**1.Ce este un switch?**

Un **switch** este un dispozitiv de rețea de tip Layer 2 (nivelul legăturii de date în modelul OSI) care conectează mai multe dispozitive într-o rețea locală (LAN) și le permite să comunice eficient între ele.

**2.Ce este un router?**

Un **router** este un dispozitiv de rețea de tip Layer 3 (nivelul de rețea din modelul OSI) care conectează **rețele diferite între ele** și **dirijează pachetele de date** între aceste rețele pe baza adreselor IP.

**3.Ce este WLC-3504?**

Un **WLC-3504** (Wireless LAN Controller 3504) este un dispozitiv Cisco specializat care administrează o rețea wireless formată din mai multe **Access Point-uri (AP-uri)**.

WLC-ul preia controlul asupra configurației și managementului AP-urilor, oferind o rețea wireless unificată și ușor de administrat

**4. Ce este HomeRouter-PT-AC?**

Un **HomeRouter-PT-AC** este un dispozitiv disponibil în **Cisco Packet Tracer**, care simulează un **router wireless de uz casnic**, similar cu cele furnizate de furnizorii de internet (ISP) pentru acasă sau birouri mici.

**5.Ce este un Multilayer Switch?**

Un **Multilayer Switch (MLS)** este un switch care combină funcțiile unui **switch de Layer 2** (comutare pe baza adreselor MAC) cu cele ale unui **router de Layer 3** (rutare pe baza adreselor IP). Cu alte cuvinte, este un **switch care poate face și rutare între VLAN-uri**, nu doar comutare.

Ce poate face un MLS?:  
1. Activare rutare Layer 3:

Switch(config)# ip routing

2. Creare interfețe virtuale pentru VLAN-uri:

Switch(config)# interface vlan 10

Switch(config-if)# ip address 192.168.10.1 255.255.255.0

Switch(config-if)# no shutdown

3. Configurare porturi în VLAN:

Switch(config)# interface range fa0/1 - 5

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 10

4. Rutare statică dacă e conectat și la alte rețele:

Switch(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

**6. Ce face un Server DNS?**

Un **server DNS (Domain Name System)** are rolul de a **traduce numele de domeniu** (ex: www.google.com) în adrese IP (ex: 142.250.180.68), pe care calculatoarele le pot înțelege și folosi pentru a comunica în rețea.

**7. Ce face un Server Radius?**

Un **server RADIUS** (Remote Authentication Dial-In User Service) este un server de **autentificare centralizată** folosit în rețele pentru a verifica identitatea utilizatorilor care vor să se conecteze, de obicei la:

* Rețele wireless (Wi-Fi cu autentificare 802.1X)
* VPN-uri
* Switchuri sau routere (acces la consola de administrare)

**Cum funcționează într-o rețea:**

1. Un utilizator (sau dispozitiv) încearcă să se conecteze la rețea (ex: printr-un Access Point configurat cu WPA2-Enterprise).
2. Access Point-ul trimite cererea de autentificare către serverul RADIUS.
3. Serverul RADIUS verifică datele și răspunde cu:
   * **Access-Accept** (dacă sunt corecte)
   * **Access-Reject** (dacă sunt greșite)
4. Dacă e acceptat, utilizatorul primește acces la rețea.

**8. Ce face un Server DHCP?**

Un **server DHCP** (Dynamic Host Configuration Protocol) este un dispozitiv sau serviciu de rețea care **atribue automat adrese IP** și alte setări de rețea (cum ar fi gateway-ul, DNS-ul etc.) dispozitivelor care se conectează la rețea.

**9. Ce face un Server Web?**

Un **server web** este un dispozitiv sau aplicație care **stochează și livrează pagini web** către clienți (de exemplu, browsere web) prin intermediul protocolului **HTTP** sau **HTTPS**.

**10.Ce face un 3702i?**

Un **Cisco Aironet 3702i** este un **Access Point (AP) de tip enterprise**, folosit pentru a furniza **conectivitate wireless** într-o rețea. În **Cisco Packet Tracer**, îl găsești ca dispozitiv **3702i**, fiind unul dintre AP-urile moderne care **lucrează împreună cu un WLC (Wireless LAN Controller)**.

**11. Ce face un Server Syslog?**  
Un **server Syslog** (System Logging Server) este un dispozitiv care colectează și stochează **mesaje de log (jurnal)** trimise de echipamentele din rețea — cum ar fi routere, switchuri, WLC-uri sau firewall-uri.

**12. Ce este DHCP și la ce se folosește?**  
DHCP (Dynamic Host Configuration Protocol) este un protocol de rețea folosit pentru **alocarea automată de adrese IP** și alte setări de rețea (cum ar fi subnet mask, gateway și DNS) către dispozitivele care se conectează la rețea.

Se folosește pentru a evita configurarea manuală a fiecărui dispozitiv și pentru a **asigura o administrare eficientă și fără conflicte de IP**.

13. **Ce este un trunk și la ce se folosește într-o rețea?**  
Un **trunk** este o conexiune între două echipamente de rețea (de obicei switch-uri, routere sau WLC/AP) care **poate transporta trafic din mai multe VLAN-uri simultan**.

Este esențial în rețele cu VLAN-uri multiple, pentru ca datele din diferite VLAN-uri să poată circula pe același cablu între echipamente.

14. Ce este un VLAN :

Un VLAN (Virtual Local Area Network) este o retea logica care separa dispozitivele dintr-o retea fizica in mai multe domenii de broadcast, chiar daca acestea sunt conectate la acelasi switch.

15.Ce sunt interfetele virtuale pentru VLAN URI?

O inetrfata virtuala pentru vlan ( denumita si SVI – switched Virtual Interface) este o interfata logica create pe un multilayer switch care permite rutarea intre VLAN uri.

Fiecare SVI este asciat cu un VLAN si are o adresa IP care actioneaza ca gateway oentru toate dispozitivele din acel VLAN.

O **Access List (ACL)** pe echipamentele Cisco este un set de reguli care controlează **ce trafic este permis sau blocat** pe interfețele unui router sau switch Layer 3. Practic, este un **filtru de pachete**.

**🔐 Ce face o ACL:**

* Permite sau blochează traficul pe baza unor criterii: **IP sursă/destinație**, **porturi**, **protocole**.
* Poate fi aplicată pe o interfață:
  + **inbound** (traficul care intră)
  + **outbound** (traficul care iese)

access-list 10 permit 192.168.1.10

interface g0/0

ip access-group 10 in

STP(spanning tree protocol)

este un protocol de rețea utilizat pentru prevenirea buclelor de rețea în topologiile de rețea care folosesc comutatori (switch-uri) și interconexiuni redundante

**⚙️ Ce face STP?**

* Detectează topologia rețelei
* **Dezactivează automat legăturile redundante** (le pune în standby)
* Menține o **topologie fără bucle** (un „arbore” logic)
* Dacă o legătură activă cade, **activează automat** una de rezervă

**🧱 Structură STP:**

1. **Bridge ID** – format din:
   * Prioritate STP (default 32768)
   * MAC-ul switch-ului
2. **Root Bridge** – switch-ul ales cu cel mai mic Bridge ID  
   ➜ devine „centrul” rețelei
3. **Porturi STP**:
   * **Root Port** – portul cu cea mai bună cale spre Root Bridge
   * **Designated Port** – portul activ pe fiecare segment
   * **Blocked Port** – port dezactivat pentru a preveni buclele

PRIORITATE STP

**🧠 Cum funcționează:**

Fiecare switch are un **Bridge ID** format din:

* **Prioritate STP** (default: **32768**)
* **MAC Address** al switch-ului

STP alege ca **Root Bridge**:

1. Switch-ul cu **cea mai mică prioritate**
2. Dacă prioritățile sunt egale ➜ **cea mai mică adresă MAC**

**RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)**

**RSTP** este o versiune **îmbunătățită și mai rapidă** a protocolului STP clasic (802.1D), folosit pentru **prevenirea buclelor de rețea** în topologii Ethernet cu legături redundante.

**EtherChannel** este o tehnologie Cisco care permite **gruparea mai multor conexiuni fizice** (de obicei între switch-uri sau între un switch și un server/router) într-un **singur canal logic** pentru a:

**✅ Beneficii:**

* **Crește lățimea de bandă**: de exemplu, 2 legături de 1 Gbps = 2 Gbps total.
* **Redundanță**: dacă un cablu pică, traficul continuă pe celelalte.
* **Previne bucle STP**: STP vede EtherChannel-ul ca o singură legătură.

**Ce se întâmplă când prioritatea e egală:**

* HSRP compară **prioritatea** (default este 100).
* Dacă prioritățile sunt egale, **routerul cu IP-ul mai mare** va deveni **Active**.
* Celălalt router va deveni **Standby**.

Dacă vrei control clar asupra routerului activ, setează o **prioritate diferită** cu comanda:

standby 1 priority 120

**8. Ce face un Server DHCP?**

Un **server DHCP** (Dynamic Host Configuration Protocol) este un dispozitiv sau serviciu de rețea care **atribuie automat adrese IP** și alte setări de rețea (cum ar fi gateway-ul, DNS-ul etc.) dispozitivelor care se conectează la rețea network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

Prioritatea pe router

**1. Prioritatea în HSRP (Hot Standby Router Protocol)**

Determină **care router devine activ** într-un grup HSRP.

**📌 Default: 100**

Routerul cu **prioritate mai mare devine Active**.

**🔧 Comandă:**

interface GigabitEthernet0/0

standby 1 ip 192.168.1.1

standby 1 priority 120

standby 1 preempt

* priority 120 – setează prioritatea
* preempt – permite routerului să preia rolul activ dacă are prioritate mai mare

Prioritatea pe swich

**Cum funcționează prioritatea în STP:**

* Fiecare switch are un **Bridge ID**, format din:
  + **Prioritate STP** (default: 32768)
  + **MAC Address** al switchului
* STP alege ca **Root Bridge** switchul cu **cel mai mic Bridge ID**.
  + Adică: **cea mai mică prioritate**, iar dacă e egală, **cea mai mică adresă MAC**.

# Exemplu: setează prioritatea la 24576 (mai mică decât defaultul 32768)

Comenzi: spanning-tree vlan 1 priority 24576

Port Security pe switch-uri

**🔐 Ce face Port Security:**

* Permite un număr maxim de adrese MAC pe un port.
* Poate bloca portul dacă o adresă necunoscută încearcă să se conecteze.
* Poate **salva** adresele MAC învățate automat.

# 1. Activezi modul de acces pe port

interface FastEthernet0/1

switchport mode access

# 2. Activezi port security

switchport port-security

# 3. Limitezi numărul de adrese MAC permise (ex: 1)

switchport port-security maximum 1

# 4. Setezi acțiunea dacă apare o adresă neautorizată

switchport port-security violation shutdown # sau restrict, protect

# 5. Alegi metoda de înregistrare a MAC-ului

switchport port-security mac-address sticky # MAC-urile se învață automat și se salvează

# 6. (opțional) Specifici o MAC fixă

# switchport port-security mac-address 00AA.BBCC.DDEE

Port switching

**1. Comutarea porturilor pe un switch (Switching Ports)**

Se referă la **funcționarea normală a unui switch**, care "comută" (switch) pachetele între porturi:

* Switch-ul învață **adresele MAC** de pe fiecare port.
* Când primește un cadru, îl transmite **doar pe portul unde se află MAC-ul destinație** (nu către toate porturile).
* Acest comportament eficient se numește **switching**.

**Ce este un trunk și la ce se folosește într-o rețea?**  
Un **trunk** este o conexiune între două echipamente de rețea (de obicei switch-uri, routere sau WLC/AP) care **poate transporta trafic din mai multe VLAN-uri simultan**.

Este esențial în rețele cu VLAN-uri multiple, pentru ca datele din diferite VLAN-uri să poată circula pe același cablu între echipamente.

Cum se face vlan pe multilayer switch

Pe un **multilayer switch (MLS)**, poți crea **VLAN-uri** și poți configura **Inter-VLAN Routing**, adică routing între ele **direct pe switch**, fără a folosi un router extern.

CREEM VLAN URILE, LE DAM NUME DACA TREBUIE dupa care:

interface fa0/1

switchport mode access

switchport access vlan 10

exit

interface fa0/2

switchport mode access

switchport access vlan 20

exit

SI DAM IP ROUTING

Vlan

Un VLAN (Virtual Local Area Network) este o retea logica care separa dispozitivele dintr-o retea fizica in mai multe domenii de broadcast, chiar daca acestea sunt conectate la acelasi switch.

**Când folosești RIP:**

* **Ai mai multe routere** (sau multilayer switchuri) și vrei ca ele să își partajeze tabelele de rutare.
* De exemplu, ai:
  + VLAN 10 → pe Switch1
  + VLAN 20 → pe Switch2
  + Conectate prin routere sau MLS-uri diferite

În acest caz, **RIP poate fi folosit** să învețe rutele între echipamente.

??Ce modalitati de comunicare inter-Vlan exista?

**Modalități de comunicare inter-VLAN:**

**✅ 1. Router-on-a-Stick (cu un router Layer 3 și trunk)**

* Se folosește un **router obișnuit** conectat la un switch printr-un port **trunk**.
* Routerul are **subinterfețe** (câte una pentru fiecare VLAN), fiecare cu o adresă IP.

DNS Server

Un server DNS (Domain Name System) este un server specializat care traduce nume de domenii în adrese IP și invers. DNS-ul este esențial pentru funcționarea internetului, deoarece permite utilizatorilor să acceseze site-uri web, servicii și alte resurse online folosind nume ușor de reținut în loc de adrese IP numerice.

Switch vs MultiLayerSwitch

layer2 - layer3

conecta dispozitive într-o rețea locală (LAN) - rutare între diferite VLAN-uri (rutare inter-VLAN)

comutarea și direcționarea traficului la nivelul interfeței de rețea - flexibilitate și capacitate de a gestiona rețele mai complexe

Securitate pe switchport

PortFast și BPDU Guard sunt caracteristici oferite de switch-urile de rețea, în special de switch-urile care utilizează protocolul (STP) sau protocolul similar Rapid Spanning Tree Protocol. Aceste caracteristici sunt utilizate pentru a optimiza performanța și securitatea rețelelor, în special în ceea ce privește convergența rețelei și prevenirea buclelor de comutare.

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security violation shutdown

VLAN pe Router

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip add 192.168.1.1 255.255.255.0

Cum functioneaza proiectul?

**1. Branch Office**

* Dispozitive: 2 PC-uri, 1 Switch 2960, 1 Router ISR4331, 1 WLC-3504, 1 AP 3702i, 3 Laptopuri
* VLAN-uri: 10 (PC), 11 (WiFi), 13 (Guest), 99 (WiFi Mgmt), 100 (MGMT), 101 (BlackHole)
* Trunkuri între Router, WLC, AP; Native VLAN 99
* DHCP Relay către DC; Routing inter-VLAN prin subinterfețe pe BR-R1
* Wireless configurat pe WLC cu 3 SSID-uri (PSK, 802.1x, Guest)
* Port-security activ pe porturi PC

**2. Home Office**

* Dispozitive: HomeRouter-PT-AC, 1 PC, 2 Laptopuri, 1 Smartphone
* Rețea locală: 10.101.1.0/24
* DHCP + NAT în router; toate dispozitivele primesc IP din DHCP
* Wireless funcțional prin HomeRouter, nu implică VLAN-uri

**3. Central Office**

* Dispozitive: 2 Routere ISR, 1 Multilayer Switch, 2 Switchuri 2960, 1 WLC, 2 AP-uri, 3 Laptopuri, 2 PC-uri, 1 Server Syslog
* VLAN-uri: 8 (Syslog), 10 (PC), 11 (WiFi), 13 (Guest), 99 (Mgmt WiFi), 100 (MGMT)
* Inter-VLAN routing cu subinterfețe pe routere
* DHCP local pe routere + HSRP activ pe toate VLAN-urile
* Etherchannel: LACP în ASW1, PAGP în ASW2
* Wireless configurat pe WLC cu autentificare RADIUS (din DC)
* Port-security + VLAN 101 pentru securitate

**4. Data Center**

* Dispozitive: 2 Routere ISR, 2 Switchuri Layer 3, 2 Switchuri de acces, 4 Servere (DNS, DHCP, RADIUS, WEB)
* VLAN-uri: 8 (DNS), 9 (RADIUS), 10 (DHCP), 11 (WEB), 99 (Native), 100 (MGMT)
* SVI pe switchuri + HSRP pentru toate VLAN-urile
* DHCP server configurat pentru Branch
* Port-security cu 1 MAC fix pe servere
* Etherchannel (LACP) între DC-CSW1 și DC-CSW2
* Routing static pe routere și switchuri

**5. Servicii Centrale**

* DNS: Rezolvă savnet.ro / www.savnet.ro în IP web server (10.1.11.50)
* DHCP: Distribuie IP în Branch (prin DHCP Relay)
* RADIUS: Autentificare 802.1X pentru wireless (WLC-uri)
* WEB: Pagina: "Welcome to Savnet"
* SYSLOG: Centralizează loguri din rețea

**Intrebari**

***Pentru Reteaua Branch Office***

**🔸 *Cine oferă IP-urile și cum ajung pachetele DHCP la server?***

IP-urile sunt oferite de un server DHCP din Data Center. Routerul ISR4331 are configurat ***ip helper-address*** pe fiecare interfață de VLAN, redirecționând cererile către serverul central.

**🔸 Cine face rutarea între VLAN-uri în Branch?**  
→ Routerul BR-R1, prin subinterfețe configurate pe portul Gi0/0/1.

**🔸 Cum se conectează laptopurile la rețea în Branch Office?**  
→ Prin Access Point BR-AP1 care emite SSID-uri gestionate de WLC. Conexiunea este wireless, iar traficul ajunge în VLAN11 sau VLAN13.

***Pentru Reteaua Home Office***

**🔸 *Cine oferă adresele IP în Home Office?***

Routerul HomeRouter-PT-AC acționează ca server DHCP și oferă adrese IP pentru toate dispozitivele locale (prin cablu sau Wi-Fi).

**🔸 *Cum comunică dispozitivele între ele?***

Toate sunt în aceeași rețea locală 10.101.1.0/24, iar HomeRouter gestionează tot traficul intern și extern.

**🔸 *Este rețeaua wireless separată de cea cablată?***

Nu, în cazul HomeRouter-PT-AC, wireless și cablul fac parte din aceeași rețea. Toate dispozitivele primesc IP-uri din același interval și pot comunica direct.

***Pentru Reteaua Central Office***

**🔸 *Cum se face rutarea între VLAN-uri în Central Office?***

Prin multilayer switch-ul central, care are interfețe virtuale (SVI) pentru fiecare VLAN și comanda ip routing activată.

**🔸 *Cum sunt conectate AP-urile și ce VLAN-uri traversează?***

AP-urile sunt conectate în trunk pe switch-uri de acces și permit VLAN-uri: OFFICE\_WIFI (11), WIFI\_MGMT (12), GUEST (13). Astfel, pot transmite mai multe SSID-uri gestionate de WLC.

**🔸 *Care este rolul serverului Syslog?***

Adună loguri de sistem (mesaje de eroare, conectări, configurări) de la echipamentele rețelei pentru monitorizare și depanare.

**🔸 Cum este configurată redundanța între routerele din Central Office?**  
→ Cu HSRP: CO-R1 și CO-R2 partajează IP-uri virtuale pentru fiecare VLAN și se preiau automat în caz de eroare.

**🔸 Ce este HSRP și cum l-ai aplicat în Central Office?**  
→ Hot Standby Router Protocol. Am folosit HSRP pentru VLAN-urile 8, 10, 11, 13, 99 și 100, cu R1 activ pentru unele și R2 activ pentru altele.

**Pe scurt:**

HSRP permite configurarea a **două sau mai multe routere** pentru a acționa ca **un singur gateway virtual** pentru stațiile dintr-o rețea. Scopul său este să asigure **continuitatea serviciului de rutare** în caz că routerul principal (activ) cade.

**Cum funcționează:**

* Se creează o **adresă IP virtuală** (ex: 192.168.1.1), care este gateway-ul pentru PC-uri.
* Un router este ales drept **Active Router** – răspunde pachetelor trimise la IP-ul virtual.
* Altul devine **Standby Router** – stă în așteptare, monitorizează activul.
* Dacă routerul activ cade, cel standby preia automat rolul și continuă să proceseze traficul.

**🔸 Ce este EtherChannel și unde l-ai folosit în Central Office?**  
→ Este o tehnologie de agregare a linkurilor. Am folosit LACP cu ASW1 și PAGP cu ASW2, configurate pe trunk-uri.

**🔸 Cum sunt autentificați utilizatorii wireless în Central Office?**  
→ Prin SSID-ul Office\_802.1x, care folosește serverul RADIUS din Data Center

***Pentru Reteaua Data Center***

**🔸 Cine oferă IP-urile în rețea și cum ajung cererile DHCP acolo?**  
→ DC-DHCP1 oferă IP-urile. Cererile DHCP ajung acolo prin comanda ip helper-address configurată pe routerele din locații.

**🔸 *Cum funcționează autentificarea wireless centralizată?***

WLC-urile trimit cererile de autentificare către serverul RADIUS (DC-RADIUS1) folosind protocolul RADIUS. Acesta validează utilizatorii și decide dacă primesc acces.

**🔸 *Care este rolul serverului DNS?***

Traduce nume de domenii în adrese IP. De exemplu, când un laptop face ping la www.site.local, DNS-ul returnează IP-ul serverului web.

**🔸 Cum se face autentificarea 802.1X și unde este configurat serverul RADIUS?**  
→ Clienții WiFi trimit cererea de autentificare către WLC, care o redirecționează către DC-RADIUS1. Acesta verifică username și parolă.

Pentru **WIRELESS**

**🔸 Care este diferența între SSID-ul Office\_PSK și Office\_802.1x?**  
→ Office\_PSK folosește o parolă predefinită, iar Office\_802.1x folosește autentificare individuală pe bază de cont prin RADIUS

SECURITATE ȘI MANAGEMENT

**🔸 Ce măsuri de securitate ai implementat pe switchuri?**  
→ Port-security cu limită de MAC-uri, VLAN 101 pentru porturi nefolosite, STP Rapid, BPDUGuard și PortFast pe porturi de access.