SUBIECTE REZOLVATE RL
[DATI CTRL+C NU CTRL+X!!!] >.<
MULTE MULTIMIRI LUI TUMI SI CELOR CARE AU COMPLETAT DOCS-UL <3

SUCCES -- HAI BA CA TRECEM :)

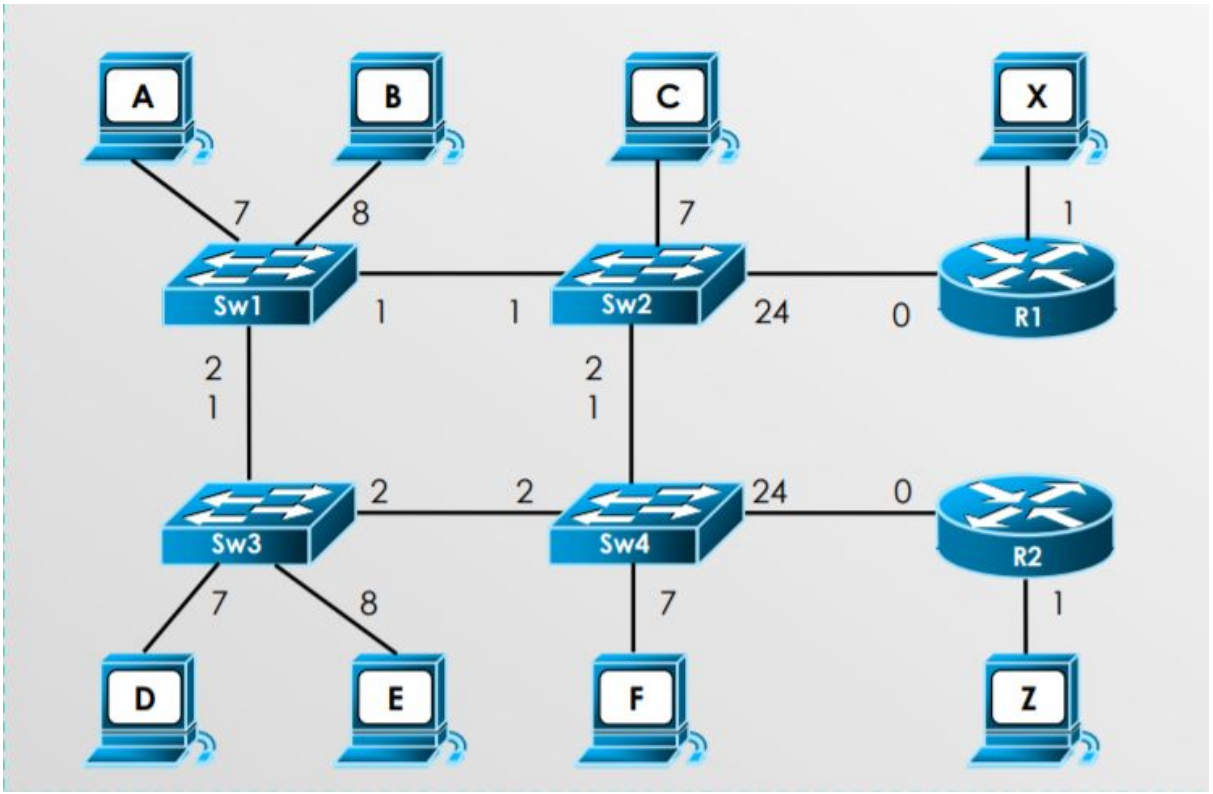
Orice rezolvare sau sugestie sau informaţie adiţională este binevenită.

NU fiţi bulangii să ştergeţi chestii OK sau să faceţi troll inutil.
Oricum voi face copii din când în când ca să salvez ce s-a pus în regulă.

CUM E EXAMENUL?

SUBIECTUL 1: ADRESARE DE NIVEL 2 ŞI COMUTARE:

00: Care va fi conţinutul tabelelor CAM de pe Sw1 şi Sw2?



Reţeaua este proaspăt reiniţializată. În reţea se trimit următoarele pachete: A → B, C → Z, C → A

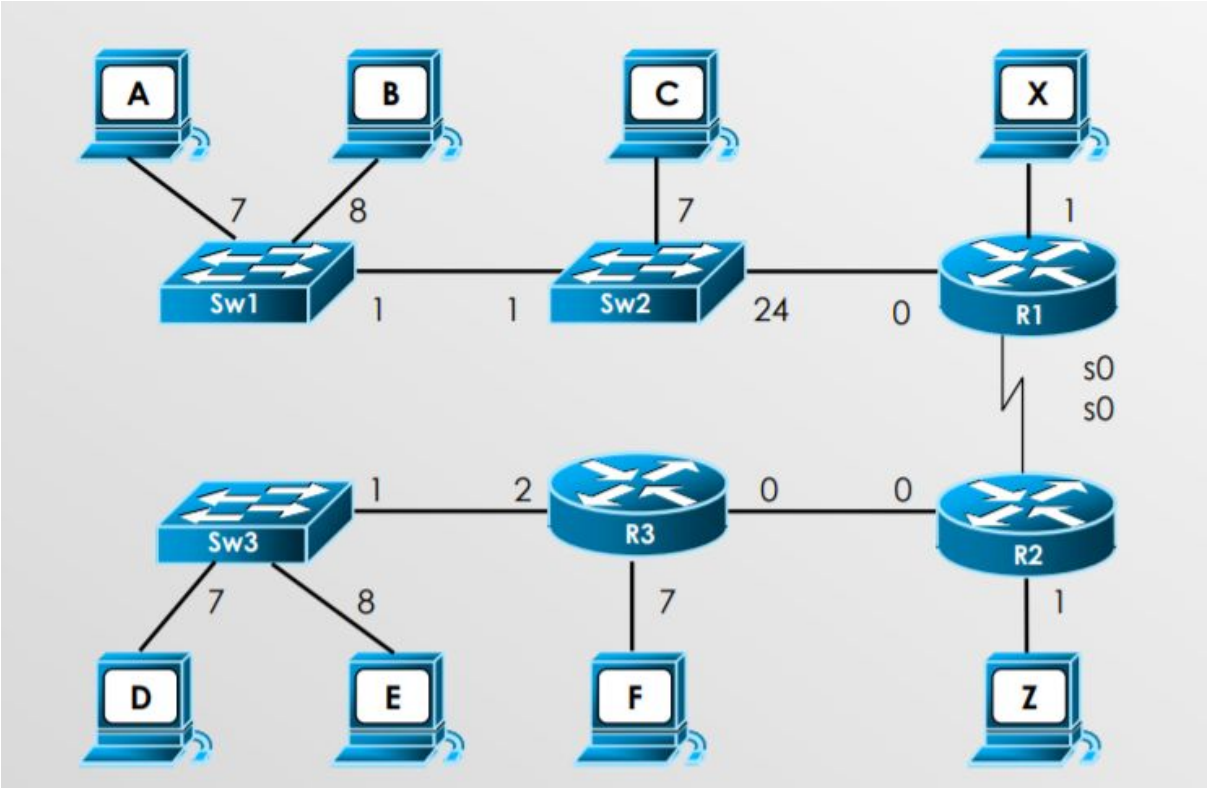
SW1: port 7 - MAC A; (port 2 - MAC A sau port 1 MAC A posibila suprascriere din cauza buclei în reţea dacă nu avem STP); sau port 2 - MACport 1 - MAC C C (depinde de STP)

SW2: port 1 - MAC A sau port 2 - MAC A (depinde de STP); port 7 MAC C (sau port 1 MAC C sau port 2 - MAC C posibila suprascriere din cauza buclei în reţea dacă nu avem STP);

Cred ca depinde si dacă pachete aşteaptă un reply (de tipul ICMP ECHO), astfel ar apărea şi MAC-ul lui B în Sw1.

SW1:
SW2:
A->B
SW1: MAC A – 7
SW2: MAC A – 1 sau MAC A – 2
C->Z
SW1: MAC A – 7, MAC C – 1 sau MAC C – 2
SW2: MAC A – 1 sau MAC A – 2, MAC C – 7
C->A
SW1: MAC A – 7, MAC C – 1 sau MAC C – 2
SW2: MAC A – 1 sau MAC A – 2, MAC C – 7

01: Ce antete diferite apar în reţea?



Reţeaua este proaspăt reiniţializată. În reţea se trimit următoarele pachete: C → A şi A → E
C → A: MAC C, MAC A, IP C, IP A;
A → E: MAC A, MAC R1/0, IP A, IP E;
MAC R1/s0, MAC R2/s0, IP A, IP E;
MAC R2/0, MAC R3/0, IP A, IP E;
MAC R3/0, MAC E, IP A, IP E;

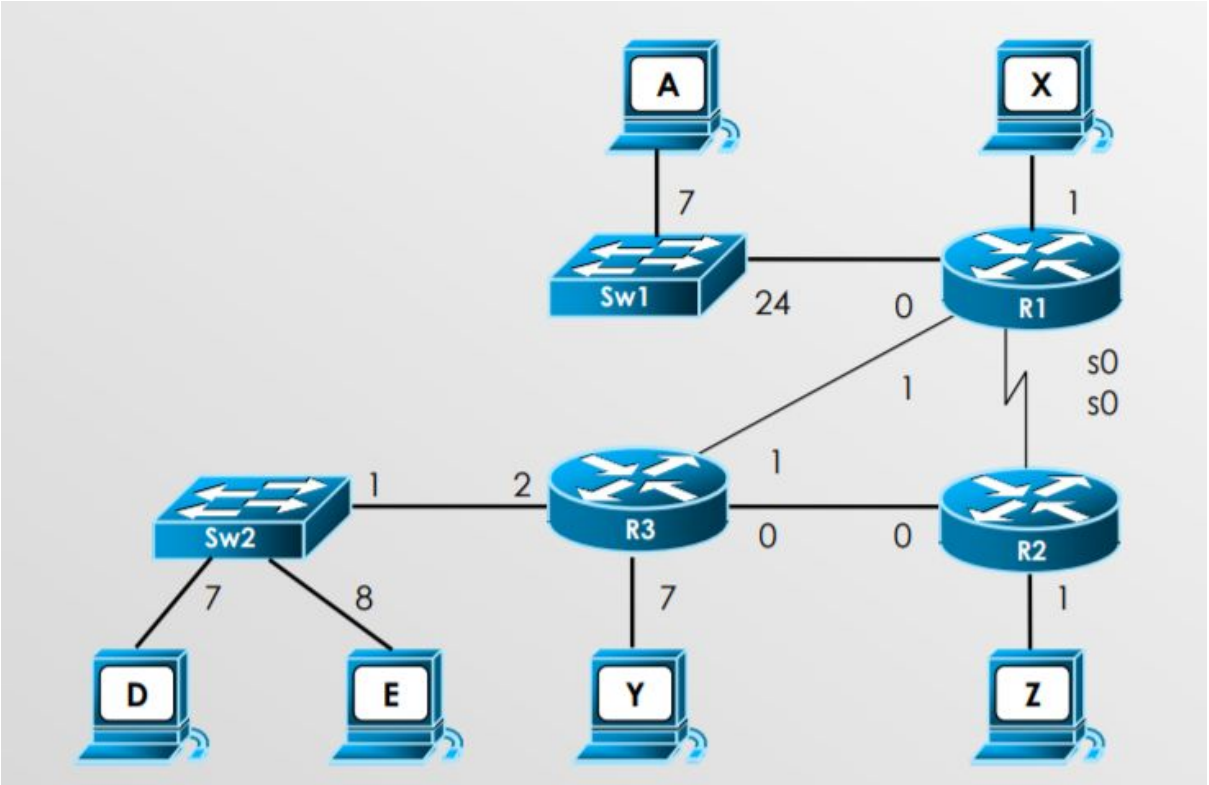
EDIT: modificat ultima linie, sarisem peste R3, de la R2 direct la E :) multumesc

c -> a
ARP populata:
MAC dest A, MAC sursa C, IP dest A, IP sursa C

APR nepopulata: (nu face careva si pt a->e :)))
ARP rq: MAC dest FFFF…, MAC sursa C, IP dest A, IP sursa C
ARP rs: MAC dest C, MAC sursa A, IP dest C, IP sursa A,
MAC dest A, MAC sursa C, IP dest A, IP sursa C, Date

(da, este bine sa stim si ca se incepe cu ARP rq)

02: Conţinutul tabelelor ARP de pe nodurile A şi Z?



Nodurile X, Y şi Z sunt senzori ce nu au resurse pentru a rula o stivă TCP/IP completă, motiv pentru care vor comunica bazându-se pe Proxy ARP. Tabelele ARP sunt complet populate.

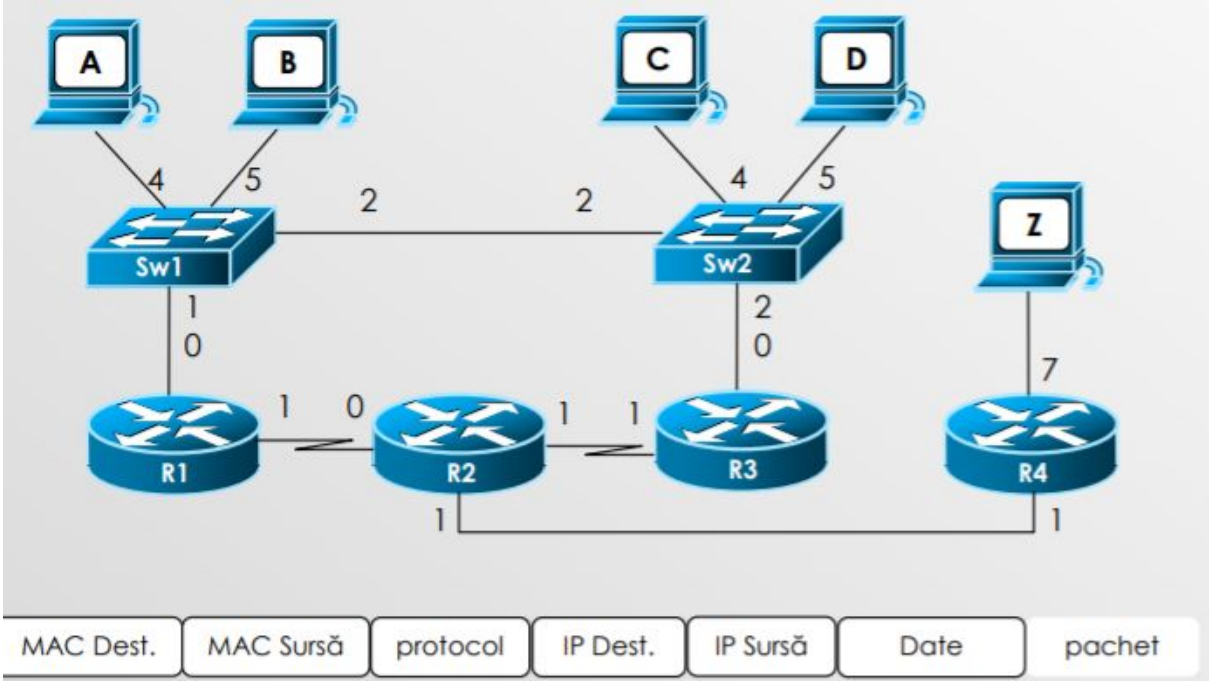
Care e rezolvarea corecta pana la urma ca nu inteleg nimic ++ nu stiu coae -> cu verde

A are ca default gateway R1/0 si va asocia MAC R1/0 cu IP R1/0; cunoaste ca alte statii sunt in afara retelei sale; cererile ARP contin adresa IP R1/0; Daca cererile sunt in aceeasi retea, cererea ARP va contine adresa IP destinatie;
Z va asocia orice adresa IP din afara retelei cu MAC R2/1; nu cunoaste unde sunt alte statii;
Deci, raspuns: Pe nodul A se cunoaste MAC R1/0 asociat cu IP R1/0, pe Z nu se cunoaste niciun MAC

Eu as zice ca rezolvarea e alta: router R2 are configurat proxy ARP, tabela ARP de pe Z o sa aiba pentru orice IP asociat MAC-ul lui R2/1. Iar pentru A, cred ca e discutie daca are default gate pe R1, sau functioneaza tot prin proxy ARP. Pentru cazul cu default gate, tabela ARP o contina doar IP lui R1/0 si MAC-ul lui R1/0. Pentru proxy ARP o sa fie similar cu ce am scris la Z, adica o sa aiba pentru fiecare IP, MAC-ul lui R1/0. Daca nu este clar sau corect as aprecia niste feedback. -- Pentru Z nu cred ca poate stoca o tabela ARP, doar o asociere temporara IP/MAC. Pentru A, ar avea stocat in tabela sa ARP doar MAC-urile din reteaua locala, asa ca va fi maxim MAC-ul lui R1/0 (chiar daca are default gateway sau nu, care este folosit doar in caz ca se trimite in alta retea).

E normal ca R1 sa aibe doua porturi 1? -- Nu, insa mai sunt desene facute aiurea. Cred ca portul dintre R1 si X e diferit fata de cel dintre R1 si R3. In mod normal nu ar avea cum sa aiba doua porturi cu acelasi nume

03: Enumeraţi în ordine echipamentele parcurse

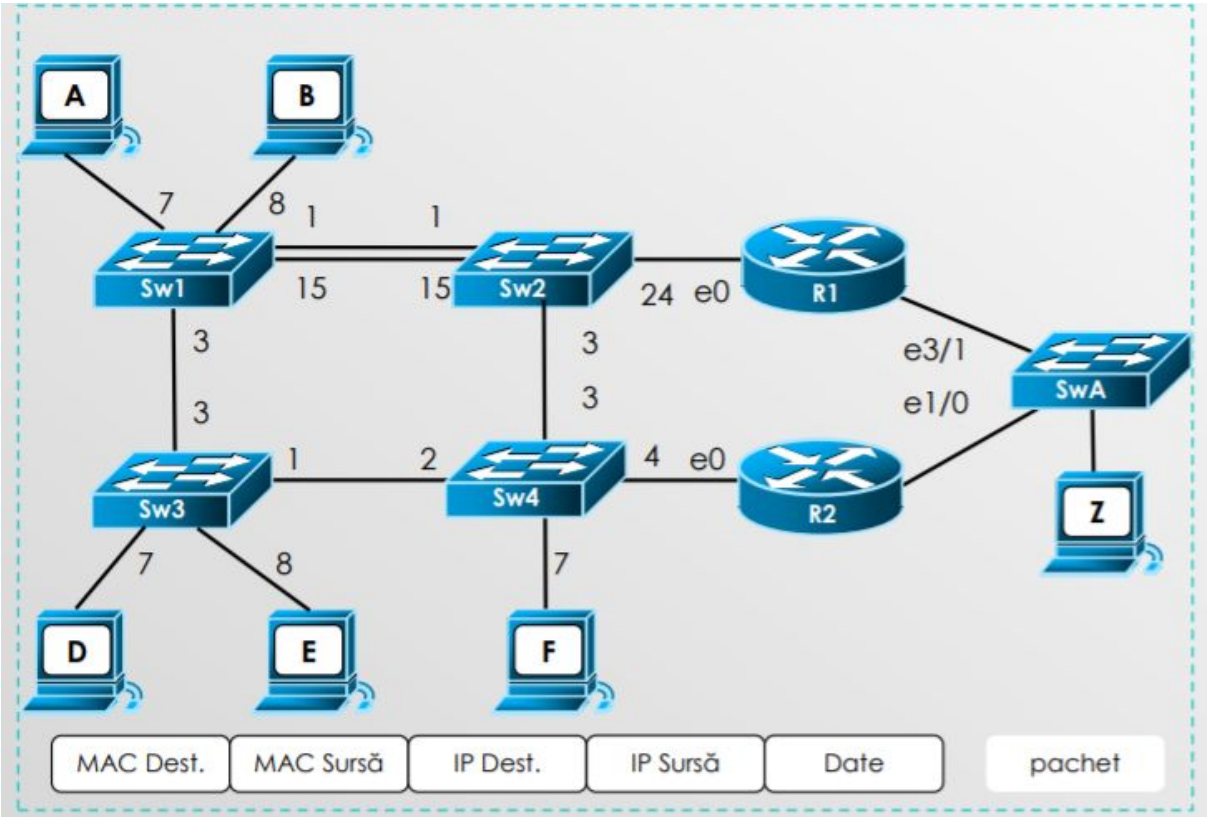


Pe Sw1 şi Sw2 toate porturile impare vor fi configurate în VLAN 10, iar toate porturile pare pe VLAN 20. Ce echipamente vor fi implicate în comutarea traficului de la staţia A la staţia D?

Nu exista conexiune de la A spre D.
A → SW1 → SW2 → C (da drop), R3

Si aici as propune o alta rezolvare: se observa ca statia A este in VLAN-ul 20, iar statia D este in VLAN-ul 10, ceea ce inseamna ca nu exista o conexiune directa intre cele doua. Se poate discuta daca conexiunile dintre cele doua switch-uri si dintre switch-uri si router este de tip trunk. In caz afirmativ, daca oricare dintre R1 sau R3 are configurat router-on-a-stick, atunci se poate ajunge de la A la D. -- De acord, insa daca ar fi vreun trunk sau RoaS ar trebui sa specifice explicit in enunt. Ei zic portul (im)par VLAN (im)par si atat, ceea ce intuitiv duce la Caz 4. Intre rutere efectiv nu ni s-a zis nimic si au porturile numite ampulea :)

Caz 1: Daca R1 este configurat cu router-on-a-stick:
Drum: A->Sw1->R1->Sw1->Sw2->D (cu asumarea ca intre SW1 si SW2 e trunk)
Caz 2: Daca R3 este configurat cu router-on-a-stick:
Drum: A->Sw1->Sw2->R3->Sw2->D (cu asumarea ca intre SW1 si SW2 e trunk)
Caz 3: Daca R1 si R3 sunt configurate cu router-on-a-stick:
Drum: Cred ca e identic cu R1?
Caz 4: Daca nici R1 si nici R3 nu sunt configurate cu router-on-a-stick:
Drum: Aici nu sunt sigur, insa cred ca nu exista un drum. Nu stiu daca conteaza cum ar fi configurat R2. -- Ar conta pentru alte cazuri in cazul lipsei trunk intre SW1 si SW2



04: Ce antete diferite apar în rețea?

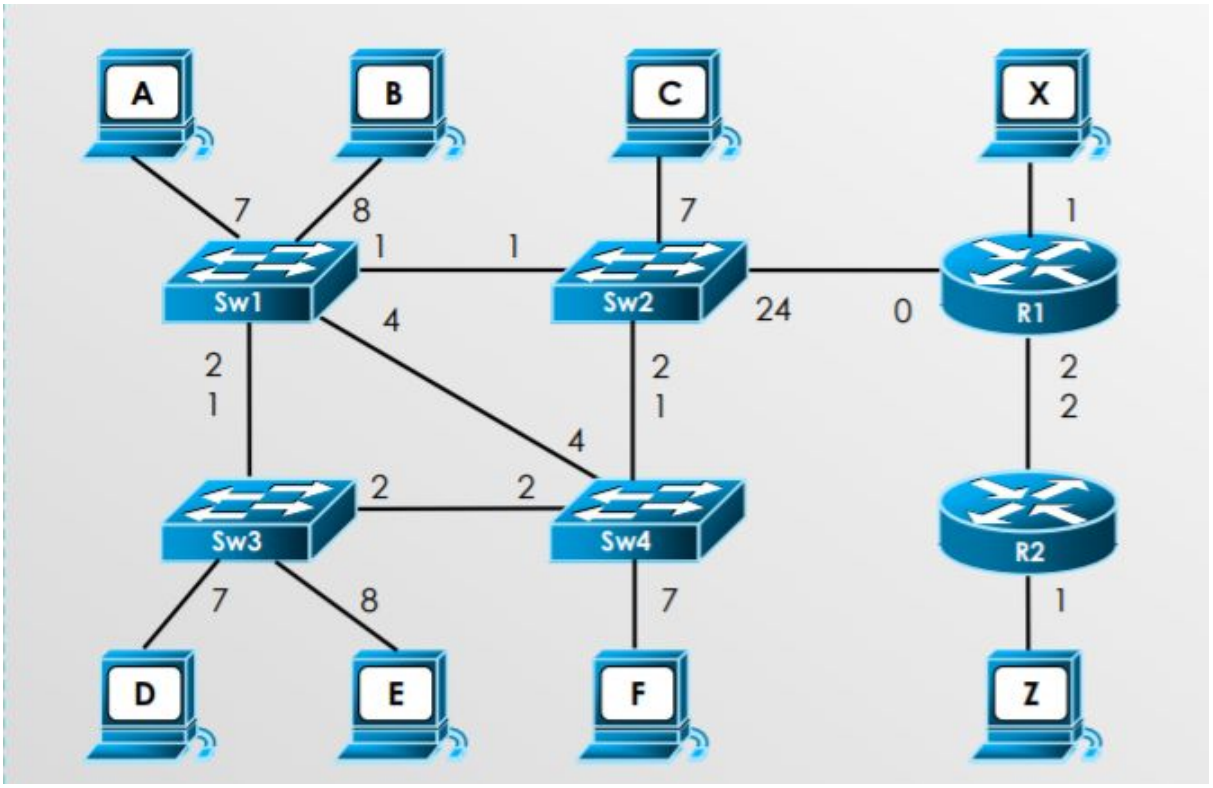
Scrieţi toate antetele diferite a cadrelor ce vor apare în cazul în care staţia A îi trimite un singur cadru staţiei F, apoi F trimite un cadru către Z.

A → F: MAC F, MAC A, IP F, IP A (daca se stie deja MAC F, daca nu, se face ARPrq)
F → Z: MAC e0 (oricare), MAC F, IP Z, IP F → MAC Z, MAC e3/1 sau e1/0, IP Z, IP F (folosind formatul de antet din diagrama)

De la F -> Z as zice ca depinde de configuratia lui R1 si R2. Daca sunt configurate ca proxy ARP sunt ca mai sus. Daca sunt configurate cu default gateway vine:
F -> e0: MAC e0 (oricare), MAC F, IP e0 (oricare), IP F
e0 -> Z: MAC Z, MAC e0, IP Z, IP e0

-- Chiar si cu default gateway nu cred ca se schimba IP pe parcurs :?
Nici eu nu cred ca se schimba adresa ip pe parcurs in cazul cu default gateway. Cred ca ar trebui sa fie(in cazul cu default gateway):
F -> e0: MAC e0, MAC F, IP Z, IP F
e0 -> Z: MAC Z, MAC e0, IP Z, IP F

05: Ce porturi vor ajunge în starea blocat?

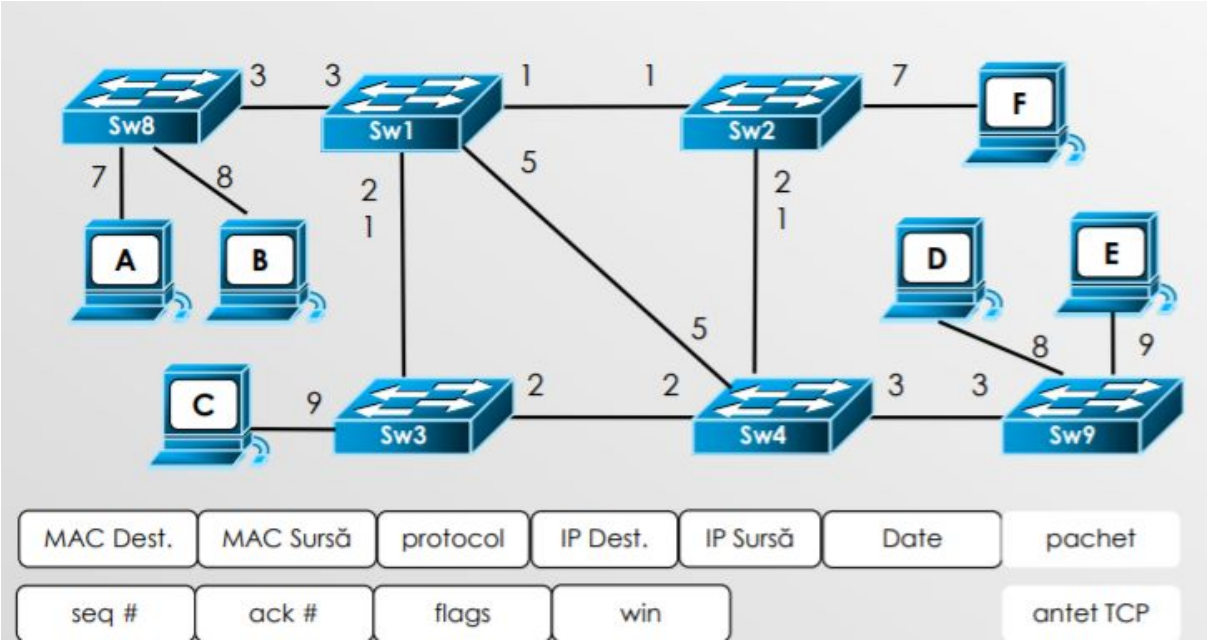


Ştiind că MAC(Sw1)<MAC(Sw2)< MAC(Sw3)<MAC(Sw4), legătura directă între sw1 şi sw4 este de 10 Mbps, iar restul legăturilor sunt FastEthernet, aplicaţi algoritmul STP pentru reţeaua dată.

(In cazul in care prioritatile sunt egale)
SW1 root bridge: 1, 4, 2 des ports, 7, 8 nu intra la STP
SW2: 1 root port, 2 des port, 7, 24 nu intra la STP
SW3: 1 root port, 2 des port, 7, 8 nu intra la STP
SW4: 1 root port, 4, 2 blocked ports, 7 nu intra la STP

Intrebare: STP nu opereaza doar pe retea de switch-uri? Are sens sa fie incluse si porturile catre end-device-uri, respectiv router? -- ai dreptate, voi modifica [MODIFICAT]

06: Ce porturi vor fi definite ca porturi rădăcină?

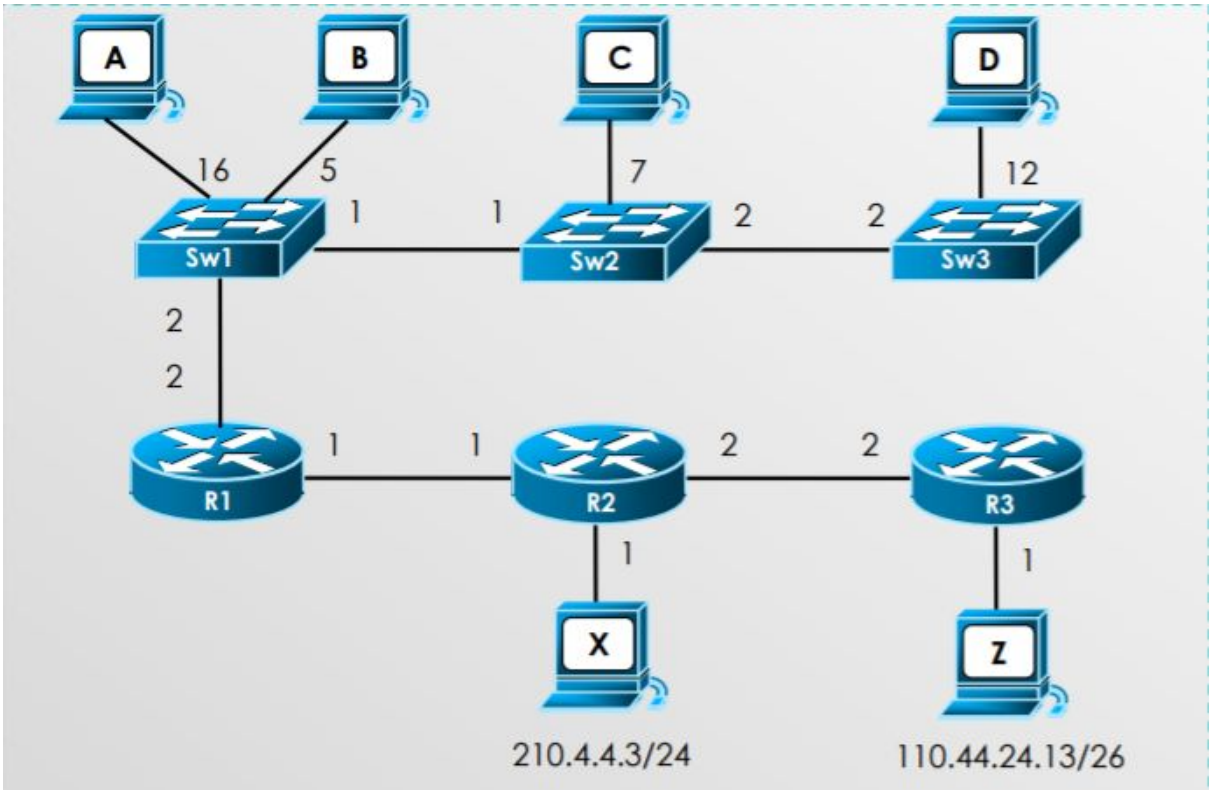


Conexiunea între Sw1 şi Sw4 este GigaEthernet, restul legăturilor fiind FastEthernet. MAC(Sw1)< MAC(Sw2)< .. < MAC(Sw9). Aplicaţi algoritmul STP

(In cazul in care prioritatile sunt egale)
SW1 root bridge: 3, 1, 5, 2 des ports
SW2: 1 root port, 2 blocked port, 7 nu intra la STP *
SW3: 1 root port, 2 blocked port, 9 nu intra la STP *
SW4: 5 root port, 3, 1, 2 des ports -- aici 1 si 2 nu sunt des? Ca legatura dintre sw1 ai sw4 e mai rapida.. si s-ar alege porturile 1 si 2 designated pe sw4. Si porturile 2 pe sw3 si sw2 ar fi blocked… eu asa cred! (+1) -- asa e, modific acum [MODIFICAT]
SW8: 3 root port, 7, 8 nu intra la STP *
SW9: 3 root port, 8, 9 nu intra la STP *

* = port catre statie, nu intre switch-uri (nu poate crea loop in topologie)

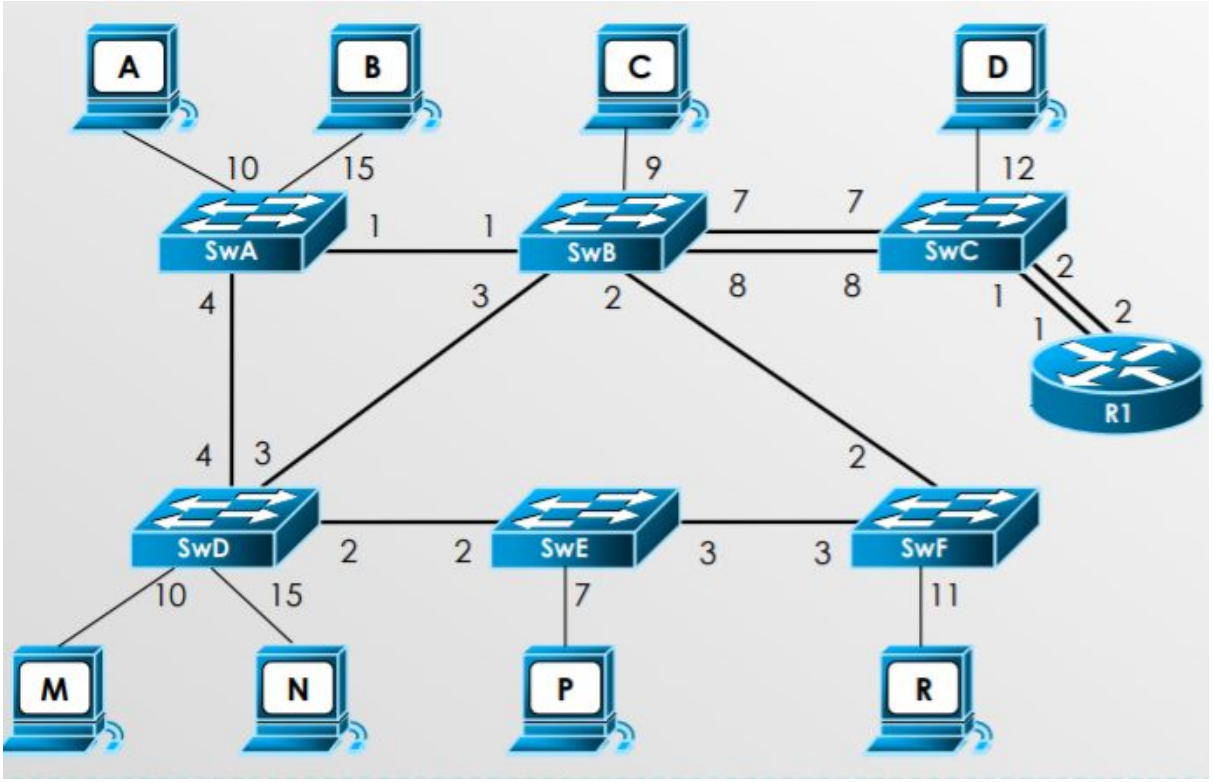
07: Care va fi conţinutul tabelei CAM pe Sw3?



Reţeaua este proaspăt reiniţializată. În reţea se trimit următoarele pachete: A → B, R1 → Z, C → Z, C → A

A → B: port 2 - MAC A;
R1 → Z: nimic nou
C → Z: port 2 - MAC C;
C → A: nimic nou
Final: MAC A si MAC C pe port 2

08: Ce echipamente vor fi traversate când A trimite un pachet la B?

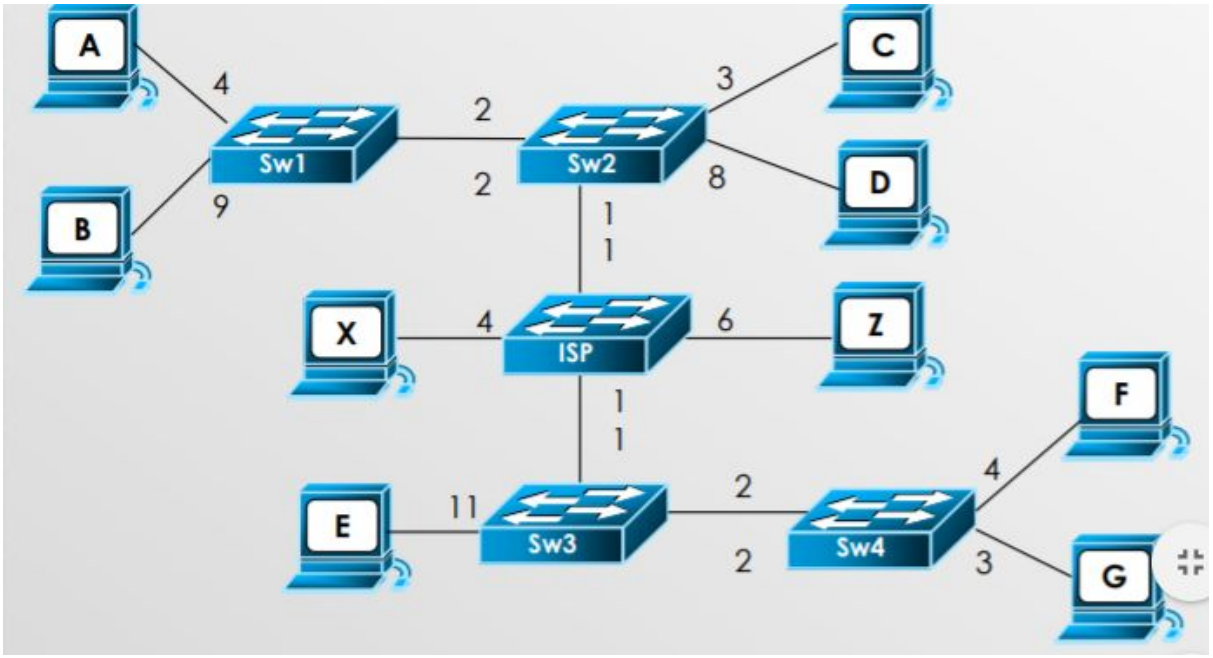


Reţeaua este proaspăt reiniţializată. În reţea toate porturile pare sunt în VLAN10, cele impare în VLAN9 În reţea se trimit următoarele pachete: A → B

Nu se ajunge de la A la B.
A → SWA → SWD → M (da drop), SWE

(Discutie daca intre switchuri sunt legaturi de tip trunk sau nu si cum e legat R1)

09: Ce intrări vor fi în tabela CAM pe Sw1 şi Sw4?



Reţeaua este proaspăt reiniţializată. În reţea toate porturile pare sunt în VLAN10, cele impare în VLAN9 În reţea se trimit următoarele pachete: A → D, E→ D, D → C, C → A

SW1: port 4 - MAC A, port 2 - MAC D ←- cred. Si eu zic la fel (+ 4 asa)
SW4: nimic, gol ca mintea mea

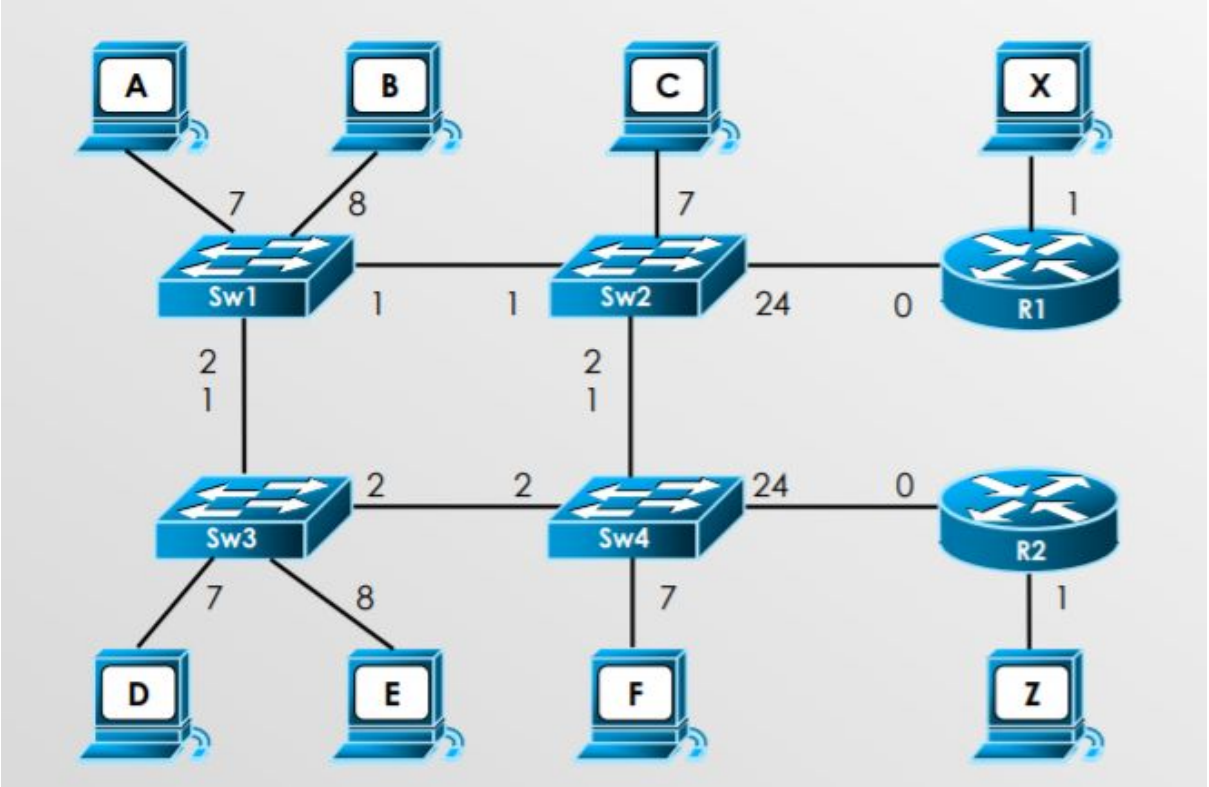
ISP nu este switch? -- L-am luat ca fiind Internet Service Provider, adica o retea mare. Nu stiu daca e corect tho

Daca e switch, asa ar fi corect? (Intreb, nu sunt sigur) -- Ai luat in calcul faptul ca sunt in VLAN-uri diferite? Spre exemplu, cum ar putea ajunge un mesaj de la E la Sw4? E e in VLAN9 si Sw4 are port de acces in VLAN10. Ahh, nu ma gandisem sa iau in calcul faza cu vlanurile, merci de pont :))

Super merci de clarificari, va pup <3

SUBIECTUL 2: ADRESARE DE NIVEL 3 ŞI RUTARE:

00: Descrieţi tabela de rutarea de pe R1.



Toate porturile 7 vor fi configurate în VLAN7. Toate porturile 8 vor fi configurate în VLAN8. Toate adresele din reţea sunt alocate din spaţiul 188.17.32.64/27.

[ACTUALIZAT]

C (retea X-R1 cu masaca /30, R1/1)
S (retea R2-Z cu masca /30, IP R2/0 ca next-hop)
C (retea R1-R2 cu masca /28, conectata pe R1/0, in care intra si subretelele 7 si 8:
    C (VLAN7 cu masca /29, R1/0.subinterfata7)
    C (VLAN8, cu masca /30 R1/0.subinterfata8)

- (se ia in calcul si alea 2 adrese de broadcast/gateway cand subnetez vlanul?) -> Da. Acum am luat. Multumesc. [MODIFICAT]

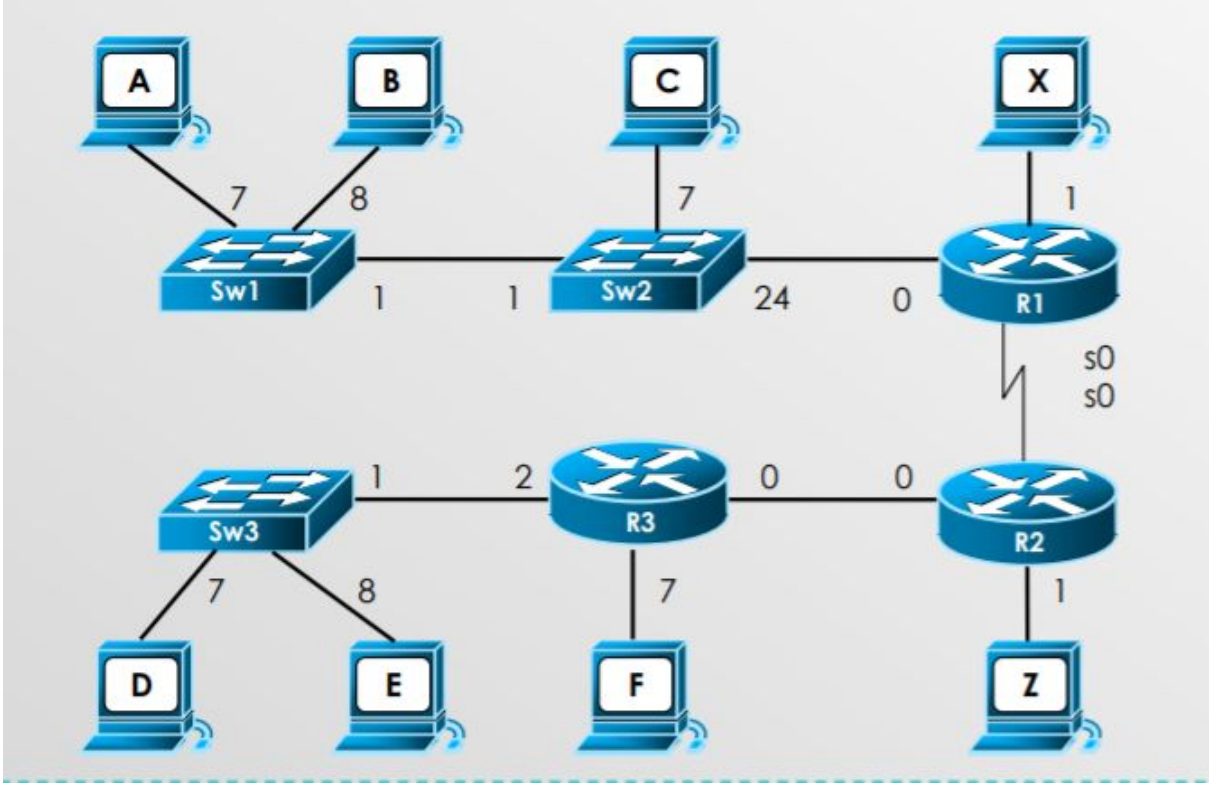
Poate explica careva va rog? :))

Explicatie: *adresele sunt alocate ca exemplu, se pot pune si in alta ordine

- Suma componetelor din reteaua R1-R2 (unde intra si subretelele VLAN7 si VLAN8) -> /28 -> 188.17.32.64/28 pentru tot ce e intre cele doua rutere R1-R2, dintre care impartim cum urmeaza:
    - subreteaua VLAN7, cu 4 statii + retea & bcast VLAN7 -> 6 adrese -> /29 -> 188.17.32.64/29.
        //nu treabuie o adresa si pentru R2/0.7? -- adresele logice R1/0.7 si R2/0.7 nu au acelasi IP ca R1/0?
        Nu cred, vezi curs 4, slide 33: “Fiecare subinterfaţă va avea adresa sa proprie de nivel 3”
    - subreteaua VLAN8, cu 2 statii + retea & bcast VLAN8 -> 4 adrese -> /30 -> 188.17.32.72/30.
    - 2 adrese pentru R1/0 si R2/0 + retea & bcast retea mare -> 4 adrese -> /30 -> 188.17.32.76/30
- o retea intre R1 si X -> adresa ruter, adresa X + retea & bcast -> 4 adrese -> /30 -> (188.17.32.80/30)
- o retea intre R2 si Z -> adresa ruter, adresa Z + retea & bcast -> 4 adrese -> /30 -> (188.17.32.84/30)

Pentru R1, toate retelele mai putin cea dintre R2 si Z sunt conectate direct C, iar reteaua aia e pusa cu ruta statica S cu R2/0 ca next-hop
Cred ca nu ai luat in calcul si adresele IP pentru interfetele ruterului cand ai alocat adresele. (*deci la VLAN 8 nu ar fi si adresa IP de pe interfata ruterului ? Adica ar fi 3 in loc de 2 + adrese retea si broadcast?)
-> Acum da, multumesc. [MODIFICAT]
!! NOTA: Important la acest exercitiu e **tabela de rutare din R1 nu subnetarea**, asa ca nu pierdeti mult timp cu ea daca nu o intelegeti.

01: Care vor fi adresele IP configurate pe R1?



Adresa privata pe R1/0 de tip /29. Adresele de iesire ale R1/1 si R1/s0 pentru translatare; Adresa 141.85.37.1/30 pentru R1/1 si adresa 141.85.37.5/30 pentru R1/s0 (un exemplu).

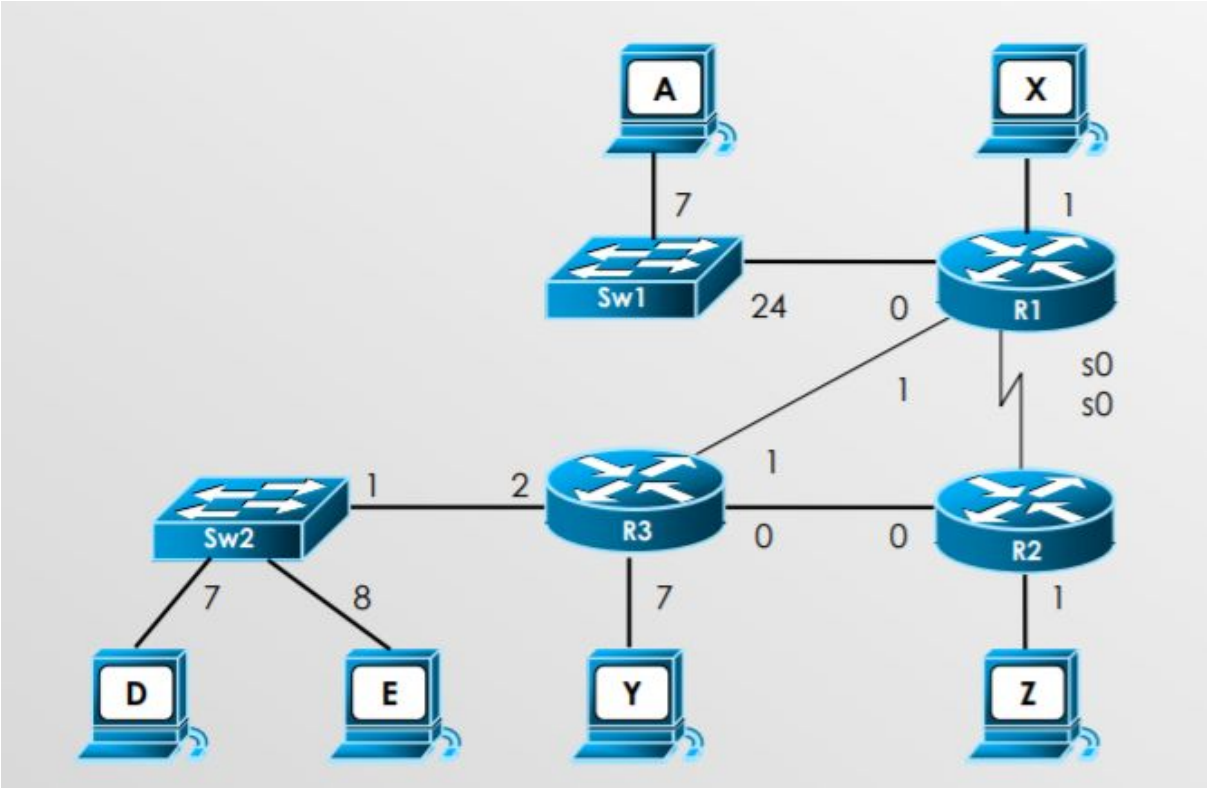
Poate explica cineva aici exact procesul ca nu prea inteleg de ce la seriala am /30 ca as avea 4 calculatoare + 2 adrese (bcast/gateway) = 6 deci mi-ar trebui 3 biti, nu ar trebui sa am /29? (Stiu ca nu e corect dar intreb ca nu prea am inteles :)), ca in video nu prea e explicat de ce), thanks -- De unde 4 calculatoare? A, B, C sunt in retea privata cu R1/0, iar X e in alta retea, publica, cu R1/1.
Da, ar trebui /29 deoarece am 4 interfete(R1/1, X, R1/s0, R2/s0) + 2 adrese(bcast/gateway). Din spatiul /30 mai raman doar 2 asignabile. -- X si R1/1 nu sunt in retea diferita fata de R1/s0 si R2/s0? Gen doua retele de /30 (de aia sunt .1 si .5)

Explicatie: R1 e conectat la 3 retele, una cu X si portul 1 (2 IP-uri publice necesare in retea, un IP public necesar pe R1/1, deci /30 e suficient), una cu R2 (2 IP-uri publice necesare in retea, un IP public necesar pe R1/s0, deci /30 e suficient), si una privata cu statiile A, B, C (4 IP-uri private necesare, dintre care un IP privat necesar pe R1/0, deci /29 e suficient).

La A,B,C nu ar fi doar o adresa pe care o pui la toate? -- nu, vezi MV-urile de pe OpenStack, avem IP-uri diferite in aceeasi retea privata :)

[AVETI GRIJA SA NU MAI STERGETI CHESTII PLS]

02: Ce antete diferite apar în rețea?



În cele două rețele cu switchuri s-au folosit adrese private, astfel R1 şi R3 vor asigura translatare de adresă cu supraîncărcare (PAT). Descrieţi toate antetele de nivel 3 diferite, ce apar în rețea când staţia A trimite un pachet către staţia D.

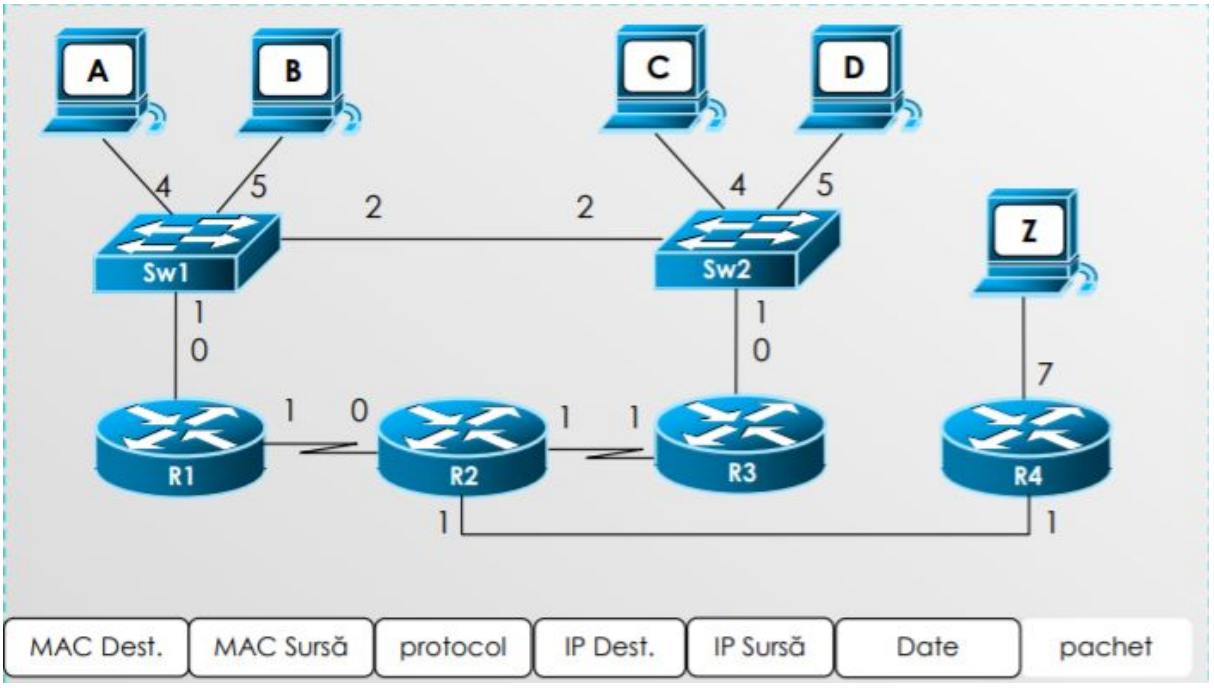
IP A → IP R3/1(.portD) (MAC A, MAC R1/0)(Aici nu ar trebui sa fie IP R3/2?? - nu cred, ca R3/2 este in reteaua privata, deci A nu ii stie IP-ul)
IP R1/1(.portA) → IP R3/1(.portD) (MAC R1/1, MAC R3/1)
IP R1/1(.portA) → IP D (MAC R3/2, MAC D)

Puteti explica aici ?

Explicatie: R1 si R3 folosesc PAT, deci IP-urile lui A si D vor fi private. A nu va cunoaste IP-ul lui D si nici D pe al lui A, insa ambele vor cunoaste IP-ul public al ruterului la care e conectat destinatarul si portul asociat pentru comunicarea (la nivel aplicatie). Deci A, cand trimite catre D, nu ii stie adresa IP, dar stie adresa IP R3/1 si portul aplicatiei. Dupa ce pachetul de la A trece de R1, si R1 va trebui sa ascunda adresa lui A (ca e si ea privata), deci va suprascrie IP sursa cu IP-ul lui R1/0(.portA)

Merita mentionat si ca in cazul PAT “comunicatia nu poate fi initiata de o statie din Internet”, deci exista posibilitatea ca statia A sa nu poata trimitie un pachet catre D. -- Buna mentiune, totusi, daca sunt configurate reguli de trecere pentru anumite IP-uri, merge.
Aprob si eu ca nu poti initia comunicatia din internet, iar in cazul de fata presupunem ca avem acelasi port asociat mereu, dar PAT este un NAT DINAMIC, nu o sa fie mereu acelasi port.

03: Descrieţi antetele pachetelor



Se defineşte un tunel între R3 şi R4. Tot traficul destinat staţiei Z va fi rutat prin acest tunel. Descrieți antetele pachetelor ce apar când D trimite un cadru către Z.

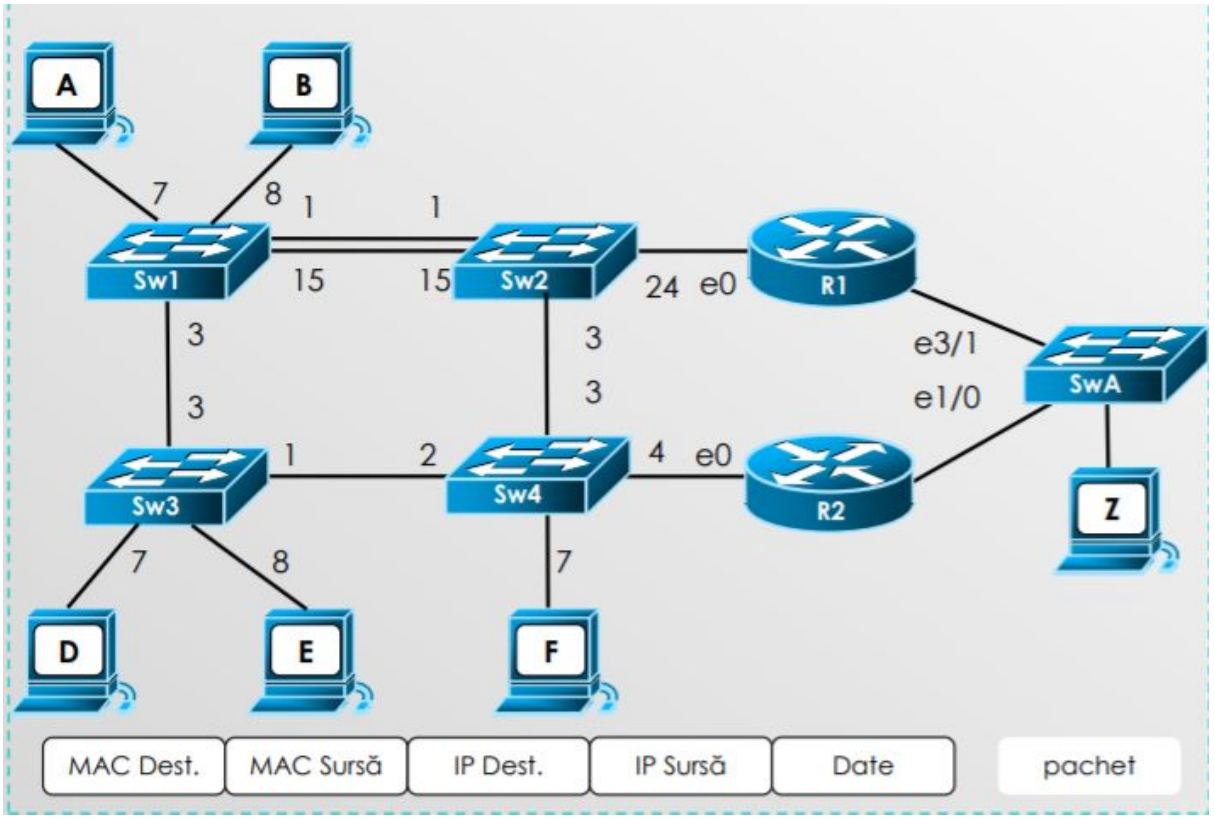
MAC D, MAC R3/0, IP D, IP Z
MAC R3/1, MAC R2/1, IP D, IP Z incapsulat in IP R3/1 IP R4/1
MAC R2/1, MAC R4/1, IP D, IP Z incapsulat in IP R3/1 IP R4/1
MAC R4/7, MAC Z, IP D, IP Z

Ar merge sa tinem cont si de TTL-uri, cum e exemplul din curs (curs 9, slide 27):
statia D: MAC D, MAC R3/0, IP D, IP Z, TTL: X
ruter R3: MAC D, MAC R3/0, IP D, IP Z, TTL: X-1
ruter R3: MAC R3/1, MAC R2/1, IP D, IP Z incapsulat in IP R3/1 IP R4/1, TTL: Y
ruter R2: MAC R2/1, MAC R4/1, IP D, IP Z incapsulat in IP R3/1 IP R4/1, TTL: Y-1
ruter R4: MAC R2/1, MAC R4/1, IP D, IP Z incapsulat in IP R3/1 IP R4/1, TTL: Y-2
ruter R4: MAC R4/7, MAC Z, IP D, IP Z, TTL: X-1

-- foarte frumos varianta adaugata cu TTL-uri!

Se tine cont de R2 daca definim un tunel? adica nu e ca si cum am un pachet?
| MAC R3/ 1 | MAC R4 / 1 | IP D | IP Z | -- Da, se tine cont, adica pachetul tot trebuie sa treaca pe acolo fizic, doar ca fiind incapsulat se intampla doua lucruri: 1) nu scade TTL-ul initial (X in cazul de sus), 2) adresele IP initiale sursa/destinatie nu sunt vizibile decat dupa decapsulare

04: Alocaţi adrese pentru toate echipamentele din reţea din spaţiul 10.1.50.0/24.



Pe Sw1 se închid porturile 1, 15. Toate staţiile conectate pe un port mai mic sau egal cu 7 vor fi în VLAN 10, cele pe un port strict mai mare decât 7 vor fi în VLAN 20

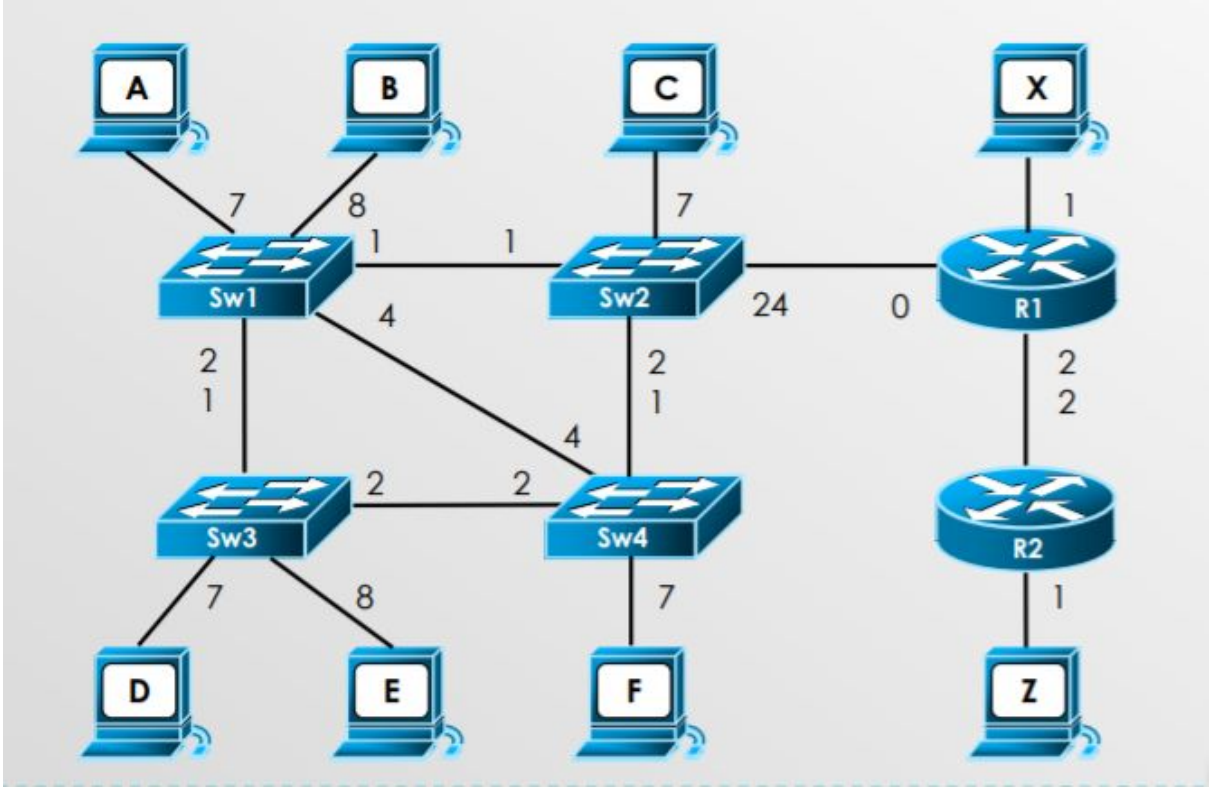
E neaparat sa fac impartire optima? -- daca optim = eficient, cam da

VLAN 10 va avea A, D, F, R2/e0 deci /29 - 10.1.50.0-7/29 (1-6 alocabile)
VLAN 20 va avea B, E, R1/e0 deci /29 - 10.1.50.8-15/29 (9-14 alocabile)
reteaua cu SWA va avea R1, R2, Z deci /29 - 10.1.50.16-23/29 (17-22 alocabile)

Propun o rezolvare usor diferita, tinand cont de pentru fiecare subinterfata de pe R1/e0 si R2/e0 trebuie alocata o adresa IP din VLAN-ul respectiv (nu sunt 100% ca e corect, as vrea niste feedback):
VLAN 10 va avea A, D, F, R1/e0.10, R2/e0.10 deci /29 - 10.1.50.0-7/29 (1-6 alocabile)
VLAN 20 va avea B, E, R1/e0.20, R2/e0.20 deci /29 - 10.1.50.8-15/29 (9-14 alocabile)
reteaua cu SWA va avea R1, R2, Z deci /29 - 10.1.50.16-23/29 (17-22 alocabile)

-- Este o varianta valida, depinde de interpretare (daca sunt rutere on a stick sau au acces doar pe un singur VLAN, cel din port. In primul caz e nevoie de subinterfete, in al doilea nu)

05: Ce informaţii se vor afla în tabela de rutare de pe R1?



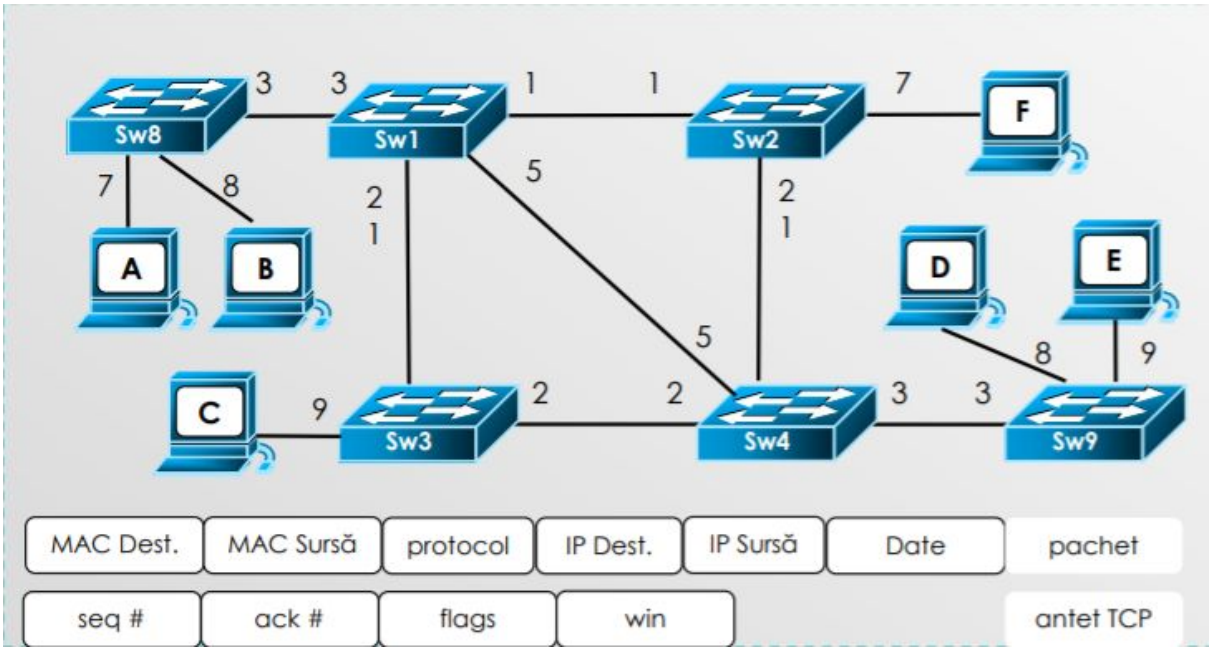
Sunt definite următoarele VLAN-uri: VLAN2: A, C VLAN3: B, D VLAN4: E, F Alocaţi adrese din spaţiul 199.11.32.128/25

[ACTUALIZAT]
C 199.11.32.128/30 R1/1
C 199.11.32.132/30 R1/2
S 199.11.32.136/30 IP R2-Z
C 199.11.32.140/29 R1/0.2
C 199.11.32.148/29 R1/0.3
C 199.11.32.156/29 R1/0.4

Intrebare: Adresele nu trebuie alocate de la cele mai multe la cele mai putine? (adica cele cu /29 sa fie alocate primele). Propun:
C 199.11.32.128/29; R1/0
C 199.11.32.136/29; R1/0
C 199.11.32.144/29; R1/0
C 199.11.32.152/30; R1/1
C 199.11.32.156/30; R1/2
S 199.11.32.160/30; R1/2

A doua e o propunere valida, pentru ca intr-adevar e de bun-simt sa aloci incepand cu cele mai multe, insa nu este o regula generala de eficienta. Deci si prima este corecta. Cred ca mai important la acest exercitiu este sa stim cum arata tabela de rutare (ce retea cum e conectata)

06: Ce adrese vor rămâne nealocate?

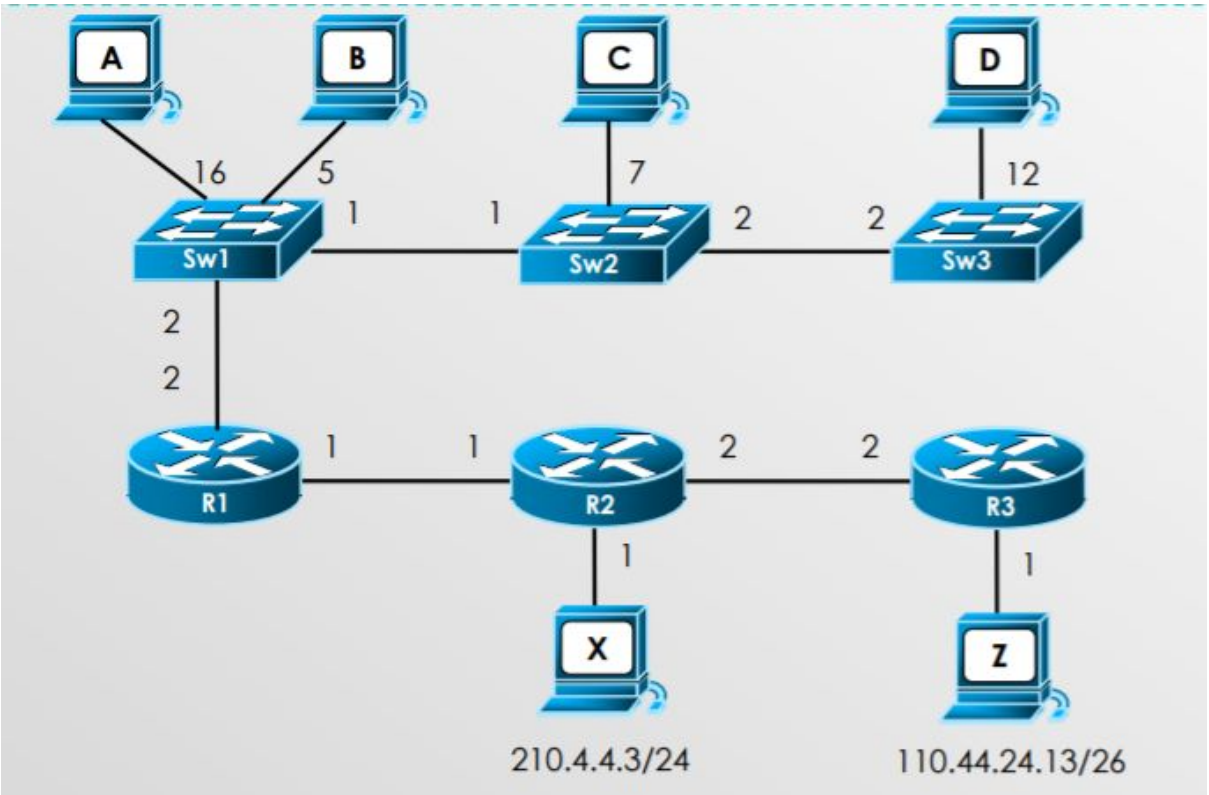


Pe Sw1 sunt închise porturile 1 şi 2. Staţia F este staţia administratorului. Sunt definite următoarele VLAN-uri: VLAN11: A, C VLAN12: B VLAN13: D, E Restul porturilor sunt porturi trunchi cu VLAN nativ 10, inclusiv Sw2,7 Alocaţi eficient adrese din spaţiul 19.12.48.192/26

Vor ramane nealocate un /30 de la VLAN12 si un /30 de la F daca B si F nu primesc valori din aceeasi /30, plus toate cele ramase pana la /26 dupa ce se vor adauga urmatoarele:
19.12.48.192/30 pentru VLAN11
19.12.48.196/30 pentru VLAN13
19.12.48.200/30 pentru VLAN12
adica 12 adrese folosite din 64 posibile, adica 52 nealocate
Daca F si B sunt puse separat se va aloca si 19.12.48.204/30 pentru F, deci 50 nealocate

Presupun ca daca F e statie de administrator, atunci are acces la fiecare VLAN, adica ca are 3 adrese IP:
VLAN11: A, C, F.11 => 19.12.48.192/29 => se irosesc 3 adrese
VLAN13: D, E, F.13 => 19.12.48.200/29 => se irosesc 3 adrese
VLAN12: B, F.12 => 19.12.48.208/30 => nu se iroseste nimic
Raman liber spatiul de la 19.12.48.212 - 19.12.48.255, deci 42 de adrese nealocate
Total adrese nealocate: 42 + 3 + 3 = 48 -- Tind sa cred ca legatura Sw2-F e trunk. Si daca nu ar fi, cred ca o statie normala (PC) nu poate avea mai multe IP-uri decat daca are mai multe interfete (motive hardware: placi de retea). Deci nu stiu ce sa zic de a doua metoda. Un ruter poate face asta pentru ca este configurat astfel hw, la un PC e mai complicat.

07: Care va fi conţinutul tabelei de translatare pe R1?



R1 realizează translatare cu supra încărcare pentru reţeaua locală. Descrieţi conţinutul tabelei de translatare de pe R1, ştii că avem două sesiuni web deschise de pe A către Z şi o sesiune ssh deschisă de pe staţia D către serverul X.

[ACTUALIZAT]
ce vine de la A pe portul 80 (sau 443) al R1/2 se duce la 110.44.24.13(:80/:443) si invers
ce vine de la D pe portul 22 al R1/2 se duce la 210.4.4.3(:22) si invers

1) A catre Z (Dc la A e :80? Ca la sursa nu dai portul pe care te conectezi ci portul pentru adresa privata, check curs 8 slide 10) -- curs 9 slide 12, trimiti portul asa cum e, identificatorul se asociaza la translatare, adica abia in tabela ruterului

S: IP A:80/:443 -> S: IP R1/1:port
D: 110.44.24.13:80/:443 -> D: 110.44.24.13:80/:443

2) Z catre A

S: 110.44.24.13:80:/443 <- 110.44.24.13:80/:443
D: IP A:80/:443 <- D: IP R1/1:port

3) D catre X

S: IP D:22 -> S: IP R1/1:port
D: 210.4.4.3:22 -> D: 210.4.4.3:22

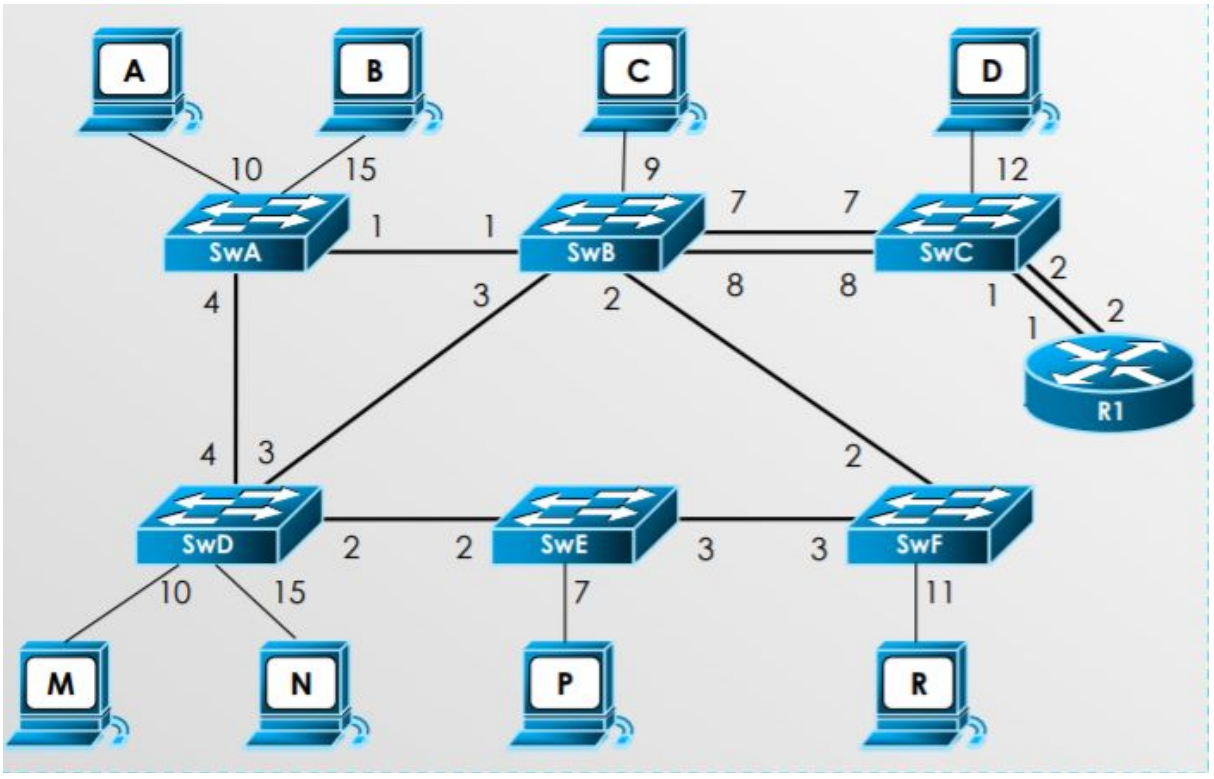
4) X catre D

S: 210.4.4.3:22 <- S: 210.4.4.3:22
D: IP D:22 <- D: IP R1/1:port

port = numar pana in 64000 alocat de catre R1 la translatare

Aici nu era R1/1 peste tot?? Stiu ca se foloseste interfata de iesire a ruterului cand face translatari +1 -- ba da, modific acum [MODIFICAT]

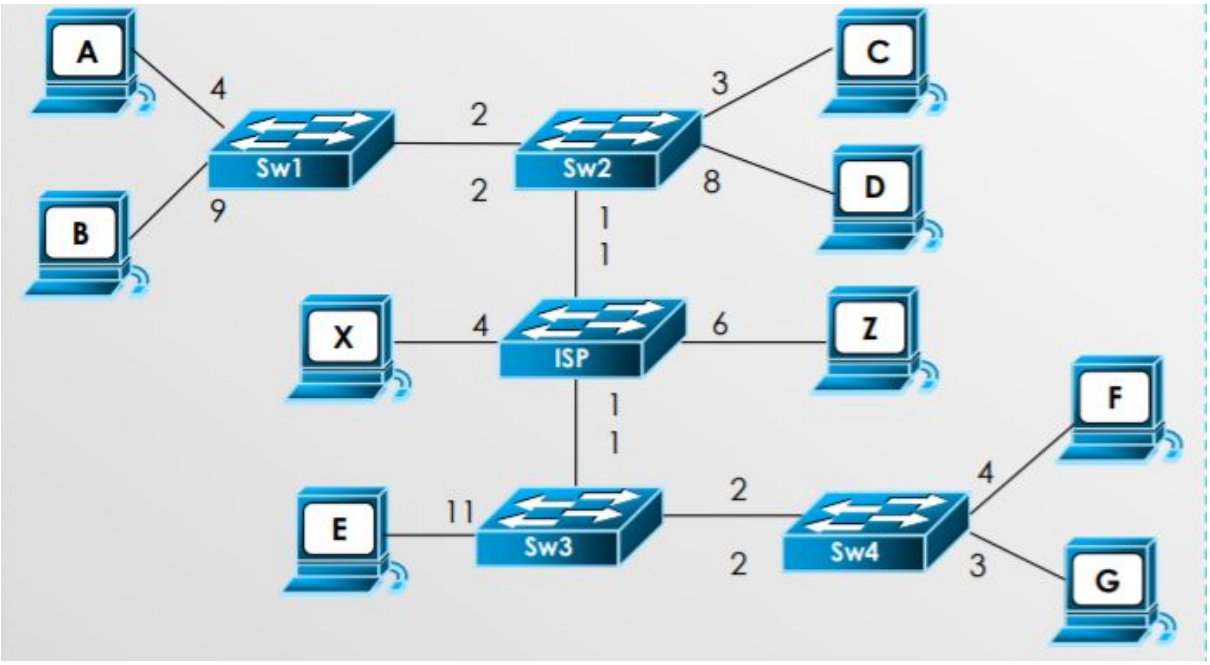
08: Ce adrese va avea configurat ruterul R1?



În reţea toate porturile pare sunt în VLAN10, cele impare în VLAN9. Alocaţi eficient adrese din spaţiul 14.44.32.64/26

3 statii + R2/2 in VLAN10, deci 14.44.32.64/29, cu R2/2 14.44.32.65/29
5 statii + R1/2 in VLAN9, deci 14.44.32.72/29, cu R1/2 14.44.32.73/29

09: Ce antete diferite apar în rețea?

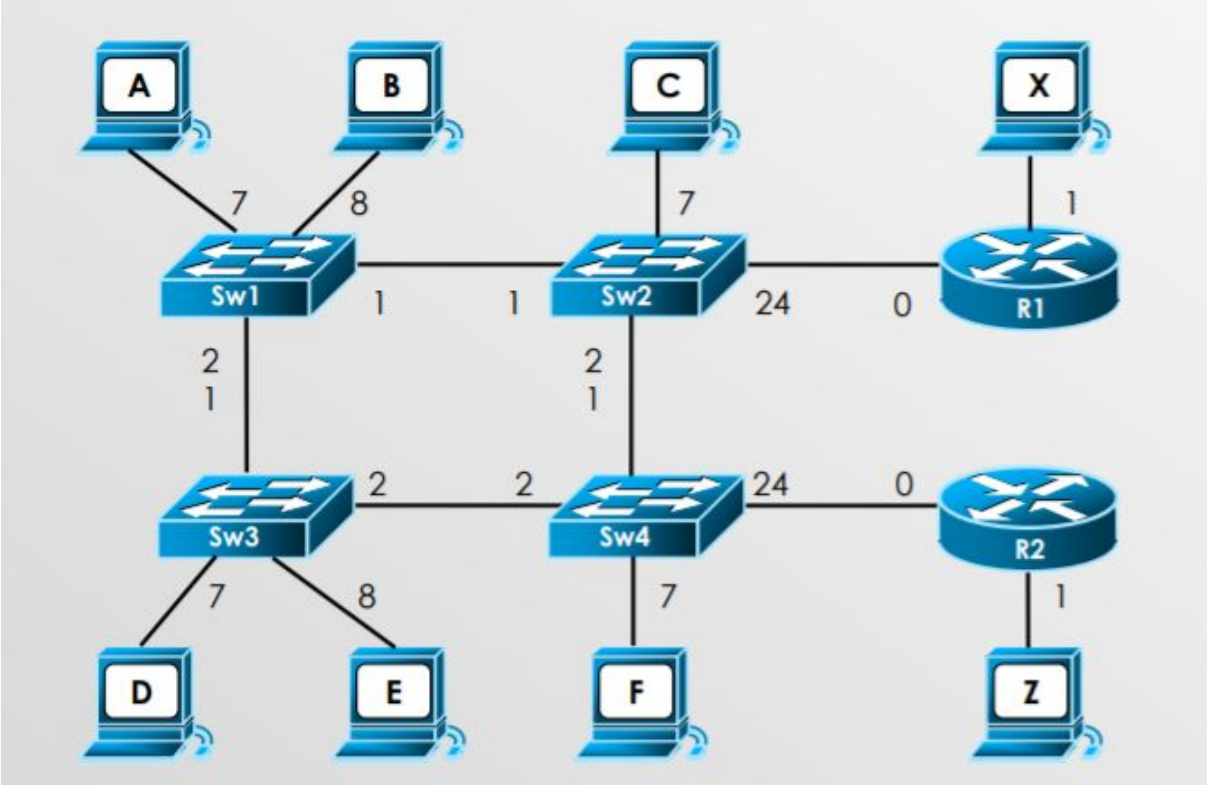


Sunt definite următoarele VLAN-uri: • Porturile cu valori între 2-7 vor fi în VLAN222 • Porturile cu valori mai mari de 8 vor fi în VLAN888 Administratorul se decide să tuneleze traficul între Sw2 şi Sw3 folosind VLAN 500. Scrieţi toate antetele diferite a cadrelor ce apar când sunt trimise următoarele cadre: A→F (şi D→Z).

A → F: MAC A, MAC ISP1 (sus), IP A, IP F; MAC ISP1 (sus), MAC ISP1 (jos), IP ISP1 (sus), IP IPS1 (jos), MAC ISP1 (jos), MAC F, IP A, IP F
D → Z: MAC D, MAC ISP1 (sus), IP D, IP Z; MAC ISP1 (sus), MAC ISP1 (jos), IP ISP1 (sus), IP IPS1 (jos), MAC ISP1 (jos), MAC Z, IP D, IP Z
Nu se ajunge de la D la Z. Traficul va fi tunelat direct spre Sw3.

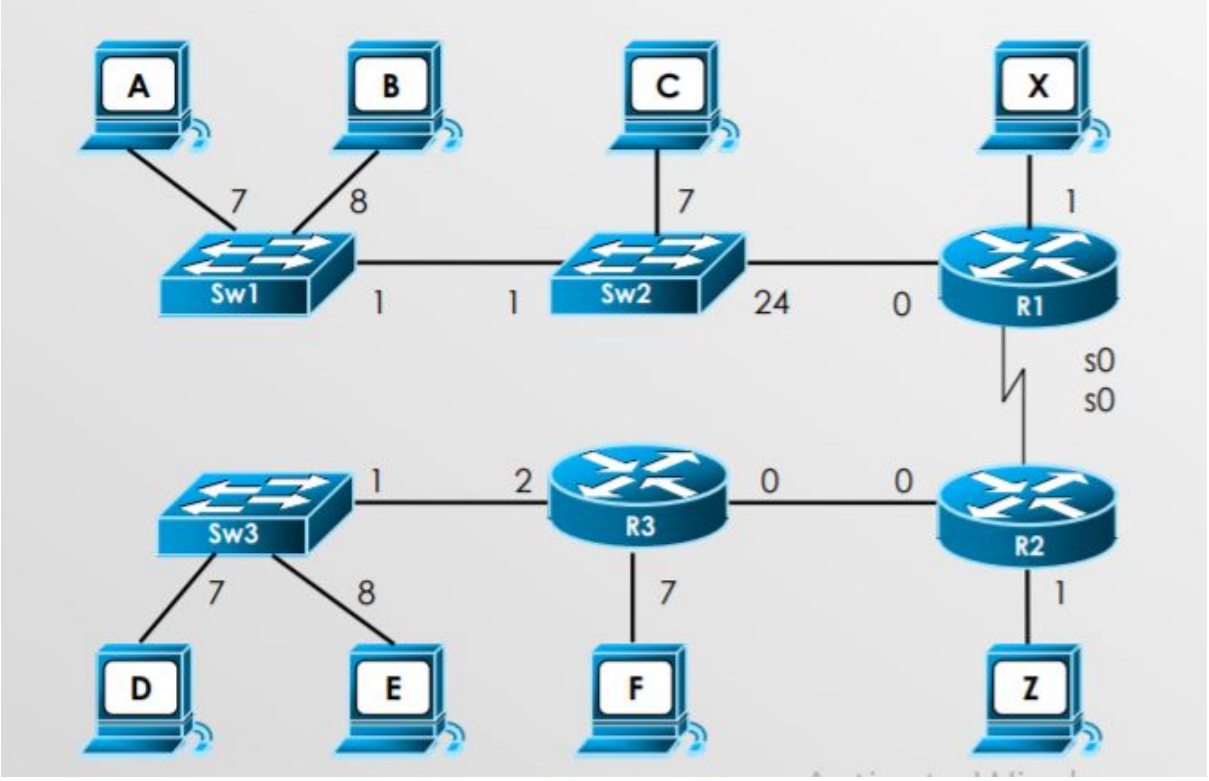
SUBIECTUL 3: SECURITATE:

00: Descrieți un atac DoS inițiat de stația X către stația Z.



Un atac de tip DoS Smurf attack ar insemna ca X sa trimita ping-uri catre reteaua dintre R1 si R2 cu adresa sursa (spoofed) reprezentata de IP-ul lui Z. Toate statiile din retea vor raspunde catre Z, astfel incat Z poate primi mai mult trafic decat poate procesa. Daca Z e un server, X poate face si TCP SYN flood (initiind un numar mare de conexiuni half-open)

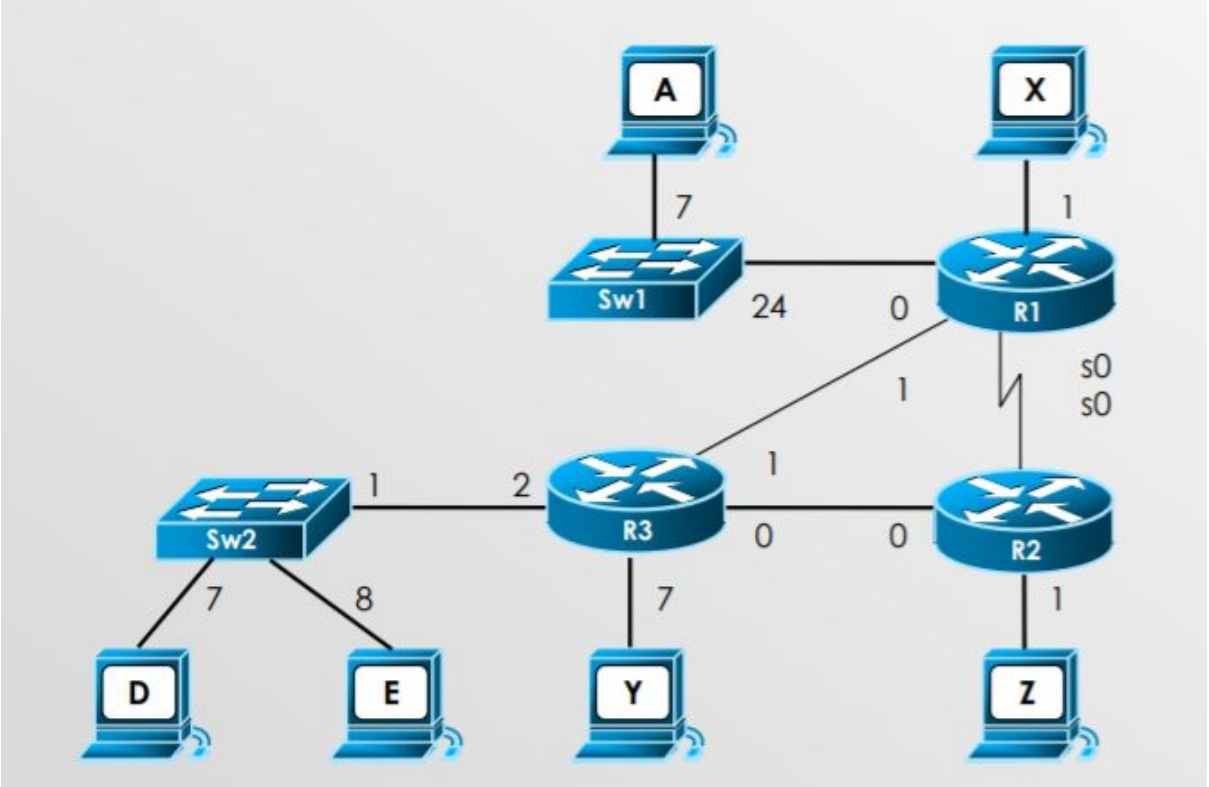
01: Ce antete diferite apar în rețea?



Staţia B iniţiază un atac VLAN hopping. Descrieţi toate antetele cadrelor ce apar în rețea pentru acest atac.

v1 (Switch spoofing): B negociaza o legatura trunk cu SW1 prin DTP, apoi poate trimite trafic (cadre 802.1Q) in orice VLAN care porneste de la el.
v2 (Double tagging - nu necesita DTP): B trebuie sa fie in VLAN-ul nativ de pe un trunk. Pune antet din orice VLAN de atacat si apoi inca un antet din VLAN-ul nativ. Switch-ul inlatura antetul nativ si pachetul va fi comutat pe VLAN-ul de atacat.

02: Ce atacuri poate iniţia staţia D împotriva nodului Y?



Atacuri de tip DoS (vezi ex0).
Si DDoS: smurf attack -- da, este inclus in ex0 tho

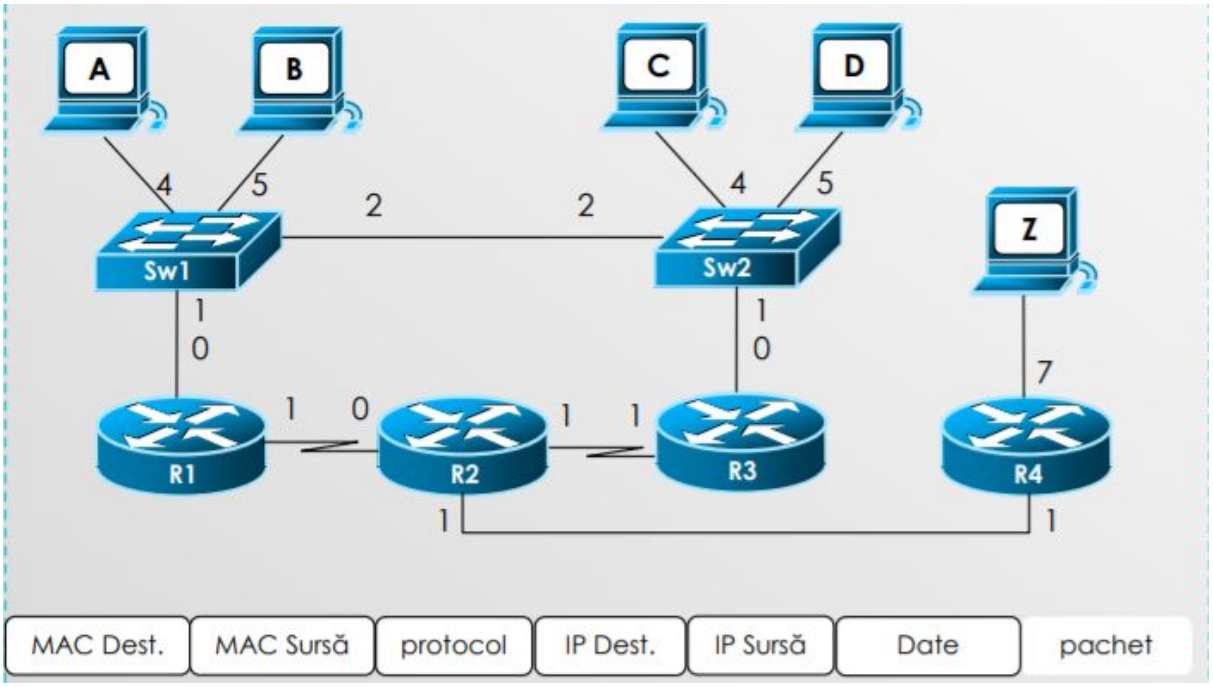
Nu exista nicio retea in topologie cu suficiente statii ca sa poti face un DoS. 2 pinguri pe care le-ar putea primi de la D si E nu sunt suficiente pentru un DoS. -- Asa e, dar teoretic merge. Si o singura statie iti poate congestiona traficul daca trimite junk continuu - ex: SYN attack.

Cred ca un atac de recunostere, cum ar fi un port scan, ar fi realizabil. Sau pentru ceva mai dur, se poate sparge parola de la router cu un dictionar si apoi se poate face un Sniffing (tcpdump sau wireshark pe portul 7).

Daca Y e un server public, cu putine statii si multe procese se poate incerca un Slowloris attack. Dar atlceva de tip DoS nu prea vad.

Port scan poti sa faci doar in retea, D si Y nu sunt in aceeasi retea

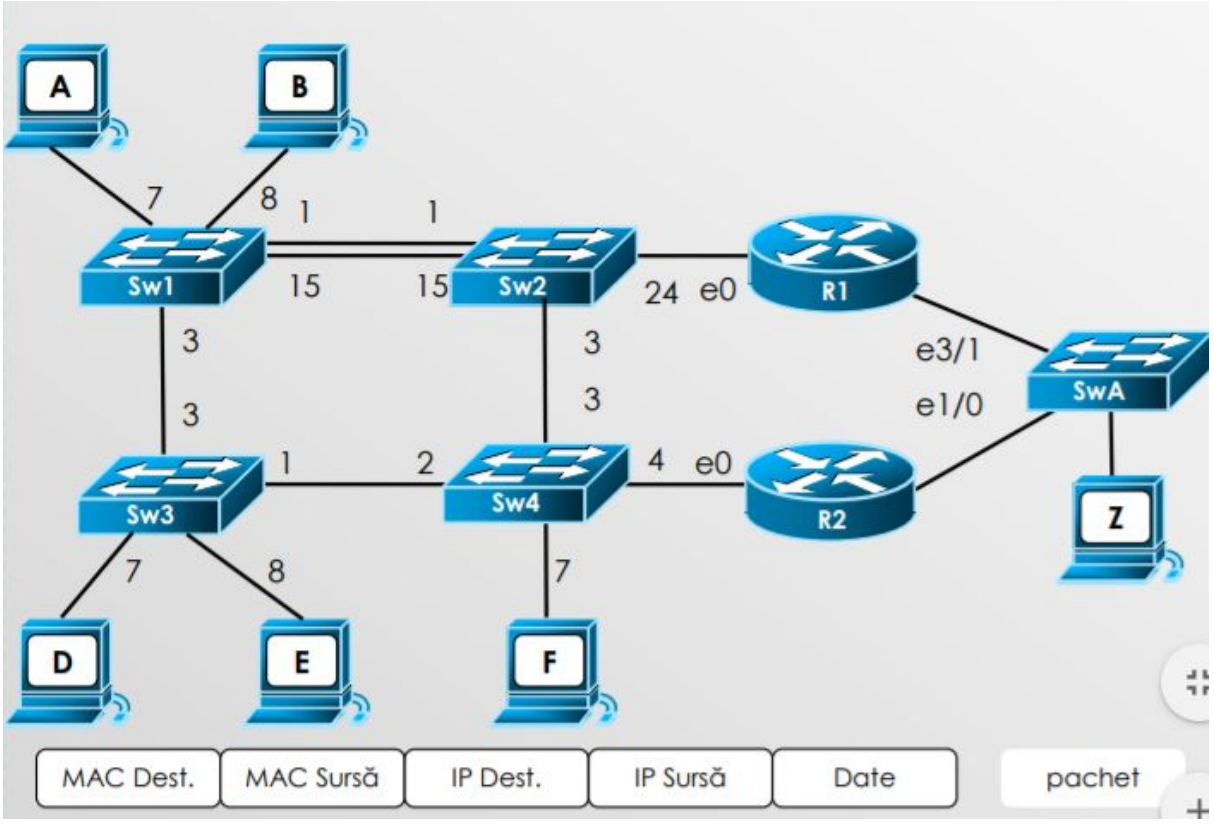
03: Ce impact va avea compromiterea Sw1?



Ce echipamente din rețea vor fi afectate, dacă un atacator obține acces privilegiat pe Sw1?

SW1 va putea initia un atac STP pe SW2 (nu prea are sens, poti detalia te rog? -- STP e un protocol care functioneaza permanent pe switchuri ca sa le stabileasca o ierarhie intre porturi in functie de prioritatea switchurilor; SW1 corupt poate trimite continuu variatii de prioritate proprie spre SW2, care nu mai poate calcula cum trebuie STP si se blocheaza traficul), astfel blocand comunicarea intre toate statiile din retea cu ruterele, implicit cu exteriorul.
De asemenea, poate rescrie tabela CAM (desi nu e un impact la fel de mare ca atacul STP).

04: Ce se modifică în rețea în urma unui atac ARP Poisoning inițiat de pe stația A către F?



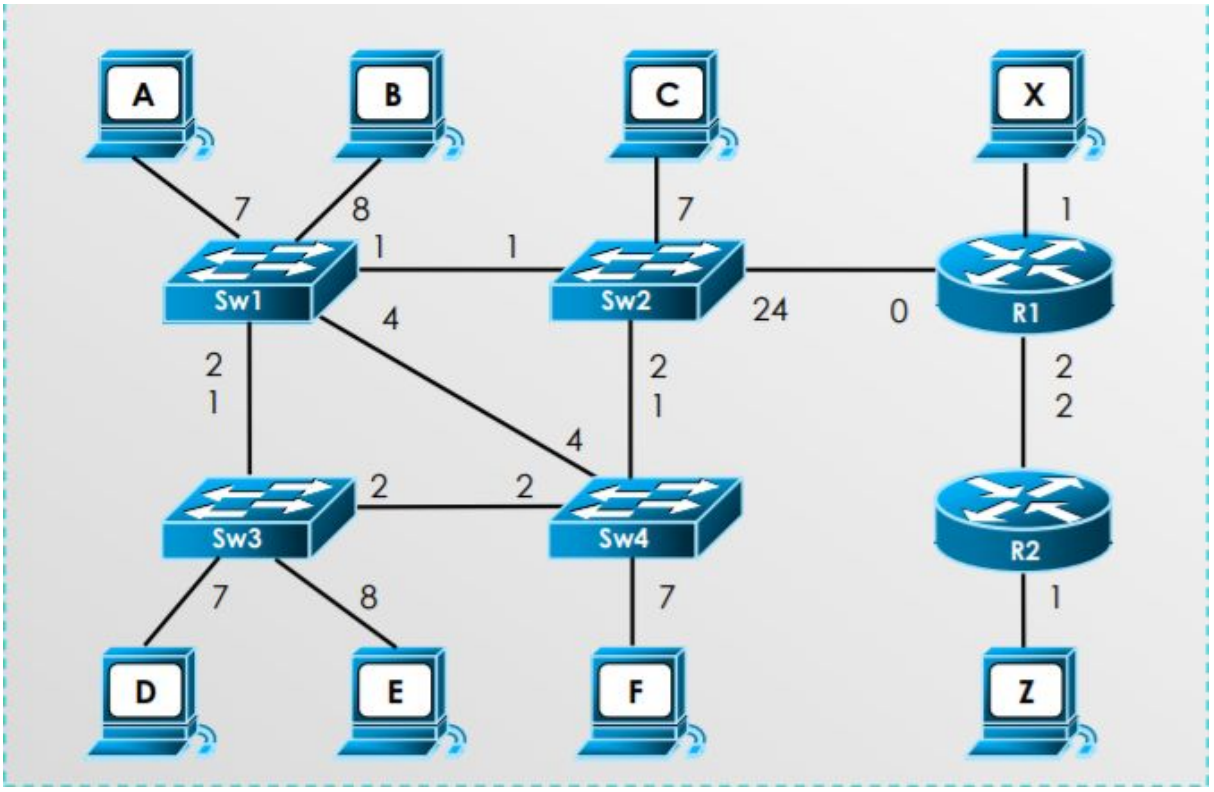
Pe Sw1 se închid porturile 3, 15 Ce se modifică în rețea în urma unui atac ARP Poisoning inițiat de pe stația A către F?.

A va putea minti orice statie ca adresa lui IP este, de fapt, a altei statii din retea, astfel primind traficul care nu ii este destinat, creand un atac de tip MITM. Daca ii trimite lui F un mesaj de tip (StatieX.IP - A.MAC), mesajele din F catre StatieX vor ajunge in A. Apoi A va trimite corect mesajul din F catre StatieX.

ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.

-- Da, poti face si DoS. Tho, cred ca e mult mai convenabil ca atacator, daca poti, sa faci MITM in loc de DoS.

05: Configuraţi securitatea pe R1

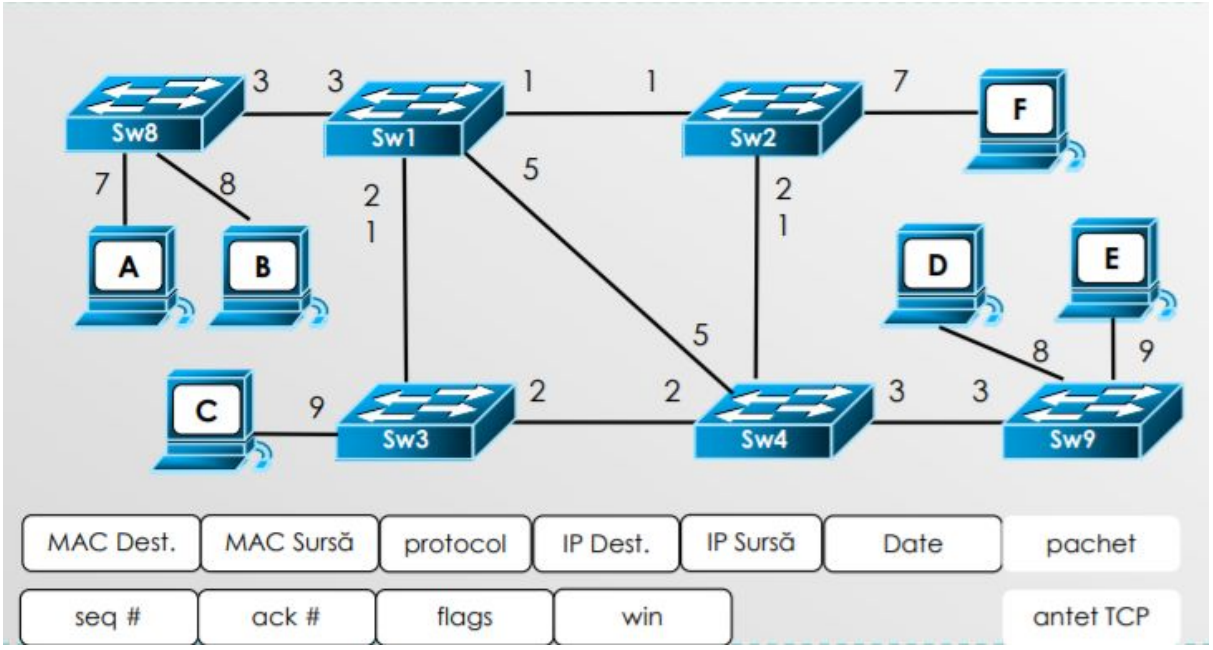


Ruterul R1 va trebui să accepte acces de ssh doar de la staţia X şi să permită doar traficul de web din şi spre reţeaua locală (conectată pe interfaţa Eth0), cu excepţia serverului de monitorizare F ce trebuie să fie accesibil doar în cadrul reţelei locale

Chain: INPUT
-s IP.X -p tcp --dport 22 -j ACCEPT
-p tcp --dport 22 -j DROP

Chain: FORWARD
-s Retea -p tcp --dport 80/443 -j ACCEPT
-d IP.F -j DROP
-d Retea -p tcp --dport 80/443 -j ACCEPT

06: Care este efectul unui atac ARP Poisoning împotriva staţiei F ?

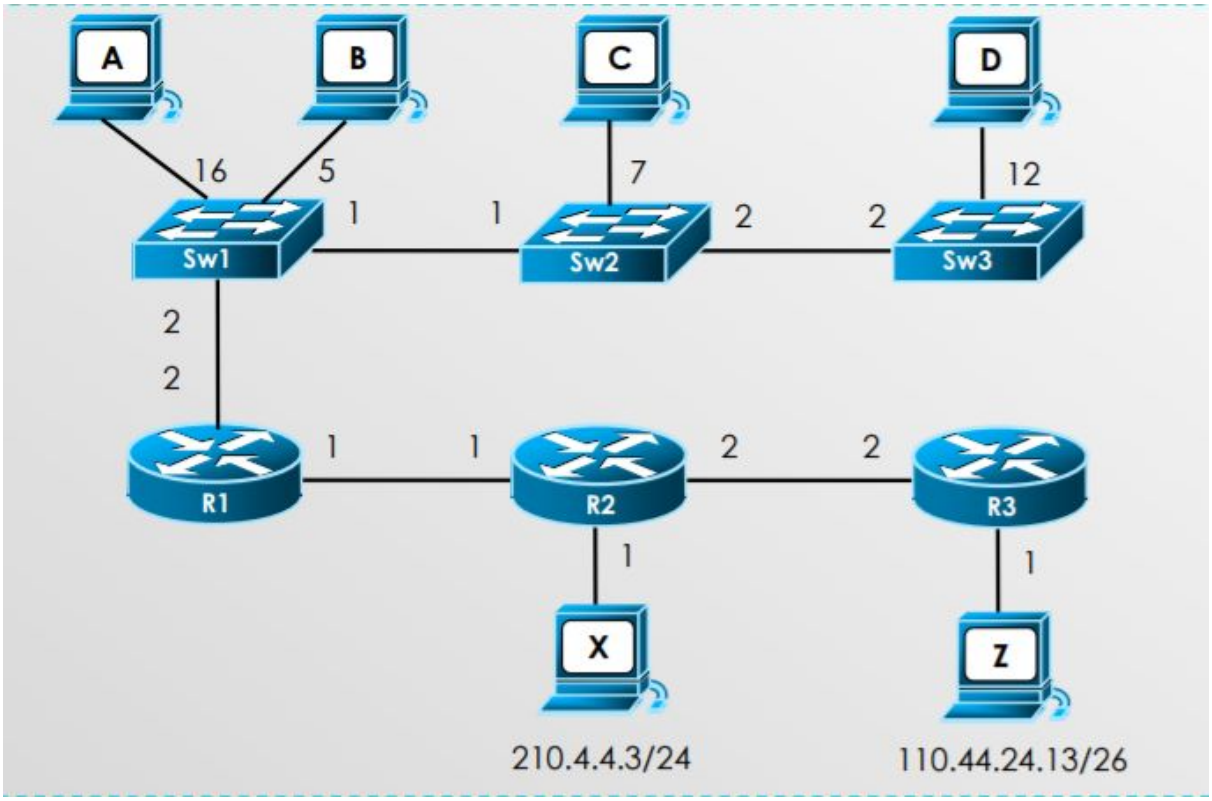


Pe Sw1 sunt închise porturile 1 şi 2. Staţia F este staţia administratorului. Sunt definite următoarele VLAN-uri: VLAN11: A, C VLAN12: B VLAN13: D, E Restul porturilor sunt porturi trunchi cu VLAN nativ 10, inclusiv Sw2,7

Cu ce ma ajuta chestia asta cu VLAN? Ce treaba are cu MITM? -- Teoretic poti face ARP poisoning si MITM doar in VLAN-uri in care ai acces. Daca, spre exemplu, era D corupta, nu F, D putea ataca doar E. F e pe nativ, deci poate trimite oriunde (folosind dubla incapsulare). Probabil e ca sa iti dai seama ca daca se corupe ceva de pe vlan nativ, si restul de VLAN-uri sunt vulnerabile.

Intrucat F este administrator, interceptarea mesajelor folosind ARP poisoning ca metoda de MITM poate corupe mai multe echipamente de retea daca sunt luate datele necesare (exemplu accesarea switchurilor). Totusi, F fiind administrator este posibil sa stie deja asocierile corecte dintre IP si MAC pentru toate statiile astfel incat sa isi dea seama de atac.

07: Configuraţi securitatea pe R3



Ruterul R3 acceptă şi iniţiază conexiuni doar de la/către staţia Z. Pentru reţeaua locală va accepta doar orice trafic destinat staţiei Z, **cu excepţia staţiei X** ce poate comunica cu orice destinaţie din reţeaua locală.

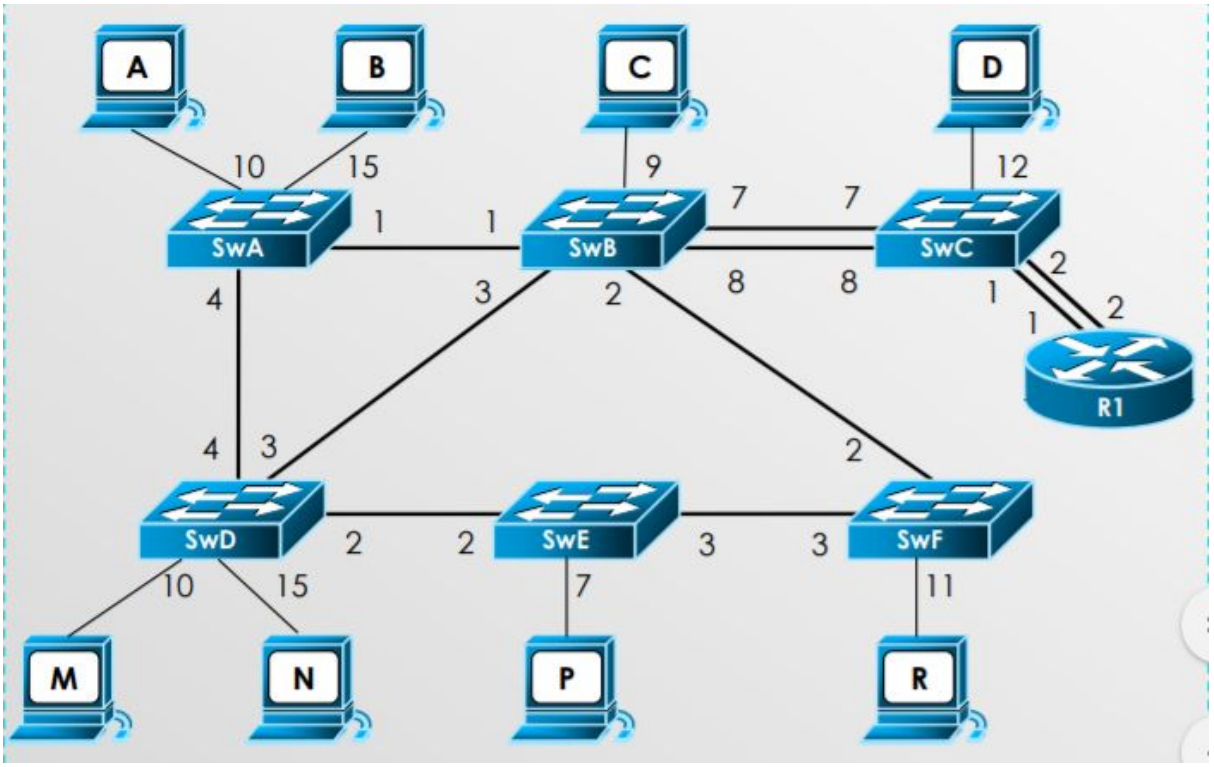
La ce se refera acel `cu exceptia statiei X?`.
Eu am inteles ca X poate comunica cu oricine din reteaua lui Locala, care e pe R2(deci este singur in RL-ul lui). Eu as da drop pe forward la toate pachetele ce vin de la X(pentru ca zice cu exceptia X in cerinta) -- cred ca se refera la reteaua locala R3-Z, fiindca e vorba de R3. Anume pentru reteaua R3-Z va accepta doar ce vine pentru Z, nu si pentru R3/1. Exemplu A poate trimite doar catre Z, nu catre R3/1. X are insa voie sa trimita trafic si la R3/1 si la Z.

Chain: INPUT
-s 110.44.24.13 -j ACCEPT
-i R3/2 -j DROP

Chain: OUTPUT
-d 110.44.24.13 -j ACCEPT
-i R3/2 -j DROP

Chain: FORWARD
-s 210.4.4.3 -j ACCEPT
-d 110.44.24.13 -j ACCEPT
-i R3/2 -j DROP

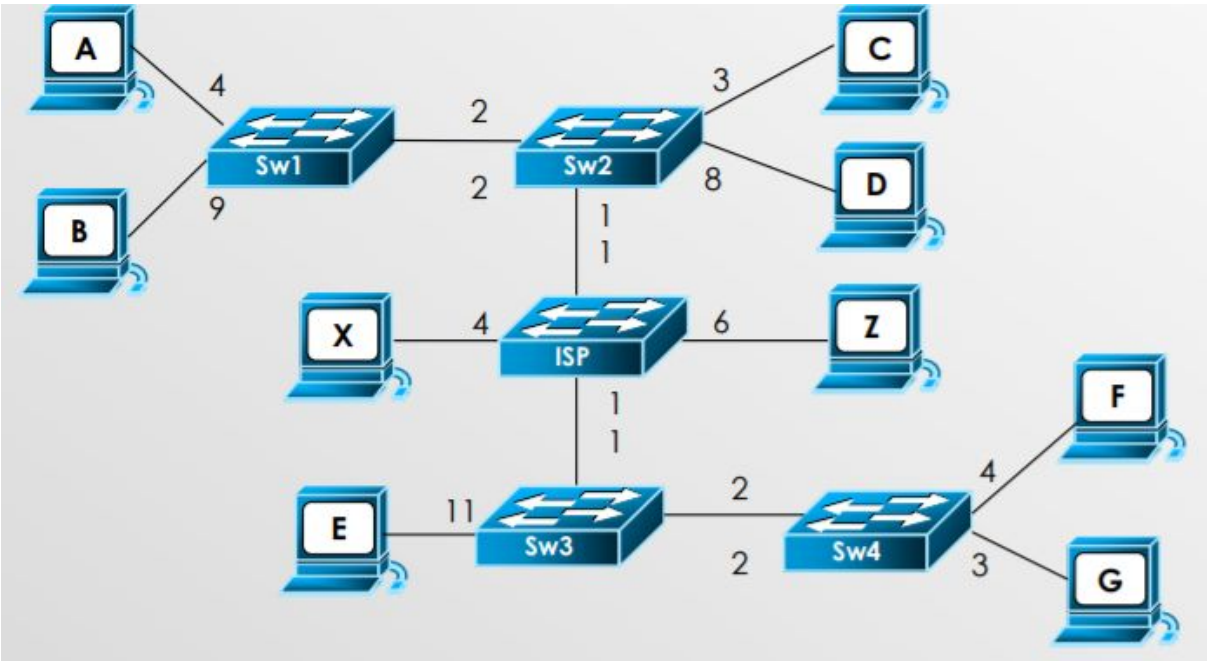
08: Care va fi efectul compromiterii SwE?



În rețea toate porturile pare sunt în VLAN10, cele impare în VLAN9.

SWE poate genera un atac STP in retea, blocand astfel functionarea switchurilor in cascada. Intrucat este conectat pe ambele VLAN-uri, actiunea se poate extinde pana la limita domeniilor de broadcast, afectand SWD si SWA pe VLAN10 si SWF pe VLAN9, dar si statiile legate de acestea.

09 Ce impact va avea compromiterea Staţiei A?



Toate staţiile conectate pe port mai mic de 7 vor fi in VLAN 500. Toate staţiile conectate pe port mai mare de 7 vor fi in VLAN 700. Legăturile dintre Sw1-Sw2 şi Sw3-Sw4 vor fi configurate ca trunchi cu VLAN nativ 500, restul legăturilor vor fi trunchi cu VLAN nativ 1. Ce impact va avea compromiterea Staţiei A?

In primul rand, A poate initia VLAN Hopping deoarece este pe VLAN-ul nativ dintre SW1 si SW2, deci va avea acces pe VLAN 700 (prin dubla incapsulare). Avand acces la atat de multe statii, va putea sa initieze un atac de tip de tip DoS Smurf Attack chiar catre statii la care nu are acces direct. De asemenea, poate incerca un double VLAN Hopping pentru VLAN-urile cu nativ 1, desi este destul de laborios si va necesita o cunoastere buna a retelei in prealabil.