării.

```
Router(config-view)# commands parser-mode {include | include-exclusive | exclude} [all] [interface interface-name | command]
```

Commands	Description
commands	Adaugă comenzi sau interfețe la o vizualizare.
parser-mode	Modul în care există comanda specificată; de exemplu, modul EXEC.
include	Adaugă o comandă sau o interfață la vizualizare și permite ca aceeași comandă sau interfață să fie adăugată la alte vizualizări.
include-exclusive	Adaugă o comandă sau o interfață la vizualizare și exclude aceeași comandă sau interfață de a fi adăugată la toate celelalte vizualizări.
exclude	Exclude o comandă sau o interfață din vizualizare.
all	Un „wildcard” care permite fiecărei comenzi dintr-un mod de configurare specificat care începe cu același cuvânt cheie sau fiecare subinterfață pentru o interfață specificată să facă parte din vizualizare.
interface *interface-name*	Interfață care este adăugată la vizualizare.
command	Comanda care este adăugată la vizualizare.

Pasul 5. Ieșire din modul de configurare a vizualizarii tastând comanda de ***exit***.

Exemplul de mai jos arată configurația a trei vederi. Observați în exemplu este că pentru comanda secretă acceptă doar criptarea MD5 (tip 5). De asemenea, se observa că atunci când o comandă a fost adăugată la o vizualizare înainte ca parola să fie atribuită, a apărut o eroare.

```
R1(config)# aaa new-model
R1(config)# parser view SHOWVIEW
R1(config-view)#  secret ?
0     Specifies an UNENCRYPTED password will follow
5     Specifies an ENCRYPTED secret will follow
LINE  The UNENCRYPTED (cleartext) view secret string
R1(config-view)# secret cisco
R1(config-view)# commands exec include show
R1(config-view)# exit
R1(config)#  parser view VERIFYVIEW
R1(config-view)#  commands exec include ping
% Password not set for the view VERIFYVIEW
R1(config-view)#  secret cisco5
R1(config-view)#  commands exec include ping
R1(config-view)# exit
R1(config)# parser view REBOOTVIEW
R1(config-view)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
R1(config)#
```

Verificarea configurației vizualizării utilizând comanda ***show running-config***.

```
R1# show running-config
<output omitted>
parser view SHOWVIEW
 secret 5 $1$GL2J$8njLecwTaLAc0UuWo1/Fv0
 commands exec include show
!
parser view VERIFYVIEW
 secret 5 $1$d08J$1zOYSI4WainGxkn0Hu7lP1
 commands exec include ping
!
parser view REBOOTVIEW
 secret 5 $1$L7lZ$1Jtn5IhP43fVE7SVoF1pt.
 commands exec include reload
!
```

5.2.4 - Configure Role-Based CLI Superviews

Pașii de configurare a unei supervizuări sunt în esență aceiași cu configurarea unei vizualizări CLI, cu excepția faptului că comanda view view-name este utilizată pentru a atribui comenzi supervizualizării. Administratorul trebuie să fie în vizualizarea rădăcină pentru a configura o vizualizare superioară. Pentru a confirma că este utilizată vizualizarea rădăcină, se utilizează fie comanda enable view, fie enable view root. Când vi se solicită, introduceți parola secretă.

Există patru pași pentru a crea și gestiona o supraveghere.

Pasul 1. Creare vizualizare utilizând comanda parser view view-name superview și intrare în modul de configurare superview. Adăugarea cuvântului cheie supravizualizare la vizualizarea parser creează o supravizualizare și intră în modul de configurare.

```
Router(config)# parser view view-name superview
```

Pasul 2. Atribuirea unei parole secrete vizualizării folosind comanda parolă secretă. Aceasta setează o parolă pentru a proteja accesul la supraveghere. Parola trebuie creată imediat după crearea unei vizualizări; în caz contrar, va apărea un mesaj de eroare.

```
Router(config-view)# secret password
```

Pasul 3. Atribuire vizualizare existentă utilizând comanda view view-name în modul de configurare a vederii. Aceasta adaugă o vizualizare CLI la supraveghere. Pot fi adăugate mai multe vizualizări. Vizualizările pot fi partajate între superviziunile.

```
Router(config-view)# view view-name
```

Pasul 4. Ieșire din modul de configurare a supravegherii tastând comanda ***exit***.

Mai mult de o vizualizare poate fi atribuită unei supervizualizări, iar vizualizările pot fi partajate între supervizualizări. Exemplul arată configurarea a trei supervizări: USER, SUPPORT și JR-ADMIN.

```
R1(config)# parser view USER superview
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
R1(config-view)# exit
R1(config)#
R1(config)# parser view SUPPORT superview
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIE
% Invalid view name SHOWVIE
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# exit
R1(config)#
R1(config)# parser view JR-ADMIN superview
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# view REBOOTVIEW
R1(config-view)# exit
R1(config)#
```

Exemplul de mai jos afișează superviziunile configurate în configurația care rulează.

Pentru a accesa vizualizările existente, se introduce comanda enable view view-name în modul utilizator și se introduce parola care a fost atribuită vizualizării personalizate. Se utilizeaza aceeași comandă pentru a comuta de la o vizualizare la alta.

```
R1# show running-config
<output omitted>
!
```

```
parser view SUPPORT superview
 secret 5 $1$Vp1O$BBB1N68Z2ekr/aLHledts.
 view SHOWVIEW
 view VERIFYVIEW
!
parser view USER superview
 secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/
 view SHOWVIEW
!
parser view JR-ADMIN superview
 secret 5 $1$8kx2$rbAe/ji220OmQ1yw.568g0
 view SHOWVIEW
 view VERIFYVIEW
 view REBOOTVIEW
```

5.2.5 - Verify Role-Based CLI Views

Pentru a verifica o vizualizare, se utilizeaza comanda enable view. Se introduce numele vizualizării de verificat și se furnizeaza parola pentru conectare la vizualizare. Se utilizeaza comanda semnului de întrebare (?) pentru a verifica dacă comenzile disponibile în vizualizare sunt corecte.

Exemplul activează supravegherea USER și listează comenzile disponibile în vizualizare.

```
R1# enable view USER
Password: <cisco1>
 R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
 R1# show ?    banner      Display banner information
  flash0:     display information about flash0: file system
  flash1:     display information about flash1: file system
  flash:      display information about flash: file system
  parser      Display parser information
  usbflash0:  display information about usbflash0: file system
```

Exemplul de mai jos activează supravegherea SUPPORT și listează comenzile disponibile în vizualizare.

```
R1# enable view SUPPORT
Password: <cisco1>
 R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  ping         Send echo messages
  show         Show running system information
 R1#
```

Acest exemplu activează vizualizarea JR-ADMIN și listează comenzile disponibile în vizualizare.

```
R1# enable view JR-ADMIN
Password:
 R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  ping         Send echo messages
  reload       Halt and perform a cold restart
  show         Show running system information
 R1#
```

Dacă nu se specifica o vizualizare pentru comanda enable view, așa cum se arată, se poate face conectarea ca root. Din vizualizarea rădăcină, se utilizeaza comanda show parser view all pentru a vedea un rezumat al tuturor vizualizărilor. Se poate observa cum asteriscul identifică superviziunile.

```
R1# show parser view
Current view is 'JR-ADMIN'
R1# enable view
Password:

R1# show parser view
Current view is 'root'
 R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 USER *
 SUPPORT *
 JR-ADMIN *
 -------(*) represent superview-------
R1#
```

5.3 SUMMARY

Configurare niveluri de privilegii - Software-ul Cisco IOS are două metode de furnizare a accesului la infrastructură: nivel de privilegii și CLI bazat pe roluri. În mod implicit, CLI-ul software Cisco IOS are două niveluri de acces la comenzi: modul User EXEC (nivel de privilegiu 1) și modul EXEC privilegiat (nivel de privilegiu 15). Există 16 niveluri de privilegii în total. Cu cât este mai mare nivelul de privilegii, cu atât mai mult acces la router are un utilizator. Pentru a configura un nivel de privilegii cu anumite comenzi, se utilizează nivelul de privilegiu exec [comandă]. Se utilizează comanda nume de utilizator pentru a atribui un nivel de privilegii unui anumit utilizator. Se utilizează comanda enable secret

pentru a atribui un nivel de privilegii unei anumite parole pentru modul EXEC. Utilizarea nivelurilor de privilegii are limitările sale:

- *Nu există control de acces la anumite interfețe, porturi, interfețe logice și sloturi pe un router.*
- *Comenzile disponibile la niveluri de privilegii inferioare sunt întotdeauna executabile la niveluri superioare.*
- *Comenzile setate special la un nivel de privilegii mai înalt nu sunt disponibile pentru utilizatorii cu privilegii mai mici.*
- *Atribuirea unei comenzi cu mai multe cuvinte cheie permite accesul la toate comenzile care folosesc acele cuvinte cheie. De exemplu, permiterea accesului la show ip route permite utilizatorului accesul la toate comenzile show și show ip.*

Configurare CLI bazat pe roluri - Într-un efort de a oferi mai multă flexibilitate decât permit nivelurile de privilegii, Cisco a introdus caracteristica de acces CLI bazată pe roluri în Cisco IOS Release 12.3(11)T. Accesul CLI bazat pe roluri permite administratorului de rețea să creeze diferite vederi ale configurațiilor routerului pentru diferiți utilizatori. CLI bazat pe roluri oferă trei tipuri de vederi care dictează ce comenzi sunt disponibile. Vizualizarea rădăcină are aceleași privilegii de acces ca un utilizator care are privilegii de nivel 15. Cu toate acestea, o vizualizare rădăcină nu este același lucru cu un utilizator de nivel 15. Doar un utilizator de vizualizare root poate configura o nouă vizualizare și poate adăuga sau elimina comenzi din vizualizările existente. Un set specific de comenzi poate fi grupat într-o vizualizare CLI. Spre deosebire de nivelurile de privilegii, o vizualizare CLI nu are ierarhie de comandă și nici vizualizări superioare sau inferioare. O vizualizare nu moștenește comenzi de la nicio altă vizualizare. O supervizualizare constă dintr-una sau mai multe vizualizări CLI. Administratorii pot defini ce comenzi sunt acceptate și ce informații de configurare sunt vizibile. Superview-urile permit unui administrator de rețea să atribuie utilizatorilor și grupurilor de utilizatori mai multe vizualizări CLI simultan, în loc să fie nevoit să atribuie o singură vizualizare CLI pentru fiecare utilizator cu toate comenzile asociate cu acea singură vizualizare CLI. Înainte ca un administrator să poată crea o vizualizare, AAA trebuie să fie activat folosind comanda aaa new-model. Pentru a configura și edita vizualizări, un administrator trebuie să se conecteze ca vizualizare rădăcină utilizând comanda EXEC cu privilegii de vizualizare activată. Se poate folosi și comanda enable view root. Când vi se

solicită, introduceți parola secretă de activare. Există cinci pași pentru a crea și gestiona o anumită vizualizare. Pașii de configurare a unei supervizuări sunt în esență aceiași cu configurarea unei vizualizări CLI, cu excepția faptului că comanda view view-name este utilizată pentru a atribui comenzi supervizualizării.