AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Abbaszadə Aysel Rövşən qızı
Aşurov Ülvi İzzət oğlu
Babayeva Gülmirə Nazim qızı
Quliyev Elgün Arzu oğlu
Rəsulzadə Fərid Ehtibar oğlu

Korporativ şirkətin şəbəkə infrastrukturunun layihələndirilməsi, simulyasiyası və analizi

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter sistemləri və şəbəkələri"

Elmi rəhbər: **t.e.n., Dosent Cəfərov Nizami Duman oğlu**

BAKI – 2023

MÜNDƏRİCAT

İxtisarların siyahısı

VLAN – Virtual Local Area Network;

IP – Internet Protocol;

SSH – Secure Shell;

DHCP – Dynamic Host Confiquration Protocol;

WAP – Wireless Application Protocol;

WLC – Wireless LAN Controller;

WAN – Wide Area Network;

PT – Packet Tracer;

IOS – Internetwork Operation System;

RIP – Routing Information Protocol;

EIGRP – Enhanced Interior Gateway Routing Protocol;

IDPS – Intrusion Detection and Prevention Systems *(Müdaxilənin Aşkarlanması və Qarşısının Alınması Sistemləri)*;

DLP – Data Loss/Leak Prevention *(Məlumat İtkisinin Qarşısının Alınması)*;

DAC – Discretionary Access Control *(İxtiyari Giriş Nəzarəti)*;

RBAC – Role-Based Access Control (*Rol Əsaslı Giriş Nəzarəti)*;

ABAC – Attribute-Based Access Control (*Atribut Əsaslı Giriş Nəzarəti)*;

MAC – Mandatory Access Control *(Məcburi Giriş Nəzarəti)*;

CCTV – Closed Circuit Television *(Qapalı Dövrəli Televiziya)*;

UPS – Uninterruptible Power Supply *(Fasiləsiz Enerji Təchizatı)*;

OSPF – Open Shortest Path First.

Giriş

Mövzunun aktuallığı. Korporativ şirkət şəbəkə infrastrukturunun dizaynı, simulyasiyası və təhlili işinin aktuallığı bugünkü texnoloji əsaslı biznes mənzərəsində böyük əhəmiyyət kəsb edir. Bir-birinə bağlı sistemlərə və verilənlərə əsaslanan proseslərə artan etibarla, yaxşı dizayn edilmiş şəbəkə infrastrukturu müxtəlif şöbələr və yerlərdə hamar və səmərəli kommunikasiya, məlumat ötürülməsi və əməkdaşlığı təmin edir. Simulyasiya və təhlil vasitəsilə potensial darboğazlar, zəifliklər və miqyaslılıq problemləri müəyyən oluna və proaktiv şəkildə həll oluna bilər, fasilələri minimuma endirir və ümumi şəbəkə performansını optimallaşdırır. Bu hərtərəfli yanaşma bizneslərə məhsuldarlığı artırmağa, əməliyyatları sadələşdirməyə və getdikcə bir-biri ilə əlaqəli və dinamik bazarda rəqabət üstünlüyünü qorumağa imkan verir.

İşin məqsədi. Təşkilat daxilində məlumat və resursların səmərəli və təhlükəsiz hərəkətini təmin etməkdir. Şəbəkə arxitekturasını diqqətlə tərtib etməklə şirkətlər onların əməliyyat ehtiyaclarını və gələcək böyüməsini dəstəkləyən etibarlı və genişlənə bilən infrastruktur yarada bilərlər. Simulyasiya müxtəlif şəbəkə ssenarilərini və konfiqurasiyalarını sınaqdan keçirməyə imkan verir.

Tədqiqat metodları və texnologiyaları. Tezis texnologiyası, Drag&Drop, İyerarxik Şəbəkə Dizaynı, Şəbəkə cihazlarının düzgün kabellərlə birləşdirilməsi, VLAN-ların yaradılması və portlara VLAN nömrələrinin təyin edilməsi, Alt şəbəkə və IP ünvanlanması, İnter-VLAN marşrutlaşdırmanın konfiqurasiyası, DHCP Serverinin konfiqurasiyası, SSH konfiqurasiyası, texnologiyalarından,simulyasiya və layihələndirmə metodlarından və analiz mərhələsindən istifadə edilmişdir.

İşin strukturu və həcmi. İş 97 səhifədən ibarətdir. 5 fəsil və 14 paraqrafdan təşkil olunub. 150 şəkil və 1 cədvəl mövcuddur. İşdə 10 ədəbiyyatdan istifadə olunmuşdur.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Aşurov Ülvi İzzət oğlu

CISCO PACKET TRACER PAKET ŞƏBƏKƏ SİMULYASİYASININ TƏTBİQİNİN ÜSTÜNLÜKLƏRİ

Mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter sistemləri və şəbəkələri"

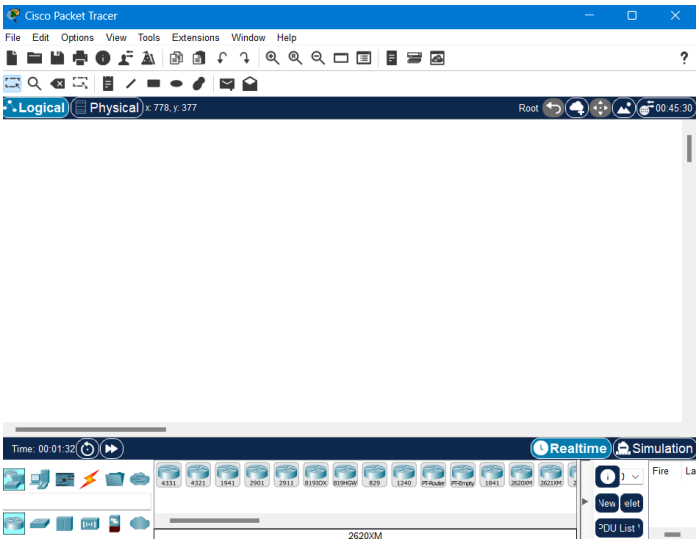
Elmi rəhbər: **t.e.n., Dosent Cəfərov Nizami Duman oğlu**

BAKI – 2023

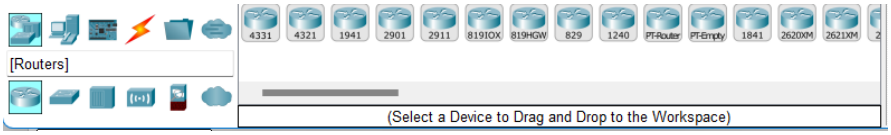
I FƏSİL. CISCO PACKET TRACER PAKET ŞƏBƏKƏ SİMULYASİYASININ TƏTBİQİNİN ÜSTÜNLÜKLƏRİ

1.1. Cisco Packet Tracer şəbəkə modelləməsi

Şəbəkədə serverlər, marşrutlaşdırıcılar, kommutatorlar kimi cihazları fiziki olaraq istifadə etmək əvəzinə, virtual mühitdə real mühit şəraitinə yaxın simulyasiya etməyə imkan verən proqramlar mövcuddur. Bu fəsildə Cisco Packet Tracer proqramı (Şək.1.1) ilə korporativ şirkətin şəbəkə modelləşdirilməsi və təhlili aparılacaqdır. Packet Tracer Cisco Systems üçün işləyən Dennis Frezzo tərəfindən hazırlanmış şəbəkə protokolu simulyatorudur [1,2].



Şəkil 1.1. Packet Tracer ekran görüntüsü.

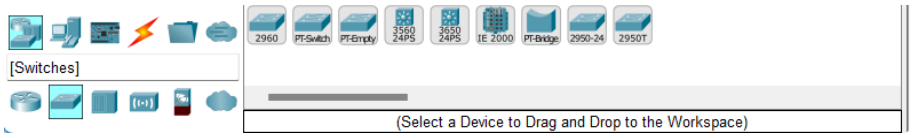


Şəkil 1.2. Yönləndirmə cihazları

Bu nişanlar marşrutlaşdırıcıları (Şək.1.2) vizual şəkildə təmsil etmək və xüsusi marşrutlaşdırıcı modellərini müəyyən etmək və seçmək üçün sürətli istinad təmin etmək üçün istifadə olunur.

Ümumi Router İkonunun işarəsi ümumi marşrutlaşdırıcını təmsil edir və tez-tez xüsusi dizaynı və ya seriyası olmayan əsas marşrutlaşdırıcı modelləri üçün istifadə olunur. O, adətən kiçik dairələr və ya kvadratlarla təmsil olunan çoxsaylı port və ya

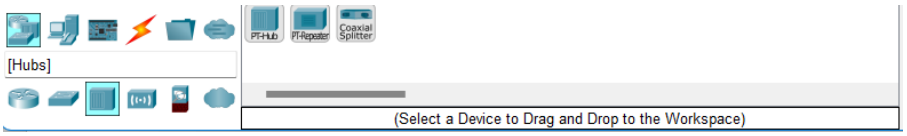
interfeysləri olan düzbucaqlı formaya malikdir. Cisco 1941 marşrutlaşdırıcısı nişanı Cisco 1941 seriyalı marşrutlaşdırıcını təmsil etmək üçün istifadə olunur. O, adətən fərqli əyri küncləri olan düzbucaqlı qutuya bənzəyir və ön tərəfdə "1941" model nömrəsini göstərir. Xüsusi nişanlar və onların görünüşü proqramın versiyasından və yeniləmələrindən asılı olaraq dəyişə bilər.



Şəkil 1.3. Keçidlər

Cisco Packet Tracer-də keçid nişanları (Şək.1.3) şəbəkə topologiyalarında istifadə üçün mövcud olan müxtəlif keçid modellərinin qrafik təsvirləridir. Bu nişanlar açarları əyani şəkildə təsvir edir və xüsusi keçid modellərini müəyyən etmək və seçmək üçün sürətli istinad təmin edir.

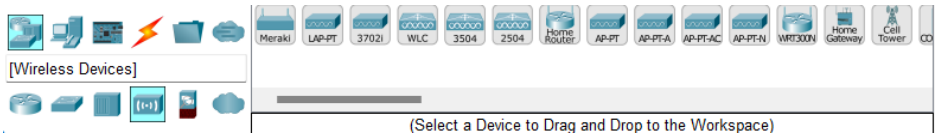
Ümumi keçid nişanının işarəsi ümumi keçidi təmsil edir və tez-tez xüsusi dizaynı və ya seriyası olmayan əsas keçid modelləri üçün istifadə olunur. O, adətən kiçik kvadratlar və ya dairələrlə təmsil olunan çoxsaylı portlar və ya interfeysləri olan düzbucaqlı formaya malikdir. Cisco Catalyst 2960 keçid nişanı Cisco Catalyst 2960 seriyalı açarları təmsil edir. O, adətən fərqli əyri küncləri olan düzbucaqlı qutuya bənzəyir və ön tərəfdə "2960" model nömrəsini göstərir. Cisco 3560 keçid nişanı Cisco Catalyst 3560 seriyalı açarları təmsil etmək üçün istifadə olunur. O, Cisco Catalyst 2960 ikonasına oxşar dizayna malikdir, lakin ön tərəfdə model nömrəsi "3560" göstərilir. Cisco 3750 keçid nişanı Cisco Catalyst 3750 seriyalı açarları təmsil edir. O, adətən yuvarlaq küncləri olan düzbucaqlı formaya malikdir və ön tərəfdə "3750" model nömrəsini göstərir. Cisco 2960 Yığcam Keçid İkonası: Cisco 2960 Yığcam keçid işarəsi Cisco Catalyst 2960 açarlarının yığcam modellərini təmsil etmək üçün istifadə olunur. Digər keçid nişanları ilə müqayisədə daha kiçik forma faktoruna malik ola bilər.



Şəkil 1.4. Qovşaqlar.

Qovşaqlar (Şək.1.4) cihaz əlaqələri üçün əlavə portlar təmin etməklə şəbəkənin əhatə dairəsini genişləndirmək üçün istifadə olunur. Məlumat paketlərini yalnız nəzərdə tutulan alıcıya yönləndirmək üçün intellektə malik olan açarlardan fərqli olaraq, hublar yayım rejimində işləyir. Məlumat paketi mərkəzə çatdıqda, o, təkrarlanır və nəzərdə tutulan təyinat yerindən asılı olmayaraq bütün qoşulmuş cihazlara göndərilir. Bu o deməkdir ki, hub-a qoşulmuş bütün qurğular hər bir paketi qəbul edir və paketin onlar üçün nəzərdə tutulub-tutulmadığını müəyyən etmək ayrı-ayrı cihazlardan asılıdır.

Qovşaqlar ümumiyyətlə açarlardan daha az səmərəli hesab olunur, çünki onlar daha çox toqquşma və şəbəkə sıxlığı yaradır. Birdən çox cihaz eyni vaxtda məlumat ötürməyə çalışdıqda toqquşmalar baş verir və bu, şəbəkə performansının azalmasına səbəb olur. Qovşaqların kommutatorlar kimi şəbəkə trafikini idarə etmək imkanı olmadığı üçün onlar paketləri xüsusi cihazlara prioritetləşdirə və ya yönləndirə bilməzlər.



Şəkil 1.5. Simsiz qurğular.

Simsiz cihazlar (Şək.1.5) fiziki kabellərə və ya simli birləşmələrə ehtiyac olmadan məlumat ötürə və mübadilə edə bilən elektron cihazlara aiddir. Bu cihazlar radio dalğaları və ya infraqırmızı siqnallar kimi simsiz texnologiyalardan istifadə edərək məlumatların efir dalğaları üzərindən ötürülməsi və qəbul edilməsi üçün istifadə olunur.

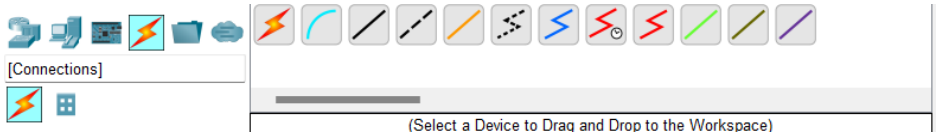
Cisco Packet Tracer-də şəbəkə topologiyalarında müxtəlif növ simsiz cihazları təmsil etmək üçün müxtəlif simsiz cihaz nişanları mövcuddur. Bu nişanlar simsiz cihazları vizual olaraq təmsil edir və simsiz şəbəkələrin dizaynında və simulyasiyasında kömək edir.

Simsiz Router İkonu: Bu işarə ənənəvi simli marşrutlaşdırıcının funksionallığını simsiz giriş imkanları ilə birləşdirən simsiz marşrutlaşdırıcını təmsil edir. O, adətən ondan çıxan simsiz siqnal dalğaları olan düzbucaqlı qutuya bənzəyir.

Simsiz Giriş Nöqtəsi (WAP) İkonu: Simsiz giriş nöqtəsi simvolu simsiz cihazların simli şəbəkəyə qoşulmasına imkan verən cihazı təmsil edir. O, adətən ondan çıxan simsiz siqnal dalğaları ilə kiçik kvadrat və ya düzbucaqlı qutuya bənzəyir.

Wireless LAN Controller (WLC) İkonu: Simsiz LAN nəzarətçi ikonu simsiz şəbəkədə çoxsaylı giriş nöqtələrini idarə edən və idarə edən mərkəzləşdirilmiş cihazı təmsil edir. O, adətən simsiz siqnal dalğaları olan düzbucaqlı qutuya bənzəyir və göstərilən əlavə idarəetmə xüsusiyyətlərinə malik ola bilər.

Simsiz Müştəri İkonu: Bu işarə simsiz şəbəkəyə qoşulan noutbuk və ya smartfon kimi simsiz müştəri cihazını təmsil edir. O, adətən noutbuk və ya mobil telefon kimi cihazın formasına bənzəyir.



Şəkil 1.6. Kabellər

Cisco Packet Tracer-də şəbəkə cihazları arasında müxtəlif növ əlaqələri təmsil etmək üçün müxtəlif əlaqə nişanları (Şək.1.6) mövcuddur. Bu nişanlar edilən əlaqə növünü vizual olaraq təsvir edir və şəbəkə topologiyalarının layihələndirilməsi və simulyasiyasına kömək edir. Cisco Packet Tracer-də rastlaşa biləcəyiniz bəzi ümumi əlaqə nişanları bunlardır:

Ethernet Bağlantısı İkonu: Bu işarə şəbəkə cihazları arasında simli Ethernet bağlantısını təmsil edir. O, adətən hər iki ucunda birləşdiriciləri olan Ethernet kabelinə bənzəyir.

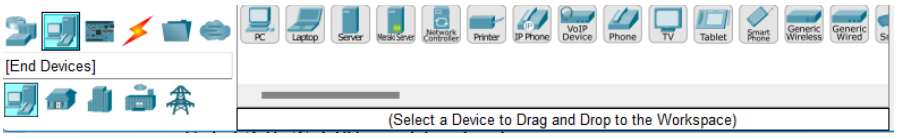
Serial Bağlantı İkonu: Serial qoşulma nişanı tez-tez marşrutlaşdırıcıları və ya digər şəbəkə cihazlarını birləşdirmək üçün istifadə olunan serial əlaqəni təmsil edir. O, adətən hər bir ucunda serial konnektoru olan kabelə bənzəyir.

Konsol Bağlantısı İkonu: Konsol bağlantısı ikonu şəbəkə cihazlarının komanda xətti interfeysinə (CLI) daxil olmaq üçün istifadə edilən konsol bağlantısını təmsil edir. O, adətən bir ucunda konsol konnektoru, digərində isə serial konnektoru olan kabelə bənzəyir.

Fiber Optik Bağlantı İkonu: Bu işarə yüksək sürətli və uzun məsafəli məlumat

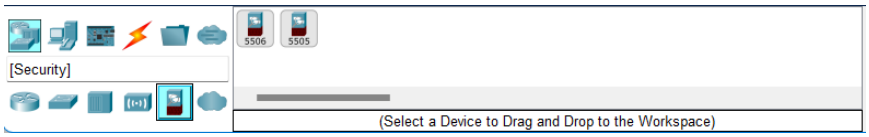
ötürülməsi üçün istifadə olunan fiber optik əlaqəni təmsil edir. Adətən hər iki ucunda fiber optik birləşdiriciləri olan kabelə bənzəyir.

Simsiz Bağlantı İkonu: Simsiz əlaqə nişanı şəbəkə cihazları arasında simsiz əlaqəni təmsil edir. O, adətən simsiz siqnalları təmsil edən əyri xətlərə və ya dalğalara bənzəyir.



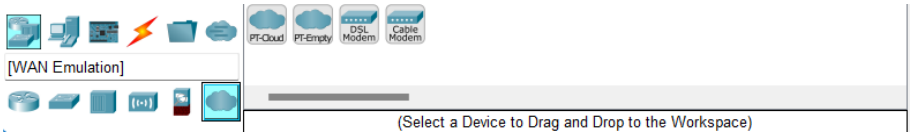
Şəkil 1.7. Son istifadəçi cihazları.

Cisco Packet Tracer tipik şəbəkə infrastrukturunda olan müxtəlif növ şəbəkə cihazlarını simulyasiya etmək və təmsil etmək üçün istifadə edilə bilən müxtəlif son cihazlar (Şək.1.7) təklif edir. Bu son cihazlar real şəbəkə cihazlarının funksionallığını və davranışını təqlid etmək üçün nəzərdə tutulmuşdur.



Şəkil 1.8. Təhlükəsizlik cihazları.

Cisco Packet Tracer istifadəçilərə şəbəkə təhlükəsizliyi konsepsiyalarını (Şək.1.8) tədqiq etməyə və simulyasiya etməyə imkan verən müxtəlif təhlükəsizlik xüsusiyyətləri və funksiyaları ehtiva edir. O, xüsusi təhlükəsizlik cihazları və ya alətləri ilə eyni səviyyəli təhlükəsizlik xüsusiyyətlərini təklif etməsə də, simulyasiya edilmiş şəbəkə mühitində təhlükəsizlik konfiqurasiyalarını öyrənmək və tətbiq etmək üçün platforma təqdim edir.



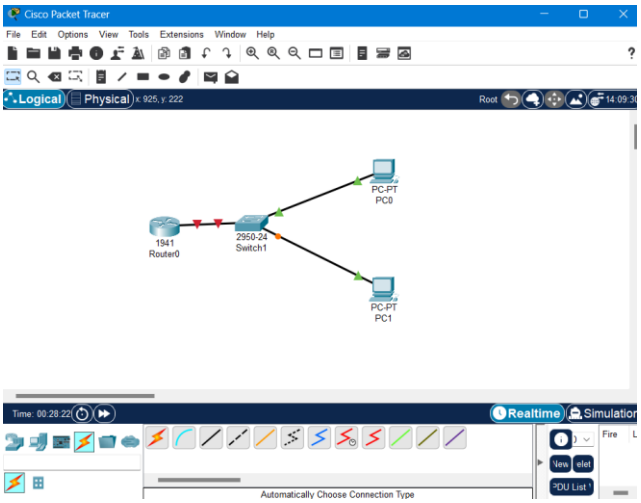
Şəkil 1.9. Qlobal şəbəkənin elementləri.

Cisco Packet Tracer istifadəçilərə proqram daxilində Wide Area Network (WAN) (Şək.1.9) əlaqələrini simulyasiya etməyə imkan verən WAN emulyasiya xüsusiyyətləri təklif edir. Bu xüsusiyyətlər istifadəçilərə virtual WAN bağlantıları yaratmağa, WAN texnologiyalarını konfiqurasiya etməyə və coğrafi cəhətdən səpələnmiş yerlərdə

şəbəkə davranışını simulyasiya etməyə imkan verir. Cisco Packet Tracer-də PT Bulud (Packet Tracer Cloud) istifadəçilərə bulud əsaslı şəbəkədən istifadə edərək Geniş Sahə Şəbəkəsi (WAN) əlaqələrini simulyasiya etməyə imkan verən xüsusiyyətdir.

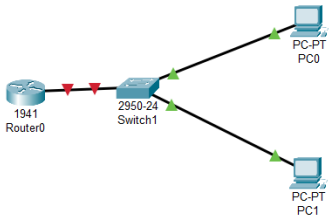
PT Cloud WAN bağlantısını simulyasiya edərək, internet üzərindən bir çox şəbəkə yerini birləşdirən virtual şəbəkə xidməti təminatçısını təmsil edir. PT Bulud, adətən marşrutlaşdırıcılar və ya şəbəkə yerləri arasında şəbəkə topologiyasında yerləşdirilən Paket İzləyicisində bir cihaz kimi təmsil olunur. WAN bağlantısını asanlaşdıran bulud əsaslı xidmət təminatçısı kimi çıxış edir.

Simulyator ekranında istifadə edəcəyimiz şəbəkə cihazları sol alt küncdə texniki xüsusiyyətləri ilə birlikdə verilmiş modellər seçilərək şəkildə göstərilən boş yerə sürüklə və burax idarəsi ilə yerləşdirilə bilər. Qurğuları bir-birinə bağlamaq üçün istifadə edilən kabel tipi seçildikdən sonra qoşulacaq modelin üzərinə klikləməklə portlar müəyyən edilərək əlaqə qurulur. Bu dizayn yalnız real mühitdə fiziki əlaqəyə bərabərdir və sonra konfiqurasiya parametrləri cihazlarda tətbiq olunacaq [3,4].



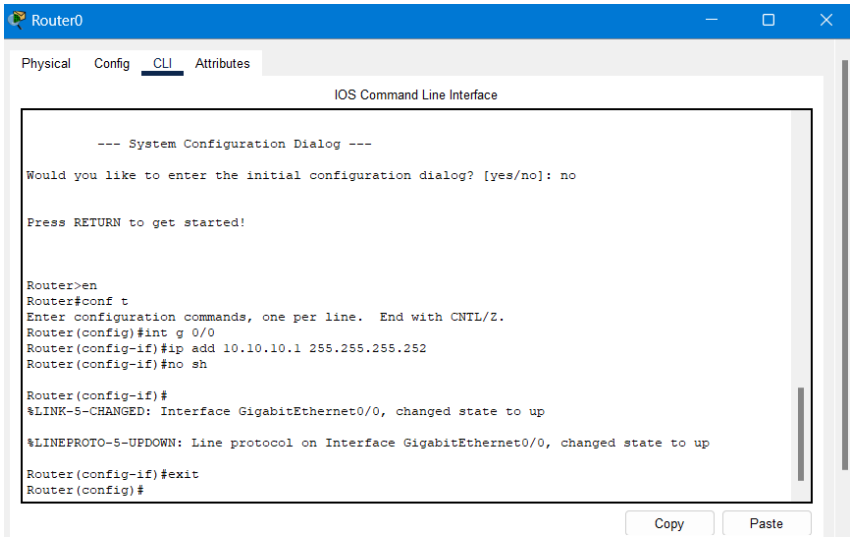
Şəkil 1.10. Packet Tracer-də şəbəkə dizaynı

Bir router, açar və iki kompüterdən ibarət sadə bir şəbəkə dizaynı (Şək.1.10) üçün aşağıdakı kimi bir topologiyadan istifadə edərək (Şək.1.11) paketlərin orta çatdırılma müddətini ölçmək mümkündür.



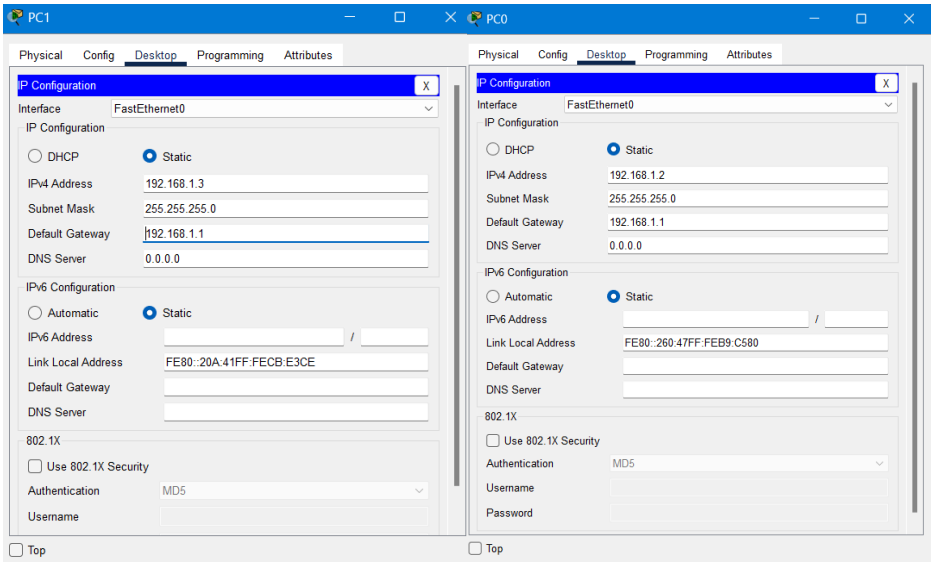
Şəkil 1.11. Şəbəkə topologiyasına aid bir nümunə

Konfiqurasiya (Şək.1.12) parametrləri üçün keçid və marşrutlaşdırıcının IP ünvanları və port bağlantısı parametrlər cihazda IOS əməliyyat sisteminin komanda xətti interfeysi nişanında kodlanır [5].



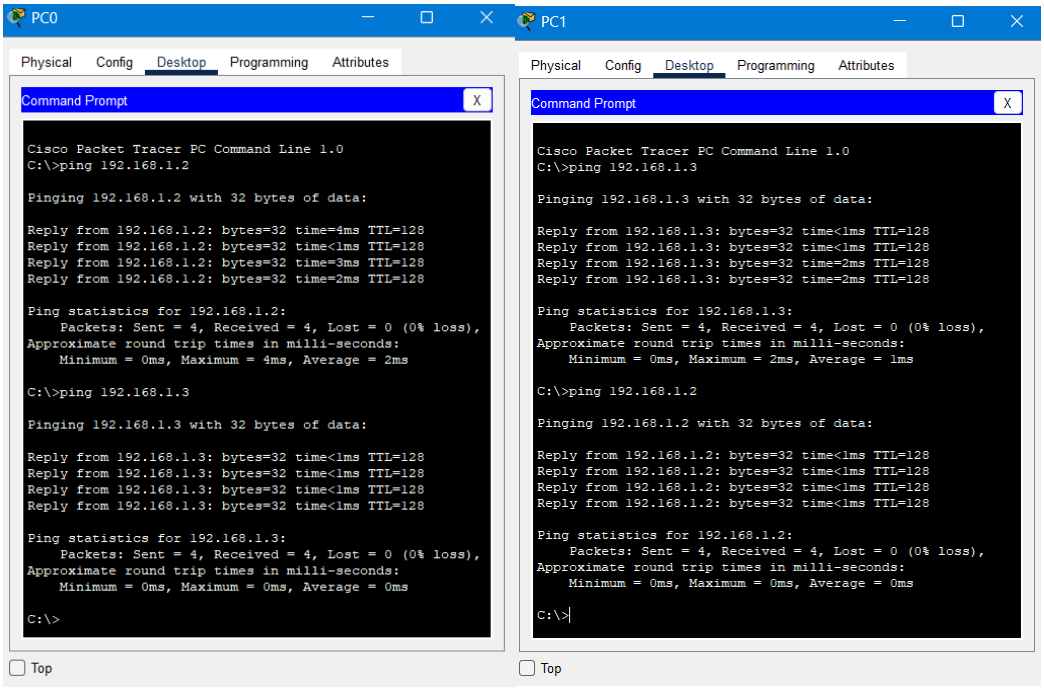
Şəkil 1.12. Router konfiqurasiyası.

Kompüterlərin İP ünvanını təyin etmək üçün (Şək.1.13) kompüter simulyasiya interfeysində təriflər aparılır.



Şəkil 1.13. IP konfiqurasiya parametrləri.

Kompüterin komanda ekranından şəbəkənin mövcudluğuna nəzarət etmək üçün digər şəbəkə elementlərinə ping paketi göndərilir (Şək.1.14). Müşahidə olunan vaxt kompüterdən marşrutlaşdırıcıya 1 millisaniyə, kompüterdən kompüterə isə 1 millisaniyədən az olaraq müəyyən edilmişdir [4].

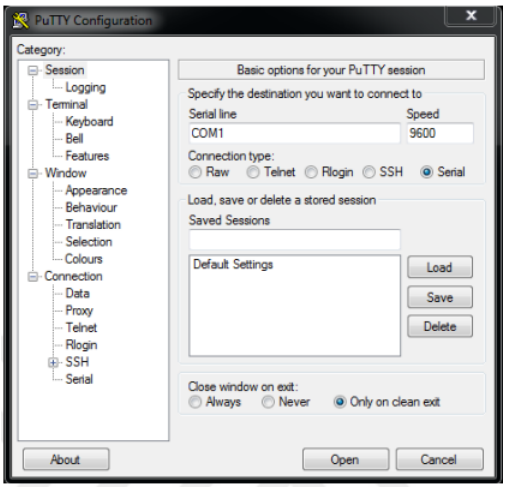


Şəkil 1.14. Kompüterin əmr ekranı

1.2. Real mühitdə şəbəkə modelinin analizi

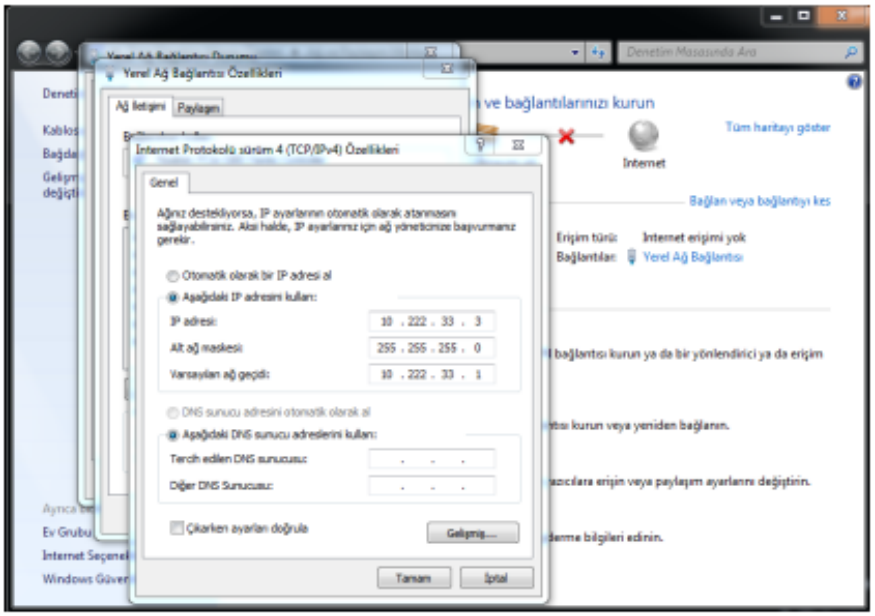
Simulyasiya mühitində tərtib etdiyimiz eyni şəbəkə topologiyasını, onun iki kompüter, keçid və marşrutlaşdırıcı ilə qarşılıqlı əlaqəsini müşahidə etmək üçün real mühit yaradılmışdır.

Simulyasiya mühitində olduğu kimi, konfiqurasiya parametrlərini etmək üçün marşrutlaşdırıcıdan başlayaraq cihazda şəbəkə ünvanları və port bağlantısı parametrləri IOS əməliyyat sisteminin komanda xətti interfeysi pəncərəsində Putty tətbiqi (Şək.1.15) vasitəsilə edildi.

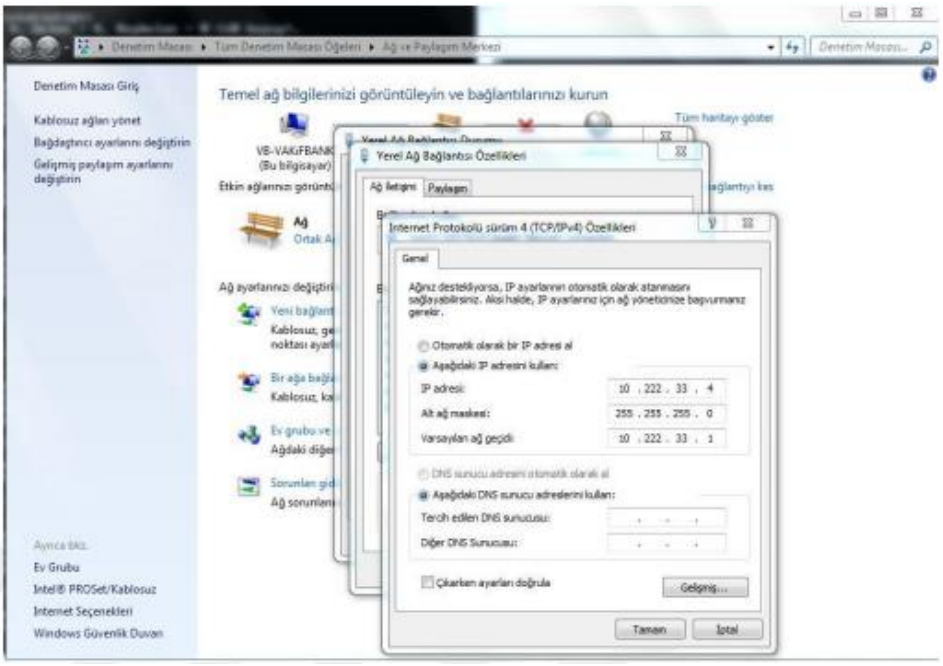


Şəkil 1.15. Putty konfiqurasiya ekranı.

Şəbəkə kartındakı kompüterlərin IP ünvanını təyin etmək (Şək.1.16, Şək.1.17) üçün hər bir kompüter üçün fərdi identifikasiya aparılır.

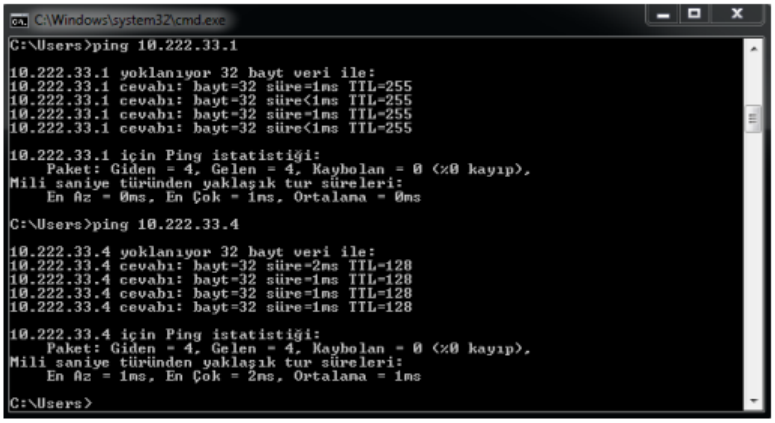


Şəkil 1.16. PC-1 IP ünvanının tərifi



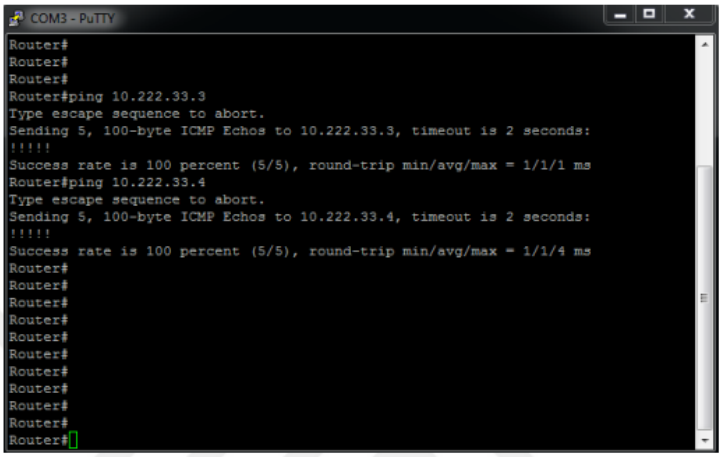
Şəkil 1.17. PC-2 IP ünvanının tərifi.

Kompüterin komanda ekranından şəbəkənin mövcudluğuna nəzarət etmək üçün digər şəbəkə elementlərinə ping paketi göndərilir (Şək.1.18). Müşahidə olunan vaxtın kompüterdən marşrutlaşdırıcıya 1 millisaniyədən, kompüterdən kompüterə isə 1 millisaniyədən az olduğu müəyyən edilib.



Şəkil 1.18. Kompüter marşrutlaşdırıcısı arasında paket göndərmə vaxtı.

Routerdən (Şək.1.19) kompüterlərə göndərilən ping paketinin giriş vaxtları da 1 millisaniyə olaraq ölçüldü.



Şəkil 1.19. Routerdən kompüterə paketin ötürülmə vaxtı.

1.3.. Şəbəkə topologiyalarında informasiya mübadiləsi protokolunun qarşılaşdırılması.

Şəbəkədə marşrutlaşdırma funksiyası rabitə protokolları vasitəsilə həyata keçirilir. Hər bir rabitə protokolunda bu funksiyalar fərqli şəkildə yerinə yetirilə bilər və şəbəkə performansını dəyişə bilər [6].

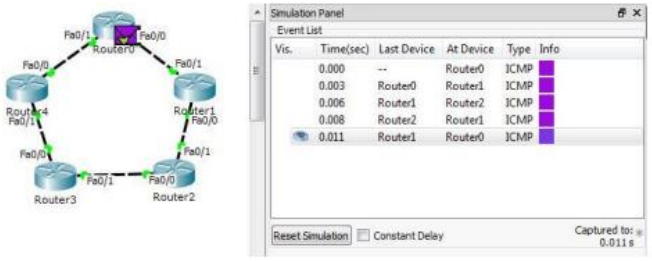
Sadə bir topologiyada şəbəkələr arasındakı performans fərqi iki marşrutlaşdırma protokolunun şəbəkə performansını, paketin gediş-gəliş müddətini və inteqrasiya vaxtını ölçməklə müşahidə edilə bilər. Bu səbəbdən şəbəkədə RIPv2 və EIGRP marşrutlaşdırma protokollarının cavabları yalnız marşrutlaşdırıcılardan ibarət olan dörd sadə şəbəkə topologiyasında müşahidə edilmişdir [7]. Topologiyalarda ping paketinin göndərilmə vaxtları və ən uzaq məsafələr arasında marşrutlaşdırıcının inteqrasiya müddətləri ölçüldü.

- Halqa Topologiyasında RIPv2 və EIGRP Performansı

Halqa topologiyasında paketlərin göndərilməsinin iki fərqli yolu seçilə bilər. Buna görə də, ping paketinin göndərilməsini seçərkən dəyərlər paketləri marşrutlaşdırıcı 0-dan marşrutlaşdırıcı 2-yə və ya ən uzaqda olan marşrutlaşdırıcı 3-ə göndərməklə ölçülə bilər.

Halqa topologiyası (Şək.1.20) üçün RIPv2 rabitə protokolunda paketin ayrılması

və çatma vaxtı cəmi 11 millisaniyə ərzində tamamlanır.

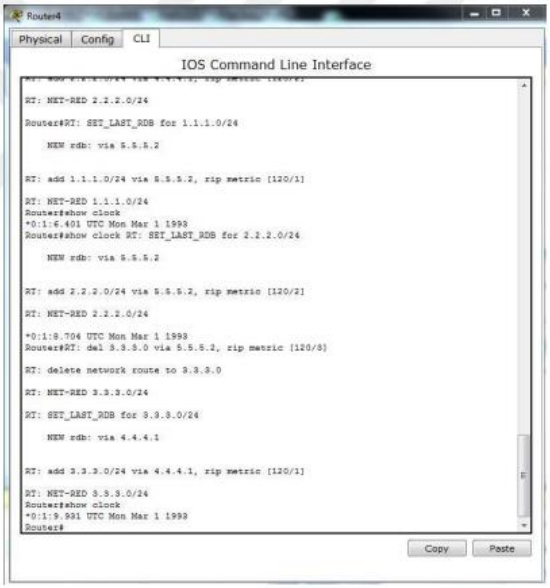


Şəkil 1.20. Halqa topologiyası RIPv2 paketinin gediş-gəliş vaxtı.

Şəbəkədəki digər qurğular haqqında marşrutlaşdırma məlumatları hələ öyrənilmədiyi üçün şəbəkəyə yeni qoşulmuş bir marşrutlaşdırıcıda yalnız birbaşa qoşulmuş şəbəkələrin məlumatları mövcuddur. Bunu "Show IP route" əmri ilə müşahidə edə bilərik.

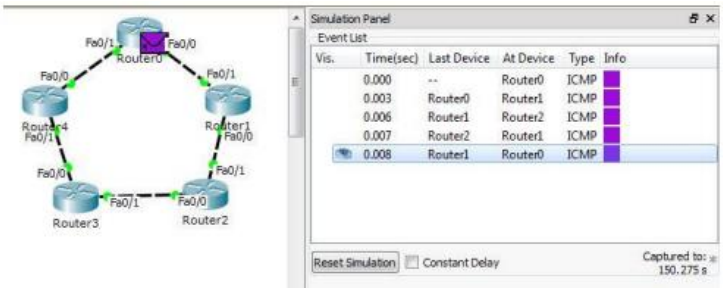
"IP marşrutlaşdırmasını aradan qaldır" əmri aktivləşdirildikdən sonra, marşrutlaşdırıcının marşrutlaşdırma cədvəlindəki dəyişikliklər ekranda qeyd olunacaq. Bu yolla, marşrutlaşdırmaya daxil olan və ya marşrutlaşdırma cədvəlindən çıxan şəbəkələri dərhal müşahidə edə bilərik.

RIPv2 protokolunda (Şək.1.21) halqa topologiyası üçün inteqrasiya vaxtı 69 saniyə olaraq müəyyən edilmişdir. Başqa sözlə, o, bu müddət ərzində bütün qoşulmuş şəbəkələri aşkarlaya bilib və paketləri göndərib qəbul etməyə hazır olub.



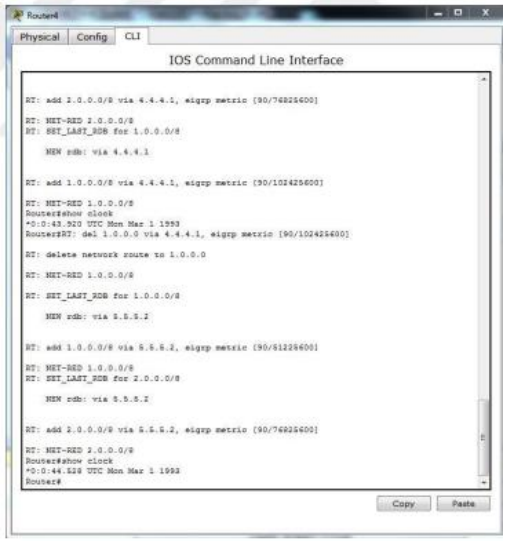
Şəkil 1.21. Halqa topologiyası RIPv2 inteqrasiya vaxtı.

Eyni şəkildə, halqa topologiyasında EIGRP ping paketinin (Şək.1.22) gediş-gəliş vaxtı 8 millisaniyə kimi ölçüldü və müşahidə edildi.



Şəkil 1.22. Halqa topologiyası EIGRP paketinin gediş-gəliş vaxtı

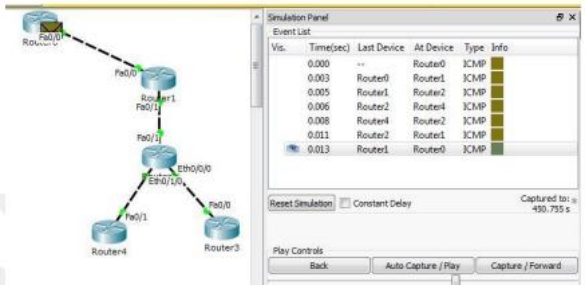
Halqa topologiyası üçün EIGRP protokolunda inteqrasiya (Şək.1.23) müddəti 44 saniyə olaraq müəyyən edilmişdir.



Şəkil 1.23. Halqa topologiyası EIGRP inteqrasiya vaxtı.

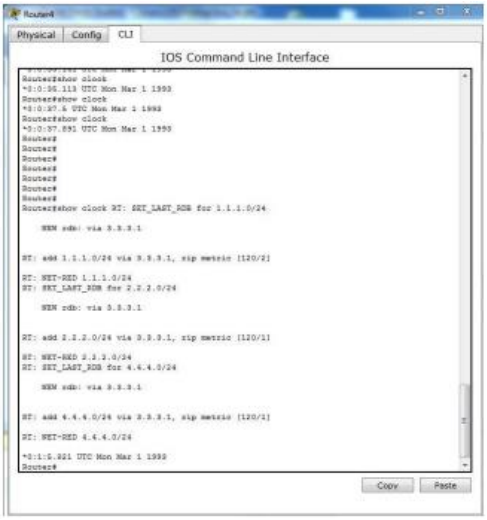
- İerarxik Topologiya RIPv2 və EIGRP Performansı

İerarxik topologiyada paketlər marşrutlaşdırıcı 0-dan 3 və ya 4-cü marşrutlaşdırıcıya ən uzaq məsafələrə göndərilə bilər. Ölçmə nəticəsində RIPv2 marşrutlaşdırma protokolu (Şək.1.24) üçün gediş-gəliş müddəti 13 millisaniyə olaraq təyin olundu.



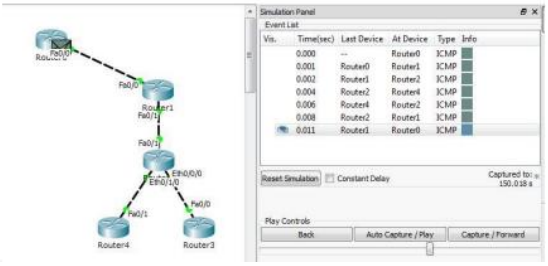
Şəkil 1.24. İerarxik topologiya RIPv2 paketinin gediş-gəliş vaxtı.

İerarxik topologiyada RIPv2 marşrutlaşdırma protokolunda inteqrasiya müddəti (Şək.1.25) 65 saniyə müşahidə edilmişdir.



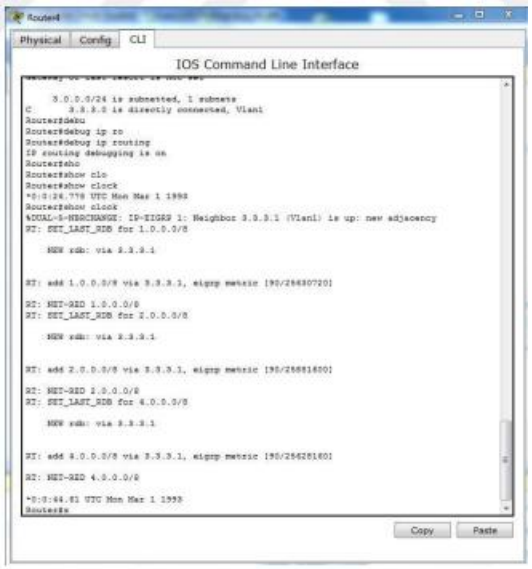
Şəkil 1.25. İerarxik topologiya RIPv2 inteqrasiya vaxtı.

İerarxik topologiyada EIGRP protokolu üçün ping vaxtı (Şək.1.26) 11 millisaniyə olaraq təyin edilmişdir.



Şəkil 1.26. İerarxik topologiya EIGRP paketinin gediş-gəliş vaxtı.

İerarxik topologiya üçün inteqrasiya müddəti EIGRP protokolunda 44 saniyə ərzində tamamlandı (Şək.1.27), bu RIPv2-dən xeyli qısa idi.

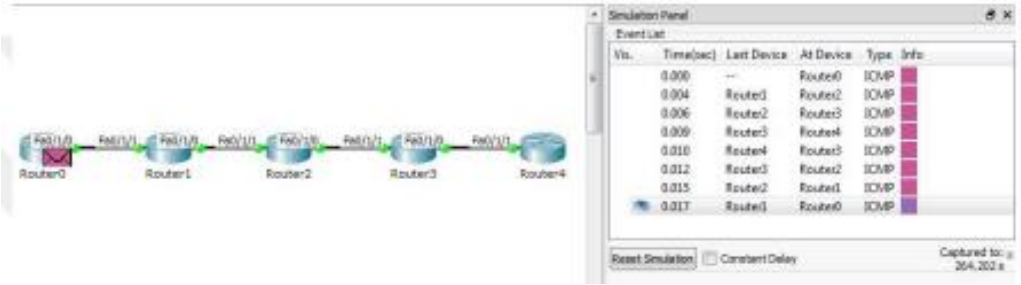


Şəkil 1.27. İerarxik topologiya EIGRP inteqrasiya vaxtı.

- Şin Topologiyası RIPv2 və EIGRP Performansı

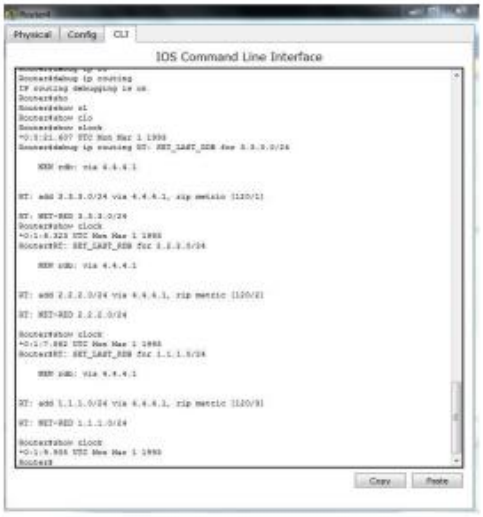
Performans dəyişikliyi paketlərin ən uzaq məsafələr arasında göndərilməsi ilə ölçüldüyü üçün, şin topologiyası üçün aşağıdakı topologiyada 0-dan marşrutlaşdırıcıya 4-ə qədər simulyasiya cihazında ping paketinin gəliş və getmə vaxtı müşahidə olunur.

Digər topologiyalarla müqayisədə, marşrutlaşdırıcı qurğu arasında məntiqi məsafəyə görə bu topologiyada paketin ən uzaq cihaza göndərilmə vaxtı daha yüksəkdir. RIPv2 protokolunda ping paketi 17 millisaniyədən sonra əsas marşrutlaşdırıcıya çatdı (Şək.1.28).



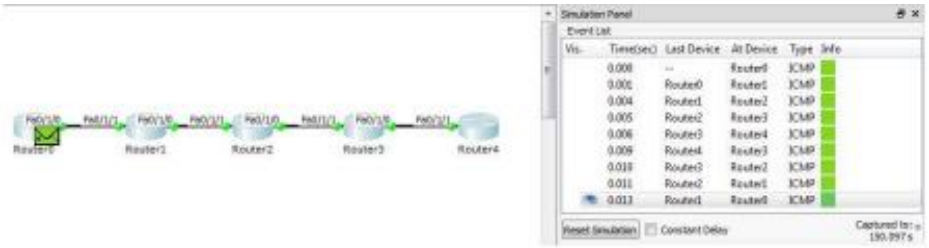
Şəkil 1.28. Şin topologiyası RIPv2 paketinin gediş-gəliş vaxtı

RIPv2 protokolunda şin topologiyası üçün inteqrasiya vaxtı 69 saniyə olaraq müşahidə edilmişdir (Şək.1.29).



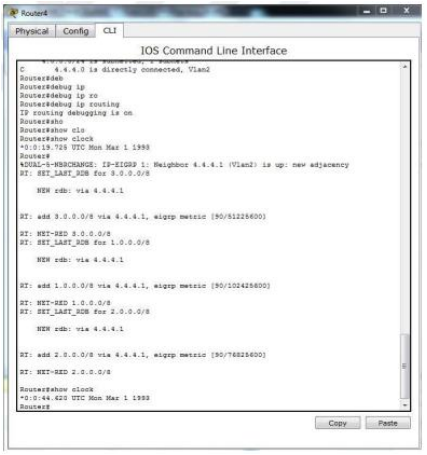
Şəkil 1.29. Şin topologiyası RIPv2 inteqrasiya vaxtı.

Şin topologiyası EIGRP protokolu ilə tərtib edildikdə, müşahidə edilən paket marşrutu RIPv2 protokolundan daha qısa müddətdə tamamlandı (Şək.1.30) və bu dəyər 13 millisaniyə kimi ölçüldü.



Şəkil 1.30. Şin topologiyası EIGRP paketinin gediş-dönüş vaxtı.

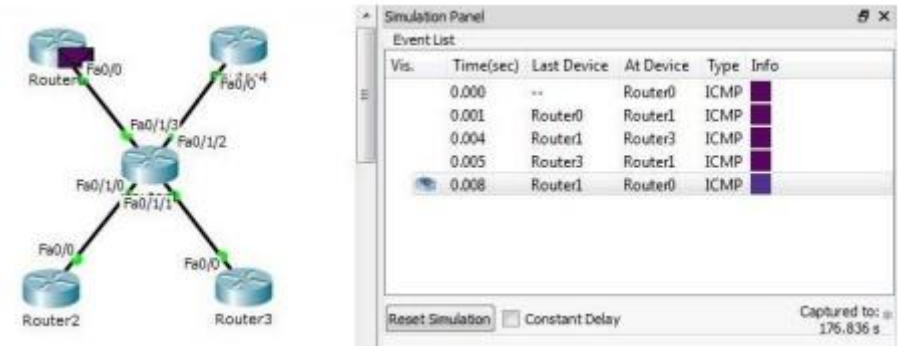
EIGRP ilə inteqrasiya vaxtı (Şək.1.31) eyni topologiyada müşahidə edilən RIPv2-dən üstün olmaqla 44 saniyə idi.



Şəkil 1.31. Şin topologiyası EIGRP inteqrasiya vaxtı.

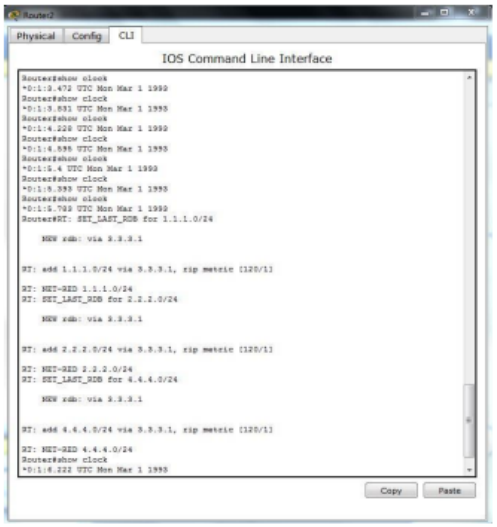
- Ulduz Topologiyası RIPv2 və EIGRP Performansı

Ulduz topologiyasında, marşrutlaşdırıcı 0 digər marşrutlaşdırıcılardan bərabər məsafədə olduğundan, bu vaxtı müəyyən etmək üçün hər hansı ən uzaq marşrutlaşdırıcıya paketlərin göndərilməsi kifayət edəcəkdir. Buna görə də, biz simulyasiya qurğusunda marşrutlaşdırıcı 0-dan 3-cü marşrutlaşdırıcıya paketlər göndərdiyimiz zaman, RIPv2 marşrutlaşdırma protokolunun gediş-gəliş vaxtı 8 millisaniyə kimi müəyyən edilir (Şək.1.32).



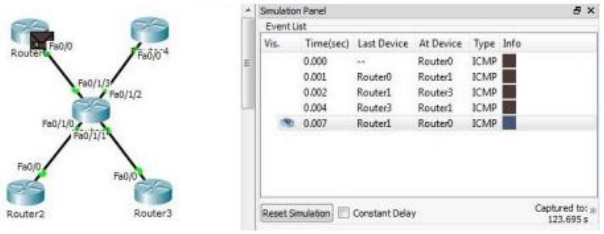
Şəkil 1.32. Ulduz topologiyası RIPv2 paketinin gediş-gəliş vaxtı.

Eyni şəkildə, bu marşrutlaşdırma protokolunda inteqrasiya müddəti 66 saniyə olaraq müşahidə edilmişdir (Şək.1.33).

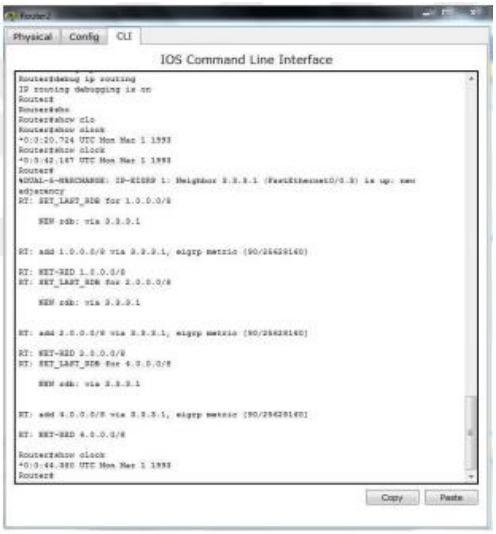


Şəkil 1.33. Ulduz topologiyası RIPv2 inteqrasiya vaxtı paketinin gediş-gəliş vaxtı.

Ulduz topologiyasındakı EIGRP protokolu üçün ping vaxtı RIPv2 protokolu ilə eyni idi və 7 millisaniyə olaraq təyin olundu (Şək.1.34, Şək.1.35).



Şəkil 1.34. Ulduz topologiyası EIGRP paketinin gediş-gəliş vaxtı



Şəkil 1.35. Ulduz topologiyası EIRP inteqrasiya vaxtı

RIPv2 və EIGRP protokollarında halqa, iyerarxik, şin və ulduz topologiyaları araşdırılmış, paketin gediş-gəliş vaxtları və inteqrasiya müddətləri ölçülmüşdür.

Topologiyalar arasında ulduz topologiyası cihazlar arasındakı məsafənin qısa olması səbəbindən digər topologiyalardan daha yaxşı performans göstərmiş və şin topologiyasındakı cihazlar arasında məsafənin daha çox olması səbəbindən gediş-gəliş müddəti daha uzun müddətdə tamamlanmışdır.

RIPv2 protokolu ilə hazırlanmış topologiyaların gediş-gəliş və inteqrasiya müddətlərinin EIGRP protokolundan daha uzun tətbiq edildiyi müşahidə edilmişdir. Sadə topologiyalarda marşrutlaşdırma protokolları arasında inteqrasiya müddətləri bir-birinə yaxındır.Müşahidə olunsa da, EIGRP RIPv2-dən daha əlverişli olduğunu sübut etdi (Cədvəl 1.1).

Dəyişənlər / Topologiya növü	Gediş - Gəliş vaxtı		İnteqrasiya vaxtı	
	RIPv2	**EIGRP**	**RIPv2**	**EIGRP**
Halqa topologiyası	11ms	8ms	69,93s	44,52s
İerarxik topologiya	13ms	11ms	65,82s	44,61s
Şin topologiyası	17ms	13ms	69,90s	44,62s
Ulduz topologiyası	8ms	7ms	66,22s	44,38s

Cədvəl 1.1. RIPv2 və EIRP performansının müqayisəsi.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Rəsulzadə Fərid Ehtibar oğlu

KORPORATİV ŞƏBƏKƏDƏ TƏHLÜKƏSİZLİYİN AŞKARLANMASI VƏ ONLARA QARŞI MÜBARİZƏNİN İDARƏ OLUNMASI

Mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter sistemləri və şəbəkələri"

Elmi rəhbər: **t.e.n., Dosent Cəfərov Nizami Duman oğlu**

BAKI – 2023

II FƏSİL. KORPORATİV ŞƏBƏKƏDƏ TƏHLÜKƏSİZLİYİN AŞKARLANMASI VƏ ONLARA QARŞI MÜBARİZƏNİN İDARƏ OLUNMASI

2.1. Firewall texnologiyaları və onların xarici təhlükələrdən qorunmasında effektivliyi

Müasir bir-biri ilə əlaqəli dünyada şəbəkə təhlükəsizliyi böyük əhəmiyyət kəsb edir. Təşkilatlar, müəssisələr və fərdlər ünsiyyət, məlumatların saxlanması və məlumat mübadiləsi üçün böyük ölçüdə kompüter şəbəkələrinə etibar edirlər. Bununla belə, bu etibar onları hakerlər, viruslar, zərərli proqramlar və icazəsiz giriş cəhdləri kimi müxtəlif xarici təhlükələrə də məruz qoyur. Bu riskləri azaltmaq üçün firewall texnologiyaları şəbəkə təhlükəsizliyi üçün mühüm vasitələr kimi ortaya çıxdı. Bu yazı müxtəlif növ firewall texnologiyalarını və şəbəkələri xarici təhlükələrdən qorumaqda onların effektivliyini araşdırmaq məqsədi daşıyır.

Firewall Texnologiyalarının növləri: Firewalllar etibarlı daxili şəbəkə ilə etibarsız xarici şəbəkə arasında maneə rolunu oynayır, daxil olan və gedən şəbəkə trafikini süzür və idarə edir. Hər birinin öz mexanizmləri və imkanları olan bir neçə növ firewall texnologiyası var [10]:

a) *Paket Filtrləmə Firewallları:* Paket filtrləmə firewallları OSI modelinin şəbəkə qatında (Layer 3) işləyir. Onlar əvvəlcədən müəyyən edilmiş qaydalar və ya filtrlər əsasında fərdi məlumat paketlərini yoxlayırlar. Bu filtrlər mənbə IP ünvanı, təyinat IP ünvanı, port nömrələri və protokollar kimi meyarlara əsasən paketə icazə verilməsini və ya bloklanmasını müəyyənləşdirir. Paket filtrləmə firewallları sadə və səmərəli olsa da, paketlərin məzmununu yoxlamaq qabiliyyəti yoxdur və IP saxtakarlığı kimi müəyyən növ hücumlara həssasdırlar.

b) *Vəziyyətli Təftiş Firewallları:* Dinamik paket filtrləmə firewallları kimi də tanınan vəziyyətə uyğun yoxlama firewallları paket filtrləmə imkanlarını əlavə

kontekst məlumatlandırması ilə birləşdirir. Bu firewalllar şəbəkə əlaqələrinin vəziyyətini izləyən vəziyyət cədvəlini saxlayır. Onlar paket məzmununu yoxlaya, hər bir əlaqənin vəziyyətini izləyə və trafikə icazə vermək və ya bloklamaqla bağlı daha ağıllı qərarlar qəbul edə bilərlər. Şəbəkə trafikinin kontekstini təhlil edərək paket süzgəcindən keçirən təhlükəsizlik duvarları ilə müqayisədə vəziyyətə uyğun yoxlama firewallları təkmilləşdirilmiş təhlükəsizlik təklif edir.

c) *Tətbiq səviyyəli firewalllar:* Proxy firewall kimi də tanınan tətbiq səviyyəli təhlükəsizlik divarları OSI modelinin tətbiq səviyyəsində (Layer 7) işləyir. Onlar müştərilər və serverlər arasında vasitəçi rolunu oynayır, bütün daxil olan və gedən trafiki ələ keçirir və yoxlayır. Şəbəkə paketlərinin məzmununu araşdıraraq, bu firewalllar daha ətraflı təhlükəsizlik siyasətlərini tətbiq edə və xüsusi proqram səviyyəsindəki hücumlara qarşı qoruma təmin edə bilər. Bununla belə, bütün trafikin proksiləşdirilməsi ilə bağlı əlavə emal xərcləri şəbəkə performansına təsir göstərə bilər.

Firewall Texnologiyalarının Effektivliyi: Firewall texnologiyaları şəbəkələrin xarici təhlükələrdən qorunmasında mühüm rol oynayır, lakin onların effektivliyi müxtəlif amillərdən asılıdır:

- ✓ Girişə Nəzarət: Firewalllar təşkilatlara hansı şəbəkə trafikinə icazə verildiyini və ya bloklandığını müəyyən etmək üçün girişə nəzarət siyasətlərini müəyyən etməyə imkan verir. Bu siyasətləri tətbiq etməklə, təhlükəsizlik duvarları icazəsiz giriş cəhdlərinin, zərərli fəaliyyətlərin və şəbəkə müdaxilələrinin qarşısını ala bilər. Optimal mühafizəni təmin etmək üçün effektiv konfiqurasiya və firewall qaydalarının müntəzəm yenilənməsi vacibdir.
- ✓ Təhlükənin aşkarlanması və qarşısının alınması: Qabaqcıl təhlükə aşkarlama imkanları ilə təchiz edilmiş təhlükəsizlik divarları zərərli proqramlar, viruslar və müdaxilə cəhdləri kimi müxtəlif növ təhdidləri müəyyən edib blok edə bilər. Dərin paket yoxlaması, müdaxilənin aşkarlanması sistemləri (IDS) və

müdaxilənin qarşısının alınması sistemləri (IPS) kimi xüsusiyyətlər hücumların aşkarlanması və qarşısının alınmasında firewallların effektivliyini artırır.

- ✓ Daimi Yeniləmələr və Baxım: Yaranan təhlükələrə qarşı effektiv qalmaq üçün təhlükəsizlik divarları ən son təhlükəsizlik yamaları, proqram təminatı yeniləmələri və təhlükə kəşfiyyatı lentləri ilə müntəzəm olaraq yenilənməlidir. Bundan əlavə, firewall qeydlərinin monitorinqi və dövri auditlərin aparılması şəbəkə təhlükəsizliyinə xələl gətirə biləcək potensial zəiflikləri və ya konfiqurasiya xətalarını müəyyən etməyə kömək edə bilər.

Firewall texnologiyaları təşkilatları və şəxsləri xarici təhlükələrdən qoruyan şəbəkə təhlükəsizliyinin əvəzsiz komponentləridir. Müvafiq firewall həllərini tətbiq etməklə bu cür təşkilatlar öz şəbəkələrini qorumaq üçün güclü müdafiə mexanizmi yarada bilərlər. Firewall texnologiyalarının effektivliyi danılmaz olsa da, onların qüsursuz olmadığını və müdaxilənin aşkarlanması sistemləri, şifrələmə protokolları və işçilərin məlumatlandırılması təlimi kimi digər təhlükəsizlik tədbirləri ilə tamamlanmalı olduğunu qəbul etmək vacibdir [8].

Firewall texnologiyalarının maksimum effektivliyini təmin etmək üçün təşkilatlar aşağıdakı ən yaxşı təcrübələri nəzərə almalıdırlar:

- Təşkilatlar öz şəbəkələrini qorumaq üçün güclü müdafiə mexanizmi yarada bilərlər. Firewall texnologiyalarının effektivliyi danılmaz olsa da, onların qüsursuz olmadığını və müdaxilənin aşkarlanması sistemləri, şifrələmə protokolları və işçilərin məlumatlandırılması təlimi kimi digər təhlükəsizlik tədbirləri ilə tamamlanmalı olduğunu qəbul etmək vacibdir.
- Firewall texnologiyalarının maksimum effektivliyini təmin etmək üçün təşkilatlar aşağıdakı ən yaxşı təcrübələri nəzərə almalıdırlar:
- Fərdi Konfiqurasiya: Firewalllar təşkilatın xüsusi təhlükəsizlik tələblərinə uyğun olaraq konfiqurasiya edilməlidir. Buraya girişə nəzarət siyasətlərinin müəyyən edilməsi, müvafiq qeydiyyat və monitorinq qaydalarının yaradılması və şəbəkənin ehtiyaclarına uyğunlaşdırılmış müdaxilənin qarşısının alınması sistemlərinin tətbiqi daxildir.

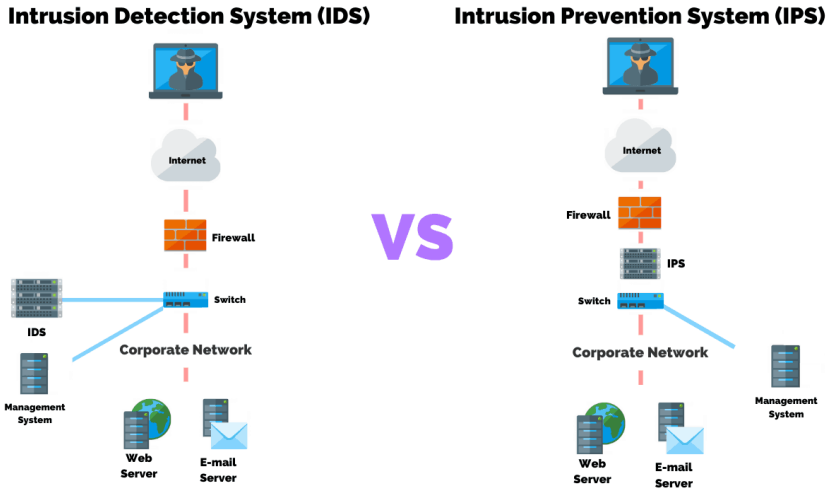
- Daimi Monitorinq və Baxım: Potensial təhlükəsizlik insidentlərini dərhal aşkar etmək və onlara cavab vermək üçün təhlükəsizlik duvarı qeydlərinin və xəbərdarlıqlarının davamlı monitorinqi vacibdir. Bundan əlavə, zəifliklər aradan qaldırmaq və optimal performansı təmin etmək üçün proqram təminatı yeniləmələri, təhlükəsizlik yamaları və qaydalara baxış kimi müntəzəm texniki xidmət tapşırıqları yerinə yetirilməlidir.
- Təhdid Kəşfiyyatının İnteqrasiyası: Təhlükə kəşfiyyatı məlumatlarının firewalllara inteqrasiyası onların yaranan təhlükələri aşkar etmək və bloklamaq qabiliyyətini artıra bilər. Məlum zərərli İP-lər, domenlər və hücum nümunələri haqqında ən son məlumatlarla yenilənməklə təşkilatlar inkişaf edən kibertəhlükələrə qarşı müdafiələrini gücləndirə bilərlər.
- İstifadəçi məlumatlandırması və təlimi: Firewallların qabaqcıl imkanlarına baxmayaraq, onlar insan səhvlərinin və ya daxili təhlükələrin qarşısını ala bilmirlər. Fişinq cəhdlərini tanımaq, güclü parollardan istifadə etmək və təhlükəsiz axtarış vərdişlərini tətbiq etmək kimi şəbəkə təhlükəsizliyi üçün ən yaxşı təcrübələr barədə işçilərin maarifləndirilməsi uğurlu hücumların ehtimalını azaltmaq üçün çox vacibdir.
- Laylı Müdafiə Strategiyası: Firewalllar çoxsaylı təhlükəsizlik tədbirlərini özündə birləşdirən laylı müdafiə strategiyasının bir hissəsi kimi nəzərdən keçirilməlidir. Firewallları müdaxilənin aşkarlanması və qarşısının alınması sistemləri, antivirus proqramı, şəbəkə seqmentasiyası və güclü autentifikasiya mexanizmləri ilə birləşdirmək müdafiə qatlarını əlavə edir və müvəffəqiyyətli pozuntu şanslarını azaldır.

Yekun olaraq, firewall texnologiyaları şəbəkə təhlükəsizliyinin vacib komponentləridir və xarici təhdidlərə qarşı kritik birinci müdafiə xəttini təmin edir. Müvafiq firewall həllərini tətbiq etməklə, onları effektiv şəkildə konfiqurasiya etməklə və ən yaxşı təcrübələrə əməl etməklə təşkilatlar şəbəkə təhlükəsizliyi vəziyyətini əhəmiyyətli dərəcədə artıra bilər. Bununla belə, yadda saxlamaq lazımdır ki, firewall müstəqil həllər deyil və şəbəkə mühafizəsinin çoxsaylı aspektlərini əhatə edən

hərtərəfli təhlükəsizlik strategiyasının bir hissəsi olmalıdır.

2.2.Hücumun aşkarlanması və qarşısının alınması sistemləri və onların şəbəkə təhlükəsizliyində rolu

Müasir bir-biri ilə əlaqəli dünyada şəbəkə təhlükəsizliyi həm fərdlər, həm də təşkilatlar üçün kritik bir problemə çevrilmişdir. Kiber təhdidlərin və mürəkkəb hücumların sayının artması məxfi məlumatın məxfiliyi, bütövlüyü və əlçatanlığı üçün əhəmiyyətli risklər yaradır. Bu riskləri azaltmaq üçün Intrusion Detection and Prevention Systems (IDPS) şəbəkə infrastrukturlarının zərərli fəaliyyətlərdən qorunmasında mühüm rol oynayır (Şək.2.1.).



Şəkil 2.1. Hücumun Aşkarlanması Və Qarşısının Alınması Sistemləri (IDPS)

Hücumun aşkarlanması və qarşısının alınması sistemləri şəbəkə mühitində icazəsiz giriş cəhdlərini, zərərli fəaliyyətləri və siyasət pozuntularını aşkar etmək və onlara cavab vermək üçün nəzərdə tutulmuş təhlükəsizlik mexanizmləridir. Onların əsas məqsədi potensial təhlükələri müəyyən etmək və onların şəbəkənin bütövlüyünü pozmasının qarşısını almaqdır. IDPS şəbəkə trafikinə nəzarət etmək, anomaliyaları və ya məlum hücum nümunələrini müəyyən etmək və aşkar edilmiş təhdidləri azaltmaq üçün müvafiq tədbirlər görmək üçün avadanlıq, proqram təminatı və analitik üsulların birləşməsindən istifadə edir.

Şəbəkə təhlükəsizliyində IDPS-in rolu çoxşaxəlidir. Birincisi, IDPS şəbəkə trafikinə davamlı olaraq nəzarət etməklə və onu müdaxilə əlamətləri və ya zərərli davranışlar üçün təhlil etməklə proaktiv müdafiə mexanizmi kimi xidmət edir. Şəbəkə paketlərini yoxlayaraq, IDPS müxtəlif növ hücumları, o cümlədən şəbəkə skanını, port skanını və kobud giriş cəhdlərini aşkar edə bilər. Bu real vaxt rejimində monitorinq uğurlu müdaxilə riskini minimuma endirməklə potensial təhlükələri tez aşkar etməyə və onlara cavab verməyə imkan verir [9,10].

İkincisi, IDPS ənənəvi firewall və antivirus həllərini tamamlayaraq əlavə təhlükəsizlik səviyyəsini təmin edir. Firewall paket başlıqlarını araşdıraraq şəbəkəyə girişi idarə edir, antivirus proqramı isə məlum zərərli kodun müəyyən edilməsinə və bloklanmasına diqqət yetirir. Bununla belə, bu ənənəvi təhlükəsizlik tədbirləri mürəkkəb hücumları və ya sıfır gün zəifliklərini aşkar etmək üçün kifayət olmaya bilər. Digər tərəfdən, IDPS şəbəkə paketlərinin məzmununu təhlil edə, onların faydalı yükünü zərərli kod və ya normal şəbəkə trafikindən kənara çıxan davranış nümunələri üçün yoxlaya bilər. Bu proaktiv yanaşma şəbəkənin ümumi təhlükəsizlik vəziyyətini artırır.

Bundan əlavə, məcburi köçkünlər insidentlərə reaksiya və məhkəmə-tibbi araşdırmalara kömək edir. Təhlükəsizliyin pozulması halında, IDPS hücumun xarakteri, təsirə məruz qalan sistemlər və potensial zəifliklər haqqında dəyərli məlumat verən xəbərdarlıqlar və jurnal faylları yaradır. Bu jurnallar insidentdən sonrakı təhlil, təcavüzkarın üsullarının müəyyən edilməsinə kömək etmək, pozuntunun dərəcəsini müəyyən etmək və gələcək hadisələrin qarşısını almaq üçün bərpa tədbirlərini həyata keçirmək üçün istifadə edilə bilər. İnsidentlərə reaksiya və məhkəmə-tibbi analizi asanlaşdırmaqla, IDPS təşkilatlara təhlükəsizlik təcrübələrini təkmilləşdirməyə və oxşar təhlükələrə qarşı müdafiələrini gücləndirməyə kömək edir.

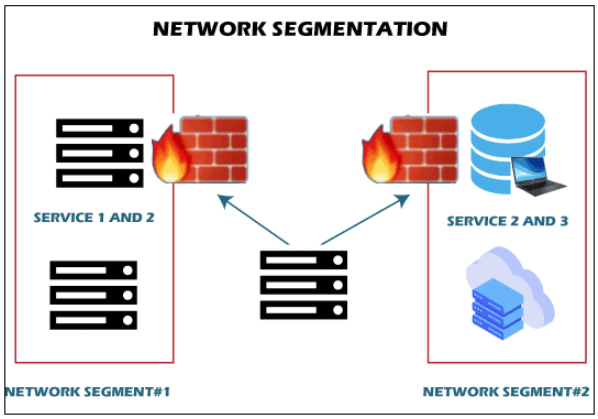
Qeyd etmək vacibdir ki, IDPS müstəqil həll yolu deyil, hərtərəfli şəbəkə təhlükəsizliyi strategiyasının tərkib hissəsidir. Onlar firewall, antivirus proqramı, təhlükəsiz şəbəkə arxitekturası və istifadəçi məlumatlandırma təlimi kimi digər təhlükəsizlik tədbirləri ilə birlikdə yerləşdirilməlidir. Bu elementləri birləşdirərək

təşkilatlar müxtəlif növ təhdidlərə qarşı laylı müdafiəni təmin edən dərin müdafiə yanaşması qura bilərlər [8,10].

Nəticə olaraq, Hücumun Aşkarlanması və Qarşısının Alınması Sistemləri şəbəkə trafikini aktiv şəkildə izləməklə, potensial müdaxilələri aşkar etməklə və icazəsiz girişin qarşısını almaqla şəbəkə təhlükəsizliyində mühüm rol oynayır. Onlar ənənəvi təhlükəsizlik tədbirlərinin effektivliyini artırır, real vaxt rejimində təhlükənin aşkar edilməsini təmin edir və insidentlərə cavab və məhkəmə-tibbi araşdırmalara kömək edir. Optimal şəbəkə təhlükəsizliyini təmin etmək üçün təşkilatlar inkişaf etməkdə olan təhlükə mənzərəsinə cavab verən vahid təhlükəsizlik strategiyasının bir hissəsi kimi IDPS-lərin yerləşdirilməsini nəzərdən keçirməlidir. IDPS və digər təhlükəsizlik texnologiyalarının imkanlarından istifadə etməklə, fərdlər və təşkilatlar öz şəbəkələrini, məlumatlarını və ümumi rəqəmsal aktivlərini daha yaxşı qoruya bilərlər.

2.3. Şəbəkənin seqmentasiyası və potensial təhlükəsizlik pozuntusunun təsirinin azaldılmasının əhəmiyyəti

Məlumatların pozulması və kibertəhlükələrin getdikcə təkmilləşdiyi bugünkü bir-biri ilə əlaqəli dünyada təşkilatlar öz həssas məlumatlarını qorumaq üçün hərtərəfli təhlükəsizlik tədbirləri görməlidirlər. Potensial təhlükəsizlik pozuntusunun təsirini azaltmaqda mühüm rol oynayan mühüm strategiyalardan biri şəbəkənin seqmentləşdirilməsidir. Şəbəkə seqmentasiyası (Şək 2.2.) təhlükəsizliyi artırmaq, girişi idarə etmək və pozuntu halında təcavüzkarların yanal hərəkətini məhdudlaşdırmaq üçün kompüter şəbəkəsinin daha kiçik, təcrid olunmuş alt şəbəkələrə bölünməsini nəzərdə tutur.



Şəkil 2.2. Şəbəkənin seqmentasiyası

İlk növbədə şəbəkə seqmentasiyası şəbəkə infrastrukturu daxilində maneələr yaratmaqla təcavüzkarlara qarşı əlavə müdafiə qatını təmin edir. Şəbəkəni çoxsaylı seqmentlərə bölməklə təşkilatlar həssas məlumatları və ya qiymətli əqli mülkiyyəti saxlayan serverlər kimi kritik resursları təcrid edə bilər. Pozulma halında, bu seqmentləşdirmə təcavüzkarın şəbəkə daxilində yanal hərəkət imkanlarını məhdudlaşdırır, onların digər seqmentlərə icazəsiz giriş əldə etməsinə mane olur. Hətta bir seqment təhlükə altına düşsə belə, təsirin qarşısını almaq olar və şəbəkənin qalan hissəsi qorunur, potensial zərər və itkiləri azaldır.

Bundan əlavə, şəbəkə seqmentasiyası təşkilatlara ümumi təhlükəsizliyi artıraraq, incə dənəli giriş nəzarəti siyasətlərini həyata keçirməyə imkan verir. İstifadəçilərin və ya cihazların rolu və tələblərinə əsasən müxtəlif seqmentlərə müxtəlif təhlükəsizlik səviyyələri və giriş hüquqları təyin edilə bilər. Məsələn, təşkilatın işçilərə, qonaqlara və xarici podratçılara həsr olunmuş seqmentləri ola bilər, onların hər biri müxtəlif səviyyəli giriş imtiyazlarına malikdir. Bu dənəvər nəzarət hücum səthini minimuma endirir və icazəsiz istifadəçilərin kritik resurslara daxil olmasını məhdudlaşdırır. [9,10] Əlavə olaraq, hər bir seqmentin spesifik ehtiyaclarına və risklərinə uyğunlaşdırılmış Müdaxilənin Aşkarlanması və Qarşısının Alınması Sistemləri (IDPS) və ya Məlumat İtkisinin Qarşısının Alınması (DLP) sistemləri kimi seqmentə xas təhlükəsizlik siyasətləri tətbiq oluna bilər.

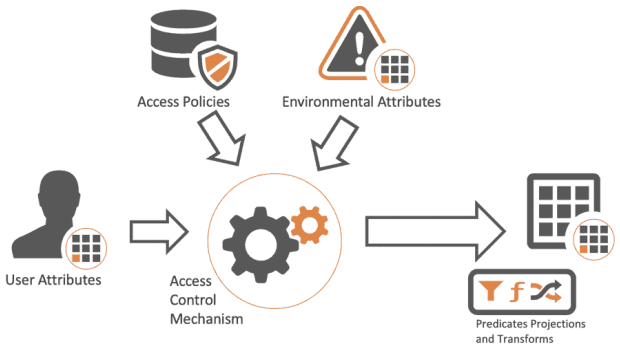
Nəhayət, şəbəkənin seqmentasiyası təhlükəsizlik pozuntusu halında insidentlərə cavab vermək və saxlama səylərini asanlaşdırır. Təşkilat bir seqmentdə pozuntu və ya

şübhəli fəaliyyət aşkar etdikdə, o seqmenti tez bir zamanda təcrid edə, əlavə zərərin qarşısını ala və ümumi şəbəkəyə təsirini minimuma endirə bilər. Seqmentləşdirilmiş arxitektura təhlükəsizlik qruplarına bütün şəbəkəni pozmadan səylərini insidentin qarşısını almaq, səbəbi araşdırmaq və bərpa tədbirlərini həyata keçirməyə yönəltməyə imkan verir. Bu, cavab müddətini yaxşılaşdırır, dayanma müddətini azaldır və təşkilatın təhlükəsizlik insidentindən tez sağalmaq qabiliyyətini artırır. [9]

Nəticə olaraq, şəbəkə seqmentasiyası maneələr yaratmaq, giriş nəzarətini gücləndirmək, uyğunluq tələblərinə cavab vermək və insidentlərə cavab verməklə potensial təhlükəsizlik pozuntularının təsirini azaltmaqda mühüm rol oynayır. Şəbəkəni daha kiçik, təcrid olunmuş seqmentlərə bölməklə, təşkilatlar hücum səthini əhəmiyyətli dərəcədə azalda və icazəsiz girişi məhdudlaşdıra bilər. Getdikcə mürəkkəbləşən təhlükə mənzərəsində şəbəkə seqmentasiyası təşkilatlara öz dəyərli aktivlərini qorumaq, biznesin davamlılığını qorumaq və kibertəhlükələrə qarşı dayanıqlılıq yaratmaq səlahiyyətini verən mühüm təhlükəsizlik tədbiri kimi dayanır.

2.4. Girişə nəzarət mexanizmləri və onların şəbəkə resurslarına icazəli girişin təmin olunmasında rolu

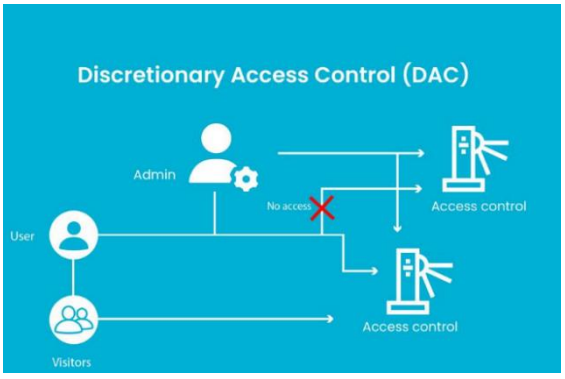
Girişə nəzarət mexanizmləri (Şək.2.3.) şəbəkə resurslarına səlahiyyətli girişin təmin edilməsində mühüm rol oynayır. Rəqəmsal sistemlərin yayılması və şəbəkə mühitlərinə olan etibarın artması ilə həssas məlumatların qorunması və icazəsiz girişin qarşısının alınması zərurəti böyük əhəmiyyət kəsb edir. Girişə nəzarət mexanizmləri istifadəçi imtiyazlarını idarə etmək, təhlükəsizlik siyasətlərini tətbiq etmək və qiymətli şəbəkə resurslarını qorumaq üçün çərçivə təmin edir. Bu yazı müxtəlif girişə nəzarət mexanizmlərini və onların şəbəkə resurslarının məxfiliyini, bütövlüyünü və əlçatanlığını qorumaqda əhəmiyyətini araşdırmaq məqsədi daşıyır [9].



Şəkil 2.3. Girişə nəzarət mexanizmi

Girişə nəzarət xüsusi resurslara daxil olmağa cəhd edən şəxslərə və ya qurumlara icazələrin verilməsi və ya rədd edilməsi prosesidir. Bu, təhlükəsizlik siyasətlərinə uyğunluğu təmin etmək üçün istifadəçilərin şəxsiyyətlərinin autentifikasiyasını, hərəkətlərinə icazə verilməsini və fəaliyyətlərinin yoxlanılmasını əhatə edir. Girişə nəzarət mexanizmlərini tətbiq etməklə təşkilatlar icazəsiz giriş, daxili təhdidlər və məlumatların pozulması ilə bağlı riskləri azalda bilər.

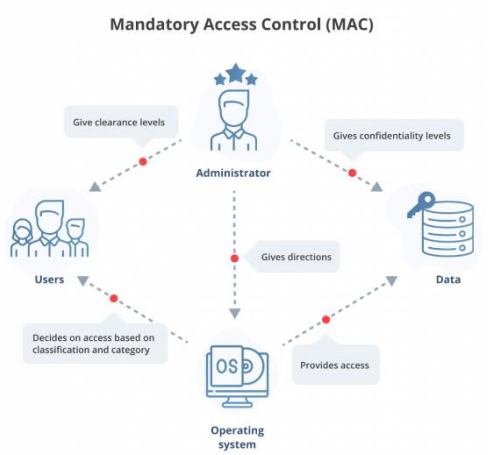
Girişə nəzarət mexanizminin birinci növü *ixtiyari giriş nəzarətidir (DAC)* (Şək.2.4.). DAC-da resurs sahibi resursa kimin daxil ola biləcəyini və hansı hərəkətləri yerinə yetirə biləcəyini müəyyən edir. Bu model fərdlərə giriş hüquqlarını və icazələrini təyin etməklə öz resursları üzərində nəzarəti həyata keçirməyə imkan verir. Bununla belə, DAC-ın məhdudiyyətləri var, çünki o, istifadəçinin ixtiyarına çox etibar edir və bu, uyğun olmayan və potensial olaraq etibarsız giriş nəzarəti qərarlarına səbəb ola bilər.



Şəkil 2.4. İxtiyari giriş nəzarəti (DAC)

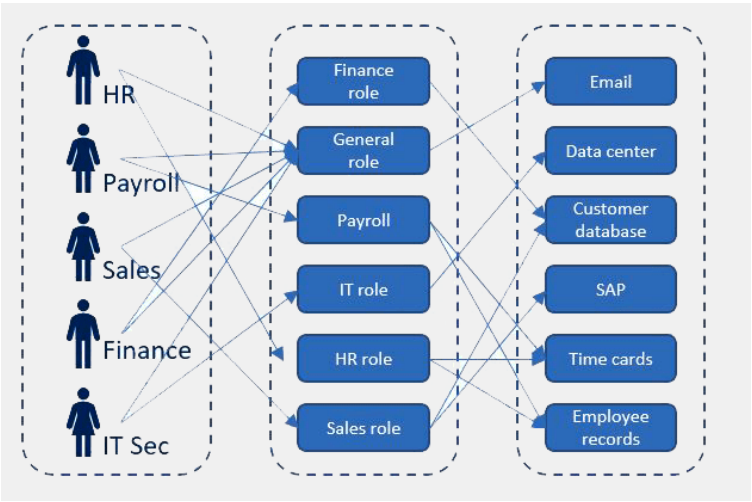
DAC məhdudiyyətlərini aradan qaldırmaq üçün *məcburi giriş nəzarəti (MAC)* (Şək.2.5.) tətbiq edildi. MAC-da giriş qərarları resursun təsnifatı və həssaslığına və

istifadəçinin təhlükəsizlik rəsmiləşdirilməsinə əsaslanır. [9,10] Bu model, fərdi seçimlərdən asılı olmayaraq, girişə nəzarət siyasətlərinin sistem boyu ardıcıl olaraq tətbiq edilməsini təmin edir. MAC adətən hərbi və hökumət sektorları kimi yüksək həssas məlumatların qorunmasının vacib olduğu mühitlərdə istifadə olunur.



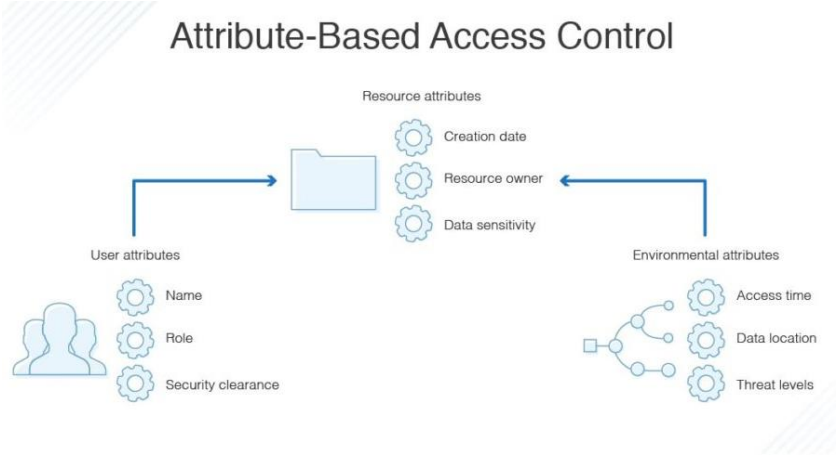
Şəkil 2.5. Məcburi giriş nəzarəti (MAC)

Rol əsaslı giriş nəzarəti (RBAC) (Şək.2.6) başqa bir geniş yayılmış giriş nəzarət mexanizmidir. RBAC istifadəçilərə təşkilat daxilindəki rollarına əsasən icazələr təyin edir. Fərdi giriş hüquqlarını idarə etmək əvəzinə, RBAC rolları müəyyən etməyə və onları müvafiq imtiyazlarla əlaqələndirməyə diqqət yetirir. Bu yanaşma oxşar məsuliyyətləri olan istifadəçiləri qruplaşdırmaq və onların rol tələbləri əsasında giriş verməklə girişin idarə edilməsini asanlaşdırır. RBAC girişə nəzarət siyasətlərinin səmərəli idarə olunmasını təmin etməklə təhlükəsizliyi yaxşılaşdırır və inzibati xərcləri asanlaşdırır.



Şəkil 2.6. Rol əsaslı giriş nəzarəti (RBAC)

Qeyd etməyə dəyər başqa bir giriş nəzarət mexanizmi *atribut əsaslı giriş nəzarətidir (ABAC)* (Şək.2.7.). ABAC giriş nəzarəti ilə bağlı qərarlar qəbul edərkən istifadəçi atributları, resurs atributları və ətraf mühit şəraiti kimi çoxsaylı atributları nəzərə alaraq daha incə bir yanaşma tətbiq edir. Bu model təşkilatlara giriş vaxtı, yer və istifadəçi davranışı kimi kontekstual məlumatları özündə birləşdirən mürəkkəb siyasətləri müəyyən etməyə imkan verir ki, girişin verilməsi və ya rədd edilməsini müəyyən etsin. [10] ABAC xüsusilə mürəkkəb və inkişaf edən mühitlərdə girişə nəzarət üçün çevik və dinamik çərçivə təmin edir.



Şəkil 2.7. Atribut əsaslı giriş nəzarəti (ABAC)

Girişə nəzarət mexanizmləri tək bir yanaşma ilə məhdudlaşmır, lakin çox vaxt xüsusi təhlükəsizlik tələblərinə cavab vermək üçün çoxsaylı modellərin birləşməsindən istifadə edir. Məsələn, şəbəkə istifadəçi rollarını və icazələrini idarə etmək üçün RBAC-dan istifadə edə bilər, eyni zamanda yüksək məxfi məlumatlar üzərində ciddi nəzarəti həyata keçirmək üçün MAC-ı birləşdirə bilər. Girişə nəzarət mexanizminin seçimi resursların həssaslığı, tənzimləyici tələblər və təşkilatın risk iştahı kimi amillərdən asılıdır.

Yekun olaraq, girişə nəzarət mexanizmləri şəbəkə resurslarına səlahiyyətli girişi təmin etmək üçün çox vacibdir. Onlar istifadəçi imtiyazlarını idarə etmək, təhlükəsizlik siyasətlərini tətbiq etmək və qiymətli məlumatı qorumaq üçün çərçivə təmin edir. Müvafiq girişə nəzarət mexanizmlərini tətbiq etməklə təşkilatlar icazəsiz giriş, daxili təhdidlər və məlumatların pozulması ilə bağlı riskləri azalda bilər. İstər ixtiyari giriş nəzarəti, istər məcburi giriş nəzarəti, istər rol əsaslı giriş nəzarəti, istərsə də atribut

əsaslı giriş nəzarəti olsun, hər bir mexanizm təşkilatın ümumi təhlükəsizlik vəziyyətinə töhfə verir və məlumatların məxfiliyinin, bütövlüyünün və mövcudluğunun qorunmasında mühüm rol oynayır. şəbəkə resursları.

2.5. Məlumat mərkəzləri, server otaqları və şəbəkə şkafları kimi şəbəkə infrastrukturu üçün fiziki təhlükəsizlik tədbirləri.

Müasir rəqəmsal əsrdə şəbəkə infrastrukturu bütün ölçülü təşkilatlarda mühüm rol oynayır. Məlumat mərkəzləri, server otaqları və şəbəkə şkafları fiziki təhlükələrdən qorunmalı olan həssas məlumat və avadanlıqları saxlayır. Bu həyati aktivləri qorumaq üçün güclü fiziki təhlükəsizlik tədbirlərinin həyata keçirilməsi vacibdir. Bu məqalə şəbəkə infrastrukturunu qorumaq, məlumat və sistemlərin məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək üçün istifadə edilə bilən müxtəlif fiziki təhlükəsizlik tədbirlərini araşdırır[8,9,10].

1. Girişə Nəzarət Sistemləri: Girişə nəzarət sistemləri şəbəkə infrastrukturunun fiziki təhlükəsizliyini qorumaq üçün əsasdır. Aşağıdakı tədbirlər həyata keçirilə bilər:

a) *Biometrik Doğrulama:* Barmaq izi və ya irisin skan edilməsi kimi biometrik identifikasiyanın həyata keçirilməsi məhdud ərazilərə daxil olan şəxslərin müəyyən edilməsi və yoxlanması üçün yüksək təhlükəsiz üsul təmin edir. Bu, icazəsiz giriş riskini əhəmiyyətli dərəcədə azaldır.

b) *Ağıllı Kart Sistemləri:* Ağıllı karta əsaslanan girişə nəzarət sistemləri giriş əldə etmək üçün istifadəçilərdən öz etimadnamələri ilə kodlanmış unikal kartı təqdim etməyi tələb edir. Bu sistemlər giriş hadisələrini izləyə və qeyd edə, monitorinq və audit fəaliyyətlərinə kömək edə bilər.

c) *Açar Kartlar və PİN Kodlar:* Unikal fərdi identifikasiya nömrələri (PIN) ilə birləşən açar kart sistemləri əlavə təhlükəsizlik səviyyəsini təmin edir. Məxfiliyi qorumaq üçün PIN-lər mütəmadi olaraq dəyişdirilə bilər və əsas kartlar itirildikdə və ya işçinin işdən çıxarılması halında asanlıqla ləğv edilə bilər.

2. Video Nəzarət: Video nəzarət sistemləri şəbəkə infrastrukturuna icazəsiz girişin monitorinqi və qarşısının alınmasında mühüm rol oynayır. Aşağıdakı mülahizələr mühümdür:

a) *CCTV Kameraları:* Qapalı dövrəli televiziya (CCTV) kameraları giriş nöqtələri, server rəfləri və avadanlıq otaqları kimi kritik sahələri əhatə etmək üçün strateji şəkildə yerləşdirilməlidir. Gecə görmə qabiliyyətinə malik yüksək keyfiyyətli kameralar hər zaman aydın görüntüləri təmin edir.

b) *Hərəkət Sensorları:* Nəzarət sistemi ilə inteqrasiya olunmuş hərəkət sensorları qadağan olunmuş ərazilərdə gözlənilməz hərəkət aşkar edildikdə xəbərdarlıqları işə sala və video çəkilişləri çəkə bilər.

c) *Uzaqdan Monitorinq:* Canlı kamera lentlərinə və uzaq yerlərdən qeydə alınmış kadrlara giriş real vaxtda görünməni təmin edir və potensial təhlükəsizlik pozuntularına tez cavab verməyə imkan verir.

3. Perimetr Təhlükəsizliyi: Məlumat mərkəzlərinin, server otaqlarının və şəbəkə şkaflarının perimetrinin mühafizəsi icazəsiz girişin qarşısını almaq üçün vacibdir. Aşağıdakı tədbirlər perimetrin təhlükəsizliyini artırır:

a) *Qılıncoynatma və maneələr:* Hasar, darvazalar və turniketlər kimi fiziki maneələr giriş nöqtələrinin sərhədlərini müəyyən etmək və onlara nəzarət etmək üçün quraşdırılmalıdır. Bu maneələr çəkindirici rol oynayır və yalnız səlahiyyətli işçilərə girişi məhdudlaşdırır.

b) *Hücumun aşkarlanması sistemləri:* Perimetrdə müdaxilənin aşkarlanması sistemlərinin yerləşdirilməsi təhlükəsizlik işçilərini hasarları kəsmək və ya maneələrə dırmaşmaq kimi hər hansı pozuntu cəhdlərini aşkarlaya və xəbərdar edə bilər.

c) *Mühafizəçilər:* Giriş nöqtələrinə nəzarət edən, patrul aparan və potensial təhlükəsizlik insidentlərinə cavab verən təlim keçmiş təhlükəsizlik işçilərinin işə götürülməsi əlavə fiziki təhlükəsizlik səviyyəsini artırır.

4. Ətraf Mühitə Nəzarətlər: Şəbəkə infrastrukturunun qorunması yalnız icazəsiz girişdən qorunmaqdan daha çoxunu əhatə edir. Avadanlıqların düzgün işləməsini və

uzunömürlülüyünü təmin etmək üçün optimal ekoloji şəraitin saxlanılması çox vacibdir:

a) *Temperatur və Rütubətin Monitorinqi:* Məlumat mərkəzlərində, server otaqlarında və şəbəkə şkaflarında temperatur və rütubət sensorlarının quraşdırılması, real vaxt rejimində monitorinq və avadanlıqların işinə xələl gətirə biləcək dalğalanmalar zamanı xəbərdarlıq etməyə imkan verir.

b) *Yanğınsöndürmə Sistemləri:* Sprinklerlər və ya qaz əsaslı söndürmə kimi avtomatik yanğınsöndürmə sistemlərinin tətbiqi şəbəkə infrastrukturuna yanğınla bağlı ziyan vurma riskini azaldır.

c) *Fasiləsiz Enerji Təchizatı (UPS):* UPS sistemlərinin elektrik kəsilməsi və gərginlik dəyişmələrinə qarşı qoruyucu vasitələrin yerləşdirilməsi, potensial avadanlıq zədələnməsinin və ya məlumat itkisinin qarşısının alınması.

Şəbəkə infrastrukturu üçün fiziki təhlükəsizlik tədbirləri, o cümlədən məlumat mərkəzləri, server otaqları və şəbəkə şkafları həssas məlumatların və kritik avadanlıqların qorunması üçün həyati əhəmiyyət kəsb edir. Girişə nəzarət sistemlərini, video nəzarəti, perimetr təhlükəsizliyini və ətraf mühitə nəzarəti birləşdirən çox səviyyəli yanaşma icazəsiz giriş, oğurluq, vandalizm və ətraf mühit təhlükələri ilə bağlı riskləri azaltmağa kömək edir. Bu fiziki təhlükəsizlik tədbirlərini həyata keçirməklə təşkilatlar öz şəbəkə infrastrukturunun məxfiliyini, bütövlüyünü və əlçatanlığını təmin edə bilərlər.

Qeyd etmək vacibdir ki, fiziki təhlükəsizlik tədbirləri güclü kibertəhlükəsizlik təcrübələri ilə birlikdə həyata keçirilməlidir. Fiziki təhlükəsizlik tədbirləri fiziki təhdidlərə qarşı qorunma təmin etsə də, kiber təhlükələr də əhəmiyyətli risklər yaradır. Buna görə də, fiziki və kibertəhlükəsizlik tədbirlərini birləşdirən kompleks yanaşma vahid təhlükəsizlik mövqeyi üçün çox vacibdir.

Fiziki təhlükəsizlik tədbirlərinin effektivliyini qiymətləndirmək və təkmilləşdirilməsi lazım olan sahələri müəyyən etmək üçün mütəmadi olaraq qiymətləndirmələr və auditlər aparılmalıdır. Təhlükəsizlik protokolları və prosedurları sənədləşdirilməli və şəbəkə infrastrukturuna çıxışı olan bütün işçilərə çatdırılmalıdır.

İşçilərin fiziki təhlükəsizliyin qorunmasında öz rol və məsuliyyətlərini başa düşmələrini təmin etmək üçün davamlı təlim və maarifləndirmə proqramları həyata keçirilməlidir [8,9].

Bundan əlavə, fiziki təhlükəsizlik texnologiyaları və ən yaxşı təcrübələr üzrə ən son irəliləyişlərdən xəbərdar olmaq vacibdir. Texnologiya inkişaf etdikcə yeni təhdidlər yarana bilər və təhlükəsizlik tədbirləri buna uyğunlaşdırılmalıdır. Fiziki təhlükəsizlik tədbirlərini mütəmadi olaraq nəzərdən keçirmək və yeniləmək təşkilatlara potensial zəifliklərin qarşısını almağa kömək edəcək.

Yekun olaraq, məlumat mərkəzləri, server otaqları və şəbəkə şkafları daxil olmaqla şəbəkə infrastrukturunun qorunması güclü fiziki təhlükəsizlik tədbirləri tələb edir. Girişə nəzarət sistemləri, video nəzarət, perimetr təhlükəsizliyi və ətraf mühitə nəzarət hərtərəfli fiziki təhlükəsizlik strategiyasının mühüm komponentləridir. Bu tədbirləri həyata keçirməklə təşkilatlar icazəsiz giriş, oğurluq, vandalizm və ətraf mühit təhlükələri riskini minimuma endirərək, şəbəkə infrastrukturunun düzgün işləməsini və təhlükəsizliyini təmin edə bilər.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Abbaszadə Aysel Rövşən qızı

KORPORATİV ŞİRKƏTİN ŞƏBƏKƏ İNFRASTRUKTURUNUN LAYİHƏLƏNDİRİLMƏSİ VƏ SİMULYASİYASI

Mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter sistemləri və şəbəkələri"

Elmi rəhbər: **t.e.n., Dosent Cəfərov Nizami Duman oğlu**

BAKI – 2023

III FƏSİL. KORPORATİV ŞİRKƏTİN ŞƏBƏKƏ İNFRASTRUKTURUNUN LAYİHƏLƏNDİRİLMƏSİ VƏ SİMULYASİYASI

3.1. Korporativ şirkətin şəbəkə infrastrukturunun layihələndirilməsi

Dissertasiya işinin praktiki hissəsi olaraq, biz müasir korporativ bir şirkətin İT infrastrukturunu layihələndirib, onun necə işləyəcəyini həyata keçirəcəyik.

Bu infrastruktur 3 mərtəbəli binadan ibarətdir. Birinci mərtəbədə üç şöbə (hüquq, ümumi işlər və logistika), ikinci mərtəbədə üç şöbə (Maliyyə, HR və Satış/Marketinq), üçüncü mərtəbədə isə İT və Admin yerləşir. Beləliklə, dizayn və icra zamanı aşağıdakılar nəzərə alınmalıdır;

- Hər mərtəbəni birləşdirən üç marşrutlaşdırıcı, yəni 3 ədəd Router olmalıdır (hamısı İT departamentində server otağında yerləşdirilməlidir).
- Bütün marşrutlaşdırıcılar (routerlar) serial DCE kabelindən istifadə edərək bir-birinə qoşulmalıdır.
- Routerlər arasında şəbəkə 10.10.10.0/30, 10.10.10.4/30 və 10.10.10.8/30 olmalıdır.
- Hər mərtəbədə bir switchin olması lazımdır (müvafiq mərtəbədə yerləşdirilir).
- Hər mərtəbədə noutbook və telefonlara qoşulmuş Wi-Fi şəbəkələri olmalıdır.
- Hər bir şöbədə printerin olması gözlənilir.
- Hər bir şöbənin aşağıdakı detallarla fərqli VLAN-da olması gözlənilir;
- 1-ci mərtəbə;

- Hüquq - VLAN 80, 192.168.8.0/24 şəbəkəsi
- Ümumi işlər - VLAN 70, 192.168.7.0/24 şəbəkəsi
- Logistika - VLAN 60, 192.168.6.0/24 şəbəkəsi

- 2-ci mərtəbə;

- Maliyyə - VLAN 50, 192.168.5.0/24 şəbəkəsi
- HR- VLAN 40, 192.168.4.0/24 şəbəkəsi

- Satış/Marketinq - VLAN 30, 192.168.3.0/24 şəbəkəsi

•3-cü mərtəbə;

- Admin- VLAN 20, 192.168.2.0/24 şəbəkəsi

- IT- VLAN 10, 192.168.1.0/24 şəbəkəsi

•Marşrutları avtomatik elan etmək üçün marşrutlaşdırma protokolu kimi OSPF-dən istifadə edilməlidir.

•Şəbəkədəki bütün cihazların DHCP serveri kimi konfiqurasiya edilmiş müvafiq router ilə IP ünvanını dinamik şəkildə əldə etməsi lazımdır.

•Şəbəkədəki bütün cihazların bir-biri ilə əlaqə saxlaması lazımdır.

•Təhlükəsiz şəkildə uzaqdan daxil olmaq üçün bütün marşrutlaşdırıcılarda SSH konfiqurasiya edilməlidir.

•İT departamentində Test-PC adlı PC-ni fa0/2 portuna əlavə etməli və uzaqdan girişi yoxlamaq üçün ondan istifadə edilməlidir.

•Yalnız Test-PC-nin fa0/2 portuna daxil olmasına icazə vermək üçün port təhlükəsizliyini İT departamentində switch üçün konfiqurasiya edilməlidir (bağlanma rejiminin pozulması ilə mac-ünvanı əldə etmək üçün sticky-mac adres üsulundan istifadə edilməlidir).

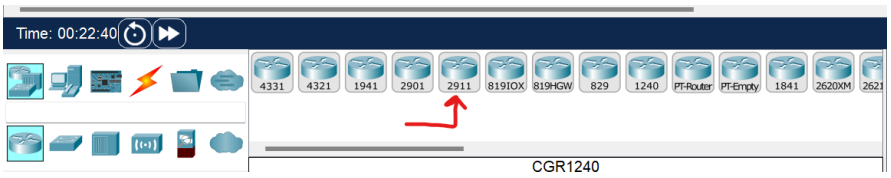
Tətbiq olunacaq İT Texnologiyaları

1. Cisco Packet Tracer istifadə edərək şəbəkə topologiyasının yaradılması.
2. İyerarxik Şəbəkə Dizaynı.
3. Şəbəkə cihazlarının düzgün kabellərlə birləşdirilməsi.
4. VLAN-ların yaradılması və portlara VLAN nömrələrinin təyin edilməsi.
5. Alt şəbəkə və IP ünvanlanması.
6. İnter-VLAN marşrutlaşdırmanın konfiqurasiyası (Router on a stick technology).
7. DHCP Serverinin konfiqurasiyası (Router'da DHCP Server konfiqurasiyası).
8. Təhlükəsiz Uzaqdan giriş üçün SSH konfiqurasiyası.

9. Switchlərdə switch portunun təhlükəsizliyinin və ya Port-Təhlükəsizliyinin konfiqurasiyası.
10. WLAN və ya simsiz şəbəkənin konfiqurasiyası (Cisco Access Point).
11. Host Cihaz Konfiqurasiyaları.
12. Şəbəkə Əlaqəsinin Sınaq və Yoxlanması.

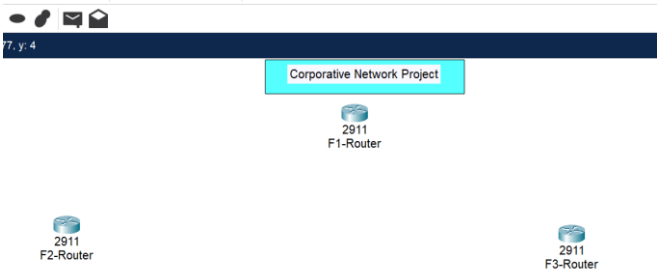
Gəlin korporativ şirkət şəbəkəmizi dizayn etməyə və konfiqurasiya etməyə başlayaq. Bunun üçün əvvəldə də qeyd etdiyimiz kimi Cisco vendorunun "Cisco Packet Tracer" simulation tool'dan istifadə edəcəyik. Bu tool'u yükləyib və quraşdırmaq üçün Cisco'nun rəsmi veb-səhifəsinə daxil olaraq, oradan qeydiyyatdan keçməli və daha sonra bu tool'u yükləməliyik. Bu mərhələləri etdiyimizi nəzərə alaraq, "Cisco Packet Tracer" simulation tool'u açaq.

İlk növbədə yuxarıdakı dokumentasiyada da qeyd etdiyimiz kimi, infrastruktur 3 mərtəbədən ibarətdir və hər mərtəbədə də müvafiq şöbələr fəaliyyət göstərir, bu səbəbdən biz bu 3 mərtəbəni fiziki şəkildə şəbəkə üzərində birləşdirmək üçün 3 ədəd Router'dan istifadə edəcəyik. Yəni, bu 3 ədəd Router hər biri bir mərtəbəyə cavabdehlik daşıyacaq. Router'ları yerləşdirmək üçün "**Network Devices**" bölməsindən **Router** seçməliyik (Şək.3.1): burda 2911 modeli tam şəkildə bizim tələblərimizi qarşılayacağına görə onu seçirik. Bu modeldən 3 dənəsini Cisco Packet Tracer'də iş masasına yerləşdirək.



Şəkil 3.1. Routerin seçilməsi

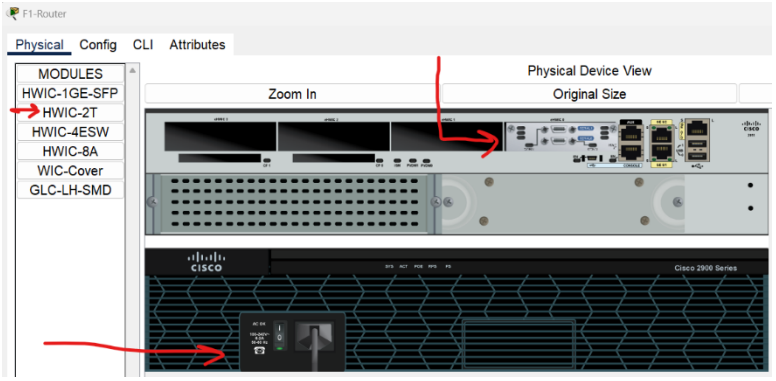
Daha sonra Router'ların üzərinə clickləyərk onları cavabdehlik daşıyacağı mərtəbələrə uyğun adlandıraq (Şək.3.2).



Şəkil 3.2. Roterların adlandırılması

Bundan sonra keçək digər mərhələyə, yəni dokumentasiyada qeyd olunduğu kimi Routerları **serial DCE cable** vasitəsilə bir-birinə birləşdirməyə. Bunun üçün Packet Tracer'da "Connection" bölməsinə gəlməli və oradan Serial DCE cable'I seçməliyik. **Serial cable**'lar Routerlarda yalnız **Serial interface**'lərə qoşulur. Router'lar bir-biriləri ilə Serial cable vasitəsilə əlaqə saxlayır. Bu səbəbdən də biz bu labda bu routerları serial cable vasitəsilə bir-birinə birləşdiririk. Router'da yerləşən Console və ya Auxilary portlara daha sonra Ethernet, FastEthernet, Gigabitethernet, 10GigabitEthernet kimi interface'lərə bu cable'ı qoşa bilmərik təbii ki, çünki bu interface'lərə uyğun olan cable deyil. Serial Cable'lar yalnız Serial Interface'lərə qoşulur. Router'larda default olaraq Serial Interface olmadığına görə İlk növbədə Serial Interface'lər əlavə etməliyik Routerlara.

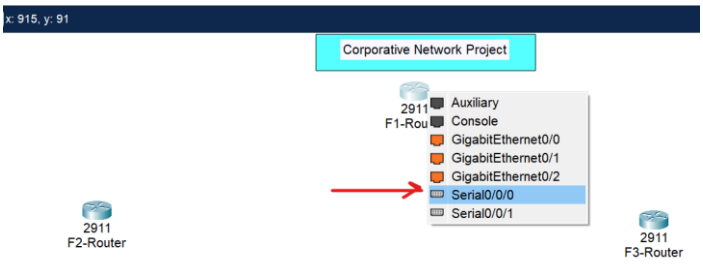
Serial interfeysləri qoşmaq üçün İlk növbədə routera klikləyirik və fizikal taba gəlirik. Serial interfeysin qoşulması üçün əvvəlcə router söndürülməlidir. Daha sonra "HWIC-2T" modulunu routera əlavə edirik (Şək.3.3) (DRAG&DROP vasitəsi ilə). Bu modulu boş yuvaya əlavə etdikdən sonra router'ı yandırırıq. Eyni əməliyyatı digər routerlarda da yerinə yetiririk.



Şəkil 3.3. "HWIC-2T" modulunu routera əlavə edirik

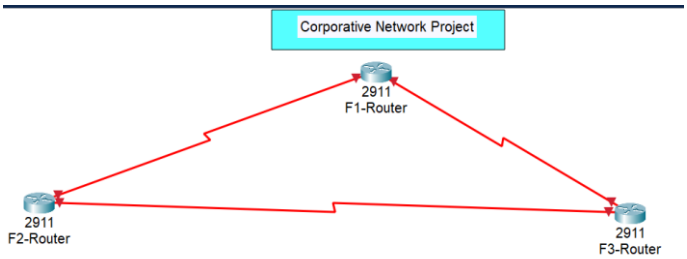
3.2. Korporativ şirkətin şəbəkə infrastrukturunun simulyasiyası

Serial interfeysləri qoşduqdan sonra növbəti proses routerlar'ı bir-biri ilə Serial DCE kabelindən istifadə edərək qoşmaqdır. Serial DCE kabelinin qoşulması üçün "CONNECTİON" bölümündən Serial DCE kabelini seçirik (Şək.3.4) və router üzərinə gəlib müvafiq Serial İnterfeysə birləşdiririk. Birləşdirdikdən sonra yekun routerlar arası əlaqə bu cür görsənəcək:



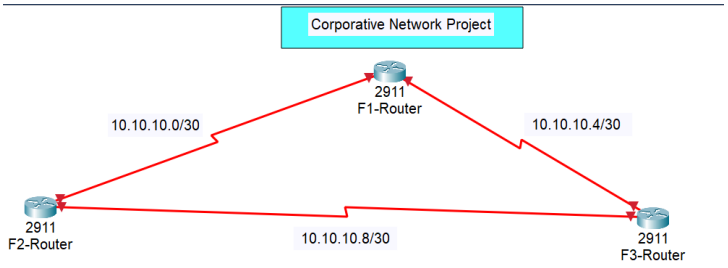
Şəkil 3.4. Serial DCE kabelinin seçilməsi

Router'lar arası yekun dizayn (Şək.3.5.):



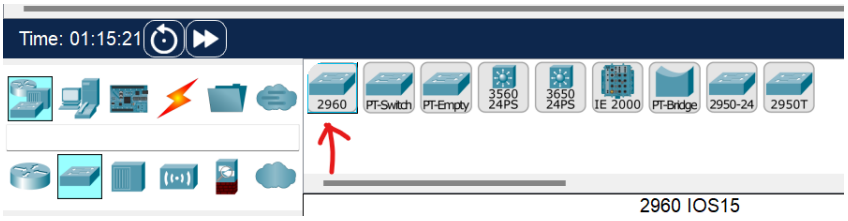
Şəkil 3.5. Yekun dizayn

3. İlk mərhələdə, Place Note-dan istifadə edərək dokumentasiyada verilən tapşırığa uyğun olaraq müvafiq şəbəkələri router'lar arasında qeyd edirik (Şək.3.6).

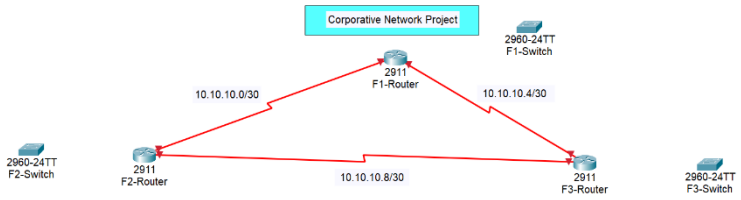


Şəkil 3.6. Şəbəkələrin routerlara qeyd edilməsi

4. İndi sıra hər mərtəbəyə uyğun olaraq switch-in quraşdırılmasıdır (Şək.3.8). Hər mərtəbəyə bir switch quraşdırılmalıdır. Bunun üçün Cisco Packet Tracer-da Network Devices bölməsində Switch tabına keçirilir və buradan uyğun switch seçilir (Şək.3.7) (Biz 2960 model switch seçəcəyik).

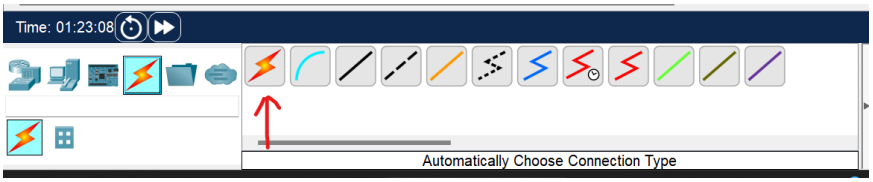


Şəkil 3.7. Switch-in seçilməsi



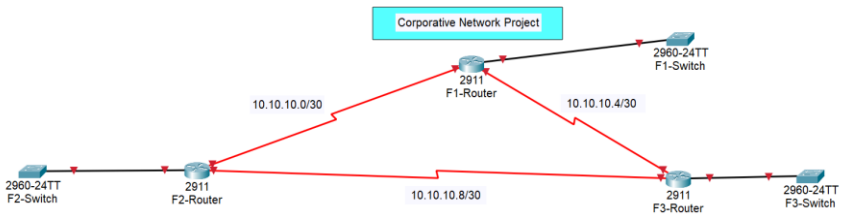
Şəkil 3.8. Switch-in quraşdırılması

Switch-ləri uyğun mərtəbələrə yerləşdirdikdən sonra, sıra onları müvafiq routerlarla birləşdirməkdədir. Bunun üçün "Connection" bölməsinə gəlib avtomatik qoşulmanı seçə bilərik (Şək.3.9).



Şəkil 3.9. Avtomatik qoşulmanın seçilməsi

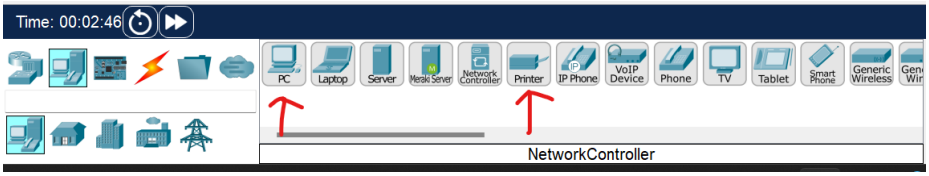
Seçdikdən sonra switch ilə müvafiq router-ı birləşdiririk (Şək.3.10).



Şəkil 3.10. Switch ilə router-un birləşdirilməsi

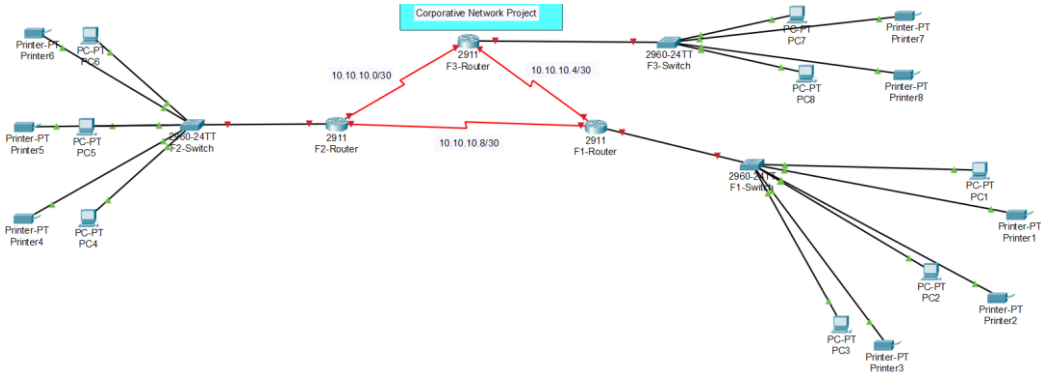
5. Hər mərtəbə laptopların və smartfonların qoşulması üçün Wi-Fi şəbəkə ilə təmin olunmalıdır. Bundan əlavə, hər departamentdə bir ədəd şəbəkə printeri

quraşdırılmalıdır. Qeyd etmişdik ki, birinci mərtəbədə 3 departament mövcuddur (hüquq, ümumi işlər, logistika). Həmçinin ikinci mərtəbədə 3 departament (maliyyə, HR, Satış/Marketinq) və üçüncü mərtəbədə də 2 departament (admin, IT) olacaq. Bütün mərtəbələrdə yerləşən hər departament üçün bir PC və bir printer (Şək.3.11) dizayn etməyə başlayaq:



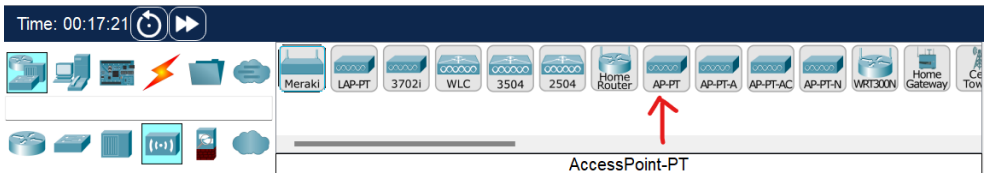
Şəkil 3.11. PC və printerin dizaynı

Dizaynı bitirdikdən sonra onları kabelləşdirməyə başlayaq və bunun üçün avtomatik kabelləşmədən istifadə edək (Şək.3.12):



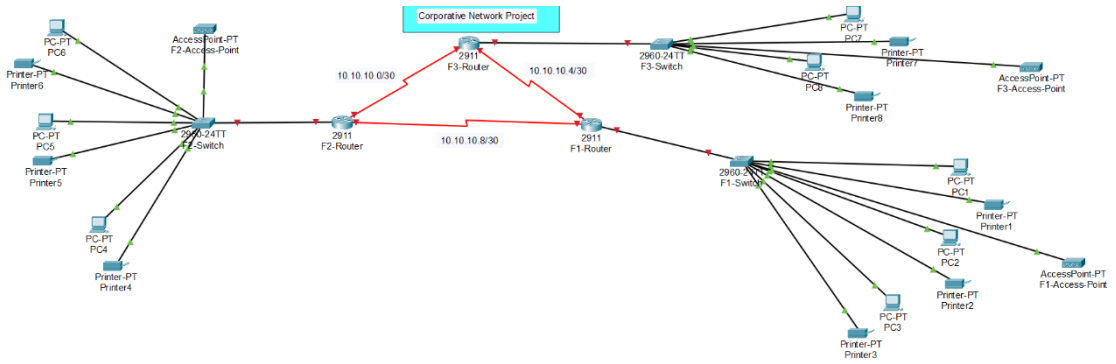
Şəkil 3.12. Avtomatik kabelləşmənin istifadəsi

Yuxarıda qeyd etdiyimiz kimi laptop və smartfonların Wi-Fi şəbəkəsinə bağlana bilməsi üçün Wi-Fi şəbəkəsi quraşdırmalıyıq. Bunun üçün hər mərtəbəyə müvafiq olaraq Access Point dizayn edək. Access Pointləri dizayn etmək üçün Network Device bölməsindən Access Point tabına gələrək uyğun Access Pointi seçək (Şək.3.13):



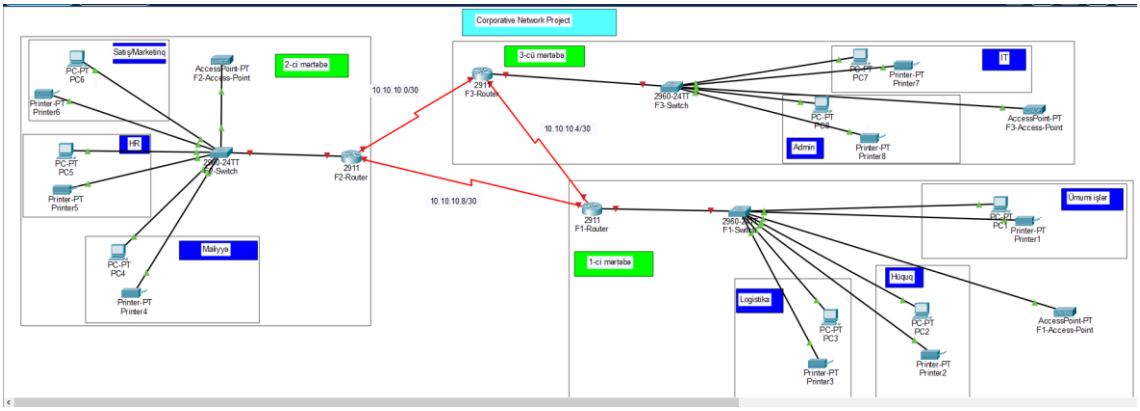
Şəkil 3.13. Access Point-in seçilməsi

Dizayn etdikdən sonra Access Pointləri müvafiq mərtəbədəki switch-lərə quraşdıraq (Şək.3.14).



Şəkil 3.14. Access Point-lərin switch-lərə quraşdırılması

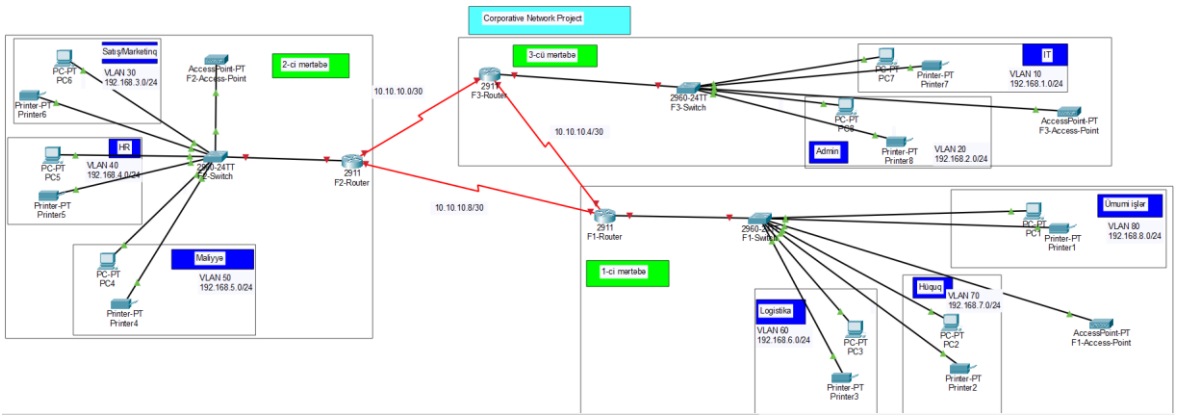
İndi isə topologiyanı qarışdırmamaq üçün mərtəbələri və departamentləri uyğun olaraq "Draw Rectangle" ilə dizayn edək (Şək.3.15).



Şəkil 3.15. "Draw Rectangle" ilə dizayn edilməsi

Yekun şəkildən də göründüyü kimi, mərtəbələri və departamentləri yuxarıda verdiyimiz tapşırığa əsasən ayırdıq.

Yuxarıda tapşırıqda verilən VLAN'ları da "Place Note" ilə qeyd edək hər bir departamentə uyğun olaraq; hər departamentə uyğun olacaq VLAN'ları "Place Note" ilə bir-bir qeyd etdik (Şək.3.16) dizayn şəklində;



Şəkil 3.16. VLAN'ları "Place Note" ilə bir-bir qeyd edilməsi

İndi növbə konfiqurasiya hissəsindədir ki, bu dizaynda qeyd etdiklərimizi İlk növbədə reallaşdıraq, konfiqurasiya edək və daha sonra növbəti tapşırıqları yerinə yetirək. Konfiqurasiya mərhələsinə başlamalıyıq İndi. Bildiyimiz kimi, Router'lar Serial DCE kabel vasitəsilə bir-birilərinə birləşdiriliblər. Bu router'lar arasında şəbəkə traffikinin aktivləşməsi üçün "clock rate" funksiyasını Serail DCE interface'lərdə aktivləşdirməliyik. Bir-birinə qoşulmuş 2 router arasında yalnız birində "Clock Rate" funskiyası görünür və həmin görünən interface'də bu aktiv olunmalıdır.

Routerlər kontekstində saat tezliyi marşrutlaşdırıcının CPU-nun işləmə sürətinə aiddir. Saat tezliyi herts (Hz) ilə ölçülür və o, marşrutlaşdırıcının məlumat paketlərini emal edə və əmrləri yerinə yetirə bilmə sürətini müəyyən edir.

Saat tezliyi tez-tez müxtəlif marşrutlaşdırıcı modellərinin emal gücünü müqayisə etmək üçün istifadə olunur, daha yüksək saat sürətləri ümumiyyətlə daha yaxşı performansı göstərir. Bununla belə, nüvələrin sayı və yaddaşın miqdarı kimi digər amillərin də marşrutlaşdırıcının ümumi performansında əhəmiyyətli rol oynadığını qeyd etmək vacibdir.

Bəzi hallarda, saat tezliyi marşrutlaşdırıcıda seriyal interfeysinin sürətini tənzimləmək üçün də istifadə edilə bilər. Bu, adətən marşrutlaşdırıcının marşrutlaşdırıcının standart sürətindən daha aşağı sürətlə məlumat göndərən bir cihaza qoşulduğu hallarda edilir. İnterfeysdə saat tezliyini təyin etməklə, marşrutlaşdırıcı məlumatların müvafiq sürətlə ötürülməsini təmin edə və hər hansı məlumat itkisinin və ya səhvlərin qarşısını ala bilər.

Birinci, "F3-Router"a keçək; və onun "CLI (Komandası Line Interface)" mode'nu açaq ki, əmrlər toplusu ilə biz bu router'i konfiqurasiya etməyə başlayaq və onun Se 0/0/0 interface'nə daxil olaq. Bunun üçün:

Enable komandası'dan istifadə edərək, keçid edirik privilege mode'a və "configure terminal" komandası ilə keçirik global konfiqurasiya rejiminə və burdan da interface'i qeyd edərək interface'ə daxil oluruq və "no shutdown" komandası ilə Router'in bu interface'in yandırırıq (Şək.3.17). Təhlükəsizlik səbəblərinə görə Router'in bütün interface'ləri default olaraq sönülü olur.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int se 0/0/0
Router(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
```

Şəkil 3.17. Router'in interface'in yandırılması

Eyni şeyləri se 0/0/1 interface'i və gig 0/0 interface'ləri üçün də edək;

Bunları edəndən sonra sıra, F3-Router'da olan DCE interface'lər üçün clock rate'i konfiqurasiya etməkdədir. Birinci se 0/0/0 interface'ə keçək (Şək.3.18): və "clock rate ?" qoyaraq əmrə baxaq:

```
Router(config)#int se 0/0/0
Router(config-if)#clock rate ?
Speed (bits per second
  1200
  2400
  4800
  9600
  19200
  38400
  56000
  64000
  72000
  125000
  128000
  148000
  250000
  500000
  800000
  1000000
  1300000
  2000000
  4000000
  <300-4000000>  Choose clockrate from list above
Router(config-if)#clock rate
```

Şəkil 3.18. se 0/0/0 interface'ə keçid

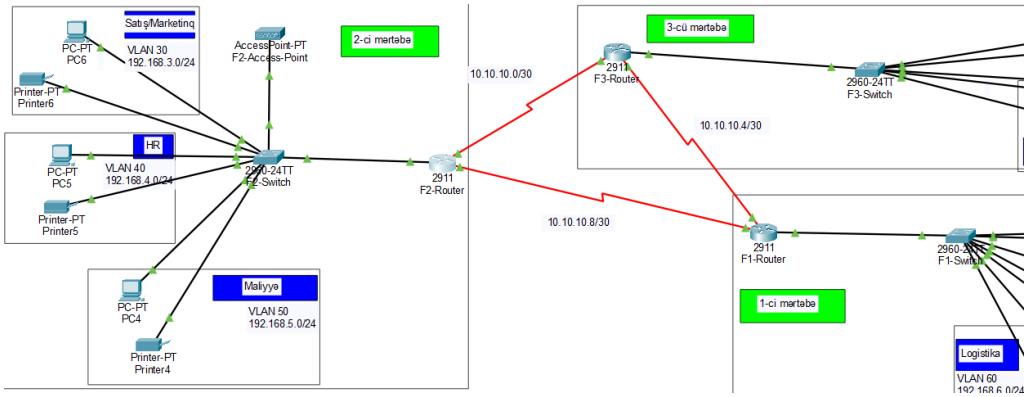
Yuxardakı şəkildə görsənən clock rate parametrlərindən birini seçə bilərik; 64000'i seçək; eynisini digər serial interface üçün də edək; bu konfiqurasiyanı bitirəndən sonra "write memory" əmri ilə etdiyimiz konfiqurasiyanı cihazın flash memory'nə yaddaşa verək; ya da "do wr" komandası ilə. Həmçinin "hostname" komandası ilə router'in adını dəyişərək "F3-Router" edək və eyni configi digər router'larda da edərək hostname'lərin dəyişək.

Keçək "F1-Router"a; burda da eyni qayda ilə İlk növbədə router'ın bütün interface'lərin yandıraq və əgər dce interface mövcuddursa onda clock rate parametri təyin edək; amma görürük ki, bu router'in heç bir dce interface'i yoxdur.

Keçək "F2-Router"a, burda da eyni configləri edək Router'in bütün aktiv

interface'lərin yandıraq və mövcud olan bir dce interface'də clock rate parametrin təyin edək; burda da clock rate parameter olaraq 6400 bps təyin edək; etdiyimiz konfiqurasiyanı yaddaşa verməyə unutmayaq;

Bu konfiqurasiyaları edəndən sonra görürük ki, routerlar arasında olan əlaqələr qırmızıdan yaşıla doğru dəyişib, həmçinin switch və router arasındakı əlaqələr də elədir. Bunun səbəbi odur ki, router'ların bütün aktiv interface'lərini yandırdıq (Şək.3.19);



Şəkil 3.19. Router'ların bütün aktiv interface'lərinin yandırılması

İndi, switch'lərə keçərək onlarda VLAN konfiqurasiyasına başlaya bilərik (Şək.3.20);

Keçək, 1-ci mərtəbədə yerləşən, "F1-Switch"ə baxaq. Bildiyimiz kimi 1-ci mərtəbədə 3 departament mövcuddur və hərəsinin öz fərqli VLAN'ı var. Switch'ə clickləyib, "CLI" rejimə keçək. Bunları etməmişdən əvvəl bütün switch'lərin hostname'in öz mərtəbələrinə uyğun dəyişək, "hostname" əmri ilə. İndi sıra VLAN'ları konfiqurasiya etməkdədir. Birinci başlayaq, "Ümumi işlər" departamentindən, bu olmalıdır 80-ci VLAN'da, həmin departamentdə olan pc və printer "F1-Switch"in fa 0/2 və fa 0/3 interface'lərinə qoşulubdur. Deməli biz switchin bu portlarını 80ci VLAN etməliyik; bunun üçün Switch'də yazaq qlobal konfiqurasiya rejimində:

Int range fa 0/2-3 -- bu komandası ilə 2ci və 3cü portlara eyni anda daxil oluruq

Switchport mode access -- bu komandası ilə həmin portları access mode'a keçiririk. Birmənalı olaraq comp,printer, ip phone kimi avadanlıqların qoşulduğu portlar access rejimdə olmalıdır.Amma switch'lərin bir-birinə qoşulduqları portlar trunk rejimə keçirilir. Çünki access mode'da olan portdan yalnız 1 VLAN barəsində

data və məlumat gedir. Lakin trunk rejimdə olan portdan 1'dən çox VLAN barəsində informasiya axını keçir;

Switchport access vlan 80 --- bu komandası ilə isə həmin portları 80-ci Vlan'a salırıq.

```
F1-Switch(config)#
F1-Switch(config)#
F1-Switch(config)#int ran
F1-Switch(config)#int range fa0/2-3
F1-Switch(config-if-range)#swit
F1-Switch(config-if-range)#switchport m
F1-Switch(config-if-range)#switchport mode a
F1-Switch(config-if-range)#switchport mode access
F1-Switch(config-if-range)#sw
F1-Switch(config-if-range)#switchport a
F1-Switch(config-if-range)#switchport access v
F1-Switch(config-if-range)#switchport access vlan 80
% Access VLAN does not exist. Creating vlan 80
F1-Switch(config-if-range)#
```

Şəkil 3.20. fa 0/2 və fa 0/3 portlarının 80-ci VLAN-a salınması

Eyni konfiqurasiyanı "Hüquq" departamenti üçün edək. Həmin departament 70-ci Vlan'da olmalıdır.fa0/4 və fa 0/5 portlar (Şək.3.21);

```
F1-Switch(config)#int range fa0/4-5
F1-Switch(config-if-range)#swit
F1-Switch(config-if-range)#switchport m
F1-Switch(config-if-range)#switchport mode a
F1-Switch(config-if-range)#switchport mode access
F1-Switch(config-if-range)#sw
F1-Switch(config-if-range)#switchport a
F1-Switch(config-if-range)#switchport access v
F1-Switch(config-if-range)#switchport access vlan 70
% Access VLAN does not exist. Creating vlan 70
F1-Switch(config-if-range)#
```

Şəkil 3.21. fa0/4 və fa 0/5 portlarının 70-ci VLAN-a salınması

Eyni konfiqurasiyanı "Logistika" departamenti üçün edək. Həmin departament 60-cı Vlan'da olmalıdır. fa0/6 və fa 0/7 portlar (Şək.3.22);

```
F1-Switch(config)#int range fa0/6-7
F1-Switch(config-if-range)#switch
F1-Switch(config-if-range)#switchport a
F1-Switch(config-if-range)#switchport access m
F1-Switch(config-if-range)#switchport m
F1-Switch(config-if-range)#switchport mode a
F1-Switch(config-if-range)#switchport mode access
F1-Switch(config-if-range)#sw
F1-Switch(config-if-range)#switchport a
F1-Switch(config-if-range)#switchport access v
F1-Switch(config-if-range)#switchport access vlan 60
% Access VLAN does not exist. Creating vlan 60
F1-Switch(config-if-range)#
```

Şəkil 3.22. fa0/6 və fa 0/7 portlarının 60-cı VLAN-a salınması

Yuxarıda qeyd etdiyimiz kimi, bu portlar access rejimdə olmalıdır ona görə ki, həmin portdan 1 vlan barəsində info və data keçəcək. Amma bu switch'in "F1-Router"a

birləşən portunu biz mütləqdir ki, trunk rejimdə kökləməliyik. Ona görə ki, həmin interface'dən bu switch'də olan bütün vlanlar barəsində info və data axmalıdır ki, bütün device'lar bir-biri ilə əlaqə saxlaya bilsin.

Buna görə də "F1-Switch"in fa 0/1 portuna daxil olaraq, həmin interface'I "trunk" rejimdə kökləyirik (Şək.3.23);

```
Enter configuration commands, one per line.  End with CNTL/Z.
F1-Switch(config)#int fa 0/1
F1-Switch(config-if)#switch
F1-Switch(config-if)#switchport m
F1-Switch(config-if)#switchport mode t
F1-Switch(config-if)#switchport mode trunk

F1-Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up

F1-Switch(config-if)#
```

Şəkil 3.23. "F1-Switch"in fa 0/1 portunun interface'I "trunk" rejimdə köklənməsi

Bəli, artıq hazırdır, "F1-Switch"də konfiqurasiya olunan bütün vlanlar trunk portdan keçə biləcək.

Bunu edəndən sonra bütün konfiqurasiyanı yaddaşa verə bilərik;

"F2-Switch"ə keçək İndi. Burda da 3 VLAN olacaq. Başlayaq "Maliyyə"dən,"Maliyyə" olmalıdır 50-ci VLAN'da (Şək.3.24). Switch'in fa 0/6 və fa 0/7 portları.

```
F2-Switch>
F2-Switch>en
F2-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
F2-Switch(config)#int range fa0/6-7
F2-Switch(config-if-range)#sw
F2-Switch(config-if-range)#switchport m
F2-Switch(config-if-range)#switchport mode a
F2-Switch(config-if-range)#switchport mode access
F2-Switch(config-if-range)#sw
F2-Switch(config-if-range)#switchport a
F2-Switch(config-if-range)#switchport access vlan 50
% Access VLAN does not exist. Creating vlan 50
F2-Switch(config-if-range)#
```

Şəkil 3.24. fa0/6 və fa 0/7 portlarının 50-ci VLAN-a salınması

Daha sonra keçək, "HR" departamentinə, bu olmalıdır 40-cı VLAN'da; Switch'in fa 0/4 və fa 0/5 portları (Şək.3.25);

```
F2-Switch(config)#int range fa0/4-5
F2-Switch(config-if-range)#swi
F2-Switch(config-if-range)#switchport m
F2-Switch(config-if-range)#switchport mode a
F2-Switch(config-if-range)#switchport mode access
F2-Switch(config-if-range)#sw
F2-Switch(config-if-range)#switchport a
F2-Switch(config-if-range)#switchport access vla
F2-Switch(config-if-range)#switchport access vlan 40
% Access VLAN does not exist. Creating vlan 40
```

Şəkil 3.25. fa 0/4 və fa 0/5 portlarının 40-cı VLAN-a salınması

Növbə, "Satış/marketinq" departamentidir, bu departament 30-cu VLAN'da olmalıdır. Switch'in fa0/2 və fa0/3 interface'ləri bu vlan'a keçməlidir (Şək.3.26).

```
F2-Switch(config)#int range fa0/2-3
F2-Switch(config-if-range)#swi
F2-Switch(config-if-range)#switchport m
F2-Switch(config-if-range)#switchport mode a
F2-Switch(config-if-range)#switchport mode access
F2-Switch(config-if-range)#sw
F2-Switch(config-if-range)#switchport a
F2-Switch(config-if-range)#switchport access v
F2-Switch(config-if-range)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Şəkil 3.26. fa0/2 və fa0/3 portlarının 30-cu VLAN-a salınması

Və son olaraq, "F2-Switch"in fa 0/1 interface'in yəni router'a birləşən interface'in trunk rejimə keçirməliyik (Şək.3.27) ki, özündə olan VLAN'ların məlumatların keçirə bilsin və local şəbəkədə olan digər switch'lərə otursun;

```
F2-Switch(config)#int fa 0/1
F2-Switch(config-if)#swit
F2-Switch(config-if)#switchport m
F2-Switch(config-if)#switchport mode t
F2-Switch(config-if)#switchport mode trunk

F2-Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

Şəkil 3.27. "F2-Switch"in fa 0/1 portunun interface'I "trunk" rejimdə köklənməsi

Və edilən konfiqurasiyanı yaddaşa verək;

İndi keçək "F3-Switch"ə, burda 2 VLAN olacaq, admin və IT vlanları. Başlayaq, "IT" vlanından. IT Vlanı olmalıdır 10-cu Vlan'da və switch'in fa 0/2 və fa 0/3 portlarındadır (Şək.3.28) ;

```
F3-Switch>en
F3-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
F3-Switch(config)#int range fa0/2-3
F3-Switch(config-if-range)#switch
F3-Switch(config-if-range)#switchport m
F3-Switch(config-if-range)#switchport mode a
F3-Switch(config-if-range)#switchport mode access
F3-Switch(config-if-range)#sw
F3-Switch(config-if-range)#switchport a
F3-Switch(config-if-range)#switchport access v
F3-Switch(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
F3-Switch(config-if-range)#
```

Şəkil 3.28. fa 0/2 və fa 0/3 portlarının 10-cu VLAN-a salınması

Keçək "Admin" Vlan'a, bu 20-ci vlan'da olmalıdır. Switch'in fa 0/4 və fa0/5 portları bu vlan'a salınmalıdır (Şək.3.29);

```
F3-Switch(config)#int range fa0/4-5
F3-Switch(config-if-range)#swi
F3-Switch(config-if-range)#switchport m
F3-Switch(config-if-range)#switchport mode a
F3-Switch(config-if-range)#switchport mode access
F3-Switch(config-if-range)#sw
F3-Switch(config-if-range)#switchport a
F3-Switch(config-if-range)#switchport access vla
F3-Switch(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
F3-Switch(config-if-range)#
```

Şəkil 3.29. fa 0/4 və fa0/5 portlarının 20-ci VLAN-a salınması

Bundan sonra, Switch'in router'a baxan fa 0/1 interface'in trunk rejimə keçirək (Şək.3.30);

```
F3-Switch(config)#int fa 0/1
F3-Switch(config-if)#swit
F3-Switch(config-if)#switchport m
F3-Switch(config-if)#switchport mode t
F3-Switch(config-if)#switchport mode trunk

F3-Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

Şəkil 3.30. fa 0/1 interface'in trunk rejiminə keçirilməsi

Konfiqurasiyanı yaddaşa verək.

Uğurlu şəkildə, bütün switchlərdə, departamentlərə uyğun olan Vlanları yaratdıq və onları uyğun olduqları interface'lərdə köklədik, bundan savayı, switchlərin magistral portunda trunk rejimini köklədik ki, başqa switchlər üçün özündən həmin vlanlar barəsində məlumatı keçirə bilsin.

İndi Növbə, router'ların interface'lərinə IP ünvan təyin etməkdədir. Əvvəlcədən tapşırıqda qeyd olunan şəbəkəyə əsasən IP ünvanları təyin etməliyik, bizim

topologiyamizda router'lar arasında fərqli şəbəkələr mövcuddur.

Başlayaq, "F1-Router"dan; Onun 2 serial və 1 gigabit Ethernet interface'i var. Keçək, se 0/0/0 interface'nə. Fikir versək, F3 ilə F1 arasındakı şəbəkə 10.10.10.4/30 şəbəkədir. Burda /30 bitmask o deməkdir ki, 255.255.255.252 bu subnet'də, 32-30=2 2 üstü 2 -2 = 2 dənə host ola bilər max, yerde qalan 2 Ip'dən biri subnet digəri isə broadcast IP'dir. Bunu ona görə edirik ki, IP'ə qənaət edək, boş yere IP israfçılığı etməyək, bizə nə qədər lazımdırsa, minimum o qədər IP işlətməliyik və buna görə də subnet təyin etməliyik. Bu səbəbdən, se 0/0/0 interface'nə 10.10.10.5 IP adres'i (Şək.3.31) təyin edək.

```
F1-Router>en
F1-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
F1-Router(config)#int se0/0/0
F1-Router(config-if)#ip addre
F1-Router(config-if)#ip address 10.10.10.5 255.255.255.252
F1-Router(config-if)#
```

Şəkil 3.31. se 0/0/0 interface'nə 10.10.10.5 IP adres'i təyin edilməsi

"F1-Router"in se 0/0/1 interface'nə keçək. Bu olmalıdır 10.10.10.8/30 subnetində. Bu interface'ə isə 10.10.10.9 IP ünvanın təyin edək (Şək.3.32);

```
F1-Router(config)#
F1-Router(config)#int se 0/0/1
F1-Router(config-if)#ip address 10.10.10.9 255.255.255.252
F1-Router(config-if)#
```

Şəkil 3.32. se 0/0/1 interface'nə 10.10.10.9 IP adres'i təyin edilməsi

Və bu konfiqurasiyanı yaddaşa verib həqiqətən də bu IP ünvanlar interface'lərə təyin olundumu onu yoxlayaq (Şək.3.33), bunun üçün **"sh ip int br"** komandası'dan istifadə edirik; görürük ki, Bəli həqiqətən də təyin olunubdur.

```
F1-Router#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            10.10.10.5      YES manual up                    up
Serial0/0/1            10.10.10.9      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
F1-Router#
```

Şəkil 3.33. IP ünvanlar interface'lərə təyin olunub-olunmamasının yoxlanılması

Keçək, "F2-Router"a;

Int se 0/0/0'a daxil olaq və bu olmalıdır 10.10.10.0/30 subnetində, biz bura 10.10.10.1 IP'ni təyin edək (Şək.3.34).

```
F2-Router>en
F2-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
F2-Router(config)#int se 0/0/0
F2-Router(config-if)#ip address 10.10.10.1 255.255.255.252
F2-Router(config-if)#
```

Şəkil 3.34. se 0/0/1 interface'nə 10.10.10.1 IP adres'i təyin edilməsi

Daha sonra, keçək se 0/0/1 interface'nə və bu olmalıdır 10.10.10.8/30 subnetində, biz 10.10.10.9 IP'ni F1-Router'un se 0/0/1 interface'nə təyin etdiyimiz üçün yerde boş qalan 10.10.10.10 IP (Şək.3.35) ünvanın bura təyin edəcəyik;

```
F2-Router(config)#int se 0/0/1
F2-Router(config-if)#ip address 10.10.10.10 255.255.255.252
F2-Router(config-if)#
```

Şəkil 3.35. se 0/0/1 interface'nə 10.10.10.10 IP adres'i təyin edilməsi

Konfiqurasiyanı yaddaşa verək və yoxlayaq (Şək.3.36) görək IP'lər interface'lərə həqiqətən də təyin olunub mu. Bəli, hər şey düzgündur;

```
F2-Router#wr
Building configuration...
[OK]
F2-Router#
F2-Router#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            10.10.10.1      YES manual up                    up
Serial0/0/1            10.10.10.10     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
F2-Router#
```

Şəkil 3.36. IP ünvanlar interface'lərə təyin olunub-olunmamasının yoxlanılması

Keçək, "F3-Router"a

Se 0/0/0 interface'e daxil olaq və bu interface 10.10.10.4/30 subnetində olmalıdır, bu subnetde də cemi bir IP 10.10.10.6 boşda qaldıgi üçün həmin IP'ni təyin edək bura (Şək.3.37);

```
F3-Router>en
F3-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
F3-Router(config)#
F3-Router(config)#int se 0/0/0
F3-Router(config-if)#ip address 10.10.10.6 255.255.255.252
F3-Router(config-if)#
```

Şəkil 3.37. se 0/0/0 interface'nə 10.10.10.6 IP adres'i təyin edilməsi

Daha sonra keçək, se 0/0/1 interface'e və bu interface 10.10.10.0/30 subnetində olmalıdır, bu subnetden isə yalniz 10.10.10.2 IP'i (Şək.3.38) boşda olduğu üçün həmin IP'ni bura təyin edək;

```
F3-Router(config)#
F3-Router(config)#int se 0/0/1
F3-Router(config-if)#ip address 10.10.10.2 255.255.255.252
F3-Router(config-if)#
```

Şəkil 3.38. se 0/0/1 interface'nə 10.10.10.2 IP adres'i təyin edilməsi

Konfiqurasiyanı yaddaşa verək və IP'lərin təyin olundugunu (Şək.3.39) tesdiq edək:

```
F3-Router#wr
Building configuration...
[OK]
F3-Router#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            10.10.10.6      YES manual up                    up
Serial0/0/1            10.10.10.2      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
F3-Router#
```

Şəkil 3.39. IP ünvanlar interface'lərə təyin olunub-olunmamasının yoxlanılması

Beləliklə, routerların interface'ləri üçün də IP ünvanları təyin etmeyi bitirdik;

"INTERVLAN Routing" – İndi Növbə, InterVLAN Routing'i konfiqurasiya etməkdədir. Bunu edəndən sonra DHCP Server'i konfiqurasiya edirik. Bizdə hər departament fərqli VLAN'larda olduğu üçün, bu o deməkdir ki, onlar virtual olaraq hamısı fərqli şəbəkələrdədir. Bildiyimiz kimi, fərqli şəbəkələrdəki host'lar bir-birilərin normalda görə bilmirlər. Onların bir-birini görməsi üçün biz məhz "InterVLAN Routing" kökləməliyik ki, bu VLAN'lar bir-birilərini tanısınlar. Bundan sonra isə, hər VLAN'da olan host'lara avtomatik şəkildə IP adresin təyin olunması üçün DHCP Server qaldırmalı və onu kökləməliyik. IP parametrlərə uyğun olaraq VLAN'lar da veriləcək.

Daxil olaq, "F1-Router"a:

"InterVLAN Routing" konfiqurasiya etmək üçün, İlk növbədə subinterface'lər yaratmalıyıq router'da.VLAN nömrəsi və IP ünvan təyin edəcəyik. Bu subinterface və bu IP adres, həmin reflektiv VLAN'ın default gateway'i kimi özünü aparacaq, yəni xarici şəbəkəyə çıxışı məhz həmin subinterface yerinə yetirəcək.

Gigabitethernet 0/0 interface'ə daxil olaq, subinterface yaratmaq üçün **"int gig 0/0."** komandası ilə İlk növbədə subinterface içərisinə keçməliyik. Bildiyimiz kimi, 1-ci mərtəbədə 3 departament olduğundan, deməli 3 dənə fərqli VLAN olacaq (Bizdə bu

mərtəbədə 80,70,60 Vlan'ları mövcuddur). Bu səbəbdən, birinci yazaq, "**int gig 0/0.80**" həmin subinterface'i yaradaq (Şək.3.40). Subinterface'in uğurla yarandığını görürük;

```
F1-Router(config)#int gig 0/0.80
F1-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.80, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.80, changed state to up

F1-Router(config-subif)#
```

Şəkil 3.40. "**int gig 0/0.80**" həmin subinterface'i yaradılması

Bundan sonra, "**encapsulation dot1Q 80**" komandası ilə encapsulation'u aktivləşdiririk. Həmin VLAN'da, vlan nömrəsi burda mütləq düzgün qeyd olunmalıdır. Bundan sonra bu subinterface üçün, IP adres təyin etməliyik. Bilməliyik ki, həmin subinterface'ə təyin edəcəyimiz IP adres, həmin VLAN üçün "Default Gateway" rolunu oynayacaq, xarici şəbəkəylə əlaqəsini həmin subinterface təyin edəcək. 80-ci VLAN, 192.168.8.0/24 subnetinə sahibdir. Gəlin, subinterface üçün IP adres'i 192.168.8.1 kimi təyin edək (Şək.3.41).

```
F1-Router(config-subif)#encaps
F1-Router(config-subif)#encapsulation do
F1-Router(config-subif)#encapsulation dot1Q ?
  <1-4094>  IEEE 802.1Q VLAN ID
F1-Router(config-subif)#encapsulation dot1Q
% Incomplete command.
F1-Router(config-subif)#encapsulation dot1Q 80
F1-Router(config-subif)#ip address 192.168.8.1 255.255.255.0
F1-Router(config-subif)#
```

Şəkil 3.41. Subinterface üçün 192.168.8.1 IP adres-nin təyin edilməsi

Bu subinterface hazırdır.

İndi keçək, 70-ci VLAN üçün, subinterface yaratmağa. Eyni qayda ilə davam edək. İlk növbədə subinterface yaradaq, encapsulation'u hazır edək və aid olduğu subnetdən həmin subinterface üçün 1'ci IP'ni verək (Şək.3.42). Bu subinterface 192.168.7.0/24 subnetində olmalıdır.

```
F1-Router(config)#int gig 0/0.70
F1-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.70, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.70, changed state to up

F1-Router(config-subif)#encapsulation dot1Q 70
F1-Router(config-subif)#ip address 192.168.7.1 255.255.255.0
F1-Router(config-subif)#
```

Şəkil 3.42. Subinterface üçün 192.168.7.1 IP adres-nin təyin edilməsi

Keçək, 60-cı VLAN üçün subinterface yaratmağa. Bu VLAN 192.168.6.0/24 subnetində olmalıdır. Subinterface üçün IP adres təyin edəndə bu subnetden 1'ci IP'ni

verək (Şək.3.43);

```
F1-Router(config)#int gig 0/0.60
F1-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed state to up

F1-Router(config-subif)#encapsulation dot
F1-Router(config-subif)#encapsulation dot1Q 60
F1-Router(config-subif)#ip add
F1-Router(config-subif)#ip address 192.168.6.1 255.255.255.0
F1-Router(config-subif)#
```

Şəkil 3.43. Subinterface üçün 192.168.6.1 IP adres-nin təyin edilməsi

Və sonda etdiyimiz bütün kökləmələri yaddaşa verək.”F1-Router”da onun cavabdeh olduğu bütün VLAN’lar üçün, InterVlan Routing yaratdıq və köklədik ki, həmin VLAN’da olan hostlar xarici şəbəkəyə çıxa bilsinlər. DHCP Serveri’də konfiqurasiya etdikdən sonra, həmin vlan’ların hostları avtomatik IP adres alandan sonra, bir-biriləri ilə kommunikasiya qura biləcəklər baxmayaraq ki, onlar fərqli şəbəkələrdədirlər. Bu zaman, 70-ci vlan’da olan host, 60-cı Vlan’da olan hostla əlaqə qura biləcək, çünki InterVlan Router’da routing köklənilib.

“DHCP Server”. Gəlin, digər router’lara keçmədən, elə bu Router’da “DHCP Server”i konfiqurasiya edək ki (Şək.3.44), VLAN’lardaki hostlar avtomatik IP adres alsınlar və artıq bir-birilərin heç bir problem olmadan görə bilsinlər. Bildiyimiz kimi, 3 departament var Bizdə 1-ci mərtəbədə, deməli Bizdə 3 dənə IP pool olmalıdır hər departament, vlan üçün fərqli IP hovuzu yaratmalıyıq. İlk növbədə, “**service dhcp”** komandası ilə DHCP Service’i aktivləşdirək. “Ümumi işlər” departamenti üçün IP pool yaradaq:

“**ip dhcp pool Umumi_işlər”** komandası ilə IP pool’a ad verək;

“**network 192.168.8.0 255.255.255.0”** komandası ilə, IP poola aid olacaq subnet’i qeyd edirik;

İndi Növbə, bu network üçün default gateway’i göstərməkdir, Default gateway isə bizim bu VLAN üçün yaratdığımız subinterface’ə təyin etdiyimiz IP ünvan olacaq, yəni 192.168.8.1/24 adres’i;

“**default-router 192.168.8.1”**

“dns-server 192.168.8.1” – DNS Server ünvanını da elə Default Gateway’də olan subinterface’in ünvanın göstəririk;

```
F1-Router(config)#service dhcp
F1-Router(config)#ip dhcp pool Umumi Isler
                               ^
% Invalid input detected at '^' marker.

F1-Router(config)#ip dhcp pool Umumi_isler
F1-Router(dhcp-config)#network 192.168.8.0 255.255.255.0
F1-Router(dhcp-config)#default-router 192.168.8.1
F1-Router(dhcp-config)#dns-server 192.168.8.1
F1-Router(dhcp-config)#
```

Şəkil 3.44. Router'da "DHCP Server"i konfiqurasiya edilməsi

Bu departament üçün, pool hazırdır.

Keçək "Hüquq" departamenti üçün DHCP Server kökləməyə (Şək.3.45). Eyni qayda ilə davam edəcək, sadəcə düzgün VLAN və subneti, default gateway ünvanı göstərmək lazımdır;

```
F1-Router(config)#ip dhcp pool Huquq
F1-Router(dhcp-config)#network 192.168.7.0 255.255.255.0
F1-Router(dhcp-config)#default-router 192.168.7.1
F1-Router(dhcp-config)#dns-server 192.168.7.1
F1-Router(dhcp-config)#
```

Şəkil 3.45. "Hüquq" departamenti üçün IP pool hazırlanması

Bu departament üçün də IP pool hazırladıq. İndi Növbə, "Logistika" departamentinin Vlan'ı üçün IP pool hazırlamaqdadır (Şək.3.46), həmin departament 60-cı Vlan'dadır və subneti 192.168.6.0/24'dür, Default gateway və DNS server ünvanı kimi isə bu vlan üçün yaratdığımız subinterface'i göstərməliyik;

```
F1-Router(config)#ip dhcp pool "Logistika"
F1-Router(dhcp-config)#network 192.168.6.0 255.255.255.0
F1-Router(dhcp-config)#default-rote
F1-Router(dhcp-config)#default-rou
F1-Router(dhcp-config)#default-router 192.168.6.1
F1-Router(dhcp-config)#dns
F1-Router(dhcp-config)#dns-server 192.168.6.1
F1-Router(dhcp-config)#end
F1-Router#
%SYS-5-CONFIG_I: Configured from console by console

F1-Router#wr
Building configuration...
```

Şəkil 3.46. "Logistika" departamenti üçün IP pool hazırlanması

Burda da yaratdıq, bundan sonra bu router'daki konfiqurasiyanı yaddaşa verə bilərik. Yaratdığımız IP pool'lara baxmaq üçün isə "**sh ip dhcp pool**" komandasından istifadə edək (Şək.3.47): gördüyümüz kimi 3 ədəd ip pool var, yaratdığımıza uyğun olaraq, "Ümumi işlər", "Hüquq" və "Logistika" hamsi da öz network vlan'dadır düzgün olaraq. Hələ heç bir cihazı bura qoşmadığımıza görə bu pool'lar aktiv deyil;

```
F1-Router#sh ip dhcp pool

Pool Umumi_isler :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.8.1          192.168.8.1      - 192.168.8.254     0    / 0     / 254

Pool Huquq :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.7.1          192.168.7.1      - 192.168.7.254     0    / 0     / 254

Pool Logistika :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.6.1          192.168.6.1      - 192.168.6.254     0    / 0     / 254
F1-Router#
```

Şəkil 3.46. IP pool'lara baxmaq üçün "**sh ip dhcp pool**" komandasının istifadəsi

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Quliyev Elgün Arzu oğlu

KORPORATİV ŞİRKƏTİN ŞƏBƏKƏ İNFRASTRUKTURUNUN ANALİZİ

Mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter sistemləri və şəbəkələri"

Elmi rəhbər: **t.e.n., Dosent Cəfərov Nizami Duman oğlu**

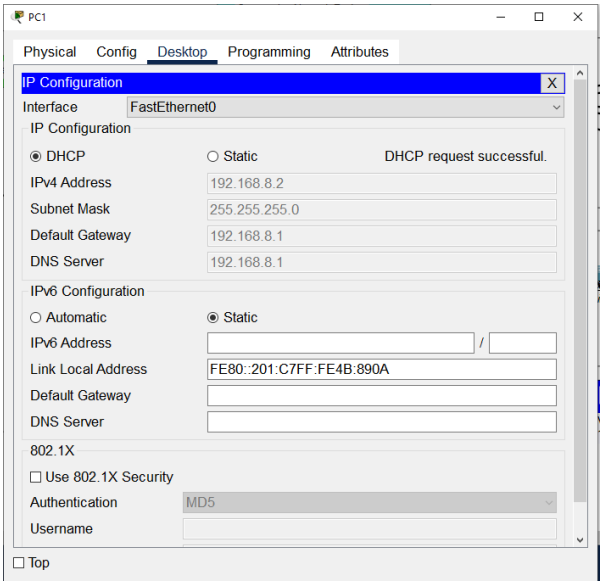
BAKI – 2023

IV FƏSİL. KORPORATİV ŞİRKƏTİN ŞƏBƏKƏ İNFRASTRUKTURUNUN ANALİZİ

4.1. Korporativ şirkətin şəbəkə infrastrukturunun IP ünvanlarının analizi

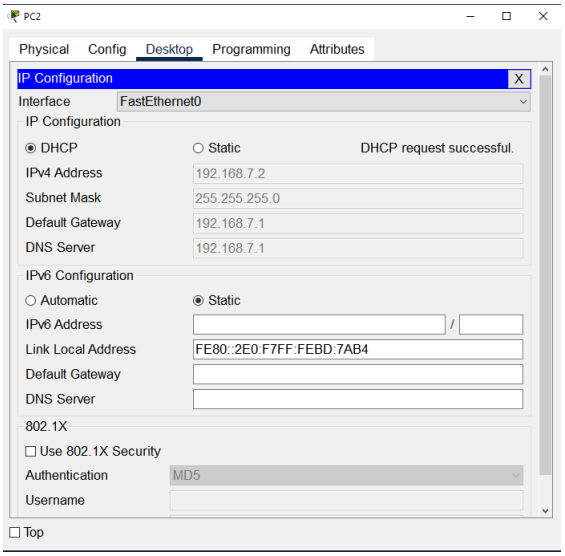
Gəlin bunu test edək görək düzgün işləyir mi, “Ümumi işlər” , “Hüquq” və “Logistika” departamentin PC’lərində IP config’i “dynamic” edək (Şək.4.1) ki, ilk növbədə DHCP Server’dən IP adres ala bilsinlər.

“Ümumi işlər” departamentində olan PC gördüyümüz kimi aldı və həqiqətəndə 8.0 subnetindən IP aldı, Default router və dns server’də düzgün qeyd olunubdur;



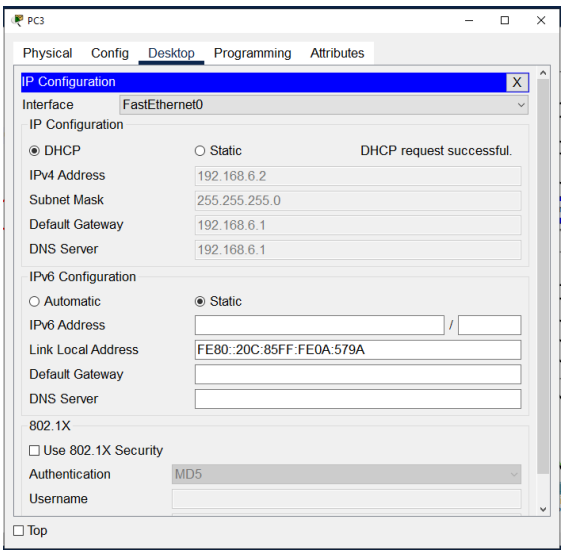
Şəkil 4.1. Departamentlərin PC’lərində IP config’i “dynamic” edilməsi

“Hüquq” departamentini qoşaq (Şək.4.2). Gördüyümüz kimi, bu departament PC’də DHCP Server’dən düzgün IP config aldı, ilk başda buna 7.0 subnetindən olan IP təyin edildi.



Şəkil 4.2. "Hüquq" departamentinin qoşulması

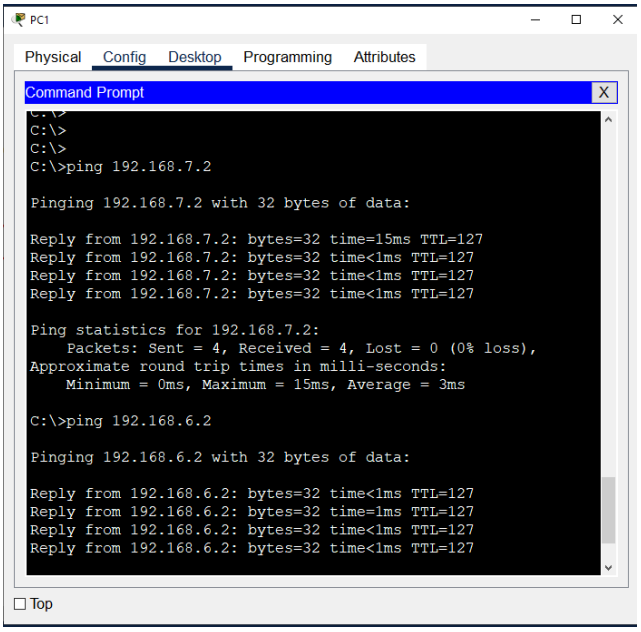
Son olaraq, "Logistika" departamentini də qoşaq (Şək.4.3). Bu da düzgün şəkildə, öz subnetinə uyğun olan IP'ni aldı;



Şəkil 4.3. "Logistika"departamentinin qoşulması

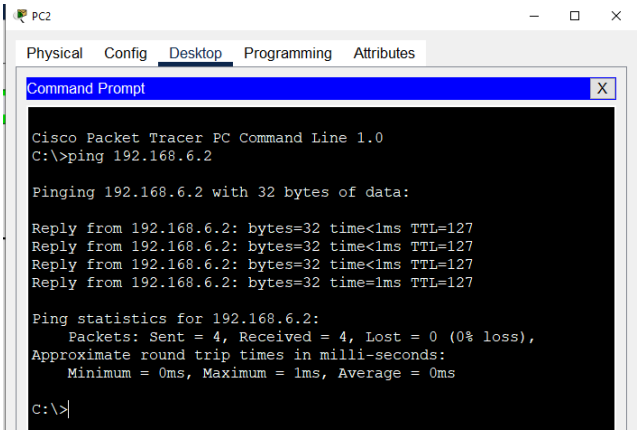
İndi bu departamentlər fərqli vlanlarda, yəni fərqli şəbəkələrdə olduğu üçün normalda bu vlanda olan PC'lər bir-birilərini görə bilməzlər, biz bunu əvvəlcədən həll etdik, "InterVlan routing"i məhz buna görə konfiqurasiya etdik ki, fərqli Vlan'ların nümayəndələri "F1-Router" üzərindən bir-birilərin görə bilsinlər. İndi bunu yoxlayaq görək, həqiqətən də fərqli Vlan'ların nümayəndələri bir-birilərin görə bilirlər? Bunun üçün "Ümumi işlər" departamentinin PC'dən, "Hüquq" departamentinin PC'nə və "Logistika" departamentinin PC'nə ping ataq (Şək.4.4):

Aşağıdaki şəkildən gördüyümüz kimi, həqiqətən də bütün hər şey düzgün konfiqurasiya olunub, həm DHCP Server, həm Intervlan Routing, həm də şəbəkənin dizaynı. Bu səbəbdən də fərqli Vlanların nümayəndələri bir-birilərin heç bir problem olmadan tam şəkildə görə bilirlər.



Şəkil 4.4. "Ümumi işlər" departamentinin PC'dən, "Hüquq" və "Logistika" departamentinin PC'nə ping atılması

İndi isə, Logistika və Hüquq departamentləri arasındakı əlaqəni də yoxlayaq (Şək.4.5) , onların PC'lərindən bir-birilərinə ping ataq. Bəli heç bir problem olmadan görürlər.



Şəkil 4.5. Logistika və Hüquq departamentləri arasındakı əlaqənin yoxlanılması

"F1-Router" və 1-ci mərtəbədə olan departamentlərdə hələki işimizi bitirdik. Biz burda Vlanlar, subinterface'lər, InterVlan Routing, DHCP Server konfiqurasiya etdik

və köklədik. Sonda da bütün bunların düzgün işlədiyini görmək üçün testlərdən keçirdik. İndi növbə eyni tip konfiqurasiyanı “F2-Router”, yəni 2-ci mərtəbədə və “F3-Router” 3-cü mərtəbədə yerinə yetirməkdədir;

Başlayaq, “F2-Router”dan, yəni 2-ci mərtəbədəki departamentlərdən;

“Satış/marketinq” departamentinin VLAN’ı üçün, subinterface kofiqurasiya edək (Şək.4.6) subnetə uyğun olaraq və default gateway ünvanı bu subinterface’ə kökləyək;

```
F2-Router(config)#int gig 0/0.30
F2-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to
up

F2-Router(config-subif)#encapsulation dot
F2-Router(config-subif)#encapsulation dot1Q 30
F2-Router(config-subif)#ip ad
F2-Router(config-subif)#ip address 192.168.3.1 255.255.255.0
```

Şəkil 4.6. Satış/marketinq” VLAN’ı üçün subinterface kofiqurasiya edilməsi

İndi də “HR” Vlan’ı üçün edək (Şək.4.7):

```
F2-Router(config)#int gig 0/0.40
F2-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

F2-Router(config-subif)#en
F2-Router(config-subif)#encapsulation
F2-Router(config-subif)#encapsulation dot1Q 40
F2-Router(config-subif)#ip
F2-Router(config-subif)#ip ad
F2-Router(config-subif)#ip address 192.168.4.1 255.255.255.0
```

Şəkil 4.7. “HR” VLAN’ı üçün subinterface kofiqurasiya edilməsi

“Maliyyə” departamentinin Vlan’ı üçün də edək (Şək.4.8):

```
F2-Router(config)#int gig 0/0.50
F2-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

F2-Router(config-subif)#en
F2-Router(config-subif)#encapsulation d
F2-Router(config-subif)#encapsulation dot1Q 50
F2-Router(config-subif)#ip ad
F2-Router(config-subif)#ip address 192.168.5.1 255.255.255.0
```

Şəkil 4.8. “Maliyyə” VLAN’ı üçün subinterface kofiqurasiya edilməsi

Subinterface’ləri köklədik, InterVlan routing’in işləməsi üçün, İndi də hər vlan üçün DHCP Server’i konfiqurasiya edək və kökləyək:

DHCP Serveri kökləməyə “Maliyyə” vlan’dan başlayaq (Şək.4.9);

```
F2-Router(config)#service dhcp
F2-Router(config)#ip dhcp pool Maliyye
F2-Router(dhcp-config)#network 192.168.5.0 255.255.255.0
F2-Router(dhcp-config)#default-router 192.168.5.1
F2-Router(dhcp-config)#dns-server 192.168.5.1
F2-Router(dhcp-config)#
```

Şəkil 4.9. “Maliyyə” VLAN’ı üçün DHCP Server’i konfiqurasiya edilməsi

“HR” departamenti üçün (Şək.4.10):

```
F2-Router(config)#ip dhcp pool HR
F2-Router(dhcp-config)#network 192.168.4.0 255.255.255.0
F2-Router(dhcp-config)#default-router 192.168.4.1
F2-Router(dhcp-config)#dns-server 192.168.4.1
F2-Router(dhcp-config)#
```

Şəkil 4.10. “HR”VLAN’ı üçün DHCP Server’i konfiqurasiya edilməsi

“Satış/Marketinq” departamenti üçün (Şək.4.11):

```
F2-Router(config)#ip dhcp pool Satis/Marketing
F2-Router(dhcp-config)#network 192.168.3.0 255.255.255.0
F2-Router(dhcp-config)#default-router 192.168.3.1
F2-Router(dhcp-config)#dns-server 192.168.3.1
F2-Router(dhcp-config)#
F2-Router(dhcp-config)#
```

Şəkil 4.11. “Satış/Marketinq”VLAN’ı üçün DHCP Server’i konfiqurasiya edilməsi

“**sh ip dhcp pool**” komandası ilə yaratdığımız IP pool’lara nəzər yetirək: hər şey düzgündür (Şək.4.12).

```
F2-Router#sh ip dhcp pool

Pool Maliyye :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                  Leased/Excluded/Total
 192.168.5.1          192.168.5.1      - 192.168.5.254     0    / 0     / 254

Pool HR :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                  Leased/Excluded/Total
 192.168.4.1          192.168.4.1      - 192.168.4.254     0    / 0     / 254

Pool Satis/Marketing :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                  Leased/Excluded/Total
 192.168.3.1          192.168.3.1      - 192.168.3.254     0    / 0     / 254
F2-Router#
```

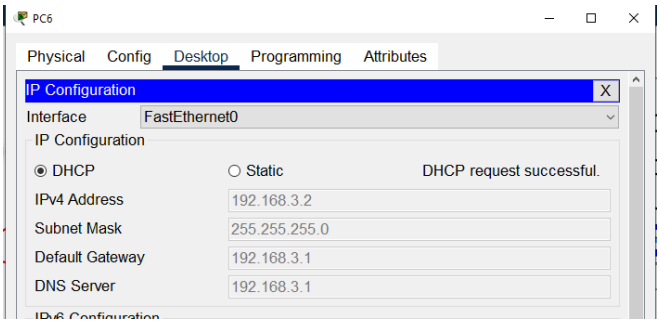
Şəkil 4.12. IP pool’lara baxmaq üçün “**sh ip dhcp pool**” komandasının istifadəsi

4.2. Korporativ şirkətin şəbəkə infrastrukturunun DHCP Serverinin iş rejimlərinin təhlili

İndi isə DHCP Server’in düzgün işlədiyini test etmək üçün ilk növbədə

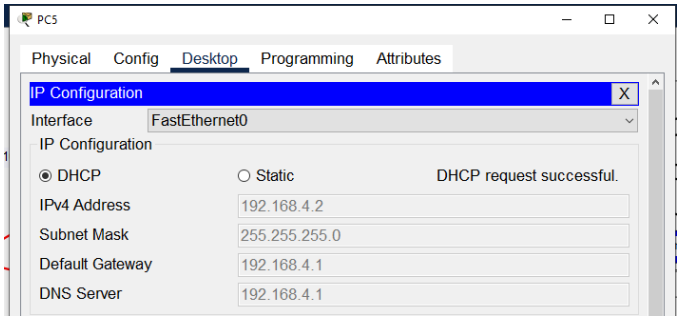
departament PC'lərdə "dynamic" qoşulmaları yoxlayaq (Şək.4.13).

"Satış/Marketinq": hər şey düzgündür və topologiyaya uyğundur;



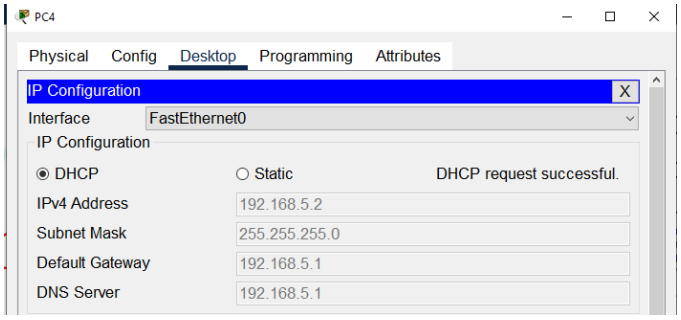
Şəkil 4.13. "Satış/Marketinq" PC-ində "dynamic" qoşulmaların yoxlanılması

"HR": hər şey düzgün konfiqurasiya olunubdur (Şək.4.14).



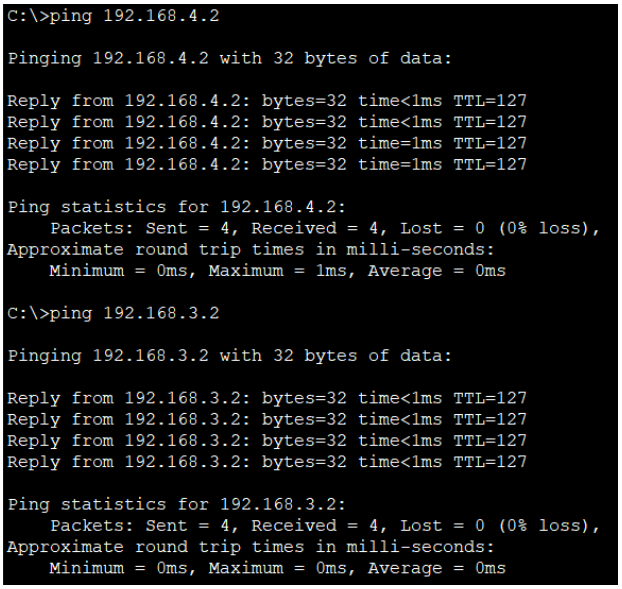
Şəkil 4.14. "HR"departament PC-ində "dynamic" qoşulmaların yoxlanılması

"Maliyyə": hər şey düzgündür (Şək.4.15).



Şəkil 4.15. "Maliyyə" departament PC-ində "dynamic" qoşulmaların yoxlanılması

DHCP Server'in düzgün işlədiyindən əmin olduq, indi isə növbə konfiqurasiya etdiyimiz "Intervlan Routing"in düzgün işlədiyini test etməkdir (Şək.4.16), bunun üçün "Maliyyə" vlan'da olan PC'dən fərqli vlan'larda olan "HR" və "Satış/Marketinq" departamentindəki PC'lərə ping ataq: gördüyümüz kimi hər şey düzgün konfiqurasiya olunub, "Intervlan routing" düzgün konfiqurasiya olunduğuna görə biz, "Maliyyə" vlan'da olan pc'dən fərqli vlandaki pc'ləri görə bildik.



Şəkil 4.16. "Intervlan Routing"in düzgün işlədiyinin test edilməsi

"F2-Router" və 2-ci mərtəbədə də hələki işlərimizi bitirdik. Burda subinterface'lər, DHCP Server, Intervlan Routing konfiqurasiya etdik.

İndi "F3-Router" və 3-cü mərtəbədə olan departament vlan'larına keçək. Burda da digərlərindəki kimi eyni kökləmələri edəcəyik. IT Vlan (Şək.4.17):

```
F3-Router(config)#int gig 0/0.10
F3-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

F3-Router(config-subif)#enc
F3-Router(config-subif)#encapsulation dot
F3-Router(config-subif)#encapsulation dot1Q 10
F3-Router(config-subif)#ip ad
F3-Router(config-subif)#ip address 192.168.1.1 255.255.255.0
```

Şəkil 4.17. IT Vlan köklənməsi

Admin Vlan (Şək.4.18):

```
F3-Router(config)#int gig 0/0.20
F3-Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

F3-Router(config-subif)#en
F3-Router(config-subif)#encapsulation do
F3-Router(config-subif)#encapsulation dot1Q 20
F3-Router(config-subif)#ip address 192.168.2.1 255.255.255.0
```

Şəkil 4.18. Admin Vlan köklənməsi

DHCP Server: Burda DHCP Server'i kökləməyə başlayaq. Bu 2 departament üçün 2 fərqli IP pool yaradaq (Şək.4.19).

```
F3-Router(config)#service dhcp
F3-Router(config)#ip dhcp pool IT
F3-Router(dhcp-config)#network 192.168.1.0 255.255.255.0
F3-Router(dhcp-config)#default-router 192.168.1.1
F3-Router(dhcp-config)#dns-server 192.168.1.1
F3-Router(dhcp-config)#
```

Şəkil 4.19. DHCP Server-inin köklənməsi

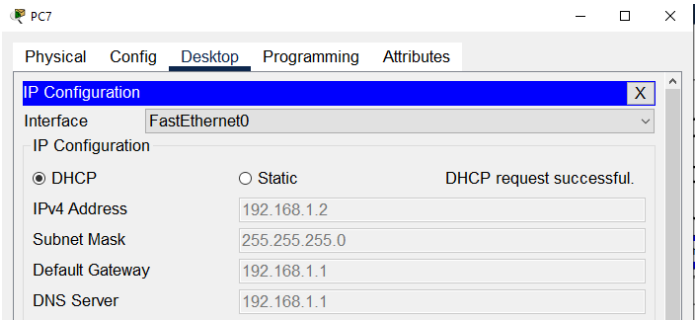
İndi də "Admin Vlan" üçün IP pool yaradaq (Şək.4.20):

```
F3-Router(config)#ip dhcp pool Admin
F3-Router(dhcp-config)#network 192.168.2.0 255.255.255.0
F3-Router(dhcp-config)#default-router 192.168.2.1
F3-Router(dhcp-config)#dns-server 192.168.2.1
F3-Router(dhcp-config)#
```

Şəkil 4.20. "Admin Vlan" üçün IP pool yaradılması

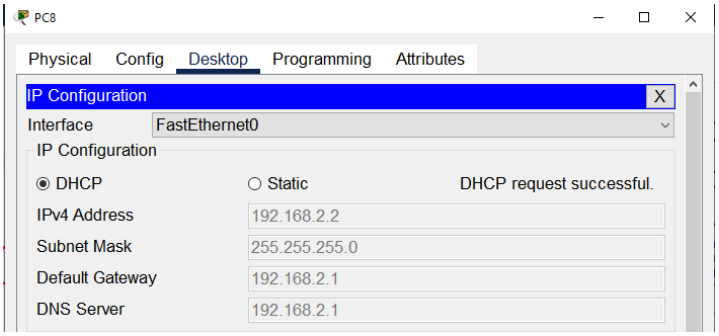
Birinci DHCP Server'in düzgün işlədiyini test edək.

IT Vlan (Şək.4.21):



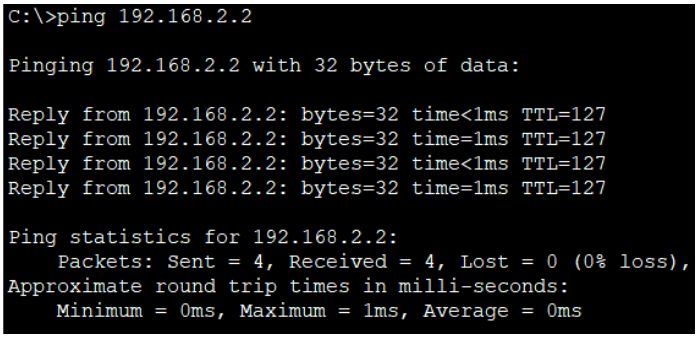
Şəkil 4.21. IT Vlan üçün DHCP Server'inin düzgün işlədiyinin test edilməsi

Admin Vlan (Şək.4.22):



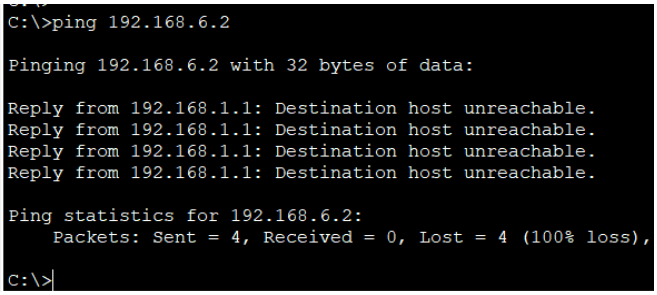
Şəkil 4.22. Admin Vlan üçün DHCP Server'inin düzgün işlədiyinin test edilməsi

Gördüyümüz kimi düzgün işləyir, indi isə "InterVlan Routing"i yoxlayaq (Şək.4.23), yəni fərqli vlan'ların bir-birini görməsini, PC'lərdən bir-birinə ping ataq: hər şey problemsiz şəkildə, düzgün işləyir.



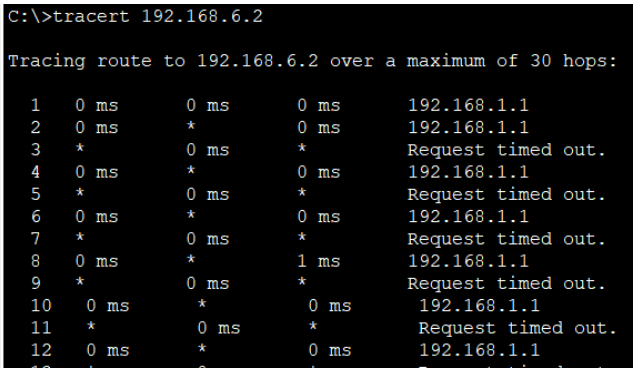
Şəkil 4.23. "InterVlan Routing"i yoxlanılması

Bizə tapşırıq verilmişdi ki, bütün şəbəkədə hostlar bir-birilərin görə bilməlidirlər. Amma biz indi "IT" vlan'da olan PC'dən "Logistika" vlan'da olan PC'ə ping atsaq (Şək.4.24) görəcəyik ki, onlar bir-birilərin görmürlər. "Destination host unreachable" error'un verir.



Şəkil 4.24. "IT" vlan'da olan PC'dən "Logistika" vlan'da olan PC'ə ping atılması

Yəni ICMP packet'i default-gateway rolunu oynayan router'a çatır və orda qırılır. Hətta bunu sübut da edə bilərik. Həmin ICMP packet'in Default Gateway'də qırıldığını sübut etmək üçün "Logistika" vlan'dakı PC'nın IP ünvanına "**tracert**" edək (Şək.4.25): Bəli dediyimiz kimi, həqiqətən də bu ICMP Packet'i default gateway'də qırılır, onu keçə bilmir.



Şəkil 4.25. "Logistika" vlan'dakı PC'nın IP ünvanına "**tracert**" edilməsi

Bunun isə səbəbi ona görədir ki, "F3-Router"i "F1-Router"un daxilində olan

şəbəkələri və vlanları, subnetləri görə bilmir. Router'ların bir-birilərinin daxilində olan şəbəkələr və vlanlar barədə məlumatlı olması üçün, bir-birilərinin daxili şəbəkələrini görə bilməsi üçün biz hər hansı bir dinamiki marşrutlaşdırma protokolundan istifadə edərək şəbəkəmizdə olan bütün router'larda onu kökləməliyik ki, router'lar bir-birilərinin daxilində olan şəbəkələri elan eləsinlər və digərləri həmin elanları öz "routing table"da qeyd etsinlər və həmin şəbəkələrə cavabdeh olan router'i tanısınlar ki, həmin ünvana getmək lazım olanda hansı router'a müraciət edəcəklərindən xəbərləri olsun. Bir neçə dinamiki marşrutlaşdırma protokol'u mövcuddur. Biz dinamiki marşrutlaşdırma protokolu olaraq "**OSPF (Open Shortest Path First)**" seçək.

"**F1-Router**"a daxil olaraq, OSPF'i kökləməyə başlayaq (Şək.4.26):

"**router ospf 10"--** burda ospf protocol'u aktivləşdiririk və ona hər hansı bir proses ID təyin etdik, 10 ID'ni təyin etdik, bu bütün router'larda eyni olacaq bu process ID;

"**network …"** – daha sonra "F1-Router" un cavabdeh olduğu şəbəkələri burda qeyd edirik ki, elan edən zaman desin ki, mən bu şəbəkələrə cavabdehlik daşıyıram. Topologiyadan baxanda görürük ki, "F1-Router" 5 şəbəkəyə cavabdehlik daşıyır, 10.10.10.4/30; 10.10.10.8/30; 192.168.8.0/24; 192.168.7.0/24; və 192.168.6.0/24 şəbəkələrinə. Birinci 10.10.10.4./30 subnetini elan edək və bu network üçün "area" elan etməliyik, məs, "area 0" seçək, backbone area;

"**network 10.10.10.4 255.255.255.252 area 0"**

Daha sonra, digər şəbəkələri də eyni bu qayda ilə elan edək "F1-Router"da və sonda yaddaşa vərək.

```
F1-Router>en
F1-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
F1-Router(config)#
F1-Router(config)#router ospf 10
F1-Router(config-router)#network 10.10.10.4 255.255.255.252 area 0
F1-Router(config-router)#network 10.10.10.8 255.255.255.252 area 0
F1-Router(config-router)#network 192.168.8.0 255.255.255.0 area 0
F1-Router(config-router)#network 192.168.7.0 255.255.255.0 area 0
F1-Router(config-router)#network 192.168.6.0 255.255.255.0 area 0
F1-Router(config-router)#end
F1-Router#
%SYS-5-CONFIG_I: Configured from console by console

F1-Router#wr
```

Şəkil 4.26. OSPF'inin köklənməsi

Etdiyimiz “OSPF” konfiqurasiyasına baxmaq üçün bunu etmək üçün “sh ip ospf int” , “sh ip ospf” , “sh ip ospf neighbor” kimi command’lardan istifadə edə bilərik. Hal-hazırda basqa heç bir router’da “OSPF”i konfiqurasiya etməyimizə görə, “neighbor” command’da heç bir info əldə edə bilməyəcəyik, amma digər komandaları ları yoxlaya bilərik (Şək.4.27). Gördüyümüz kimi, “Backbone (area 0)”da 5 dənə interface olduğun göstərir və həqiqətən də belədir.

```
F1-Router#sh ip ospf
 Routing Process "ospf 10" with ID 192.168.8.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 5
        Area has no authentication
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 1. Checksum Sum 0x0028ec
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Şəkil 4.27. “OSPF” konfiqurasiyasına baxılması

“**F2-Router”:** İndi keçək, “F2-Router”da “OSPF”i konfiqurasiya etməyə (Şək.4.28). Bu router’da 5 şəbəkəyə cavabdehlik daşıyır: 10.10.10.0/24; 10.10.10.8/24; 192.168.3.0/24; 192.168.4.0/24 və 192.168.5.0/24 şəbəkələrinə. Burda da şəbəkələri elan eləməyə başlayan zaman “**router ospf 10”** yəni bütün router’larda eyni “Process ID”ni qeyd etməliyik;

```
F2-Router(config)#router ospf 10
F2-Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
F2-Router(config-router)#network 10.10.10.8 255.255.255.252 area 0
F2-Router(config-router)#net
00:14:19: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.8.1 on Serial0/0/1
from LOADING to FULL, Loading Do
F2-Router(config-router)#network 192.168.3.0 255.255.255.0 area 0
F2-Router(config-router)#network 192.168.4.0 255.255.255.0 area 0
F2-Router(config-router)#network 192.168.5.0 255.255.255.0 area 0
F2-Router(config-router)#
```

Şəkil 4.28. “F2-Router”da “OSPF”i konfiqurasiyası edilməsi

Bundan sonra “sh ip ospf neighbor” “sh ip ospf” kimi commandlar’la OSPF protokolunu monitorinq edə bilərik (Şək.4.29); gördüyümüz kimi “F1-Router”in 192.168.8.1 interface’i ilə “OSPF neighborhood” əlaqəsi qurulubdur;

```
F2-Router#sh ip ospf process
                ^
% Invalid input detected at '^' marker.

F2-Router#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.8.1       0   FULL/  -        00:00:37    10.10.10.9      Serial0/0/1
F2-Router#sh ip ospf
 Routing Process "ospf 10" with ID 192.168.5.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
```

Şəkil 4.29. OSPF protokolunun monitorinq edilməsi

"**F3-Router":** İndi Növbə, sonuncu "F3-Router"da OSPF"i konfiqurasiya etməkdədir (Şək.4.30). Bu router isə, 10.10.10.0/30; 10.10.10.4/30; 192.168.1.0/24 və 192.168.2.0/24 şəbəkələrinə cavabdehlik daşıyır. Burda da bu şəbəkələri elan edən zaman, area 0 olan backbone area'a salınmalıdır.

```
F3-Router(config)#router ospf 10
F3-Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
F3-Router(config-router)#network 10.10.10.4
00:20:58: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.5.1 on Serial0/0/1 from LOADING to FULL, Loading Don
                          ^
% Invalid input detected at '^' marker.

F3-Router(config-router)#network 10.10.10.4 255.255.255.252 area 0
F3-Router(config-router)#network 192.168.1.0 255.255.255
00:21:17: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.8.1 on Serial0/0/0 from LOADING to FULL, Loading
Done
.0 area 0
F3-Router(config-router)#network 192.168.2.0 255.255.255.0 area 0
F3-Router(config-router)#
```

Şəkil 4.30. "F3-Router"da OSPF"inin konfiqurasiya edilməsi

Burda da bitirdik OSPF konfiqurasiyanı, indi isə "sh ip ospf neighbor"; "sh ip ospf process ID"; "sh ip ospf interface" kimi command'lar vasitəsilə OSPF"in statusuna baxa bilərik bu router'da (Şək.4.31):

Gördüyümüz kimi "F1-Router"in 2 dənə OSPF qonşusu var, həqiqətən də belədir. Daha sonra, onun "OSPF Routing" prosesin yerinə yetirən interface'i olan 192.168.2.1'i görə bilirik;

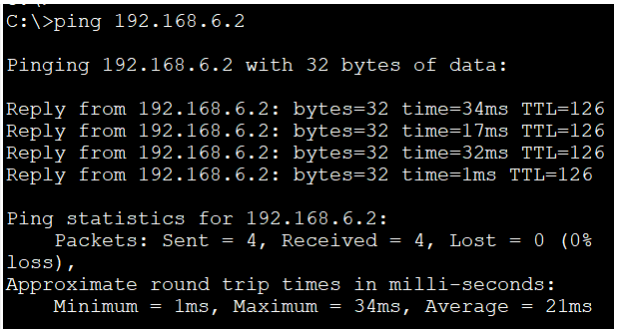
```
F3-Router#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.8.1       0   FULL/  -        00:00:37    10.10.10.5      Serial0/0/0
192.168.5.1       0   FULL/  -        00:00:38    10.10.10.1      Serial0/0/1
F3-Router#
F3-Router#sh ip ospf 10
 Routing Process "ospf 10" with ID 192.168.2.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 4
```

Şəkil 4.31. OSPF"in statusuna baxılması

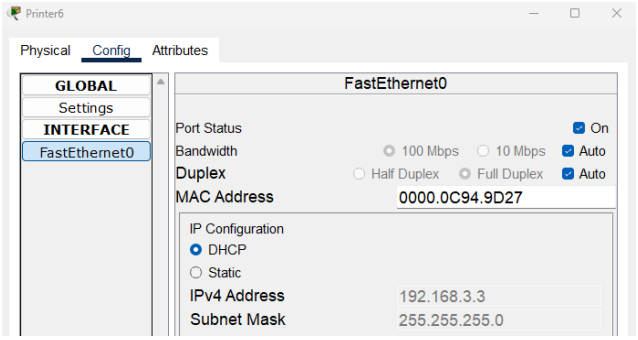
Biz “OSPF” protokol’u konfiqurasiyasın tamamilə bitirdik şəbəkədə olan bütün Router’larda. Əgər, “OSPF” düzgün konfiqurasiya olunubdursa, biz heç bir problem olmadan fərqli mərtəbələrdə yerləşən departament VLAN’lardan bir-birinə ping ataraq onlar arasındakı connection’u yoxlaya bilərik (Şək.4.32), əgər ping’lər düzgün getsə, dəməli həm connection, həm də konfiqurasiya düzgün edilibdir.

Gəlin “İT” departamentinin VLAN’dan “Logistika” departamentinin VLAN’da olan PC’ə ping ataq, OSPF’i konfiqurasiya etməmişdən əvvəl ping getmirdi, İndi getməlidi: Bəli getdi.



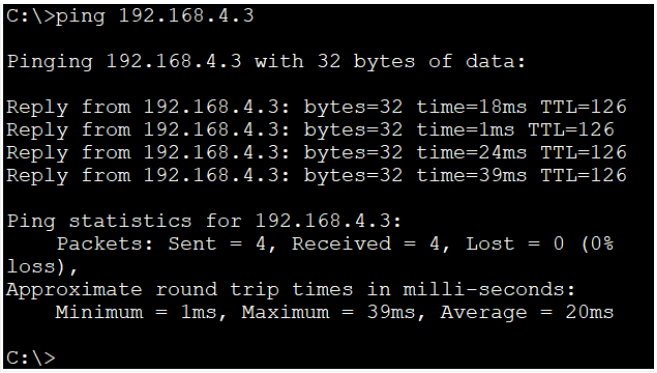
Şəkil 4.32.“OSPF”-in düzgün konfiqurasiya olunub-olunmamasının yoxlanılması

Xatırlayırıqsa, biz hər departamentə bir ədəd şəbəkə printeri qoşmuşduq. İndi gəlin, bu şəbəkə printerlərinin də avtomatik şəkildə IP ünvan ala bilməsi üçün, onlarda DHCP’ni aktivləşdirək (Şək.4.33). Bütün departament’də olan şəbəkə printerlərini bu qayda ilə DHCP Server’dən IP address almasını təmin edək;



Şəkil 4.33. Printerlərin IP ünvan ala bilməsi üçün onlarda DHCP’ni aktivləşdirilməsi

Bunları da edəndən sonra, gəlin İT departament VLAN’dan “HR” Vlan’da olan şəbəkə printerinə olan connection’u yoxlayaq (Şək.4.34), ona ping ataq: gördüyümüz kimi, düzgün şəkildə ping gedir, heç bir problem olmadan;



Şəkil 4.34. İT departament VLAN'dan "HR" Vlan'da olan şəbəkə printerinə connection'ının yoxlanılması

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazma hüququnda

Babayeva Gülmirə Nazim qızı

KORPORATİV ŞİRKƏTİN ŞƏBƏKƏ İNFRASTRUKTURUNUN KONFİQURASİYASI

Mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter sistemləri və şəbəkələri"

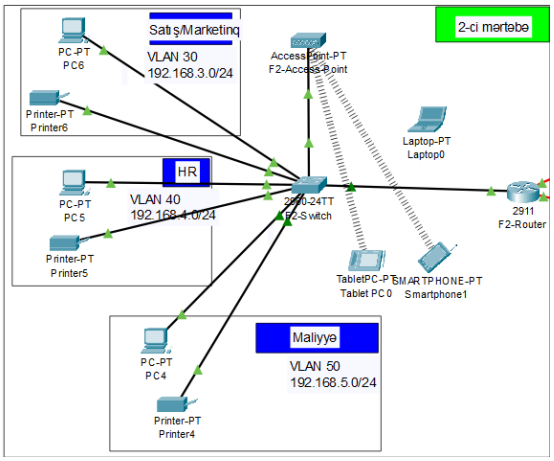
Elmi rəhbər: **t.e.n., Dosent Cəfərov Nizami Duman oğlu**

BAKI – 2023

V FƏSİL. Korporativ şirkətin şəbəkə infrastrukturunun konfiqurasiyası

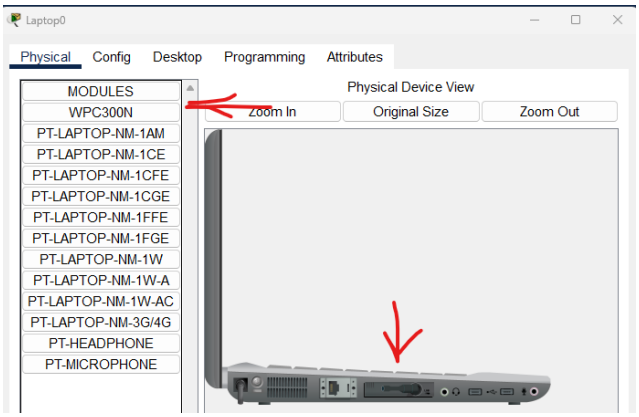
5.1. Korporativ şirkətin şəbəkə infrastrukturunun Wi-Fi network konfiqurasiyası

Xatırlayırıqsa, bizə verilən tapşırıqlardan biri də hər mərtəbədə, laptop və smartphone'ların qoşulması üçün müvafiq Wi-Fi şəbəkəsinin yaradılması və konfiqurasiya olunması idi. Gəlin indi bunu kökləməyə başlayaq. Bunun üçün, müvafiq olaraq hər mərtəbəyə "Access Point" yerləşdirmişdik. Bunu etməmişdən qabaq hər mərtəbəyə 1 ədəd laptop, tablet və smartphone dizayn edək (Şək.5.1).



Şəkil 5.1. Laptop, tablet, smartphone dizaynı

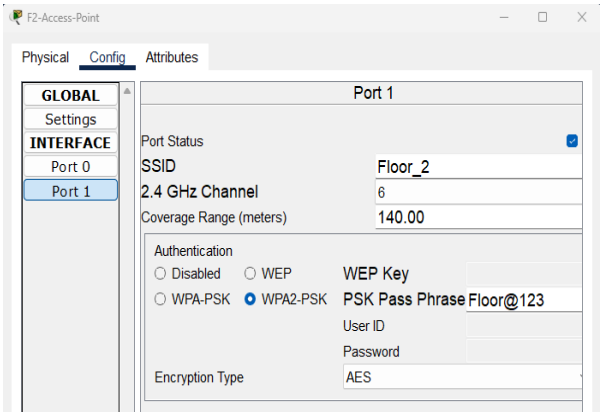
Amma laptop'a ilk növbədə "Wireless module" əlavə olunmalıdır (Şək.5.2), bunun üçün laptop'a gəlib, daha sonra laptop'u söndürüb, onda ethernet module'u çıxarıb, əvəzinə wireless module əlavə edib, daha sonra laptop'u yandırmaq lazımdır.



Şəkil 5.2. Wireless module əlavə edilməsi

Daha sonra, "**F2-Access-Point**"ə keçid edək və burda "**Port 1**" üzərinə gələk.

SSID olaraq, yəni Wi-Fi network name olaraq “**Floor_2**” təyin edək. Authentification type olaraq isə “**WPA2-PSK**” seçək, password olaraq: “**Floor@123**” təyin edək (Şək.5.3).



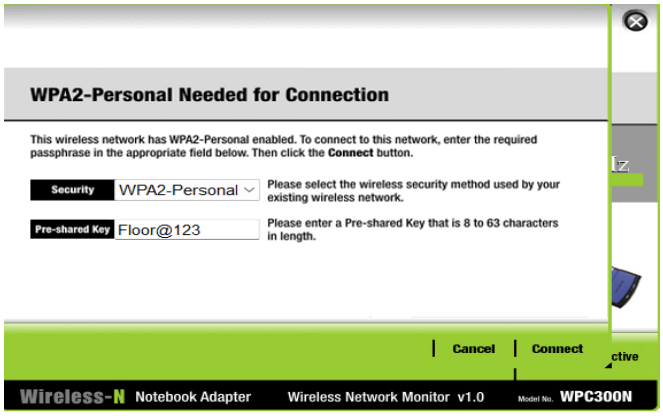
Şəkil 5.3. Wi-fi password təyin olunması

Bunu edəndən sonra, bu AP’e qoşulan cihazlar atılacaq burdan, çünki AP’də konfiqurasiya dəyişikliyi baş verib və yəni Wi-Fi network yaradılaraq, password əlavə olunub, İndi bu məlumatları cihazlarda qeyd edərək, həmin “**Floor_2**” wi-fi şəbəkəsinə qoşulmaq lazımdır. İlk öncə, laptop’dan başlayaq, laptop’u bu Wi-Fi şəbəkəsinə qoşmaq üçün, “**PC Wireless**” bölməsinə keçid etməliyik. Burda da “**Connect**” tab’na keçid edərək, refresh etməliyik ki, yaratdığımız Wi-Fi network burda görünsün və biz ona daxil ola bilək (Şək.5.4). Aşağıdakı şəkildən də, gördüyümüz kimi, yaratdığımız “**Floor_2**” Wi-Fi network’u burda görsəndi, gəlin indi ona qoşulmağa cəhd edək.

Şəkil 5.4. Wi-fi network görüntüsü

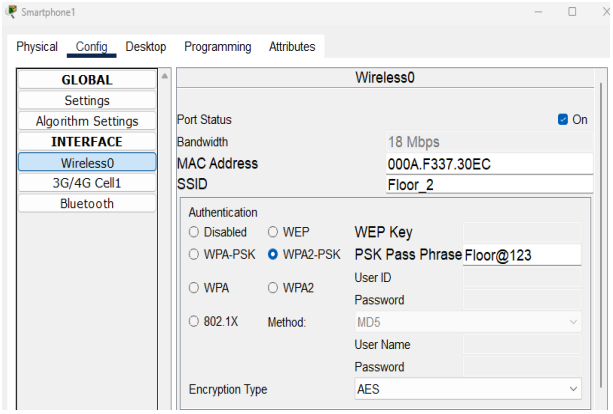
Və bu bölmədə ona təyin etdiyimiz Pre-shared-key, yəni, Wi-Fi password’u daxil

edərək qoşulma cəhdi edək (Şək.5.5);



Şəkil 5.5. Wi-Fi qoşulma

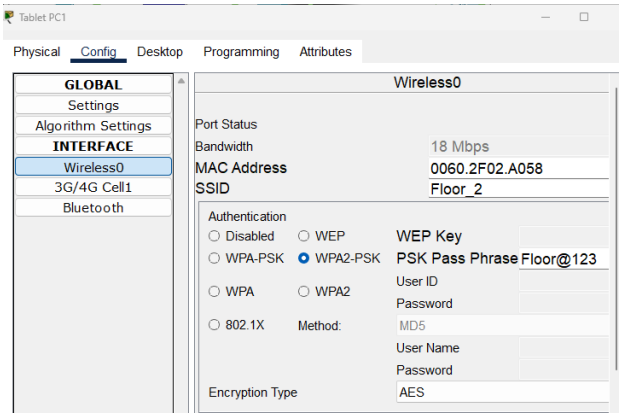
Bəli, həqiqətən də laptop "**Wireless connection**" üzərindən AP'in payladığı "**Floor_2**" Wi-Fi network'a uğurla qoşuldu. İndi gəlin digər cihazları qoşaq bu "**Floor_2**" Wi-Fi şəbəkəsinə. **Smartphone**'dan başlayaq: **Config** bölməsində, **Wireless0** tab'a keçid edək və burda "**Floor_2**" wireless network'a aid məlumatları qeyd edək, Wi-Fi adi, authentification type və pre-shared-key (Şək.5.6);



Şəkil 5.6. Wi-Fi şəbəkəsinin qoşulması

Və bu konfiqurasiyanı edəndən sonra, smartphone'da "**Floor_2**" Wi-Fi network'a qoşuldu uğurlu şəkildə.

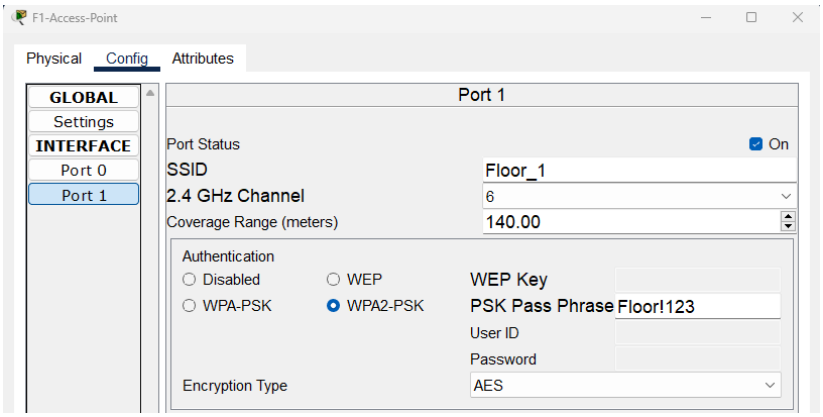
İndi sıra Tablet'i konfiqurasiya edərək "**Floor_2**" Wi-Fi şəbəkəsinə qoşmaqdır. Bunun üçün, "**Config**" bölməsində yerləşən "**Wireless0**" tab'a keçid edirik və "**Floor_2**" Wi-Fi şəbəkəsinə aid olan konfiqurasiyaları qeyd edirik (Şək.5.7). Aşağıdakı şəkildən görə bilərik ki, bütün device'lar uğurlu şəkildə "**F2-Access-Point**" üzərindən paylanan "**Floor_2**" Wi-Fi şəbəkəsinə uğurlu şəkildə qoşulubdur.



Şəkil 5.7. Wi-Fi şəbəkəsinə aid olan konfiqurasiyalar

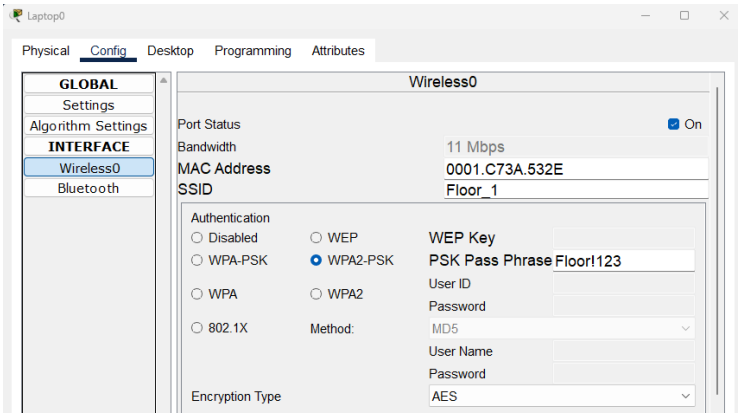
Floor 1: İndi sıra 1-ci mərtəbə üçün Wi-Fi şəbəkəsi yaratmaqdır. İlk növbədə bu mərtəbə üçün, 1 laptop, 1 smartphone və 1 tablet dizayn edək. Bunu etdikdən sonra, "**F1-Access-Point**"də "**Wi-Fi**" network yaradaq adını da "**Floor_1**" təyin edək, təhlükəsiz metod kimi WPA2-PSK seçək və Pre-shared-key olaraq isə "Floor!123" təyin edək.

Aşağıdakı şəkildə "F1-Access-Point" üzərində "Floor_1" görürük (Şək.5.8).



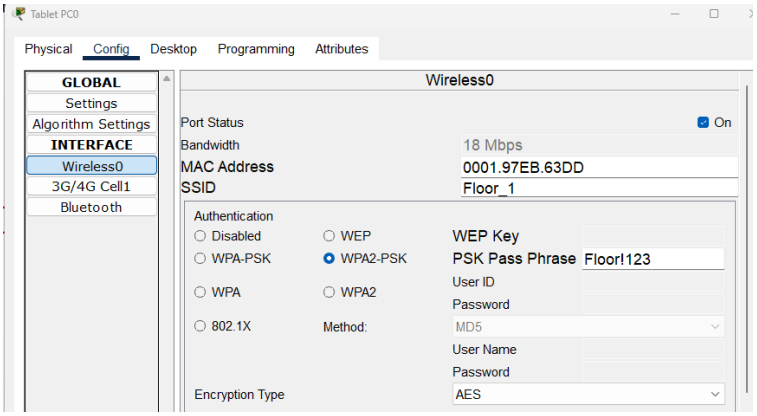
Şəkil 5.8. "F1-Access-Point" üzərində "Floor_1"

İndi laptop'dan başlayaraq bu cihazları həmin, "**Floor_1**" Wi-Fi şəbəkəsinə qoşaq; Əvvəlki kimi, ilk növbədə laptop'a wireless module əlavə edək (Şək.5.9).



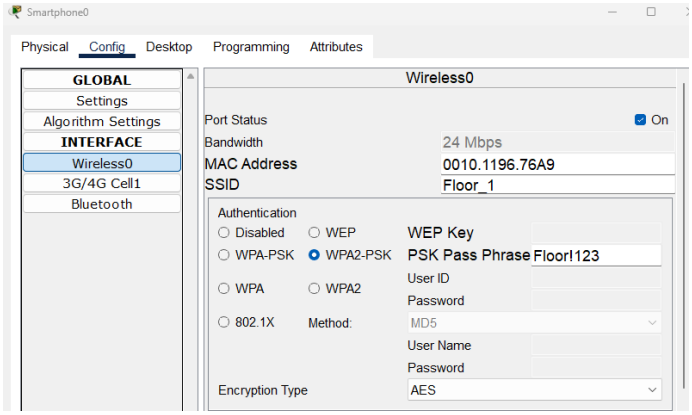
Şəkil 5.9. Laptop'a wireless module əlavə edilməsi

Tableti konfiqurasiya etməyə başlayaq (Şəkil 5.10.) indi də:



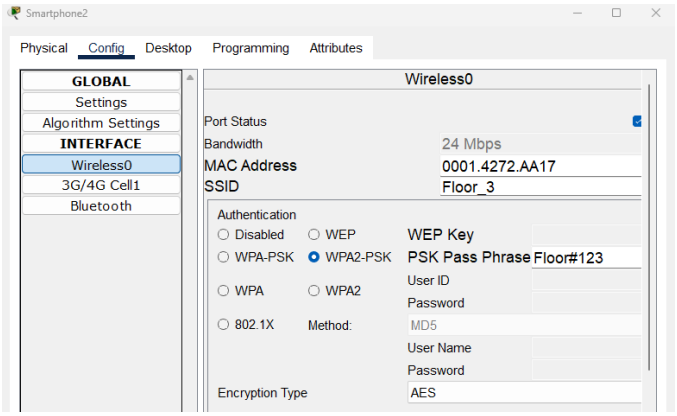
Şəkil 5.10. Tabletin konfiqurasiyası

Smartphone üçün (Şək.5.11):



Şəkil 5.11. Smartphone konfiqurasiyası

Floor 3: 3-cü mərtəbə üçün də eyni qayda da yerinə yetirək "Wi-Fi" şəbəkəsinin konfiqurasiyasını. Bu mərtəbədə bir dənə smartphone dizayn edək, "F3-Access-Point"də "Wi-Fi" network yaradandan sonra (Şək.5.12).



Şəkil 5.12. "F3-Access-Point"də "Wi-Fi" network yaradılması

5.2. Korporativ şirkətin şəbəkə infrastrukturunun "SSH" konfiqurasiyası

Router'lara uzaqdan təhlükəsiz şəkildə qoşulma üçün, onlarda "SSH" (Secure Shell - Təklükəsiz Shell) konfiqurasiyasını kökləməliyik ki, İT Vlan'dan biz Router'lara SSH ilə qoşula bilək, daha Router'lara qoşulma üçün, onlara directly yaxınlaşmayaq.

"**F1-Router"dan** Başlayaq SSH konfiqurasiya etməyə**:** İlk növbədə, router'ların hostname'ləri fərqli olmalıdır bir-birindən, yəni router'lar hostname'e malik olmalıdir, biz bunu onedən etmişdik Xatırlayırıqsa, hər bir router'a cavabdeh olduğu mərtəbəyə uyğun hostname təyin etmişdik. Bunu etdikdən sonra, SSH konfiqurasiyasını yerinə yetirmək üçün bizə "**domain name"** konfiqurasiyası lazımdır.

"**ip domain-name company"** – burda çox zaman domain-name kimi şirkətin adı istifadə olunur.

Domain-name'i konfiqurasiya etdikdən sonra biz "username & password" konfiqurasiya etməliyik qoşulma üçün.

"**username admin password root123"** username və password'u bu cür təyin edək;

Bunu da təyin etdikdən sonra, növbəti mərhələ crypto'nu generate etməkdir.

"**crypto key generate rsa"** – deyək, və **1024** bİTlik crypto key təyin edə bilərik

təhlükəsiz qoşulma üçün, yəni qoşulma zamanı yazacağımız username & password, daha sonra qoşulmadan sonra göndərilən bütün məlumatlar **1024** bitlik rsa ilə şifrələnərək göndəriləcək ki, bu da 3-cü şəxslərin bizim göndərdiyimiz məlumatları ələ keçirən zaman, həmin məlumatları oxumasının qarşısını alacaq, çünki göndərilən bütün məlumatlar şifrələnmiş şəkildə olur ki, həmin şifrələməni də açmaq üçün 3-cü şəxsdə həm public həm də private key olmalıdır ki, həmin key'ləri də 3-cü şəxsin ələ keçirməsi demək olar ki, çox çətindir.

Bunu da edəndən sonra, Növbəti mərhələ, **SSH'i** virtual interface'də aktivləşdirməkdir. Bunu etmək üçün:

"**line vty 0 15" –** bu o deməkdir ki, eyni zamanda bu router'a 16 virtual connection yarana bilər. Yəni məs, eyni anda 16 dənə virtual qoşulma imkanı yaradır router'a.

" **login local" –** bununla biz, yaratdığımız "username & password"un bu router'a qoşulmasına imkan yaradırıq.

"**transport input SSH" –** Bununla isə biz, bu yaratdığımız virtual qoşulmanı SSH'e çeviririk, çünki default olaraq yaradılan virtual connection "Telnet" üzərindən gedir, lakin "telnet" üzərindən məlumatlar açıq şəkildə gedir, yəni burda heç bir şifrələmə metodu tətbiq edilmir, bu səbəbdən 3-cü şəxslər həmin məlumatları ələ keçirsələr, məlumatları çox rahat şəkildə oxuya biləcəklər. Bu səbəbdən, biz ilk növbədə SSH köklədik router'da, daha sonra virtual əlaqəni yaradıb və yaratdığımız həmin virtual əlaqəni SSH'a transport etdik. Sonda da bu konfiqurasiyanı Router'in yaddaşına veririk (Şək.5.13).

```
F1-Router(config)#ip domain-name company
F1-Router(config)#username admin password root123
F1-Router(config)#crypto key generate rsa
The name for the keys will be: F1-Router.company
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

F1-Router(config)#line vty 0 15
*Mar 1 1:23:32.530: %SSH-5-ENABLED: SSH 1.99 has been enabled
F1-Router(config-line)#login local
F1-Router(config-line)#transport input SSH
F1-Router(config-line)#
```

Şəkil 5.13. "F1-Router" konfiqurasiyası

"**F2-Router**" – İndi isə, SSH'i 2-ci mərtəbəyə cavabdehlik daşıyan Router'da konfiqurasiya etməyə başlayaq (Şək.5.14).

```
F2-Router(config)#ip domain-name company
F2-Router(config)#username admin password root123
F2-Router(config)#crypto key generate rsa
The name for the keys will be: F2-Router.company
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

F2-Router(config)#line vty 0 15
*Mar 1 1:26:2.648: %SSH-5-ENABLED: SSH 1.99 has been enabled
F2-Router(config-line)#login local
F2-Router(config-line)#transport input ssh
F2-Router(config-line)#
```

Şəkil 5.14. "F2-Router" konfiqurasiyası

"**F3-Router"** – sonda, SSH konfiqurasiyasini 3-cü mərtəbəyə cavabdehlik daşıyan router'da etməyə başlayaq (Şək.5.15).

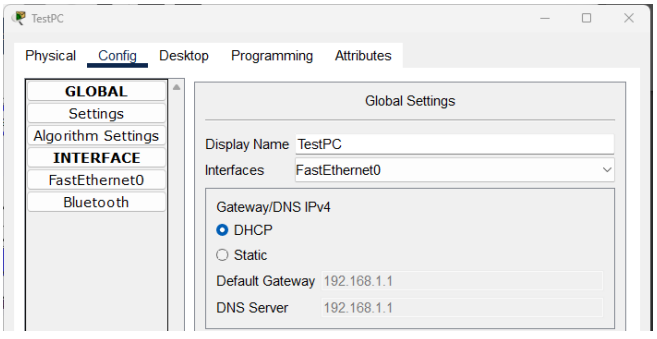
```
F3-Router(config)#ip domain-name company
F3-Router(config)#username admin password root123
F3-Router(config)#crypto key generate rsa
The name for the keys will be: F3-Router.company
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

F3-Router(config)#line vty 0 15
*Mar 1 1:28:15.737: %SSH-5-ENABLED: SSH 1.99 has been enabled
F3-Router(config-line)#login local
F3-Router(config-line)#transport input ssh
F3-Router(config-line)#
```

Şəkil 5.15. "F3-Router" konfiqurasiyası

SSH konfiqurasiyani uğurla yerinə yetirdik. Bizə verilən 12-ci tapşırıqda deyilirdi ki, "İT departamentində Test-PC adlı PC-ni fa0/2 portuna əlavə etməli və uzaqdan girişi (SSH) yoxlamaq üçün ondan istifadə edilməlidir." Bizim şəbəkə dizaynımızda bu artıq hazırdır. "İT" departament'də həmin PC'ni switch'in fa0/2 portuna qoşmuşuq. Sadəce PC'nin "**config**" panel'ə daxil olaraq, orda display name olaraq "**Test-PC**" edək ilk növbədə (Şək.5.16).



Şəkil 5.16. Test-PC konfiqurasiya

İndi isə, bu Test-PC'dən SSH ilə router'lara uzaqdan qoşulmanı yoxlayaq, görək həqiqətən işləyirmi.

Cihazların Təhlükəsizlyi: Amma bunu etməmişdən öncə ilk növbədə gəlin, bütün router'larda "**console mode (directly qoşulma, console cable vasitəsilə**)" və "**Privileged Mode**"a password təyin edək, yəni **console connection**'a keçmək üçün bizdən password tələb etsin və əlavə olaraq **privileged mode'a** keçmək üçün bizdən əlavə password tələb etsin, bu şəbəkənin təhlükəsizliyi üçün vacib məsələlərdən biridir: Başlayaq "**F2-Router"**dan, içərisinə daxil olaq:

1. Birinci "**Console mode**"-a **username & password** təyin edək. Bunun üçün:

"line console 0" – ona görə "line console 0" yazırıq ki, cihazda cəmi 1 ədəd console port mövcuddur, əgər 2 dənə console port olsaydı, o zaman "line console 0 1" yazacaqdıq, amma belə şey mümkün deyil, switch və router'larda cəmi 1 ədəd console port olur, directly qoşulma üçün.

"login local" – yaradacağımız username&password'u əvvəlcədən bura təyin edirik ki, yalnız həmin username&password'la cihaza daxil olmaq mümkün olsun.

"exit"

"username admin password cisco" command'lardan istifadə edək (Şək.5.17).

```
F2-Router(config)#
F2-Router(config)#
F2-Router(config)#line console 0
F2-Router(config-line)#login local
F2-Router(config-line)#exit
F2-Router(config)#username admin password cisco
F2-Router(config)#
```

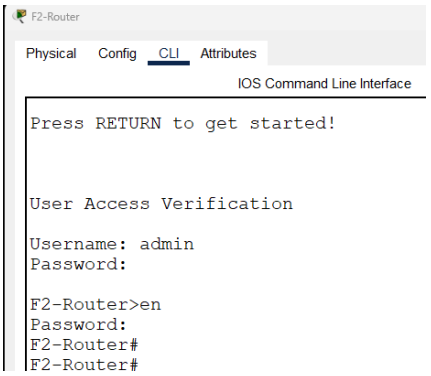
Şəkil 5.17. "username admin password cisco" komandası

2. "**Privileged Mode" –** İndi isə, privilege mode üçün username & password təyin edək, bunu isə onun üçün edirik ki, kimsə console giriş üçün username password'u əldə edib cihaza daxil olsa belə "privileged mode" üçün təyin olunan username & password'u bilmədiyi üçün cihazda heç nə edə bilməyəcək. Onu təyin etmək üçün:

"**enable password cisco" –** bu əmrlə, "privileged mode" üçün cisco password'un təyin edirik;

İndi yoxlayaq görək işləyirmi (Şək.5.18): gördüyümüz kimi, cihaza daxil olanda bizdən ilk növbədə "**Console mode**" üçün təyin etdiyimiz **username& password**'u istədi çünki, **console connection** ilə daxil oluruq cihaza, **həmin username &**

password'u daxil etdikdən sonra cihaza daxil olduq, amma daha sonra "**privileged mode**"a keçmək istəyəndə bizdən "**privileged mode**" üçün təyin etdiyimiz **password'u** istəyir, onu da daxil etdikdən sonra, biz **privilege mode'a** uğurla keçə bilirik.



Şəkil 5.18. "privileged mode" üçün cisco password'un yoxlanması

Amma bu etdiyimiz konfiqurasiyanın bir mənfi tərəfi var ki, yazdığımız username & password'ların heç biri şifrələnmir, yəni açıq şəkildə cihazın yaddaşında saxlanılır, bunu görə bilməyimiz üçün: "**sh running config | include password"** command'dan istifadə edə bilərik (Şək.5.19): görürük ki, bütün təyin etdiyimiz **username & password**'lar görünür. Bunun səbəbi odur ki, "**service password-encryption"**u aktivləşdirməmişik.

```
F2-Router#
F2-Router#sh run
F2-Router#sh running-config | include password
no service password-encryption
enable password cisco
username admin password 0 cisco
F2-Router#
```

Şəkil 5.19. "sh running config | include password"

Gəlin indi onu da aktivləşdirib daha sonra yoxlayaq, aktivləşdirmək üçün "**service password-encryption"** command'dan istifadə edə bilərik (Şək.5.20). Artıq, password encryption service'in aktivləşdirəndən sonra, görürük ki, təyin etdiyimiz password'lar sifrələnib, default olaraq "**MD5**" şifrələmə metodu ilə şifrələnir, bunu da dəyişib daha güclü olan **sha256** və.s istifadə edə bilərik hətta. Bunu etmək üçün, "**enable algoritm-type sha256 secret password"** command'dan istifadə edə bilərik.

```
F2-Router#sh run
F2-Router#sh running-config | include password
service password-encryption
enable password 7 0822455D0A16
username admin password 7 0822455D0A16
F2-Router#
```

Şəkil 5.20. "service password-encryption"

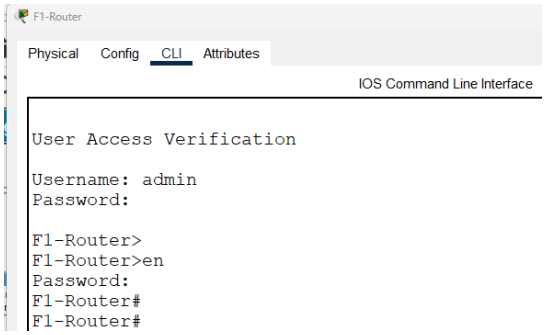
Əgər istəyiriksə "**privilege mode**" üçün birbaşa yazdığımız password şifrələnsin, birdə sonradan "**service password-encryption"** command'ın yazmayaq, bunun üçün username & password təyin edən zaman, "**password"** command əvəzinə "**secret"** command istifadə etməliyik. Digər cihazlarda da bu əməliyyatları yerinə yetirək.

- "**F1-Router"** (Şək.5.21)

```
F1-Router(config)#line con 0
F1-Router(config-line)#login local
F1-Router(config-line)#exit
F1-Router(config)#username admin password cisco
F1-Router(config)#
F1-Router(config)#enable secret cisco
F1-Router(config)#serv
F1-Router(config)#service p
F1-Router(config)#service password-encryption
F1-Router(config)#
F1-Router(config)#do wr
Building configuration...
[OK]
```

Şəkil 5.21. "F1-Roter" "secret" komandası

İşləməyini yoxlayaq (Şək.5.22):



Şəkil 5.22. "F1-Roter" "secret" komandası yoxlamaq

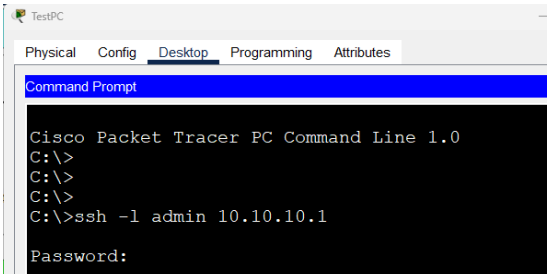
Digər cihazlarda da etdiyimiz eyni konfiqurasiyaları yerinə yetirək. Bütün switch və router'larda təhlükəsizlik konfiqurasiyalarını bitirdik.

İndi **SSH** qoşulmanı yoxlaya bilərik:

Bunu etmək üçün "Test-PC"də "**Command Prompt (CMD**)" bölməsinə keçid edək. Bura daxil olandan sonra isə:

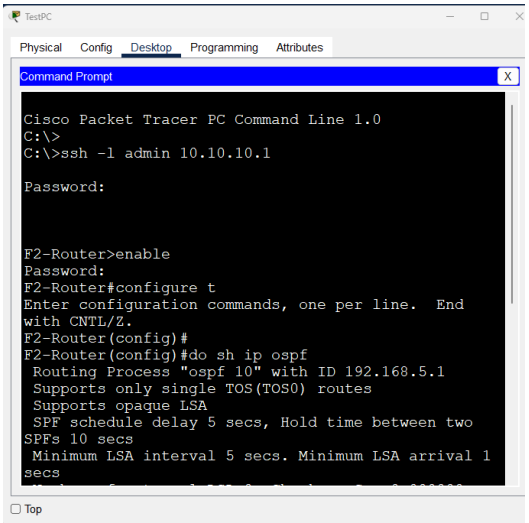
"**ssh -l username destination IP address" –** yəni, username hissəsinə router'da yaratdığımız "admin" username'in yazacayıq, destination IP address yerinə isə

qoşulacağımız avadanlığın IP ünvanını qeyd edəcəyik. İndi, biz istəyirik ki, bu Test-PC'dən 2-ci mərtəbəyə cavabdehlik daşıyan **"F2-Router"**a qoşulaq. İndi sual yarana bilər ki, biz həmin router'ın hansı interface'nə qoşulaq onun axı 5 dənə fərqli interface'i (2'li real interface, yerdə qalan 3'ü isə virtual interface'dir) var. Bu sualım cavabı bizim şəbəkə dizaynımızda belədir ki, fərqi yoxdur hər 5 interface'nə SSH üzərindən qoşularaq bu router'i idarə edə bilərik, çünki biz şəbəkəmizdə InterVlan Routing və OSPF konfiqurasiya etdiyimizdən fərqli Vlan'da olan subnetdən başqa router'in cavabdehlik daşıdığı fərqli Vlan'a connection yarada bilərik. Bunun səbəbi şəbəkəmizdə həm InterVlan Routing həm də OSPF'i uğurlu şəkildə köklədiyimizə görədir. Yoxlayaq bunu (Şək.5.23):



Şəkil 5.23. OSPF'i uğurlu şəkildə köklənməsinin yoxlanması

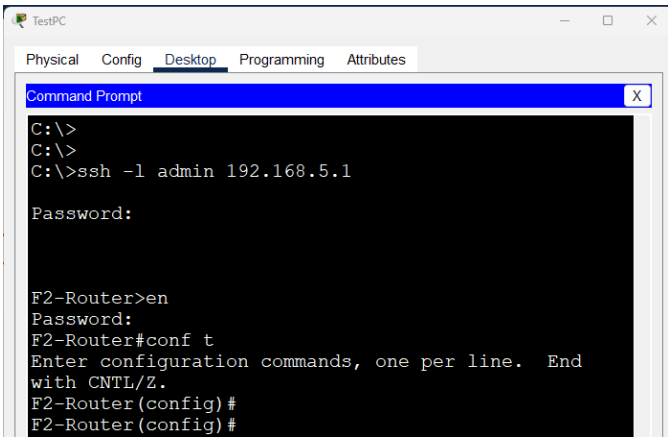
Görürük ki, qoşulma oldu və bizdən password istəyir, bu password bizim user-name&password yaradan zaman, təyin etdiyimiz password'dur, bu password'u da yazaq, bu password'u yazanda görünmür, çünki qoşulma secret şəkildədir;



Şəkil 5.24. "F2-Router'ın içərisinə daxil olunması

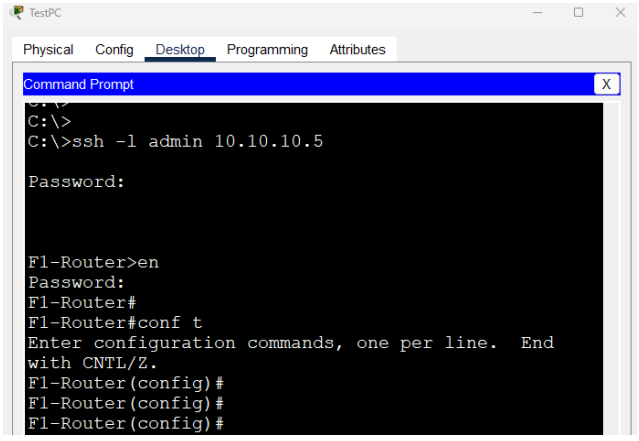
Yuxarıdakı şəkildən görürük ki, "F2-Router'ın içərisinə uğurla daxil olduq

(Şək.5.24), daha sonra “privileged mode”a keçmək üçün də təyin etdiyimiz password’u yazdıq və uğurla içərisinə keçdik. İndi gəlin test olaraq, “F2-Router”in içərisinə yaratdığımız virtual interface üzərindən qoşulmanı yoxlayaq, əlbəttə ki, bu da uğurla olacaq: Bəli həqiqətən də SSH ilə “F2-Router’a virtual interface üzərindən qoşulma uğurlu oldu (Şək.5.25).



Şəkil 5.25. “F2-Router’a virtual interface üzərində qoşulma

“**F1-Router”** – İT Vlan’da olan “Test-PC”dən SSH vasistəsi ilə “**F1-Router”**a qoşulmağa cəhd edək: gördüyümüz kimi burda da connection uğurlu oldu (Şək.5.26).



Şəkil 5.26. SSH vasitəsi ilə “F1-Router”a qoşulma

Keçək ən sonuncu həll etməyə: “Yalnız Test-PC-nin fa0/2 portuna daxil olmasına icazə vərmək üçün port təhlükəsizliyini İT dəpartamentində switch üçün konfiqurasiya edilməlidir (bağlanma rejiminin pozulması ilə mac-ünvanı əldə etmək üçün **sticky-mac address** üsulundan istifadə edilməlidir).”

Yəni, switch’in fa 0/2 portune İT Vlan’a məxsus olan Test-PC’dən başqa device qoşulsa həmin port avtomatik sönsün, işləməsin. Bunu da stick-mac address

texnologiyasi ilə yerinə yetirəcəyik. Ümumiyyətlə, bu üsul MAC address hesabına baş vərir, belə ki, "Test-PC" cihazının mac-address'i həmin porta tanıdılacaq və fa 0/2 portuna həmin mac address'dən fərqli mac address'li cihaz qoşulan kimi port avtomatik sönəcək. Bunun səbəbi odur ki, mac address'lər unikal olurlar.

"**F3-Switch"ə** daxil olaq bunu konfiqurasiya etmək üçün və bu commandları yazaq:

"**interface fa0/2** " – command ilə, fa 0/2 interface'nə daxil olaq;

"**switchport port-security**" – bu command ilə, port security'ni aktivləşdiririk bu interface'də;

"**switchport port-security maximum 1**" – bu command'da, deyirik ki, maximum 1 device üçün port-security işləsin.

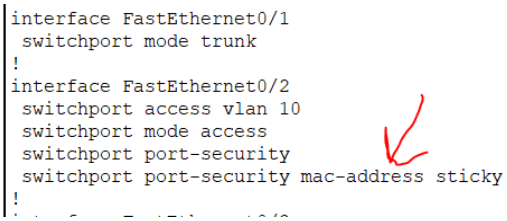
"**switchport port-security mac-adress sticky**" – bu command'la, daha biz "Test-PC" device'in mac address'in manual olaraq əlimizlə yazmırıq, deyirik ki, hal-hazırda porta qoşulu olan cihazın mac-address'in özünə yapışdır, onu özündə qeyd et.

"**switchport port-security violation shutdown**" – bu command'la deyirik ki, əgər sən özündə qeyd etdiyin mac-address'dən fərqli mac-address'li cihaz bu porta qoşularsa, o zaman portu avtomatik söndür, disable et (Şək.5.27).

```
F3-Switch(config)#int fa 0/2
F3-Switch(config-if)#switchport port-security
F3-Switch(config-if)#sw
F3-Switch(config-if)#switchport p
F3-Switch(config-if)#switchport port
F3-Switch(config-if)#switchport port-security ma
F3-Switch(config-if)#switchport port-security maxo
F3-Switch(config-if)#switchport port-security maxi
F3-Switch(config-if)#switchport port-security maximum 1
F3-Switch(config-if)#switch
F3-Switch(config-if)#switchport p
F3-Switch(config-if)#switchport po
F3-Switch(config-if)#switchport port-security ma
F3-Switch(config-if)#switchport port-security mac
F3-Switch(config-if)#switchport port-security mac-address s
F3-Switch(config-if)#switchport port-security mac-address sticky
F3-Switch(config-if)#sw
F3-Switch(config-if)#switchport por
F3-Switch(config-if)#switchport port-security via
F3-Switch(config-if)#switchport port-security vio
F3-Switch(config-if)#switchport port-security violation sh
F3-Switch(config-if)#switchport port-security violation shutdown
F3-Switch(config-if)#
```

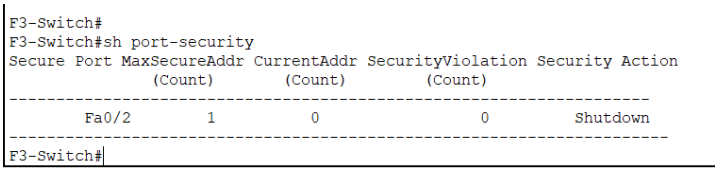
Şəkil 5.27. "switchport port-security violation shutdown"

İndi həqiqətən "port-security"nin bu interface'də işlədiyini sübut etmək üçün, "**sh start**" commandın yazaq və konfiqurasiyamıza baxaq: görürük ki, həqiqətən də fa 0/2'də sticky mac-address aktivdir (Şək.5.28);



Şəkil 5.28. "sh start"

"**sh port-security"** kamandasını da yoxlayaq: Bəli fa 0/2 interface'də port-securityinin həqiqətən də aktiv olduğunu görürük (Şək.5.29):



Şəkil 5.29. "sh port-security"

Bununla da biz, bütün tapşırıqları uğurla yerinə yetirmiş olduq və etdiyimiz bütün dizayn, konfiqurasiyaları, kökləmələri bir-bir test'dən keçirib, analiz edib həqiqətən də uğurla işlədiyini sübut etdik.

NƏTİCƏ

Disertasiyanı reallaşdırmaq üçün mövcud uyğun sistemlər araşdırılmış və qarşıya qoyulan məqsədi reallaşdırmaq üçün aşağıdakı işlər görülmüşdür.

- Cisco Packet Tracer şəbəkə modelləməsi;
- Real mühitdə şəbəkə modelinin analizi;
- Şəbəkə topologiyalarında informasiya mübadiləsi protokolunun qarşılaşdırılması;
- Firewall texnologiyaları və onların şəbəkələrin xarici təhlükələrdən qorunmasında effektivliyi;
- Hücumun aşkarlanması və qarşısının alınması sistemləri və onların şəbəkə təhlükəsizliyində rolu;
- Şəbəkənin seqmentasiyası və potensial təhlükəsizlik pozuntusunun təsirinin azaldılmasında əhəmiyyəti;
- Girişə nəzarət mexanizmləri və onların şəbəkə resurslarına icazəli girişin təmin olunmasında rolu;
- Məlumat mərkəzləri, server otaqları və şəbəkə şkafları kimi şəbəkə infrastrukturu üçün fiziki təhlükəsizlik tədbirləri;
- Korporativ şirkətin şəbəkə infrastrukturunun layihələndirilməsi;
- Korporativ şirkətin şəbəkə infrastrukturunun simulyasiyası;
- Korporativ şirkətin şəbəkə infrastrukturunun IP ünvanlarının analizi;
- Korporativ şirkətin şəbəkə infrastrukturunun DHCP severinin iş rejimlərinin təhlili;
- Korporativ şirkətin şəbəkə infrastrukturunun Wi-Fi network konfiqurasiyası;
- Korporativ şirkətin şəbəkə infrastrukturunun “SSH” konfiqurasiyası.

Nəticədə yaradılan simulyasiya ilkin sınaq yoxlamadan keçirilmişdir.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT

1. Jahanirad, M., and Nabhani, Y., and Md.Noor, R., 2012, Comphensive Network Security Approach: Security Breachs at Retail Compans – A Case Study, *IJCSNS*, 12 (8), 107-112.

2. Janitor, J., and Jakab, F., and Kniewald, K., 2010, Visual Learning Tools for Teaching / Learning Computer Networks, *6th International Conference on Networking and Services* (ICNS), 7-13 March 2010 Cancun, IEEE, IEEE, 978-1-4244-5927-8, 351-355.

3. Frezzo, D.C., and Behrens, J. T., and Mislevy, R. J., 2010, Design Patterns for Learningand Assessment: Facilitating the Introduction of a Complex Simulation-Based Learning Environment into a Community of Instructors, *Journal of Science Education and Technology*, 19 (2), 105-114.

4. Bursac, M., Pantic, M., 2011, The Application of Network Simulators and Their Significance in Educating and Enabling Students to Apply them in Solving Traffic and Transport Problems, *MTCAJ*, 0626, 20-26.

5. Jesin, A., 2014, *Packet Tracer Network Simulator*, Pack Publishing Ltd., Birmingham, ISBN: 978-1-78217-042-6.

6. Oppenheimer. P., 2011, *Top-Down Network Desing*, 3rd ed., Cisco Systems, Inc., Indianapolis, ISBN: 978-1-58720-283-4.

7. Nazumudeen, N., and Mahendran, C., 2014, Performance Analysis of Dynamic Routing Protocols Using Packet Tracer, *IJIRSET*, 3 (1), 570-574.

8. "Firewalls and Internet Security: Repelling the Wily Hacker" by William R. Cheswick and Steven M. Bellovin

9. "Firewall Design and Analysis" by Doug Barth and Jennifer L. Whitson

10. "Firewalls: Jumpstart for Network and Systems Administrators" by Robert L. Ziegler