UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Documentatie

-proiect PPRC-

Nume: Péntek Tamás

Specializare: TI

Grupa: 30642

Data: 15.05.2021

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Cuprins

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Laborator 1

In cadrul acestui proiect am realizat tema 5. Dupa citirea cerintelor, primul pas a fost sa aleg topologia. Pentru acest proiect am ales **topologia de tip stea** extinsa, deoarece acest tip este cel mai potrivit pentru cerinta, in acest caz avem un concentrator, de la care putem sa extindem retea si in viitor, este usor de implementat si usor de extins. In cadrul acestei topologii, este o practica buna sa avem niste legaturi si echipamente redundante, daca cade o legatura sau un echipament, atunci o sa avem un echipament de backup, care ajuta la functionarea continua, fara intreruperi si pierderi.

Dupa ce am ales topologia, am deschis programul Packet Tracker si am pus echipamentele, iar dupa aceea am interconectat aceste componente. Intre componente de acelasi tip (in cazul meu, intre switchuri) punem legaturi de tip cross-over, iar intre dispozitive diferite folosim legatura de tip straight-through.

In cerinta proiectului apare ca utilizatorii trebuie sa aiba posibilitatea de a conecta la retea atat prin cablu cat si prin wireless, din acest motiv, pe langa switchuri, am folosit si un Access Point (AP). Atat switchul, cat si Access Pointul lucreaza cu adrese MAC, dar AP este mai inteligent, AP foloseste protocolul pentru conexiuni wireless 802.11. O adresa MAC este adresa asociata fiecarui dispozitiv cu placa de retea, aceasta adresa se seteaza la fabrica si este alcatuita din doua parti: cei mai semnificativi biti arata producatorul, iar cei mai putin semnificativi biti se refera la numarul de serie a dispozitivului.

Pe langa switchuri si Access Pointuri, mai folosim niste end device-uri, si anume laptop si tableta si un alt dispozitiv de retea, un router. Switch-ul este un echipament de nivel 2, lucreaza cu adrese MAC, iar un router este un echipament de nivel 3, aceasta foloseste adrese IP.

Prima data am facut toate configurarile pentru o singura cladire, iar la final pe baza acestor configurari am mai creat inca doau topologii, pentru cele doua cladiri.

Dupa ce am avut toate dispozitivele conectate, am setat VLAN-ul in cazul switchurilor. VLAN-urile folosim pentru a crea un domeniu mai redus de broadcast, cream niste camere virtuale la care sunt conectate dispozitivele care comunica frecvent, de exemplu dispozitivele de la HR sunt in acelasi VLAN sau dispozitivele de la acelasi etaj sunt in acelasi VLAN, daca exista o comunicare frecventa dintre dispozitive. Este o practica buna sa cream mereu macar un VLAN si sa asignam acestui VLAN toate porturile unui switch, pentru ca daca lasam porturile in VLAN-ul default, sunt sanse mari ca un atacator intra foarte usor in retea noastra si obtine niste informatii confidentiale. VLAN-ul trebuie setat pe fiecare switch, pentru acesta am folosit comenzile *switchport mode access si switchport access vlan x,* unde x arata numarul VLAN-ului la care vrem sa asignam portul. O alta tehnica buna este sa denumim fiecare echipament altfel, in acest fel va fi mai usor identificarea in viitor.

Dupa ce am creat si am setat VLAN-ul pe fiecare switch, am configurat si AP-ul: am pus un text la SSID, acest text va apare la fiecare dispozitive care vede retea wireless in jurul lui, iar

ca sa securizam conectarea la retea am pus si o parola de tip WPA2, care foloseste encriptarea de tip AES. O ultima configurare in cazul AP-ului a fost alegerea Channel-ului, am ales 1, 6 si 11 in cazul celor 3 cladiri, in acest fel nu o sa deranjeze fiecare AP pe celalalt, deoarece aceste channel-uri nu au zone de frecvente comune, prin care scapam de interferenta si in acest fel o sa avem un semnal bun si continuu in fiecare cladire.

Dupa aceea am setat protocolul de Spanning Tree, care creaaza o bucla logica si folosim acest protocol ca sa cream mai multe legaturi intre dispozitive (daca cade o legatura sa avem o legatura de backup), si acest protocol gestioneaza aceste legaturi, ca sa avem o singura legatura activa la un moment dat, ca sa nu blocam cealalta legatura si sa nu consumam latimea de banda. In cazul acestui protocol am ales un bridge radacina (initial este ales by default dupa adresa MAC), si am ales switchul care este cel mai aproape de router, in acest fel am asigurat ca o transmisie de date de la router are acelasi cost, indiferent pe ce legatura trec datele sau la ce dispozitiv ajung datele. Ca sa alegem radacina, trebuie sa setam prioritatea la 0, acest lucru facem folosind comanda *spanning-tree vlan x priority 0*, unde x se refera la VLAN/VLAN-uri.

Urmeaza sa selectam adresele de IP si sa asignam fiecarei interfete folosita o adresa IP. Retea initila are adresa de IP 172.27.0.0/16, dar trebuie sa cream cateva subretele, fiecare cu 200 de hosturi. Ca sa asiguram acest numar, avem nevoie de 8 biti (in acest fel o sa avem 256-2 hosturi in fiecare subretea). In acest fel noua masca va fi 255.255.255.0 si cele 3 subretele o sa aiba adresa: 172.27.2.0/24, 172.27.3.0/24, 172.27.4.0/24. Din aceste subretele alegem 4 adrese de IP fixe, 1 pentru router si 3 pentru cele 3 switchuri (de exemplu 172.27.2.1 – gateway, 172.27.2.2 – switch1, 172.27.2.3 – switch2, 172.27.2.4 – switch3). Restul adreselor (de exemplu 172.27.2.5-254) sunt asignate automat, folosind DHCP. La fiecare dispozitiv (in afara de router) trebuie sa setam gateway-ul, care reprezinta adresa de IP a router-ului. Aceste configurari sunt realizate pe switchuri folosind comenzile: *ip address ipAdd mask; no shutdown; ip default-gateway gwAdd.* In cazul end device-uri nu trebuie sa facem aceste configurari, deorece se face automat, folosind DHCP. Ca sa functioneze DHCP, trebuie sa configuram pe router: *dhcp excluded-address startIP endIP; dhcp pool vlan_name; network ipAdd mask; default-router routerIP*. Cu aceste comenzi setam adresele de IP care vrem sa excludem (adresele deja asignate la router si switchuri), VLAN-ul in care folosim aceste adrese de IP si specificam adresa de IP a retelei si adresa de IP a routerului.

Dupa ce am terminat cu toate configurarile testam daca subretea functioneaza corect folosind comanda *ping* din command prompt-ul fiecarui dispozitiv. Pe langa aceste, pe parcurs putem sa verificam daca am setat corect cateva configurari folosind comanda *show x*, unde x poate sa fie *vlan* sau *spanning-tree*.

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Laborator 2

La acest laborator, primul pas a fost sa punem niste etichete pe langa fiecare subretea, in acest fel a fost mai usor sa identificam fiecare retea. Taskul principal la acest laborator a fost sa legam subretelele din cele trei cladiri, ca sa putem sa comunicam si sa trimitem date intre cladiri. Am pus mai multe legaturi intre routere, in acest fel putem sa garantam redundanta, daca pica o legatura intre 2 cladiri, o sa avem o legatura backup si in acest fel garantam continuitatea serviciilor. Ca sa conectam cele 3 routere din cele 3 cladiri, am folosit fibra optica. Dupa ce am facut legaturile, am configurat adresele IP pe fiecare router, in fiecare subretea. Pentru acesta, am mai folosit 3 subretele si anume: 172.27.5.0/24, 172.27.6.0/24, 172.27.7.0/24. Din aceste subretele am ales niste adrese IP si am asignat aceste adrese IP la porturile routerelor cu urmatoarele comenzi: *interface fastEthernet X, ip address IP_add net_mask, no shutdown*, unde X reprezinta numarul portului de tip fastEthernet, iar IP_add este adresa IP si net_mask este masca de retea.

Ca sa asiguram ca porturile au fost configurate cu succes, am verificat conexiunile intre routere folosind comanda *ping, show interface fastEthernet X* si *show running-config* unde X reprezinta numarul portului. Deoarece adresele IP sunt tratate de routere (adica de dispozitive de nivel 3 ISO/OSI) si fiindca routerele folosesc tabele de rutare pentru a trimite date dintr-o subretea in cealalta subretea, ar trebuit sa configuram tabela de rutare pe fiecare router. Cu comanda *show ip route* putem sa vizualizam tabela de rutare pe un router.

Pornim **protocolul OSPF** pe fiecare router si in acest fel va fi actualizat tabela de rutare pe fiecare router si ajungem din orice retea definita in orice cealalta retea definita. Pentru a configura protocolul OSPF pe un router trebuie sa rulam comanda *router ospf 1* dupa care trebuie sa enumeram cele 3 subretele, cu care acest router trebuie sa comunice: de exemplu *network 172.27.**2**.0 0.0.0.255 area 0, network 172.27.**5**.0 0.0.0.255 area 0, network 172.27.**6**.0 0.0.0.255 area 0.* Dupa aceea mai ramane un singur pas, ca sa definim ca si pasiv interfata la care este conectata fiecare switch principal din fiecare subretea. Acest lucru trebuie facut din motive de securitate, ca sa nu lasam goala nicio poarta pentru atacatori. Definim o interfata ca si pasiv cu urmatoarea comanda: *passive-interface fastEthernet X,* unde X reprezinta numarul interfetei.

Dupa ce am configurat fiecare router, putem sa verificam ca totul functioneaza bine pe fiecare router cu comanda *show ip route*. Pe langa acesta verificam si daca putem sa comunicam intre cladiri, acest lucru realizam cu comanda *ping* adica facem mai multe ping-uri intre diferite device-uri care se afla in diferite cladiri, in diferite subretele. Daca simulam caderea unei legaturi intre cele 3 routere, putem sa observam ca fiecare router actualizeaza tabela de rutare, iar daca punem inapoi legatura, iarasi se schimba fiecare tabel de rutare. Cu aceste operatii, putem sa asiguram ca tot sistemul functioneaza corect, si intr-adevar avem o comunicare intre cele 3 cladiri.

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Laborator 3

In cadrul acestui laborator, primul pas a fost sa setam DMZ, adica zona demilitarizata. In mod normal, avem retea interna, unde avem toate datele esentiale (parole, credentiale, documente de companie, etc) si trebuie sa securizam foarte bine aceasta retea, ca ceilalti din afara retelei sa nu aiba acces la aceste fisiere. Pe langa acesta, avem retea externa, adica internetul, si totusi, retea interna trebuie sa accese retea externa, nu putem sa blocam retea interna, ca altfel companie nu poate sa functioneze. Din aceste motive, trebuie sa proiectam o zona in care este permis accesul de la retea interna catre retea de internet si invers, iar in aceasta zona punem 4 servere: HTTP, FTP, DNS si MAIL care vor avea adrese publice.

Prima data am pus cele 4 servere, pe langa fiecare am pus notite, ca sa stim exact tipul serverului, dupa care cele 4 servere am legat la un switch, iar switch-ul am legat la un router. Urmatorul pas a fost sa configuram VLAN-ul, nu lasam VLAN-ul implicit din motive de securitate. Am creat un VLAN cu nume DMZ pe switch , dupa care asignam fiecare interfata acestui VLAN cu comenzile: *vlan 2; name DMZ; interface range fastEthernet 0/1-24; switchport mode access; switchport access vlan 2*, dupa care am verificat cu comanda *show vlan*, daca intr-adevar a fost creat noul VLAN.

Dupa aceea, am configurat interfata fastEthernet 1/0 pe router cu adresa 210.2.2.65/27, aceasta adresa reprezentand default gateway-ul. Pe fiecare server creat, am configurat adresa IP, gateway, DNS server in mod static, fara sa folosim DHCP, deorece vrem sa pastram aceeasi adresa de IP pentru fiecare server, nu vrem sa asignam dinamic, daca facem schimbari cu DHCP: server HTTP: 210.2.2.66, server FTP: 210.2.2.67, server DNS: 210.2.2.68, server EMAIL: 210.2.2.69. La adresa serverului DNS punem la fiecare server adresa 210.2.2.68, care reprezinta serverul de DNS nou creat. Dupa ce am terminat cu cele 4 servere, am configurat vlan-ul, adresa IP si default-gateway-ul pe switch: *interface vlan 2; ip address 210.2.2.70 255.255.255.224; no shutdown; ip default-gateway 210.2.2.65*. Ca sa testam daca exista comunicatie intre cele 4 servere si gateway, am rulat cateva ping-uri. Ca sa avem acces la aceste servere si din celalalte 3 retele, trebuie sa configuram protocolul OSPF pe router-ul la care am legat switch-ul nou: *router ospf 1; network 210.2.2.64 0.0.0.31 area 0; passive-interface fastEthernet 1/0.* Ca sa verificam daca fiecare router a invatat retea 210.2.2.64, am folosit comanda *show ip route.*

Urmatorul pas a fost sa verific daca end device-urile din fiecare retea pot sa comunice cu cele 4 servere, pentru aceasta am folosit ping. Ca sa setez noul server DNS pe fiecare device folosind DHCP, am configurat serverul DHCP pe fiecare router cu urmatoarele comenzi: *ip dhcp pool Net2/Net3/Net4; dns-server 210.2.2.68.* In acest fel, nu trebuie sa setez noul server DNS pe fiecare device, prin DHCP se actualizeaza automat adresa serverului DNS.

Dupa aceea, am configurat cele 4 servere. Am inceput cu HTTP server, ca sa personalizam pagina, am schimbat titlul in fisierul index.html de la Welcome text la numele meu. Un pas importat este sa introducem pe serverul de DNS maparea www.tamas.ro => 210.2.2.66, aceasta mapare am facut si cazul serverelor FPT si EMAIL. Pentru a testa aceasta

nou pagina, am intrat de pe mai multe device-uri pe pagina www.tamas.ro si mi-a aparut noua pagina de index.html.

Dupa serverul HTTP, urmeaza serverul FTP, am creat un nou user tamas, cu parola tamas, dupa care am testat pe un end device daca functioneaza serverul FTP: am incarcat si am descarcat cate un fisier folosind comenzile *put* si *get*.

Ultimul pas a fost sa configurez serverul de email, am creat 2 utilizatori tamas1 si tamas2 si am configurat email-ul pe doua laptopuri cu cele 2 users. Ca sa testez daca serverul de EMAIL functioneaza corect, prima data am folosit doar un singur user: adresa de send si receive este aceeasi. In acest caz am observat ca intr-adevar pot sa trimit un mail pentru acelasi utilizator, dupa care am testat si cu 2 users: de pe un laptop am trimis un mail pe un alt laptop, adica un user a trimis un email celuilalt user folosind acelasi server de EMAIL. In ambele cazuri am primit email-urile, prin care m-am asigurat ca pe langa serverul de HTTP, DNS si FTP, functioneaza si serverul de EMAIL.

Laborator 4

In cadrul acestui laborator, task-ul principal a fost conectarea retelei interne cu un Internet Service Provider. Pentru acesta, am pus un router de ISP. Deoerece in router-ul principal (la care sunt conectate serverele) nu am mai avut loc, ar trebuit sa introducem un slot nou de Ethernet in router. Ca sa introducem slotul, prima data trebuie sa oprim routerul, dar inainte de asta trebuie sa salvam configurarile cu comanda *write memory*. Atat in routerul principla, cat si in router ISP am intodus un slot de Gigabit Ethernet, pentru ca pe aceasta legatura o sa avem un trafic mare de date, deorece toata retea noastra o sa comunice pe aceasta legatura cu ISP si cu Internet.

Dupa ce am conectat cele doua routere cu fibra optica, am configurat adresele pe ambele routere cu comanda: *interface gigabitEthernet 6/0, ip address 210.2.2.33/34 255.255.255.224, no shutdown*. Ca sa testam conexiunea intre cele doua routere, am folosit comanda *ping*.

Ca sa comunicam cu retea externa, adica cu Internet, trebuie sa avem adrese publice. Pana la acest moment noi am avut doar niste adrese private cu care am comunicat si am trimis date in retea interna. Ca sa obtinem niste adrese publice, avem 2 posibilitati: Proxy si translatare de adrese. In cadrul acestui laborator am implementat translatarea de adrese: routerul ia pachetul de la adresa private si transmite mai departe pe o adresa publica catre routerul de ISP, practic inlocuieste adresa privata din request cu o adresa publica si aceasta mapare intre adresa privata si publica este salvata in tabela de translatare. Ca sa configuram acest lucru pe routerul principal, folosim NAT-ul clasic.

Primul pas a fost sa configuram NAT pool-ul dupa care am configurat si lista de control al accesului cu urmatoarele comenzi: *nat pool tamas 210.2.2.35 210.2.2.62 netmask*

255.255.255.224, access-list 10 permit 172.27.0.0 0.0.255.255, ip nat inside source list 10 pool tamas. Practic cu acesta comenzi am configurat adresele publice posibile (210.2.2.35 – 210.2.2.62) si faptul ca poate sa primeasca o adresa publica orice adresa privata din retea 172.27.0.0. Dupa ce am terminat cu aceste configurari, am configurat interfetele routerului, cel care merge spre ISP va fi o interfata de tip outside, la interfata care merge catre servere nu punem nimic si la restul interfetelor punem inside: *interface fastEthernet 0/0, ip nat inside; interface fastEthernet 4/0, ip nat inside; interface fastEthernet 5/0, ip nat inside; interface gigabitEthernet 6/0, ip nat outside*. La final testam daca translatarea functioneaza corect folosind comanda *ip nat translations* pe routerul principal.

Ca sa simulam retea de internet, am pus o retea alcatuita dintr-un switch, un laptop si un server. Punem legaturile intre dispozitive dupa care setam adresele IP (100.0.0.1/8 – default gateway, 100.0.0.2/8 – server si 100.0.0.3/8 – laptop) si testam conectivitatea cu comanda *ping*. Ca sa asiguram comunicarea intre retea noastra si internet, configuram o rutare statica catre adresa 0.0.0.0 folosind ca si next hop adresa 210.2.2.33: *ip route 0.0.0.0 0.0.0.0 210.2.2.33*. Aceasta configurare este facuta pe routerul principal, care este conectat cu router ISP si cu servere. Pe langa acesta, mai configuram si protocolul OSPF: *router ospf 1, default-information originate*. Dupa ce am terminat cu aceste configurari, verificam pe cele trei routere daca avem o rutare corecta catre internet, cu comanda *show ip route.*

Ultimul pas este sa configuram inca o rutare statica, ca sa avem o comunicare intre routerul de ISP si fiecare server (HTTP, DNS, etc.), pentru ca pana acum am configurat doar retea interna. Acest lucru facem cu comanda: *ip route 210.2.2.64 255.255.255.224 210.2.2.34.* Dupa ce am terminat si cu aceasta configurare, testam cu comanda *ping* daca exista comunicare intre diferitele dispozitive (de exemplu intre o tableta si laptop de pe internet sau intre serverul de HTTP si laptop de pe internet).

Laborator 5

La ultimul laborator, scopul principal a fost sa setam serviciul de DNS si EMAIL pe retea mai mica, care este alcatuita dintr-un switch, laptop si server si care practic simuleaza retea de internet si sa securizam retea. Deoarece este vorba despre o retea destul de mica, am setat atat serviciul de DNS, cat si serviciul de EMAIL pe acelasi server, nu am configurat diferite servere pentru fiecare serviciu.

Primul pas a fost sa setam serviciul de DNS pe server, adica sa adaugam adresa de IP a serverului de email. Pentru a verifica daca sistemul functioneaza corect, am testat de pe laptop conexiunea folosind comanda ping: *ping mail.tamas.com.* Dupa ce am configurat DNS-ul, am configurat si servicul de EMAIL: am creat domain name (mail.tamas.com) si am creat un nou user (tamas3). Urmatorul pas a fost sa setez utilizatorul pe laptop, si sa trimit un mail la aceeasi adresa de email ca sa verific functionalitatea.

Ca sa asiguram trimiterea unui mail intre cele doua retele, adica intre retea companiei si retea care simuleaza internetul, am adaugat adresa de IP a serverelor de EMAIL in ambele servere de DNS. Pentru a testa functionalitatea, am trimis un email de pe un laptop care se afla intr-o cladire a companiei catre laptopul care se afla in retea mica. Acest email a ajuns cu succes, dupa care am dat un reply la acest email, in acest fel am verificat daca functioneaza serverele de email in ambele directii, adica pot sa trimit si sa receptionez email-uri de la companie catre retea mica si invers.

Dupa aceea, am configurat routerul principal ca sa pot sa configurez remote. Pentru aceasta am avut 2 posibilitati: sa folosesc telnet sau ssh. Fiindca ssh este mai safe, decat telnet, am configurat conexiunea prin ssh pe routerul principal. Cu comanda *show privilege* am posibilitatea sa verific la care nivel de privilegiu sunt. Pentru accesarea routerului principal in mod remote, am creat 3 utilizatori, fiecare cu un nivel de privilegiu diferit: *username u1 privilege 1 password u1, username u2 privilege 7 password u2, username u3 privilege 15 password u3*. Dupa aceea am verifica daca au fost create utilizatorii cu comanda *show running-config.*

Dupa ce am creat utilizatorii, am configurat protocolul ssh pe router-ul principal: prima data am schimbat hostname-ul routerului: *hostname MainRouter*, dupa care urmeaza configurarea: *ip domain -name tamas.ro, crypto key generate rsa (*cu aceasta comanda setez algoritmul RSA ca si algoritm de criptare care foloseste criptarea asimetrica cu public si private keys), *line vty 0 2, transport input ssh, login local* (cu aceasta comanda specific ca utilizatorii care pot sa acceseze routerul remote, sunt definite local, in router). Dupa ce am terminat cu configurarea protocolului ssh, am testat daca pot sa accesez routerul principal de pe un laptop ruland comanda *ssh -l u7 210.2.2.65*. Ultimul pas a fost sa setez o parola pe routerul principal ca sa pot sa intru in mod privilegiat si cand accesez routerul in mod remote: *enable secret u15*; dupa care am testat tot asa, de pe un laptop daca pot sa accesez modul privilegiat in mod remote.

Pe parcursul laboratoarelor de PPRC am reusit sa urmaresc pe domnul profesor si am reusit sa configurez fiecare dispozitiv (laptop, tablet, server, switch, router). Pe langa acesta am testat cu succes fiecare dispozitiv configurat, din care reiese faptul ca toate dispozitivele configurate functioneaza corect. Ceea ce nu am reusit sa adaug la acest proiect este sa implementez doua masuri suplimentare de securizare a retelei. Ca si masura suplimentara pentru a securiza retea ar fi: sa configurez un server AAA; sa configurez un server de syslog, sa adaug extended access-list sau sa configurez port-security pe switchuri.

UNIVERSITATEA TEHNICĂ
DIN CLUJ-NAPOCA

Topologia finala a proiectului