

Capitolul 1: LAN Design

Obiective

- Importanța rețelelor locale
- Componentele unui LAN
- Modele de design a unui LAN

Elementele unui LAN

- Echipamente
 - switch
 - layer 2 cu sau fără management
 - layer 3 / multilayer – cu management
 - wireless access point
 - end devices
 - PC, laptop, server, imprimantă în rețea, IP Phone
- Protocole
 - Ethernet/FastEthernet/Gigabit Ethernet/10 Gigabit Ethernet
 - 802.11a, 802.11b/g, 802.11n
 - STP, VTP, DTP, 802.1q, 802.3a/f

3

La nivelul unui LAN întâlnim o serie de echipamente ce rulează la diferite niveluri ale stivei OSI precum: switch-uri de Layer 2 și 3, wireless access point-uri, și end device-uri.

Din punct de vedere al protocolelor ce rulează în cadrul unui LAN amintim următoarele: Ethernet, FastEthernet, Gigabit Ethernet, protocole de transmisie a datelor folosind unde radio, precum 802.11a, 802.11b/g și 802.11n. Cel din urmă este singurul standard wireless ce folosește ambele frecvențe 2.4 și 5Ghz, având o lățime de bandă de până la 300Mbps.

Despre STP, VTP, DTP și 802.1q vom vorbi mai pe larg în cursurile următoare.

Ethernet Switch

- **Cisco Catalyst**

- Densitate de porturi Ethernet
 - nu există porturi seriale pe switch-uri
- Tipuri:
 - configurație fixă (2960, 3560)
 - modulare (6500, 4000)
 - stackable (3750)
 - tehnologia **StackWise** (Cisco)



4

Echipamentele de switching produse de Cisco fac parte din seria Cisco Catalyst și sunt disponibile în 3 variante :

Switch-uri cu configurație fixă având un număr limitat de porturi și facilități ce nu pot fi schimbată.

Switch-uri modulare ce permit adăugarea de module ce pot crește numărul de porturi disponibile. Switch-urile sunt produse cu dimensiuni de șasiu diferite ce permit adăugarea unui număr diferit de module.

Switch-uri „stackable” ce folosesc tehnologia StackWise ce permite interconectarea mai multor switch-uri având un comportament unitar. Echipamentele se leagă folosind un cablu de „backplane” special, ce oferă o lățime de bandă mărită.

Evoluție LAN

- Nevoile noi au dus la tehnologii noi.
- Nevoi noi
 - Mobilitate
 - Prioritizare trafic
 - Securitate
 - Voce și video
- Soluții tehnologice
 - Wireless
 - Quality of Service (QoS)
 - Port Security
 - Voice over IP (VoIP)

5

Odată cu creșterea nevoilor utilizatorilor, tehnologiile la nivel de rețele locale s-au dezvoltat într-un ritm alert. Astfel cerința de mobilitate a fost rezolvată prin dezvoltarea tehnologiilor fără fir.

Nevoia de trafic de voce a fost adresată prin introducerea tehnologiei VoIP și pentru prioritizarea traficului s-au introdus mecanisme de Quality of Service (QoS).

Una din cele mai mari probleme ale rețelelor actuale este securitatea, problemă adresată de Cisco atât prin echipamente dedicate (ASA) cât și prin securitate la nivelul echipamentelor de rețea (port security).

Rețele convergente

- = rețea de **date** + rețea de **voce**
- Concept nou în networking
 - a nu se confunda cu noțiunea din protocoale de rutare de „aceeași viziune a rețelei din partea tuturor echipamentelor”
- Nevoi în rețele convergente:
 - Quality of Service
 - pachetele de voce/video au prioritate mai mare
 - High Availability

6

Convergența este procesul prin care se combină comunicarea video, de voce și de date. Rețele convergente există de ceva vreme, dar, până acum nu au fost fezabile decât pentru companiile mari din cauza infrastructurii complexe și a dificultății de administrare a rețelei.

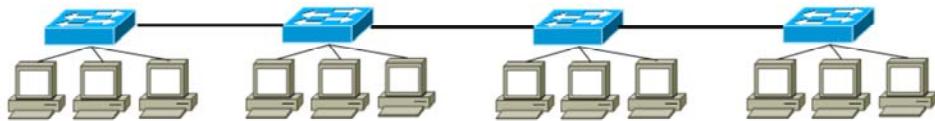
O rețea convergentă are nevoie de o cât mai bună administrare a traficului deoarece traficul de voce și video trebuie să fie clasificat și prioritizat în rețea.

Din cauza traficului intens ce trebuie suportat de un LAN, în rețelele convergente din zilele noastre trebuie asigurată o politică ce garantează High Availability .

Lipsa scalabilității rețelelor locale

- Model plat

-Nescalabil



- **Soluția:** Modelul ierarhic

- The 3 Layer Model

- Access Layer
- Distribution Layer
- Core Layer

7

În ziua de azi, atunci când se creează o rețea locală trebuie luati în calcul numeroși factori ce îi pot influența performanța în viitor.

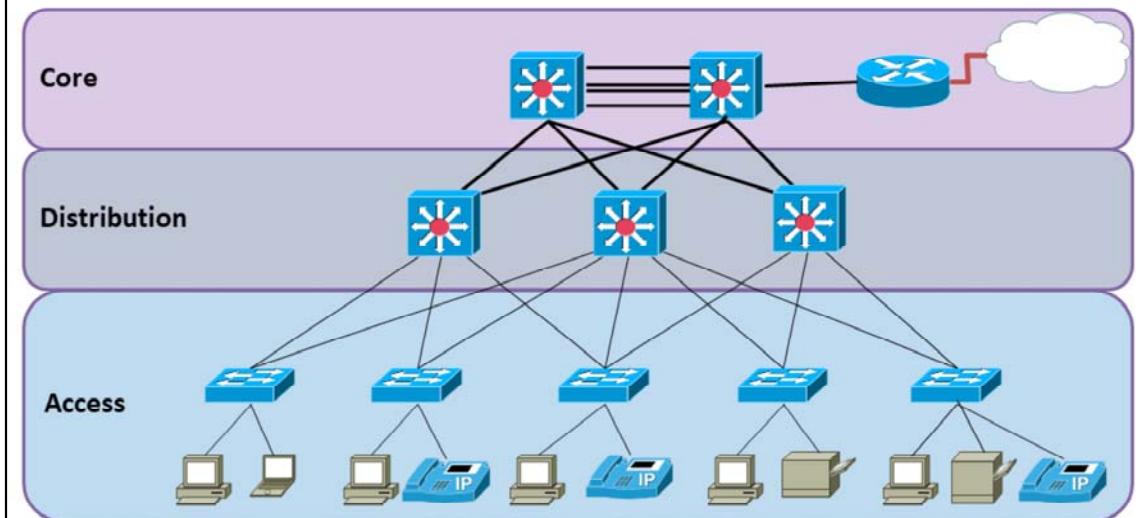
Tinând cont de cerințele actuale trebuie să ne asigurăm că rețeaua noastră îndeplinește următoarele criterii:

- Este scalabilă
- Poate oferi redundanță
- Este ușor de administrat
- Prezintă un nivel de securitate sporit
- Oferă un nivel maxim de performanță.

Din această cauză a fost introdus modelul ierarhic.

The 3 Layer Hierarchical Model

The 3 Layer Model



9

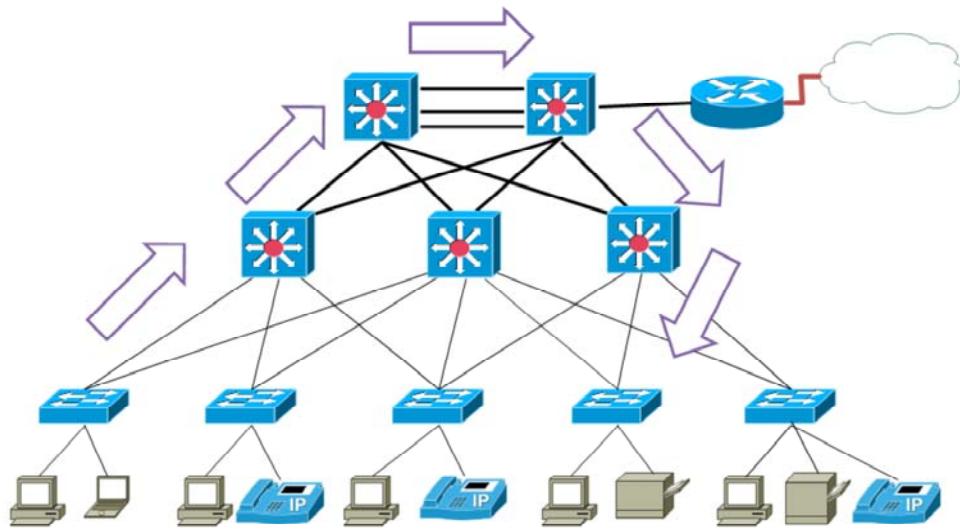
Modelul ierarhic presupune împărțirea rețelei în 3 niveluri:

Nivelul Access este interfața cu echipamentele terminale cum ar fi PC-uri, imprimante și telefoane IP. Acest nivel poate conține rutere, switch-uri, bridge-uri, hub-uri și access point-uri. Rolul principal al nivelului Access este acela de a facilita conectarea unui echipament la rețeaua locală și de a controla echipamentele ce au acces la aceasta.

Nivelul Distribution centralizează datele primite de la switch-urile de nivel Access înainte de a fi trimise la nivelul Core, pentru a fi rutate către destinația finală.

Nivelul Core reprezintă nivelul de bază, denumit și backbone, a cărui funcție principală este transmiterea informațiilor în mare viteză către destinația finală.

Network Diameter



10

În momentul în care se realizează o topologie de rețea folosind modelul ierarhic, un factor foarte important devine diametrul rețelei.

În general, diametrul reprezintă o modalitate de a măsura distanța, însă, în acest caz, termenul este folosit pentru a reprezenta numărul maxim de echipamente pe care un pachet trebuie să le străbată în drum către destinație.

Într-o rețea locală trebuie păstrat un diametru al rețelei cât mai mic pentru a asigura o latență minimă între echipamente.

Avantajele unui model ierarhic ⁽¹⁾

- Scalabilitate
- Redundanță
- Performanță



11

Rețelele ce folosesc modelul ierarhic scalează foarte bine. Modularitatea design-ului permite adăugarea de noi echipamente odată ce rețeaua se extinde. Deoarece fiecare nivel este consistent, extinderea este ușor de planificat și implementat.

Odată cu creșterea rețelei, accesibilitatea devine din ce în ce mai importantă. Se poate crește dramatic accesibilitatea folosind implementări ce oferă redundantă în rețelele create după modelul ierarhic. Switch-urile de la nivelul Access sunt conectate la cel puțin 2 switch-uri de la nivelul Distribution pentru a asigura redundantă. În cazul în care unul din cele 2 switch-uri pică, traficul va fi suportat de un alt switch de la nivelul Distribution.

Performanța comunicării este asigurată prin evitarea link-urilor pe care datele comunică la viteză suboptimală.

Avantajele unui model ierarhic (2)

- Securitate
- Ușurință de administrare
- Ușurință de întreținere și reparare



12

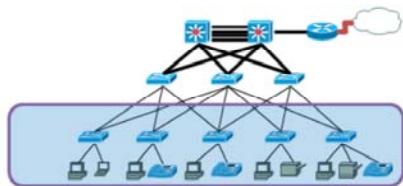
Switch-urile de nivel Access pot fi configurate cu diferite opțiuni de port security ce oferă control asupra echipamentelor ce urmează a fi conectate la rețea. De asemenea, modelul ierarhic oferă flexibilitatea de a folosi politici de securitate mai avansate la nivelul Distribution. Astfel, la acest nivel se pot restrictiona protocoale folosite, precum IP sau HTTP.

Modelul ierarhic oferă consistență pentru toate switch-urile de la același nivel făcând astfel administrarea lor mult mai simplă. Adăugarea de noi switch-uri este de asemenea simplificată deoarece configurațiile pot fi replicate pe un alt switch de același nivel cu foarte puține modificări.

Un alt avantaj al modelului ierarhic este acela că oferă consistență între switch-urile ce operează la același nivel, și astfel permite troubleshooting-ul rapid și simplificat al oricărei probleme apărute.

Access Layer

- Conectare end-devices la rețea
 - PC, Laptop, IP Phone
- Switch-uri L2 și AP-uri
- **VLAN-uri**
- Security
 - port security
- QoS
 - marcarea tipului de trafic
- **Power over Ethernet (802.3a/f)**



13

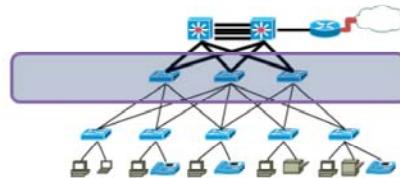
Nivelul Access facilitează conectarea echipamentelor terminale la rețea. Din această cauză switch-urile de la nivelul Access trebuie să ofere facilități cum ar fi port security, VLAN-uri, Power over Ethernet (PoE) și agregare de link-uri.

Viteza la nivelul portului este o altă caracteristică ce trebuie luată în considerare pentru switch-urile de la nivelul Access. În funcție de performanțele cerute administratorul trebuie să decidă între porturi FastEthernet și Gigabit Ethernet.

Power over Ethernet este o altă funcționalitate necesară la nivel Access, care permite alimentarea echipamentului prin același cablu care realizează conectarea la rețea. În cazul switch-urilor Cisco, această funcționalitate crește dramatic prețul echipamentului.

Distribution Layer

- Controlează traficul între Access și Core
- Switch-uri L2 și L3
- **Inter-VLAN Routing**
 - layer 3 switching
- Redundanță
 - pentru legăturile spre access și spre core
- Politici de securitate
 - Inter VLAN
- QoS
 - păstrarea calității pe drum



14

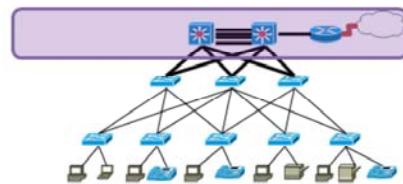
Switch-urile de la nivelul Distribution au rolul de a colecta datele de la nivelul Access și de a trimite traficul mai departe către nivelul core. La nivelul Distribution sunt necesare switch-uri de nivel 3 deoarece acest nivel trebuie să asigure rutare inter-VLAN cât și să suporte politici avansate de securitate ce vor fi aplicate traficului de nivel rețea.

O altă cerință a unui switch de nivel Distribution este aceea de a oferi suport QoS pentru a menține prioritizarea traficului ce vine de la nivelul Access.

Este foarte important ca switch-urile de nivel Distribution să suporte redundanță pentru a oferi accesibilitate adecvată.

Core Layer

- Do one thing and do it well: packet switching
 - fără politici de securitate
- Switch-uri puternice L3 și routere
- Uplink către WAN/Internet
- Redundanță și High Availability
- Agregare legături (**EtherChannel**)



15

Nivelul Core al modelului ierarhic reprezintă backbone-ul de mare viteză al rețelei și necesită switch-uri ce oferă viteze de forwarding foarte mari. Switch-urile de la acest nivel trebuie să suporte agregare de link-uri (de până la 10 Gb) pentru a putea asigura o lățime de bandă adecvată pentru traficul ce vine de la nivelul Distribution.

Accesibilitatea nivelului Core este de asemenea critică, motiv pentru care trebuie implementată redundanță. O altă funcționalitate foarte importantă a acestui nivel este Quality of Service.

Capitolul 2: Concepte introductive de switching

Generații de Ethernet

		Bandwidth	CSMA/CD	Duplex	Tip cablu
Ethernet	~1980	10Mb/s	Da	Half/Full	Coaxial, torsadat, fibră
Fast Ethernet	1995	100Mb/s	Da	Half/Full	Torsadat, fibră
Gigabit Ethernet	1999	1Gb/s	Da	Half/Full	Torsadat, fibră
10 Gigabit Ethernet	2002	10Gb/s	Nu	Full	Torsadat, fibră
40/100 Gigabit Ethernet	2010	40/100Gb/s	Nu	Full	Torsadat, fibră

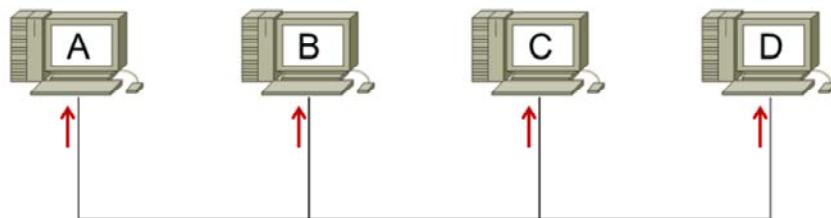
17

Ethernet-ul a fost proiectat în anii 1970 la centrul de cercetare PARC® (Palo Alto Research Center), la momentul respectiv divizia a companiei XEROX®, folosind ca sursă de inspirație sistemul ALOHAnet al universității din Hawaii. Promovarea acestuia ca standard a început în 1979, când DEC® (Digital Equipment Corporation), Intel® și XEROX® au colaborat în acest sens. Primul standard, numit "DIX" (de la Digital/Intel/Xerox) a fost publicat în 1980. Aceasta specifica o viteză de 10 Mb/s și adrese sursă și destinație pe 48 de biți. Standardul oficial de Ethernet (IEEE 802.3) a fost lansat în 1983.

De atunci, dezvoltarea și îmbunătățirea acestui standard au continuat, urmărind obținerea de viteze din ce în ce mai mari și a unei eficiențe cât mai ridicate a transmisiei datelor, ultima versiune specificând viteze de 40 și 100 Gb/s.

CSMA/CD

- Carrier Sense



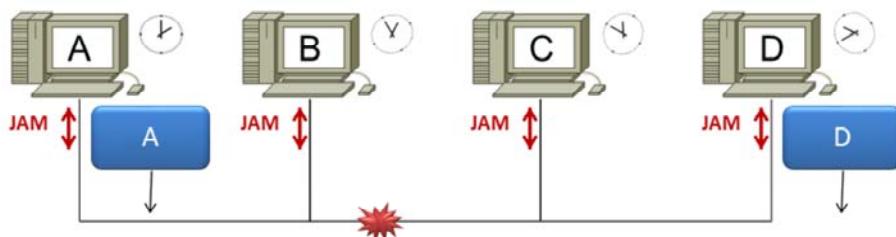
18

CSMA/CD este un protocol de control a accesului la mediul de comunicație, implementat la nivelul Access la rețea (stiva TCP/IP) / în subnivelul MAC al nivelului Legătură de date (stiva OSI), care ajută la împărțirea largimii de bandă între echipamente, reducând probabilitea ca două dintre acestea să transmită simultan și este folosit doar în cazul comunicațiilor half-duplex. Această variantă a protocolului nu garantează eliminarea totală a coliziunilor.

Carrier Sense: Toate echipamentele care doresc să transmită trebuie mai întâi să verifice dacă mediul este liber. Dacă nu este detectat nici un semnal, rezultă că nici un alt echipament nu comunică în acel moment și pot începe să transmită. Altfel, se va aștepta o anumită perioadă, după care se va relua acest proces. După finalizarea transmisiei se va reveni la starea de verificare a mediului. Această "ascultare" are loc și în timpul transmisiei pentru a detecta eventualele semnale simultane de la alte stații (coliziuni).

CSMA/CD

- **Multiple Access**
- **Collision Detection**
 - jam signal
 - random backoff



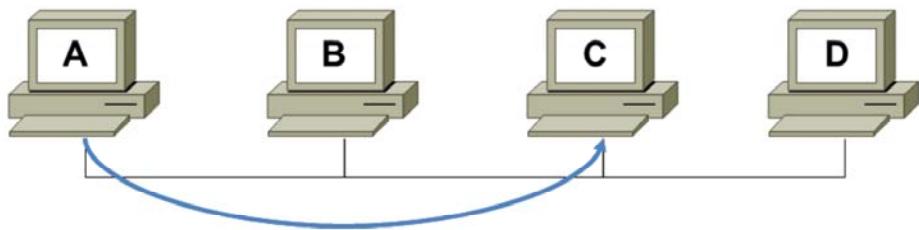
19

Multiple Access: Mai multe echipamente comunică peste același mediu.

Collision Detection: Coliziunile sunt detectate datorită creșterii amplitudinii semnalului la producerea lor, moment în care echipamentele implicate în coliziune (care transmiteau) emit un semnal de bruiaj (Jam Signal). Astfel, toate echipamentele conectate la mediu sunt informate de producerea unei coliziuni și pornesc un algoritm de backoff. Acesta presupune oprirea transmisiei pentru o durată aleatoare (Random Backoff), care va fi mai lungă pentru echipamentele care au produs coliziunea. După expirarea acestei perioade, fiecare echipament revine în starea de "ascultare a mediului".

Comunicația Unicast

- Un singur receptor



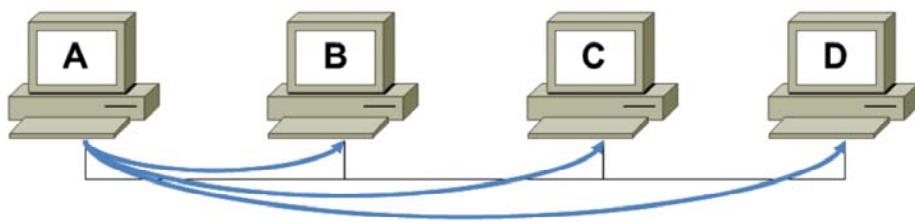
20

Comunicația la nivelul 2 (stiva OSI) / 1 (stiva TCP/IP) poate avea loc în 3 moduri diferite: unicast, broadcast și multicast.

În cazul comunicației unicast, cadrul este trimis de un host unui destinatar unic. Altfel spus, la schimbul de informații participă un singur emițător și un singur receptor. Acest mod de transmisie este cel predominant în rețelele locale și în Internet. Printre protoalele care folosesc acest tip de comunicație amintim: HTTP, FTP, SMTP, Telnet.

Comunicația Broadcast

- Cadru trimis tuturor adreselor
- Adresă MAC destinație - FF:FF:FF:FF:FF:FF

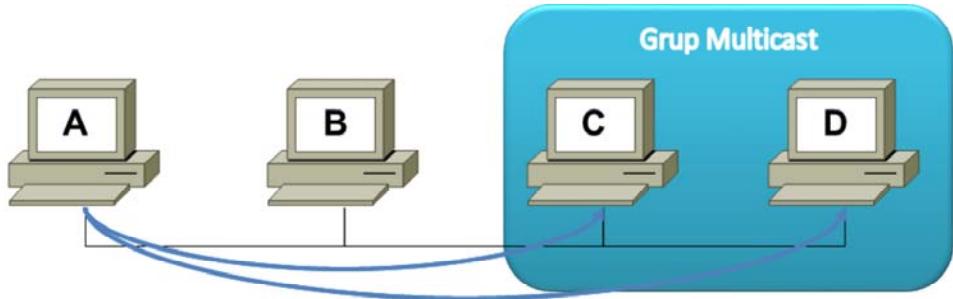


21

În cazul comunicației broadcast, cadrul transmis de un host este destinat tuturor celorlalte host-uri care aparțin domeniului de broadcast al emițătorului. Orice echipament care primește un broadcast pe una dintre interfețele sale este obligat să-l proceseze. Această formă de comunicație este necesară în situațiile în care se dorește trimiterea același mesaj tuturor dispozitivelor din aceeași rețea (exemplu: mesajul de query al protocolului ARP).

Comunicația Multicast

- Cadru trimis unui grup specific
- Adresă MAC destinație – paritatea primului octet este impară



22

În comunicația de tip multicast, destinația cadrului este o grupare specifică de echipamente (clienti). Singura formă de multicast este one-to-many: o singură stație trimite cadre către un grup de stații. Cadrele au întotdeauna în câmpul Adresă sursă o adresă unicast. Adresa de multicast nu poate să apară decât în câmpul Adresă destinație. Clientii unei transmisii multicast trebuie să fie membrii unui grup logic de multicast (multicast group) pentru a primi cadrele. Exemple de fluxuri de date multicast pot fi transmisiile video și / sau audio asociate aplicațiilor de comunicare și colaborare.

Cadrul Ethernet (1)

- Dimensiune cuprinsă (în general) între 64 și 1518 octeți

7	1	6	6	2	46 - 1500	4
Preambul	Delimitator început de cadru	Adresă Destinație	Adresă Sursă	Lungime/ Tip	Antet 802.2 și Date	FCS

23

Înainte de a explica rolul fiecărui câmp al cadrului Ethernet, vă reamintim faptul că acesta este rezultatul încapsulării PDU-ului de nivel 3 (stiva OSI), prin adăugarea unui header și a unui trailer.

Preambul: Acești 7 octeți conțin un sir alternativ de "0" și "1", cu rolul de a permite receptorului să detecteze apariția unui nou cadru pe mediu.

Delimitator început de cadru: Are valoarea "10101011", trecerea de la "10" la "11" semnalizând terminarea părții de sincronizare și începutul cadrului propriu-zis.

În concluzie, acești primi 8 octeți sunt folosiți pentru sincronizarea receptorului cu emițătorul.

Adresă Destinație: Adresa MAC a interfeței destinație.

Adresă Sursă: Adresa MAC a interfeței sursă.

Cadrul Ethernet (2)

- Dimensiune cuprinsă (în general) între 64 și 1518 octeți

7	1	6	6	2	46 - 1500	4
Preambul	Delimitator început de cadru	Adresă Destinație	Adresă Sursă	Lungime/ Tip	Antet 802.2 și Date	FCS

24

Lungime / Tip: Definește dimensiunea câmpului de date, fie prin specificarea lungimii efective a acestuia (valori mai mici decât 1536), fie prin specificarea protocolului de nivel superior încapsulat (valori mai mari sau egale ca 1536). Este utilizat și la verificarea integrității cadrului primit.

Antet 802.2 și Date: Conțin PDU-ul de nivel superior. Lungimea minimă a unui cadrus este de 64 octeți (ajută la detecția coliziunilor); dacă aceasta nu este atinsă, este folosit câmpul "Pad" pentru mărirea dimensiunii până la limita minimă.

FCS: Câmp folosit la detecția erorilor prin utilizarea tehnicii de CRC (cyclic redundancy check). Conține CRC-ul calculat de emițător, care, dacă nu coincide cu CRC-ul calculat de destinatar la primirea cadrului, duce la aruncarea acestuia.

Adresa MAC

- Adresă de tip BIA (Burned-in Address)
- Bitul **0** din primul octet -> Broadcast/Multicast
- Bitul **1** din primul octet -> Adresă administrată local



25

Adresa MAC este înscrisă definitiv ("arsă") în chip-ul ROM al interfeței de rețea, este reprezentată pe 48 de biți folosind 12 "cifre" hexazecimale și este compusă din 2 părți:

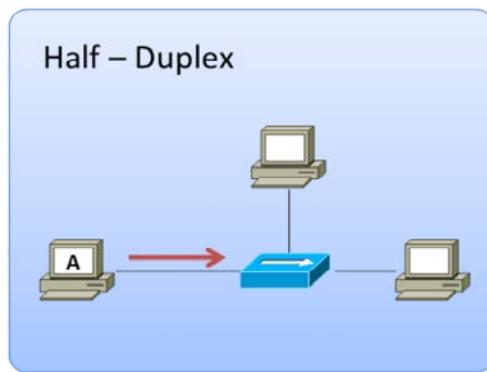
OUI Identifică, folosind 24 de biți, producătorul interfeței de rețea. Alocarea de OUI-uri este reglementată și gestionată de IEEE. Suplimentar, cei mai puțin semnificativi doi biți ai primului octet din cadrul adresei destinație determină urmatoarele:

Bitul (0): Dacă este setat, cadrul este destinat fie unui grup de multicast, fie broadcast.

Bitul (1): Dacă este setat, numărul atribuit de producător din adresa MAC a echipamentului sursă este administrat local.

Număr atribuit de producător: Identifică în mod unic interfața de rețea folosind cei 24 de biți rămași. Poate fi cea înscrisă din fabrică sau modificată prin software.

Half – Duplex



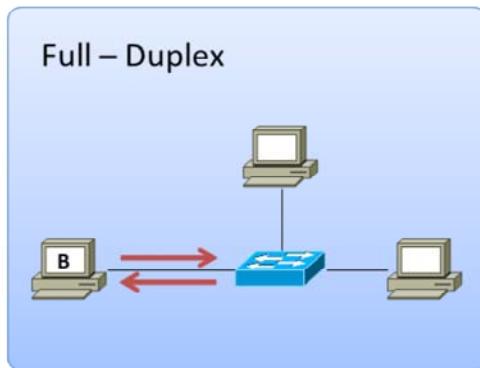
- Interfața poate să fie configurată în modurile **full**, **half** sau **auto**

26

După modul în care are loc propriu-zis comunicația din punctul de vedere al secvențierii fluxurilor de date, o putem clasifica în:

Half-Duplex: Cele două fluxuri de date (emițător → receptor și invers) nu au loc simultan, în caz contrar producându-se o coliziune. Pentru a diminua probabilitatea apariției coliziunilor și pentru a le detecta în momentele în care apar, comunicația de tip half-duplex implementează mecanismul CSMA/CD. Din păcate însă, timpii de așteptare introduse de acest mecanism duc la scăderea eficienței, motiv pentru care conexiunile half-duplex sunt întâlnite doar la echipamentele vechi, ca de exemplu hub-urile (nodurile conectate la un hub au funcționarea impusă în acest mod), switch-urile, interfețele de rețea. Din cauza acestor limitări, comunicația half-duplex a fost înlocuită cu cea full-duplex.

Full – Duplex



- Interfața poate să fie configurată în modurile **full**, **half** sau **auto**

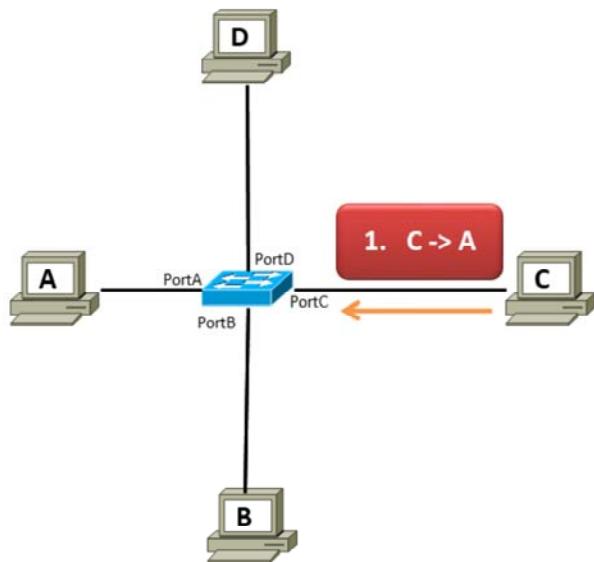
27

Full-Duplex: Cele două fluxuri de date (emisator → receptor și invers) au loc simultan, astfel încât se pot trimite și primi date în același timp. Deoarece există suport dedicat pentru traficul bidirecțional concomitent, este eliminată complet problema coliziunilor și nu mai este necesară folosirea mecanismului CSMA/CD, iar timpii de aşteptare între transmisii sunt micșorați, îmbunătățind eficiența.

Comparativ, o configurație half-duplex oferă o eficiență de 50 – 60 % din lărgimea de bandă disponibilă, în timp ce o configurație full-duplex oferă eficiență 100 % în ambele sensuri.

Pentru a putea funcționa în unul dintre cele două moduri, atât emisatorul cât și receptorul trebuie să fie configurate în mod identic (half- sau full-duplex). În cazul în care sunt configurate în modul auto, cele două interfețe vor "negocia" modul de funcționare.

Tabela MAC (1)



28

Switch-urile direcționează traficul primit pe un port de la nodul sursă către portul aferent nodului destinație folosind adresele MAC. Pentru a determina însă portul de ieșire corect, switch-ul trebuie să cunoască ce noduri se află "în spatele" fiecărui port în parte. Excepția o reprezintă traficul broadcast, care va fi replicat automat pe toate porturile în afara celor de pe care a venit.

Asocierile port – adresă MAC destinație sunt stocate de un switch în tabela MAC, pe măsură ce sunt determinate. Unui singur port îi pot fi asociate multiple adrese MAC, în cazul în care printr-un singur port se poate ajunge la mai multe noduri (exemplu: switch-uri interconectate).

Când un switch primește un cadru cu adresa MAC a destinatarului necunoscută (nu se află în tabela MAC), acesta este transmis pe toate porturile, cu excepția celui pe care a primit cadrul, și se reține în tabelă adresa MAC a nodului sursă (în cazul în care nu există deja).

Tabela MAC (2)

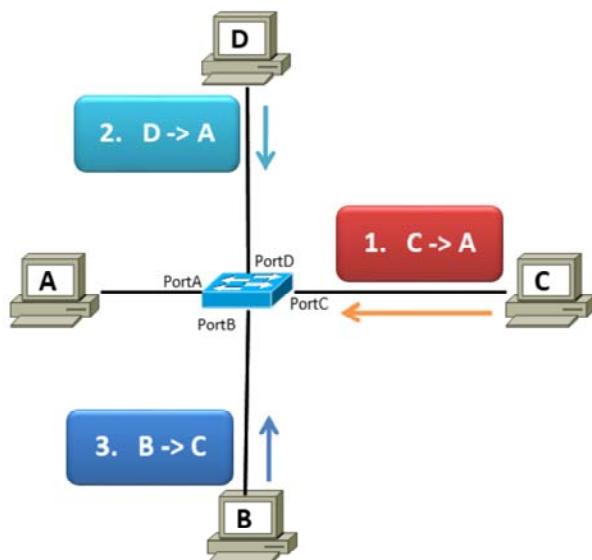


Tabela MAC
PortC: C
PortD: D
PortB: B

Tip operații
Broadcast
Broadcast
Unicast

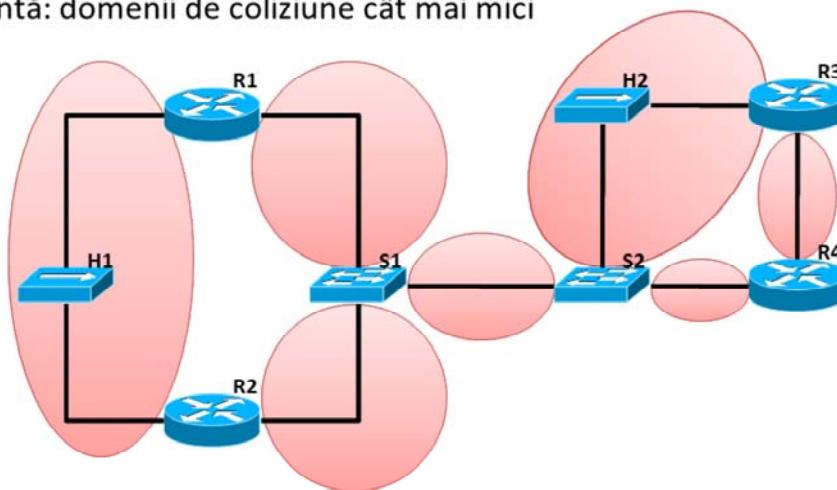
29

În momentul în care nodul destinație din prima fază răspunde sursei inițiale, adresa acestuia este introdusă în tabelă.

În momentul în care un switch-ul din figură primește de la nodul C un cadru cu destinația A (a cărei adresă MAC nu se află în tabelă), acesta este transmis pe toate celelalte porturi (broadcast, etapa 1 din figură), iar adresa MAC a nodului C este asociată portului C. Când nodul A va răspunde, switch-ul va introduce adresa MAC a acestuia în tabelă și o va asocia portului A. Presupunând totuși că nodul A nu a răspuns încă dinainte ca nodul D să trimită cadre cu destinația A, switch-ul va recurge din nou la broadcast la primirea acestora (etapa 2 din figură) (în cazul în care adresa MAC a nodului A ar fi fost deja asociată portului A, și s-ar fi transmis unicast). La primirea unui cadru de la nodul B cu destinația C, switch-ul va transmite unicat pe portul aferent deoarece adresa MAC C se află în tabela MAC (etapa 3 din figură).

Domenii de Coliziune

- Switch-urile delimită domeniile de coliziune
- Tintă: domenii de coliziune cât mai mici



30

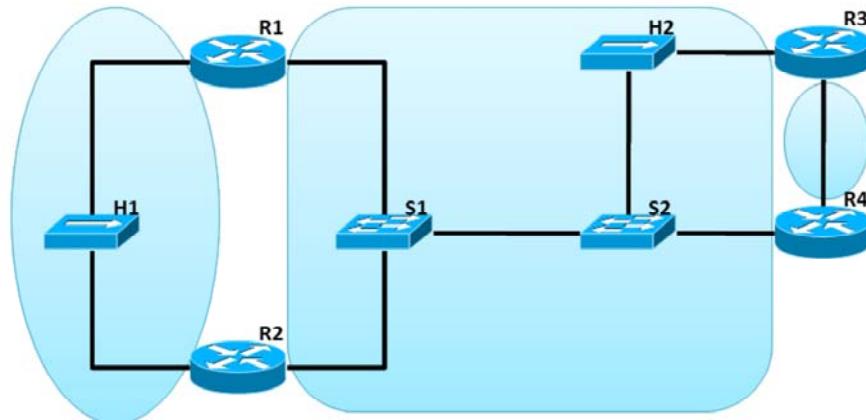
Un domeniu de coliziune este un segment al unei rețele în care pot avea loc coliziuni între cadrele transmise pe un mediu partajat (half – duplex, de exemplu cel creat de un hub). Altfel spus, este o zonă din rețea de unde provin cadre care pot produce coliziuni.

Toate nodurile conectate la un hub aparțin aceluiași domeniu de coliziune, deoarece toate împart același mediu de comunicație. În schimb, când un nod este conectat la un switch, acesta din urmă creează o conexiune dedicată pentru a separa traficul asociat nodului de restul traficului, iar domeniul de coliziune este limitat la acesta. Astfel, porturile unui switch aparțin unor domenii de coliziune distințe.

Proiectarea corectă a unei rețele presupune, printre altele, micșorarea domeniilor de coliziune, mărind astfel eficiența și procentajul lărgimii de bandă neutilizate.

Domenii de Broadcast

- Switch-urile nu delimită domeniile de broadcast
- Întă: domenii de broadcast cât mai mici



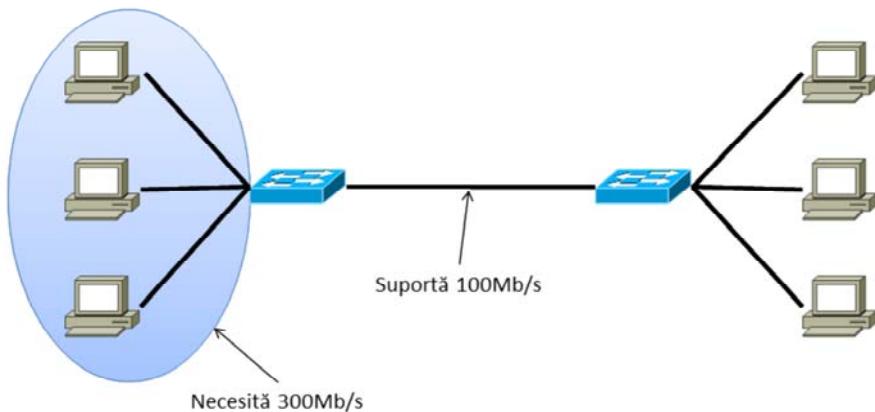
31

Domeniul de broadcast reprezintă partea unei rețele în care dacă un nod transmite un cadru broadcast, toate celalalte noduri îl vor primi. De exemplu, toate nodurile conectate la un switch aparțin aceluiași domeniu de broadcast și, evident, nodurile conectate folosind două sau mai multe switch-uri în cascadă vor apartine aceluiași domeniu de broadcast.

Broadcast-urile la nivel 2 (stiva OSI) pot fi filtrate doar de un echipament de layer 3 (exemplu: ruter) sau folosind VLAN-uri. Utilizarea VLAN-urilor este explicată în capitolul următor.

Congestii

- Fiecare dispozitiv din cale introduce latență



32

Latență este definită ca timpul necesar unui cadru sau unui pachet să ajungă de la sursă la destinația finală și este cauzată din cel puțin 3 motive:

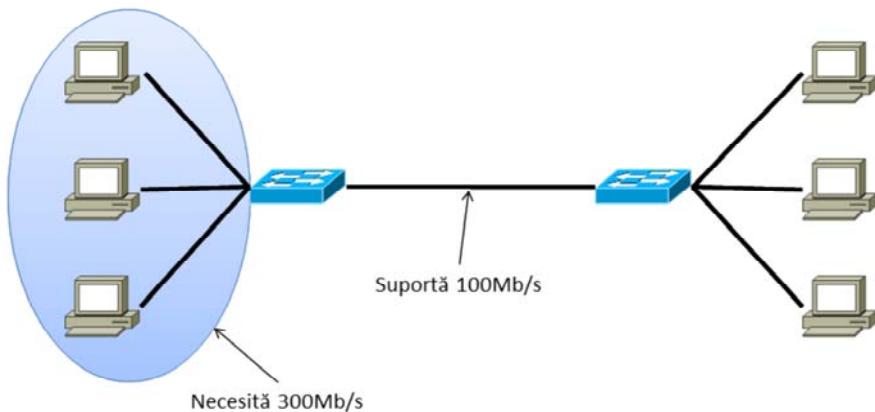
Timpul necesar interfeței de rețea a sursei să emită ("plaseze") pulsurile pe mediu și cel necesar interfeței de la destinație să le interpreteze.

Durata necesară semnalului electric să parcurgă efectiv secțiunile de cablul folosite la interconectare.

Timpul necesar "traversării" echipamentelor de rețea intermediare. De exemplu, timpul necesar unui switch (operații la nivelul 2 OSI) este mai mic decât cel necesar unui ruter (operații la nivelurile 2 și 3 OSI).

Congestii

- Rețeaua trebuie să evite apariția bottleneck-urilor



33

Congestiile apar în momentele în care lărgimea de bandă a unui mediu este mai mică decât cantitatea de date care ar trebui să traverseze mediul în unitatea de timp considerată. Cele mai des întâlnite motive ale congestiilor sunt:

- Echipamentele moderne (PC-uri, periferice, etc.) pot să proceseze și să trimită date la viteze mult mai mari decât în trecut.
- Cresterea volumului de trafic efectuat în mod ușual, depășind volumul pentru care a fost proiectat segmentul de rețea.
- Traficul de tip broadcast (de exemplu cereri ARP, DHCP, etc.) și / sau domenii de broadcast extinse.

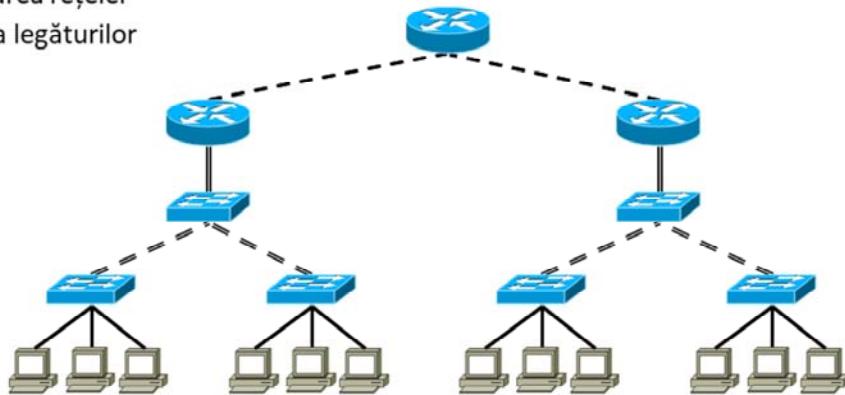
Congestiile apar și în cazul unor topologii asimetrice, în care un server este conectat pe unul dintre porturile unui switch, restul porturilor oferind conectivitate pentru 20 de clienți care trimit date la capacitatea maximă a conexiunii. În cazul în care porturile switchului sunt de viteză egală se ajunge la o congestie a legăturii pentru server. Aceasta este o congestie la nivelul rețelei. Al doilea tip de congestie apare în cazul unui volum mare de trafic. Capacitatea de comutare ușuală a unui switch Ethernet dintr-o rețea locală este în jur de 150.000 de

cadre pe secundă. În cazul depășirii limitei de comutare internă va apărea o congestie la nivelul echipamentului de rețea.

Latență și Congestii

- Soluții:

- design ierarhic
- segmentarea rețelei
- agregarea legăturilor



34

Pentru a evita creșterea latențelor și producerea congestiilor, într-un LAN se recomandă luarea următoarelor măsuri:

Folosirea unui design ierarhic la proiectarea rețelei. Modelul clasic de ierarhizare conține 3 niveluri: "core", "distribution" și "access".

Segmentarea rețelei în domenii de coliziune și de broadcast multiple și reduse ca dimensiune, prin folosirea de rutere și switch-uri. În rețelele moderne nu se mai folosesc bridge-uri și hub-uri.

Dimensionarea corectă a echipamentelor intermediare, atât din punctul de vedere al vitezelor porturilor, cât și din cel al circuitelor interne. De exemplu, un switch folosit în partea de "core" cu 24 de porturi Gigabit full-duplex trebuie să conțină circuite interne ("switch fabric") care să ofere o lățime de bandă de aproximativ 48 Gb/s.

Înlocuirea interfețelor de rețea cu unele care suportă viteze mai mari și / sau agregarea de legături. Agregarea de legături reprezintă utilizarea mai multor legături fizice între două switch-uri ca o singură legătură logică în scopul de a oferi mai multă lățime de bandă și redundanță.

Metode de forwarding

35

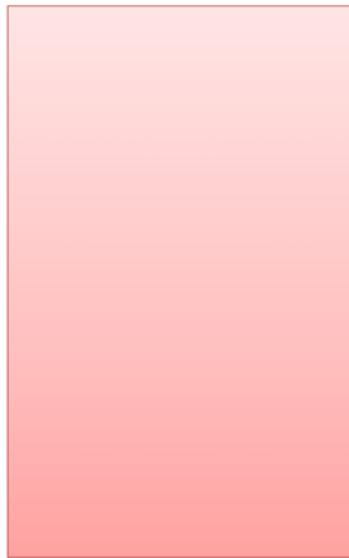
Switch-urile pot funcționa în moduri diferite, fiecare mod având avantaje și dezavantaje față de celelalte.

Principalele două metode folosite la forwarding-ul cadrelor de pe un port pe altul sunt "cut-through" și "store-and-forward" switching.

Mai mult, procesul de switching se poate desfășura fie simetric, fie asimetric, poate avea loc atât la nivelul 2 al stivei OSI, cât și la nivelul 3, iar memoria tampon poate fi ori rezervată pentru fiecare port în parte ori comună pentru toate porturile.

Toate aceste opțiuni trebuie înțelese și avute în vedere la proiectarea, îmbunătățirea sau extinderea unei rețele.

Store-and-Forward Switching

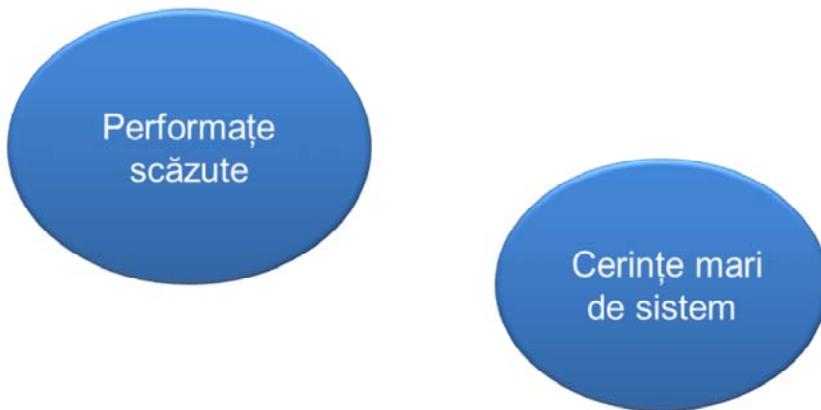


36

Dacă un switch implementează metoda "store-and-forward", atunci secvențierea operațiilor care au loc între primirea și trimiterea unui cadru are loc conform diagramei din imagine:

1. Cadrul venit pe un port este stocat într-un buffer până când este primit în totalitate.
2. Se calculează codul de CRC al cadrului primit și se determină lungimea pachetului, valoare care se compară cu cea trimisă de sursă în antetul Ethernet. Dacă cel puțin una dintre 2 valori nu coincide, pachetul este aruncat.
3. Dacă pachetul nu a fost aruncat, se determină adresa MAC a destinației.
4. Cadrul este trimis pe portul aferent adresei MAC a destinației.

Store-and-Forward Switching - Dezavantaje

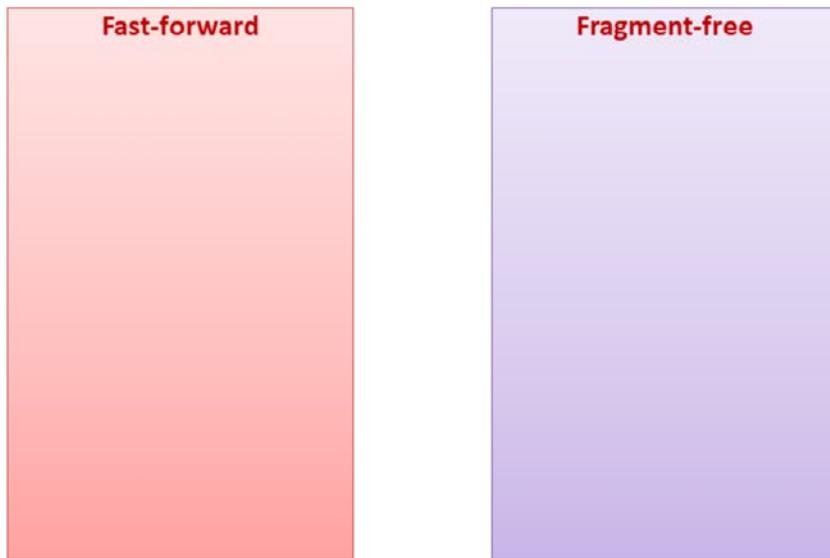


37

Dezavantajele acestei metode sunt legate de performanțe, deoarece switch-ul trebuie să memoreze întregul cadru înainte de a-l verifica și de a-l trimite, rezultând astfel latențe mai mari. În cazul în care există mai multe switch-uri de-a lungul traseului cadrului, cadrul va fi verificat de fiecare dintre ele, iar performanțele rețelei vor scădea. Un alt dezavantaj ar fi faptul că un astfel de switch necesită buffer-e de dimensiuni mai mari și mai multe cicluri CPU pentru a realiza aceste verificări decât unul care implementează metoda "cut-through".

Cu toate acestea, marea majoritate a switch-urilor moderne folosesc această metodă deoarece este necesară implementării tehnicii de QoS, iar evoluția hardware-ului folosit a făcut ca diferența din punct de vedere al latenței introduse să devină nesemnificativă.

Cut-Through Switching



38

În comparație cu metoda "store-and-forward", cea "cut-through" diferă prin următoarele aspecte:

În cazul "fast-forward" cadrul este primit până la adresa destinație, iar apoi este trimis fără a se verifica integritatea sa. Această variantă oferă cea mai mică latență și este cea obișnuită în switching-ul "cut-through".

În cazul "fragment-free" switching se primesc primii 64 de octeți (erorile apar de obicei în acest interval) și se verifică integritatea acestora. Dacă nu se detectează nici o eroare cadrul este trimis spre destinație. Această variantă reprezintă un compromis între switching-ul "store-and-forward" și cel "cut-through fast-forward" din punct de vedere al latențelor introduse și al integrității cadrelor.

Switch-urile care implementează această metodă sunt folosite de obicei pentru aplicații și în sisteme HPC (high performance computing), care necesită latențe inter-proces foarte mici.

Switching simetric/asimetric

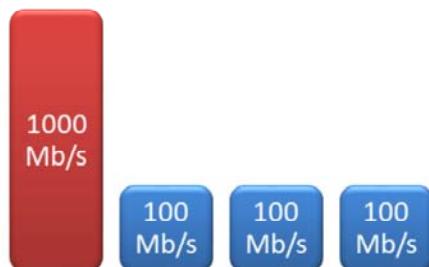
- Simetric:

- toate porturile au același bandwidth



- Asimetric:

- porturile au bandwidth diferit



39

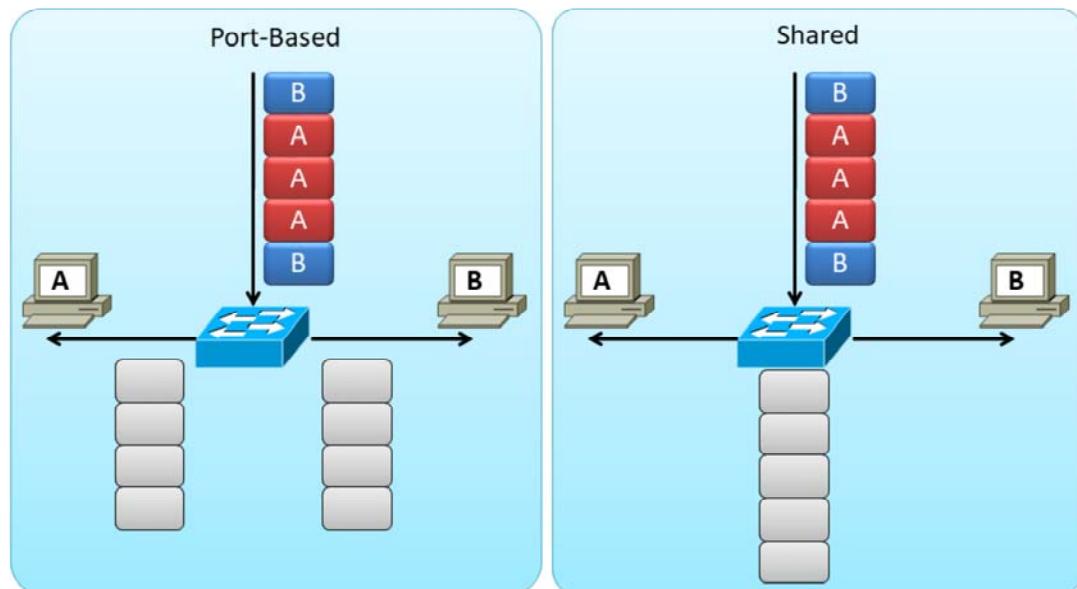
Împărțirea procesului de switching în simetric și asimetric se realizează după modul în care este alocată lărgimea de bandă porturilor:

Simetric: Toate porturile au alocată aceeași lărgime de bandă. Aceste switch-uri sunt optimizate pentru trafic distribuit.

Asimetric: Toate porturile cu excepția unuia au alocată aceeași lărgime de bandă (porturi pentru clienți). Portul rămas are o lărgime de bandă alocată mult mai mare și este dedicat conectării unui server. Aceste switch-uri sunt optimizate pentru scenarii client-server. Pentru a se putea realiza în mod optim transmisia la două viteze diferite, cadrele sunt stocate integral în memoria tampon și transmise pe porturi la momentul potrivit.

Majoritatea switch-urilor moderne sunt asimetrice datorită flexibilității oferite.

Memory Buffering



40

Stocarea cadrelor în memoria tampon are loc fie în timpul procesului de switching (parțial sau total, în funcție de metodă), fie în situația în care portul de ieșire este blocat din cauza unei congestii. Există două moduri în care se realizează această stocare temporară, și anume:

Port-Based: Fiecare port are o coadă de dimensiune fixă asociată. Ca urmare, un cadru aflat în coadă va fi trimis doar după ce toate cadrele de dinaintea sa au fost trimise. Astfel, este posibil ca un cadru să le întârzie pe toate cele care îi urmează (de exemplu, cazul portului ocupat din cauza unei congestii).

Shared: Există o singură zonă de memorie, folosită în comun de toate porturile, cantitatea de memorie alocată fiecărui fiind ajustată dinamic. Cadrele aflate în memorie sunt asociate porturilor de ieșire corespunzătoare. Numărul cadrelor aflate în memorie este limitat doar de dimensiunea acestora și nu are o valoare maximă pentru fiecare port în parte.

Layer 2 vs Layer 3 Switching (1)



Switching nivel 2



Switching nivel 3

41

Un switch de layer 2 va folosi doar informația ce se regăsește la acest nivel în procesul de switching. Astfel, în tabela sa MAC fiecarui port îi vor fi asociate una sau mai multe adrese MAC și nimic mai mult.

În schimb, un switch de layer 3 va analiza atât nivelul 2, cât și nivelul 3 în procesul de switching. Practic, asocierile din tabela MAC vor fi extinse prin adăugarea adresei IP aferente fiecărei adrese MAC și, implicit, fiecărui port.

Vom ilustra această diferență dintre cele 2 tipuri de switch-uri în exemplul următor:

Layer 2 vs Layer 3 Switching (2)



42

Să presupunem că avem host-uri din două rețele diferite (LAN 1, LAN 2) conectate la același switch de layer 2. În momentul în care un host din LAN 1 trimite un broadcast, acesta va fi retransmis de switch pe toate celalalte porturi ale sale, indiferent dacă acestea aparțin rețelei LAN 1 sau LAN 2. În această situație, host-urile din LAN 2 vor primi și procesa inutil broadcast-ul la nivelul 2, urmând să îl arunce în timpul procesării la nivelul 3. Această problemă poate fi rezolvată prin înlocuirea switch-ului cu unul de layer 3, care va ține cont de faptul că broadcast-ul are ca sursă un echipament din LAN 1 și îl va trimite mai departe doar pe celelalte porturi ale sale care aparțin LAN 1.

Suplimentar, față de un switch de layer 2, un switch de layer 3 poate să efectueze și rutare de pachete (la fel de repede precum realizează switching-ul datorită implementării în hardware a acestor funcții).

Layer 3 Switch vs Ruter

	Switch de nivel 3	ruter
Suport pentru WIC		Da
Rutare de nivel 3	Da	Da
Protocolle avansate de rutare		Da
Rutare la viteza interfeței	Da	Da

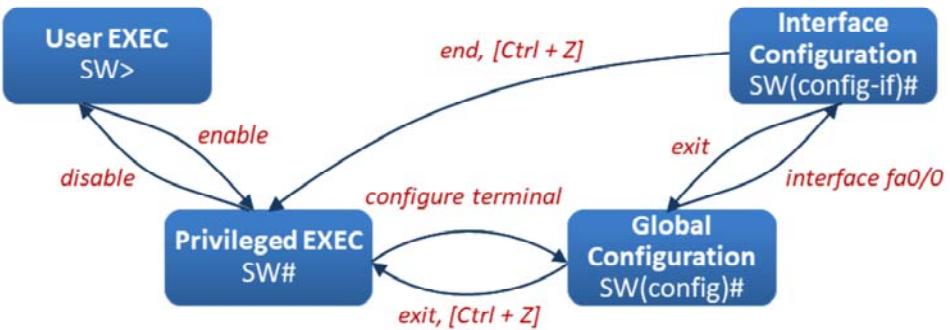
43

Cu toate că un switch de layer 3 este capabil să realizeze și rutarea pachetelor, acesta nu va putea elimina nevoia unui ruter în anumite situații. Enumerăm doar câteva dintre facilitățile oferite de rutere în plus față de majoritatea switch-urilor:

- Un ruter poate rula protocoale complexe de rutare (exemplu: BGP).
- Un ruter oferă suport mult mai flexibil pentru WIC-uri (WAN interface cards).
- Un ruter poate stabili conexiuni pentru remote-access (exemplu: VPN).

Anumite switch-uri pot oferi toate funcționalitățile enunțate mai sus(ex: Catalyst 6500).

Modurile CLI din IOS



44

Reamintim faptul că sistemul de operare Cisco IOS este organizat ierarhic în moduri de operare, fiecare mod având propriul domeniu de operare și fiind folosit în vederea realizării unor operații specifice cu ajutorul comenziilor disponibile în acesta. Modurile principale sunt (în ordine top - down):

- User executive mode
- Privileged executive mode
- Global configuration mode
- Other specific configuration mode (exemplu: Interface configuration mode)

Comenziile folosite pentru a trece dintr-un mod de operare în altul sunt prezentate în imaginea de mai sus.

Căutare ajutor

- Introducerea în CLI a caracterului “?”
- *cisco.com*
- Forumul de ajutor de pe *ccna.ro* din cadrul cursului



45

Sistemul de operare IOS oferă ajutor în două direcții:

Denumirea unei comenzi

În cazul în care se cunosc doar primele caractere dintr-o comandă, acestea pot fi introduse, după care se apasă tasta “?” (fără a se lasă spațiu între caractere și “?”). În acest moment vor fi afișate toate comenzile care încep cu sirul respectiv de caractere și sunt disponibile în modul de operare în care ne aflăm.

Sintaxa unei comenzi

În cazul în care denumirea unei comenzi este cunoscută, însă parametrii necesari completării acesteia sunt necunoscuți, se apelează tot la simbolul “?”. Introducerea acestora are ca efect afișarea tuturor parametrilor care (mai) pot fi folosiți. Dacă este afișat și “<cr>”, atunci nu mai este nevoie de nici un alt parametru pentru a asigura funcționarea comenzi.

Erori IOS

Eroare	Exemplu	Cauză	Soluție
Ambiguous command	SW# a	IOS-ul nu poate determina cu exactitate ce comandă să execute	Compleierea numelui comenzi
Incomplete command	SW# show	Sunt necesari parametri suplimentari pentru execuție	Adăugarea parametrilor lipsă
Invalid input	SW(config-if)# ip address 172.16.10.0 255.255.255.0	IOS-ul nu poate parsea sintactic comanda	Analizarea formatului comenzi

46

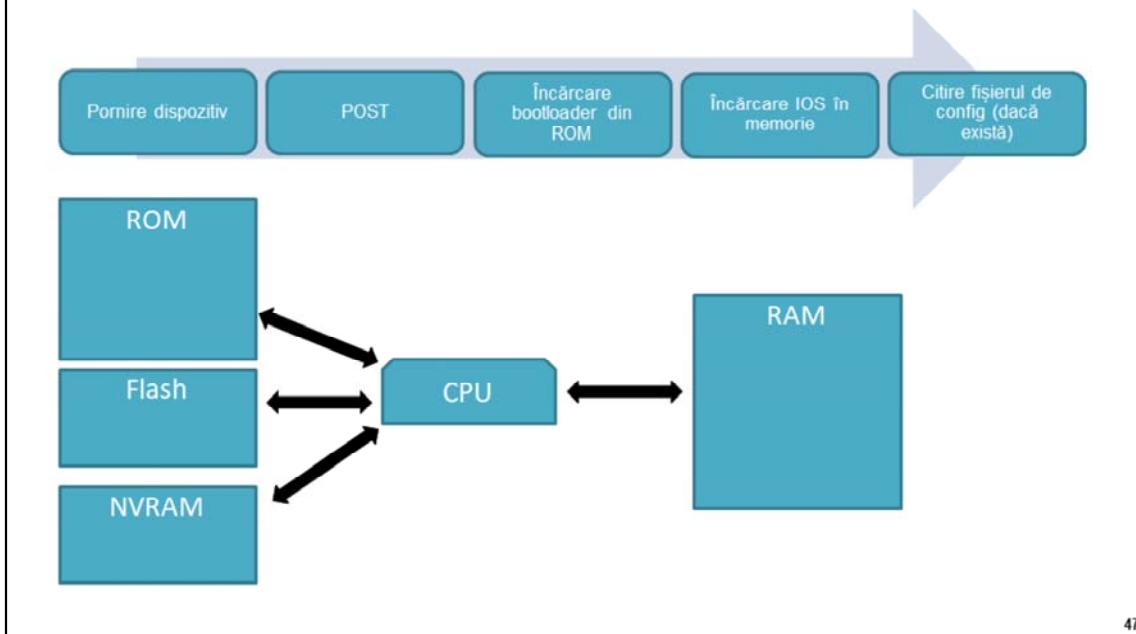
În Cisco IOS întâlnim trei tipuri de erori semnalate de sistemul de operare cu funcții de a ajuta utilizatorul să detecteze comanda dorită.

Astfel, când este semnalată eroarea "Ambiguous command" sistemul de operare nu poate determina cu exactitate care este comanda dorită. Această eroare apare cel mai adesea când comanda este executată sub o formă prescurtată care pentru IOS poate coincide cu mai multe comenzi. Pentru a rezolva această eroare este necesară scrierea numelui comenzi sub formă întreagă.

Eroarea "Incomplete command" apare atunci când o comandă este executată fără toți parametrii necesari. Soluția în acest caz este adăugarea unor parametri suplimentari.

Eroarea "Invalid input" apare atunci când comanda executată este scrisă incorrect și sistemul nu o poate interpreta. Pentru a soluționa această eroare trebuie reanalizat, deobicei din punct de vedere sintactic, formatul comenzi.

Procesul de boot



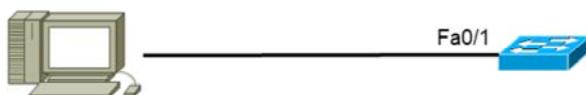
47

Secvența după care se desfășoară procesul de boot este următoarea:

- Se încarcă boot-loader-ul din memoria non-volatile (NVRAM)
 - inițializează CPU-ul la nivel scăzut
 - realizează procedura de POST (Power-On Self Test)
 - inițializează sistemul de fișiere
 - încarcă sistemul de operare IOS în memoria volatilă (RAM)
- Sistemul de operare este căutat mai întâi în flash, iar apoi, dacă nu este găsit, este căutat pe un server tftp, existent în rețea. În cazul în care și a doua încercare eșuează, se va încărca un SO minimal din ROM.
- Sistemul de operare rulează folosind configurația găsită în fișierul "config.txt" din memoria flash, dacă acesta există. Altfel va folosi o configurație "default".

Configurare conectivitate IP (1)

- Este necesară folosirea unei interfețe VLAN



```
Switch# configure terminal
Switch(config)# interface vlan 50
Switch(config-if)# ip address 192.168.10.2
255.255.255.0
Switch(config-if)# no shutdown
```

48

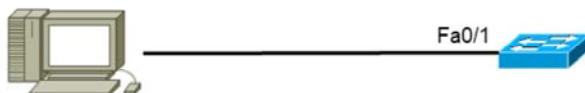
Pentru a administra un switch de la distanță este necesar ca acel switch să aibă asignată o adresă IP. Acest IP este adăugat unei interfețe virtuale numită Virtual LAN (VLAN) și apoi această interfață este asignată unui sau mai multor port-uri ale switch-ului.

În mod implicit switch-ul este administrat prin VLAN-ul 1, dar acesta poate fi schimbat cu orice VLAN dorit.

Pentru a configura o adresă IP și o mască de rețea pe VLAN-ul de administrare al unui switch, trebuie să accesăm modul de configurare al unei interfețe VLAN folosind comanda **interface vlan id_vlan** unde **id_vlan** este numărul VLAN-ului dorit. În acest mod configurăm adresa IP și masca de rețea folosind comanda **ip address adresă mască** și pornim interfața folosind comanda **no shutdown**.

Configurare conectivitate IP (2)

- Este necesară folosirea unei interfețe VLAN



```
Switch(config-if)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 50
Switch(config-if)# end
```

49

În final, trebuie ca VLAN-ul de management nou creat să fie adăugat cel puțin unei interfețe a switch-ului prin care acesta să poată fi administrat. Pentru aceasta, intrăm în modul de configurare al unei interfețe folosind comanda **interface fastethernet/serial număr_identificare_interfață** și adăugăm VLAN-ul folosind comenziile **switchport mode access** și **switchport access vlan id_vlan** unde **id_vlan** este numărul VLAN-ului.

Vom discuta mai multe despre VLAN-uri în capitolul următor.

Configurare default gateway

- Necesară pentru a putea comunica și cu alte rețele



```
Switch# configure terminal  
Switch(config)# ip default-gateway 192.168.10.1  
Switch(config)# end
```

50

Vrem să configurăm switch-ul astfel încât să putem trimite pachete IP și către rețele diferite de cea în care se află. Pentru aceasta folosim default gateway-ul. Switch-ul trimite pachete IP cu adrese destinație ce nu fac parte din rețeaua sa către default gateway.

Pentru a configura un default-gateway pe switch se folosește comanda **ip default gateway adresă** unde adresa reprezintă adresa ip a unui ruter aflat în aceeași rețea cu switch-ul. Ruter-ul va trimite pachetele primite de la switch mai departe către destinație.

Configurare duplex și viteză

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# duplex auto
Switch(config-if)# speed auto
Switch(config-if)# end
```

51

Folosind comenziile **duplex tip** și **speed valoare** putem specifica manual modul de funcționare al interfeței (half duplex, full duplex sau auto), cât și viteza port-urilor switch-urilor pentru a evita autonegocierea cu alte echipamente de rețea.

Ambele comenzi se execută din modul **interface**, și pentru a le salva în NVRAM este necesară comanda **copy running-config startup-config** sau comanda **write**.

Configurare interfață web

```
Switch# configure terminal
Switch(config)# ip http authentication enable
Switch(config)# ip http server
Switch(config)# end
```

52

Switch-urile moderne Cisco au numeroase utilitare ce necesită ca echipamentul să fie configurat ca HTTP server. Printre acestea se numără interfața web pentru echipamente Cisco, Cisco Security Device Manager, aplicații IP Phone și aplicații Cisco IOS Telephony Service.

Pentru a controla cine poate accesa serverul HTTP se poate configura opțional și autentificare.

Comenzile utile pentru configurarea switch-ului ca server HTTP se execută din modul `configure terminal` și sunt **"ip http authentication enable"** și **"ip http server"**. Pentru ca setarea să devină permanentă este necesară salvarea configurației în NVRAM folosind **`copy running-config startup-config`** sau **`write`**.

Înregistrări MAC statice

```
Switch# configure terminal
Switch(config)# mac-address-table static
      a8:12:34:56:78:90 vlan 10 interface fa0/1
Switch(config)# exit
Switch# show mac-address-table
```

53

Switch-urile folosesc tabela CAM pentru a determina pe ce porturi să trimită pachetele primite. Într-o tabelă CAM se pot înregistra adrese MAC atât static cât și dinamic.

Adresele MAC dinamice sunt adrese MAC invățate de switch care după o anumită perioadă de timp (proces numit “aging”) dispar din tabelă dacă nu sunt folosite.

Adresele MAC statice sunt adăugate de administrator pe anumite porturi. Adresele adăugate static nu dispar niciodată din tabela CAM și sunt trimise mereu pe portul pe care ele au fost setate. Adresele de tip static oferă administratorului control total asupra accesului la rețea.

Pentru a crea o mapare statică se folosește comanda **mac-address-table static mac_sursă vlan id_vlan interface fastethernet/serial id_interfață** din modul **configure terminal**.

Pentru a vizualiza MAC-urile aflate în tabela CAM se foloseste comanda **show mac-address-table**.

Comenzi show utile

Comandă	Efect
show interfaces [interface-id]	Informație despre o interfață
show startup-config	Afișează configurația încărcată la pornire
show running-config	Afișează configurația activă
show flash:	Afișează conținutul memoriei flash
show version	Informații despre hardware-ul și software-ul de sistem
show history	Istoria comenzi efectuate
show ip interface [interface-id]	Informații de nivelul 3 despre o interfață
show cdp neighbors	Vecinii descoperiți prin CDP
show mac-address-table	Afișează tabela de forwarding

54

Pentru a verifica corectitudinea configurațiilor realizate, sunt utilizate comenzi de tip **show**.

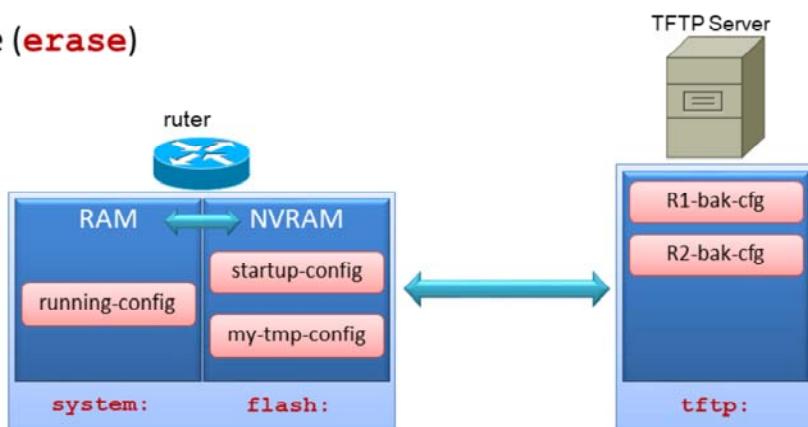
Comanda **show** se execută din modul Privileged EXEC și poate fi folosită cu diverse parametrii în funcție de configurația pe care vrem să o vizualizăm.

O comandă importantă **show** este comanda **show running-config**. Cu aceasta afișăm configurațiile ce rulează în acest moment pe switch. Pentru a afișa configurația pe care switch-ul o încarcă la boot-are se folosește comanda **show startup-config**.

O altă comandă utilă este **show interfaces [fastethernet/serial] [id_interfață]** unde parametrii aflați între [] sunt optionali. Dacă adăugam interfața dorită, această comandă ne arată starea și alte informații despre interfața respectivă. Dacă nu specificăm interfață, comanda ne arată datele pentru toate interfețele.

Manipularea configurațiilor

- Backup/restaurare (**copy**)
 - server TFTP
 - NVRAM
- Ștergere (**erase**)



55

Echipamentele Cisco permit salvarea configurațiilor în mai multe moduri.

Dacă ne dorim să păstrăm mai multe fișiere de configurare inițială putem opta să salvăm una dintre configurații în flash folosind comanda **copy startup-config flash: nume_fișier**. Salvând mai multe variante ale configurației inițiale putem să revenim în orice moment la o configurație anterioară funcțională.

Pentru a reveni la o configurație anterioară salvată în flash nu trebuie decât să copiem configurația peste cea actuală folosind comanda **copy flash: nume_fișier startup-config** și apoi să resetăm switch-ul folosind comanda "reload" din modul EXEC.

O altă metodă de a salva fișiere de configurare este folosirea unui server TFTP. Putem realiza acest lucru deoarece IOS-ul Cisco conține un client TFTP care permite conectarea la un server TFTP ce se află în aceeași rețea cu echipamentul.

Configurare acces consolă

```
Switch# configure terminal  
Switch(config)# line console 0  
Switch(config-line)# password cisco  
Switch(config-line)# login  
Switch(config-line)# end
```

56

Prin portul de consolă al unui echipament Cisco, se pot realiza orice configurații. Din acest motiv securizarea acestui port este benefică și necesară.

Pentru a realiza acest lucru setăm autentificarea pe portul de consolă folosind o parolă de login.

Pentru a seta această parolă intrăm în modul de configurare **config-line** folosind comanda **line console 0** din modul **global config**. Pentru a determina autentificarea prin parolă se folosește comanda **password parolă**. Pentru ca unui utilizator să îi fie necesară parola la conectarea prin portul de consolă trebuie ca la final să folosim comanda **login**.

Pentru a reveni la conectare fără parolă trebuie ca din modul config-line să executăm comenziile **no password** și **no login**.

Configurare acces terminal virtual

```
Switch# configure terminal
Switch(config)# line vty 0 4
Switch(config-line)# password cisco
Switch(config-line)# login
Switch(config-line)# end
```

57

Porturile vty ale unui switch permit accesarea acestuia de la distanță. Prin porturile de vty se pot realiza orice fel de configurații. Astfel, accesul fizic la echipament nu este neapărat necesar și este foarte important ca porturile vty să fie securizate.

Pentru a oferi un minim de securitate acestor porturi putem să setăm o parolă pentru accesul prin liniile de vty. Pe un switch Cisco pot fi numeroase porturi de vty pentru ca mai mulți administratori să poată configura switch-ul în același timp. Astfel, pentru a securiza switch-ul, trebuie ca toate porturile să necesite introducerea parolei.

Pentru a intra în modul de configurare a liniilor vty se folosește comanda **line vty *primul_port* *ultimul_port*** unde între *primul_port* și *ultimul_port* este intervalul port-urilor de acces la distanță. Pentru a seta apoi parola, se procedează idem ca la securizarea portului de consolă, folosind comanda **password *parolă*** urmată apoi de comanda **login**.

Configurare parolă EXEC

- Protejează accesul la modul Privileged Exec

```
Switch# configure terminal  
; dacă se dorește afișarea în text clar:  
Switch(config)# enable password cisco  
; dacă se dorește afișarea hash-ului:  
Switch(config)# enable secret cisco  
Switch(config)# end
```

58

În modul Privileged Exec, orice utilizator poate configura toate opțiunile disponibile pe echipament, inclusiv folosirea comenzi de tip **show** pentru observarea parolelor necriptate. Din acest motiv este foarte importantă securizarea accesului la acest mod.

Comanda **enable password parolă** permite setarea unei parole pentru restricționarea accesului la modul Privileged Exec. Folosind această comandă parola este salvată necriptat în running și startup config. Astfel, folosind comenzi de tip **show**, parola poate fi citită din fișierele de configurare. Din aceasta cauză Cisco a introdus comanda **enable secret parolă** ce salvează parola sub formă de hash în fișierele de configurare.

Criptarea parolelor

- Comanda criptează parolele în text clar din configurații
- Folosește criptare type 7
- Parolele astfel criptate sunt foarte ușor de spart

```
Switch# show running-config
...
    password cisco
...
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
...
    password 1511021F0725
...
```

59

Când configurăm parole în Cisco IOS CLI, implicit toate parolele (exceptând enable secret) sunt salvate în format clear text în fișierele de configurare startup-config și running-config.

Folosind comanda **service password-encryption** toate parolele din sistem sunt stocate sub forma criptată. Imediat ce comanda a fost executată din modul global config, toate parolele salvate în fișierele de configurare sunt convertite într-o formă criptată.

Configurare bannere

- Login banner

```
Switch(config)# banner login "Accesul interzis!"
```

- MOTD banner

```
Switch(config)# banner motd "Test congestie joi"
```

60

Cisco IOS permite configurarea unor mesaje ce apar oricărei persoane ce se autentifică pe echipament.

Aceste mesaje se numesc banner login sau banner motd (Message Of The Day).

Pentru a configura un mesaj ce va aparea înainte de autentificarea cu username si parolă, se folosește comanda **banner login mesaj**. Mesajul trebuie scris intre ghilimele.

Comanda **banner motd mesaj** configurează un mesaj ce va apărea la accesarea echipamentului de la distanță.

Configurare Telnet

- Telnet

```
Switch(config)# line vty 0 4
Switch(config-line)# transport input telnet
```

61

Un switch Cisco poate fi accesat de la distanță prin două metode: Telnet și SSH.

Telnet este un protocol popular deoarece majoritatea sistemelor de operare din ziua de azi conțin un client de Telnet preinstalat. Este metoda originală ce este suportată pe toate echipamentele Cisco, însă este nesecurizată deoarece protocolul transmite toate datele necriptat.

În mod implicit, echipamentele pot fi accesate folosind Telnet, însă, pentru a specifica explicit acest lucru se poate folosi comanda **transport input telnet** din modul de configurare al liniilor de vty.

Configurare SSH

- SSH

```
Switch(config)# ip domain-name somedomain.com
Switch(config)# crypto key generate rsa
Switch(config)# ip ssh version 2
Switch(config)# line vty 0 4
Switch(config-line)# transport input ssh
```

62

SSH a devenit protocolul preferat de conectare la distanță pe echipamentele Cisco, deoarece acesta adresează problema securității introdusă de folosirea protocolului Telnet. Comunicația SSH între client și server este criptată. Actualmente echipamentele Cisco suportă atât SSH versiunea 1 cât și SSH versiunea 2. Se recomandă folosirea SSH v2 atunci când este posibil deoarece criptarea folosită este mai puternică decât în cazul versiunii anterioare.

SSH poate folosi diferite standarde de criptare a datelor (DES, 3DES). Pentru a implementa SSH este necesară generarea unor chei RSA. RSA folosește o cheie publică și o cheie privată pentru a realiza autentificarea. Algoritmii de autentificare vor fi studiați în detaliu la CCNA4.

Atacuri de securitate (1)

- MAC address flooding
- DHCP spoofing

63

MAC address flooding

Se generează și se trimită unui switch trafic "fals" folosind un număr foarte mare de adrese MAC sursă pentru a umple tabela MAC a switch-ului. În momentul în care aceasta a ajuns la limita superioră, switch-ul se va comporta ca un hub, permitând unui atacator conectat la switch să "vadă" tot traficul care trece prin acesta.

DHCP spoofing

Se activează un server DHCP "pirat" în rețeaua țintă, care să raspundă cererilor DHCP înaintea server-ului legitim, configurând astfel hosturile după dorința atacatorului. Din acest moment, tot traficul destinat gateway-ului din acea rețea poate fi redirectat către atacator.

Atacuri de securitate (2)

- DHCP starvation
- Atacuri folosind CDP
- Brute Force
- DoS

64

DHCP starvation

Se trimit un număr mare de cereri DHCP false, epuizând astfel spațiul de adrese IP disponibil.

Brute Force

Spargerea unei parole prin generarea tuturor combinațiilor posibile, începând cu cele uzuale.

DOS (Denial Of Service)

Atacuri care au ca rezultat blocarea accesului la o resursă sau un serviciu.

Port Security

- Limitează adresele MAC permise pe un port
- Pe o interfață se pot configura
 - un grup de adrese MAC valide
 - o singură adresă MAC validă
 - comportamentul portului când o regulă este încălcată
- Adrese MAC sigure
 - statice
 - dinamice
 - sticky

65

Adresele MAC sigure pot fi statice (configurate manual, salvate în tabela CAM și în fișierul de configurație în mod automat), dinamice (învățate și salvate în tabela MAC în mod dinamic) și "sticky"(învățate și salvate în tabela MAC și în fișierul de configurație în mod dinamic).

Următoarele 2 situații se consideră o încălcare a regulilor de securitate:

- Se depășește numărul maxim de adrese MAC definit pentru o interfață a switch-ului.
- O adresă MAC învățată sau configurată pe o interfață securizată este depistată pe o altă interfață securizată din același VLAN.

Port Security

- Limitează adresele MAC permise pe un port
- Pe o interfață se pot configura
 - un grup de adrese MAC valide
 - o singură adresă MAC validă
 - comportamentul portului când o regulă este încălcată
- Adrese MAC sigure
 - statice
 - dinamice
 - sticky

66

Interfețele unui switch pot fi configurate să se comporte într-unul dintre modurile următoare:

- Protect: La atingerea pragului maxim de adrese MAC pentru o interfață, cadrele primite pe aceasta cu adresa MAC sursă necunoscută vor fi aruncate. Nu are loc o informare a faptului că a avut loc o încălcare a regulilor de securitate.
- Restrict: La fel ca modul "protect", cu diferența că are loc o informare a faptului că a avut loc o încălcare a regulilor de securitate.
- Shutdown: Acesta este modul implicit. În cazul apariției unei încălcări a regulilor de securitate, interfața în cauză este trecută imediat în modul "error-disabled". În plus, are loc o și informare a faptului că a avut loc o încălcare a regulilor de securitate. Reducerea interfeței în starea normală se face prin oprirea ("shutdown") și repornirea acesteia ("no shutdown").

Configurare Dynamic Port Security

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# end
```

67

Cu ajutorul port-security pe un switch se pot specifica adresele MAC ce sunt permise pe fiecare port sau acțiuni specifice când o adresă MAC neautorizată încearcă să se conecteze pe acel port.

Pentru a activa port-security se intră în modul interfeței dorite folosind comanda **interface fastethernet id_interfață**, se trece portul în modul access folosind comanda **switchport mode access** și se introduce comanda **switchport port-security**.

Adresele MAC permise pe fiecare port pot fi specificate în 3 moduri:

1. Static, configurate manual folosind comanda **switchport port-security mac-address adresa_mac**.
2. Dinamic, adrese învățate automat de switch ce sunt salvate numai în tabela de adresare. Acestea se sterg la resetarea switch-ului.
3. Sticky, adresele sunt învățate automat de switch, iar apoi acestea pot fi salvate în startup-config.

Configurare Sticky Port Security

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security
    maximum 50
Switch(config-if)# switchport port-security
    mac-address sticky
Switch(config-if)# end
```

68

Pentru a configura port security de tip sticky, primul pas constă în trecerea interfeței în mod access folosind comanda **switchport mode access** urmată de comanda de activare a port security **switchport port-security**.

Pentru a specifica numărul maxim de adrese ce vor fi invățate pe acest port vom utiliza comanda **switchport port-security maximum număr_de_adrese**.

Pentru a activa port security de tip sticky folosim comanda **switchport port-security mac-address sticky**. Odată executată această comandă, switch-ul va învăța primele 50 de adrese ce se vor conecta pe acel port , numai acelea având access. Pentru a reține acele adrese este necesară salvarea configurației curente în startup-config.

Capitolul 3: VLAN-uri

Extinderea rețelei

- Hub
 - extinde domeniul de coliziune
 - trimite toate pachetele broadcast
- Switch (default)
 - segmentează domeniul de coliziune
 - extinde domeniul de broadcast
 - trimite pachete atât unicast cât și broadcast

70

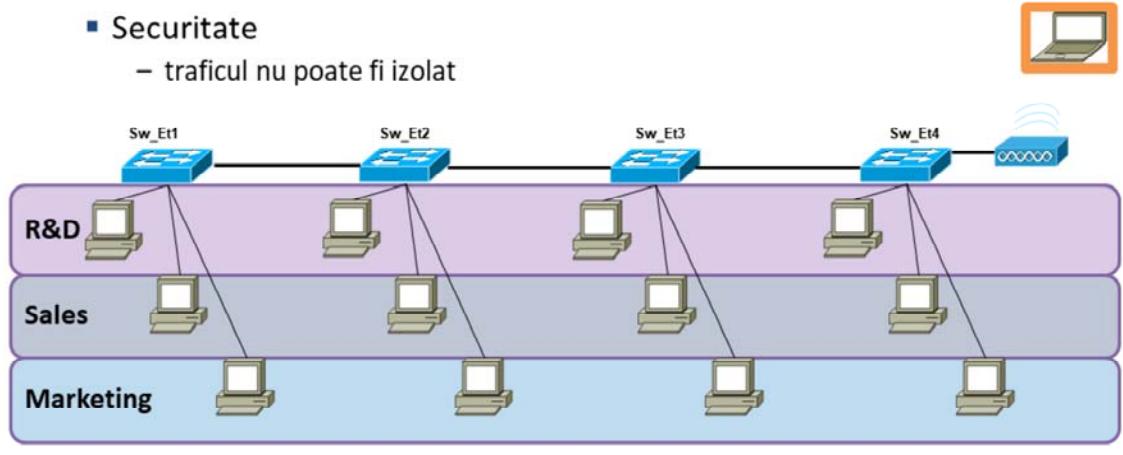
În rețelele actuale se urmărește reducerea dimensiunii domeniilor de broadcast prin separarea acestora în funcție de departamentele specifice fiecarei companii.

Hub-ul este un echipament de rețea ce nu se mai folosește în ziua de astăzi, deoarece extinde domeniile de coliziune, astfel creând riscuri de securitate și un overhead considerabil din cauza trimiterii pachetelor pe toate porturile.

Echipamentul folosit preponderent în rețelele actuale este switch-ul. Acesta segmentează domeniul de coliziune, oferă securitate la nivel de porturi și reduce mult overhead-ul rețelei deoarece folosește predominant transmisie de tip unicast. VLAN-urile sunt o tehnologie ce se mapează perfect pe rețelele locale actuale ce folosesc switch-uri.

Probleme într-o rețea locală

- Broadcast-uri
 - trafic inutil
- Securitate
 - traficul nu poate fi izolat



71

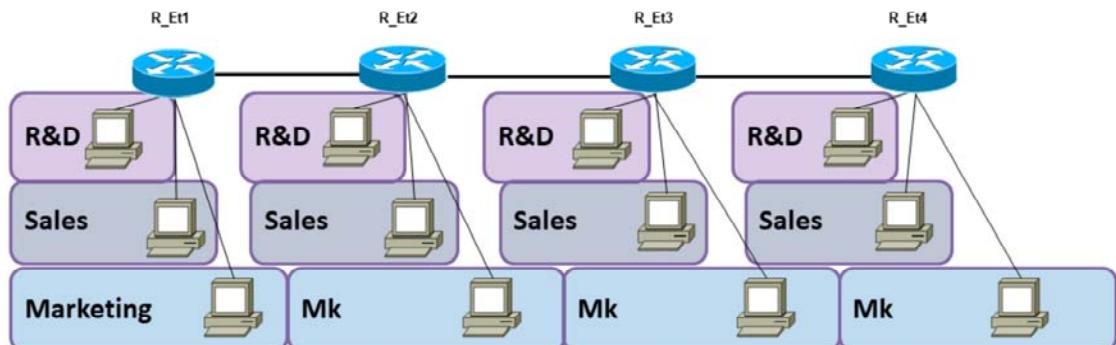
Cu cât avem un număr mai mare de echipamente într-o rețea locală (switch-uri, stații) cu atât numărul pachetelor de broadcast va fi mai mare. Acest lucru creează trafic inutil pe link-urile rețelei, deoarece switch-ul mărește domeniul de broadcast. Un mesaj cu destinația 255.255.255.255 va fi reprodus de fiecare switch pe traseu către toate stațiile din toate departamentele.

O altă problemă majoră în rețelele locale este securitatea. Pachetele trimise broadcast în rețelele locale pot fi interceptate de toate stațiile conectate la rețea.

Vom observa în continuare soluțiile de rezolvare a acestor probleme.

Soluție folosind rutere

- Deficiențele soluției
 - ruterele sunt scumpe
 - porturile pe rutere sunt scumpe
 - prea multe domenii de broadcast



72

O soluție pentru separarea domeniilor de broadcast în funcție de specificul departamentelor este cea în care echipamentele intermediare sunt înlocuite de rutere.

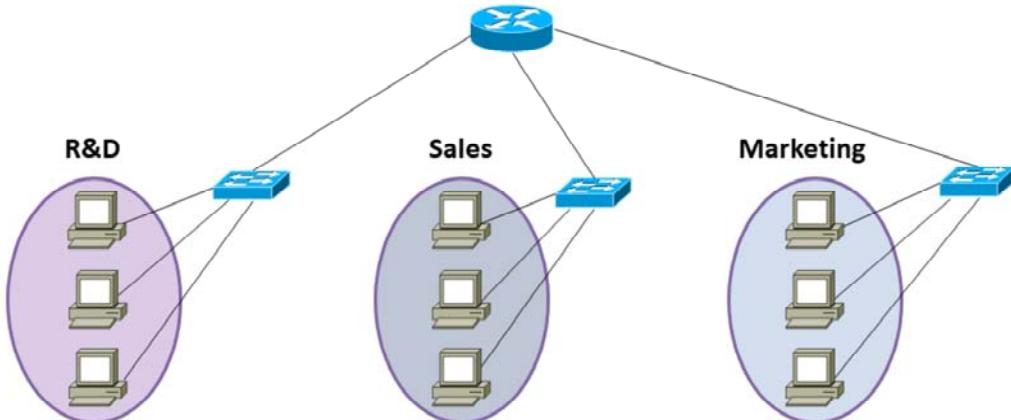
Ruterele fiind echipamente ce iau decizii în funcție de nivelul 3, separă departamentele în rețele diferite. Fiecare interfață a unui ruter delimită un domeniu de broadcast, deci dimensiunea unui domeniu de broadcast va fi minimizată cu ajutorul acestei soluții.

De asemenea, pe rutere se pot implementa politici de filtrare a traficului astfel încât să se poată controla traficul de la o subretea la cealaltă.

Neajunsul acestei soluții, în afara de costul ridicat al echipamentelor, este faptul că ruterele introduc un overhead foarte mare în rețea locală (fiecare calculator să fie într-o rețea unică și să existe rutare end-to-end).

Soluție folosind ruter și switchuri

- Mai ieftină
- Mai eficientă



73

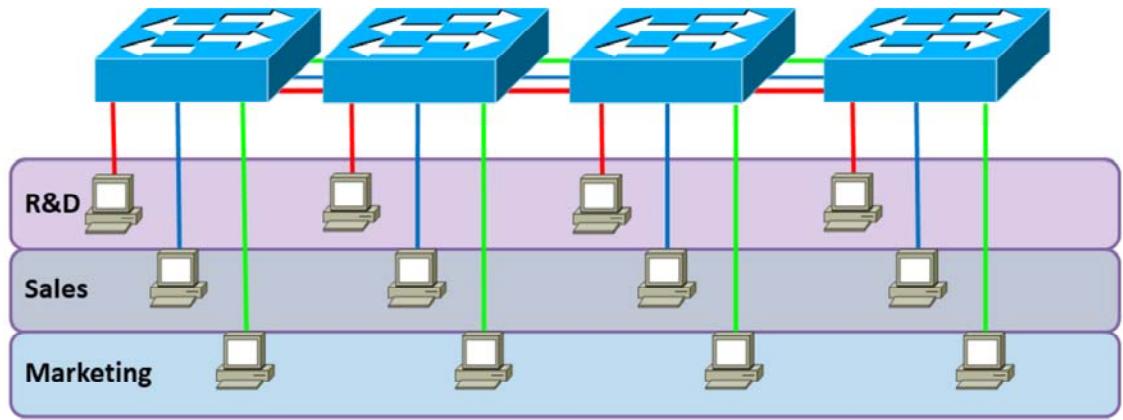
O combinație între primele două soluții ar însemna legarea stațiilor de pe fiecare departament la câte un switch, urmând ca apoi switch-urile să fie conectate la un ruter care stabilește politicile de trimis ale pachetelor.

Această soluție deși rezolvă problema domeniilor de broadcast este nerecomandată datorită faptului că este nescalabilă. Pentru a implementa această soluție, este necesar ca toate echipamentele terminale ale aceluiași departament să fie legate la același switch. Spre deosebire de exemplul anterior, soluția prezentată este mult mai eficientă dar oferă foarte puțină flexibilitate la nivelul fizic .

Această soluție este mai ieftină decât precedenta, dar în funcție de numărul de departamente al companiei poate presupune topologii foarte complicate.

Soluție folosind VLAN-uri

- Împărțire a rețelei în funcție de departament nu în funcție de așezarea geografică



74

Soluția optimă pentru rezolvarea problemei domeniilor de broadcast a diferitelor departamente într-o rețea locală este folosirea tehnologiei Virtual LAN (VLAN). Aceasta permite unui administrator de rețea să creeze grupuri de echipamente ce se află în rețele independente la nivel logic chiar dacă folosesc aceeași infrastructură la nivel fizic. Această tehnologie permite crearea mai multor rețele de nivel 3 în aceeași rețea locală folosindu-se aceeași infrastructură de switching.

De asemenea putem folosi un VLAN pentru a ne structura geografic rețeaua astfel încât aceasta să poată scala fără modificarea drastică a topologiei inițiale.

Reguli

- Un VLAN corespunde unui subnet
 - un VLAN este un domeniu de broadcast
- Un VLAN este configurat per port
 - stațiile nu știu că aparțin unui VLAN
- Pentru a comunica între VLAN-uri este nevoie de un dispozitiv Layer 3
 - ruter
 - switch L3
- Un switch are câte o tabelă MAC pentru fiecare VLAN

75

Pentru ca stațiile să comunice în același VLAN ele trebuie să aibă un IP și o mască de rețea consistentă pentru întreg VLAN-ul . Port-ul switch-ului la care este conectată stația trebuie să fie asignat VLAN-ului din care face parte echipamentul terminal. Un port al unui switch ce este atribuit exclusiv unui singur VLAN se numește un port de tip Access.

Stațiile aflate în VLAN-uri diferite, chiar dacă sunt conectate la același switch, nu pot comunica între ele. Pentru a rezolva această problemă avem nevoie de un echipament de nivel 3 (Switch Layer 3, Ruter). Switch-ul menține o tabelă CAM pentru fiecare VLAN în care reține MAC-urile stațiilor ce se conectează la switch pe porturile asignate VLAN-ului respectiv.

Beneficii VLAN-uri

- Securitate sporită
- Reducerea costurilor
- Performanță crescută
- Delimitare domenii Broadcast
- Management simplificat al rețelei

76

VLAN-urile presupun securitate sporită deoarece grupurile ce au de transmis date confidențiale sunt separate de restul rețelei. Reducerea costului provine din lipsa necesității unor echipamente ce operează la nivelul 3 sau mai sus în stiva OSI și din folosirea mai eficientă a lătimii de bandă existente.

Performanța sporită se datorează împărțirii în domenii de broadcast astfel reducând traficul ce nu este necesar tuturor echipamentelor din rețea.

VLAN-urile simplifică mult administrarea rețelei deoarece utilizatorii ce au nevoi similare împart același VLAN.

LAN-uri Virtuale

- **VLAN implicit: VLAN1**
 - creat automat pe switch-uri
 - nu poate fi șters
 - inițial toate porturile sunt în VLAN 1
- **VLAN 2 – 1001**
 - Ethernet VLAN
- **VLAN 1002 – 1005**
 - Token Ring și FDDI VLAN
 - create automat pe switch și nu pot fi șterse
- **VLAN 1006 - 4096**
 - extended VLANs

77

VLAN-urile standard se află între ID-urile 1 - 1005 . Aceste VLAN-uri se împart în VLAN-uri Ethernet (cu valori între 2 - 1001) și VLAN-uri Token Ring și FDDI VLAN (cu valori 1002 - 1005), cele din urmă creându-se automat pe switch și neputând fi șterse. VLAN-urile cuprinse între ID-urile 1006 și 4096 se numesc Extended VLAN. VLAN-urile extinse suportă mai puține facilități decât VLAN-urile standard și permit unei companii enterprise să își extindă infrastructura la un număr mai mare de clienți.

VLAN-urile standard, salvate în fișierul vlan.dat în Flash, se păstrează la restartarea switch-ului.

VLAN-urile extinse nu se păstrează în vlan.dat ci în running-config. Astfel, pentru a se păstra configurația, este necesar să copiem modificările în startup-config.

Stocarea configurărilor de VLAN

- Lista de VLAN-uri standard (1-1005)
 - salvată în **vlan.dat** în Flash
 - nu se sterg la reset
 - nu se sterg dacă stergem **startup-config**
- Lista de VLAN-uri extinse (1006 – 4094)
 - salvată în **running-config**
 - se sterg la resetarea configurațiilor

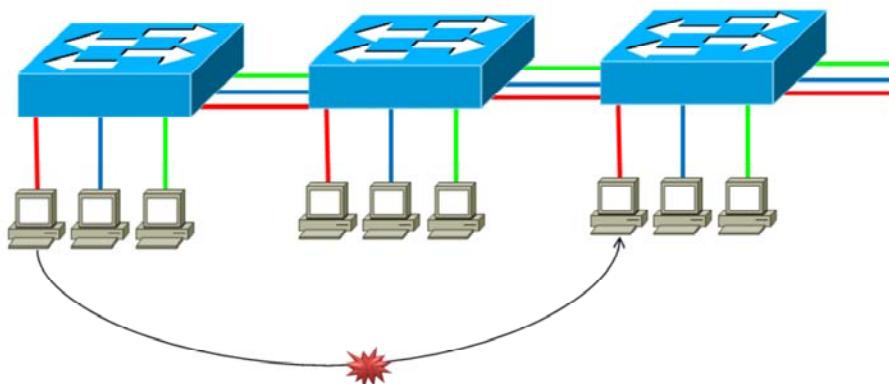
78

VLAN-urile standard se păstrează la restartarea switch-ului datorită faptului că sunt salvate în fisierul **vlan.dat** în Flash.

VLAN-urile extinse nu se păstrează în **vlan.dat** ci în **running-config**.

Consistența VLAN-urilor

- Este necesar un drum neîntrerupt între dispozitivele din același VLAN



79

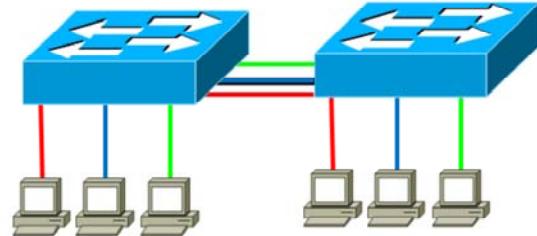
Pentru a obține conectivitate între mai multe stații aflate în același VLAN trebuie să ne asigurăm că toate switch-urile intermediare celor 2 echipamente au configurat VLAN-ul respectiv și pot trimite pachete pe acel segment.

Un switch reține în tabela CAM atât adresa MAC sursă asociată cu portul de intrare, cât și numărul VLAN-ului configurat pe acel port. Când un switch primește un pachet destinat VLAN-ului 100, acesta nu îl va putea trimite decât pe porturile ce sunt configurate să accepte trafic pentru VLAN-ul 100.

Să presupunem că 2 stații aparțin VLAN-ului 100. Dacă pe una dintre legăturile dintre switch-urile intermediare nu este permis acest VLAN, cele două stații nu vor putea comunica.

Scalabilitatea VLAN-urilor

- Pentru fiecare VLAN între două switch-uri se consumă câte două porturi
 - scump
 - nescalabil
- Soluția:
 - trunking



80

O linie trunk este o legătură point-to-point între 2 dispozitive de rețea ce poate transmite mai mult de un singur VLAN. O linie trunk VLAN îți permite să extinzi VLAN-urile peste o întreagă rețea . Un trunk nu aparține unui VLAN specific, ci este o modalitate de a transmite mai multe VLAN-uri folosind aceleasi politici, între switch-uri și rutere.

Astfel, dacă un switch va primi un pachet din VLAN-ul 10, acesta îl va putea comuta atât pe legăturile configurate explicit cu VLAN 10 cât și pe legăturile trunk, care poate transmite informații din toate VLAN-urile.

Folosirea liniilor de trunk aduce avantaje precum costuri reduse ale echipamentelor (switch-urile nu mai necesită un port separat per VLAN), oferă o scalabilitate sporită (adăugarea unui VLAN presupune doar adăugarea acestuia pe liniile de trunk).

Trunking

- Marcarea cadrelor pentru a le ghida prin rețea
 - nivel 2
 - protocoale specializate
- ISL
 - proprietar Cisco
 - încapsulare
- 802.1Q (dot1q)
 - open standard
 - tagging



81

Când un switch primește un frame pe un port configurat în mod access pentru un anumit VLAN, switch-ul decapsulează frame-ul, inserează un VLAN Tag, recalculează FCS-ul și trimite frame-ul marcat.

Pe liniile de tip trunk există două protocoale specializate ce permit transmiterea VLAN-urilor: ISL și 802.1Q.

ISL este actualmente un protocol legacy însă se mai folosește în rețele implementate cu mai mult timp în urmă. Într-un port trunk ce rulează ISL toate pachetele primite trebuie să conțină antet ISL și toate pachetele transmise sunt trimise cu un antet ISL. Frame-urile ce nu sunt marcate și sunt primite pe un trunk ISL sunt aruncate.

Câmpul dot1.q tag conține 3 biți de prioritate, un bit CFI (Canonical Format Identifier - permite transmiterea frame-urilor Token Ring pe acel VLAN) și 12 biți ce reprezintă VLAN ID-ul.

802.1q

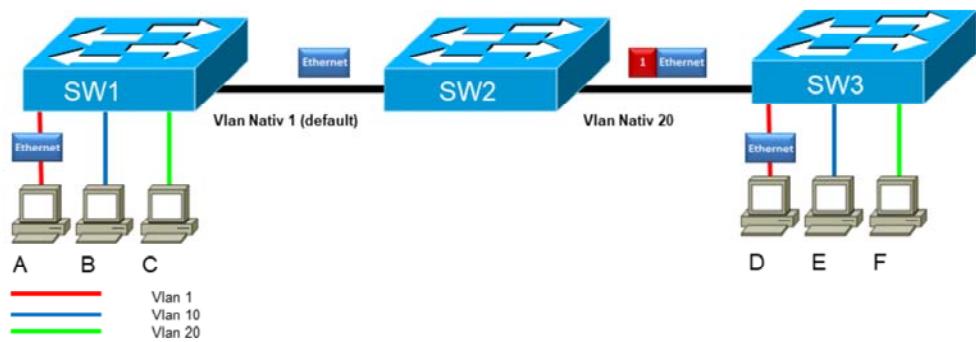
- Setat implicit pe unele switch-uri (dacă ISL nu este disponibil)
- Oferă suport pentru maxim 4096 VLAN-uri
- Fiecare legătură trunk are un **VLAN nativ**
 - implicit este VLAN 1
 - cadrele ce aparțin VLAN-ului nativ circulă nemarcate
 - switch-urile de la capătul legăturii trunk trebuie să aibă același VLAN nativ configurat

82

Protocolul 802.1Q este protocolul folosit actualmente pe toate switch-urile Cisco. Când un pachet urmează a fi trimis pe o linie de tip trunk, acestuia îi este întâi verificat marcajul. Dacă VLAN-ul ce este inclus în acel marcaj este permis pe trunk, pachetul va fi transmis mai departe cu marcajul aferent. În situația în care VLAN-ul nu este permis pe trunk, pachetul va fi aruncat.

Când pe un port trunk este primit un frame nemarcat acel frame este trimis implicit pe VLAN-ul nativ . VLAN-ul nativ standard este VLAN-ul 1.

Marcarea folosind dot1q

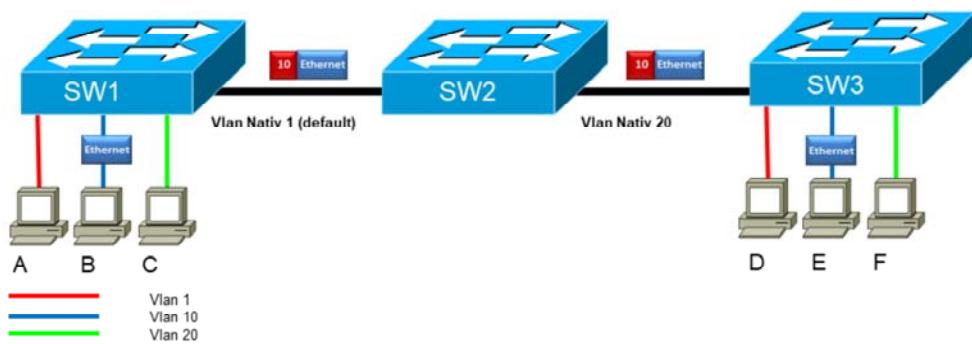


83

În această imagine observăm că PC A vrea să trimită un pachet către PC D. A se află în VLAN-ul 1, astfel că pachet-ul Ethernet trimis de PC nu va fi marcat pe legătura dintre SW1 și SW2 deoarece această legătură are ca VLAN nativ VLAN-ul 1. Pe legătura dintre SW2 și SW3 pachetul va fi marcat cu VLAN-ul 1 deoarece VLAN-ul nativ este 20. Odată ajuns pachetul la SW3 acesta va știi să îl trimită PC-ului aflat în VLAN-ul 1 și anume PC-ul D.

Un pachet destinat VLAN-ului nativ de pe o linie trunk va trece peste acea legătură fără nici un VLAN tag. Pe fiecare legătură trunk existentă poate fi configurat un alt VLAN nativ.

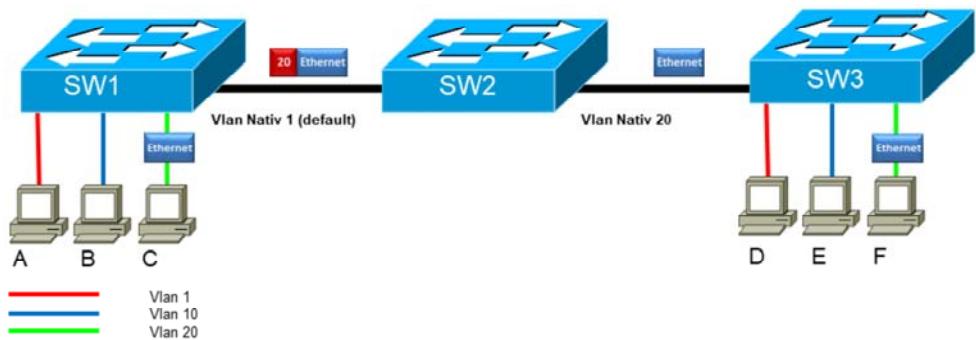
Marcarea folosind dot1q



84

Spre deosebire de situatia anterioara aici pachetul este trimis de la PC B la PC E , PC-uri ce se afla în VLAN-ul 10. Din aceasta cauza pachetul va circula atat pe link-ul SW1 - SW2 cat și pe SW2 – SW3 marcat cu VLAN-ul 10.

Marcarea folosind dot1q



85

Această situație este similară primei situații prezentate, numai că de această dată transmisia se realizează între **PC C** și **PC F**, ambele PC-uri fiind în VLAN-ul 20. Din această cauză pachetul va circula marcat pe legătura cu VLAN-ul nativ 1 și nemarcat pe legătura cu VLAN-ul nativ 20.

Crearea unui VLAN

- **vlan database**

- scos din uz (probleme de folosire)

```
Sw# vlan database
Sw(vlan)# vlan 20 name Sales
```

- **Din modul de configurare**

```
Sw(config)# vlan 10
sw(config-vlan)# name Management
```

- **La adăugarea unui port**

```
Sw(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

86

Un mod de configurare a VLAN-urilor ce a devenit actualmente legacy, este folosind comanda VLAN database. Pentru a accesa acest mod se folosea comanda **vlan database** din prompt-ul Privileged Exec. În acest mod folosind comanda **vlan id_vlan name nume_vlan** se configurează un vlan cu numele corespunzător. La ieșirea din acest mod, se aplicau toate configurațiile cu privire la VLAN-uri ce au fost introduse. Acest mod de configurare a fost înlocuit cu unul mai intuitiv. Crearea unui VLAN se realizează din modul de configurare folosind comanda **vlan id_vlan**. În urma executării acestei comenzi suntem introduși într-un mod de configurare de unde putem specifica diverse caracteristici ale VLAN-ului respectiv.

Pentru a asocia unei interfețe un VLAN este folosită comanda **switchport access vlan vlan_id** din modul de configurare al interfeței. Pe IOS-urile noi, la executarea acestei comenzi dacă VLAN-ul nu există în baza de date, el este creat automat.

Configurare mod port

- Un port poate fi în mod
 - access
 - trunk
 - dinamic
- **switchport mode { access | trunk | dynamic }**

```
Sw(config)# interface f0/1
sw(config-if)# switchport mode access
Sw(config)# interface f0/1
Sw(config-if)# switchport mode trunk
```

87

Un port pe care este configurat un singur VLAN și care este de obicei configurat pe o interfață către o stație, este un port access. Un port pe care sunt configurate mai multe VLAN-uri este un port trunk.

Porturile aflate în mod dinamic autonegociază modul în care se află portul respectiv folosind protocolul DTP (Dynamic Trunking Protocol). Acesta poate avea următoarele stări pe fiecare port:

- auto: portul dorește pasiv negocierea unui trunk. Portul va deveni trunk dacă portul aflat la capătul opus este configurat cu modul on sau desirable
- on: portul va fi trunk indiferent de modul vecinului
- off: forțează legătura să nu fie trunk, indiferent de modul vecinului
- desirable: portul va dori activ negocierea unui trunk
- nonegotiate: portul va fi trunk, dar nu va schimba mesaje DTP

Configurare port access

- Un port access poate apartine unui singur VLAN
- Portul implicit apartine VLAN-ului 1
- **switchport access vlan VLAN_NO**

```
Sw(config)# interface f0/1
Sw(config-if)# switchport mode access
Sw(config-if)# switchport access vlan 10
```

88

Pe un port aflat în modul access putem seta un singur VLAN. Pentru a configura un port în modul access sunt necesari doi pași.

Primul constă în setarea modului portului folosind comanda **switchport mode access** din modul de configurare al interfeței.

Al doilea pas constă în setarea VLAN-ului care este permis pe port folosind comanda **switchport access vlan id_vlan**. Implicit VLAN-ul permis pe toate porturile unui switch este VLAN-ul 1. Dacă comanda este folosită ulterior folosind alt VLAN, aceasta va suprascrie comanda anterioară.

De obicei acest tip de port este folosit atunci când conectăm echipamente terminale, deoarece acestea fac parte dintr-o singură rețea.

Configurare port trunk

- Un port trunk poate permite anumite VLAN-uri
- Implicit transportă toate VLAN-urile
- **switchport trunk allow vlans { add, delete, VLAN_LIST }**

```
Sw(config)# interface f0/1
Sw(config-if)# switchport mode trunk
Sw(config-if)# switchport trunk allowed vlan 1,10,20
```

89

Un port configurat în modul trunk poate permite mai multe VLAN-uri pe aceeași legătură. Un port se configurează în modul trunk folosind comanda **switchport mode trunk**. Implicit un port configurat în modul trunk permite trafic de pe toate VLAN-urile existente pe switch la acel moment.

Pentru a specifica doar VLAN-urile ce se doresc a fi transmise pe o legătură de tip trunk se folosește comanda **switchport trunk allowed vlan id_vlan** în modul interfață unde id-urile VLAN-urilor sunt specificate cu virgulă între ele.

Pentru a adăuga un VLAN la lista celor permise pe un anumit port se folosește comanda **switchport trunk allowed vlan add id_vlan**, iar pentru a șterge un VLAN se folosește comanda **switchport trunk allowed vlan delete id_vlan**.

Comenzi de vizualizare asignare VLAN

- **show vlan [brief]**

```
Sw# show vlan

VLAN Name          Status    Ports
---  -----
1   default         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                      Fa0/7, Fa0/8, Fa0/10, Fa0/11
10  Management     active
20  Sales           active
30  VLAN0030       active    Fa0/5, Fa0/6
99  VLAN0099       active
```

90

Pentru a vedea asocierile dintre VLAN-urile configurate pe un switch și interfețele acestui echipament se folosește comanda **show vlan**. În output-ul rezultat, prima coloană reprezintă id-ul VLAN-ului, a doua coloană definește numele atribuit VLAN-ului, iar a treia coloană specifică starea de funcționare a VLAN-ului. În cazul în care VLAN-ul este functional, valoarea câmpului va fi “active”. Ultima coloană reprezintă porturile ce sunt în modul access pentru VLAN-ul respectiv.

În output-ul acestei comenzi nu vor fi afișate interfețele ce se găsesc în modul trunk, deoarece o interfață aflată în acest mod aparține mai multor VLAN-uri în același timp, astfel neputând fi asociată unui singur VLAN.

Un switch pe care nu au fost realizate configurații de VLAN va afișa toate interfețele sale în VLAN-ul 1.

Comenzi de vizualizare trunk-uri

▪ **show interfaces trunk**

```
S2#show interfaces trunk

Port      Mode       Encapsulation  Status      Native vlan
Fa0/9    desirable   802.1q        trunking    1
Fa0/12   desirable   802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/9    1-4094
Fa0/12   1-4094

Port      Vlans allowed and active in management domain
Fa0/9    1,10,20,30,99
Fa0/12   1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/9    1,10,20,30,99
Fa0/12   1,10,20,30,99
```

91

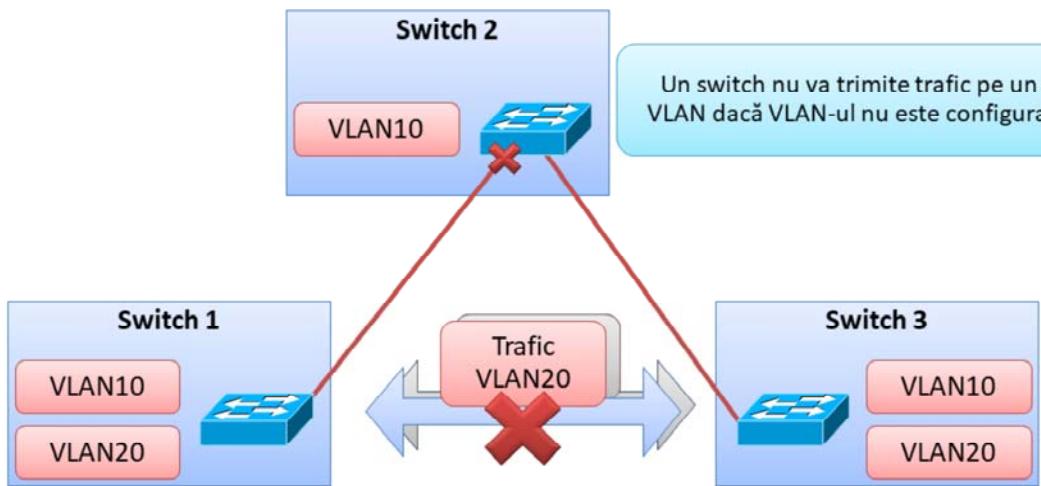
Pentru depanarea problemelor apărute și aflarea informațiilor despre interfețele care se găsesc în modul trunk se folosește comanda **show interfaces trunk** din modul de configurare global config.

Pentru fiecare port este afișat modul în care este configurat, încapsularea folosită, starea de funcționare și VLAN-ul nativ pe respectivul trunk.

În continuarea output-ului este afișată o secțiune care descrie ce VLAN-uri au fost configurate pe fiecare port, ce VLAN-uri sunt active pe fiecare port și la final o listă cu VLAN-urile ce sunt active în urma aplicării algoritmului Spanning-tree.

Capitolul 4: VTP

Nevoia de VTP



93

Odată cu creșterea numărului de switch-uri într-o rețea, administrarea VLAN-urilor și trunk-urilor devine o problemă. În desen se observă că VLAN-ul 20 este configurat pe switch-ul 1 și pe switch-ul 3 dar nu și pe switch-ul 2.

În acest caz, traficul pe VLAN-ul 20 nu va funcționa decât dacă VLAN-ul va fi adăugat manual pe switch-ul 2. De aici rezultă nevoia de a implementa un protocol pentru a rezolva această problemă. Acesta este VTP.

Ce este VTP

- Vlan Trunking Protocol
 - proprietar Cisco
 - protocol de nivel 2
 - partajează informația despre VLAN-uri (1-1005)



94

VTP permite unui administrator de rețea să configureze un switch astfel încât acesta să își propage configurațiile VLAN-urilor către alte Switch-uri din rețea.

Un switch ce rulează VTP poate fi configurat într-unul din următoarele 3 moduri: Server, Client sau Transparent fiecare cu funcționalitatea sa specifică.

Primele versiuni ale protocolului VTP partajau informații despre VLAN-urile standard (1 - 1005) dar nu și despre cele extinse (1005 - 4094). Odată cu apariția VTP version 3 acesta poate partaja informații despre ambele tipuri de VLAN-uri.

Protocolul VTP transmite informații numai peste liniile configurate în mod trunk.

Avantaje VTP

- Consistență informații de VLAN la nivel de rețea
- Monitorizare VLAN-uri
- Adăugare în mod dinamic a VLAN-urilor la liniile trunk

95

Beneficiile aduse de VTP sunt numeroase. Într-o rețea cu un număr consistent de switch-uri munca unui administrator de rețea pentru a adăuga și a asigura consistență la nivel de VLAN-uri este din ce în ce mai anevoieasă și greu de realizat.

VTP îi permite unui administrator de rețea să realizeze configurații pe un singur switch aflat în modul VTP Server, iar acesta va distribui și sincroniza informații despre VLAN-uri cu toate switch-urile ce au VTP activat în rețeaua locală.

VTP oferă configurații consistente la nivel de informații despre VLAN-uri controlând ștergerea, adăugarea sau redenumirea unui VLAN astfel încât schimbările să se propage la toate switch-urile implicate. De asemenea, VTP adaugă dinamic noile VLAN-uri primite la liniile de trunk.

Componente cheie VTP

- Domenii VTP
- Moduri VTP
- Număr de revizie
- Mesaje VTP
- VTP Pruning

96

Componențele cheie VTP sunt în număr de 5.

Domeniile VTP constau în unul sau mai multe Switch-uri interconectate. Toate switch-urile dintr-un domeniu împart aceleași configurații despre VLAN-uri folosind mesaje VTP.

Modurile VTP sunt în număr de 3, un switch putând fi configurat în oricare dintre ele: Server, Client și Transparent.

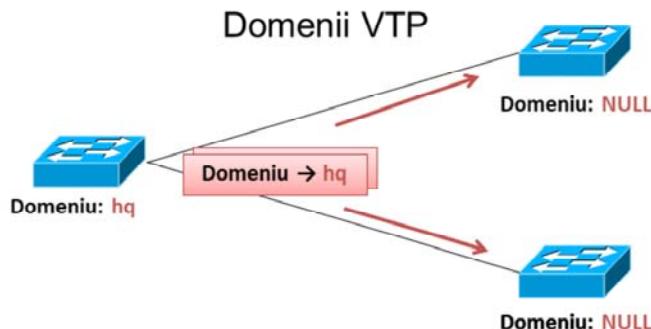
Numărul de revizie este transmis în mesaje VTP și în funcție de acesta un switch decide dacă trebuie să își resincronizeze informațiile despre VLAN-uri.

Mesajele VTP sunt folosite pentru distribuirea și sincronizarea configurațiilor VLAN-urilor în întregul domeniu.

VTP Pruning crește lățimea de bandă disponibilă în rețea reducând traficul inutil de pe liniile de trunk.

Domenii VTP

- Toate switch-urile trebuie să facă parte din același domeniu de VTP
- Pot fi învățate dinamic



97

VTP permite separarea unei rețele locale în domenii mai mici de administrat pentru a reduce munca necesară configurării.

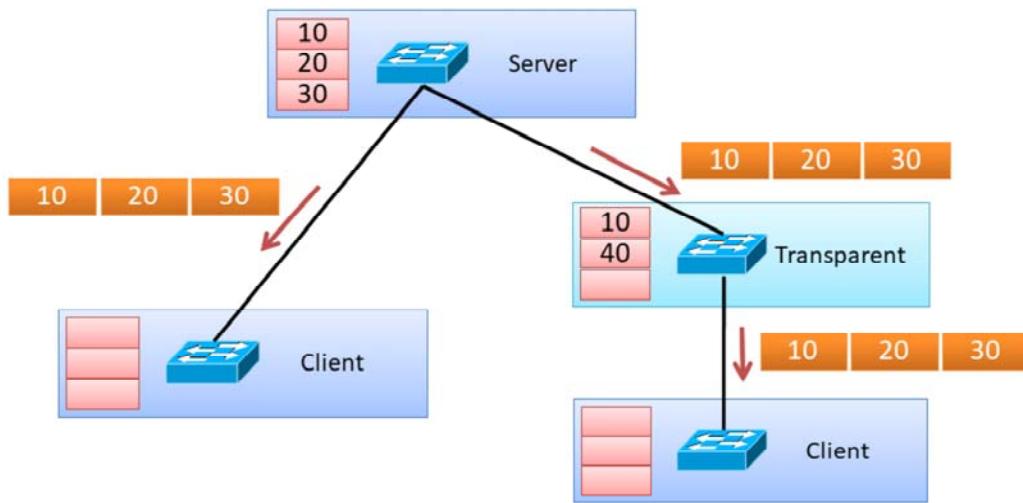
Un domeniu VTP este constituit dintr-o serie de switch-uri interconectate ce au același nume de domeniu.

Switch-urile ce rulează VTP se sincronizează numai dacă se află în același domeniu. Un switch poate fi membru al unui singur domeniu VTP. Până când nu se specifică un domeniu, pe un server VTP nu pot fi adăugate VLAN-uri sau informații pentru întreagă rețea deoarece mesajele VTP de sincronizare încep a fi transmise numai odată ce switch-ul face parte dintr-un domeniu.

Un server VTP include în pachetele trimise numele domeniului. Astfel toate switch-urile ce vor primi pachetul și nu se află deja într-un domeniu VTP își vor asocia domeniul semnalizat.

Moduri VTP

- 3 moduri de funcționare



98

Switch-ul în modul Server este cel care conține configurația ce va fi adăugată pe switch-urile aflate în mod Client.

Switch-urile ce se află în modul Transparent își păstrează configurația VLAN-urilor local, nu și-o sincronizează cu nici un alt switch din topologie. El participă în VTP doar prin transmiterea mesajelor VTP primite mai departe pe liniile de trunk.

După cum se vede în imagine switch-ul în modul Server conține VLAN-urile 10, 20 și 30. După sincronizarea VTP, switch-urile aflate în mod Client vor avea configurații identice în timp ce switch-ul aflat în mod Transparent va cunoaște în continuare doar VLAN-urile 10 și 40.

Modul server

- Modul default al unui switch
- Poate crea, șterge, redenumi VLAN-uri
- Configurează domeniul VTP pentru propagarea pe clienti
- Primește/trimite/procesează mesaje VTP
- Reține configurațiile în NVRAM

99

Pe un switch aflat în modul Server putem crea, modifica și șterge VLAN-uri pentru întregul domeniu VTP. Modul Server este modul implicit al unui Switch Cisco.

Servelele VTP își transmit configurațiile VLAN-urilor tuturor switch-urilor ce se află în același domeniu cu acesta și își sincronizează configurațiile cu celealte switch-uri în funcție de mesajele VTP trimise pe liniile de trunk. Switch-urile ce primesc mesajele VTP își compară Revision Number-ul cu cel al Server-ului VTP pentru a decide dacă trebuie să își sincronizeze informațiile cu acesta.

Configurațiile unui VTP Server sunt salvate deobicei în NVRAM dar în situații mai puțin comune îl putem găsi și în Flash. Ambele memorii sunt nevolatile, deci informațiile Server-ului se vor păstra și după o repornire a echipamentului.

Modul client

- Nu poate modifica domeniul VTP
- Nu poate crea/șterge/redenumi VLAN-uri
- Primește/trimite/procesează mesaje VTP
- Stochează informațiile despre VLAN-uri într-o bază de date din RAM -> la resetarea switch-ului, configurația se pierde

100

Pe un switch aflat în modul Client nu se pot crea, modifica sau șterge VLAN-uri. Informațiile despre VLAN-uri primite de un Client de la Server sunt salvate în vlan.dat ce nu este salvat în NVRAM. Din această cauză switch-urile aflate în modul Client necesită mai puțină memorie decât switch-urile aflate în modul Server. Când un VTP Client este repornit, el trimite un mesaj Server-ului pentru a primi configurațiile despre VLAN-uri.

Un Switch aflat în modul Client își actualizează informațiile despre VLAN-uri comparând Revision Number-ul său cu cel primit de la Server. Dacă valoarea Revision Number-ului său este mai mică decât cea din mesajul primit de la Server el își va resincroniza informațiile cu acesta.

Modul transparent

- Poate administra VLAN-uri – acestea au semnificație locală
- Transmite mai departe mesajele VTP, însă nu le procesează
- Nu-și va sincroniza niciodată baza de date cu cea a serverelor sau a clientilor
- Salvează configurațiile în NVRAM

101

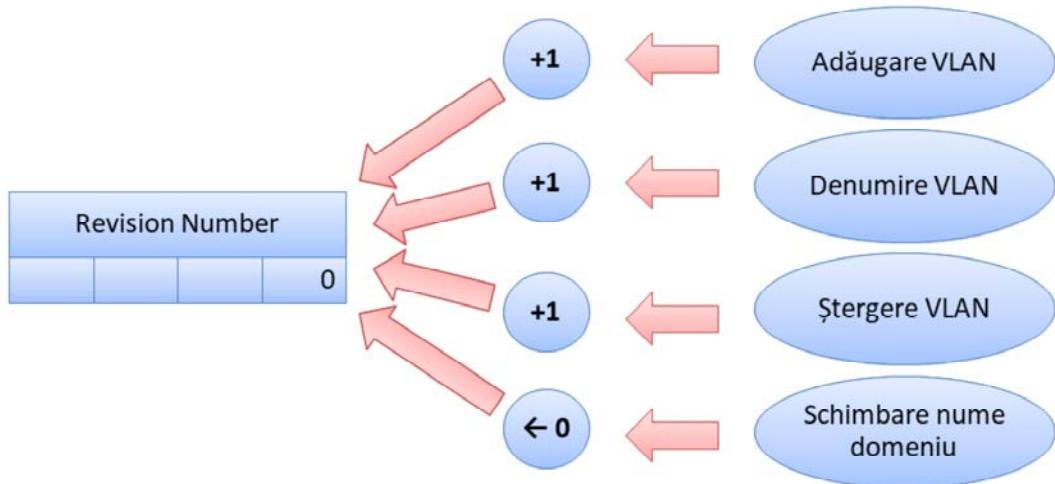
Un switch aflat în modul Transparent trimite mesajele VTP primite, pe legături trunk către alte switch-uri din rețea. Switch-urile aflate în mod VTP Transparent nu își partajează configurațiile despre VLAN-uri cu nici un alt Switch.

Un switch în mod Transparent se configurează cel mai adesea atunci când acesta are configurate VLAN-uri ce vrem să aibă numai semnificație locală și nu vrem să poată fi accesibile de oriunde din rețea.

În cazul unui switch Transparent configurațiile sunt stocate în NVRAM.

Revision Number

- Informează cât de actuală este configurația VLAN-urilor



102

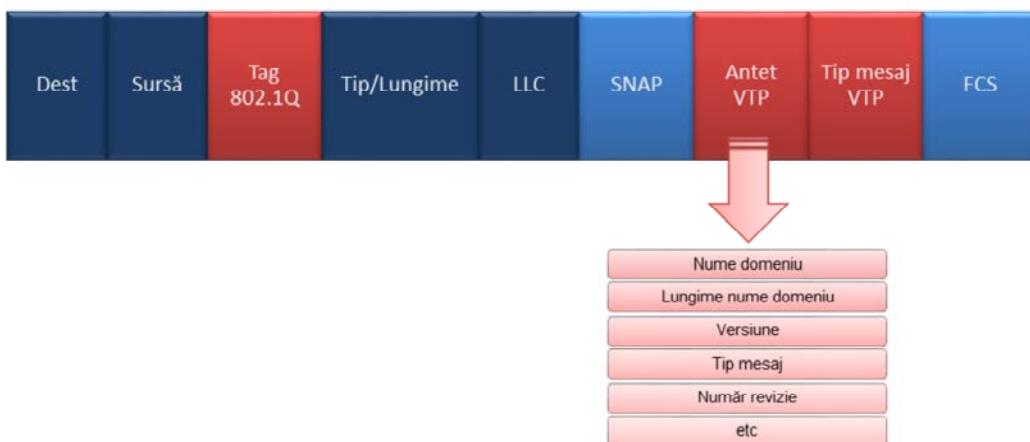
Revision Number-ul VTP este un număr format din 32 de biți ce reprezintă actualitatea configurației unui switch ce rulează VTP. Când un VLAN este adăugat, sters sau modificat, Revision Number-ul este incrementat cu 1.

La schimbarea unui domeniu VTP, Revision Number-ul nu este incrementat ci este resetat la valoarea inițială 0.

Revision Number-ul determină dacă informațiile de configurare primite sunt mai actuale decât cele salvate pe switch în acel moment. În funcție de acesta, switch-ul determină dacă își resincronizează informațiile.

Format mesaje VTP (1)

- Folosește cadre VTP



103

Mesajele VTP transmit numele domeniului VTP și schimbările de configurație ale VLAN-urilor switch-urilor ce fac parte din același domeniu VTP.

Frame-ul VTP este inserat într-un pachet de date Ethernet căruia î se adaugă un 802.1q trunk frame tag.

Câmpul Destinație conține adresa 01-00-0C-CC-CC-CC care este adresa multicast de nivel 2 prin care se transmit cadrele VTP.

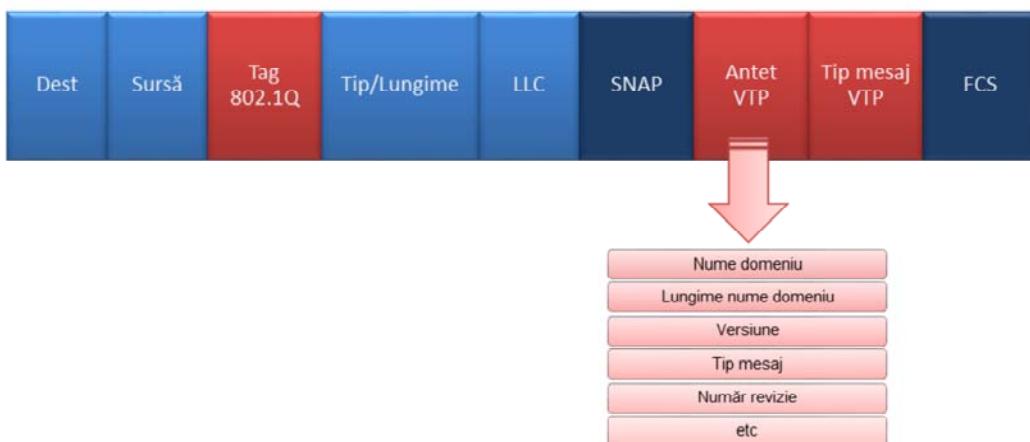
Câmpul Sursă conține MAC-ul switch-ului ce transmite mesajul.

Tag-ul 802.1q este tag-ul adăugat la transmiterea datelor pe o linie de tip trunk.

Câmpul LLC (Link Layer Control) sub-nivelul din partea de sus a nivelului Legătură de date conține un DSAP (Destination Service Access Point) și un SSAP (Source Service Access Point) cu valoarea setată AA ce reprezintă encapsulare SNAP.

Format mesaje VTP (2)

- Folosește cadre VTP



104

Câmpul SNAP (Subnetwork Access Protocol) conține un OUI (Organization Unique Identifier) cu valoarea 00000c în cazul switch-urilor Cisco și un PID cu valoarea 2003 pentru VTP. Protocolul SNAP specifică metoda standard de encapsulare a pachetelor IP și ARP în rețelele IEEE.

Antetul VTP diferă în funcție de tipul de mesaj VTP (Summary, Subset și Request) dar conține: Domain Name, Domain Name Length, Version, Configuration Revision Number.

Câmpul Tip mesaj VTP conține unul dintre cele 3 tipuri de mesaje folosite de protocol.

Câmpul de la final, FCS-ul, asigură integritatea pachetelor primite.

Tipuri de mesaje VTP

Summary

- Trimise la fiecare 5 minute de server sau client
- Trimise imediat ce a avut loc o schimbare
- Conține domeniul, numărul de revizie și alte detalii VTP

Subset

- Conține informație despre VLAN-uri
- Trimis dacă:
 - se adaugă sau șterge un VLAN
 - se suspendă sau activează un VLAN
 - se redenumește un VLAN

Request

- Cerere de mesaj Summary și Subset
- Trimis dacă:
 - s-a schimbat numele domeniului VTP
 - switch-ul a primit un mesaj Summary cu numărul de revizie mai mare

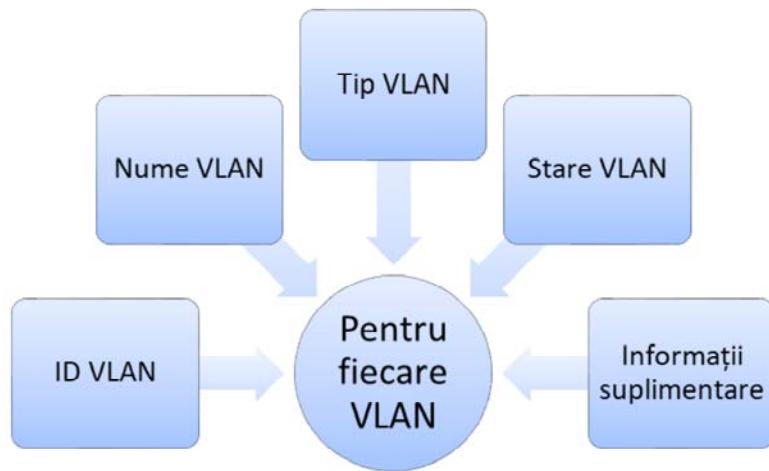
105

VTP poate trimite 3 tipuri de mesaje: Summary, Subset și Request fiecare cu funcția sa specifică.

Mesajele de tip Summary conțin: numele domeniului VTP, ultimul switch ce a modificat Revision Number-ul, timpul la care acesta a fost modificat, MTU (Maximum Transfer Unit), mărimea numelui domeniului VTP, un hash MD5 al parolei VTP dacă aceasta a fost setată, Revision Number-ul și versiunea de VTP folosită (1, 2 sau 3). Mesajele de tip Subset conțin în afară de numele domeniului și Revision Number, informații despre fiecare VLAN în parte. Mesajele de tip Subset sunt trimise dacă se adaugă, șterge, suspendă, activează sau redenumește un VLAN.

Mesajele de tip Request reprezintă cereri de mesaje Summary și Subset și sunt trimise dacă s-a schimbat numele domeniului VTP sau dacă Switch-ul a primit un mesaj cu un Revision Number mai mare decât al său.

Mesaje VTP Subset

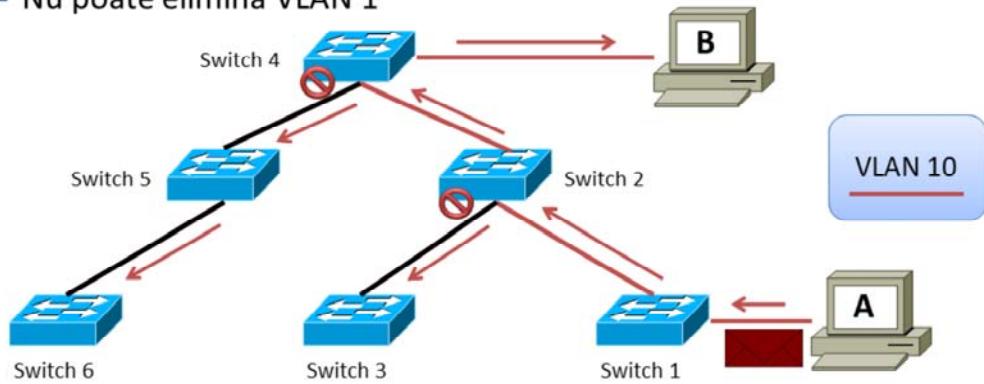


106

Mesajele de tip VTP Subset conțin informații despre fiecare VLAN și includ față de mesajul de tip Summary un câmp numit Seq-number. Acest câmp reprezintă numărul secvenței dintr-un pachet primit, de tip Summary, ce declanșează o resincronizare. Informațiile specifice despre VLAN-uri cuprind: numele VLAN-ului, tipul VLAN-ului, starea VLAN-ului și id-ul VLAN-ului.

VTP Pruning

- Previne trimitera pachetelor inutile pe anumite VLAN-uri de pe trunk-uri
- Nu poate elimina VLAN 1



107

VTP Pruning previne trimitera pachetelor inutile de broadcast de la un VLAN pe toate liniile de trunk dintr-un domeniu VTP. VTP pruning permite switch-urilor să negocieze ce VLAN-uri sunt acceptate la capătul trunk-urilor și astfel să oprească VLAN-urile ce nu vor fi niciodată folosite. VTP Pruning este implicit activat.

În imagine observăm că dacă VTP Pruning ar fi dezactivat, un pachet broadcast trimis de stația A pentru VLAN 10 ar ajunge și în switch-urile 3,5 și 6 deși acestea nu au la rândul lor nici o stație conectată în VLAN 10. Folosind VTP Pruning switch-urile scot automat VLAN-ul 10 de pe porturile pe care acesta nu este necesar astfel reducând traficul inutil de pe trunk-uri.

Configurare VTP (1)

- Configurare domeniu

```
ServerSW(config)# vtp domain cisco
```

- Configurare versiune

```
ServerSW(config)# vtp version 1
```

- Verificare status vtp

```
ServerSW# show vtp status
```

108

Pentru a configura serviciul de VTP trebuie mai întâi să se stabilească un nume de domeniu pe care îl vom seta cu ajutorul comenzi **vtp domain *domain_name***.

Putem folosi două versiuni VTP, a doua fiind cea mai utilizată deoarece realizează și verificări de consistență. Un switch în modul Transparent care folosește versiunea 2 nu va verifica numele de domeniu în momentul când transmite mai departe pachetele VTP. Configurarea versiunii de VTP se face cu comanda **vtp version *number***.

În cazul în care există VLAN-uri Token Ring, va trebui să setăm versiunea 2 de VTP datorită suportului oferit de aceasta. Modificarea versiunii de VTP nu va implica repornirea switch-ului.

În modul implicit versiunea VTP este versiunea 1.

Configurare VTP (2)

- Trecere în mod client

```
ClientSW(config)# vtp mode client
```

109

Pentru configurarea modului VTP, pe un switch se folosește comanda **vtp mode server/client/transparent** din modul global de configurare.

În modul Server (modul implicit) al VTP-ului, utilizatorul poate crea,修改, șterge VLAN-uri și poate specifica alți parametrii de configurare, precum versiunea de VTP, activarea VTP Pruning și domeniul. Serverele VTP anunță configurațiile VLAN-urilor sale către switch-urile aflate în același domeniu VTP. În acest mod de operare, switch-urile își pot sincroniza datele despre VLAN-urile vecine.

Modul VTP Client are același comportament ca și modul Server cu o singură observație: nu se pot crea, modify sau șterge VLAN-urile sub acest mod.

Switch-urile configurate în mod transparent nu participă în VTP. Pachetele VTP sunt trimise mai departe către celelalte switch-uri din domeniu.

Verificare VTP (1)

```
ClientSW# show vtp status

ClientSW#show vtp status
VTP Version : 2
Configuration Revision : 3
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
VTP Operating Mode : Client
VTP Domain Name : cisco
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xC0 0x74 0x46 0xB8 0xE4 0x0C 0x5A 0x0A
Configuration last modified by 0.0.0.0 at 3-1-93 00:08:23
```

110

Pentru verificarea VTP se folosește comanda **show vtp status**. Aceasta oferă informații cu privire la versiunea VTP folosită, numărul de revizie curentă de pe switch, numărul de VLAN-uri suportate, numărul de VLAN-uri existente pe switch, modul de operare VTP (server, client sau transparent), numele de domeniu.

Vizualizând în paralel output-ul acestei comenzi pe mai multe echipamente, se pot repera ușor neconcordanțele și greșelile de configurare VTP.

În exemplul de mai sus, versiunea VTP este 2, numărul de revizie este 3, numărul de VLAN-uri existente pe switch este 8, numele de domeniu din care face parte switch-ul este Cisco și switch-ul este Client pentru acel domeniu.

Verificare VTP (2)

- Informații despre cadrele schimbate

```
ClientsW# show vtp counters
```

```
VTP statistics:  
Summary advertisements received : 4  
Subset advertisements received : 1  
Request advertisements received : 0  
Summary advertisements transmitted : 4  
Subset advertisements transmitted : 2  
Request advertisements transmitted : 0  
Number of config revision errors : 0  
Number of config digest errors : 0  
Number of VI summary errors : 0
```

111

Cu ajutorul comenții **show vtp counters** din modul enable se pot vizualiza statistici cu privire la pachetele de VTP trimise /primite și tipul lor. Aceste statistici ar trebui să fie o dovedă în plus că VTP-ul funcționează corect.

Securizare VTP și VTP Pruning

- Configurare parolă

```
ServerSW(config)# vtp password cisco123
ServerSW(config)# vtp pruning
```

```
ClientSW(config)# vtp password cisco123
```

112

Se poate configura autentificarea pachetelor VTP. În acest caz, fiecare switch (fie că este Server sau Client) trebuie să aibă identic hash-ul rezultat în urma configurării parolei de autentificare. Configurarea parolei se face tot din modul de configurare, cu comanda **vtp password password**.

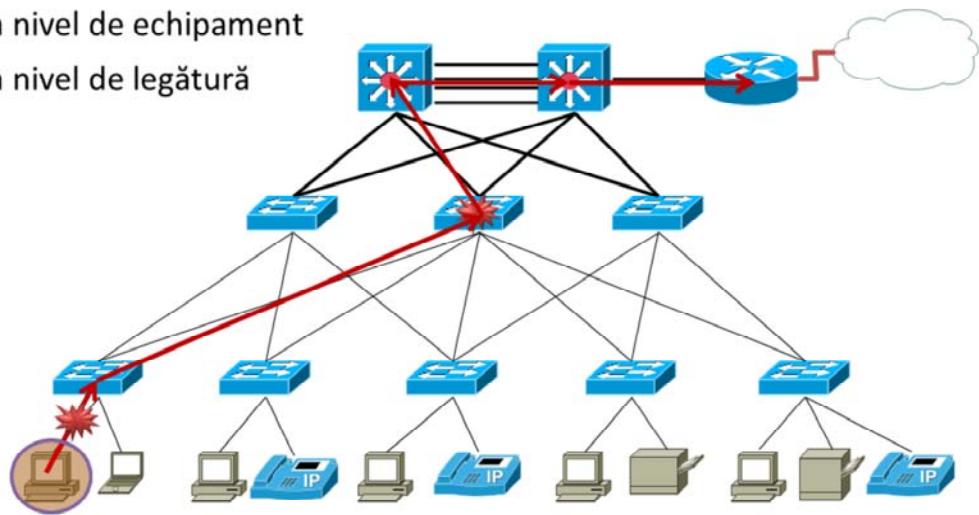
VTP, ca și funcționalitate, se asigură că fiecare switch din domeniu cunoaște VLAN-urile configurate. De multe ori însă, VTP generează trafic inutil. Orice broadcast sau unicast a cărui adresă nu este cunoscută, va fi trimis pe toate porturile switch-ului din VLAN-ul respectiv. Fiecare switch din acel VLAN va procesa broadcast-ul chiar dacă nu există utilizatori ai VLAN-ului respectiv conectați la switch. VTP pruning are rolul de a elimina traficul inutil din cadrul rețelei.

VTP Pruning se activează cu ajutorul comenzi **vtp pruning**.

Capitolul 5: STP

Redundanță

- La nivel de echipament
- La nivel de legătură



114

Modelul de design ierarhic combate problemele ce apar în topologiile plate. Una dintre ele este necesitatea de a asigura redundanță. Redundanța la nivelul 2 îmbunătățește funcționarea rețelei prin implementarea unor căi alternative prin rețea. Acest lucru este realizat prin adăugarea de noi echipamente (cu aceleași funcționalități) și de noi cabluri ce le interconectează. A avea mai multe drumuri către aceeași destinație într-o rețea, permite ca în cazul în care una dintre legături pică rețeaua să funcționeze în continuare la parametrii optimi pe una dintre căile alternative.

Odată ce un business devine din ce în ce mai dependent de o rețea, rezistența rețelei la defecte devine din ce în ce mai importantă. Redundanța este soluția pentru a asigura toleranță la defecte a unei rețele.

Bucle la nivelul 2

- Mecanism de protecție în cazul apariției unei bucle la nivelul 2
 - nu există
 - probleme ce pot apărea:
 - broadcast storms
 - copii multiple ale unui cadru
 - inconsistență tabelei CAM
- Mecanism de prevenire a buclelor la nivelul 2
 - Spanning Tree Protocol (STP)

115

Funcționarea permanentă a serviciilor de rețea a devenit unul din cele mai importante obiective pentru rețele enterprise ce se bazează în principal pe o rețea multi-layer switched pentru a îndeplini cerințele companiei. O metodă de a asigura HA (High Availability) este de a realiza redundanță la nivelul 2 al stivei OSI, al echipamentelor de rețea, modulelor și link-urilor de-a lungul întregii rețele.

Redundantă la nivelul Legătură de date introduce bucle de nivelul 2 al stivei OSI, unde pachetele sunt transmise la nesfârșit între echipamente. Acestea pot avea un efect devastator asupra întregii rețele.

Mentionăm câteva probleme ce pot apărea în cazul buclelor de nivelul 2: Broadcast storms, copii multiple ale unui cadru și inconsistență tabelei CAM.

Un mecanism de identificare și prevenire a acestor bucle este Spanning Tree Protocol.

Spanning Tree Protocol

- Standard IEEE 802.1d (1990)
- Rulează **Spanning Tree Algorithm** pe fiecare switch
- Generează o topologie logică fără bucle
 - se închid porturi astfel încât legăturile să se mapeze pe arborele general

116

În 1990, IEEE a publicat primul standard pentru acest protocol și anume 802.1D bazat pe algoritmul realizat de Perlman. Variantele următoare au fost lansate în 1998 și 2004 incorporând diferite extensii.

STP rulează pe fiecare switch din topologie un algoritm Spanning Tree Algorithm generând astfel o topologie logică fără bucle de nivel 2. STP permite realizarea de topologii cu căi redundante, fără apariția efectelor nedorite a buclelor active în rețea.

Protocolul STP forțează anumite porturi să intre într-o stare de standby astfel încât aceste porturi să nu asculte, trimită sau „flood”-eze pachete. Efectul acestor măsuri este faptul că va exista o singură cale activă de-a lungul întregii topologii.

Dacă vor exista probleme cu calea activă generată, STP va restabili conectivitatea automat reactivând unul din link-urile dezactivate anterior, dacă o asemenea cale există.

Spanning Tree Algorithm

- Rețeaua de switch-uri este un graf conex cu cicluri
- Fiecare switch din rețea este un nod în graf
 - fiecare switch are un ID unic (**bridge ID**)
- Fiecare legătură este un arc nedirecționat cu cost
 - costul este invers proporțional cu viteza legăturii
- Un switch este considerat rădăcină (**root bridge**)
- Arborele generat va fi arborele minim de acoperire
- Fiecare switch va avea drumul minim către rădăcină

117

STP folosește Spanning Tree Algorithm (STA) pentru a determina ce porturi din rețea trebuie să fie configurate să nu accepte trafic pentru a preveni apariția buclelor. STA alege un singur switch din cadrul rețelei ca Root Bridge și îl folosește ca punct de referință în calcularea căilor optime și fără bucle.

Fiecare switch ce participă în procesul de STP este un nod în graful calculat de STA și îi va fi asociat un Bridge ID unic. Protocolul va face schimb de pachete BPDU (Bridge Protocol Data Unit) pentru a determina cel mai mic Bridge ID în vederea alegerii Root Bridge-ului.

Bridge ID

- Fiecare switch are un ID unic (BID)
- Valoare pe **64 biți**
 - 16 biți **prioritatea**
 - 48 biți **adresa MAC**
- Prioritatea este implicit 32768
- Switch-ul cu BID-ul cel mai mic este root bridge-ul



118

Protocolul STP necesită ca fiecare switch din rețea să aibă asignat un **BID (Bridge ID)** unic. În versiunea inițială standardizată, în 802.1D, BID-ul era compus din 2 câmpuri: **Prioritate** și **MAC**, iar toate VLAN-urile erau reprezentate de un arbore STP comun.

Switch-ul cu **cel mai mic** BID devine Root Bridge.

Prioritatea (Bridge ID) este un câmp de o dimensiune de 16 biți ce stochează prioritatea switch-ului. Valoarea implicită a priorității este 32768, valoare de mijloc ce poate fi specificată. Datorită adăugării câmpului de VLAN ID în cadrul priorității, pentru PVST+ și PVRST+ dimensiunea câmpului ce specifică prioritatea se reduce la 4 biți. Din această cauză, în noul format, valoarea pentru prioritate se incrementează cu 4096.

Adresa MAC este un câmp de 48 de biți ce memorează adresa de Layer 2 a switch-ului respectiv.

Link cost

Viteză legătură	802.1D (1990)	802.1D (1998)	802.1t (2001)
4 MB/s	-	250	5,000,000
10 MB/s	100	100	2,000,000
16 MB/s	-	62	1,250,000
100 MB/s	10	19	200,000
1 GB/s	1	4	20,000
2 GB/s	-	3	10,000
10 GB/s	1	2	2,000

119

În momentul în care a fost ales Root Bridge-ul pentru o instanță de STP, algoritmul protocolului (STA) începe procesul de determinare a căii optime dinspre fiecare destinație din domeniul de broadcast către acesta.

Costul implicit al fiecărei căi este determinat de viteza la care operează porturile folosite în calea respectivă. Dintre cele mai importante valori amintim: porturile cu o viteza de 10GB/s ce au costul 2 , porturile cu viteza de 1 GB/s ce au costul 4, porturile cu viteza de 100 MB/s FastEthernet ce au costul 19 și porturile de 10 MB/s Ethernet ce au costul 100.

BPDU

- Mesaje trimise între switch-uri
 - Bridge Protocol Data Unit (BPDU)
 - trimise la fiecare 2 secunde
 - multicast spre **01:80:C2:00:00:00**

2 Bytes	1 Byte	1 Byte	1 Byte	8 Bytes	4 Bytes	8 Bytes	2 Bytes	2 Bytes	2 Bytes	2 Bytes	2 Bytes
Protocol Identifier	Version	Message Type	Flags	Root ID	Cost to bridge	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay

120

Alegerea Root Bridge-ului pentru instanța de STP se realizează folosind pachete BPDU (Bridge Protocol Data Unit).

Frame-ul BPDU conține douăsprezece câmpuri distincte ce sunt folosite în cadrul procesului de STP pentru a determina Root Bridge-ul și căile optime spre acesta.

Primele 4 câmpuri din cadrul BPDU-ului identifică protocolul, versiunea, tipul mesajului și flag-uri de status.

Următoarele 4 câmpuri sunt folosite pentru a specifica Root Bridge-ul și costul căii spre acesta.

Ultimale 4 câmpuri sunt valori de timere ce determină cât de des trebuie trimise pachetele.

Porturi

- Tipuri de porturi:
 - **root ports**
 - porturile care duc spre root pe calea cu costul cel mai mic
 - unul pe fiecare switch non-root
 - **designated ports**
 - porturile care permit traficul
 - **non-designated ports**
 - porturile care blochează traficul

121

În continuare vom defini rolurile port-urilor unui switch ce este clasificat drept non – designated:

- Portul ce se găsește pe calea cea mai bună spre un Root Bridge se numește **Root Port**. Aceste porturi transmit datele mai departe către **Root Bridge**, iar adresa MAC a pachetelor primite pe acest port vor fi introduse în tabela CAM. Pe un switch Non – designated poate fi definit un singur Root Port.
- Porturile **Designated** există atât pe switch-uri Root Bridge cât și pe cele care nu sunt Root Bridge. Pentru switch-urile Root Bridge toate porturile acestuia sunt porturi Designated. Pentru switch-urile ce nu sunt Root Bridge, porturile Designated permit trecerea traficului. În cadrul unui segment de rețea un singur port poate fi Designated.
- Porturile **Non – designated** sunt porturile ce nu permit transmiterea și primirea datelor și nici nu permite învățarea de noi adrese MAC.

Etapele procesului de STP

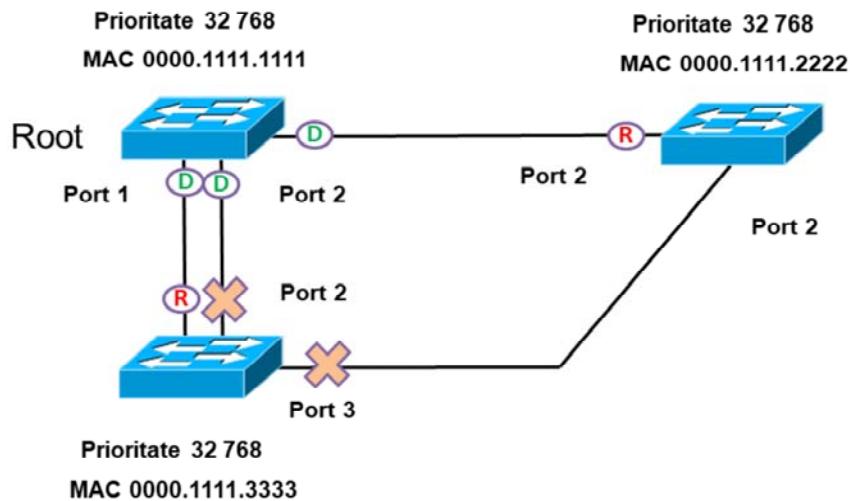
- Fiecare switch se consideră root bridge
- Se schimbă BPDU-uri și se alege un singur root bridge
- Se ia în considerare doar calea cea mai scurtă către root
- Se închid porturile care nu duc spre root pe calea cea mai scurtă

122

Procesul de STP este format din următorii pași:

- 1) Desemnarea unui Root Bridge: la început fiecare switch din rețea se consideră Root Bridge. Protocolul STP rulează un proces de determinare a unui singur switch Root Bridge în cadrul unui domeniu de broadcast. Toate porturile acestuia sunt porturi Designated.
 - 2) Selectarea Root Port-urilor: protocolul va stabili un singur Root Port pe fiecare switch ce nu a fost ales Root Bridge. Root Port-ul va fi calea de cost minim de la orice switch până la Root Bridge. Există posibilitatea să existe mai multe căi de cost egal, caz în care se va alege drept Root Port, portul cu ID-ul cel mai mic. Valoarea Port ID-ului este formată dintr-o prioritate ce poate fi configurată și numărul portului.
 - 3) Se aleg porturile Designated pe fiecare segment.
 - 4) Porturile rămase se închid (au rolul Blocked Port)
-
-
-
-
-

Exemplu Porturi



Stări Porturi în STP

- Un port face tranziția între mai multe stări

Stare port	Acțiune la nivel de Switch	Acțiune la nivel de Port
Disabled	Nu se acceptă nici un fel de trafic	Nu se transmit cadre Nu se transmit BPDU-uri
Blocking	Se primesc doar BPDU-uri	Nu se transmit cadre Se primesc BPDU-uri
Listening	Se construiește topologia STP	Nu se transmit cadre Se transmit BPDU-uri
Learning	Se construiește tabela de adrese MAC	Nu se transmit cadre Se învăță adrese MAC Se transmit BPDU-uri
Forwarding	Se transmite traficul normal	Se transmit cadre Se învăță adrese MAC Se transmit BPDU-uri

124

În starea **Disabled** portul nu va participa în procesul de STP și nu va transmite pachete și BPDU-uri.

Porturile aflate în starea **Blocking** sunt porturi non – designated și nu participă în trimiterea de pachete. Aceste porturi primesc BPDU-uri pentru a determina locația și ID-ul Root Bridge-ului și pentru a stabili rolurile fiecărui port al său (root, designated, nondesignated) în topologia finală.

Începând din momentul în care porturile ajung în starea **Listening**, STP-ul a determinat că aceste port-uri pot participa la schimbul de BPDU-uri și se începe construirea topologiei STP.

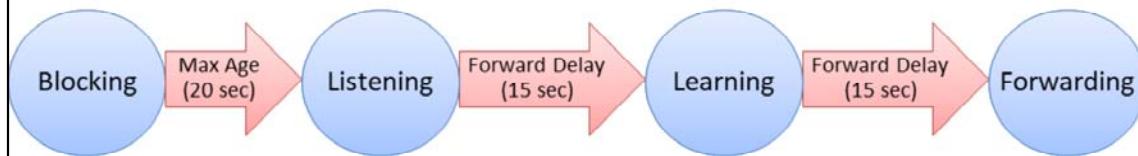
În starea **Learning**, portul se pregătește să participe în transmiterea de frame-uri și începe să își populeze tabela CAM.

Un port în starea **Forwarding** este considerat ca membru al topologiei active și va trimite frame-uri și BPDU-uri.

Timpi de tranziție

- Timere de tranziție

- stabilite de root bridge
- **Hello time:** 2 sec
- **Forwarding delay:** 15 sec
- **Max Age:** 20 sec



- timp total de convergență: 50 sec

125

Fiecare port din cadrul unui proces de STP va trebui să treacă prin stările menționate anterior. În următoarele rânduri vom specifica timpii de tranziție între stările amintite.

Portul va sta în starea Blocking timp de 20 de secunde , timpul implicit **Max Age**. În fiecare din stările următoare și anume Listening și Learning, porturile vor sta câte 15 secunde (Forwarding Delay).

Astfel timpul total de convergență este de 50 de secunde.

CST

- Common Spanning Tree
- O singură instanță de 802.1D
- Implementare pentru un singur VLAN

126

Protocolul CST (Common Spanning Tree) își asumă o singură instanță de STP pentru întreaga rețea indiferent de numărul de VLAN-uri existente. Datorită faptului că există o singură instanță, cerințele de memorie și de CPU sunt drastic micșorate în comparație cu variantele de STP apărute recent. Un dezavantaj al acestui protocol este faptul că fiind o singură instanță de STP va rezulta un singur arbore și un singur Root Bridge. Astfel tot traficul, indiferent din ce VLAN provine, va parcurge aceeași cale și poate duce la o transmitere suboptimală a datelor.

Deoarece procesul de convergență este moștenit de la standardul 802.1D, timpul de convergență este mare.

RSTP

- Rapid Spanning Tree Protocol
- IEEE 802.1w (1998)
- Timp mai bun de convergență: 3-5 secunde

127

Rapid Spanning Tree Protocol (RSTP) sau 802.1w este un protocol ce s-a lansat ca evoluție a protocolului STP, ce oferă timpi de convergență mult mai buni. Această versiune adresează multe din problemele de convergență, însă, datorită faptului că folosește tot o singură instanță de STP, nu a putut rezolva problemele legate de separarea arborilor STP în funcție de VLAN-uri. Pentru a micșora timpii de convergență, RSTP folosește mai multe resurse de memorie decât CST, însă diferențele sunt evidente: De la 50 de secunde CST la 3-5 secunde RSTP.

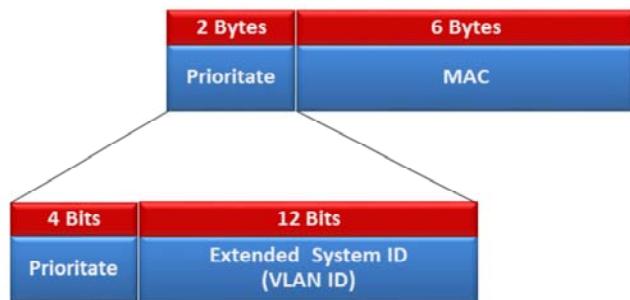
PVST/PVST+/RPVST+

- Proprietare Cisco
- Câte o instanță de STP pentru fiecare VLAN
- PVST
 - funcționează doar peste trunk-uri Cisco ISL
- PVST+
 - funcționează peste trunk-uri 802.1q
- RPVST+
 - Rapid PVST+
 - tempi de convergență similari cu RSTP

128

Per VLAN Spanning Tree Plus (PVST+) este o îmbunătățire a STP-ului ce oferă o instanță de STP pentru fiecare VLAN configurat în rețea. Fiecare instanță suportă PortFast, BPDU guard, BPDU filter, Root guard și Loop guard, noțiuni ce vor fi studiate în amănunt în cursurile de CCNP. Realizându-se o instanță pentru fiecare VLAN, numărul de resurse necesare crește (memorie și CPU), însă permite alegerea unui Root Bridge per VLAN. Timpul de convergență este asemănător cu 802.1D dar această convergență este per VLAN.

Identificarea VLAN-ului



129

Deoarece PVST+ și PVRST+, ambele fiind variațiuni ale protocolului STP, au nevoie de un arbore STP separat pentru fiecare VLAN, câmpul **Bridge ID**-ului trebuie să conțină și informații despre VLAN ID. Acest lucru este posibil prin refolosirea unei porțiuni din câmpul de prioritate pentru stocarea VLAN ID-ului.

MSTP

- IEEE 802.1s
- Extensie la RSTP pentru a putea folosi VLAN-uri

130

MST (Multiple Spanning Tree) este un standard IEEE inspirat din versiunile anterioare ale protocolului proprietar Cisco Multi-Instance Spanning Tree Protocol (MISTP). Implementarea celor de la Cisco asigură până la 16 instanțe de RSTP (802.1w) și combină mai multe VLAN-uri cu topologii fizice și logice într-o instanță comună de RSTP. Fiecare instanță suportă PortFast , BPDU guard, BPDU filter, Root guard și Loop guard.

Configurări globale

- Mod de funcționare

```
spanning-tree mode pvst | rapid-pvst | mst
```

- Setare prioritate manual

```
spanning-tree vlan VLAN_NO priority PRIORITY
```

- Setare prioritate automat

```
spanning-tree vlan VLAN_NO root primary  
spanning-tree vlan VLAN_NO root secondary
```

131

Una din comenzi foarte importante în implementarea STP-ului în infrastructura noastră este **spanning-tree mode pvst | rapid-pvst | mst** cu ajutorul căreia putem nominaliza tipul de STP.

În cazul în care dorim să influențăm alegerea Root Bridge-ului, pe anumite VLAN-uri putem folosi comenziile **spanning-tree vlan VLAN_NO root primary** și **spanning-tree vlan VLAN_NO secondary**.

Dacă avem nevoie de mai mult control pentru setarea Root Bridge-ului avem la dispoziție comanda **spanning-tree vlan VLAN_NO priority** ce ne permite să setăm prioritatea în multipli de 4096.

Configurări pe interfață

- Cost legătură

```
spanning-tree cost COST
```

- Activare portfast

```
spanning-tree portfast
```

132

Datorită faptului că tehnologia se dezvoltă foarte rapid, trebuie să ne aşteptăm ca valorile asociate costului porturilor să se schimbe pentru a acomoda viteze din ce în ce mai mari.

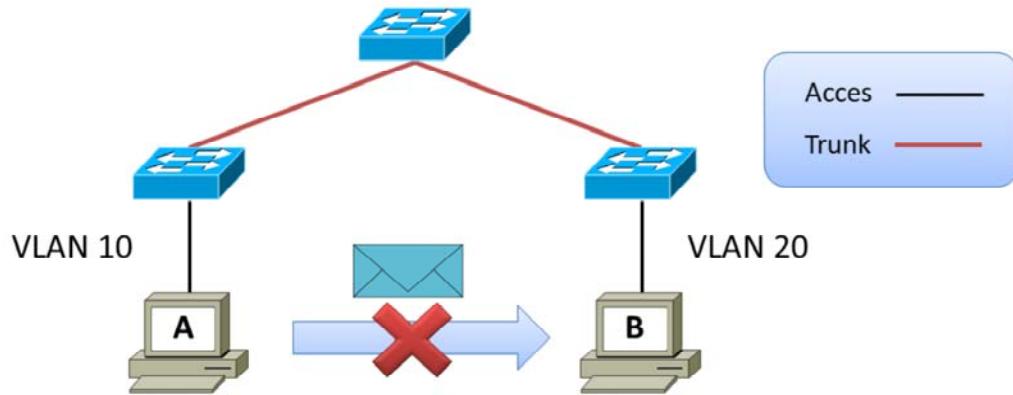
Cu toate că porturile au definite valori implicate, în momentul initializării switch-ului, aceste valori pot fi modificate, permitând administratorului să aibă control asupra căii ce este aleasă de procesul de STP. Comanda cu ajutorul căreia se realizează modificarea, este **spanning-tree cost COST**.

Există cazuri în care interconectăm echipamente terminale la switch, precum servere, imprimante, ce duc la limitarea posibilității de realizare a unei bucle de nivel 2. Aceste porturi pot fi setate să nu ruleze algoritmul de STP, micșorând astfel timpul până când intră în starea de forwarding.

Comanda folosită este **spanning-tree portfast** executată din prompt-ul interfeței.

Capitolul 6: Rutare Inter-VLAN

Comunicația inter-VLAN



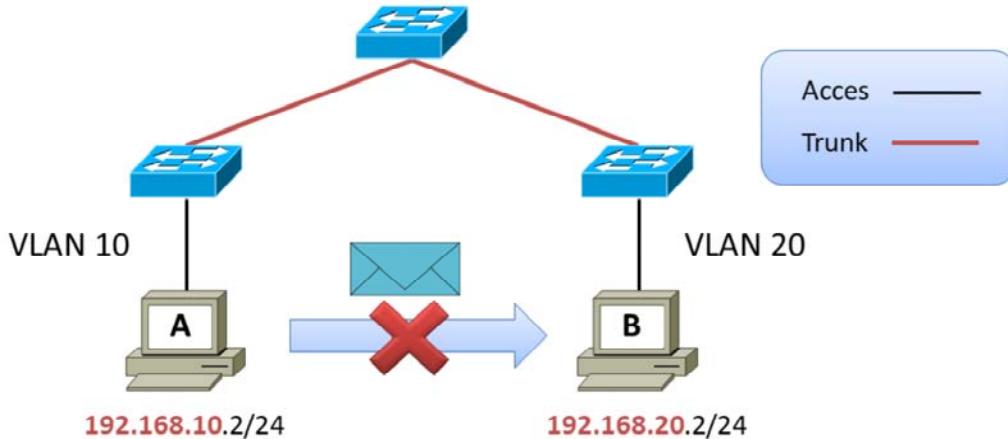
134

După cum am precizat în capitolele anterioare, VLAN-urile realizează o “împărțire” a rețelelor și o separare a traficului în cadrul nivelului 2 al stivei OSI. Mai mult, host-urile care aparțin unor VLAN-uri diferite se află și în domenii de broadcast diferenți (deoarece o asociere corectă între acestea trebuie să fie bijectivă), deci vor fi separate și la nivelul 3 al stivei OSI.

În concluzie, este mai mult decât evident faptul că nu va putea avea loc în mod implicit nici un fel de comunicație între echipamentele din VLAN-uri diferenți. Soluția o reprezintă rutarea Inter-VLAN, prezentată în paginile următoare.

Soluție folosind switch-uri L2

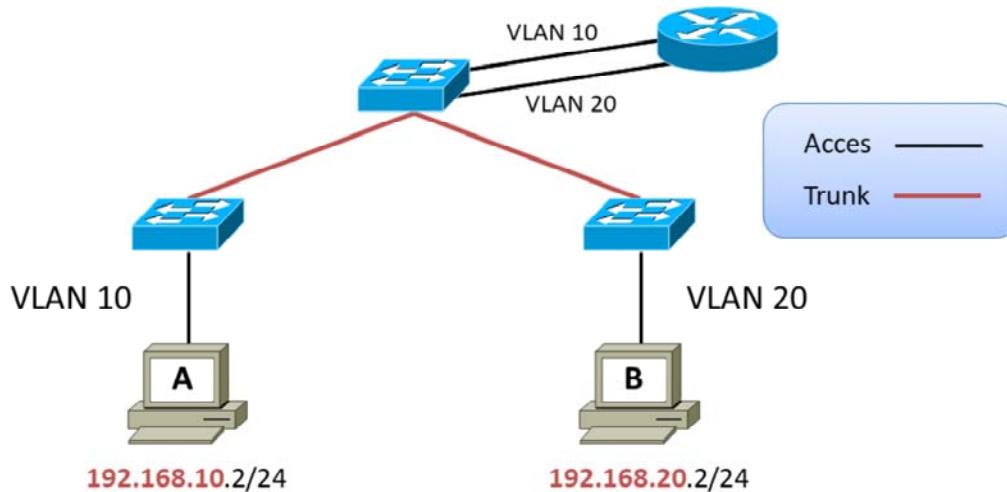
- Insuficiente, sunt necesare echipamente de nivel 3



135

Folosirea doar a echipamentelor care funcționează la nivelul 2 din stiva OSI nu este suficientă în vederea asigurării conectivității între hosturile din VLAN-uri diferite, deoarece, deși asigură toate mecanismele necesare nivelului 2, nu pot prelucra informațiile aflate la nivelul 3. În consecință, acestea nu pot efectua rutarea pachetelor între rețelele asociate fiecărui VLAN, necesitatea folosirii unui echipament de nivel 3 devenind evidentă.

Soluții folosind rutere: legături multiple



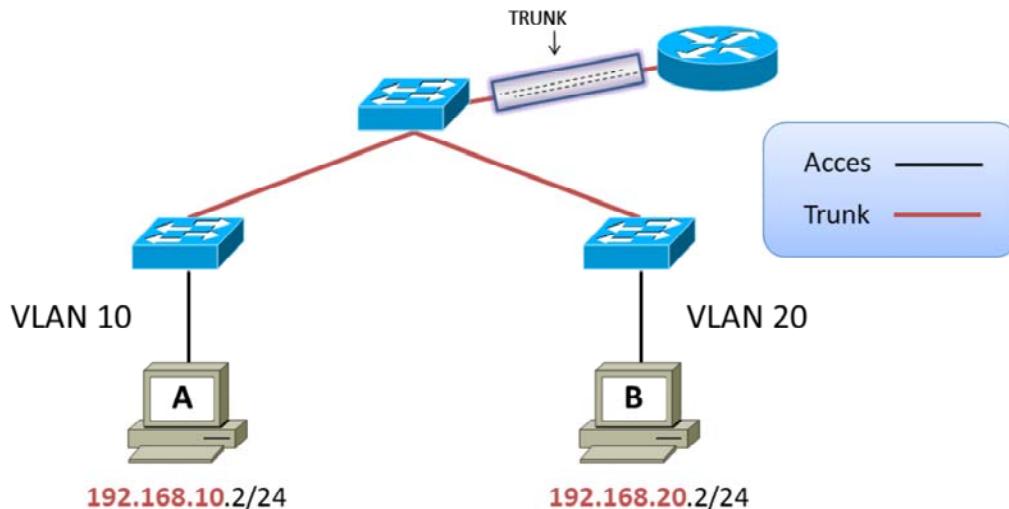
136

O soluție simplă care ar permite host-urilor din VLAN-uri diferite să comunice între ele presupune folosirea unui router, conectat la un switch prin care “trec” VLAN-urile aferente. Conexiunea se poate realiza folosind câte o legătură de tip acces pentru fiecare VLAN în parte, fiecare port de pe router primind o adresă din rețeaua asociată acestuia. Astfel, rutarea Inter-VLAN va avea loc natural, router-ul introducând automat aceste rețele în tabela sa de rutare drept “directly connected”.

Avantajul oferit de acest mod de conectare este faptul că lărgimea de bandă a fiecărei legături switch – router este folosită doar pentru traficul de la / către un singur VLAN, oferind performanțe ridicate.

Dezavantajele constau în numărul mare de porturi necesare atât pe switch, dar mai ales pe router și de faptul că pe legăturile aparținând unor VLAN-uri cu un necesar de trafic mai mic, lărgimea de bandă rămasă este nefolosită.

Soluții folosind rutere: router-on-a-stick



137

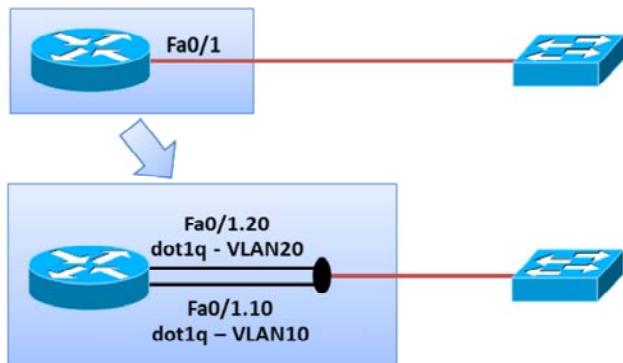
Pentru a evita dezavantajele metodei de conectare prezentate anterior se poate folosi o singură legătură fizică, dar configurață în modul trunk între switch și ruter. Această variantă presupune configurarea și a interfeței ruterului în modul trunk și, suplimentar, definirea de subinterfețe (prezentate în pagina următoare) pe aceasta, câte una pentru fiecare VLAN în parte.

Rutarea va funcționa tot de la sine, deoarece ruterul tratează subinterfețele similar interfețelor, introducând automat rețelele asociate în tabela sa de rutare drept “directly connected”. Avantajul este dat de numărul redus de porturi ale ruter-ului necesare conexiunii fizice.

Dezavantajul îl reprezintă faptul că lătimea de bandă disponibilă pe fiecare legătură de tip trunk este împărțită de VLAN-urile care îl folosesc, rezultând o lătimea de bandă per VLAN mai mică decât în cazul conectării folosind de legături individuale pentru fiecare VLAN.

Subinterfețe

- Mai multe adrese IP și încapsulări configurate pe aceeași interfață fizică
- Configurează pe o interfață conectată la un port **trunk**



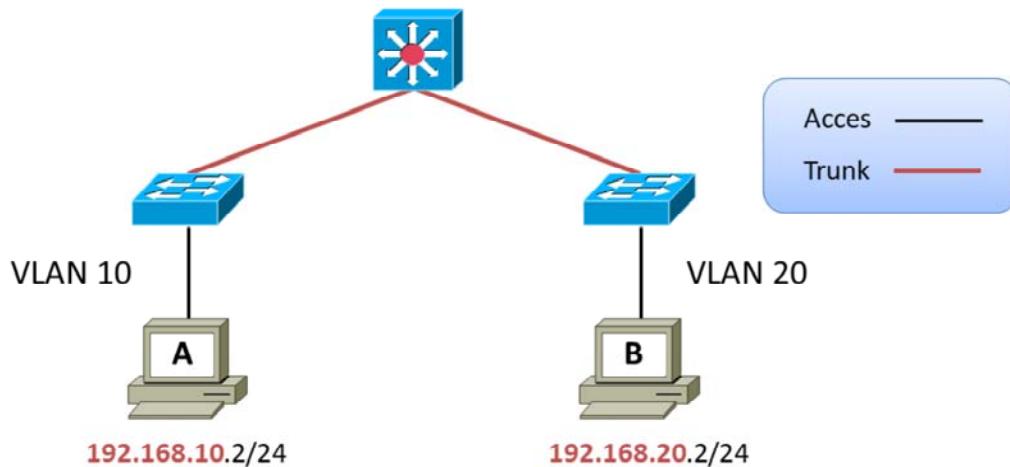
138

O subinterfață este o interfață virtuală (“software”) asociată unei interfețe fizice, și care are rolul de a facilita rutarea “logică” a pachetelor aparținând unor VLAN-uri diferite primite pe aceeași interfață fizică (trunk). Subinterfețele se configurează în același mod ca interfețele, fiecare având asociate câte o adresă IP din VLAN-ul căruia aparține, iar din punct de vedere funcțional nu există diferențe între cele două.

Practic, folosirea subinterfețelor permite unei interfețe fizice a router-ului să aparțină mai multor VLAN-uri simultan și totodată să separe traficul aferent acestora la traversarea conexiunii trunk dintre router și switch.

CCNP Preview: Switch L3

- Who needs routers anymore? L3 Switch ...

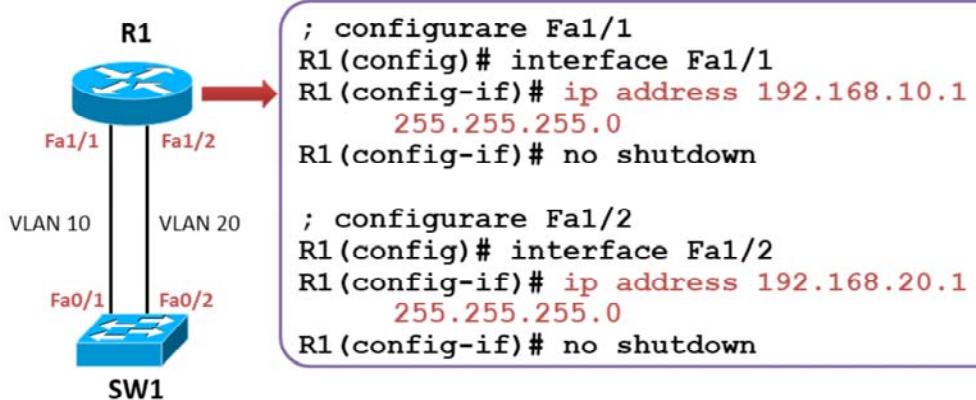


139

Există și posibilitatea evitării folosirii unui router dedicat doar rutării Inter-VLAN prin folosirea unui switch de nivel 3 în stiva OSI în locul switch-ului de nivel 2. Prin activarea funcțiilor de rutare prezente (dar dezactivate în mod implicit) în orice switch de nivel 3 putem asigura comunicarea între host-uri din VLAN-uri diferite, fără a mai fi necesară cumpărarea de echipamente suplimentare (routere) și fără a crește complexitatea configurării acestora.

Acest subiect interesant (printre multe altele) este tratat pe larg în cadrul cursurilor de CCNP.

Configurare ruter cu legături multiple



140

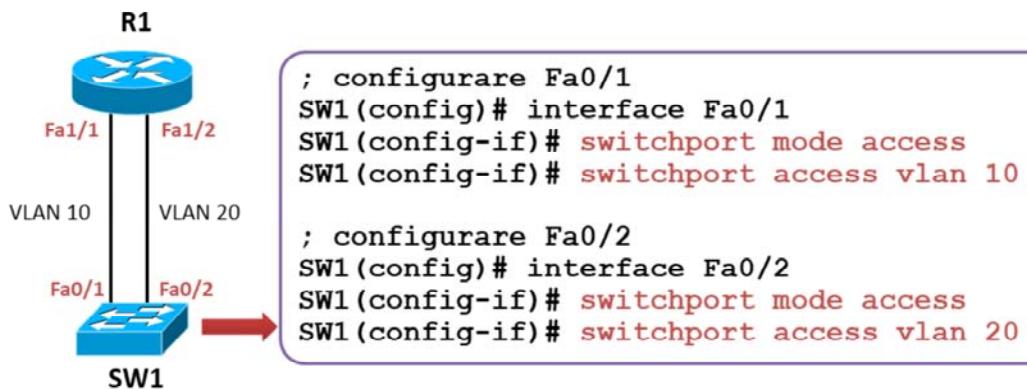
Datorită faptului că VLAN-urile segmentează domenii de broadcast, vom avea nevoie de un echipament ce operează la nivelul 3 al stivei OSI pentru a putea ruta traficul între ele.

Pentru a putea ruta pachetele între VLAN-uri, ruterele trebuie să suporte rutare de tip ISL sau 802.1Q. Cel mai puțin costisitor ruter ce are aceste funcționalități face parte din seria 2600, model EOL (End of Life). Pentru rutarea pachetelor între VLAN-uri este minim recomandată seria 2800 ce suportă numai 802.1Q, CISCO depărându-se de protocolul ISL.

O primă variantă ar fi folosirea ruterului cu interfețe pentru fiecare VLAN setat pe switch ca în exemplul de mai sus.

Configurarea ruterului constă în simpla configurare a interfețelor cu IP-urile asociate VLAN-urilor.

Configurare ruter cu legături multiple



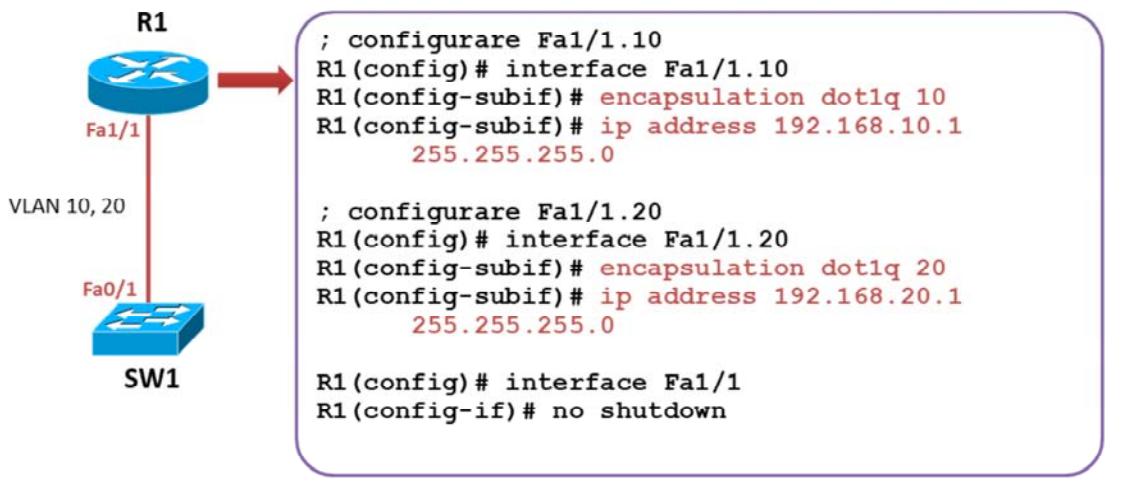
141

Pe switch vom configura fiecare legătură a acestuia ce se conectează la ruter în mod access cu ajutorul comenzi **switchport mode access**. Următorul pas constă în asocierea fiecărui VLAN pe o interfață legată la ruter. **Atenție** la adresele IP ale subrețelelor și implicit la spațiul alocat VLAN-urilor. O setare incorectă a VLAN-urilor pe interfețele switch-ului către ruter are drept consecință lipsa conectivității.

În această configurație, fiecare interfață a ruterului devine default gateway pentru echipamentele terminale ale VLAN-ului asociat.

Această soluție poate fi utilizată în cazul în care avem un număr foarte redus de VLAN-uri setate pe switch-uri. În situația în care dorim să folosim un link pentru fiecare VLAN putem opta pentru un switch de layer 3 în locul ruterului, acesta permitând un număr mai mare de conexiuni.

Configurare router-on-a-stick



142

O altă soluție pentru rutarea inter-vlan este conceptul de "router-on-a-stick". În loc să avem legături pentru fiecare VLAN, putem folosi o singură legătură Fast Ethernet și să rulăm ISL sau 802.1Q.

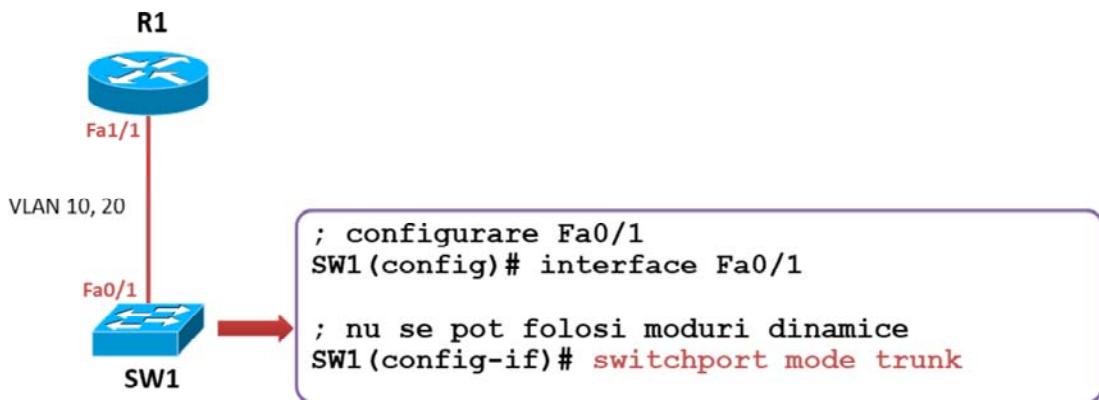
Pentru a exemplifica acest concept trebuie să definim noțiunea de sub-interfață. O sub-interfață permite configurarea a mai multor adrese IP și încapsulări configurate pe aceeași interfață fizică.

Vom porni interfața ruterului și vom crea sub-interfețele cu ajutorul comenzi **interface interface_id.subinterface_id**.

Deoarece vom folosi 802.1Q va trebui să setăm încapsularea pe interfață cu ajutorul comenzi **encapsulation dot1q VLAN_ID**.

Setarea IP-ului se va face pe sub-interfață pentru a permite transmiterea de pachete pe aceeași interfață fizică.

Configurare router-on-a-stick



143

Pentru configurarea router-on-a-stick pe partea switch-ului, va trebui să setăm interfața corespunzătoare în modul trunk folosind comanda **switchport mode trunk**.

Modul trunk trebuie specificat explicit deoarece ruterele nu suportă negocierea trunk-ului prin DTP.

Implementarea router-on-a-stick aduce după sine o mulțime de avantaje însă și dezavantaje.

Această soluție crează un SPOF (Single Point of Failure) și de multe ori un bottleneck ce duce la performanțe scăzute. Fiecare implementare trebuie bine documentată și analizată înainte pentru a alege soluția optimă de implementare în cadrul unei infrastructuri.

Troubleshooting

- Verificați că:
 - Porturile sunt asignate corect în VLAN-uri
 - Porturile de switch au fost configurate în modul corespunzător
 - Subinterefețele ruter-ului au încapsularea corectă și sunt asignate VLAN-urilor corespunzătoare
 - Schema de adresare este corectă

```
; verificare pe ruter
Router# show ip interface brief

; verificare pe switch
SW1# show interface Fa0/1 switchport
```

144

De multe ori se va întampla să vi se ceară să realizați troubleshooting pe o rețea ce nu a fost proiectată de voi.

Există 2 comenzi foarte des utilizate în depanarea rețelelor ce au nevoie de rutare inter-VLAN:

Comanda **show ip interface brief** ne permite să vizualizăm schema de adresare de pe ruter și dacă interfețele au o problemă la nivelul 1 sau 2. Dacă adresarea este corectă și nu detectăm erori la cele 3 niveluri ale stivei OSI putem trece la verificarea switch-ului.

Cu ajutorul comenzi **show interface *interface_ID* switchport** putem vizualiza modul DTP în care este trecut portul, VLAN-ul asociat, starea portului, etc.
