

Optimizarea rețelelor locale

Un switch cu 48 de porturi rezolvă coliziunile, dar lasă 48 de calculatoare într-un singur domeniu de broadcast, fără nicio separare între departamente și fără nicio cale de rezervă dacă un cablu cedează. Cursul acesta prezintă cele patru unelte care transformă o grămadă de switch-uri într-o rețea proiectată: VLAN-ul, legătura trunk, Spanning Tree și agregarea legăturilor.

Din capitolul precedent.

- Un switch **învață** din adresa MAC sursă, **comută** după adresa MAC destinație și **inundă** când nu știe unde e destinatarul.
- Switch-ul **separă** domeniile de coliziune (unul per port) dar **extinde** domeniul de broadcast - toate porturile lui formează unul singur.
- Un cadru de broadcast este inundat pe toate porturile, indiferent ce conține tabela CAM.
- Nivelul 2 **nu are TTL**. Rețineți asta - este cheia întregii a doua jumătăți a acestui curs.

OBIECTIVELE CAPITOLULUI

- Să explicați ce problemă rezolvă un VLAN și de ce nu e suficient un ruter
- Să distingeți un port de acces de un port trunk și să citiți o etichetă 802.1Q
- Să explicați rolul VLAN-ului nativ și riscul lui de securitate
- Să comparați cele două soluții de rutare între VLAN-uri
- Să explicați de ce o buclă la nivelul 2 este fatală, iar una la nivelul 3 nu
- Să rulați, pas cu pas, algoritmul STA pe o topologie dată
- Să configurați o legătură agregată și să știți ce moduri se combină între ele

4.1 Ce nu merge într-un LAN plat

Să luăm un exemplu concret. O firmă are trei departamente - contabilitate, producție și o zonă pentru vizitatori - răspândite pe trei etaje, cu câte un switch pe fiecare etaj,

toate legate între ele. Fără nicio separare logică, apar simultan cinci probleme.

Tabelul 4.1 Ce nu merge într-un LAN plat.

Problemă	Cum se manifestă	Ce am vrea
Securitate	orice stație poate încerca să acceseze orice altă stație; broadcast-urile ajung peste tot, inclusiv la vizitatori, și pot conține informație utilă unui atacator	blocarea accesului direct între departamente
Eficiență	un singur broadcast este procesat de toate stațiile din firmă; într-o rețea cu multe switch-uri, impactul devine costisitor	limitarea domeniilor de broadcast
Administrare	politicile se aplică per switch, dar departamentele sunt amestecate pe etaje	politici per departament, indiferent de locația fizică
Calitate (QoS)	telefoanele IP și videoconferința concurează cu descărcările de fișiere pentru aceeași bandă	trafic separat, cu prioritate proprie
Cost	separarea fizică ar cere switch-uri și cablare suplimentare	o soluție software peste echipamentele existente

De ce broadcast-urile sunt o problemă reală. Un cadru de broadcast nu este doar „încă un cadru”. Fiecare stație din domeniu îl primește, îl urcă până la sistemul de operare și îl procesează - chiar dacă apoi decide că nu o privește. Este muncă reală, făcută de fiecare calculator, pentru fiecare broadcast.

Într-o rețea cu 500 de stații, protocoalele obișnuite (ARP, DHCP, descoperirea de servicii, anunțuri de rețea) produc suficient trafic de broadcast cât să consume, permanent, o parte vizibilă din procesorul fiecărei stații. Iar dacă apare o buclă, așa cum vom vedea mai jos, rețeaua moare într-o secundă.

De ce nu pur și simplu un ruter?

Întrebarea e legitimă: știm din cursul trecut că ruterul separă domenii de broadcast. Răspunsul are patru părți:

1. Ruterele sunt **semnificativ mai scumpe** per port decât switch-urile.
2. Procesează nivelul 3, deci introduc **latență mai mare**.
3. Consumă **o interfață pentru fiecare segment**, iar ruterele au puține interfețe.
4. Cel mai important: ruterul separă după **cablare**, dar stațiile aceluiași departament pot fi răspândite fizic prin toată clădirea. Ar trebui să recablați clădirea la fiecare reorganizare.

4.2 Ce este un VLAN

DEFINIȚIA 4.1 (VLAN - VIRTUAL LAN). Un domeniu de broadcast format **doar din anumite porturi** ale unui sau mai multor switch-uri. Un VLAN este definit prin porturile care îi aparțin și este identificat printr-un număr - **VLAN ID** - reprezentat pe 12 biți, deci între 1 și 4094.

Analogie O clădire de birouri cu un singur hol mare, unde toată lumea aude tot. VLAN-urile sunt pereți despărțitori montați peste noapte: fizic e aceeași clădire, aceleași cabluri, aceleași switch-uri - dar acum fiecare departament se aude doar pe sine. Iar dacă cineva se mută la alt etaj, îl muți și pe el în „camera” lui, fără să spargi niciun zid.

Intern, fiecare switch asociază fiecărui port un VLAN ID. Pe echipamentele Cisco, toate porturile aparțin inițial VLAN-ului 1. Un port care aparține unui singur VLAN se numește **port de acces**; pentru stația conectată la el, apartenența la VLAN este complet **transparentă** - nu se configurează nimic pe calculator, iar utilizatorul nu are cum să afle.



Figura 4.1 Ce face, concret, un VLAN.

Regula care se uită cel mai des. Un VLAN trebuie **creat** pe switch înainte de a i se atribui porturi. Și, mai important: pentru a comuta trafic aparținând VLAN-ului X, un switch trebuie să aibă VLAN-ul X configurat local - **chiar dacă traficul doar tranzitează prin el**.

Un VLAN care „nu ajunge” este, în nouă cazuri din zece, un VLAN lipsă pe un switch intermediar. Este prima verificare la orice problemă de acest fel.

4.3 Porturi de acces și legături trunk

Până acum am lucrat cu un singur switch. Ce se întâmplă când VLAN-urile trebuie să treacă dintr-un switch în altul?

Problema

Prima idee este să folosim un cablu pentru fiecare VLAN: trei VLAN-uri, trei cabluri, trei porturi consumate la fiecare capăt. Soluția funcționează perfect - și e complet inutilizabilă. Zece VLAN-uri ar însemna zece porturi ocupate pe fiecare switch, doar pentru interconectare, plus zece cabluri de tras.

Soluția: legătura trunk

DEFINIȚIA 4.2 (PORT DE ACCES VS. PORT TRUNK). Un **port de acces** aparține unui singur VLAN. Cadrele care circulă pe el sunt cadre Ethernet obișnuite, fără nicio marcă. Aici se conectează stațiile.

Un **port trunk** transportă traficul **mai multor VLAN-uri** pe același fir. Fiecare cadru primește o etichetă care spune cărui VLAN îi aparține. Aici se conectează switch-urile între ele.

Ambele capete ale unei legături trunk trebuie configurate ca porturi trunk, iar setul de VLAN-uri permise pe ea este configurabil - implicit, toate.

Eticheta 802.1Q

Rămâne întrebarea concretă: dacă switch-ul 1 trimite pe trunk un cadru din VLAN-ul 10, cum știe switch-ul 2 în ce VLAN să îl plaseze? Răspunsul este că i se inserează 4 octeți suplimentari în cadrul Ethernet, imediat după adresa sursă.



Figura 4.2 Cadrul etichetat 802.1Q, câmp cu câmp.

Ce se întâmplă, de fapt, cu eticheta. Eticheta este pusă de switch la **intrarea pe trunk** și scoasă la **ieșirea pe un port de acces**. Stațiile nu văd niciodată o etichetă și nu trebuie configurate în niciun fel.

Excepția o constituie serverele de virtualizare și telefoanele IP, care sunt configurate deliberat ca porturi trunk, pentru că trebuie să pună singure trafic în mai multe VLAN-uri.

4.4 VLAN-ul nativ

Fiecare legătură trunk are un VLAN special, numit **nativ**, ale cărui cadre circulă **neetichetate** - în format Ethernet obișnuit, ca și cum trunk-ul nici nu ar exista.

Motivul este istoric: compatibilitatea cu echipamente care nu înțeleg 802.1Q și care, altfel, ar arunca toate cadrele de pe trunk. Cele două capete trebuie să aibă configurat **același** VLAN nativ; altfel traficul dintr-un VLAN aterizează, tăcut și fără niciun mesaj de eroare, în alt VLAN.

VLAN-ul nativ și securitatea. Faptul că VLAN-ul nativ circulă neetichetat este exact vulnerabilitatea exploatată de atacul de tip **double tagging**, discutat în cursul 12: un atacator aflat în VLAN-ul nativ construiește un cadru cu **două** etichete, primul switch o scoate pe cea exterioară, iar a doua îl duce într-un VLAN în care nu avea voie.

Recomandarea practică, valabilă în orice rețea reală: setați ca VLAN nativ un VLAN nefolosit, în care nu se află nicio stație.

Exercițiu rezolvat 4.1. Topologie: SW1 - SW0 - SW2, legate prin trunk-uri cu VLAN nativ 10. Stația A este pe SW1 în VLAN 10, stația B pe SW2 în VLAN 10, stațiile C și D pe SW0 în VLAN 20. Stația A emite un broadcast. La cine ajunge și în ce format circulă pe legături?

Rezolvare. Ajunge doar la B. Broadcast-ul se propagă exclusiv în VLAN-ul emițătorului, iar C și D sunt în VLAN 20. Traseul este A → SW1 → SW0 → SW2 → B.

Pe ambele legături trunk cadrul circulă neetichetat, în format Ethernet standard - pentru că VLAN-ul 10 este chiar VLAN-ul nativ al trunk-urilor.

Dacă VLAN-ul nativ ar fi fost 1, același cadru ar fi circulat etichetat 802.1Q cu VLAN ID 10. Aceasta e singura diferență, dar produce confuzie de fiecare dată la examen.

4.5 Rutarea între VLAN-uri

VLAN-urile izolează - asta e treaba lor. Uneori însă chiar vrem ca departamentul de producție să ajungă la serverul contabilității. Controlat, dar să ajungă.

Fiind domenii de broadcast distincte, două VLAN-uri nu pot comunica fără un dispozitiv de nivel 3. Există două soluții clasice și una modernă.

Soluția clasică: o interfață per VLAN

Ruterul primește câte o interfață fizică pentru fiecare VLAN, iar fiecare interfață se conectează la un port de acces din VLAN-ul respectiv. Traficul intră pe o interfață și iese pe alta, ruterul făcând rutarea normală între rețelele lui conectate.

Soluția router-on-a-stick

O singură interfață fizică a ruterului se leagă la un port **trunk** al switch-ului și se împarte logic în **subinterfețe**, câte una pentru fiecare VLAN. Fiecare subinterfață primește adresă IP proprie și este informată că traficul vine etichetat 802.1Q cu un anumit VLAN ID.

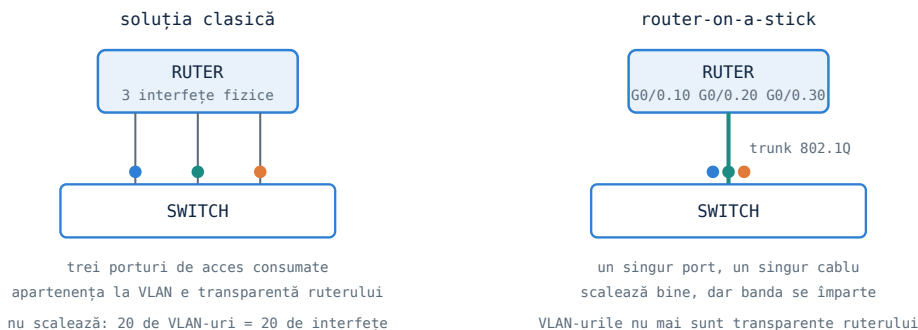


Figura 4.3 Aceeași funcție, două arhitecturi.



Figura 4.4 Traseul unui pachet prin router-on-a-stick.

Router-on-a-stick.

- Funcționează cu orice ruter, chiar și vechi
- Un singur cablu, un singur port
- Ruterul poate face simultan NAT, VPN, ACL-uri complexe
- Scalează bine la numărul de VLAN-uri

Switch de nivel 3 cu SVI

- Rutare în hardware, pe backplane - fără nicio gătuire
- Nu consumă niciun cablu și niciun port
- Echipament mai scump
- Funcții de securitate mai limitate decât ale unui ruter

Ce se folosește azi. În rețelele moderne de întreprindere, rutarea între VLAN-uri se face aproape întotdeauna pe un **switch de nivel 3**, prin interfețe virtuale numite **SVI** (Switched Virtual Interface). Traficul nu mai părăsește niciodată switch-ul.

Router-on-a-stick rămâne relevant pentru rețele mici, pentru echipamente existente și - mai ales - pentru că este cea mai clară ilustrare a ceea ce face, de fapt, eticheta 802.1Q. Îl veți configura la laboratorul 3.

4.6 Redundanța și problema buclelor

Dacă legătura dintre două switch-uri cade, stațiile din spatele lor nu mai comunică. Soluția evidentă este o legătură de rezervă. Soluția evidentă produce însă o **bucă fizică** - iar o buclă fizică într-o rețea comutată produce trei efecte simultane, toate catastrofale.



Figura 4.5 Ce se întâmplă, exact, într-o buclă de nivel 2.

De ce nivelul 3 nu are această problemă. Un pachet IP prins într-o buclă de rutare are câmpul **TTL** decrementat la fiecare ruter. Când ajunge la zero, pachetul e aruncat și se trimite un mesaj înapoi la sursă. Bucla există, produce trafic inutil și se vede imediat cu `traceroute` - dar rețeaua rămâne funcțională.

Antetul Ethernet nu are niciun echivalent al TTL-ului. Aceasta este singura, dar decisivă, diferență - și motivul pentru care STP a trebuit inventat.

4.7 Spanning Tree: rolurile și costurile

Ideea protocolului **STP** (Spanning Tree Protocol, IEEE 802.1D) este simplă și elegantă: acceptăm bucla fizică, pentru că ne trebuie redundanța, dar **blocăm logic** unul dintre porturile buclei. Dacă legătura principală cade, portul blocat este redeschis.

Algoritmul folosit se numește **STA** (Spanning Tree Algorithm) și este, în esență, calculul unui arbore de acoperire pe graful switch-urilor - o problemă clasică de teoria grafurilor, aplicată în timp real, de echipamente care nu se cunosc între ele.

Cele patru roluri

Tabelul 4.2 Cele patru roluri.

Rol	Cine îl are	Ce face portul
Root bridge	switch-ul cu cel mai mic Bridge ID din rețea	toate porturile lui sunt desemnate
Root port (RP)	câte unul singur pe fiecare switch non-root	calea cea mai bună spre rădăcină; trimite și primește date
Designated port (DP)	câte unul singur pe fiecare legătură	trimite și primește date
Blocked port (BLK)	tot ce rămâne	nu trimite și nu primește date, dar continuă să asculte BPDU-uri

De ce portul blocat continuă să asculte. Dacă ar tăcea complet, nu ar avea cum să afle că legătura principală a căzut. Ascultând în continuare mesajele STP (numite **BPDU**), observă tăcerea de pe calea principală și se poate redeschide.

Portul blocat este, cu alte cuvinte, o santinelă: nu lasă nimic să treacă, dar privește permanent și e gata să deschidă poarta.

Bridge ID: cine devine rădăcină

Fiecare switch are un identificator unic pe 64 de biți: **16 biți de prioritate** (implicit 32768) urmați de **48 de biți de adresă MAC**. Compararea se face lexicografic: întâi prioritatea, iar la egalitate adresa MAC.

Consecința practică pe care nimeni nu o vrea. Dacă nu configurați nimic, toate switch-urile au prioritatea 32768, deci decide **adresa MAC cea mai mică** - adică, statistic, echipamentul **cel mai vechi** din rețea.

Rezultatul tipic: rădăcina arborelui ajunge un switch de acces prăfuit dintr-un dulap, iar tot traficul dintre switch-urile moderne de magistrală trece prin el. Rețeaua funcționează, dar mult sub capacitatea ei, iar cauza e practic invizibilă dacă nu știți ce să căutați.

De aceea, într-o rețea reală, rădăcina se stabilește **explicit**.

Costurile legăturilor

Tabelul 4.3 Costurile legăturilor.

Lățime de bandă	Cost STP clasic	Cost în varianta extinsă
10 Mbps	100	2 000 000
100 Mbps	19	200 000
1 Gbps	4	20 000
10 Gbps	2	2 000

Costul unei căi este suma costurilor legăturilor parcurse. Observați că valorile nu sunt liniare: o legătură de 10 Mbps costă de 25 de ori mai mult decât una de 1 Gbps, deși e de 100 de ori mai lentă. Scara a fost aleasă empiric, iar la vitezele moderne a devenit prea comprimată - de aici varianta extinsă.



Figura 4.6 Calculator STP: patru switch-uri, cinci legături.

Experimentele de făcut aici.

1. Lăsați totul implicit. Cine devine rădăcină? De ce? (Uitați-vă la adresele MAC.)
2. Coborâți prioritatea switch-ului **D** la 4096. Arborele se reorganizează complet în jurul lui - aceasta este exact metoda prin care un administrator forțează rădăcina.
3. Reveniți la prioritățile egale și schimbați viteza legăturii **A–C** la 10 Mbps. Priviți cum se mută portul blocat: calea a devenit scumpă, deci STP alege altă rută.
4. Faceți două legături identice ca viteză și cost. Cum se rupe egalitatea? (Prin Bridge ID.)

4.8 Cei patru pași ai algoritmului

Switch-urile schimbă între ele mesaje numite **BPDU** (Bridge Protocol Data Unit), trimise o dată la 2 secunde pe toate porturile, către adresa multicast 01:80:c2:00:00:00. Un BPDU conține patru informații: ID-ul rădăcinii cunoscute, costul până la ea, ID-ul propriu și ID-ul portului.

1. **Alegerea rădăcinii.** Fiecare switch pornește crezând că el este rădăcina. Când primește un BPDU cu un Bridge ID mai mic, își schimbă părerea și îl propagă mai departe. După câteva secunde, toată lumea e de acord cine e rădăcina.

2. **Alegerea porturilor rădăcină.** Fiecare switch non-root alege **un singur** port: cel cu costul cumulativ minim spre rădăcină. La egalitate de cost decide Bridge ID-ul vecinului, apoi Port ID-ul.
3. **Alegerea porturilor desemnate.** Pe fiecare legătură trebuie să existe exact un port desemnat: cel al switch-ului cu cost mai mic spre rădăcină; la egalitate, cel cu Bridge ID mai mic. Rădăcina are întotdeauna **numai** porturi desemnate.
4. **Blocarea restului.** Orice port care nu e nici rădăcină, nici desemnat trece în starea *blocking*.



Figura 4.7 Puneți în ordine pașii algoritmului STA.

Exercițiu rezolvat 4.2. Cinci switch-uri au următoarele Bridge ID-uri. Care devine rădăcină?

Switch	Prioritate	Adresă MAC
A	16384	00E0.A3C9.6AB8
B	32768	0001.97DA.86E8
C	8192	00D0.BC0C.844D
D	16384	0003.E496.C80E
E	8192	0060.2F07.EB2B

Rezolvare. Se compară **întâi prioritatea**. Cea mai mică este 8192, deci rămân în cursă doar **C** și **E**. Switch-ul B, deși are cea mai mică adresă MAC dintre toate, este eliminat imediat - prioritatea lui e 32768.

Între C și E se compară **adresa MAC**: 00D0... față de 0060... Comparăția se face octet cu octet, de la stânga: primul octet e 00 la ambele; al doilea este D0 = 208 la C și 60 = 96 la E. Deci **E câștigă**.

Rădăcina este E. Capcana clasică e să vă uitați întâi la adresa MAC - prioritatea se compară prima, întotdeauna.

4.9 Stările porturilor și timpul de convergență

Un port nu trece direct din „blocat” în „funcțional”. Parcurge o serie de stări, fiecare cu rolul ei.

Tabelul 4.4 Stările porturilor și timpul de convergență.

Stare	Transmite date	Învață adrese MAC	Procesează BPDU	Durață
Disabled	nu	nu	nu	portul e închis administrativ
Blocking	nu	nu	doar primește	până la 20 s (max age)
Listening	nu	nu	trimite și primește	15 s (forward delay)
Learning	nu	da	trimite și primește	15 s (forward delay)
Forwarding	da	da	trimite și primește	stare finală

De ce există starea „learning”. Dacă portul ar trece direct în forwarding, tabela CAM ar fi goală și switch-ul ar inunda tot traficul - exact în momentul cel mai delicat, imediat după o reconfigurare a topologiei.

Starea *learning* îi dă 15 secunde să își umple tabela ascultând traficul, **fără** să transmită nimic. Când trece în forwarding, știe deja unde e fiecare stație.

Cincizeci de secunde de tăcere. Convergența STP clasic poate dura până la **50 de secunde**: 20 pentru max age, plus 2×15 pentru tranzițiile prin listening și learning.

Pentru un utilizator care doar și-a pornit calculatorul și așteaptă ca portul să se activeze, aproape un minut de tăcere este inacceptabil - și generează un bilet la serviciul de asistență. De aceea au apărut variantele rapide din secțiunea următoare, plus mecanismul **PortFast**, care sare peste tranziții pe porturile unde sigur nu există alt switch.

4.10 Variantele moderne de STP

Tabelul 4.5 Variantele moderne de STP.

Variantă	Standard	Ce aduce
STP	802.1D	originalul; convergență până la 50 s; un singur arbore pentru toate VLAN-urile
RSTP	802.1w	convergență în câteva secunde; roluri noi de port (alternate, backup)
PVST+	Cisco	câte un arbore pentru fiecare VLAN - permite folosirea simultană a legăturilor redundante
Rapid-PVST+	Cisco	combinația celor două de mai sus; alegerea uzuală într-o rețea Cisco
MSTP	802.1s	grupează VLAN-urile în câteva instanțe de arbore - scalează mai bine decât un arbore per VLAN

Ideea din spatele variantelor per-VLAN. Cu un singur arbore pentru toate VLAN-urile, o legătură blocată este blocată pentru tot traficul - deci un cablu scump stă complet nefolosit.

Cu un arbore separat pentru fiecare VLAN, puteți face ca VLAN-ul 10 să folosească legătura din stânga și VLAN-ul 20 pe cea din dreapta. Ambele legături transportă trafic, redundanța rămâne, iar banda disponibilă se dublează. Este exact motivul pentru care aceste variante au apărut.

4.11 EtherChannel: mai multe cabluri, o singură legătură

STP rezolvă buclele blocând porturi - ceea ce înseamnă că o legătură scumpă stă nefolosită. Agregarea legăturilor rezolvă aceeași problemă altfel: mai multe legături fizice sunt combinate într-o **singură interfață logică**, pe care STP o vede ca pe un singur link.

Nu mai există buclă, deci nu se blochează nimic, iar banda se însumează.

Analogie Patru benzi de autostradă în loc de una. Din punctul de vedere al hărții rutiere, e tot „autostrada A1” - un singur drum. Dar capacitatea e de patru ori mai mare, iar dacă o bandă se închide pentru lucrări, traficul continuă pe celelalte, fără nicio re-planificare a traseului.

Avantaje.

- Banda se adună: patru legături de 1 Gbps devin una logică de 4 Gbps
- Configurarea se face o singură dată, pe interfața logică
- Redundanță fără timpul de convergență al STP - căderea unui membru nu întrerupe legătura
- Distribuirea traficului între membri (load balancing)

Restricții

- Maximum 8 interfețe fizice într-un grup
- Toți membrii trebuie să aibă aceeași viteză, același duplex, același mod (acces sau trunk), același set de VLAN-uri permise și același VLAN nativ
- Distribuirea se face **per flux**, nu per cadru: o singură sesiune nu depășește banda unui membru

De ce distribuirea se face per flux. Dacă switch-ul ar trimite cadrele alternativ pe fiecare legătură, ele ar putea ajunge la destinație **în altă ordine** decât au plecat - legăturile nu au latențe perfect identice. Reordonarea ar strica performanța TCP mult mai mult decât ar ajuta banda suplimentară.

De aceea switch-ul calculează un hash din adresele sursă și destinație și trimite **toate** cadrele unei conversații pe aceeași legătură. Consecința practică: o singură copie de fișier între două servere nu va depăși niciodată 1 Gbps pe un canal de 4 Gbps. Banda agregată ajută la **multe** conversații simultane, nu la una singură.

Protocoloalele de negociere

Tabelul 4.6 Protocoloalele de negociere.

	PAgP	LACP
Origine	proprietar Cisco	IEEE 802.3ad, ulterior 802.1AX
Mod activ	desirable	active
Mod pasiv	auto	passive
Fără negociere	on - recomandat între echipamente de producători diferiți	

Regula de combinare este aceeași la ambele protocoale și merită memorată prin logica ei, nu prin tabel: **cel puțin un capăt trebuie să inițieze**. Două capete pasive nu vor forma niciodată un canal, pentru că amândouă așteaptă. Iar `on` nu se combină cu nimic altceva decât cu `on`, pentru că nu trimite niciun pachet de negociere - celălalt capăt nu are ce să audă.



Figura 4.8 Ce combinații formează un canal agregat.

4.12 Greșeli frecvente

Greșeli frecvente.

„Am creat VLAN-ul pe switch-urile de capăt, deci e gata”

Fiecare switch prin care tranzitează traficul trebuie să aibă VLAN-ul configurat local, chiar dacă nu are nicio stație în el.

La orice VLAN care „nu ajunge”, verificați întâi switch-urile intermediare.

„VLAN-ul nativ nu contează, e doar o setare”

Dacă cele două capete ale unui trunk au VLAN-uri native diferite, traficul dintr-un VLAN aterizează tăcut în altul - fără niciun mesaj de eroare.

Setați același VLAN nativ la ambele capete, și alegeți unul nefolosit.

„Am pus adresă IP pe interfața fizică a ruterului, la router-on-a-stick”

Adresele stau pe subinterfețe . Interfața fizică primește doar no shutdown . Dacă o lăsați închisă, toate subinterfețele sunt moarte, oricât de corect ar fi configurate.

Fizică: doar activată. Logică: adresă și încapsulare.

„STP încetinește rețeaua, hai să îl dezactivăm”

Cea mai costisitoare decizie posibilă. Fără STP, prima buclă accidentală - un cablu pus greșit de cineva grăbit - oprește complet rețeaua.

Nu dezactivați STP. Treceți pe Rapid-PVST+ și puneți PortFast pe porturile de acces.

„Am legat două switch-uri cu patru cabluri, deci am 4 Gbps”

Fără EtherChannel configurat, STP va bloca trei dintre ele - aveți 1 Gbps și trei cabluri decorative.

Agregarea trebuie configurată explicit, pe ambele capete.

4.13 Rezumat și glosar

1. **VLAN-ul** împarte un switch fizic în mai multe domenii de broadcast, definite prin porturi și independente de cablare.
2. **Trunk-ul** transportă mai multe VLAN-uri pe un singur cablu, folosind eticheta 802.1Q. VLAN-ul nativ circulă neetichetat - și de aceea trebuie ales cu grijă.
3. Comunicația între VLAN-uri cere un dispozitiv de **nivel 3**: ruter cu subinterfețe sau switch de nivel 3 cu SVI.
4. O buclă la nivelul 2 este **fatală**, pentru că lipsește TTL-ul. **STP** o rezolvă blocând logic un port.
5. **EtherChannel** transformă mai multe cabluri într-o singură legătură logică - bandă însumată, fără buclă și fără blocare.

Exerciții

1. Cate VLAN-uri pot fi identificate cu campul VLAN ID din eticheta 802.1Q?
 - a. 256
 - b. 1024
 - c. 4094 utilizabile din 4096 posibile
 - d. 65536
2. Ce se intampla cu un cadru din VLAN-ul nativ cand traverseaza un trunk?
 - a. Primeste eticheta 802.1Q ca oricare altul
 - b. Circula neetichetat, in format Ethernet standard
 - c. Este aruncat
 - d. Este duplicat pe toate VLAN-urile
3. De ce o bucla la nivelul 2 este mult mai grava decat una la nivelul 3?
 - a. Pentru ca switch-urile sunt mai lente decat ruterele
 - b. Pentru ca antetul de nivel 2 nu are camp TTL, deci nimic nu opreste cadrul
 - c. Pentru ca adresele MAC sunt mai scurte decat cele IP
 - d. Pentru ca nivelul 2 nu foloseste broadcast
4. Cate porturi radacina are switch-ul care este root bridge?
 - a. Unul
 - b. Cate unul pe fiecare legatura
 - c. Niciunul - toate porturile lui sunt desemnate
 - d. Depinde de prioritate
5. Doua switch-uri au ambele porturile LACP in modul passive. Se formeaza Ether-Channel?
 - a. Da, LACP negociaza automat
 - b. Nu, cel putin un capat trebuie sa fie active
 - c. Da, dar doar pentru VLAN-ul nativ
 - d. Doar daca vitezele difera
6. Ce se compara primul, la alegerea root bridge-ului?
 - a. Adresa MAC
 - b. Prioritatea
 - c. Numarul de porturi
 - d. Viteza legaturilor

7. La ce folosește starea learning din STP?
- a. Pentru a învăța topologia STP
 - b. Pentru a-și umple tabela CAM înainte de a începe să transmită
 - c. Pentru a negocia viteza portului
 - d. Pentru a alege VLAN-ul nativ
8. O singură copie de fișier între două servere, peste un EtherChannel de 4 Gbps. Ce debit maxim obține?
- a. 4 Gbps
 - b. 2 Gbps
 - c. 1 Gbps, pentru că distribuirea se face per flux
 - d. Depinde de VLAN

Note bibliografice

Am segmentat rețeaua locală și am făcut-o rezistentă la defecte. Ce nu am rezolvat este comunicația între rețele diferite, la scară globală - iar pentru asta adresele MAC, plate și locale, nu sunt de niciun folos. Cursul următor introduce adresarea ierarhică și nivelul 3.

La **laboratorul 3** configurați exact VLAN-urile, trunk-ul și router-on-a-stick de aici, apoi provocați o buclă și cronometrați cât durează convergența STP.

- IEEE 802.1Q - VLAN-uri și etichetarea cadrelor
- IEEE 802.1D și 802.1w - Spanning Tree și varianta rapidă
- IEEE 802.1s - Multiple Spanning Tree
- IEEE 802.1AX - agregarea legăturilor
- Cisco - ghidurile de configurare pentru VLAN, STP și EtherChannel din documentația Catalyst

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