Switching

Capitolul 2

ccna.ro
You Need To Know

Întrebarea zilei

Este importantă securitatea la nivelul legătură de date? De ce?

ccna.ro
You Need To Know

Concepte de bază

ccna.ro
You Need To Know

Etapele inițializării unui switch

POST

Boot loader

Inițializare CPU

Flash

IOS

- Power-On-Self-Test
- Program stocat în ROM
- Maparea memoriei fizice
- Sistemul de fișiere
- Sistemul de operare

ccna.ro
You Need To Know

Etapele inițializării unui switch

- POST
- **Boot loader**
- Inițializare CPU
- Flash
- IOS

- Power-On-Self-Test
- Program stocat în ROM
- Maparea memoriei fizice
- Sistemul de fișiere
- Sistemul de operare

ccna.ro
You Need To Know

Etapele inițializării unui switch

- POST
- Boot loader
- **Inițializare CPU**
- Flash
- IOS

- Power-On-Self-Test
- Program stocat în ROM
- Maparea memoriei fizice
- Sistemul de fișiere
- Sistemul de operare

ccna.ro
You Need To Know

Etapele inițializării unui switch

- POST
- Boot loader
- Inițializare CPU
- **Flash**
- IOS

- Power-On-Self-Test
- Program stocat în ROM
- Maparea memoriei fizice
- Sistemul de fișiere
- Sistemul de operare

ccna.ro
You Need To Know

Etapele inițializării unui switch

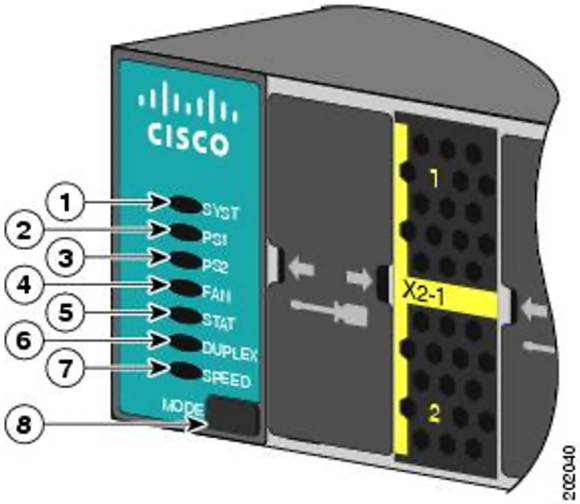
POST	• Power-On-Self-Test
Boot loader	• Program stocat în ROM
Inițializare CPU	• Maparea memoriei fizice
Flash	• Sistemul de fișiere
IOS	• Sistemul de operare

Switch boot loader

- Verifica daca SO este valid
- Ofera comenzi pentru:
  - Reincarcarea SO-ul
  - A folosi alta locatie pentru SO

LED-uri

- LED-uri de sistem
- LED-uri RPS
- Port Status LED
- Port Duplex LED
- (PoE) Mode LED
- Port Speed LED



ccna.ro
You Need To Know

LED-ul unui port

- LED-ul nu este aprins: opereaza cu 10 Mb/s
- LED-ul este verde: opereaza cu 100 Mb/s
- LED-ul este verde intermitent: opereaza cu 1000 Mb/s

Layer 3 switch vs. ruter

	Layer 3 switch	Ruter
Suport pentru WIC	✗	✓
Rutare nivel 3	✓	✓
Protocoale avansate de rutare	✗	✓
Rutare la viteza interfeței	✓	✓

SVI pentru management

1. Creare VLAN + nume

```
Sw(config)#vlan 99
Sw(config-vlan)#name Management
Sw(config-vlan)#exit
```

2. Asignare IP și mască

```
Sw(config)#interface vlan 99
Sw(config-if)#ip address 172.17.99.2 255.255.255.0
Sw(config-if)#no shutdown
```

3. Default gateway

```
Sw(config)#ip default-gateway 172.17.99.1 255.255.255.0
```

Management

ccna.ro
You Need To Know

CDP – Cisco Discovery Protocol

- Protocol proprietar Cisco folosit pentru descoperirea echipamentelor vecine
- Este pornit by default
- Deoarece oferă informații despre echipamentele din rețea, poate fi considerat un risc de securitate
- VLAN 1 este locatia default pentru a contine adresa IP pentru management

```
București(config)#(no) cdp run
```

NTP - Network Time Protocol

- Sincronizarea ceasurilor cu un server NTP
- Distanța față de cel mai apropiat server NTP orficial se numește stratum


```
Constanța(config)#ntp server 10.1.1.1
```

```
București(config)#ntp master 1
```

Recuperarea parolei

1. Se repornește echipamentul
2. În timpul secvenței de boot, se intră în modul Rommon apasând CRTL + Break
3. Se schimbă registrul de configurare cu 0x2142 (ignoră running config) și se repornește echipamentul
4. Se fac configurările necesare, se salvează și se reface registrul

Recuperarea parolei

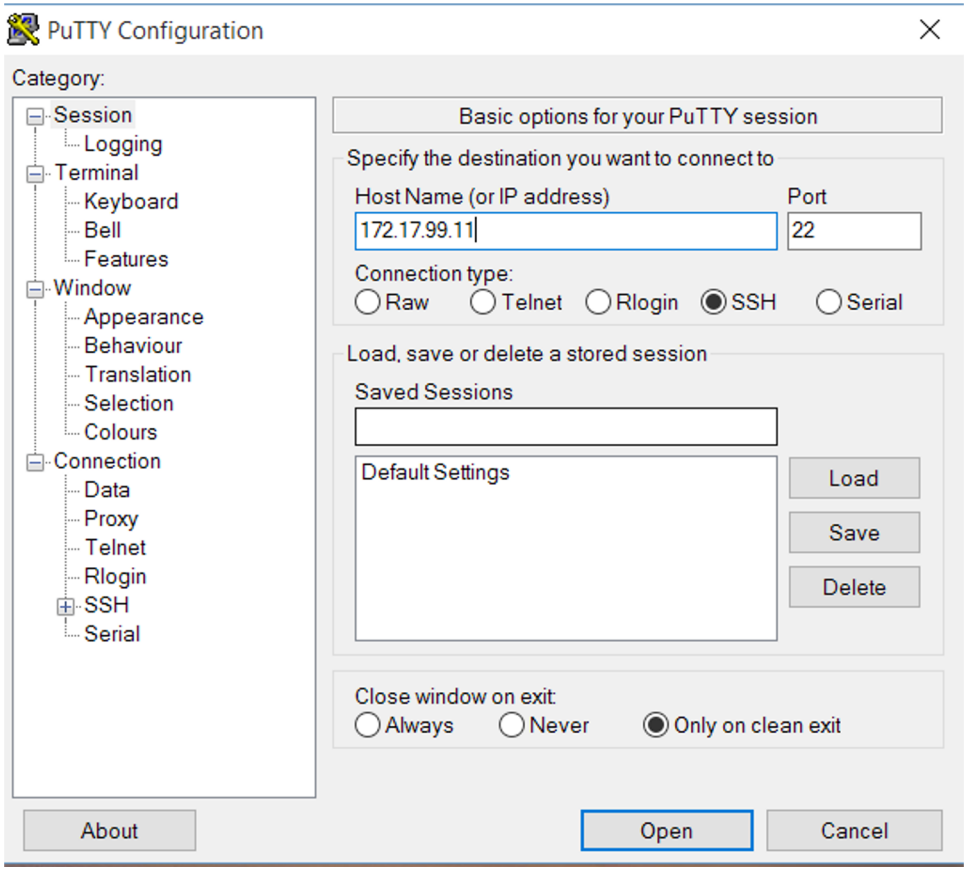
```
rommon 1 > confreg 0x2142
rommon 2 > reset
[...]
București>enable
București#copy startup running
București#conf t
București(config)#enable secret cisco
București(config)#config-register 0x2102
București(config)#end
București#write
```

Securitate

ccna.ro
You Need To Know

Acces sigur la distanță - SSH

- SSH = Secure Shell
- Conexiune la distanță criptată
- Portul 22 TCP



Configurare SSH

- Configurarea serviciului

```
Sw(config)# ip domain-name somedomain.com
Sw(config)# crypto key generate rsa
Sw(config)# username admin password ccna
```

- Aplicarea pe interfață

```
Sw(config)# line vty 0 4
Sw(config-line)# transport input ssh
```

Securitatea pe porturi

- Limitează numărul de MAC-uri pe un port
- Încercări peste limita admisă => threat alert
- Tipuri de adrese MAC securizate:
  - Static secure – sunt configurate manual
  - Dynamic secure – dispar la restart
  - Sticky secure – nu trebuie reînvățate la repornirea echipamentului

Configurări

- Dynamic Port Security

```
Sw(config)#interface fa0/1
Sw(config-if)#switchport mode access
Sw(config-if)#switchport port-security
```

- Sticky Port Security

```
Sw(config)#interface fa0/1
Sw(config-if)#switchport mode access
Sw(config-if)#switchport port-security
Sw(config-if)#switchport port-security maximum 50
Sw(config-if)#switchport port-security mac-address sticky
```

Dezactivarea porturilor inactive

- O metodă simplă de securitate care împiedică accesul neautorizat

```
Sw(config)#interface range fa 0/1 - 10
Sw(config-if)#shutdown
```

Moduri de încălcare a securității

Mod	Forwardează trafic	Trimite mesaj de log	Afișează mesaj de eroare	Crește counter încălcări	Închide port
Protect	✗	✗	✗	✗	✗
Restrict	✗	✓	✗	✓	✗
Shutdown	✗	✗	✗	✓	✓

```
Sw(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

Debugging

1. `Sw# show ip ssh`
2. `Sw# show port-secutiry [interface interface-id]`
3. `Sw# show port-security address`

Rocket Science

ccna.ro
You Need To Know

Practici în securitate

- Firewall
  - Filtrează, criptează și intermediază traficul
- Controlul accesului fizic
- Patch-uri și update-uri
- Policy de securitate
- Parole
- Antivirus

Practici în securitate

- Firewall
- Controlul accesului fizic
  - Securitate la nivel fizic
- Patch-uri și update-uri
- Policy de securitate
- Parole
- Antivirus

ccna.ro
You Need To Know

Practici în securitate

- Firewall
- Controlul accesului fizic
- Patch-uri și update-uri
  - Instalare de patch-uri de securitate
- Policy de securitate
- Parole
- Antivirus

ccna.ro
You Need To Know

Practici în securitate

- Firewall
- Controlul accesului fizic
- Patch-uri și update-uri
- Policy de securitate
  - Dezvoltarea unei politici pentru a valida identitatea angajaților
- Parole
- Antivirus

Practici în securitate

- Firewall
- Controlul accesului fizic
- Patch-uri și update-uri
- Policy de securitate
- Parole
  - Parole puternice, schimbate des
- Antivirus

ccna.ro
You Need To Know

Practici în securitate

- Firewall
- Controlul accesului fizic
- Patch-uri și update-uri
- Policy de securitate
- Parole
- Antivirus
  - Software pentru securitate

Răspunsul zilei

Răspunsul zilei

Este importantă securitatea la nivelul legătură de date? De ce?

ccna.ro
You Need To Know