WLAN

VLAN

Înainte de a putea configura un comutator, trebuie să îl porniți și să îi permiteți să treacă prin secvența de pornire în cinci pași. Acest subiect acoperă elementele de bază ale configurării unui comutator și include un laborator la sfârșit.

După ce un comutator Cisco este pornit, acesta parcurge următoarea secvență de pornire în cinci pași:

Pasul 1: În primul rând, comutatorul încarcă un program de autotestare la pornire (POST) stocat în ROM. POST verifică subsistemul CPU. Testează CPU, DRAM și porțiunea dispozitivului flash care alcătuiește sistemul de fișiere flash.

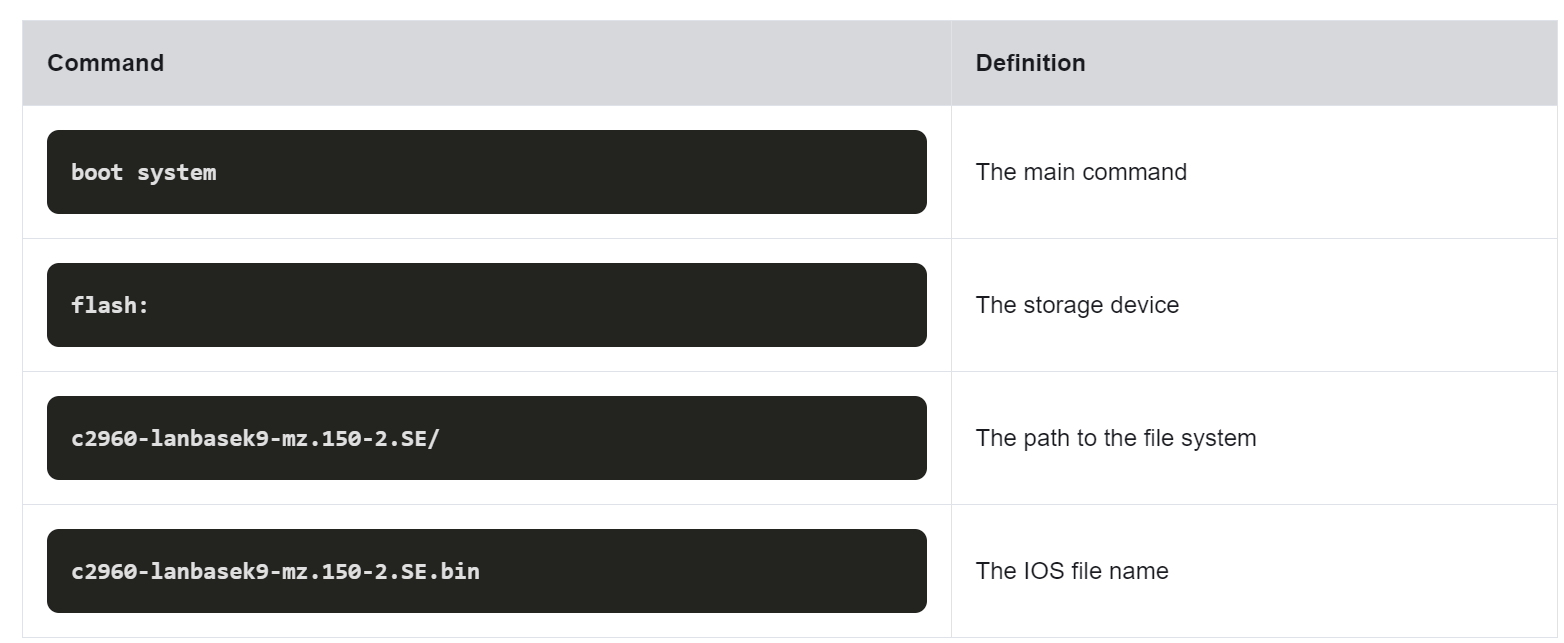
Pasul 2: Apoi, comutatorul încarcă software-ul încărcător de pornire. Încărcătorul de pornire este un mic program stocat în ROM care rulează imediat după finalizarea cu succes a POST.

Pasul 3: încărcătorul de pornire efectuează inițializarea CPU la nivel scăzut. Inițializează registrele CPU, care controlează unde este mapată memoria fizică, cantitatea de memorie și viteza acesteia.

Pasul 4: încărcătorul de pornire inițializează sistemul de fișiere flash de pe placa de sistem.

Pasul 5: În cele din urmă, încărcătorul de pornire localizează și încarcă o imagine implicită a software-ului sistemului de operare IOS în memorie și oferă controlul comutării la IOS.

S1(config)# **boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin**



LED de sistem (SYST)

Arată dacă sistemul primește alimentare și funcționează corect. Dacă LED-ul este stins, înseamnă că sistemul nu este pornit. Dacă LED-ul este verde, sistemul funcționează normal. Dacă LED-ul este portocaliu, sistemul primește alimentare, dar nu funcționează corect.

LED sistem de alimentare redundant (RPS).

Afișează starea RPS. Dacă LED-ul este stins, RPS-ul este stins sau nu este conectat corect. Dacă LED-ul este verde, RPS-ul este conectat și gata să furnizeze energie de rezervă. Dacă LED-ul clipește în verde, RPS-ul este conectat, dar nu este disponibil, deoarece furnizează energie unui alt dispozitiv. Dacă LED-ul este portocaliu, RPS-ul este în modul standby sau într-o stare de defecțiune. Dacă LED-ul clipește portocaliu, sursa de alimentare internă a comutatorului a eșuat și RPS-ul furnizează energie.

LED Stare Port

Indică faptul că modul de stare a portului este selectat atunci când LED-ul este verde. Acesta este modul implicit. Când sunt selectate, LED-urile portului vor afișa culori cu semnificații diferite. Dacă LED-ul este stins, nu există nicio legătură sau portul a fost închis administrativ. Dacă LED-ul este verde, este prezentă o legătură. Dacă LED-ul clipește verde, există activitate și portul trimite sau primește date. Dacă LED-ul este alternativ verde-chihlimbar, există o eroare a legăturii. Dacă LED-ul este portocaliu, portul este blocat pentru a se asigura că nu există o buclă în domeniul de redirecționare și nu redirecționează date (de obicei, porturile vor rămâne în această stare în primele 30 de secunde după activare). Dacă LED-ul clipește portocaliu, portul este blocat pentru a preveni o posibilă buclă în domeniul de redirecționare.

Port Duplex LED

Indică faptul că modul duplex al portului este selectat când LED-ul este verde. Când sunt selectate, LED-urile portului care sunt stinse sunt în modul semi-duplex. Dacă LED-ul portului este verde, portul este în modul full-duplex.

LED-ul pentru viteza portului

Indică faptul că este selectat modul de viteză a portului. Când sunt selectate, LED-urile portului vor afișa culori cu semnificații diferite. Dacă LED-ul este stins, portul funcționează la 10 Mbps. Dacă LED-ul este verde, portul funcționează la 100 Mbps. Dacă LED-ul clipește verde, portul funcționează la 1000 Mbps.

LED mod Power over Ethernet (PoE).

Dacă PoE este acceptat, va fi prezent un LED pentru modul PoE. Dacă LED-ul este stins, indică faptul că modul PoE nu este selectat și că niciunul dintre porturi nu a primit alimentarea sau a fost plasat într-o stare de defecțiune. Dacă LED-ul clipește portocaliu, modul PoE nu este selectat, dar cel puțin unuia dintre porturi i-a fost refuzată alimentarea sau are o defecțiune PoE. Dacă LED-ul este verde, înseamnă că modul PoE este selectat și LED-urile portului vor afișa culori cu semnificații diferite. Dacă LED-ul portului este stins, PoE este stins. Dacă LED-ul portului este verde, PoE este pornit. Dacă LED-ul portului este alternativ verde-chihlimbar, PoE este refuzat deoarece furnizarea de energie a dispozitivului alimentat va depăși capacitatea de alimentare a comutatorului. Dacă LED-ul clipește portocaliu, PoE este oprit din cauza unei defecțiuni. Dacă LED-ul este portocaliu, PoE pentru port a fost dezactivat.

**Recuperarea dintr-o blocare a sistemului**

Încărcătorul de pornire oferă acces la comutator dacă sistemul de operare nu poate fi utilizat din cauza fișierelor de sistem lipsă sau deteriorate. Încărcătorul de pornire are o linie de comandă care oferă acces la fișierele stocate în memoria flash.

Bootloader-ul poate fi accesat printr-o conexiune la consolă urmând acești pași:

Pasul 1. Conectați un computer prin cablu de consolă la portul consolei comutatorului. Configurați software-ul de emulare a terminalului pentru a vă conecta la comutator.

Pasul 2. Deconectați cablul de alimentare al comutatorului.

Pasul 3. Reconectați cablul de alimentare la comutator și, în decurs de 15 secunde, apăsați și mențineți apăsat butonul Mod în timp ce LED-ul Sistem încă clipește verde.

Pasul 4. Continuați să apăsați butonul Mod până când LED-ul de sistem devine galben pentru scurt timp și apoi verde continuu; apoi eliberați butonul Mode.

Pasul 5. Comutatorul încărcător de pornire: promptul apare în software-ul de emulare a terminalului de pe computer.

În mod implicit, comutatorul încearcă să pornească automat utilizând informațiile din variabila de mediu BOOT. Pentru a vedea calea variabilei de mediu switch BOOT, tastați comanda set. Apoi, inițializați sistemul de fișiere flash folosind comanda **flash\_init** pentru a vizualiza fișierele curente în flash, așa cum se arată în rezultat.

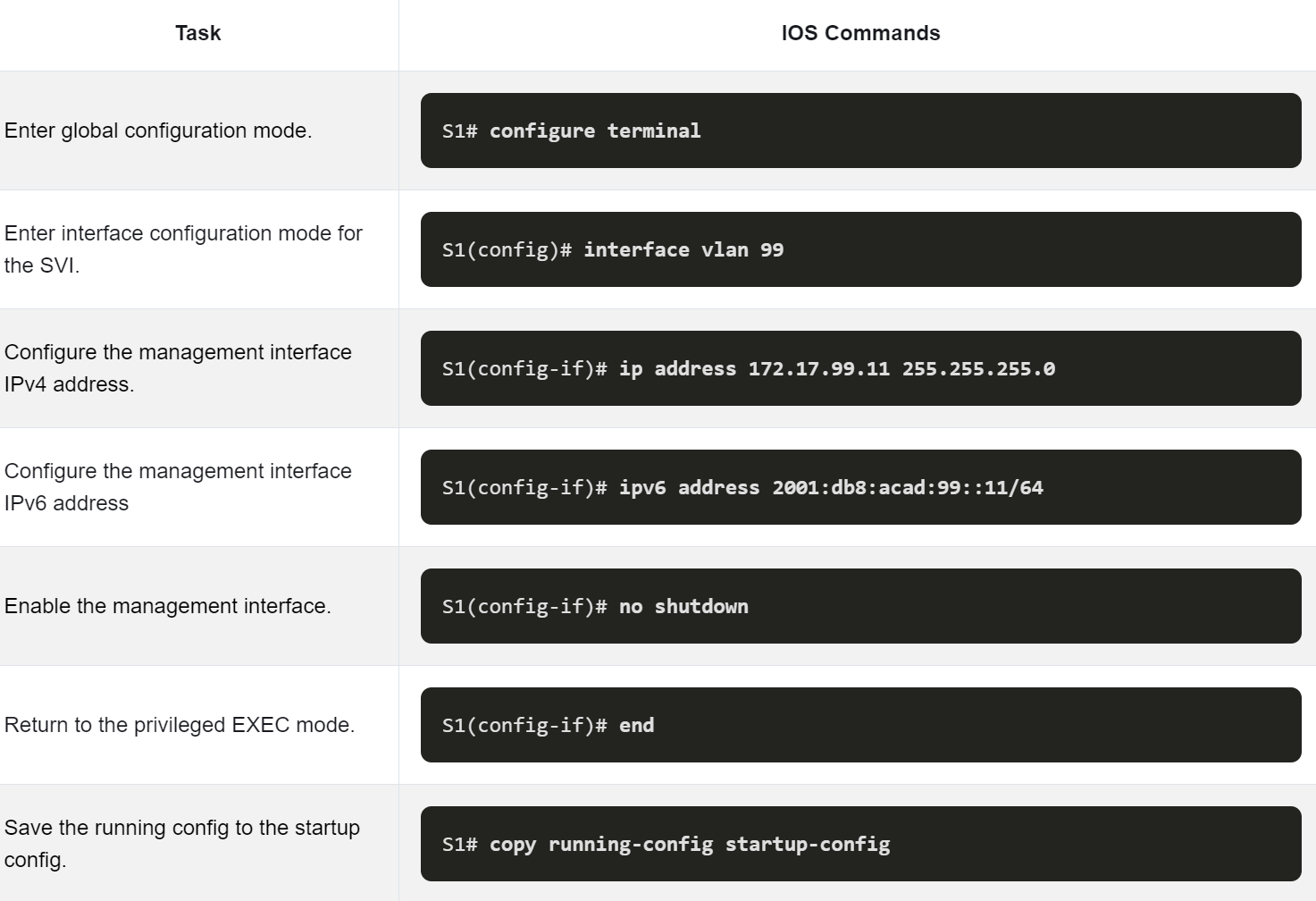
După inițializarea flash-ului, puteți introduce comanda **dir flash**: pentru a vizualiza directoarele și fișierele în flash, așa cum se arată în rezultat.

Introduceți comanda **BOOT=flash** pentru a schimba calea variabilei de mediu BOOT pe care comutatorul o folosește pentru a încărca noul IOS în flash. Pentru a verifica noua cale a variabilei de mediu BOOT, lansați din nou comanda set. În cele din urmă, pentru a încărca noul IOS, tastați comanda de pornire fără niciun argument, așa cum se arată în rezultat.

**SVI**

Pentru a pregăti un comutator pentru acces la managementul de la distanță, comutatorul trebuie să aibă o interfață virtuală a comutatorului (SVI) configurată cu o adresă IPv4 și o mască de subrețea sau o adresă IPv6 și o lungime de prefix pentru IPv6. SVI este o interfață virtuală, nu un port fizic al comutatorului.

**Configure the Management Interface**

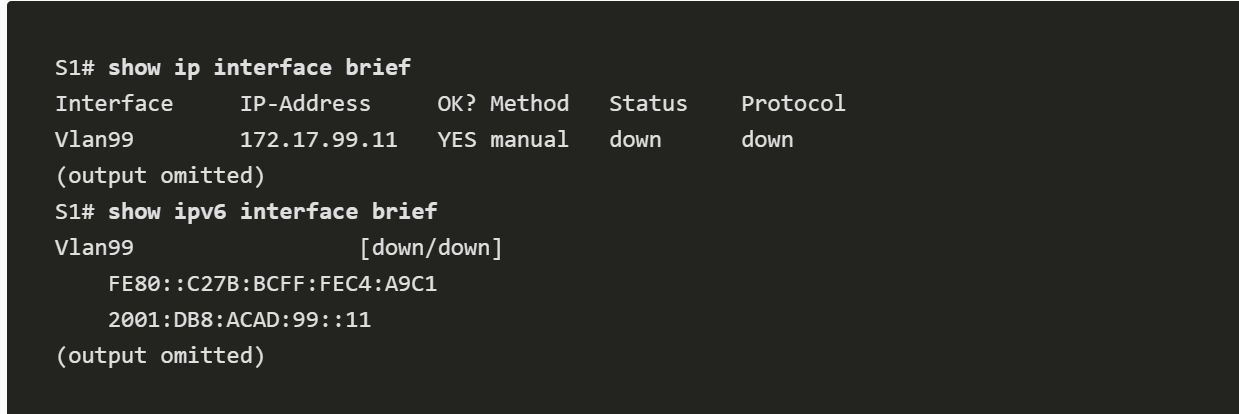


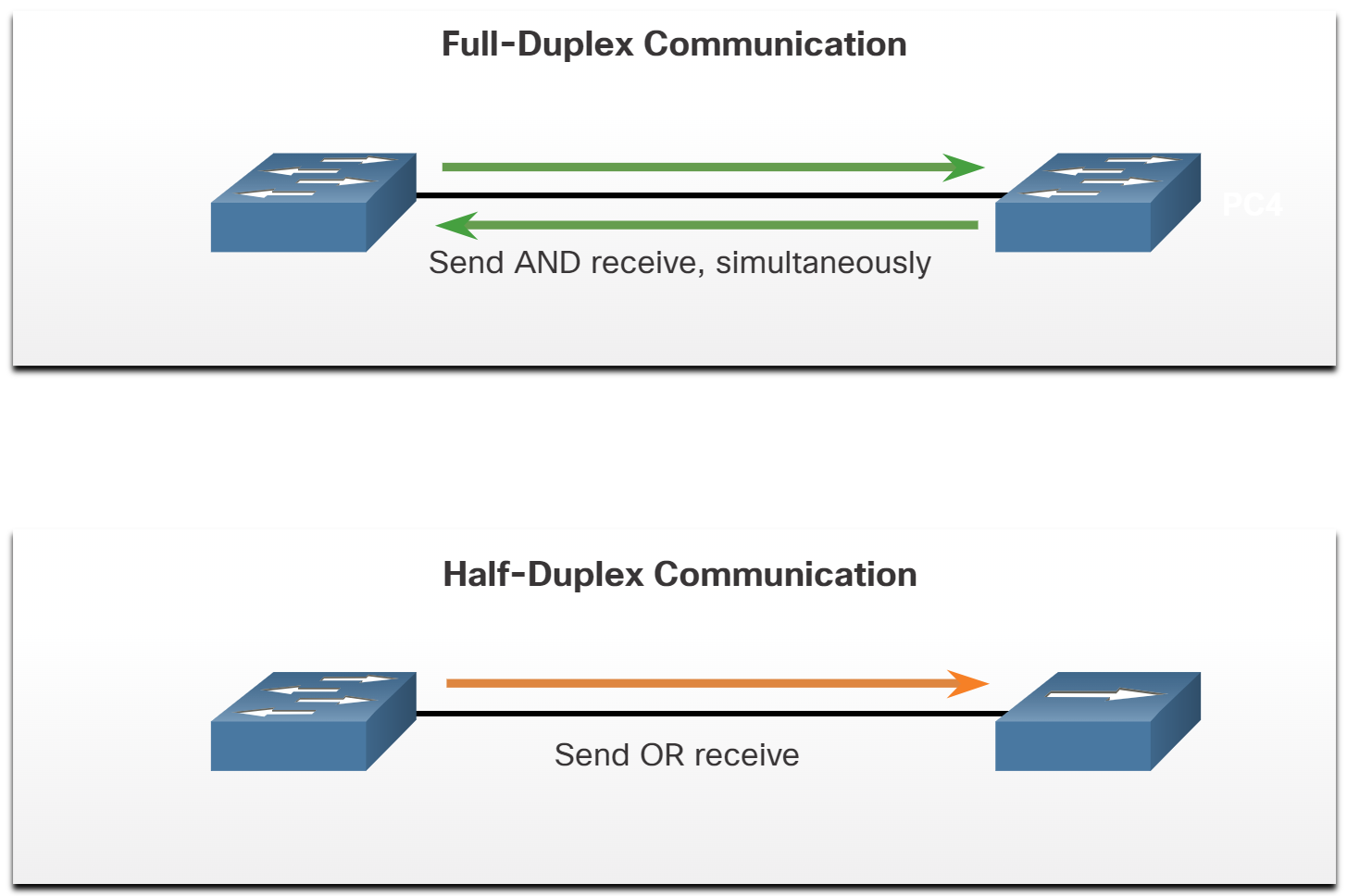
**Configure the Default Gateway (pentru acces remote nu fizic)**



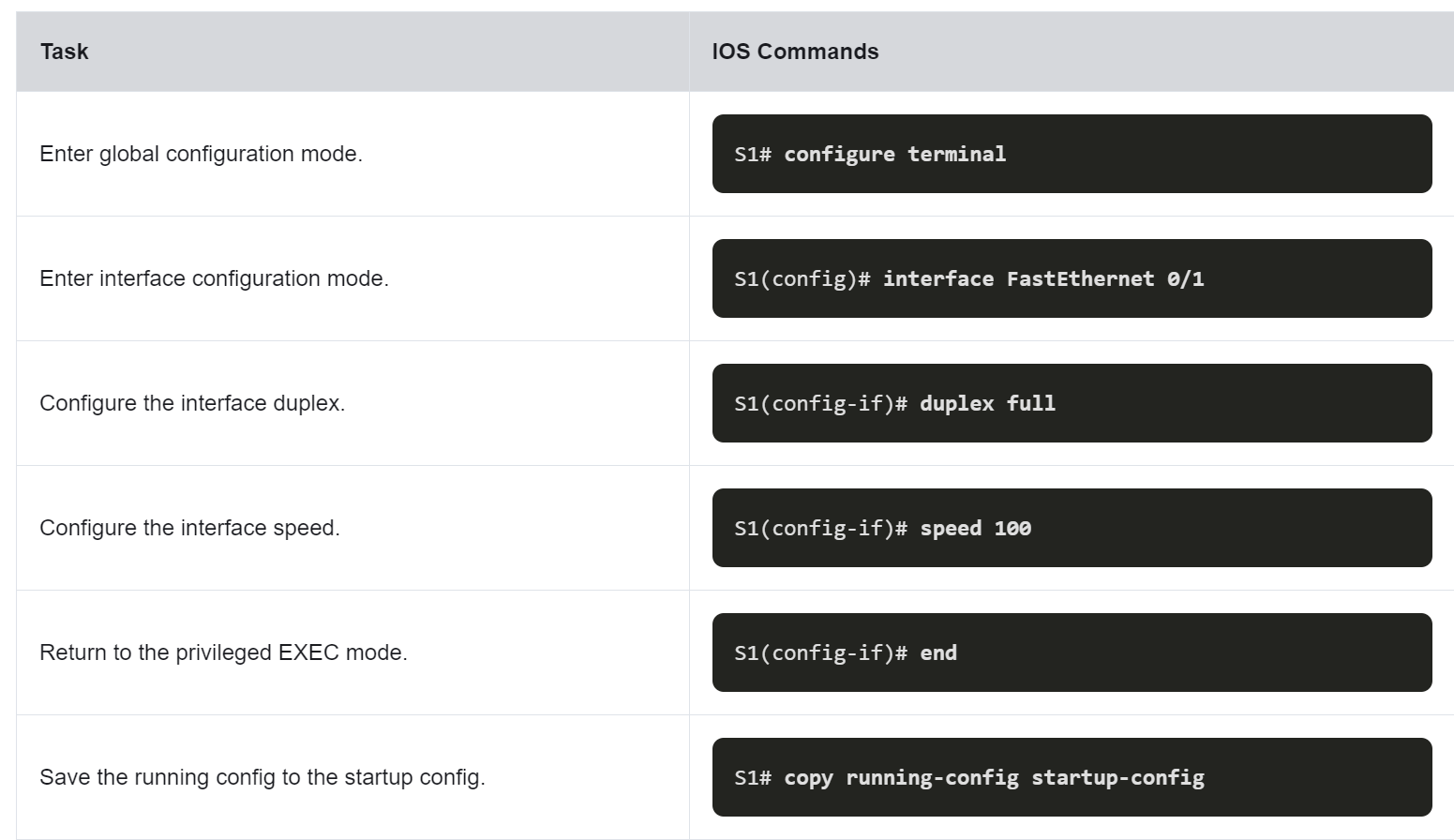
**Verify Configuration**

Comenzile **show ip interface brief** și **show ipv6 interface brief** sunt utile pentru a determina starea atât a interfețelor fizice, cât și a celor virtuale. Ieșirea afișată confirmă că interfața VLAN 99 a fost configurată cu o adresă IPv4 și IPv6.





Configurare full-duplex si viteza



**Auto-MDIX**

Când auto-MDIX este activat, interfața detectează automat tipul de conexiune prin cablu necesar (direct sau încrucișat) și configurează conexiunea în mod corespunzător. Când vă conectați la comutatoare fără caracteristica auto-MDIX, trebuie folosite cabluri directe pentru a vă conecta la dispozitive precum servere, stații de lucru sau routere. Cablurile încrucișate trebuie utilizate pentru conectarea la alte comutatoare sau repetoare.

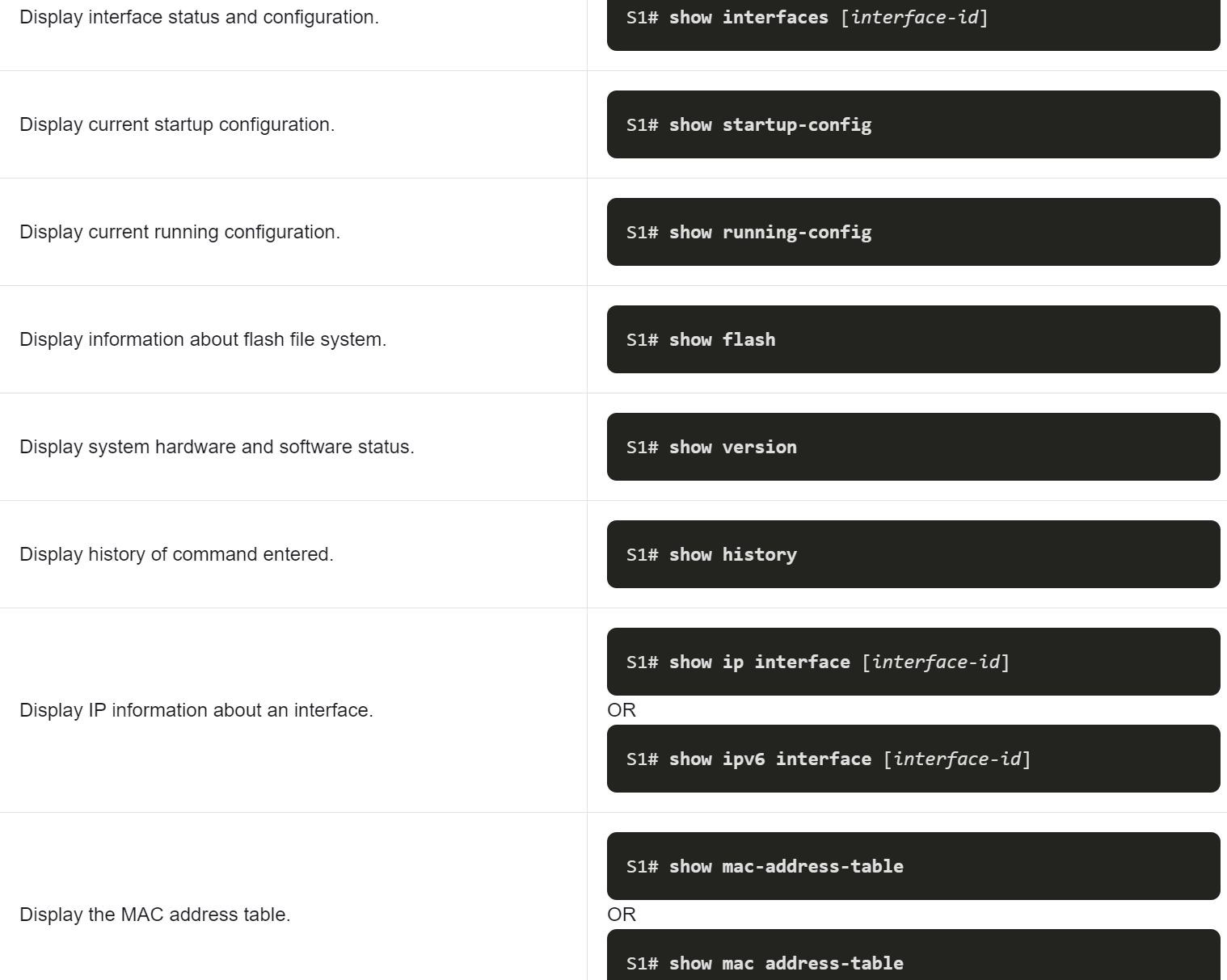
S1(config-if)# **mdix auto**

Verificare **MDIX** setat

S1# **show controllers ethernet-controller fa0/1 phy | include MDIX**

Auto-MDIX           :  On   [AdminState=1   Flags=0x00052248]

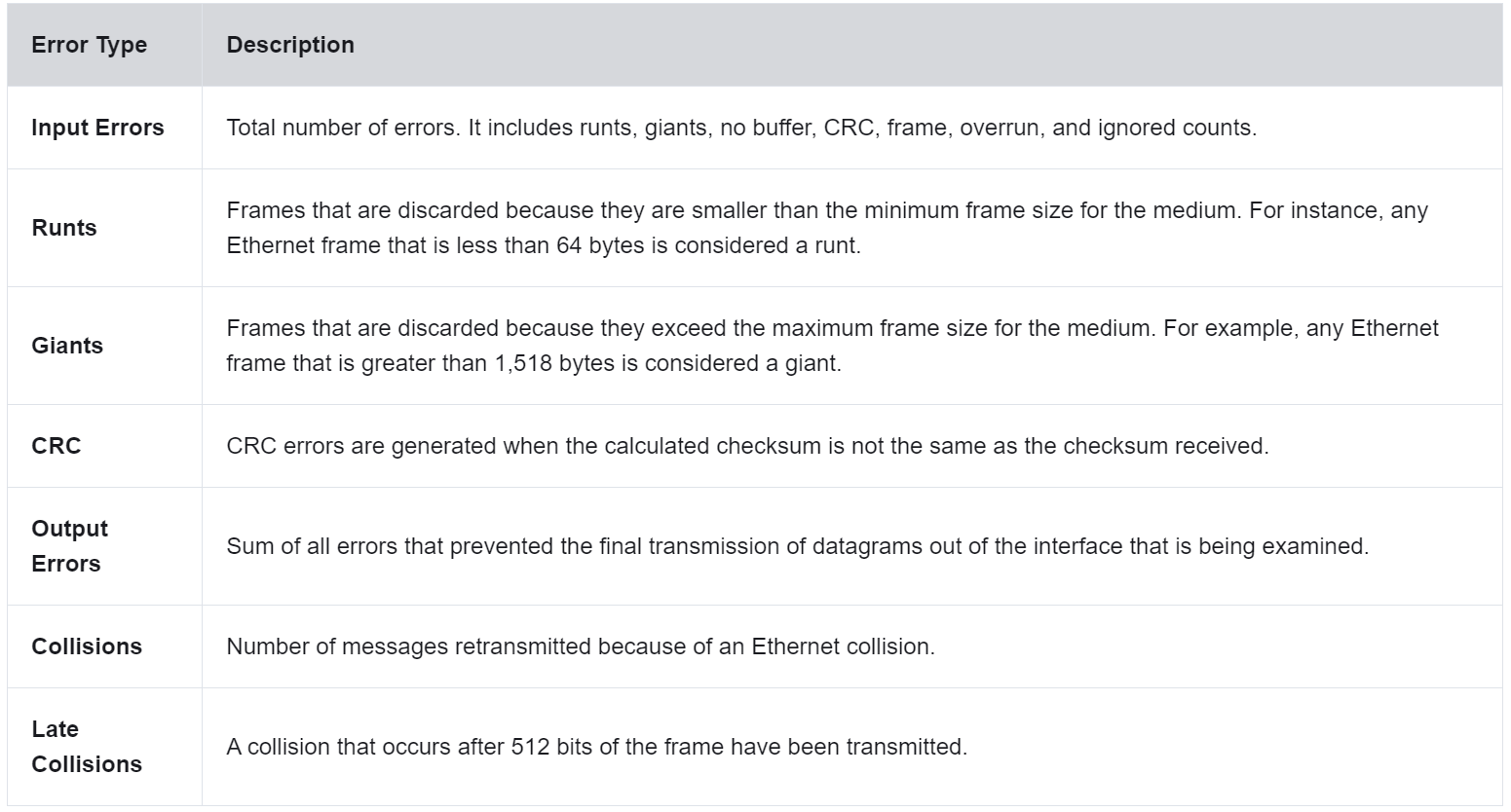
Cele mai populare comenzi pentru Switch



Comanda **show running-config** poate fi utilizată pentru a verifica dacă comutatorul a fost configurat corect.

Comanda **show interfaces** este o altă comandă folosită în mod obișnuit, care afișează informații despre stare și statistici pe interfețele de rețea ale comutatorului la fel si erorile afiseaza. Comanda show interfaces este folosită frecvent la configurarea și monitorizarea dispozitivelor de rețea.

Erori afisate prin **show interfaces**



**„Erori de intrare”** este suma tuturor erorilor din datagramele care au fost primite pe interfața examinată. Acestea includ runts, giants, CRC, fără buffer, frame, overrun și ignorate. Erorile de intrare raportate de la comanda show interfaces includ următoarele:

**Runt Frames** - Cadrele Ethernet care sunt mai scurte decât lungimea minimă permisă de 64 de octeți se numesc runt. NIC-urile defectuoase sunt cauza obișnuită a cadrelor runt excesive, dar pot fi cauzate și de coliziuni.

**Giants** - Cadrele Ethernet care sunt mai mari decât dimensiunea maximă permisă se numesc giganți.

**Erori CRC -** Pe interfețele Ethernet și seriale, erorile CRC indică de obicei o eroare media sau cablu. Cauzele comune includ interferențe electrice, conexiuni slăbite sau deteriorate sau cablare incorectă. Dacă vedeți multe erori CRC, există prea mult zgomot pe legătură și ar trebui să inspectați cablul. De asemenea, ar trebui să căutați și să eliminați sursele de zgomot.

**„Erori de ieșire”** este suma tuturor erorilor care au împiedicat transmiterea finală a datagramelor pe interfața care este examinată. Erorile de ieșire raportate de la comanda show interfaces includ următoarele:

**Coliziuni** - Coliziunile în operațiunile semi-duplex sunt normale. Cu toate acestea, nu ar trebui să vedeți niciodată coliziuni pe o interfață configurată pentru comunicații full-duplex.

**Coliziuni tardive** - O coliziune tardivă se referă la o coliziune care are loc după ce au fost transmisi 512 biți ai cadrului. Lungimile excesive ale cablurilor sunt cea mai frecventă cauză a coliziunilor târzii. O altă cauză comună este configurarea greșită duplex. De exemplu, puteți avea un capăt al unei conexiuni configurat pentru full-duplex și celălalt pentru semi-duplex. Veți vedea coliziuni târzii pe interfața care este configurată pentru semi-duplex. În acest caz, trebuie să configurați aceeași setare duplex la ambele capete. O rețea proiectată și configurată corespunzător nu ar trebui să aibă niciodată coliziuni târzii.

Enter configuration mode and set FastEthernet0/1 duplex, speed, and MDIX to auto and save the configuration to NVRAM.

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#interface FastEthernet0/1

S1(config-if)#duplex auto

S1(config-if)#speed auto

S1(config-if)#mdix auto

End out of interface configuration mode and save the configuration to NVRAM.

S1(config-if)#end

%SYS-5-CONFIG\_I: Configured from console by console

S1#copy running-config startup-config

You have successfully configured duplex, speed, and Auto-MDIX settings on a switch interface and saved the configuration to NVRAM.

**Telnet** folosește portul TCP 23. Este un protocol mai vechi care utilizează transmisia nesigură de text simplu atât a autentificării de conectare (nume de utilizator și parolă), cât și a datelor transmise între dispozitivele care comunică.

**Secure Shell (SSH)** este un protocol securizat care folosește portul TCP 22. Acesta oferă o conexiune de gestionare sigură (criptată) la un dispozitiv la distanță. SSH ar trebui să înlocuiască Telnet pentru conexiunile de gestionare. SSH oferă securitate pentru conexiunile la distanță prin furnizarea de criptare puternică atunci când un dispozitiv este autentificat (nume de utilizator și parolă) și, de asemenea, pentru datele transmise între dispozitivele care comunică.

**show version** - pentru a vedea ce IOS rulează comutatorul în prezent. Un nume de fișier IOS care include combinația „k9” acceptă caracteristici și capabilități criptografice (criptate), respectiv poate folosi **SSH protocol.**

**Ex:** S1# **show version**

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE (fc1)

**Configure SSH**

Pasul 1

Verificați suportul SSH.

Utilizați comanda **show ip ssh** pentru a verifica dacă comutatorul acceptă SSH. Dacă comutatorul nu rulează un IOS care acceptă caracteristici criptografice, această comandă este nerecunoscută.

Pasul 2

Configurați domeniul IP.

Configurați numele domeniului IP al rețelei utilizând comanda **ip domain-name *domain-name*** global configuration mode.

S1(config)# **ip domain-name cisco.com**

Pasul 3

Generați perechi de chei RSA.

Nu toate versiunile IOS sunt implicite la versiunea 2 SSH, iar versiunea 1 SSH are defecte de securitate cunoscute. Pentru a configura SSH versiunea 2, lansați comanda **ip ssh version 2** global configuration mode. Generarea unei perechi de chei RSA activează automat SSH. Utilizați comanda **cripto key generate rsa** global configuration mode pentru a activa serverul SSH pe switch și pentru a genera o pereche de chei RSA. La generarea cheilor RSA, administratorului i se solicită să introducă o lungime a modulului. Configurația eșantionului din figură folosește o dimensiune a modulului de 1.024 de biți. O lungime mai mare a modulului este mai sigură, dar este nevoie de mai mult pentru generare și utilizare.

S1(config)# **crypto key generate rsa**

How many bits in the modulus [512]: **1024**

Pasul 4

Configurați autentificarea utilizatorului.

Serverul SSH poate autentifica utilizatorii local sau folosind un server de autentificare. Pentru a utiliza metoda de autentificare locală, creați o pereche de nume de utilizator și parolă utilizând comanda pentru modul de configurare globală nume de utilizator, parolă secretă. În exemplu, administratorului utilizatorului i se atribuie parola ccna.

S1(config)# **username admin secret ccna**

Pasul 5

Configurați liniile **vty**.

Activați protocolul SSH pe liniile vty utilizând comanda **transport input ssh** line configuration mode. Catalyst 2960 are linii vty de la 0 la 15. Această configurație previne conexiunile non-SSH (cum ar fi Telnet) și limitează comutatorul să accepte numai conexiuni SSH. Utilizați comanda **line vty** global configuration mode și apoi comanda **login local** line configuration mode pentru a solicita autentificare locală pentru conexiunile SSH din baza de date locală cu nume de utilizator.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

S1(config-line)# **login local**

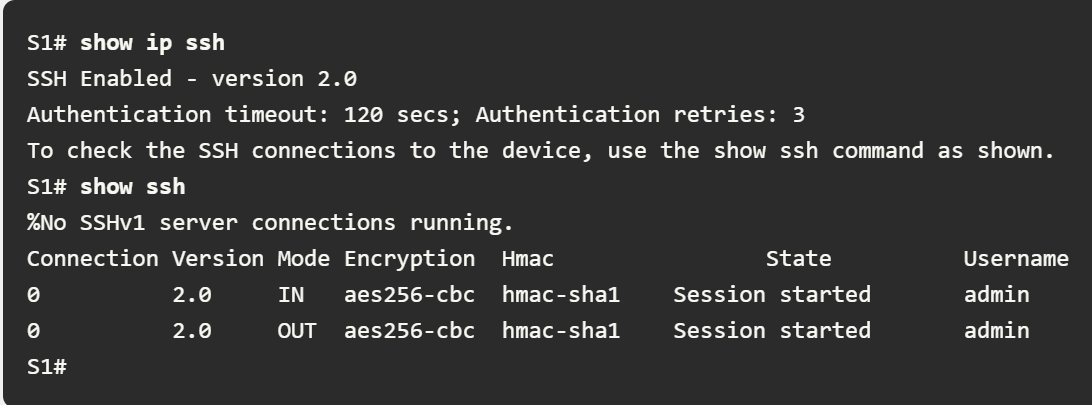
S1(config-line)# **exit**

Pasul 6

Activați SSH versiunea 2.

În mod implicit, SSH acceptă ambele versiuni 1 și 2. Când acceptă ambele versiuni, acest lucru este afișat în ieșirea **show ip ssh** ca suport pentru versiunea 2. Activați versiunea SSH utilizând comanda de configurare globală **ip ssh** versiunea 2.

S1(config)# **ip ssh version 2**



**Configurare BASIC router**

Router# **configure terminal**

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# **hostname R1**

R1(config)# **enable secret class**

R1(config)# **line console 0**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)# **service password-encryption**

R1(config)#

Acces neautorizat banner

R1(config)# **banner motd #Authorized Access Only!#**

R1(config)#

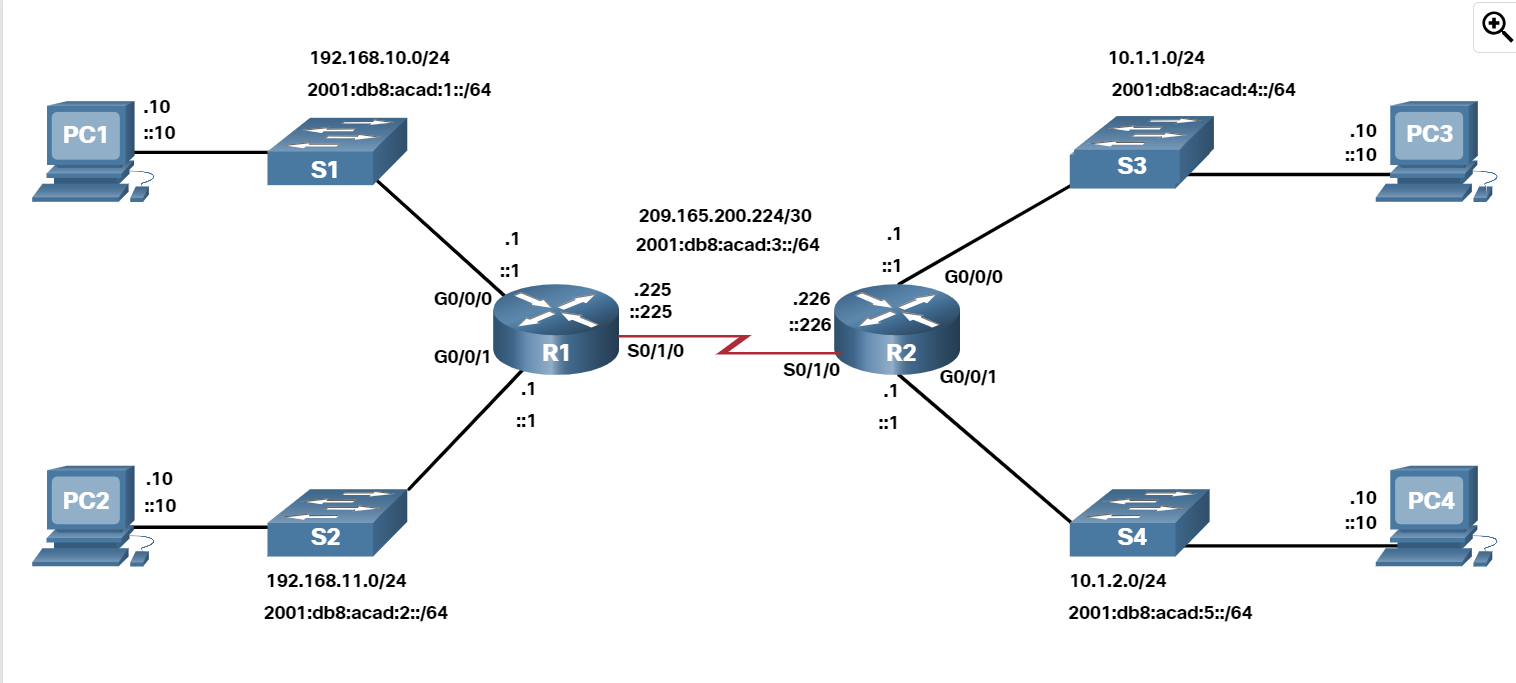
Salvare schimbari

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]



**Configure router interface**

R1(config)# **interface gigabitethernet 0/0/0**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:1::1/64**

R1(config-if)# **description Link to LAN 1**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **ip address 192.168.11.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:2::1/64**

R1(config-if)# **description Link to LAN 2**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **ip address 209.165.200.225 255.255.255.252**

R1(config-if)# **ipv6 address 2001:db8:acad:3::225/64**

R1(config-if)# **description Link to R2**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)#

Interfața **loopback** este o interfață logică care este internă routerului. Nu este atribuit unui port fizic și nu poate fi niciodată conectat la niciun alt dispozitiv. Este considerată o interfață software care este plasată automat într-o stare „up”, atâta timp cât routerul funcționează.

R1(config)# **interface loopback 0**

R1(config-if)# **ip address 10.0.0.1 255.255.255.0**

R1(config-if)# **exit**

R1(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

Următoarele comenzi sunt deosebit de utile pentru a **identifica rapid starea unei interfețe**:

* **show ip interface brief** și **show ipv6 interface brief** - Acestea afișează un rezumat pentru toate interfețele, inclusiv adresa IPv4 sau IPv6 a interfeței și starea operațională curentă.
* **show running-config interface *interface-id*** - Aceasta afișează comenzile aplicate la interfața specificată.
* **show ip route** si **show ipv6 route** - Acestea afișează conținutul tabelului de rutare IPv4 sau IPv6 stocat în RAM. În Cisco IOS 15, interfețele active ar trebui să apară în tabelul de rutare cu două intrări asociate identificate prin codul „C” (Conectat) sau „L” (Local). În versiunile anterioare de IOS, va apărea doar o singură intrare cu codul „C”.

Următoarele două comenzi sunt folosite pentru a aduna informații mai detaliate despre interfață:

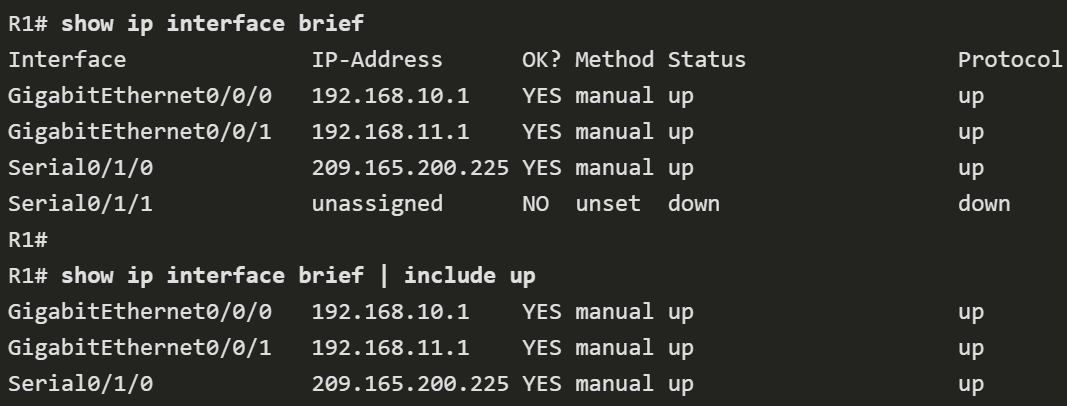
**show interfaces** - Afișează informații despre interfață și numărul de flux de pachete pentru toate interfețele de pe dispozitiv.

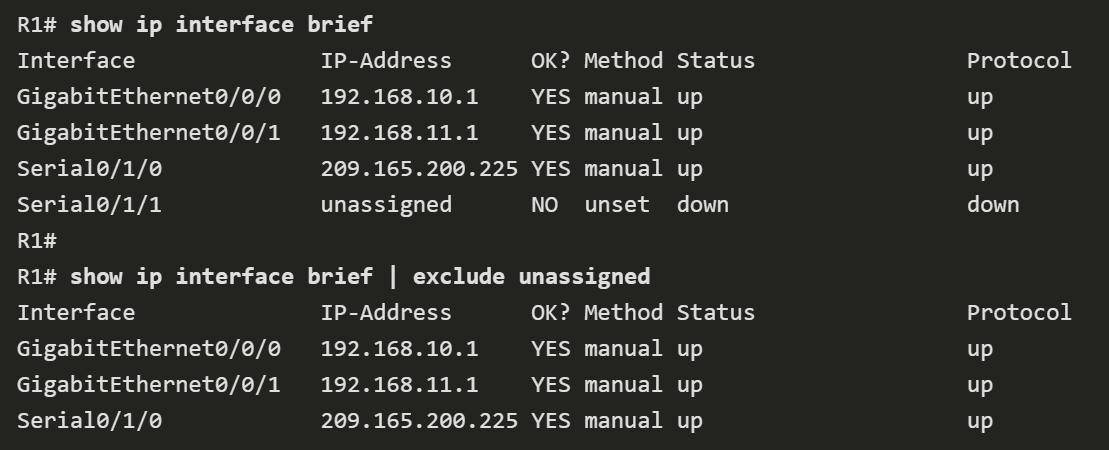
**show ip interface** and show ipv6 interface - Afișează informațiile legate de IPv4 și IPv6 pentru toate interfețele de pe un router.

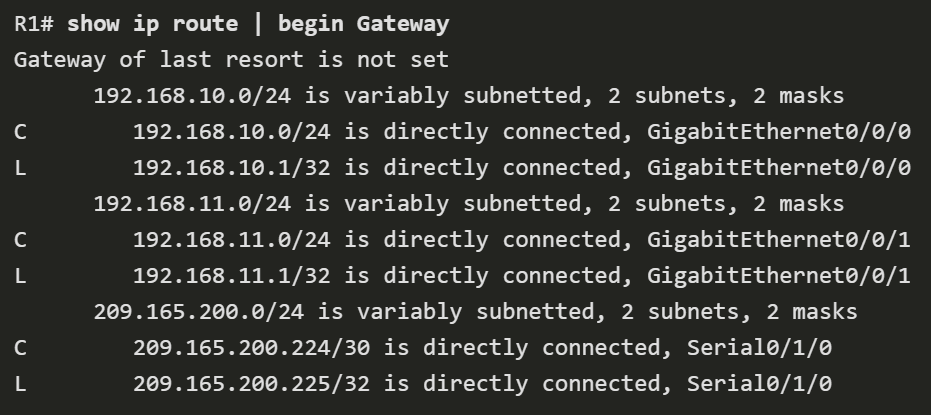
**Filtrare comanda de iesire**

R1# **show running-config | section line vty**

line vty 0 4 password 7 110A1016141D login transport input all







**Command history**

Pentru a reapela comenzile din memoria tampon de istoric, apăsați Ctrl+P sau tasta săgeată sus. Ieșirea comenzii începe cu cea mai recentă comandă. Repetați secvența de taste pentru a rememora succesiv comenzi mai vechi. Pentru a reveni la comenzile mai recente din memoria tampon de istoric, apăsați Ctrl+N sau tasta săgeată în jos. Repetați secvența de taste pentru a reapela succesiv comenzi mai recente.

R1# **terminal history size 200**

R1# **show history**

  show ip int brief

  show interface g0/0/0

  show ip route

  show running-config

  show history

  terminal history size 200

R1>terminal history size 200

Enter the command to display command history.

R1>show history

show running-config | section line con

show ip interface brief | include down

show ip interface brief | exclude up

show running-config | begin line

terminal history size 200

show history

R1>

**Ingress**- Aceasta este utilizată pentru a descrie portul în care un cadru intră în dispozitiv.

**Egress**- Aceasta este utilizată pentru a descrie portul pe care cadrele îl vor folosi atunci când părăsesc dispozitivul.

Pe măsură ce switch-ul învață relația dintre porturi și dispozitive, construiește un tabel numit tabel de adrese MAC. Acest tabel este stocat în memoria adresabilă conținutului (**CAM**), care este un tip special de memorie utilizat în aplicațiile de căutare de mare viteză. Din acest motiv, tabelul de adrese MAC este uneori numit și tabel CAM

**Următorul proces în doi pași este efectuat pe fiecare cadru Ethernet care intră într-un comutator.**

**Pasul 1**. Aflați - Examinarea adresei MAC sursă

Fiecare cadru care intră într-un comutator este verificat pentru noi informații de învățat. Face acest lucru examinând adresa MAC sursă a cadrului și numărul portului în care cadrul a intrat în switch:

Dacă adresa MAC sursă nu există în tabelul de adrese MAC, adresa MAC și numărul portului de intrare sunt adăugate în tabel.

Dacă adresa MAC sursă există, comutatorul actualizează cronometrul de reîmprospătare pentru acea intrare. În mod implicit, majoritatea switch-urilor Ethernet păstrează o intrare în tabel timp de cinci minute. Dacă adresa MAC sursă există în tabel, dar pe un port diferit, comutatorul o tratează ca pe o intrare nouă. Intrarea este înlocuită folosind aceeași adresă MAC, dar cu numărul de port mai recent.

**Pasul 2**. Redirecționare - Examinarea adresei MAC de destinație

Dacă adresa MAC de destinație este o adresă unicast, comutatorul va căuta o potrivire între adresa MAC de destinație a cadrului și o intrare din tabelul său de adrese MAC:

Dacă adresa MAC de destinație este în tabel, aceasta va redirecționa cadrul din portul specificat.

Dacă adresa MAC de destinație nu se află în tabel, comutatorul va redirecționa cadrul către toate porturile, cu excepția portului de intrare. Acesta se numește unicast necunoscut. Dacă adresa MAC de destinație este o difuzare sau o multicast, cadrul este, de asemenea, inundat de toate porturile, cu excepția portului de intrare.

**ASIC**-urile reduc timpul de gestionare a cadrelor în cadrul dispozitivului și permit dispozitivului să gestioneze un număr crescut de cadre fără a degrada performanța.

* **Store-and-forward switching**- Această metodă ia o decizie de redirecționare pe un cadru după ce a primit întregul cadru și a verificat cadrul pentru erori folosind un mecanism matematic de verificare a erorilor cunoscut sub numele de verificare ciclică a redundanței (CRC). Comutarea de stocare și redirecționare este principala metodă de comutare LAN a Cisco.
  + **Error checking**
  + **Automatic buffering**
* **Cut-through switching**- Această metodă începe procesul de redirecționare după ce adresa MAC de destinație a unui cadru de intrare și portul de ieșire au fost determinate.

**1.2.9 Syntax Checker - Configure Switch Ports**

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#interface FastEthernet0/1

S1(config-if)#duplex auto

S1(config-if)#speed auto

S1(config-if)#mdix auto

End out of interface configuration mode and save the configuration to NVRAM.

S1(config-if)#end

%SYS-5-CONFIG\_I: Configured from console by console

S1#copy running-config startup-config

**1.4.2 Syntax Checker - Configure Basic Router Settings**

Enter global configuration mode and name the router **R2**.

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R2

Configure **class** as the secret password.

R1(config)#enable secret class

Configure **cisco** as the console line password and require users to login. Then exit line configuration mode.

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

Configure **cisco** as the vty password for lines 0 through 4 and require users to login.

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

Exit line configuration mode and encrypt all plaintext passwords.

R1(config-line)#exit

R1(config)#service password-encryption

Enter the banner **Authorized Access Only!** and use **#** as the delimiting character.

R1(config)#banner motd #Authorized Access Only!#

Exit global configuration mode and save the configuration.

R1(config)#exit

R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

You successfully configured R2 with in

**1.4.5 Syntax Checker - Configure Router Interfaces**

Configure GigabitEthernet 0/0/0.

* Use **g0/0/0** to enter interface configuration mode.
* Configure the IPv4 address **10.1.1.1** and subnet mask **255.255.255.0**.
* Configure the IPv6 address **2001:db8:acad:4::1/64**.
* Describe the link as **Link to LAN 3**.
* Activate the interface.

Router(config)#interface g0/0/0

Router(config-if)#ip address 10.1.1.1 255.255.255.0

Router(config-if)#ipv6 address 2001:db8:acad:4::1/64

Router(config-if)#description Link to LAN 3

Router(config-if)#no shutdown

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Configure GigabitEthernet 0/0/1.

* Use **g0/0/1** to enter interface configuration mode.
* Configure the IPv4 address **10.1.2.1** and subnet mask **255.255.255.0**.
* Configure the IPv6 address **2001:db8:acad:5::1/64**.
* Describe the link as **Link to LAN 4**.
* Activate the interface.

Router(config-if)#interface g0/0/1

Router(config-if)#ip address 10.1.2.1 255.255.255.0

Router(config-if)#ipv6 address 2001:db8:acad:5::1/64

Router(config-if)#description Link to LAN 4

Router(config-if)#no shutdown

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

Configure Serial 0/0/0.

* Use **s0/0/0** to enter interface configuration mode.
* Configure the IPv4 address **209.165.200.226** and subnet mask **255.255.255.252**.
* Configure the IPv6 address **2001:db8:acad:3::226/64**.
* Describe the link as **Link to R1**.
* Activate the interface.

Router(config-if)#interface s0/0/0

Router(config-if)#ip address 209.165.200.226 255.255.255.252

Router(config-if)#ipv6 address 2001:db8:acad:3::226/64

Router(config-if)#description Link to R1

Router(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

You successfully configured the R2 router interfaces.

**1.5.7 Syntax Checker - Filter Show Command Output**

Enter the command to filter the show running-config output for the 'line con' section.

R1#show running-config | section line con

line con 0

password 7 05080F1C2243

transport input none

Enter the command to filter for 'down' interfaces in the brief listing.

R1#show ip interface brief | include down

Serial0/1/1 unassigned NO unset down down

Enter the command to exclude 'up' interfaces in the brief listing.

R1#show ip interface brief | exclude up

Interface IP-Address OK? Method Status Protocol

Serial0/1/1 unassigned NO unset down down

Enter the command to filter the show running-config output to begin at the word 'line'.

R1#show running-config | begin line

line con 0

password 7 05080F1C2243

transport input none

stopbits 1

line vty 0 4

password 7 110A1016141D

login

transport input all

**1.5.9 Syntax Checker - Command History Features**

Enter the command to set the number of lines in command history to 200.

R1>terminal history size 200

Enter the command to display command history.

R1>show history

show running-config | section line con

show ip interface brief | include down

show ip interface brief | exclude up

show running-config | begin line

terminal history size 200

show history

R1>

VLAN -VLAN este o rețea locală virtuală care permite gruparea dispozitivelor într-o rețea logică separată, indiferent de locația fizică a acestora.

WLAN -WLAN este o rețea locală wireless care permite dispozitivelor să se conecteze la rețea fără fir, folosind tehnologia Wi-Fi

Switch - Un switch este un dispozitiv de rețea care conectează mai multe dispozitive (computere, imprimante, servere etc.) într-o rețea locală (LAN). Acesta permite comunicarea între dispozitive prin transferul pachetelor de date într-un mod eficient și rapid.

Router - Un router este un dispozitiv de rețea care conectează două sau mai multe rețele între ele și dirijează pachetele de date între aceste rețele.

Adresa MAC - MAC (Media Access Control) este un identificator unic atribuit fiecărui dispozitiv de rețea care utilizează Ethernet sau Wi-Fi pentru a comunica. Aceasta este utilizată pentru a identifica dispozitivele la nivel de legătură de date (Layer 2) în modelul OSI.

Gateway - Un gateway (sau poartă) este un dispozitiv de rețea care servește ca punct de acces între două rețele diferite, adesea cu protocoale diferite.