

VLAN-uri, trunk-uri și rutare inter-VLAN

Un singur switch fizic devine trei rețele care nu se aud între ele, apoi două switch-uri își trimit tot traficul printr-un singur cablu, iar la final un ruter le leagă înapoi - controlat, prin subinterfețe. Lucrarea aceasta este momentul în care o rețea încetează să fie o grămadă de cabluri și devine un proiect.

OBIECTIVELE CAPITOLULUI

- Construiți topologia și configurați cele cinci VLAN-uri pe toate switch-urile
- Demonstrați izolarea între VLAN-uri înainte de configurarea ruterului
- Configurați trunk-urile cu VLAN nativ 99 și listă explicită de VLAN-uri permise
- Capturați și documentați o etichetă 802.1Q din modul Simulation
- Configurați router-on-a-stick și demonstrați conectivitate completă între toate cele trei VLAN-uri
- Realizați aceeași funcție cu un switch 3560 și SVI-uri; comparați traseul pachetului în ambele variante
- Adăugați bucla, observați STP și forțați rădăcina pe SW-CORE
- Provocați cele patru defecte din secțiunea 10 și notați, pentru fiecare, comanda de diagnostic

3.1 Problema pe care o rezolvă VLAN-urile

O firmă are trei departamente răspândite pe două etaje. Fiecare etaj are câte un switch. Contabilitatea nu are voie să vadă traficul producției, iar vizitatorii nu au voie să vadă nimic.

Fără VLAN-uri, aveți exact două soluții și amândouă sunt proaste: fie cumpărați câte un switch separat pentru fiecare departament, la fiecare etaj - șase switch-uri în loc de două -, fie trageți cabluri dintr-un capăt în altul al clădirii. **VLAN-ul este al treilea răspuns:** același switch fizic se comportă ca mai multe switch-uri independente, iar apartenența se decide din configurație, nu din cablare.

DEFINIȚIA 3.1 (VLAN). O rețea locală virtuală. Fiecare port al switch-ului este atribuit unui VLAN, iar switch-ul refuză să comute cadre între VLAN-uri diferite. Două calculatoare în porturi vecine, dar în VLAN-uri diferite, sunt la fel de izolate ca și cum ar fi în clădiri diferite.

DEFINIȚIA 3.2 (PORT DE ACCES). Un port care aparține unui singur VLAN și pe care circulă cadre *netichetate* - obișnuite. Aici se leagă calculatoarele, care nu știu și nu trebuie să știe nimic despre VLAN-uri.

DEFINIȚIA 3.3 (PORT TRUNK). Un port care transportă cadre din mai multe VLAN-uri deodată, pe același cablu. Ca să nu se amestece, fiecare cadru primește o *etichetă* de 4 octeți cu numărul VLAN-ului - standardul 802.1Q. Aici se leagă switch-urile între ele și switch-ul de ruter.

DEFINIȚIA 3.4 (VLAN NATIV). Singurul VLAN care circulă *netichetat* pe un trunk. Există din motive istorice, este o sursă clasică de atacuri, și de aceea se alege deliberat un VLAN gol, în care nu se află nicio stație.

Ce facem astăzi, în trei fraze. Împărțim un switch în trei VLAN-uri și dovedim că izolarea funcționează. Legăm switch-urile prin trunk-uri și dovedim că același VLAN se aude peste două switch-uri, dar VLAN-urile diferite tot nu. La final punem un ruter deasupra, ca departamentele să poată vorbi între ele - dar numai prin el, unde putem controla ce trece.

3.2 Echipamente necesare

Tabelul 3.1 Echipamente necesare.

Buc.	Echipament	Model	Categoria din Packet Tracer	La ce folosește aici
3	Switch	2960	Network Devices → Switches	SW-A (etajul 1), SW-B (etajul 2), SW-CORE
1	Ruter	4331	Network Devices → Routers	rutarea între VLAN-uri
6	Calculator	PC-PT	End Devices → End Devices	PC1 ... PC6, câte două de fiecare departament
6	Cablu drept	Copper Straight-Through	Connections	stații → switch-uri, switch → ruter
2	Cablu inversor	Copper Cross-Over	Connections	SW-A ↔ SW-CORE, SW-B ↔ SW-CORE

Pentru secțiunea opțională cu switch de nivel 3, mai aveți nevoie de un switch 3560 (tot din *Network Devices → Switches*), care îl înlocuiește pe SW-CORE. Pentru secțiunea de Spanning Tree, un al treilea cablu inversor, între SW-A și SW-B.

Regula cablurilor, pe scurt. Switch ↔ switch înseamnă *cross-over*. Switch ↔ ruter și stație ↔ switch înseamnă *straight-through*. În bancul de lucru din pagină cablurile sunt deja puse corect; în Packet Tracer le alegeți voi.

3.3 Topologia și planul

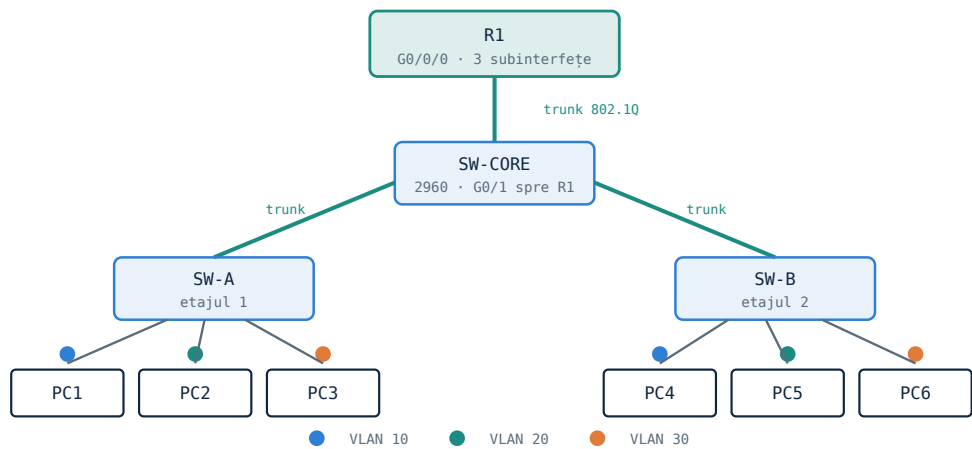


Figura 3.1 Trei departamente răspândite pe două etaje. Fiecare etaj are un switch, dar departamentele nu coincid cu etajele - exact situația pentru care au fost inventate VLAN-urile.

Tabelul 3.2 Topologia și planul.

VLAN	Nume	Rețea	Gateway	Stații
10	ADMIN	192.168.10.0/24	192.168.10.1	PC1 (.11), PC4 (.14)
20	PRODUCTIE	192.168.20.0/24	192.168.20.1	PC2 (.12), PC5 (.15)
30	OASPETI	192.168.30.0/24	192.168.30.1	PC3 (.13), PC6 (.16)
99	NATIV	-	-	niciuna - VLAN nativ, deliberat gol
999	NEFOLOSIT	-	-	porturile inactivate

Tabelul 3.3 Topologia și planul.

Switch	Porturi de acces	Porturi trunk
SW-A	Fa0/1 → VLAN 10, Fa0/2 → VLAN 20, Fa0/3 → VLAN 30	G0/1 spre SW-CORE
SW-B	Fa0/1 → VLAN 10, Fa0/2 → VLAN 20, Fa0/3 → VLAN 30	G0/1 spre SW-CORE
SW-CORE	niciunul	G0/1 spre R1, G0/2 spre SW-A, G0/3 spre SW-B

Observați o simetrie utilă. SW-A și SW-B au exact aceeași configurație. Le veți scrie identic, ceea ce înseamnă că o puteți copia - și, în practică, exact așa se lucrează: se scrie o dată, se verifică, apoi se aplică pe restul.

3.4 Bancul de lucru

Topologia din figura 1, cablată, cu adresele stațiilor deja puse. Restul îl configurați voi, urmând pașii din secțiunile 5–7. Obiectivele din dreapta se bifează singure.

3.5 Pasul 1: crearea VLAN-urilor

1. Verificați punctul de plecare

Înainte de orice configurare, dați de pe PC1 un ping către PC4:
pe PC1

```
ping 192.168.10.14
```

Funcționează. Toate cele șase stații sunt, deocamdată, într-o singură rețea de nivel 2 - VLAN-ul 1, cel implicit. Rețineți rezultatul: peste cinci minute nu va mai merge, și acesta este scopul.

2. Creați VLAN-urile - pe toate cele trei switch-uri

identic pe SW-A, SW-B și SW-CORE

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name ADMIN
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name PRODUCTIE
Switch(config-vlan)# vlan 30
Switch(config-vlan)# name OASPETI
Switch(config-vlan)# vlan 99
Switch(config-vlan)# name NATIV
Switch(config-vlan)# vlan 999
```

```
Switch(config-vlan)# name NEFOLOSIT
Switch(config-vlan)# exit
```

Nu este nevoie să ieșiți din modul `config-vlan` între ele: comanda `vlan 20` funcționează direct din interiorul VLAN-ului 10.

Inclusiv SW-CORE, care nu are nicio stație Un switch nu poate comuta traficul unui VLAN pe care nu îl are configurat local, chiar dacă doar îl tranzitează. *Un VLAN lipsă pe un switch intermediar este cauza numărul unu a problemelor din această lucrare* - și una dintre cele mai frecvente în rețelele reale.

3. **Atribuiți porturile de acces**
pe SW-A - identic pe SW-B

```
SW-A(config)# interface fastEthernet 0/1
SW-A(config-if)# switchport mode access
SW-A(config-if)# switchport access vlan 10
SW-A(config-if)# switchport nonegotiate
SW-A(config-if)# spanning-tree portfast
SW-A(config-if)# exit
```

```
SW-A(config)# interface fastEthernet 0/2
SW-A(config-if)# switchport mode access
SW-A(config-if)# switchport access vlan 20
SW-A(config-if)# switchport nonegotiate
SW-A(config-if)# exit
```

```
SW-A(config)# interface fastEthernet 0/3
SW-A(config-if)# switchport mode access
SW-A(config-if)# switchport access vlan 30
SW-A(config-if)# switchport nonegotiate
SW-A(config-if)# end
```

Ce face fiecare linie:

Comanda	Efectul
<code>switchport mode access</code>	declară portul ca port de utilizator, nu de legătură între switch-uri
<code>switchport access vlan 10</code>	îl mută în VLAN-ul 10
<code>switchport nonegotiate</code>	oprește DTP, deci portul nu poate fi păcălit să devină trunk (atacul de <i>switch spoofing</i> din cursul 12)
<code>spanning-tree portfast</code>	portul intră imediat în funcțiune, fără cele 30 de secunde de așteptare STP

4. **Verificați izolarea - aici se vede rezultatul**
pe SW-A

```
SW-A# show vlan brief
```

Trebuie să vedeți exact asta:
ce trebuie să apară

VLAN	Name	Status	Ports
1	default	active	G0/1, G0/2
10	ADMIN	active	Fa0/1
20	PRODUCTIE	active	Fa0/2
30	OASPETI	active	Fa0/3

```
99 NATIV active
999 NEFOLOSIT active
```

Acum testați, de pe PC1:
pe PC1

```
ping 192.168.20.12
ping 192.168.10.14
```

Amândouă trebuie să eșueze. Primul, pentru că PC2 este în alt VLAN. Al doilea, pentru că PC4 este pe alt switch și trunk-ul nu există încă. Eșecul este dovada că ați configurat corect.

Întrebare

PC1 și PC2 sunt conectate la același switch fizic, la două porturi vecine. De ce nu se aud?

► Vezi răspunsul

3.6 Pasul 2: legăturile trunk

1. Configurați trunk-urile

Trei switch-uri, patru porturi de legătură. Toate primesc aceeași configurație:
pe SW-A, portul spre SW-CORE

```
SW-A(config)# interface gigabitEthernet 0/1
SW-A(config-if)# switchport mode trunk
SW-A(config-if)# switchport trunk native vlan 99
SW-A(config-if)# switchport trunk allowed vlan 10,20,30,99
SW-A(config-if)# switchport nonegotiate
SW-A(config-if)# end
```

Repetăți identic pe:

- SW-B, portul G0/1
- SW-CORE, portul G0/2 (spre SW-A)
- SW-CORE, portul G0/3 (spre SW-B)
- SW-CORE, portul G0/1 (spre R1) - da, și acesta: ruterul primește cadre etichetate

Cele două setări de disciplină `switchport trunk allowed vlan`: lăsată implicit, o legătură trunk transportă *toate* cele 4094 de VLAN-uri posibile. Declarând explicit lista, reduceți traficul inutil și limitați ce poate injecta un atacator.

`switchport trunk native vlan 99`: VLAN-ul nativ trebuie să fie unul gol. Dacă ar rămâne VLAN 1, o stație din VLAN 1 ar putea executa atacul de *double tagging* din cursul 12.

2. Verificați

pe SW-A

```
SW-A# show interfaces trunk
```

ce trebuie să apară

Port	Mode	Encapsulation	Status	Native vlan
G0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
G0/1	10,20,30,99

Dacă *Status* arată *not-trunking*, portul nu are legătură activă: verificați cablul sau capătul celălalt. Dacă *Native vlan* diferă între cele două capete ale aceleiași legături, IOS afișează un avertisment în consolă - nu îl ignorați, este exact vulnerabilitatea pe care încercați să o închideți.

3. Testați din nou izolarea pe PC1

```
ping 192.168.10.14
ping 192.168.20.15
```

Test	Rezultat așteptat	De ce
PC1 → PC4	merge	același VLAN 10, deși pe switch-uri diferite: cadrul a traversat trunk-ul, etichetat
PC1 → PC5	nu merge	trunk-ul transportă ambele VLAN-uri, dar nu le amestecă

Aceasta este ideea centrală a lucrării, într-o singură propoziție: **un trunk transportă mai multe VLAN-uri fără să le unească.**

4. Priviți eticheta 802.1Q

În bancul din pagină: dați `ping 192.168.10.14` de pe PC1 și priviți tabelul *Traseul ultimului pachet*. Coloana lipsă de pe portul de acces și prezentă pe trunk este chiar eticheta - segmentele dintre switch-uri poartă VLAN 10, cele dinspre stații nu poartă nimic.

În Packet Tracer: în *Simulation*, filtrat pe ICMP și ARP, faceți clic pe plicul de pe legătura trunk și deschideți *Outbound PDU Details*. Veți vedea, în structura cadrului Ethernet, un câmp suplimentar de 4 octeți, cu TPID 0x8100 și VLAN ID 10. Comparați cu același cadru pe un port de acces: acolo eticheta nu există. Aceasta este, la propriu, întreaga diferență dintre un port de acces și un port trunk.

3.7 Pasul 3: router-on-a-stick

Cele trei VLAN-uri sunt acum trei rețele complet separate. Departamentul ADMIN trebuie totuși să ajungă la resursele din PRODUCTIE. Ne trebuie un dispozitiv de nivel 3 - dar ruterul are o singură interfață liberă, iar noi avem trei rețele.

Soluția: **subinterfețele**. Aceeași interfață fizică se împarte logic în trei, fiecare cu adresa ei și cu eticheta ei de VLAN.

1. Configurați subinterfețele pe R1 pe R1

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
```

```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# no ip address
R1(config-if)# no shutdown
R1(config-if)# exit
```

```
R1(config)# interface gigabitEthernet 0/0/0.10
R1(config-subif)# description Gateway VLAN 10 ADMIN
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit
```

```
R1(config)# interface gigabitEthernet 0/0/0.20
```

```
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
```

```
R1(config)# interface gigabitEthernet 0/0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.168.30.1 255.255.255.0
R1(config-subif)# exit
```

```
R1(config)# interface gigabitEthernet 0/0/0.99
R1(config-subif)# encapsulation dot1Q 99 native
R1(config-subif)# end
```

```
R1# copy running-config startup-config
```

Trei greșeli care se fac de fiecare dată 1. `no shutdown` se dă pe interfața fizică. Dacă ea rămâne închisă, toate subinterfețele sunt moarte, oricât de corect ar fi configurate. Încercați: dați `shutdown` pe `G0/0/0` și priviți cum se sting toate obiectivele deodată.

2. Interfața fizică nu primește adresă IP - adresele stau pe subinterfețe.

3. Numărul subinterfeței (`.10`) nu are nicio semnificație pentru echipament; ceea ce contează este `encapsulation dot1Q 10`. Folosiți totuși același număr - vă va salva o oră de depanare peste șase luni.

2. Verificați rutarea completă

pe R1

```
R1# show ip interface brief
R1# show ip route
```

În tabela de rutare trebuie să apară **exact trei rute conectate**, marcate `C`, câte una pentru fiecare VLAN. Dacă apar doar două, una dintre subinterfețe nu are adresă sau are eticheta greșită.

pe PC1

```
ping 192.168.10.1
ping 192.168.20.12
ping 192.168.30.13
tracert 192.168.30.16
```

`tracert` va arăta exact un salt intermediar: gateway-ul. Traficul dintre două VLAN-uri urcă până la ruter și coboară înapoi pe același fir - de aici și denumirea de „router on a stick”.

3. Măsurăți gâtuirea

Tot traficul dintre toate VLAN-urile trece de două ori prin același cablu `G0/0/0`: o dată în sus, o dată în jos. Într-o rețea reală, aceasta este limita arhitecturii - și motivul pentru care secțiunea următoare există.

În Packet Tracer, rulați simultan de pe PC1 și PC4 ping-uri masive (`ping -n 200 -l 1400`) către stații din alt VLAN și comparați timpii cu cei obținuți când rulați singuri.

3.8 Varianta modernă: switch de nivel 3

Înlocuiți SW-CORE cu un switch **3560** și eliminați complet ruterul. Rutarea se face acum în hardware, pe back-plane-ul switch-ului, fără niciun cablu implicat. În bancul din pagină, aceeași demonstrație se face activând rutarea chiar pe SW-CORE.

```
SW-CORE(config)# ip routing

SW-CORE(config)# interface vlan 10
SW-CORE(config-if)# ip address 192.168.10.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# exit

SW-CORE(config)# interface vlan 20
SW-CORE(config-if)# ip address 192.168.20.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# exit

SW-CORE(config)# interface vlan 30
SW-CORE(config-if)# ip address 192.168.30.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# end

SW-CORE# show ip route
```

Listingul 3.1 pe SW-CORE copiază

Nu le faceți pe amândouă deodată. Dacă lăsați și ruterul, și SVI-urile configurate, cele trei gateway-uri vor exista în două locuri - adrese IP duplicate. În bancul din pagină, scoateți întâi cablul lui R1 din panoul *Cablurile*, sau dați shutdown pe interfața lui fizică.

Router-on-a-stick.

- Funcționează cu orice ruter, chiar și vechi
- Ruterul poate face și NAT, VPN, ACL-uri complexe
- Configurare simplă, ușor de explicat

Switch de nivel 3 cu SVI

- Rutare în hardware, fără gătuire
- Nu consumă niciun cablu și niciun port
- Echipament mai scump; funcții de securitate mai limitate decât la un ruter

Testați aceleași ping-uri ca înainte. Rezultatul funcțional este identic, dar traficul nu mai iese niciodată din switch - verificați cu `tracert`, unde saltul intermediar rămâne unul singur, dar este chiar switch-ul.

3.9 Spanning Tree, observat

Adăugați o legătură directă între SW-A și SW-B, configurată tot ca trunk. În bancul din pagină: alegeți SW-A, din panoul *Cablurile* apăsați *leagă* pe portul G0/2 și alegeți SW-B : G0/2. Ați creat o buclă fizică între cele trei switch-uri - exact situația din cursul 4.

```
SW-A# show spanning-tree
SW-CORE# show spanning-tree
```

Listingul 3.2 observarea arborelui copiază

1. Identificați care switch a devenit **root bridge** - apare cu mențiunea `This bridge is the root`. Fără nicio configurare, decide adresa MAC cea mai mică, deci de regulă cel mai vechi echipament din rețea. Ra-reori cel pe care l-ați fi ales voi.
2. Găsiți portul aflat în starea `BLK`, cu rolul `Altn`. Acela este cablul pe care STP l-a scos din uz ca să rupă bucla. Legătura există fizic, dar nu transportă nimic.

- 3. Verificați că ping-ul dintre PC1 și PC4 funcționează în continuare: bucla a fost neutralizată fără să se piardă conectivitatea.
- 4. Forțați rădăcina pe switch-ul din centru, unde vă convine să fie:

```
SW-CORE(config)# spanning-tree vlan 10,20,30,99 root primary
SW-A(config)# spanning-tree vlan 10,20,30,99 root secondary
```

Listingul 3.3 rădăcina, stabilită explicit copiază

Rulați din nou `show spanning-tree` pe SW-CORE: acum el este rădăcina, iar portul blocat s-a mutat. Comanda `root primary` nu face nimic magic - pune prioritatea la 24576, o valoare mai mică decât cea implicită (32768), iar prioritatea mai mică câștigă alegerea.

Exemplul 3.1. Deconectați cablul dintre SW-CORE și SW-A. Cronometrați cât durează până când ping-ul dintre PC1 și PC4 începe să funcționeze din nou, prin legătura de rezervă.

Rezolvare. Aproximativ 30–50 de secunde cu STP clasic: max age (20 s) plus tranzițiile prin listening și learning (2 × 15 s). Activați apoi modul rapid și repetați măsurătoarea:

pe toate switch-urile

```
Switch(config)# spanning-tree mode rapid-pvst
```

Convergența scade la câteva secunde. Este exact motivul pentru care nicio rețea modernă nu mai rulează 802.1D clasic.

3.10 Patru defecte de diagnosticat

Provoacă-le pe rând, în bancul de lucru. De fiecare dată notați **ce comandă v-a arătat problema** - asta rămâne util după laborator.

Tabelul 3.4 Patru defecte de diagnosticat.

Defect	Cum îl produceți	Simptom	Comanda care îl scoate la iveală
VLAN lipsă pe switch-ul de tranzit	pe SW-CORE: <code>no vlan 20</code>	VLAN 10 și 30 merg peste trunk, VLAN 20 nu	<code>show vlan brief</code> pe SW-CORE
VLAN scos din lista permisă	pe SW-A <code>G0/1: switchport trunk allowed vlan 10,30,99</code>	PC2 nu mai ajunge nicăieri în afara switch-ului	<code>show interfaces trunk</code>
Port lăsat în VLAN 1	pe SW-B: <code>no switchport access vlan 10</code> pe Fa0/1	PC4 dispare din rețeaua lui, dar cablul e verde	<code>show vlan brief</code> pe SW-B
Etichetă greșită pe subinterfață	pe R1: <code>encapsulation dot1Q 25</code> în loc de 20	VLAN 20 nu are gateway; celelalte funcționează	<code>show running-config</code> pe R1

Tiparul comun. Toate cele patru defecte produc același simptom general - „un VLAN nu merge, celelalte da” - și niciunul nu se vede în starea cablurilor. Când auziți acest simptom, ordinea de verificare este întotdeauna aceeași: VLAN-ul există pe *toate* switch-urile de pe drum? Portul de acces e în VLAN-ul corect? VLAN-ul e permis pe *fiecare* trunk? Subinterfața ruterului are eticheta corectă?

3.11 Provocare

Exemplul 3.2. VLAN-ul 30 este pentru vizitatori. Politica firmei cere: **vizitatorii au acces la Internet, dar nu la nicio resursă internă**. În laboratorul acesta încă nu aveți Internet, așa că simulați-l cu un server plasat într-un VLAN 40, 192.168.40.0/24.

Cerințe:

1. PC3 și PC6 (VLAN 30) trebuie să ajungă la serverul din VLAN 40
2. PC3 și PC6 **nu** trebuie să ajungă la nicio stație din VLAN 10 sau 20
3. Stațiile din VLAN 10 și 20 trebuie să ajungă peste tot, inclusiv la stațiile din VLAN 30

Punctul 3 este partea interesantă: traficul de la ADMIN spre OASPETI trebuie să treacă, dar cel invers nu. Gândiți-vă ce fel de listă de acces vă trebuie și pe ce direcție se aplică. Formulați în cuvinte regula exactă și motivați plasarea ei - configurarea propriu-zisă o veți face în laboratorul 6.

Rezolvare. O listă **standard** nu ajunge: ea filtrează doar după sursă, iar sursa este aceeași (VLAN 30) și în traficul permis (spre VLAN 40) și în cel interzis (spre VLAN 10 și 20). Vă trebuie o listă **extinsă**, care să vadă și destinația.

Regula ar suna astfel: „respinge traficul IP cu sursa în 192.168.30.0/24 și destinația în 192.168.10.0/24 sau 192.168.20.0/24; permite restul”. Plasarea corectă este pe subinterfața G0/0/0.30, direcția in - adică cât mai aproape de sursă, ca traficul interzis să nici nu ajungă la ruter.

Punctul 3 funcționează automat cu această plasare: traficul ADMIN → OASPETI intră pe G0/0/0.10, unde lista nu este aplicată, deci nu este filtrat.

3.12 Ce se predă

Tabelul 3.5 Ce se predă.

Livrabil	Format	Punctaj
Fișierul Packet Tracer cu VLAN-uri, trunk-uri și rutare inter-VLAN funcționale	.pkt	35 %
Captura etichetei 802.1Q, comentată	document	15 %
Cele patru defecte, cu simptom și comandă de diagnostic	document	20 %
Comparația router-on-a-stick / switch de nivel 3, cu traseul pachetului în ambele	document	15 %
Provocarea: regula formulată în cuvinte, cu plasarea justificată	document	15 %

Exerciții

1. Doua stații sunt în porturi vecine ale aceluiași switch, dar în VLAN-uri diferite. Se aude?
 - a. Da, sunt pe același switch
 - b. Nu: switch-ul nu comută între VLAN-uri, tabela MAC este indexată și după VLAN
 - c. Da, dacă au aceeași mască
 - d. Doar prin broadcast
2. Ce transportă un port trunk?
 - a. Un singur VLAN, mai repede
 - b. Cadre din mai multe VLAN-uri, fiecare cu o etichetă 802.1Q de 4 octeți
 - c. Doar trafic de management
 - d. Doar cadre netichetate

3. De ce se alege un VLAN nativ gol, de exemplu 99?
 - a. Ca sa fie mai rapid
 - b. Pentru ca traficul VLAN-ului nativ circula netichetat; daca ar fi VLAN-ul statiilor, ar fi posibil atacul de double tagging
 - c. Pentru ca IOS o cere
 - d. Ca sa incapa mai multe VLAN-uri
4. Ati configurat corect trei subinterfete pe ruter, dar nimic nu functioneaza. Ce verificati intai?
 - a. Adresele IP ale statiilor
 - b. Daca interfata fizica are no shutdown
 - c. Masca de retea
 - d. Cablul de consola
5. Un VLAN merge intre statiile de pe acelasi switch, dar nu si spre celalalt switch. Unde cautati?
 - a. La adresele IP
 - b. La lista switchport trunk allowed vlan si la existenta VLAN-ului pe switch-ul de tranzit
 - c. La masca de subretea
 - d. La viteza portului
6. Ce face comanda spanning-tree vlan 10 root primary?
 - a. Blocheaza un port
 - b. Pune prioritatea switch-ului la 24576, deci il face sa castige alegerea radacinii
 - c. Dezactiveaza STP
 - d. Face portul sa treaca direct in forwarding

Extras din volumul „Rețele Locale - Note de curs și lucrări de laborator”. Varianta online a acestui capitol conține figurile în formă interactivă.