AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

KAMİL ZEYNALOV NADİR

"Korporativ şəbəkələrin proqram konfiqurasiyasının idarə olunması"

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: 060509- "Kompüter elmləri"

İxtisaslaşma: "İdarəetmənin informasiya texnologiyalar"

Elmi rəhbər:
f.r.e.n.,dos. A.X.ABDULLAYEV

Magistr proqramının rəhbəri:
akad. Ə.M.ABBASOV

Kafedra müdiri: akad. Ə.M.ABBASOV

BAKI – 2019

MÜNDƏRİCAT

GİRİŞ

Mövzunun aktuallığı. Korporasiya termini latıncada “corporatio” sözündən götürülmüş və “birlik” anlamı daşıyır.Korporativ şəbəkə anlamı da müəyyən birliklər,idarə və müəssisələrin informasiya paylaşımı etməsi üçün formalaşdırılmış mürəkkəb strukturlardır.Şəbəkə formalaşdırılarkən əsas olan yüksək əlçatalığın təmini,informasiyanın təhlükəsiz paylaşımının təmini və performansın mümkün olduğu qədər yüksəldilməsidir.Günümüzdə istənilən profilə malik şirkət üçün onun kompüter şəbəkəsinin əhəmiyyəti çox önəmlidir.Çünki hazırda elektron sistemlər idarəetmənin mərkəzləşdirilməsi,ümumi resurslara çıxışı və bu kimi önəmli məsələləri özündə cəmləyir.

Tədqiqatın əsas məqsədi və vəzifələri. Biz şəbəkələrin məlumat mübadiləsi üçün istifadə etdiyini qeyd etdik. Amma əsl səbəblər nədir ?

Təşkilatların şəbəkələrə ehtiyacı varmı?

Bu səbəblər iki kateqoriyaya bölünə bilər:

• Paylaşma: Şəbəkələr faylların, məlumat bazalarının və mediyanın paylaşılmasına icazə verir.

• Əlaqə: Şəbəkələr e-poçt, mesajlaşma və faks imkanları üçün vacibdir.

Aralarında elektrik əlaqələri olan müstəqil kompüterlər qrupu kompüter şəbəkəsi adlanır. Burada kompüterlər bir-birinə bağlıdır, onlar aralarında məlumat mübadiləsi edə biləcəklər. Bu gün geniş istifadə olunan kompüter şəbəkələri böyük kompüter sistemləri ilə müqayisədə xərc, etibarlılıq baxımından üstünlük təşkil edir, həm də şirkətlər üçün resurs paylaşma, kommunikasiya mühiti və e-ticarət təmin edir.Şəxsi istifadəçilər üçün uzaqdakı məlumatları əlçatan etməklə yanaşı, ünsiyyətə və interaktiv əyləncələrə çıxışı təmin edir.

Tədqiqatın informasiya bazası və işlənməsi metodları. Kompüter şəbəkələri istifadə olunan ötürülmə texnologiyalarına əsasən yayımlanan şəbəkələr

(LAN, MAN və peyk şəbəkələri) və nöqtə-nöqtəyə şəbəkələr (WAN və əlaqəli şəbəkələr) olaraq iki kateqoriyaya bölünür. Digər tərəfdən, fiziki ölçülərinə görə, onlar LAN, MAN, WAN və əlaqəli şəbəkələr kimi dörd sinifə bölünə bilər. LAN'larda üç növ əlaqə istifadə olunur: ümumi yol, üzük və ulduz. WAN-da ulduz, üzük, ağac, tam əlaqə, kəsici üzüklər və qeyri-müntəzəm əlaqə növləri istifadə edilə bilər. Yayım şəbəkələrində ən vacib məsələ, çox sayda istifadəçinin vahid ötürülmə vasitəsinə çıxışının olması və onların məlumatlarını itkisiz göndərməsidir.İstifadəçinin ötürülmə kanalına çıxışı MAC protokolu ilə təmin edilir. WAN'lar alt şəbəkələr və şəbəkə kompüterlərindən ibarətdir. Subnet marşruzatorlarından isə onları bir-birlərinə bağlayan ötürmə xəttlərini birləşdirmək üçün istifadə olunur. Şəbəkə dizaynının mürəkkəbliyini azaltmaq üçün şəbəkə arxitekturası laylı bir strukturda nəzərdə tutulmuşdur.Şəbəkələrinin qarşılıqlı əlaqəsini müəyyən edən qaydalara protokollar deyilir. Şəbəkə yaradan təbəqələr və istifadə etdiyimiz protokollar şəbəkə quruluşunu təyin edir. Eyni kompüterin iki bitişik qatın arasındakı hissə interfeysi adlanır. İki qonşu qat arasında xidmət mübadiləsi xidmət vasitələri tərəfindən icra edilir. Şəbəkə strukturunu təyin edən iki model var: OSI istinad modeli və TCP / IP modeli. OSI ISO tərəfindən hazırlanmış və İTU tərəfindən təsdiq edilmişdir; TCP / IP modeli, standart bir tətbiq modeli olaraq yayımlanmadı və ARPANET protokol quruluşunun araşdırılması nəticəsində əldə edildi. Bir rabitə sisteminin məqsədi, resursları bir nöqtədən digərinə məlumatı çatmağı nəzərdə tutur. İnformasiya analog və ya rəqəmsal siqnala çevrildikdən sonra analog və ya rəqəmsal kommunikasiya sistemləri vasitəsilə ötürülür. Analoq ünsiyyət vəziyyətində, siqnalın bant genişliyi sistemin bant genişliyindən artıq olmamalıdır, rəqəmsal ünsiyyətdə isə siqnalın ötürmə sürəti sistemin kanal tutumundan artıq olmamalıdır. Müəyyən bir sayda kompüter və müəyyən bir sahədə yaradılan şəbəkə növü LAN adlanır.LAN şəbəkələri (yerli şəbəkə) kompüter, şəbəkə interfeysi kartı, şəbəkə kabelləri, şəbəkə trafiki nəzarətçiləri və digər ətraf mühit cihazlarından ibarətdir. Şəbəkə istifadəçilərinin sayının artması və şəbəkənin böyüməsi baxımından şəbəkənin

genişləndirilməsi nəticəsində yaranan növ geniş sahə şəbəkəsi(WAN) adlanır. Geniş sahə şəbəkələri müxtəlif bölgələrdə kompüter və ya serverləri olan yerli şəbəkələrin birləşməsini təşkil edir.Şəbəkələr arasında əlaqə fiber optik kabellər və ya peyklər vasitəsilə edilə bilər.

Tədqiqatın elmi yeniliyi. Bu dissertasiya işində təkcə korportiv şəbəkənin formalaşdırılması və məlumat mübadiləsinin təmini yox,həmçinin bu mübadilənin tam təhlükəsiz aparılması üçün zəruri olan metodlardan necə istifadə edilməsi haqda da gediş bəhs olunub.

Tədqiqatın praktiki əhəmiyyəti. Hazırda istifadə olunan şəbəkə modelləri üzərində incələmələr aparılaraq onların ən uyğun tərəflərindən cari işdə geniş istifadə olunub.Ona görə də bu model tətbiq edilərsə çox effektiv nəticə əldə oluna bilər.

Dissertasiya işinin strukturu. Dissertasiya işi giriş, 3 fəsil, hər fəsil üzrə alt başlıqlar, nəticə və istifadə olunmuş ədəbiyyat hissələrindən ibarətdir.

I Fəsil.Korporativ şəbəkələrin proqram konfiqurasiyasının idarə olunması problemləri.

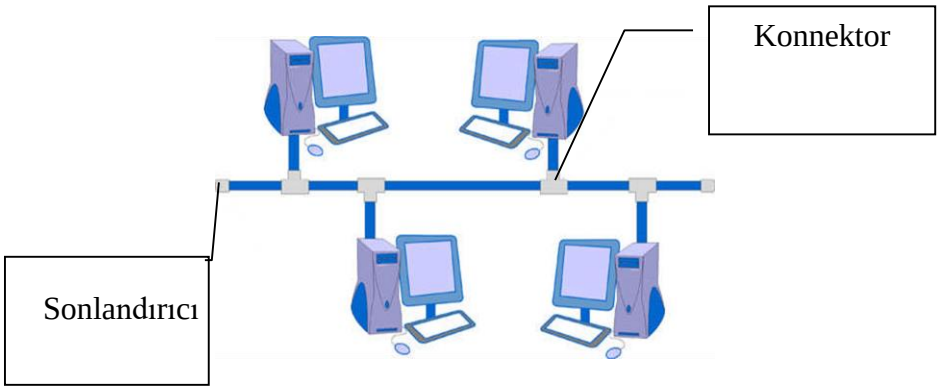
1.1 Korporativ şəbəkələrinin struktur quruluş modelləri - Topoloji modellər

Topologiya, kompüterlər bir-birinə necə bağlanıldığını müəyyən edən ümumi bir termindir.Aşağıdakı topologi stukturlar var:

- Bus topologiyası
- Ulduz topologiyası
- Ağac topologiyası
- Halqa topologiyası

Bus topologiyası

Bütün terminallar bir kabel xətti ilə əlaqələndirilir. Burada göndərilən siqnal bütün terminallardan keçir. Siqnal bir hədəfə çatana və ya bir sonlandırıcıya çatana qədər səyahət edir. Xəttin məlumat axını iki yönlüdür.Məlumat hər iki istiqamətdə ötürülür,ancaq birdən artıq istifadəçi eyni zamanda məlumat göndərsə bu paket mübadiləsi ləngiləmələrlə müşayət olunur. Bunun qarşısını almaq üçün, şəbəkə mübadiləsini tənzimləyən şəbəkə protokollarından istifadə edilməlidir.



Şəkil 1.0: Yol (Bus) topologiyası

Üstünlükləri;

• Ucuzdur və asan qurulur.

• Kabel quruluşu təhlükəsizdir.

• Heç bir mərkəzi vahid tələb olunmur.

Çatışmazlıqları;

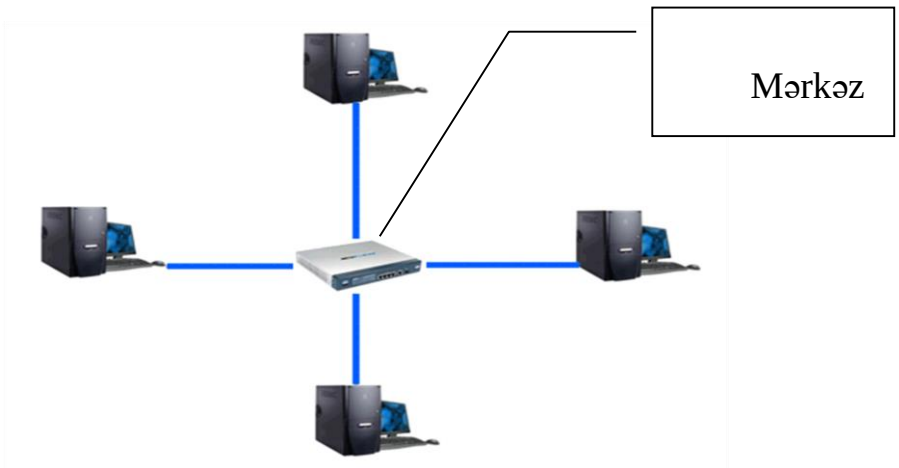
• Ən böyük çatışmazlığı odur ki, stansiyada olan səhv (əlaqəsizlik, söndürmə, qısa dövrə və s.) bütün sistemə təsir göstərir.

• Problem aşkarlanması çətindir.

• 30-a qədər stansiya bağlana bilər.

Ulduz topologiyası;

Ən çox istifadə olunan topoloji tipdir. Bu topologiyada hər bir kompüter şəbəkə ünsiyyətinin həyata keçirilməsi üçün mərkəz vahidi (keçid, mərkəz, və s.) adlandırdığımız qurğulara bağlıdır. Əslində, göndərilən siqnal ilk təyinat istiqamətinə yönəldilən mərkəzi birliyə çatır.



Şəkil 1.2:Ulduz (Star) topologiyası

Üstünlükləri;

• Stansiyanın olmaması şəbəkəyə təsir göstərmir.

• Şəbəkəyə yeni bir stansiya əlavə etmək asandır.

• Problem aşkarlanması asandır.

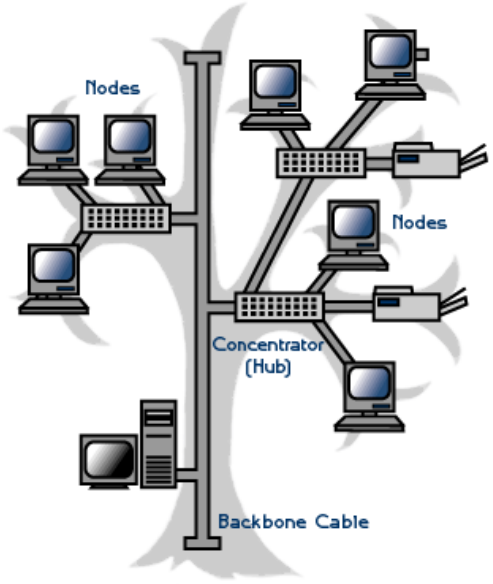
Çatışmazlıqları;

• Mərkəzi vahidin olmaması bütün sistemə təsir göstərir.

• Digər topologiyalara nisbətən bahalıdır, çünki çox sayda kabellər istifadə olunur.

Ağac topologiyası;

Tez-tez ulduz topologiyasında şəbəkələri birləşdirmək üçün istifadə olunur. Beləliklə, şəbəkələr genişləndirilə bilər. Ağacın filialları müxtəlif topologiyalarda şəbəkələri təmsil edir və ağacın daxilinə aid ola bilərlər.

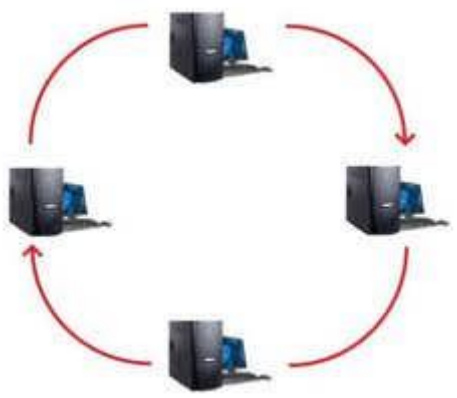


Şəkil 1.3: Ağac (Tree) topologiyası

Halqa topologiyası;

Bu, bütün qovşaqların məntiqi bir dairə kimi birləşdiyi bir növ topologiyadı. Hətta göndərilən siqnal hədəflərə çatana qədər bütün terminallara çatır və hər

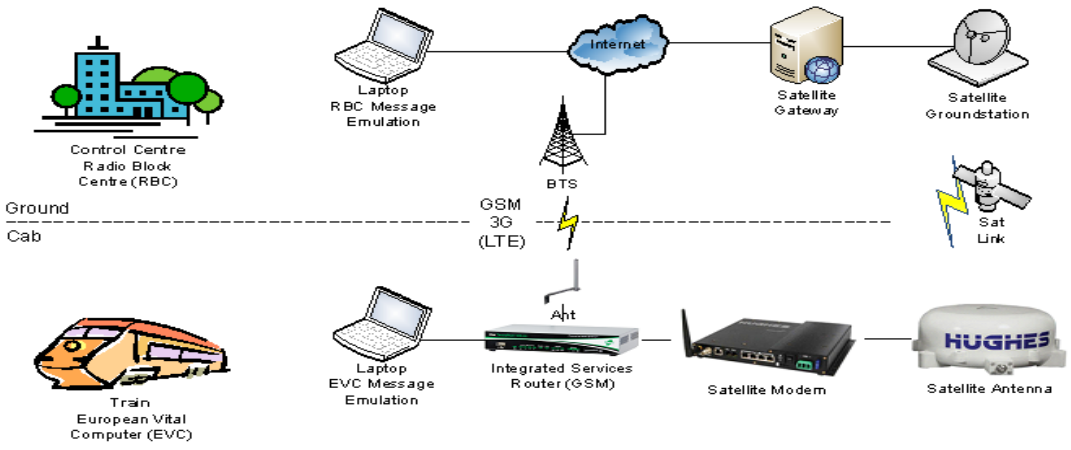
terminalı məlumatı özünnən sonrakına göndərir. Bu topologiyanın ən əhəmiyyətli çatışmazlığı, hər hansı bir qovşaqda və ya kabel ilə bağlı bir problemin bütün sistemə təsir etməsidir.



Şəkil 1.4: Halqa topologiyası

1.2 Şəbəkələrin tipləri

Şəbəkə əlaqə növləri simli və simsiz olmaqla 2 yerə bölünür. Kabel bağlantısı şəbəkə cihazlarının kabel ilə bir-birinə bağlı olduğu quruluşdur. Kabel bağlantısındaki kabel uzunluğunun artırılması kommunikasiya işinə mənfi təsir göstərir.



Şəkil 1.5 Simli şəbəkələr

Simsiz bağlantı simli kommunikasiyaya alternativ olaraq RF (Radio Frequency) texnologiyasından istifadə edərək havada informasiya mübadiləsi aparan çevik bir ünsiyyət formasıdır. Bununla əlaqədar, şəbəkə cihazları

(kompüterlər, printerlər, kameralar və s.) simsiz qurğular (Wireless Bridge) və avadanlıqlarla bir-birinə bağlıdır.

Şəkil 1.6 simsiz şəbəkələr

Şəbəkə, paylaşma məqsədləri üçün iki və ya daha çox cihazı birləşdirərək yaradılmış bir quruluşdur.Bu, yüzlərlə iş yeri və ya fərdi kompüterdən və ya bir-birinə bağlı iki kompüterdən ibarət ola bilər. Bu şəbəkələr istifadə sahələrinə görə təsnif edilir.

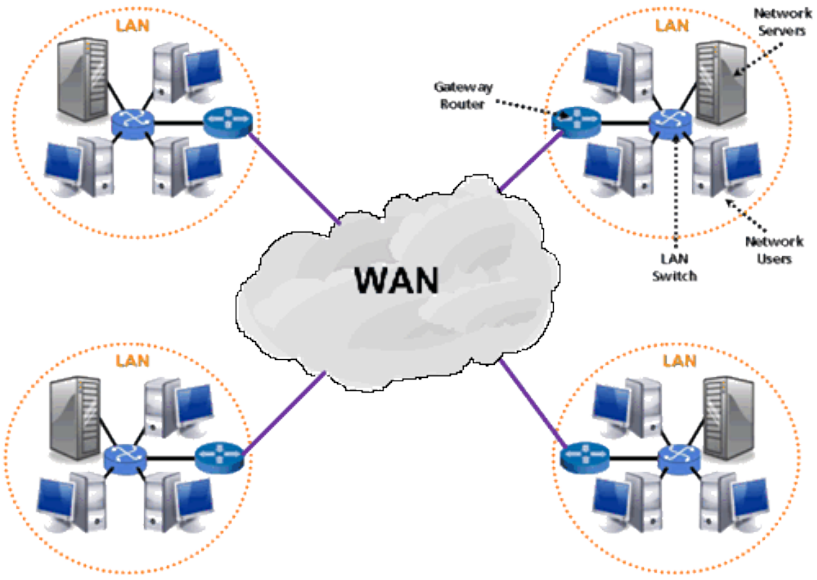
Yerli Şəbəkələr (LAN)

Müəyyən bir sayda kompüterlərdən təşkil edilmiş və müəyyən bir sahədə yaradılan şəbəkə növüdür. Yerli şəbəkələr kompüter, şəbəkə interfeysi kartları, şəbəkə kabellərindən, şəbəkə trafiki nəzarətçilərindən və digər periferik cihazlardan ibarətdir. Bir ofisdə və ya binada işləyən printer, fayl və proqram paylaşma kimi işləri lokal şəbəkələrdə asanlıqla və effektiv şəkildə həyata keçirə bilərik.

Şəkil 1.7 LAN

Geniş sahə şəbəkəsi (WAN)

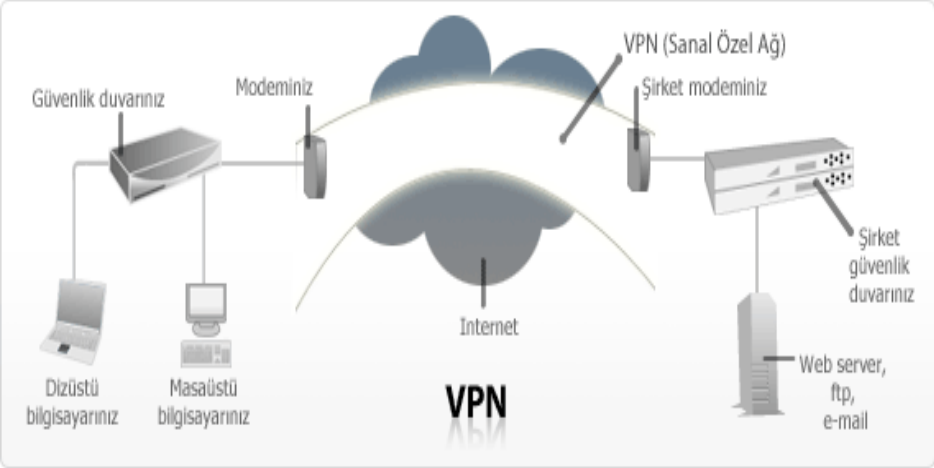
Şəbəkə istifadəçilərinin sayının artması və şəbəkə baxımından şəbəkənin genişləndirilməsi nəticəsində yaranan şəbəkə növü geniş sahə şəbəkəsi adlanır.



Şəkil 1.8 WAN

Şəxsi virtual şəbəkələr (VPN)

İnternet və xüsusi virtual şəbəkələr kimi ictimai şəbəkələr vasitəsilə istifadəçilər korporativ resurslarına təhlükəsiz şəkildə daxil ola bilməsini VPN təmin edir. Şəxsi virtual (virtual fərdi şəbəkə) şəbəkələr uzaqdan etibarlı istifadə üçün istifadə olunan bir texnologiyadır.



Şəkil 1.9 VPN

1.3 Korporativ şəbəkə strukturunun təşkili vasitələri

Şəbəkə qurğuları kompüter və ya oxşar rəqəmsal sistemlərin işləməsinə və bir-biri ilə ünsiyyətinə imkan verən cihazlardır.Şəbəkə quruluşu bu cür cihazları birləşməsindən ibarətdir.

Şəbəkə kartı;

Kompüterləri və digər cihazları şəbəkəyə birləşdirən qurğu şəbəkə interfeysi kartı (NIC) adlanır. Anakartla kompüter spesifikasiyasına uyğun olaraq inteqrasiya edilə bilər və ya anakartın hər hansı bir periferik yuvasına yerləşdirilə bilər. ISA, PCI, USB, PCMCI kimi portları istifadə edən şəbəkə interfeysi kartları var. Şəbəkə interfeysi kartlarında hər hansı digər kartda olmayan 48-bit fiziki ünvan var. Bu ünvan MAC (Media Access Control) ünvanı adlanır. MAC ünvanı istifadəçilər üçün şəbəkə məlumat axını nəzarət etmək üçün istifadə olunur. Şəbəkə kartı kompüter şəbəkələrindəki kompüterlər arasında məlumat ötürür və qurğular digər kompüterlər tərəfindən istifadə oluna bilər. Ethernet kartlarını çıxışa bağlayarkən məlumat kabel vasitəsilə bölüşmək üçün açıq olan digər kompüterlərə və ya cihazlara ötürülür.

Şəkil 2.0 Şəbəkə kartı

Kommutator/Switch;

Switch, ümumi istifadə və ya paylaşma üçün şəbəkə qurğularını bağlayan şəbəkə sistemlərindəki yeganə cihazdır və məlumatları digər kompüterlərdən süzərək digər kompüterlərə göndərir. Klassik hublardan fərqi; yalnız daxil olan məlumatları istənilən cihaza göndərir, hub daxil olan məlumatları bütün qurğulara göndərir və yalnız müvafiq cihaz data alır. Hal-hazırda hublar keçid cihazları ilə əvəz olunur. Dəyişən cihaz modelləri 4-5-8-16-24-26-48 portu ilə bu gün mövcuddur. Switch MAC ünvanlarına baxaraq cihaz portlarına bağlı kompüterləri tanıyır. Quruluşdakı yerləşdirmələri yerinə yetirmək üçün MAC ünvanlarını MAC cədvəlində saxlayır. Bu, çatan məlumat paketlərinin MAC ünvanlarını yoxlayır və onları yalnız hədəf MAC ünvanına malik olan kompüterə bağlanan porta göndərir. Bu, şəbəkədəki münaqişələrin qarşısını alır.

Şəkil 2.1 Kommutator

Router/Yönləndirici;

Router əsasən marşrutlaşdırma vəzifəsi kimi xidmət edir. LAN-LAN və ya LAN-WAN arasında əlaqə yaratmaq üçün istifadə olunur. LAN və WAN əlaqələri üçün ayrıca portlar da mövcuddur və rezerv port yuvaları əlavə edilə bilər. Lazım olduqda bu portlara LAN və ya WAN portları əlavə edilə bilər. Router əməliyyat sistemləri ilə proqramlaşdırılmış və zəruri düzəlişlər edildikdə uzaq bir şəbəkəyə daxil olmaq üçün bir çox mövcud yoldan ən yaxşı seçim edə bilər.

Şəkil 2.2 Router

Modem;

Cihazların telefon xəttləri ilə internet çıxışı almasını təmin edir. Standart telefon xətlərində yalnız səs ötürülə bilər. Bu halda məlumatları səs və səsi məlumata çevirmək lazımdır. Bu dönüşüm çox yüksək sürətlə aparılmalıdır. Lakin, telefon xətlərinin keyfiyyəti çox yüksək sürətə imkan vermir. Buna görə hər şey modemlərin öz xüsusiyyətlərindən asılıdır. Modemin missiyası kompüterdən alınan rəqəmsal məlumatları analoq məlumatlara çevirib göndərmək və analoq məlumatları rəqəmsala çevirib kompüterə ötürməkdən ibarət hesab edilə bilər.

'Dial Up' modemlər;

Bu inkişaf etmiş ölkələrdə istifadə müddətini başa vurmuş olan, lakin bəzi ölkələrdə hələ də geniş istifadə olunan bir əlaqə formasıdır. Normal bir telefon xətti, Dial Up modem və internetə giriş kodu bu əlaqəni istifadə etmək üçün kifayətdir. Bağlantı qurulduqda, mobil operator tərəfindən İnternet Servis Provayderləri (İnternet Servis Provayderləri) üçün verilən xüsusi bir giriş nömrəsi

modem tərəfindən yığılır. Dial Up telefon xəttindən istifadə etdiyindən, internetə qoşulmaq və eyni zamanda telefon zəngləri etmək mümkün olmayacaqdır. Dial Up modemlərin sürəti 2400, 9600, 14400, 28000, 33600, 56000 bps-ə çata bilər. Bu gün ən çox istifadə edilən Dial Up modemləri 56 Kbps sürətindədir

Bu modemlər daxili və xarici olmaqla 2 yerə bölünür.

• Daxili modemlər

Daxili modemlər kompüterə qoşulan digər kartlar kimi işdə bir yuvaya əlavə olunur. Cihazın elektrik təchizatından enerji təmin edir.

Şəkil 2.3 daxili modem

• Xarici modemlər

Xarici modemlər ayrı bir cihaz şəklindədir. Buna görə, kompüterə serial çıxdıqdan birinə birləşdirilən kabel vasitəsilə bağlanır. Onlar kompüterdən kənarda olduğundan gücünü kompüterdən ala bilmirlər. Buna görə onların ayrıca adapteri var. Bağlantı telefon xəttini modemə və modemi telefon cihazına qoşaraq yaradılır.

Şəkil 2.4 xarici modem

ADSL modemler;

ADSL (asimmetrik rəqəmsal abunəçi xətti) mövcud telefon xəttindən yüksək məlumat, səs və video rabitə təmin edən sürətli və təhlükəsiz, daimi modem texnologiyasıdır. Bu texnologiya ilə əlaqə qurulduqda, splitter telefonun paralel olaraq işləməsini təmin edir. Həm internet, həm də telefon rabitəsi eyni zamanda istifadə edilir.

Şəkil 2.5 Ayırıcı (splitter)

ADSL modemləri əlaqə növlərinə görə dörd qrupda nəzərdən keçirilir:

- **Ethernet modemlər**

Ethernet portları ilə kompüterlə əlaqə qurur. Buna görə, kompüterinizdə 'Ethernet kartı' olmalıdır.

- **USB modemlər**

Kompüterin USB portu ilə əlaqəli bu modemlər kompüterin daxilində yox kənarda yerləşir. Bəzi modellər enerji təchizatı tələb edir, digərləri isə USB portundan gücə əsaslanır.

- **PCI modemlər**

Bu tip modemlər kompüterin PCI yuvasına yerləşdirilir və sürücüsünü quraşdırdıqdan sonra dial-up kimi istifadə olunur.

- **Simsiz modemlər**

Struktur baxımından simsiz modemlər eyni zamanda şəbəkəyə qoşulmaq və simsiz şəbəkə kartı daxil olmaqla,internet şəbəkəsini daxil etməklə bu kompüterlərin şəbəkəyə daxil edilməsinə imkan verərək,kompüterlərə birləşdirilir.RF (radio frekanslı) texnologiyasından istifadə edən bu modemlərdə internetə çıxış modemin yerləşdiyi yerdən asılı olaraq dəyişə bilər. Məhdud

yerlərdə zəif siqnal gücü azalıb performansa düşməsinə səbəb ola bilər.

Şəkil 2.6 Kabelsiz modem

• VDSL modemlər

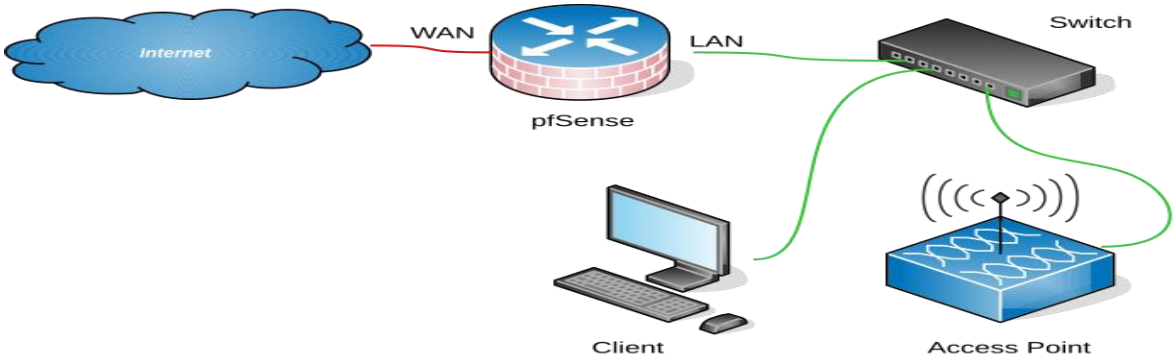
VDSL (çox yüksək məlumat dərəcəsi dijital abunəçi xətti) DSL texnologiyasıdır ki, məlumatların dövriyyəsini telefon xəttləri üzərindən çox yüksək sürətlə çatdırır. 13 və 52 Mbps arasında yükləmə 1,5-dən 2.3 Kbps arası isə upload sürətinə çatır.

Şəkil 2.7 VDSL modem

Access Point;

Giriş nöqtəsi simli internet şəbəkəsinə simsiz çıxış təmin edir. Giriş nöqtəsi hub, kommutator və ya simli routerə yerləşdirilir və simsiz rabitə siqnalları göndərir. Bu, kompüter və qurğuların kabelsiz şəbəkəyə qoşulmasına imkan verir. Hava limanında, restoran və ya oteldə mövcud olan ümumi simsiz şəbəkə internetə

kabelsiz olaraq bağlanmağımıza vasitəçilik edir və adətən bir giriş nöqtəsi ilə əlaqələndirilir. Kompüterlərinizi kabelsiz internetə bağlamaq və simsiz rabitə təmin etmək üçün kabelsiz əlaqə təmin edən bir routeriniz varsa bir giriş nöqtəsinə ehtiyacınız yoxdur.



Şəkil 2.8 Access Point

Təkrarlayıcı/Repeatr

Zəifləyən siqnalın müxtəlif səbəblərə görə gücləndiyini və şəbəkəyə geri göndərən fəal şəbəkə cihazıdır. Təkrarlayıcıların tez-tez istifadə etdiyi mühitlər simli mühitdən fərqli olaraq simsiz mühitlərdir. Simli mühitlərdə hər bir aktiv cihaz (router, keçid, hub və s.) təkrarlayıcı olaraq işləyir.

Firewall

Dilimizə təhlükəsizlik divarı kimi tərcümə olan firewall, xüsusi şəbəkələrlə internet arasında hər iki istiqamətdə istənməyən trafikə mane olan bir proqram və ya hardware sistemidir. Təhlükəsizlik divarını səmərəli şəkildə istifadə etmək üçün internet və xüsusi şəbəkə arasındakı bütün trafik təhlükəsizlik divarı üzərindən keçməlidir və lazımi icazə / icazələr uyğun bir strategiya ilə hazırlanmalıdır.

Cisco Pix Firewall

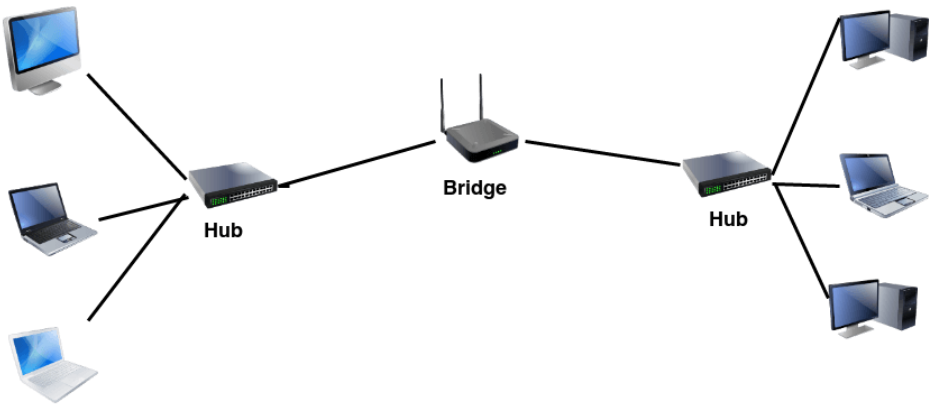
Şəkil 2.9 Firewall

Gateway

Şəbəkə tətbiqlərində fərqli yollarla istifadə edilən və qapalı bir ərazidə internetə çıxış imkanı olan cihazlardır. Digər bir istifadə üsulu fərqli protokolları istifadə edən şəbəkələri birləşdirməkdir. İnternetə və ya digər şəbəkəyə qoşulmaq üçün istifadə olunduqda, kompüterlərin TCP / IP konfiqurasiyasında gateway kimi hazırlanmış cihazın IP ünvanı müəyyən edilməlidir. Beləliklə, marşrutlaşdırıcıların (routerlər kimi) istifadəsi bu şəkildə həyata keçirilir.

Bridge

Bu iki TCP / IP şəbəkəsini birləşdirən bir cihazdır. Çoxda kompleks qurğu olmayan körpülər daxil olan paketləri (məlumat paketləri) alır və ötürür. Körpülər şəbəkə trafikinə və fiziki qoşulmalara nəzarət edən cihazlardır.



Şəkil 3.0 Bridge

1.4 Korporativ şəbəkələrdə istifadə olunan protokol və servislər

TCP

IP-nin üst qatında çalışan iki nəqliyyat qatı protokollarından biridir. İki ana kompyuter eyni şəbəkə və ya müxtəlif şəbəkələrdə bir-biri ilə etibarlı ünsiyyət qurmağa imkan verir.

TCP-nin əsas xüsusiyyətləri aşağıdakılardır:

• Əlaqəni qurmaq və bağlantını sonlandırmaq

• etibarlı paket çatdırılması

• axınının qarşısını almaq üçün axına nəzarət (axını nəzarət)

• Korlanmış və ya təkrarlanan məlumatların düzəldilməsi (səhvlərin bərpası)

TCP İnternetdə aşağıdakı funksiyaları təmin edir:

• Əsas məlumat ötürülməsi

• Etibarlılıq

• Axının sonlanmasına nəzarət

• Multiplexing

• Əlaqələr

• Full duplex bağlantı

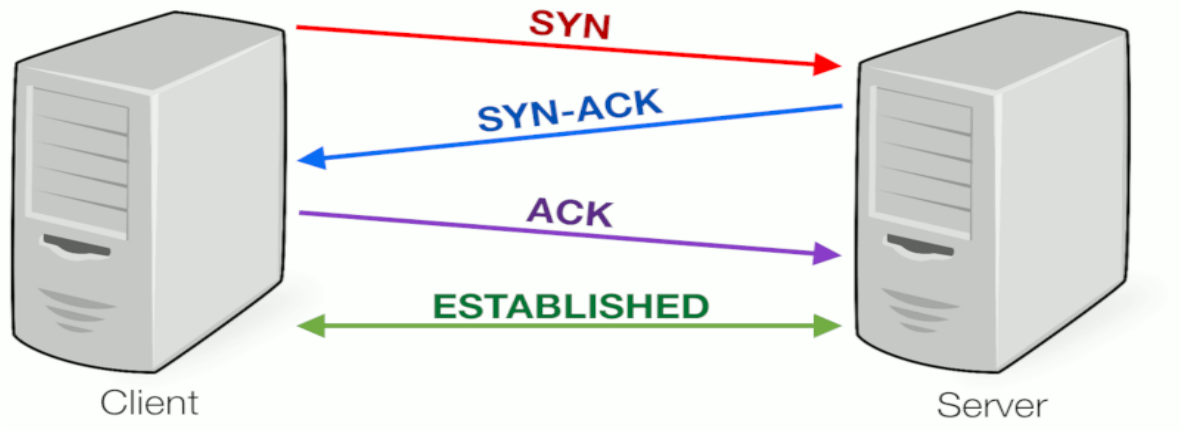
TCP bağlantısı qurulması üç addımın nəticəsində baş verir:

1-ci addımda: Mənbəyi host əlaqə qurmaq istəyən ev sahibinə bir paket göndərir. Bu paket TCP-dir

SYN = 1 və ACK = 0-dir. Göndərilən paketdə seqmentin sifariş nömrəsi X.

2-ci addım bu paket qəbul edən sahə TCP başlığında SYN = 1, ACK = 1 bit göndərir və onun sıra nömrəsini = Y və təsdiq nömrəsini, ACK nömrəsi = (X + 1) paket nömrəsinə göndərir.

3. Bundan əlavə: sorğunun cavabını tapmış müştəri təsdiq etmə paketini son mərhələdə hədəfə göndərir və əlaqə qurulur.Sonra mənbə, təyinata göndərmək istədikləri məlumat paketlərini göndərir.



Şəkil 3.1 TCP 3-way handshake

TCP və UDP üst protokollarla əlaqəli portları istifadə edirlər. 65535 ədəd port var və IANA (Internet Assigned Numbers Authority) ilk 1024 portu tanınmış portlar olaraq elan etmiştir. Bu portlardan bəziləri bunlardır:

• FTP: 21

• Telnet: 23

• SMTP: 25

• DNS: 53

UDP (User Datagram Protocol)

UDP, TCP / IP protokol qrupunun iki nəqliyyat qatı protokollarından biridir. UDP-də dəqiq qəbul və qəbul etmə mexanizmləri yoxdur. Buna görə də məlumat ötürülməsində müvəffəqiyyət təmin edə bilməz. Etibarlı transfer xidməti

vermir.Əgər paket təhlükəsiz və ardıcıl məlumat mübadiləsi edilməsini tələb edərsə, UDP yerinə TCP protokolu seçilməlidir. Bəzi UDP port nömrələri;

• Who is: 43

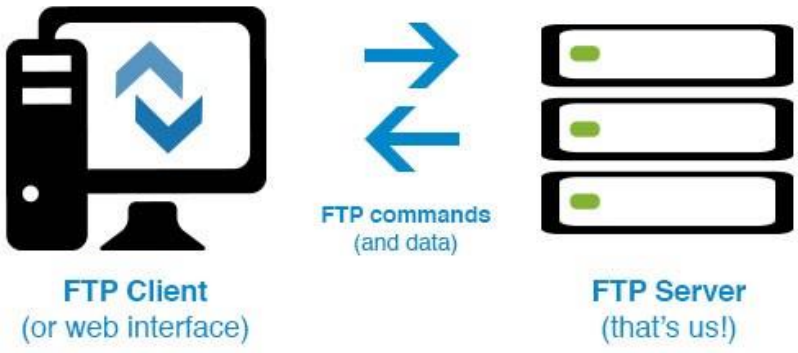
• DNS: 53

• NTP: 123

• SNMP: 161

FTP (File Transfer Protocol)

FTP (Fayl Transver Protokolu) faylları bir bağlı kompüterdən digərinə (hər iki istiqamətdə) və bu işi əksinə yerinə yetirən proqram və ya proqramlarına verilən ümumi adı göstərmək üçün hazırlanmış İnternet protokoludur. Bu ilk inkişaf etmiş internet protokollarından biridir. Faylları FTP protokolu ilə bir kompüterdən başqa bir kompüterə köçürərkən, həmin kompüterlə on-line əlaqə yaradılır və protokolu ilə təchiz edilmiş bir sıra komanda ilə iki kompüter arasında bir fayl göndərilir.



Şəkil 3.2 FTP protokolu

FTP protokolunun xüsusiyyətləri;

* Daimi əlaqələr mövcuddur.

* Data və əmrlər ayrı portdan köçürülür

* Təhlükəsizlik mexanizmini təmin edir (müştəri serverə təqdim edir)

* Anonim əlaqələrə imkan verir. Anonim istifadəçidir. Lakin bu hesab bağlana bilər.

* Kvota bantları müəyyən edilir. Bu qovluq indeks üçün kvota kimi müəyyən edilir.

* Bir çox web server, web publishing, fayl ötürülməsində ftp istifadə olunur.

* Fayl ötürülməsi məhdudlaşdırıla bilər.

* FTP, mb, gb ölçüsü faylları köçürülür. FTP HTTP-dən daha az istifadəçiyə xidmət edir.

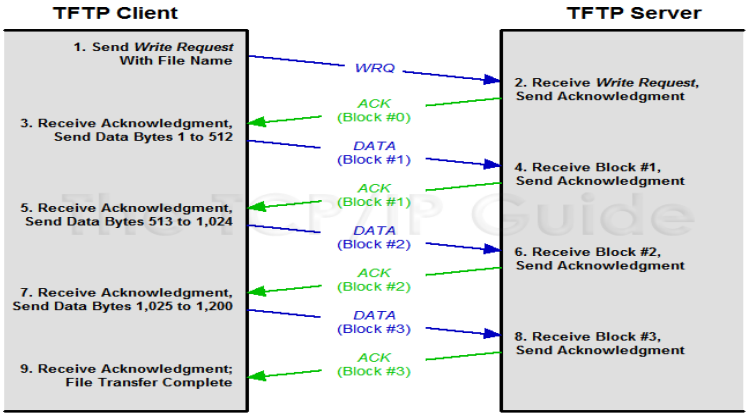
* IP məhdudlaşdırıla bilər.

* Bu Unix əsaslı bir protokol.

* HTTP serverləri üçün fayl ötürülməsini təmin edir.

TFTP (Trivial File Transfer Protocol)

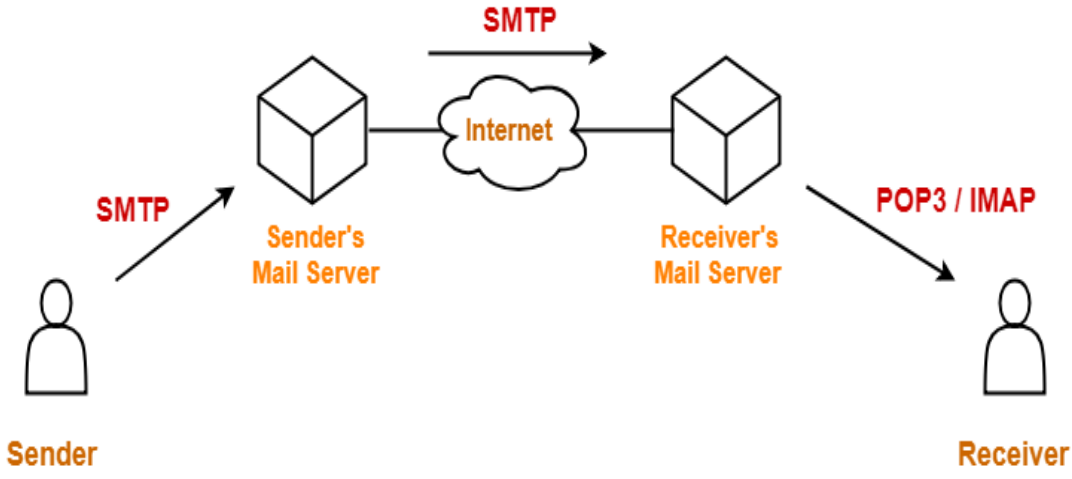
Önəmsiz Fayl Aktarımı Protokolu (TFTP) FTP-in əcdadı və sadələşdirilmiş versiyasıdır. Amma nə istədiyinizi və harada tapmaq istədiyinizi bilsəniz, bu seçməli olduğunuz protokoldur.Əlavə olaraq istifadə etmək çox asandır.Buna baxmayaraq, FTP sizə təmin etdiyi funksionallığın zənginliyini təklif etmir. TFTP-də indeks axtarış imkanı yoxdur,göndərmək və qəbul etməkdən başqa heç bir şey edə bilməzsən.Bu kiçik həcimli protokol, FTP-də olduğu kimi, məlumat hissəsindəki dataları saxlayaraq FTP-də yoxlama aparmaqla FTP-dən daha kiçik məlumat blokları şəklində göndərə bilər. Buna görə təhlükəli deyil. Təbii təhlükəsizliyə görə risklər çox azdır. Bu protokolun etibarlı olması nəzərdə tutulmayıb. Hər hansı bir problem, əlaqəni ləğv etməyə səbəb ola bilər. TFTP yalnız bəzi səhv mesajları verir və mesajlar itirilmiş zaman başa düşmək üçün itki vaxtını dəstəkləyir.



Şəkil 3.3 TFTP protokolu

SMTP (Simple Mail Transfer Protocol)

Sadə Poçt Göndərmə Protokolu (SMTP) internet vasitəsi ilə 25 nömrəli port vasitəsi ilə elektron poçt göndərməkdə kömək edir. Bizim poçt göndərmə prosesi standart poçt ötürülməsinə bənzəyir. SMTP vasitəsilə e-poçt göndərdikdə, poçtumuz SMTP serverinə köçürülür. Server vasitəsilə İnternetlə səyahət edən e-poçtumuz, daha sonra SMTP vasitəsilə e-poçtları əldə etməyə kömək edən POP / IMAP Server ilə əlaqə saxlayır. Son mərhələdə, POP / IMAP hesabı ilə göndərilən e-poçt hesaba göndərilir. 1960-cı illərdə birə bir elektron mesajların müxtəlif formaları istifadə edilmişdir. İnsanlar müəyyən hostlar üçün qabaqcıl sistemlərdən istifadə edərək, digər hostlarla əlaqə qururdu. Daha az kompüter ABŞ-da ARPANET-ə birbaşa elektron poçt göndərməklə bağlı imkana malik idi və müxtəlif sistemlərin istifadəçilərinə bir-birinə elektron poçt göndərmək üçün standartlar hazırlanmışdır.



Şəkil 3.3 SMTP protokolu

SMTP server, başlıqda qeyd etdiyimiz kimi, İnternet vasitəsilə kompüterinizdən e-poçtları əldə etməyə və digər ötürmə orqanlarına ötürməyə kömək edən server tipidir. SMTP server poçt şöbəsinin funksiyasına malikdir. Hər şeydən əvvəl o, bizdən məktublar alır və sonra poçtları nəql etmək üçün lazımi addımlar atır. Nəhayət, poçtunuzu POP / IMAP serverinə göndərir, postman kimi çıxış edir və bu şəkildə mesajlar sizə çatır. SMTP istifadəçiləri e-poçtlarına veb versiyası yerinə bir proqram vasitəsi ilə müraciət etməlidirlər. Bir çox poçt proqramı avtomatik olaraq SMTP parametrlərini istifadəçilərə əlavə edə bilər. Əgər istifadə etdiyiniz proqram bu düzəlişləri etməzsə, SMTP məlumatı üçün poçt xidmətini təmin edən server administratorundan məlumat əldə etməklə bu məlumatı proqramınıza daxil etməlisiniz.

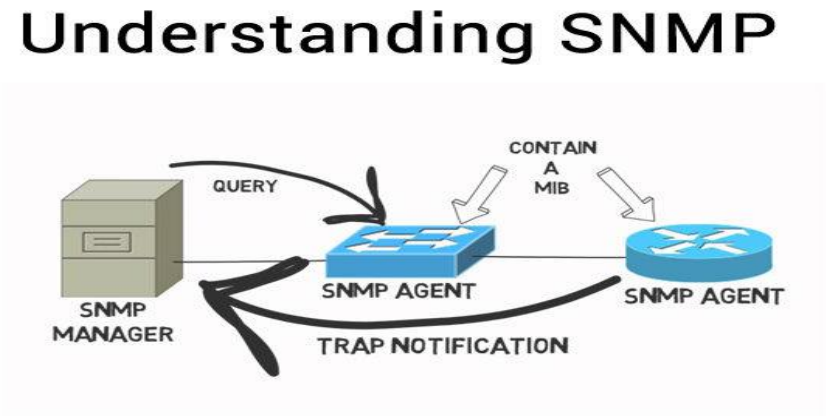
SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) 1988-ci ildə hazırlanmış bir şəbəkə idarəetmə protokudur. SNMP, şəbəkə qurğularının sürətlə artan sayını asanlıqla idarə etmək məqsədilə hazırlanmış, tədricən standart halına gəlmiş və bugünkü şəbəkə qurğunun ən önəmli bir xüsusiyyəti olmuşdur. SNMP-ni istifadə edərək internetə qoşulan hər hansı bir cihazdan (marşrutlaşdırıcılar, açarlar, printerlər, hublar, kondisionerlər, serverlər və hətta normal kompüterlər) məlumat əldə edə bilərsiniz. SNMP ilə cihazlardan öyrənilə bilən bəzi məlumatlar bunlardır:

- Sistemin işləmə müddəti
- CPU istifadə səviyyəsi
- Yaddaş və yaddaş istifadə səviyyəsi
- Cihazın istehsal məlumatı (model, seriya nömrəsi, və s.)
- Şəbəkə cihazları üçün şəbəkə axını məlumatları

Üç müxtəlif SNMP versiyası mövcuddur: SNMPv1, SNMPv2, SNMPv3. SNMPv1 ilk snmp versiyasıdır və UDP IP üzərində istifadə olunur. 1988-ci ildə RFC-də ilk dəfə rəsmi qeydiyyata alınıb. SNMPv2-də SNMPv1 nisbətən

performans, təhlükəsizlik, etibarlılıq və menecer-menecer əlaqələri inkişaf etmişdir. GetBulkRequest və getNextRequests mesajları SNMPv2 ilə istifadə olunur. SNMPv3, uzaq snmp istifadə edərək, səhv idarəetməsi, təhlükəsizlik və cihaz konfiqurasiyası kimi yeni xüsusiyyətləri gətirdi.



Şəkil 3.4 SNMP protokolu

SNMP tərkib hissələri;

Şəbəkənin idarə olunması üçün SNMP istifadə edən bir sistemdə üç əsas komponent var:

- SNMP meneceri: Şəbəkə administratoru tərəfindən istifadə olunan idarəetmə proqramı. Bu proqram SNMP vasitəsilə əldə olunan məlumatları əks etdirir.
- SNMP Agent: Bu məlumatı əldə etmək üçün cihazda olan proqramdır.
- SNMP MIB: İdarəetmə İnformatin bazası deməkdir olan MİBlər şəbəkə cihazı və şəbəkə administratoru arasında ötürülən məlumatların strukturlarını ehtiva edən komponentlərdir.

Administrator və agent arasında ünsiyyət müəyyən formalarda olan mesajlarla təmin edilir. Əlaqə üçün istifadə edilən mesajlar əsasəndir:

- SNMP GET
- SNMP GET-NEXT

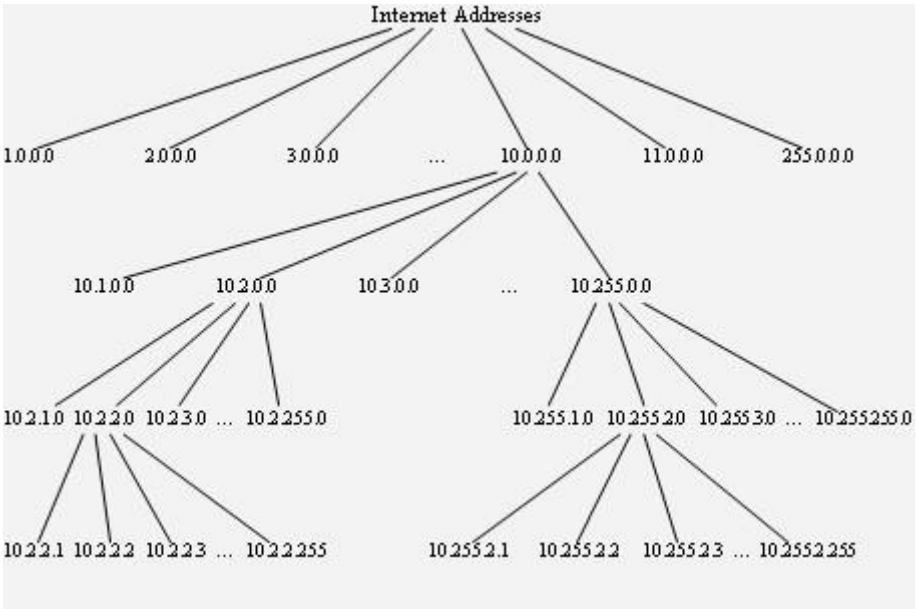
- SNMP GET-RESPONSE
- SNMP TRAP

GET və GET-NEXT mesajları dəyərləri oxumaq üçün istifadə olunur. SNMP meneceri bu mesajlarla məlumat istəmədikdə, SNMP Agent cavabı GET-RESPONSE mesajında göndərir. TRAP mesajı, SNMP Agentinə bəzi xəbərdarlıq məlumatları göndərmək üçün SNMP Agent tərəfindən istifadə olunur.

SNMP mesajları Nəqliyyat Layerində UDP istifadə edərək ötürülür. Çünki sıx ötürülən halda, TCP zəifdir və məlumat itkisi mövcuddur. UDP istifadə edərkən, zamanaşımı düzgün müəyyənləşdirmək itkisiz ünsiyyət üçün faydalı olacaq.

IP (Internet Protocol)

IP ünvanı IP şəbəkələrində hər bir cihazın olması lazım olan sayısal bir dəyərdir. IP ünvanları hardware ünvanı deyil, bir MAC ünvanı deyil, bir proqram dəyəri deyil. Yəni istənilən vaxt dəyişə bilər. Hal-hazırda dünya miqyasında istifadə edilən 4-cü versiya IP ünvanı ardıcıl 1 və 0-dan ibarət 32 bitlik bir ünvandır. İstifadəsi asanlıqla nöqtə ilə ayrılmış 4 parçadır və hər parça nöqtədə 4 rəqəm kimi yazılır. Hər parça oktet adlanır. Aşağıdakı şəkildə göstərildiyi kimi, hər bir oktet aralığı 0 ilə 255 arasında dəyişir.Oktetlər 8 bitlik hissələrdən ibarət olurlar və bir birindən nöqtə ilə ayrılırlar.Dörd çütlük əmələ gətirən bu oktetlər ipv4-ün görünüş şəklini formalaşdırırlar.İpv6-da isə onaltılıq say sistemindən istifadə olunur və onlar 6 oktetlə nöqtələrin köməyi ilə biri birindən ayrılmış şəkildə qeyd olunur.



IPv4 Ünvan Sinifləri

- Class A ünvanları: Bir çox istifadəçi ilə geniş şəbəkələr üçün nəzərdə tutulmuşdur. Class A IP ünvanları şəbəkəni müəyyən etmək üçün yalnız birinci seksiyanı istifadə edir. Qalan oktetlər istifadəçiləri müəyyənləşdirmək üçün nəzərdə tutulub. Beləliklə, 16 milyondan çox istifadəçiyə müraciət etmək mümkündür. Sınıf A ünvanının ilk biti həmişə 0 olur. Beləliklə, decimal bazasında 127 ikili bazda ən kiçik nömrə 00000000, 0 əsasda 0, ikili bazda 01111111-də ən çox saydadır. Beləliklə, 1 və 126 arasında başlayan bütün ünvanlar A ünvanlarını göstərir. 127.0.0.1 loop testi (yerli loopback) ünvanıdır. Buna görə, sinif A IP ünvanı olan şəbəkələrin sayı 126-dır.
- B sinfi ünvanları: B sinfi ünvanları normal ölçülü şəbəkələr üçün nəzərdə tutulmuşdur. B sinfi IP ünvanlarında, şəbəkə ilk 2 səkkizlik oktet ilə müəyyən edilir, digər 2 oktet isə istifadəçiyə müraciət etmək üçündür. B sinfi B ünvanlarının ilk səkkizinci hissəsinin ilk 2 biti həmişə 10-dur. Qalan 6 bit 1 və ya 0 ola bilər. B sinif ünvanları üçün ən kiçik sayı ikili bazda 10000000, decimal üzrə 128, ikili bazda isə 10111111, decimal üzrə isə 191 təşkil edir. Yəni, 128 və 191 arasında rəqəmlərlə başlayan bütün ünvanlar B sinfi ünvanlarıdır.
- Sınıf C ünvanları: C ünvanlarının maksimum 254 istifadəçisi olan kiçik şəbəkələr üçün nəzərdə tutulmuşdur. Sinif C ünvanları ikili ilə başlayır. Bu sahədə, ikili bazda ən kiçik say 11000000, ən yüksək say 192, ən çox sayı isə 11011111, onluq isə bazda 223 olur. Beləliklə, 192 və 223 nömrələri ilə başlayan ünvanlar C sinif ünvanlarıdır.

Bu üç IP sinifindən başqa, D və E sinf IP ünvanları da mövcuddur.D sinif ünvanların bir çoxu multistast üçün istifadə olunur. E sinif ünvanları isə elmi araşdırmalar üçün qorunur.

Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

ICMP (Internet Control Message Protocol)

TCP / IP protokolu paketində İnternet Protokolunun (IP) səhvləri, səhv düzəldilməsini və ya kompüterlər və arasında statistika hesabatlarını təqdim etməyə imkanları yoxdur. Əlaqəsiz bir protokol, İP, iki son nöqtə arasındakı əlaqənin İstifadəçi Məlumat Protokolu Protokolu (UDP) üzərində qurulub-edilməməsi ilə əlaqədardır. ICMP (Internet Control Message Protocol) IP paketinin məlumatlar bölməsində İnternet layınını işləyərək və problemləri ünsiyyət qurğularına çatdırmaqla məlumatlandırma mexanizmini yaradır. ICMP ümumilikdə; TTL-nin müddəti başa çatdıqda, paketin sahibini xəbərdar etmək, hər hansı bir vəziyyətdə məhv edilmiş paket haqqında geri bildirim təmin etmək, səhv baş vermiş hadisələr barədə rəy vermək və paket başqa bir şəkildə səyahət edərkən geri bildirim vermək kimi vəzifələri götürür. Məsələn, Ping və Tracert əmrləri tez-tez ICMP Echo Tələbi və ICMP Echo Cavab mesajları ilə problem həll işi üçün istifadə olunur.

Şəkil 3.5 İCMP protokolu

ICMP Paket Quruluşu

ICMP mesajları IP datagramının məlumat sahəsinə köçürülür. IP başlığındaki protokol sahəsi ICMP'nin istifadə olunduğunu göstərmək üçün 1 olaraq təyin edilir.

IP ünvanı
Növü (8)
Kodu (8)
Toplam xəta sayı (16)
Parametrlər (parametrlər olmadıqda istifadə edilmir)
Məlumat (dəyişən)

Mesaj növü ala biləcək ifadələr

ICMP paketindəki vəziyyət məlumatı tip bölməsinin qəbul etdiyi parametrlər ilə müəyyən edilir.

0 - Echo cavab (Echo Cavab) - cavab cavab
3 – Çatdırıla bilməyən (Hədəfə çatmayan)
4 - Source Quench
5 - Yenidən istiqamətləndirici tələb olunan
8 - Echo İstəyi - (ping tələbi)
9 - Router tətbiqi
10 - Router istəyi
11 – Paketin yaşam dövrü müddəti -traceroute tərəfindən istifadə olunur.
12 - Parametr problemi
13 - Zaman damgası tələbi
14 - Timestamp Cavab
15 - İnformasiya sorğusu
16 - Məlumat Cavab (Məlumat Cavabı)

17 - Ünvan Maska Tələbi
18 - Addres Mask cavab (Ünvan Maska Cavab)

DHCP (Dynamic Host Configuration Protocol)

DHCP, IP ünvanlarını və ağda istifadə olunan digər konfiqurasiya məlumatlarını mərkəzləşdirmək üçün nəzərdə tutulmuş bir IP standartıdır. Microsoft Windows Server ailəsinin hər hansı bir üzvü DHCP server kimi konfiqurasiya edilə bilər və şəbəkədə DHCP-effektiv olan kompüterlərə DHCP xidmətləri təqdim edə bilər.

DHCP, müştəri-server modelinə əsaslanan bir protokol hesab oluna bilər. Şəbəkə administratorları, müştərilərə təmin etmək üçün onların verilənlər bazasında TCP / IP konfiqurasiya məlumatlarını saxlayan bir və ya daha çox DHCP serverini quraşdırır. Bu verilənlər bazası aşağıdakı məlumatları ehtiva edir:

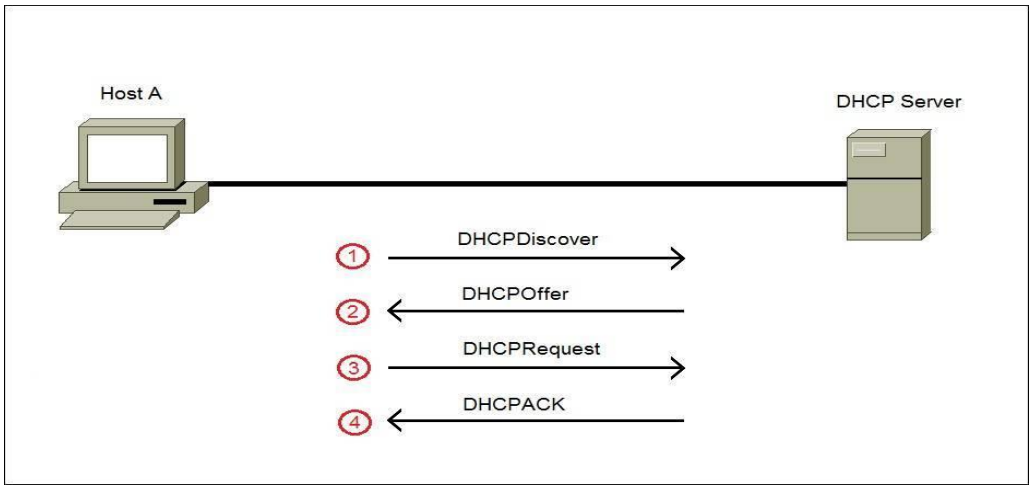
• Konfiqurasiya parametrləri şəbəkə üzrə bütün kompüterlər üçün etibarlıdır.

• Müştərilərə təyin olunacaq bir ehtiyatda saxlanılan cari IP ünvanları, eləcə də əl ilə təyin etmək üçün ayrılmış ünvanlar.

• Server tərəfindən təklif olunan kirayə müddəti. İcarə təyin edilmiş IP ünvanının istifadə müddətini müəyyənləşdirir.

Bir DHCP server şəbəkə quraşdırılıb və konfiqurasiya olunduqda, IP ünvanı təyin etməsi olan müştərilərin TCP / IP konfiqurasiyası avtomatik olaraq şəbəkəyə qoşulduqda dinamik şəkildə meydana gəlir. Eyni şəbəkədəki kompüterlər müxtəlif IP ünvanlarına malik olmalıdırlar. Bir kompüterin IP ünvanı və Subnet Mask həm həmin kompüterin yerləşdiyi alt şəbəkəni və həmin alt şəbəkədə unikal ünvanını müəyyən edir. DHCP serverinin vəzifəsi kompüterlərin IP ünvanı konfiqurasiyasını asanlaşdırmaq və bu şəbəkə mühitində idarəetməni mərkəzləşdirmək üçün istifadə edilə bilər.DHCP'li şəbəkələrdə, kompüterlər IP ünvanlarını DHCP serverinin IP ünvanı verilənlər bazasından əldə edirlər.

DHCP'nin aktiv olmadığı bir şəbəkədə, hər bir kompüterin şəbəkə konfiqurasiyası yalnız əl ilə həyata keçirilə bilər. Kiçik bir şəbəkədə çox mürəkkəb bir iş kimi görünməməsinə baxmayaraq, böyük şəbəkələrdə çətin və yorucu bir vəzifədir. Əllə konfiqurasiya edilmiş bir şəbəkədə IP ünvanlarının idarə edilməsi daha da çətinləşəcək və bu şəbəkə mühitində kolliziyalar baş verə bilər.



Şəkil 3.6 DHCP protokolu

DHCP istifadə etməmək səbəb olacağı bir digər problem isə kompüterlərin fərqli alt şəbəkələrə daşınması vəziyyətində IP ünvanlarının tək tək yenidən qurulması gərəyidir. Bir kompüter fərqli bir alt ağa keçdiyində, yeni şəbəkədəki kompüterlərlə ünsiyyətə keçə bilməsi üçün, IP ünvanı və alt ağ maskası dəyişdirilməsi lazımdır. Bu əməliyyatın sayca çox miqdarda kompüter üçün reallaşdırılması isə yaxşıca yorucu və çətin bir iş olacaq və yenə ünvanlar manual olaraq yapılandırıldığından səhvlər da ortaya çıxacaq.Bu nöqtədə, DHCP sabit və etibarlı şəbəkə mühitinin yaradılması üçün böyük üstünlüklər təklif edir. İstər kiçik diametrli olsun istər böyük, istər sabit istərsə də çox tez dəyişən bir şəbəkə strukturu olsun, mühitə əlavə olunacaq bir DHCP server rəhbərliyi böyük ölçüdə asanlaşdıracaq. Məsələn mühitdə tez yer dəyişdirən kompüterlər var isə (laptop və ya daha başqa kompüterlər), DHCP'deki kirayə müddətinin qısaldılması sayəsində müştəri daha qısa zaman aralıqlarında yeni IP ünvanını istəyəcək.

• Aralıq: Bir şəbəkə üçün mümkün IP ünvanlarının ardıcıl bir sıradır. Tərəflər normal olaraq DHCP xidmətlərini təmin edən şəbəkənizdə vahid fiziki alt şəbəkəni müəyyən edirlər. Tərəflər həmçinin, serverin şəbəkə, IP ünvanları və bütün əlaqədar konfiqurasiya detallarını müştərilərə yerləşdirmək və təyin etmək üçün əsas vasitələrini təmin edir.

• SuperScope: Overlay eyni fiziki alt şəbəkədə birdən çox məntiqi IP alt şəbəkəsini dəstəkləyərkən istifadə oluna bilən sahələrin inzibati bir qrupudur. Superscopes yalnız üzvləri əhatə edən və ya yalnız aktivləşdirilə bilən sub-scopes siyahısını ehtiva edir.

• İstisna İP Aralığı: Rezervasiya üçündür.DHCP xidmət təklifləri daxilində istisna olmaqla məhdudlaşdırılmış IP ünvanlarının ardıcıllığıdır. Rezervasiya aralıqları, bu aralıqlardakı serverin şəbəkədə DHCP klyentlərə verilmədiyindən əmin olun.

• Ünvan Aralığı: DHCP sahəsi müəyyən edildikdən və istisna fasilələri tətbiq edildikdən sonra qalan ünvanlar mövcud ünvan hovuzunu yaradır. Depoda olan ünvanlar şəbəkə üzərində DHCP müştərilərinə dinamik tapşırıq üçün server tərəfindən seçilə bilər.

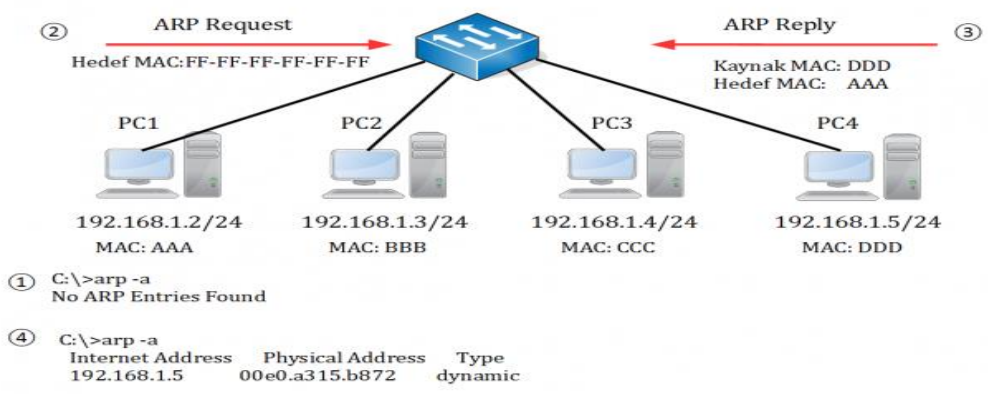
• İcarə: Kirayəlik bir müştəri kompüterinə təyin edilmiş IP ünvanından istifadə edə biləcəyi DHCP server tərəfindən göstərilən müddətdir. Kirayə müştəri üçün müəyyən edildikdə, icarə aktivdir. İcarə müddəti bitməzdən əvvəl, müştəri adətən server ilə ünvanı təyin etməlidir. Bir kirayənin müddəti başa çatarsa və ya serverdən silinsə, icarə fəaliyyəti başa çatır. İcarə müddəti icarə müddətinin necə tez-tez yerinə yetirildiyini və müştərinin server ilə icarə müddətini nə qədər tezləşdirməsini müəyyənləşdirir.

• Rezervasiya: DHCP server tərəfindən qalıcı bir ünvan lizinq təyinatı yaratmaq üçün istifadə edilir. Rezervasiyalar, alt şəbəkədə göstərilən bir cihazın həmişə eyni IP ünvanı istifadə etdiyini təmin edir. Eyni ip həmişə cihazın fiziki ünvanı (MAC) tərəfindən təmin edilir.

• Aralıq Seçimləri: DHCP-nin müştərilərinə kirayə verərkən DHCP serverinin təyin edə biləcəyi digər müştəri konfiqurasiya parametrləri var. Məsələn, bəzi ümumi seçimlər standart şlüzlər (marşrutlar), WINS serverləri və DNS serverləri üçün IP ünvanları daxildir.

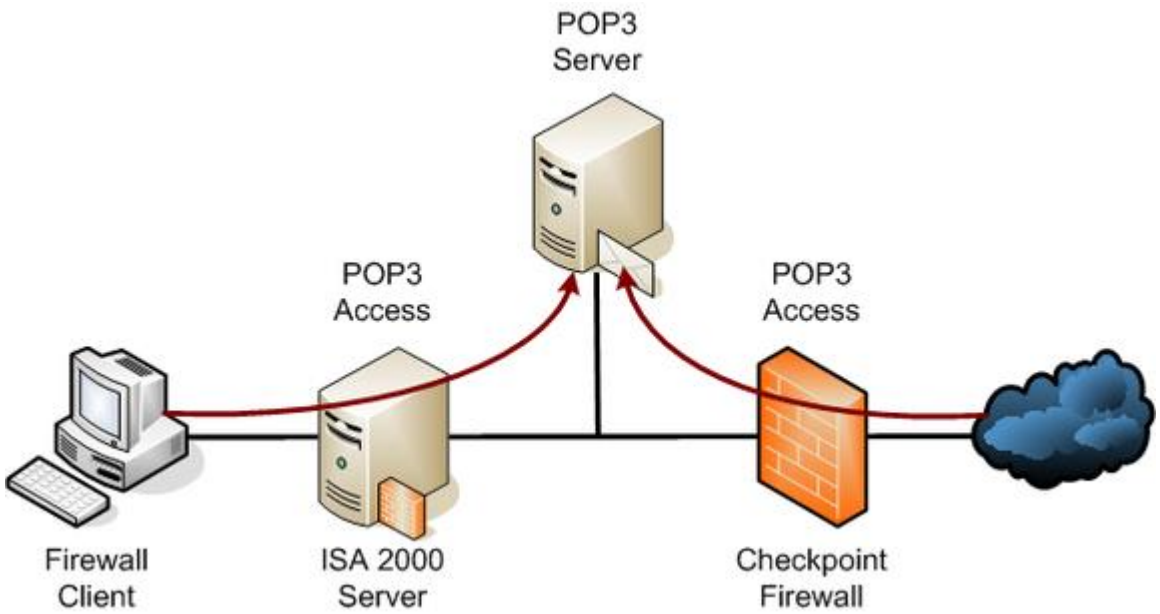
ARP (Address Resolution Protocol)

ARP (Ünvan Çevirmə Protokolu) Adres emal Protokolu, lokal şəbəkənin IP ünvanında bilinən cihazın MAC ünvanını tapmaq üçün istifadə olunur. Yerli şəbəkədə cihazlar MAC ünvanlarını istifadə edərək bir-biri ilə ünsiyyət qurur. Cihaz cihazla ünsiyyət qurarkən MAC ünvanını bilmirsə, onun IP ünvanını bilirsə, onu ARP protokolundan istifadə edə bilər. Cihazın hədəf IP ünvanını necə bildiyini deyirsinizsə, komanda xəttindən ping 192.168.1.5 daxil edərkən hədəf IP adresini cihaza çatdırdıq. PC1 PC4 ilə aşağıdakı şəkildə əlaqə saxlayın. Daha əvvəl söylədiyimiz kimi, PC1 PC4 ping ilə yoxlayır. Hər bir kompüter RAM yaddaşında bir ARP stolu tutur və ilk olaraq bu cədvəldən hədəf cihazın MAC ünvanına baxır. ARP protokolunu işlədir və ARP tələbini göndərir, başqa sözlə ünvanı həll tələbi. Paketin lokal şəbəkədə başqa bir kompüterə göndərilməsi üçün hardware ünvanının IP ünvanı ilə birlikdə tanınması lazımdır. Mənbə sistemi, ünsiyyət qurmaq istəyən hədəf sisteminin fiziki ünvanını (MAC ünvanı) öyrənmək üçün yerli şəbəkədəki bütün kompüterlərə xüsusi bir müraciət göndərir. Bu tələbə ARP tələbi deyilir.



POP3 protokolu

İnternetdə istifadə edilən protokollardan biri olan POP3 protokolu e-poçtları görmək və e-poçt göndərildiyi kompüterdən elektron poçtu yükləyə bilir. Belə bir sistem olmadığı təqdirdə e-poçtlarımızı sağlam bir şəkildə yükləmək çətin olardı. Adından göründüyü,anlaşıldığı kimi, e-poçtları idarə edən bu sistem mesajları göndərmək üçün internet poçt şöbəsi kimi fəaliyyət göstərir və elektron poçtların sahiblərinə təhlükəsiz çatdırılmasına vasitəçi olur. POP3 sistemi e-poçt ünvanlarının yülkənməsi və silinməsi üçün bir protokoldur. POP3 aşağıdakı şəkildə fəaliyyət göstərir. POP32, e-poçtları sizə çatdırmadan əvvəl serverə qoşulmalıdır. Bu əlaqə qurulduqdan dərhal sonra, POP3 mənim saytımdan mesajlar alır və onları sistemdən yeni mesajlar kimi saxlayaraq onları serverdən silər. Silinmədən sonra, bu əlaqəni ləğv edir və vəzifəsini tamamlayır. Eyni funksiyaya malik olan IMAP sistemi daha mürəkkəb bir quruluşa malikdir. Bununla yanaşı, POP3 daha sadədir. IMAP tərəfindən təmin edilən bəzi funksiyalar istifadəçilərə bu protokola daha çox seçilməsinə səbəb olur. Zaman zaman istifadəçilər bu protokolların təklif etdiyi xüsusiyyətlər daha yaxşı olduğunu müdafiə etdi. Hər iki protokol bizə internet bağlantısı olmasa da, Microsoft Outlook kimi e-poçt xidmətlərindən yüklənmiş e-poçtları oxumağa imkan verir.



Şəkil 3.7 POP3 protokolu

Telnet Protokolu;

Digər bir uzaq maşından İnternet şəbəkəsində bir çox istifadəçi maşına və bu işi yerinə yetirən proqramlara verilmiş ümumi bir TCP / IP protokoludur. Bağlı maşına daxil olmaq üçün bir istifadəçi adı və bağlantısı olması üçün bir telnet proqramına sahib olmaq lazımdır. Bununla yanaşı, bəzi kitabxanalar və ictimai telnet əsaslı web xidmətləri əlaqə zamanı istifadəçi adını tələb edə bilməz və ya istifadəçi adını və şifrəsini yazdığınız zaman avtomatik olaraq bağlandığınızda yazmaq lazımdır. Telnet, BBS (Bulletin Board Systems) indi İnternet üzərindən sistemlərə daxil olmaq üçün geniş istifadə olunur. Telnet giriş proqramları, əməliyyat sistemi ilə günümüzün əməliyyat sistemlərinin əksəriyyətində gəlir. Çox istifadəçi əməliyyat sistemi (UNIX və VMS) adətən istifadəçilərə mətn əsaslı interfeys təmin edir və bütün əməliyyatlar əmr sətrindən klaviatura vasitəsilə həyata keçirilir. Virtual serverinizə Telnet vasitəsi ilə qoşulduğunuz zaman, uzaqdan UNIX əməliyyat sisteminə qoşulur. Bu, UNIX əmrləri yazmaq, proqramların işlədilməsi və maşının önünə oturmuş kimi sistemi idarə edə bilərsiniz. Telnet proqramlarında, telnet ünvanı, yuxarıda olduğu kimi komanda xəttindən də daxil edilə bilər və proqram menyusu sisteminə də daxil edilə bilər. 1980-ci illərdə (və 1990-cı illərin əvvəllərində) ZMODEM, KERMIT kimi bəzi məşhur Telnet proqramları kompüterdən-kompüterə faylların ötürülməsi protokollarını dəstəkləyir. Server kompüteri bu qoşulma zamanı Unix-Linux əməliyyat sistemində işləyir. Telnet müştəri xarici kompüterdə (terminaldə) işlədilməlidir. Bir müştəri serverə qoşulduqda, müştəri kompyuter serverin terminalına (terminalına) çevrilir. Telnet protokolu istifadəçi adınızı və şifrənizi bağlı olduğunuz şəbəkədə asanlıqla görünən PLAİN TEXT (düz mətn) formatında göndərir. Bu, istifadəçi adınızı və şifrənizi şəbəkəni dinləyənlər tərəfindən asanlıqla görünə bilər. Ağınızdakı hər kəsə etibar edirsinizsə, Telnet-dən istifadə etməklə yanlış bir şey yoxdur. Ancaq təhlükəsizlik haqqında ən az narahatlıq varsa,

hesabınıza qoşulduqda telnet istifadə etməməyiniz yaxşıdır. Hər hansı bir Windows əməliyyat sistemi olan bir maşından Telnetə qoşulmaq istəyirsinizsə, aşağıdakı əməliyyatları yerinə yetirməlisiniz.

1- İşə sal Start -> Run menu

2- Komanda xəttində Telnet,Bağlamaq istədiyiniz maşının IP ünvanı və ya hostname adı yazaraq enter-ə Basın

3- Adresi düzgün daxil edərsəniz, əmr sətrini görəcəksiniz.

II Fəsil.Korporativ şəbəkələrin proqram konfiqurasiyasının idarə olunmasının autentifikasiya alqoritmi.

2.1 Şəbəkə təhlükəsizliyi anlayışı

Kompüter şəbəkələrinin genişləndirilməsi ilə, internet vasitəsilə elektron müəssisələrin ortaya çıxması və internet vasitəsilə ticarət yayılması ilə, kompüter şəbəkələri hücumlara qarşı zəifliyi göstərməyə başladı.Şəbəkələrdə bu zəifliklər məhsul itirilməsi və şirkətlərə ciddi ziyan vurulması ilə nəticələnir.İnternet şəbəkəsi fərdi və ya iş münasibətləri arasında informasiya axını təmin edən və tənzimləyən bir əlaqə vasitəsi halına gəldi.İnternetdə informasiya itkisi və ya gizlilik pozuntuları ola bilər.İnternetdə belə təhlükəsizlik boşluqları istifadəçiləri internetdən istifadə zamanı daha diqqətli olmaları məcburiyyətinə gətirir.Bu web-based şirkətlər üçün böyük bir riskdir.Belə təhlükəsizlik zəifliklərinə qarşı tədbirlərin görülməsi şəxsi istifadəçilər və şirkətlər üçün ön plana çıxmışdır.Bütün kabel və simsiz kompüter şəbəkələri gündəlik istifadə üçün vacibdir.Kompüter sənayesində çalışanların əksəriyyəti kompüterdə vaxtlarını keçirirlər.Eyni zamanda fərdlər və təşkilatlar elektron poçt, redaktə, fayl idarə edilməsi və hesablama, eləcə də bu sektorda işləyənlər digər bu kimi müxtəlif funksiyalar üçün kompüterlər və şəbəkələrdən istifadə edirlər.Təhlükəsiz boşluğu olan şəbəkədə icazəsiz şəxsin hücumu yüksək qiymətli şəbəkə fasilələrinə səbəb ola bilər.Bəd niyyətli istifadəçilər, proqram zəifliklərı, istifadəçi adı və istifadəçinin şifrə proqnozlaşdırılması və fiziki risklər kimi aşağı səviyyəli texniki üsullardan istifadə etməklə şəbəkəyə asanlıqla daxil ola bilər. İnformasiya oğurluğu qorunan şəbəkə məlumatlarını əldə etmək üçün icazəsiz şəbəkə sızmasının olduğu bir hücumdur.Bir təcavüzkar daha əvvəl bir server və ya kompüterdə identifikasiyası üçün oğurladığı məlumatları istifadə edə və fayllarda saxlanan məlumatları oxumağa başlaya bilər.Bu cür məlumatın oğurlanması ölkəmizdə cinayət kimi

qadağandır.Qeydiyyatdan keçmiş məlumatların oğurlanması,kompüter istifadə edərək iqtisadi fırıldaqçılıq,məlumat və ya şəbəkələrin təxribatı Azərbaycan Respublikası qanunvericiliyində cinayət qəbul edilməkdədir.

Kimlik Oğurluğu

Kimlik oğurluğu şəxsin razılığı olmadan şəxsi məlumatların alınmasıdır. Kimlik oğurluğu kredit kartı nömrəsi, sürücü lisenziya nömrəsi, vətəndaşlıq nömrəsi, İnternet bankı məlumatı, e-poçt şifrəsi parolunu və digər mühüm şəxsi məlumatları əldə etmək üçün istifadə edilən fırıldaqçılıq növüdür.Konstitutsiyaya görə bu bir cinayətdir.

Şəkil 3.8 Kimlik saxtakarlığı

Məlumat itkisi

Verilən məlumatlar istifadə edilən fərdi kompüterlərdə elektron mühitdə saxlanılır. Bu məlumatların əlçatmazlığı və ya olmaması məlumatların itirilməsi adlanır. Məlumatlar şəbəkə kompüterlərində saxlanıla və ya başqa yerə kopyalana bilər. Bəd niyyətli insanlar gizli şəkildə rabitəni izləyə və ya göndərilən məlumat

paketini dəyişdirə bilərlər. Bunu bir çox metoddan istifadə edərək reallaşdıra bilərlər. Məsələn, informasiya ünsiyyətində alıcının IP nömrəsini istifadə edərək, göndərilən məlumatı alıcı olduğu kimi istifadə edə bilərlər.

Xidmət pozulması

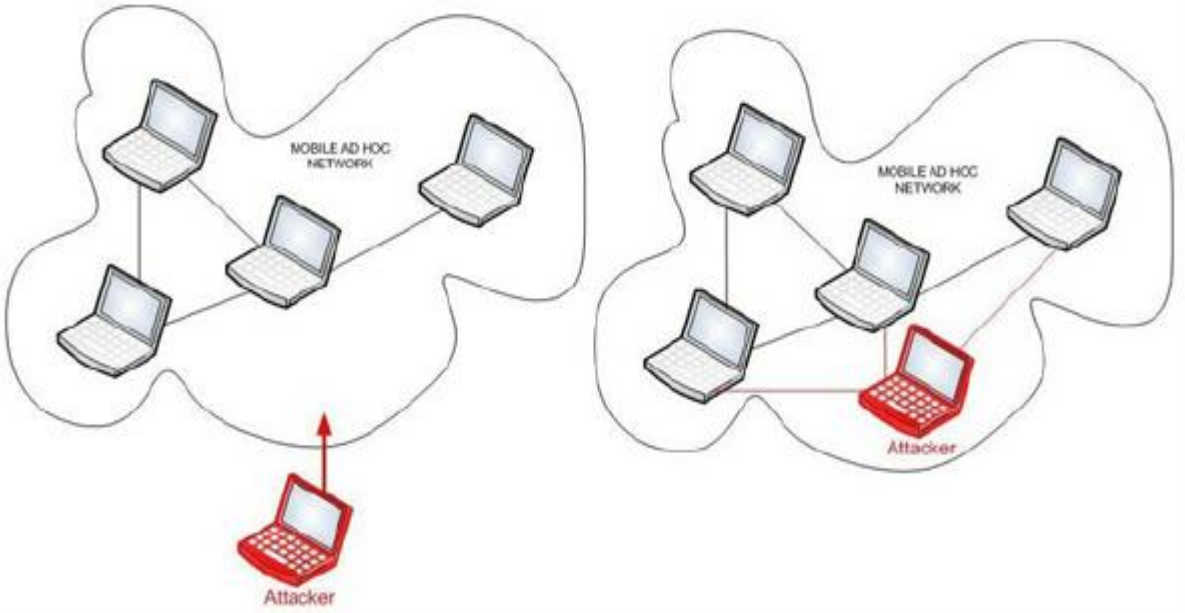
Bu, istifadəçilərin fərdi və ya müəssisələrdəki qanuni hüquqlarından istifadə etməsinin qarşısını almaq kimi müəyyən edilə bilər. Şəbəkə istifadəçisi istifadəçi adı və şifrəni istifadə edə bilmir və istifadəçilər veb xidmətinə qoşula bilmirlər.

Şəbəkə təhlükəsizliyi təhdidləri

İnformasiya texnologiyalarının inkişafı istifadəçilərə böyük rahatlıq təmin edir, eyni zamanda onlara bir çox təhdidlər gətirir. Rabitə şəbəkələrində olan zəifliklər şəxsi məlumatları istifadəçilər sisteminin ələ keçirilməsindən və böyük firmaların gizli məlumatlarının əldə edilməsindən və maddi mənfəət qazanmasından kənara çıxmağa başladı. Şəbəkənin inkişafı ilə şəbəkə tətbiqi də gözlənilmədən genişlənmişdir. Şəbəkənin idarə edilməsi və şəbəkə təhlükəsizliyi şəbəkə qurulduqdan və istifadəyə verildikdən sonra əhəmiyyət qazanmışdır. Şəbəkə, bugünkü texnologiyanın qurulması və istismarı ilə tamamlanmadığından, əsas iş şəbəkənin icra və etibarlılığını təmin etməkdən ibarət olmağa başlayıb. Ümumiyyətlə, şəbəkə quruluşuna edilən hücumların əksəriyyəti daxili şəbəkədən gəlir. Şəbəkə kompüter tərəfindən verilən xidmətdən asılı olaraq müxtəlif hücumlara məruz qala bilər və fərqli hücum növləri təhdid təşkil edə bilər. Şəbəkə üzərindəki hücumlar sistem və proqram təminatına yönəldilə bilər. Sistem təminatına olan hücumlarda hədəf məlumat saxlama qaynaqları və şəbəkə qurğuları ola bilər. Proqrama hücumlar isə istifadəçi məlumatlarına çıxış təmin etmək üçün ola bilər. Potensial hücum mənbələri modemlə və ya digər çıxış vasitəsilə İnternet bağlantısı sahəsində kompüterin birləşdiyi genişzolaqlı şəbəkə üzərindən ola bilər.

Xarici və Daxili Təhlükələr

Xarici təhdidlər şəbəkədən kənarda çalışan istifadəçilərdən gəlir. Bu insanlar kompüter sistemlərinə və ya şəbəkələrə giriş icazəsinə malik deyillər. Xarici təcavüzkarlar adətən internet üzərindən şəbəkə hücumlarını, simsiz şəbəkələrdən və ya dial-up məlumat serverlərindən keçirirlər. Bu hücumlar maddi və mənəvi zərərlərə gətirib çıxarır və təhlükəsizliyi onların qarşısını almaq üçün təhlükəsizliyi artırmaq mütləqdir.



Şəkil 3.9 Daxili və Xarici hücum

Daxili təhlükələr;

İstifadəçi öz hesabı vasitəsilə və ya şəbəkə avadanlıqlarına fiziki çıxışı olduqda şəbəkəyə icazəsiz daxil olduqda baş verir. Daxili təcavüzkar prinsipləri bilir və fərdləri tanıyır. Bu insanlar adətən hansı məlumatın daha həssas olduğunu bilirlər.Amma daxili hücumlar həmişə qəsdli şəkildə olmayacaqdır.Bəzi hallarda təhlükəsizlikdən xəbərsiz olan bir işçinin daxili şəbəkə üçün risk törədə biləcək virusa yoluxması və ya xarici sızma üçün vasitə olması halları da müşayət olunur.

Sosial mühəndislik

Sosial mühəndislik, insanların ünsiyyətində və insan davranış modellərini açıq olaraq tanıma və bundan istifadə edərək təhlükəsizlik proseslərinin aradan

qaldırılması üsuluna əsaslanan müdaxilələrə verilən adadır. Sosial mühəndis, istifadəçiyə şifrəsini sistem cavabdehi olduğunu söyləyərək və ya bir texnik olduğunu deyib fiziki olaraq içəri sızan ya da zibil qutularını qarışdıraraq məlumat toplamaqla məlumatları əldə edə bilər. Təşkilatın işçiləri öz şəxsiyyətlərini sübut etməyən şəxslərə məlumat verməməlidirlər və həmçinin iş həyatını və şəxsi həyatı fərqləndirməlidirlər. Müəssisə siyasətində belə hallarla əlaqədar lazımi xəbərdarlıq və tədbirlər görülməlidir.

Şəkil 4.0 Sosial mühəndislik

Məlumatın toplanması,əlaqələrin qurulması və nəhayət istismar etmək. Sosial Mühəndislik, şübhəsiz ki, bir anda baş verməyən bir vəziyyətdir. Bunları etmək və digər tərəfdən aldatmaq və ya inandırmaq üçün xüsusi addımları və yolları tətbiq edirlər.Aşağıdakı addımlara baxaq:

- Məlumat Toplama: Birincisi, aldadılacaq qurban haqqında məlumatın maksimum səviyyəsi toplanır və bir çox xüsusiyyətlər araşdırılır. Əldə edilən məlumat şirkətin veb saytları, digər nəşrlər və hədəf sistemində işləyən işçilər vasitəsilə toplanır.

- Hücum Planı: Hücumçular hücumu necə yerinə yetirmək istədiklərini izah edirlər.
- Hücum Vasitələri: Hücumun başlanması zamanı təcavüzkarın istifadə edəcəyi kompüter proqramları daxildir.
- İnformasiyanın istifadəsi: Təşkilatın təsisçilərinin doğum tarixləri kimi bir çox sosial mühəndislik taktikası zamanı toplanan məlumatlar parol təxminləri üçün istifadə edilə bilər.

Şəkil 4.1 Sosial mühəndislik (2)

Sosial mühəndislərin bacarıq tələbləri aşağıdakılardır:

- İnandırıcılıq bacarıqları inkişaf etmiş olmalıdır.
- Yüksək təsir xüsusiyyətlərinə malik olmalıdırlar.
- Onlar aldatmaqdan çəkinməzlər.
- Digər tərəfə məlumatlı olduğunu göstərmək bacarığı.
- Sennarilər istehsal qabiliyyəti olduqca yüksək olmalıdır.

Sosial mühəndislikdə ən çox istifadə edilən üsullardan biri phishingdir, buna görə də bir azda phishing haqda danışaq.

Phishing,kredit kartı və bank hesabı nömrələri,şifrə və İnternet istifadəçilərinin ŞV nömrələri kimi həssas məzmun əldə etmək üçün təcavüzkarın sosial mühəndislik hücumudur.Phishing hücumlarında, istifadəçi saxta bir e-poçt ilə sıxışdırılır. Təcavüzkar hədəflənmiş məlumatlara çatmaq üçün məhşur firma və bank adlarına bənzər saxta adlar istifadə edərək məqsədinə çatmağa çalışır.Zərərli şəxs adətən bankın kimliklərini istifadə edərək hədəf istifadəçiyə bir məktub göndərir. Göndərilən məktubun məzmunu sistemin yeniləmələri və ya təkmilləşdirilməsi səbəbindən istifadəçi tərəfindən verilən ünvana daxil edilməlidir. Poçt vasitəsilə ötürülən ünvan ID istifadə olunan təşkilatın dəqiq sürətidir. Şəxs bu sayta real bir sayt olaraq daxil olduqda və məlumat yazılırsa, bütün məlumatlar indi zərərli şəxsin əlinə keçmiş olacaqdır.

Bu hücumdan necə qorunmaq olar?

- Etibarlı mənbələr məlumat istəmirlər: Müştərilərinizin məlumatınıza ehtiyacı yoxdur. İstifadəçi adı və şifrənizi poçt və ya saytlar vasitəsilə tələb edən əlaqələrə diqqət etməyin.
- Tanılamadığınız e-poçtları oxumayın və silməyin: Bilməyən insanlar və ya təşkilatlar tərəfindən göndərilən e-poçtları silin. Bu cür mailler bir phishing hücumu ola bilər.
- Ünvanı yoxlayın: Phishing hücumlarında ən mühüm amillərdən biri brauzerdəki ünvanı yoxlamaqdır. Bir xarakter dəyişməsi gözlənilməz nəticələrə gətirib çıxara bilər.
- Təhlükəsizliyi yoxlayın: Banklar, alış-veriş saytları və HTTPS təhlükəsizliyi protokolu kimi istifadəçi məlumatları transfer prosesində istifadə olunur. Bu protokoldakı məlumat ötürülməsi şifrələnir və təhlükəsizlik yüksək səviyyədədir.

- Bank hesabınızı yoxlayın: Periodik olaraq mailinizi yoxlayın. E-poçt ünvanınıza göndərilən e-poçtları silməyin və Whois verilənlər bazasından ünvanın yerləşdiyi sayt haqqında məlumat toplayın.

Şəkil 4.2 Phishing

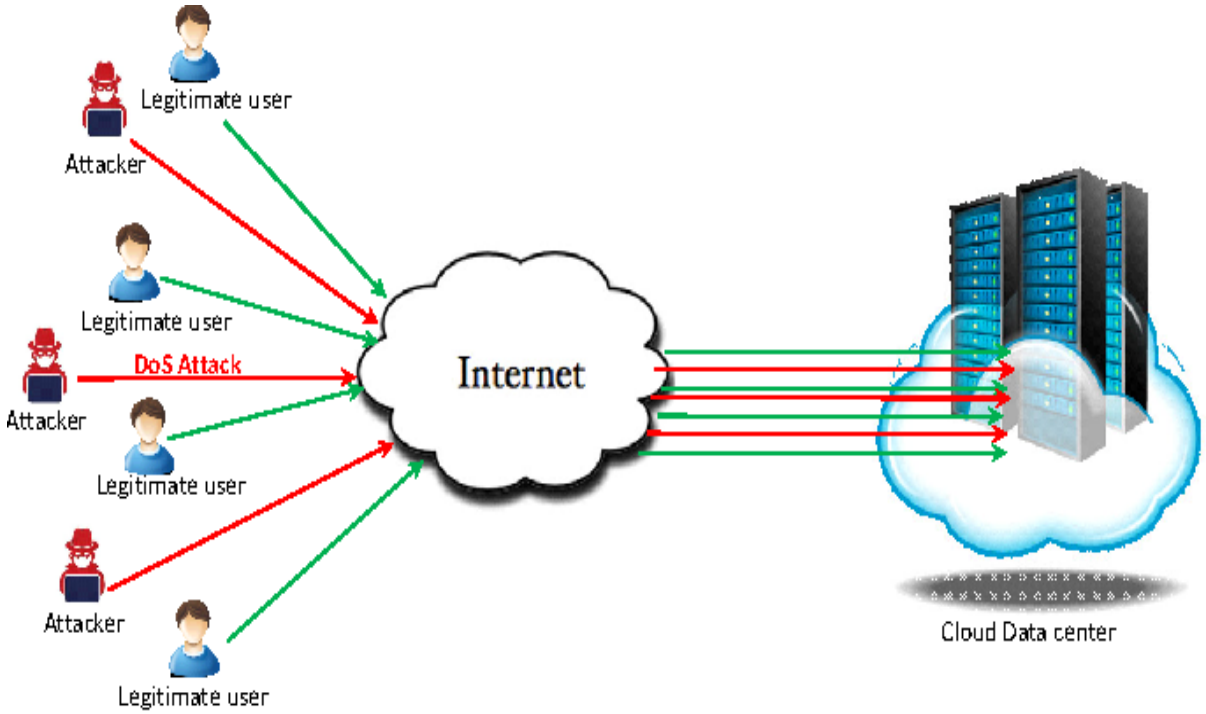
Denial of service–DoS (Servisin sıradan çıxarılması)

Bu hücum fəaliyyətdə olan önəmli servislərin fəaliyyətinə əngəl yaratmaq üçün sistemə ardıcıl paketlər göndərilir.Sistemə müntəzəm və davamlı hücumlar nəticəsində sistem xidmətə göstərməkdən imtina edir və iflic duruma düşür. DoS hücumları ilə hədəf sisteminə aid resursları istehlak etmək də nəzərdə tutulur. Bu hücum, çox əhəmiyyətli serverlərin xidmət xaricində olduğu kimi problemlərə yol açа bilər. DoS hücumları iki mərhələdən ibarətdir:

- DoS hücum zamanı hücum edən sistemlər hazırlanır və ələ keçirilir.Lazımi proqramlar bu sistemlərdə quraşdırılır.
- Hazır olan sistemlərlə hədəf sistemi hücum edilir.

Dos hücum növlərinin bəziləri bunlardır:

- Buffer overrun: Bir sistem tərəfindən qarşılanmayan bir trafik göndərməklə bir yayınma durumudur.Yaddaş serverləri yaddaşda eyni məlumat şəklində saxlanılan yaddaş blokudur. Bu ən yaygın hücum formasıdır.
- SYN hücumları: Bu hücum tipində təcavüzkar bir çox SYN paketini hədəf maşına İnternetdə istifadə edilməyən IP ünvanlarını istifadə edərək göndərir. Hədəf maşın hər bir qəbul edilmiş SYN paketi üçün resursları ayırır və SYN paketinin gəldiyi IP ünvanına bir təsdiq paketi (SYN-ACK) göndərir. Hədəf maşın SYN-ACK paketini bir neçə dəfə təkrar edir, çünki istifadə edilməmiş IP ünvanından cavab ala bilmir. Təcavüzkar bu üsulu yuxarıya tətbiq edərkən hədəf maşın ayırdığı resurslara görə yeni bir əlaqəni yaratmağa imkan vermir və maşına fəaliyyətsiz qalır.
- Treadrop hücumları: İnternet üzərindən bir kompüterə çatan paketlər onları kompüterə bölməklə ötürülür. Paket məlumatlarını təhlil edərkən paketlərdə ofsetlər istifadə olunur. Bu ofset məlumatları üst-üstə düşməməlidir. Teardrop hücumlarında göndərən paket paketin üstünə göndərir. Paketi alan kompüterdə belə bir vəziyyətə nəzarət edə bilən mexanizm yoxdursa, sistem çökər.
- Smurf hücumları: Bu cür hücumda, təcavüzkar hədəf kompüteri ping edəcək. Lakin, ping paketi hədəf maşının IP ünvanından gələn kimi görünəcək. Bu vəziyyətdə, hədəf maşın şəbəkənin bütün maşınları tərəfindən pingə məruz qalacaq. Beləliklə hədəf maşın bu trafikə cavab verə bilmir və əlaqə itirilmiş olur.
- Aşırı yükləmə xidməti: Bu hücum növü müəyyən istifadəçiləri və xidmətləri azaltmaq üçün istifadə olunur. Təcavüzkar istifadəçi üçün xüsusi bir port və bir çox ICMP paketini (Internet Control Message Protocol) göndərir. Bu hadisə şəbəkə monitoru ilə asanlıqla başa düşülür.



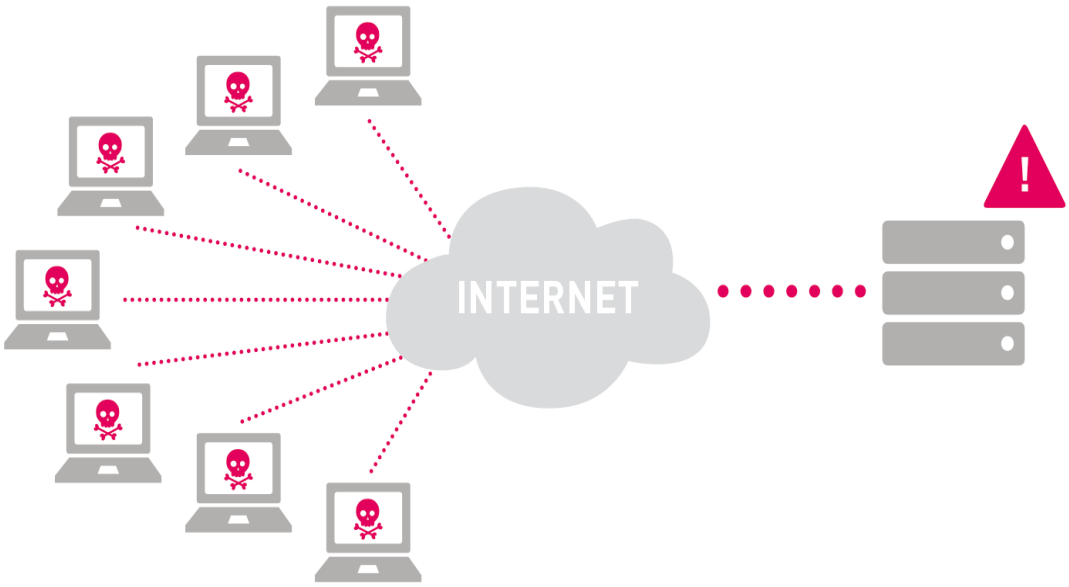
Şəkil 4.3 DoS Attack

Dos hücumlarından özünüzü qorumaq üçün iki yol var:

- Bant genişliyi hücumları və qorunma metodları: Bu tip hücumlar DoS hücumlarını müdafiə etmək üçün ən çətindir, buna görə hücumlara səbəb olan paketlər təhlükəsizlik tələb olunduğu sistemin girişinə daxil olmadan bu paketləri qəbul etməyini dayandırmalıdır. Şəbəkə daxilindən qabaq paketlərin bağlanması üçün eyni növ paketlərin TCP SYN, UDP və ya ICMP kimi izləmə və nəzarət etməyə imkan verən proqram təminatı quraşdırmaq lazımdır.
- Sistem və xidmət hücumları və qorunma üsulları: Bu növ hücumlar bütün şəbəkə deyil, bir və ya daha çox sistemə qarşı yönəldilmişdir. Bu hücumlar, vahid vaxt başına çox sayda paket göndərilərək, yaddaşda problem yaradan və çox sayda etibarlı istək göndərməklə həyata keçirilə bilər.Standart olaraq, şəbəkə kartı hər dəfə paket qəbul edildikdə prosessor üçün sorğu yaradır. İşlemci, bu paketin ağ kartından alınması üçün müəyyən bir zaman alır. TCP SYN paketləri SYN ACK paketləri cavab olaraq göndərilmədən bir qədər

vaxt keçməlidir. Eynilə, TCP, UDP və ICMP paketləri SYN-ə qədər vaxt vermir, lakin hələ müəyyən bir müddətə səbəb olur. Bununla yanaşı, paketlərin ölçüsü və sayı bant genişliyində baş verə biləcək problemlərə böyük təsirə malikdir.

Bəzi hallarda maşın sahibinin razılığı ilə Ddos hücumunun bir hissəsi ola bilər. Bunun bir nümunəsi 2010-cu ildə WikiLeaks tərəfdarları tərəfindən böyük kredit kartı şirkətlərinə qarşı təşkil edilən Ddos hücumudur. Belə hallarda axış tərəfdarları Ddos proqramını quraşdırmaq və idarə etmək üçün icazə verilir. MyDoom'un Ddos mexanizmindən fərqli olaraq hər hansı bir IP ünvanı ona qarşı çevrilə bilər.Tanınmış veb-saytların mövcud istifadəsini qanuni istifadəçilərdən məhrum etmək üçün istifadə edir. Daha qabaqcıl təcavüzkarlar, DDOS vasitələrini qəsb etmək üçün istifadə edirlər. DDoS hücumu (Distributed Denial of Service hücumu) birdən çox sistem,sistemin resurslarını və ya bant genişliyini hədəfləyərkən baş verir, bu da adətən bir və ya daha çox web serveridir. Bu sistemlər təcavüzkarlara müxtəlif üsullardan istifadə etməyə şərait yaradır.



Şəkil 4.3 DDoS Attack

Spam

E-poçt tələb edilmədikdə və insanlara bu elektron poçta zorla göndərildikdə, bu spam adlanır. Spam, adətən, kütləvi və ya kommersiya məqsədi ilə ola bilər.Satıcılar bəzən hədəflənən marketinqlə məşğul olmaq istəmirlər. E-poçt reklamlarını mümkün qədər çox son istifadəçiyə göndərmək istəyir, onun məhsulları və ya xidmətlərinin birinə maraqlı olmasını ümid edir.Spam,internet xidmət provayderini, e-poçt serverlərini və fərdi son istifadəçi sistemlərini daha çox yükləyə biləcək ciddi bir şəbəkə təhdididir. İndiyə qədər hər bir istifadəçinin hər il 3000-dən çox spam e-poçtu qəbul etdiyi təxmin edilir. Spam böyük miqdarda internet bant genişliyi istehlak edir və bu gün bir çox ölkələrin spam istifadəsi haqqında qanun qəbul etməsi üçün ciddi zərurət var. Spam, ev kompüterlərini idarə etmək üçün viruslar, qurdlar və trojan atları kimi proqram texnikalarını istifadə edir. Bu kompüterlər sonra sahibinin məlumatı olmadan spam göndərmək üçün istifadə edilə bilər. Spam e-poçt və ya ani mesajlaşma proqramı vasitəsilə göndərilə bilər. Əlbəttə ki, spam gəldikdən sonra, hadisə başa çatmır, spam alan şəxs SPAM göndərənlər tərəfindən birbaşa izlənilir.

2.2 Korporativ şəbəkələrdə istifadə olunan authentifikasiya və kriptologiya mexanizmləri

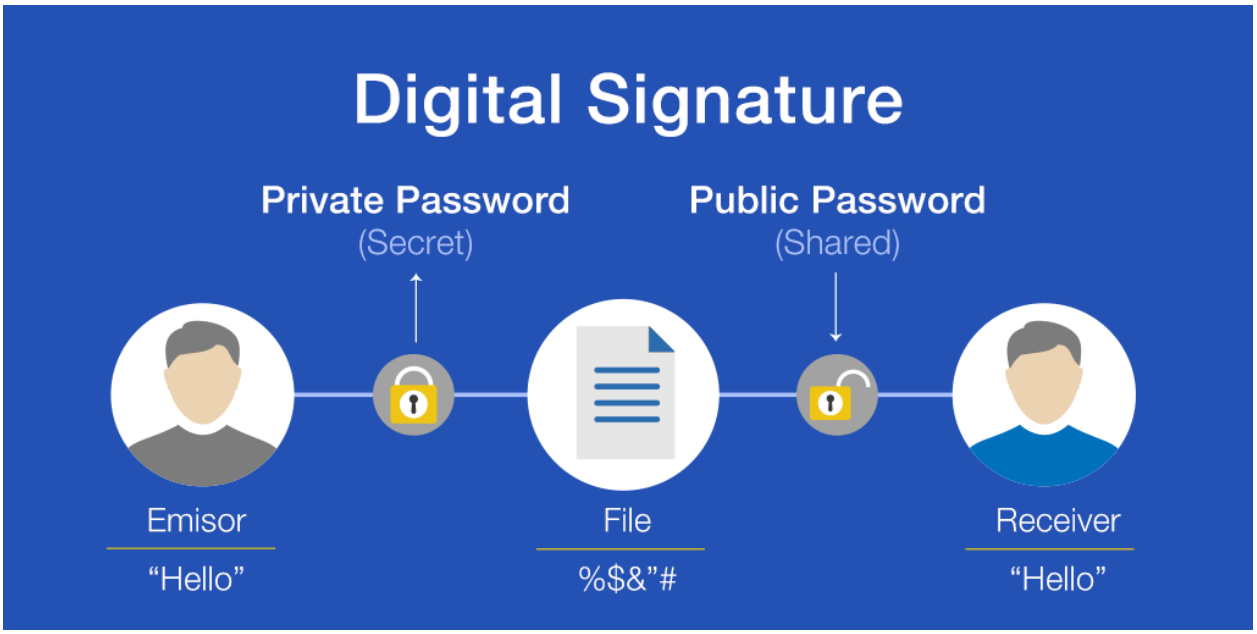
Authentifikasiya

Bu məlumatların təhlükəsizliyində istifadə olunan məsələdir. Sadəcə bir istifadəçi və ya proqramın bir sistemə daxil olmağı və ya girəcəyi təqdirdə nə qədər iş edə biləcəyini müəyyən edən quruluşdur. Sadə mənada cib telefonlarında və ya demək olar ki, hər bir qapının kilidlərində istifadə olunan və bu kilidləri açan açarlarda istifadə edilən PIN (şəxsi şəxsiyyət nömrəsi) etibarlı bir icazə kimi qəbul edilə bilər. Qapını açmağa icazə verən şəxs qapı açan açarı daşıyan şəxsdir. Məsələn, ATM maşınından pul çəkmək istəyən bir şəxsə icazə vermək üçün həm həmin kartın debet kartına, həm də paroluna malik olmalıdır. Bu halda, kart və parol cütü icazə üçün istifadə olunur. Kompüter elmində istifadə edilən məlumatların təhlükəsizliyi baxımından üç növ səlahiyyət verilə bilər:

- Parol
- Elektron imzalar
- Rəqəmsal Sertifikatlar

Rəqəmsal imza bir məlumat mənbəyini təsdiqləyərkən istifadə edilə bilər. Beləliklə, tam istifadəçinin gözlənilən şəxs olduğuna əmin ola bilərsiniz. Rəqəmsal imza sadəcə bir şəxsin assimetrik şifrələmə (ümumi açar şifrələməsi) istifadə edərək gözlənilən şəxs olduğunu təmin edir.Bunu etmək üçün ictimaiyyətə verilən bir parol (məsələn, İnternet vasitəsilə) alınır və məlumatı həmin mənbədən açmaq üçün istifadə olunur. Mənbədən verilən məlumatlar artıq səlahiyyətli şəxsin şəxsi açarı ilə şifrələndiyindən, yalnız istifadəçinin real ictimai açarı ilə bu şifrə açа bilməlidir. Məsələn, istifadəçi sistemə giriş üçün tələb olunan şifrəni öz şəxsi açarı ilə asimmetrik şifrələmə üsulu ilə şifrələyir. Şifrəli məlumatları serverə göndərir və sistemə giriş tələb edir.Server, istifadəçiyə açıq olan ictimai açarı istifadə edərək

şifrəli bir parol açmağa çalışır. Aldığınız dəyər serverdəki parolla eyni olsa, istifadəçi icazə verilir və sistemə giriş imkanı verilir.



Şəkil 4.4 Rəqəmsal İmza

Yuxarıdakı rəqəmdə göstərildiyi kimi istifadəçinin ictimai açarı və istifadəçinin səlahiyyət məlumatları ayrıca icazə sisteminə göndərilir. Bu iki məlumatdan istifadə edərək sistem istifadəçinin avtorizasiya məlumatlarına çatır və bu məlumatı sistemdə olan məlumatlarla müqayisə edir. Hər hansı bir təcavüzkarın sistemə sızması üçün sistemdə icazə verilən ictimai açardan gizli saxlanılan xüsusi açarı əldə etməsi lazımdır. Bu proses asimmetrik şifrələmə metoduna görə dəyişir, baxmayaraq ki, bu, adətən çətin və vaxt aparan bir prosesdir.

Elektron imzalar aşağıdakı hallarda istifadə olunur;

- Məlumatın doğru mənbə tərəfindən yaradıldığını sübut etmək üçün,
- Şəxsi açarı və imzanı istifadə edərək istifadəçi kimliyini təsdiq etmək üçün,
- PKI sertifikatlarının etibarlılığı və bütövlüyünü sübut etmək üçün,
- Təhlükəsiz vaxt mənbəyindən etibarlı bir zaman damgasını təmin etmək.

Rəqəmsal imzalar üç növ təhlükəsizlik xidməti təklif edir;

1. İmzalanmış məlumatların etibarlılığı
2. İmzalanmış məlumatların bütövlüyünün qorunması
3. İmza surətinin qorunması

Rəqəmsal imza üçün yuxarıda göstərilən xidmətləri təmin etmək üçün lazım olan bəzi xüsusiyyətlər aşağıdakılardır:

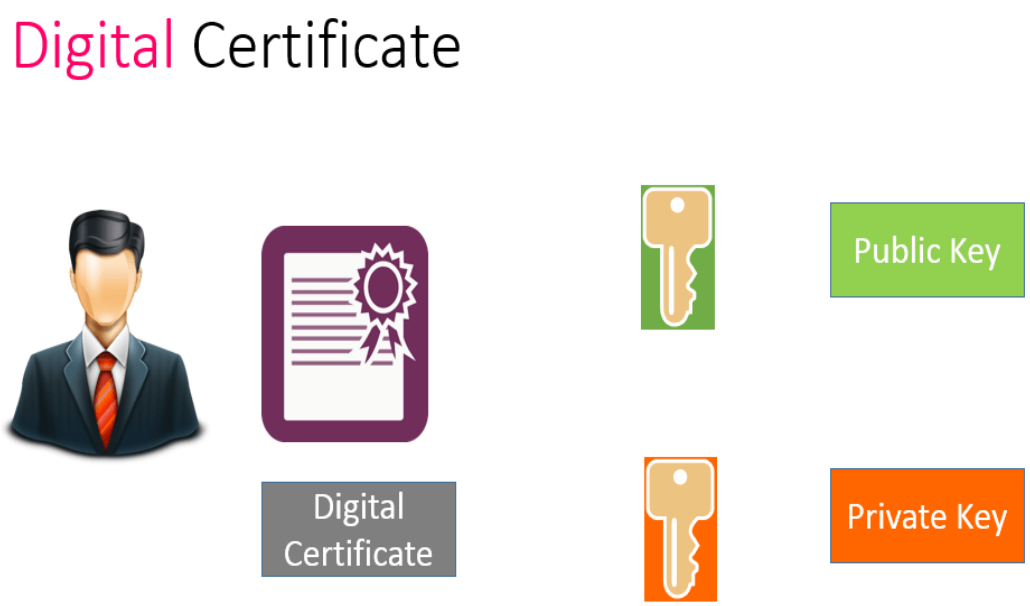
- İmza təhlükəsiz və təkrarsızdır. Sənədin imzalanması imzalayanya aiddir (başqası deyil).
- İmza hər sənəd üçün ayrı olaraq istehsal olunur və yenidən istifadə edilə bilməz.
- Sənəd imzalanandan sonra yenidən dəyişdirilə bilməz.

Rəqəmli imza bəzi ölkələrdə normal imzaya bərabər tutulur. Bu şərtlərin başında sertifikat orqanlarının təhlükəsizliyi gəlir. Cisco və Microsoft kimi şirkətlər də bəzi cihazlarında rəqəmsal imza istifadə edirlər. Rəqəmsal imza prosesi 6 addımda baş verir və hash funksiyasına əsaslanır.

1. İmzalayan sənədin haşını yaradır.
2. Alınan məlumatlar xüsusi bir şifre ile şifrelenir.
3. Şifrələnmiş hash (imza) sənədə əlavə olunur və təyinatı üzrə göndərilir.
4. Hədəf imzalanmış sənədi alır və əlavə olaraq resursun ictimai əsasını alır.
5. İctimai açarı istifadə edərək, şifrəli sənədin kodunu çıxarır. Beləliklə, mənbənin haşı əldə edilir.
6. Hədəf sonra orijinal sənədin haşını yaradır və mənbədən hash dəyərini müqayisə edir. Haşımın dəyəri uyğun olarsa, sənədin etibarlı olduğu

və yol boyunca eyni qaldığı aydın olur və mənbə düzgünlüyü doğrulanır.

Sertifikatlar, avtorizasiya zamanı istifadəçinin gözlənilən şəxs olduğundan əmin olmaq üçün istifadə edilə bilər. Sertifikatlar şəxsi məlumat və parol hissələri ilə etibarlı mənbə (sertifikat orqanı) tərəfindən təsdiq edilmək üçün nəzərdə tutulub. Server istifadəçi təsdiq etməzdən əvvəl istifadəçi sertifikatını sertifikatlaşdırma orqanından tələb edir. Istifadəçinin ictimai açarı onu əldə etdiyi sertifikatla təsdiqləyir və icazə zamanı istifadəçinin məlumatını açır. Məlumat doğru olduqda sistem istifadəçi tərəfindən icazə verilir.



Şəkil 4.5 Rəqəmsal Sertifikat

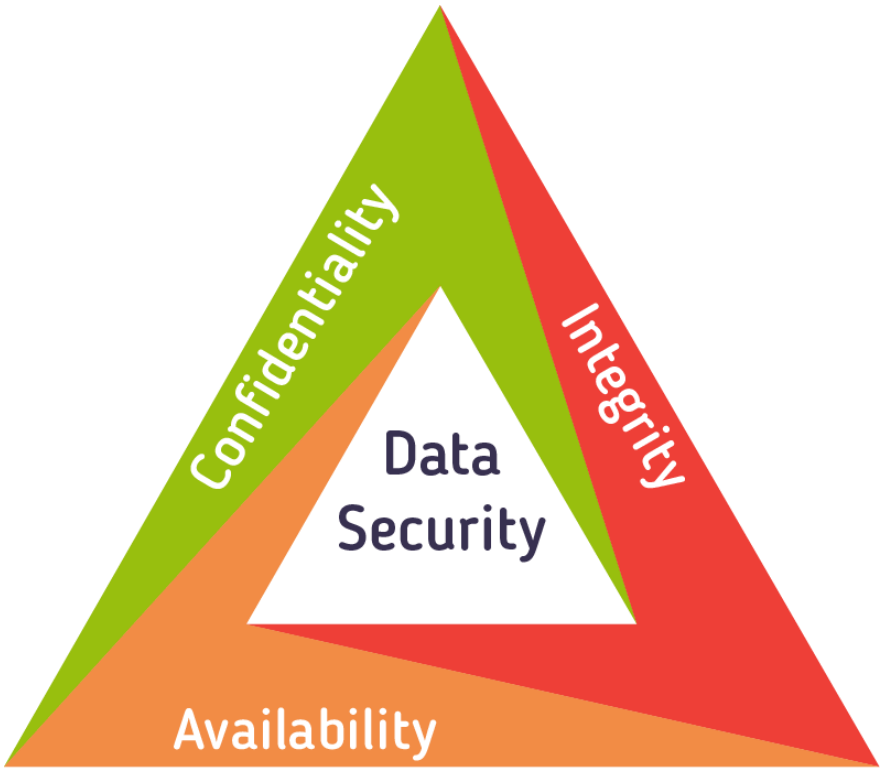
Certificate Authority: Qəbul edən və qəbul edən tərəflərdən kənarda üçüncü elementdir. İstifadəçinin sertifikatı CA tərəfindən təsdiqlənmişdir. Beləliklə, xidmət təminatçısının düzgün olduğundan əmin olunur. Bundan əlavə, hər bir CA öz imzası ilə sertifikat və ictimai açarı var.Bu sertifikata CA sertifikatı da deyilir.

2.3 Korporativ şəbəkələrdə informasiya tamlığının və məxviliyinin təmini üsulları

İnformasiya təhlükəsizliyi korporativ kompüter sistemlərinin təhlükəsiz istifadə olunmasını təmin edən bir sahədir və təşkilatların ən əhəmiyyətli aktivi olan "data/məlumat" bu sahə və onun mütəxəssisləri tərəfindən mühafizə olunur. İnformasiya təhlükəsizliyi; informasiya sistemlərinin əsas xüsusiyyətləri, şəbəkə xüsusiyyətləri və kommunikasiya texnologiyaları kimi yönləri özündə cəmləyir. Texniki məsələlərlə yanaşı, təşkilatlar informasiya təhlükəsizliyi barədə tam məlumatlı olmalıdır və təhlükəsizlik siyasəti yaratmalıdırlar. İnformasiya təhlükəsizliyi informasiya təhlükəsizliyini idarə edən İT mütəxəssisləri və keyfiyyətl mütəxəssisləri tərəfindən təmin edilir.

CİA üçlüyü;

CIA üçlüyü kimi tanınan gizlilik, bütövlük və mövcudluq, bir təşkilat daxilində informasiya təhlükəsizliyi siyasətinə istiqamətlənmiş bir modeldir. Modelin ad qısaltmasının Amerika Mərkəzi Kəşfiyyat Agentliyi ilə eyni olmasına görə qarışıqlığın qarşısını almaq üçün onu bəzən AIC üçlü modeli də (mövcudluq, bütövlük və məxfilik) adlandırırlar. Üçlünün elementləri təhlükəsizliyin ən mühüm üç hissəsi hesab olunur. Bu kontekstdə məxfilik informasiya əldə etməyi məhdudlaşdıran bir sıra qaydalardır, bütövlük məlumatın etibarlı və doğru olduğuna dair əminliyidir və mövcudluğu səlahiyyətli şəxslər tərəfindən məlumatlara etibarlı giriş təminatının mövcudluğudur.



Şəkil 4.5 CİA modeli

Confidentiality/Məxvilik:

Məxfilik gizliliyə təxminən bərabərdir. Məxfiliyin təmin edilməsi üçün həyata keçirilən tədbirlər, həqiqi məlumatların səhv insanlara çatmasını qarşısını almaq üçün nəzərdə tutulur və doğru insanları əslində əldə edə biləcəyinə əmin olmaq üçün nəzərdə tutulur.Verilənlərə giriş nəzərdən keçirmək səlahiyyətinə malik olanlara məhdud olmalıdır. Məlumatların istifadəyə yararsız hala düşməsi halında dəyə biləcək zərərin miqdarına və növünə görə məlumatlar təsnifləşdirilməlidirlər.

Bəzən məlumatların məxfiliyinin qorunması həmin sənədləri istifadə edəcək aidiyyatı şəxslərə xüsusi hazırlığın keçilməsi kimi təlimlərlə də təmin oluna bilər. Bu cür təlimlər adətən bu məlumatları təhlükə altına biləcək risklərin şəxslərə bildirilməsi kimi tədbirlər daxildir. Təlim, səlahiyyətli insanları risk faktorları ilə tanış etməyə və onlara qarşı necə qorunmağa kömək edə bilər. Təlimin digər aspektləri güclü parol və şifrələrlə bağlı məlumatlandırma,həmçinin sosial

mühəndislik metodları haqqında xəbərdar etmə və xaricdən ola biləcək hər çür dəhdidə qarşı istifadəçilərdə təsəvvür formalaşdırmaqdan ibarət hesab oluna bilər. Məxfiliyin təmin edilməsi üçün istifadə edilən metodların yaxşı bir nümunəsi, bankda online olduğunda bir hesab nömrəsi və ya marşrutlaşdırma nömrəsi almağınız saylıla bilər.Data şifrələməsi gizlilik təmin etmək üçün ümumi bir üsuldur. İstifadəçi identifikasiyası və şifrələri standart prosedur təşkil edir.İki faktorlu identifikasiya isə artıq bir normaya çevrilir. Digər variantlar biometrik yoxlama və təhlükəsizlik vasitələridir.Bundan əlavə, istifadəçilər məlumatın saxlandığı yerlərin sayını və tələb olunan əməliyyatı başa çatdırmaq üçün faktiki olaraq neçə dəfə ötürüldüyünə görə ehtiyat tədbirləri ala bilər. Həddindən artıq həssas sənədlər, tam müdafiəli kompüterlərdə, etibarlı məlumat saxlama qurğularında və ya yalnız kağız şəklində saxlanılması bu kimi tədbirlərə misal ola bilər.

Integrity/Tamlıq;

Integrity bütün həyat dövründə məlumatların tamlığını, düzgünlüyünü və etibarlılığını təmin edir.Məlumatların daşınma zamanı dəyişdirilməməli və məlumatların icazəsiz şəxslər tərəfindən dəyişdirilə bilməməsini (məsələn, gizlilik pozuntusu ilə) təmin edilməsi üçün addımlar atılmalıdır. Bu tədbirlər fayl icazələrini və istifadəçi giriş nəzarətini ehtiva edir. Versiyaya nəzarət istifadəçilər tərəfindən səhv dəyişikliklərin və ya təsadüfən silinmənin qarşısını almaq üçün istifadə edilə bilər. Bundan əlavə, elektromaqnit təsirlər (EMP) və ya server qəzası kimi qeyri-insani hadisələri nəticəsində baş verə biləcək hər hansı bir dəyişikliyi aşkar etmək üçün bəzi vasitələr olmalıdır. Bəzi məlumatlar bütövlüyünün yoxlanılması üçün yoxlamalar, hətta kriptoqrafik yoxlamaları özndə ehtiva edə bilər. Təsirə məruz qalan məlumatları düzgün vəziyyətinə qaytarmaq üçün ehtiyyat nüsxələrin mövcudluğu mütləq amildir.

Availability/Əlçatalıq;

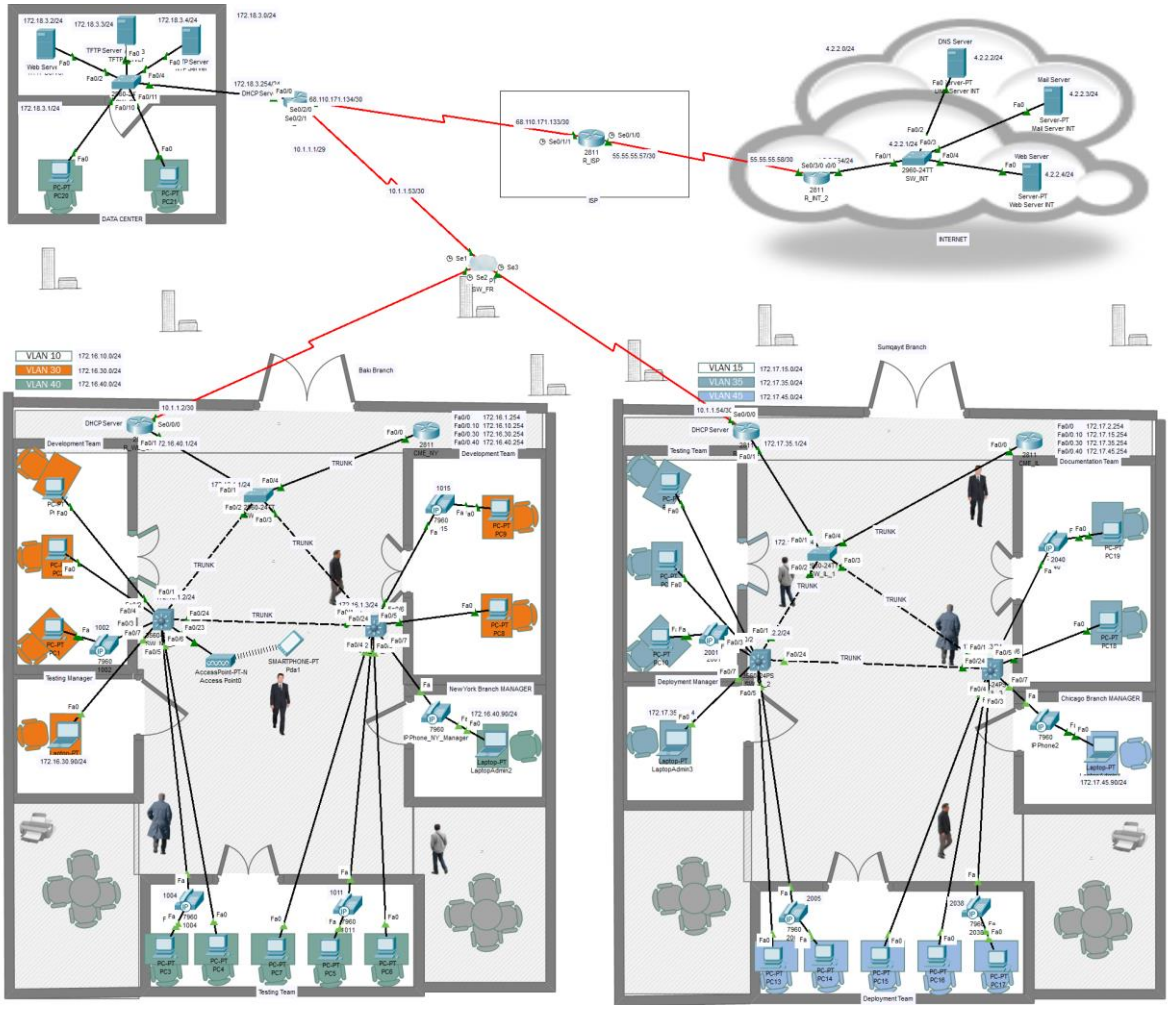
Mövcudluğun təmini bütün avadanlıqları qorumaq,lazım olduqda dərhal təmirini aparmaq və proqram xətalarından azad olan düzgün işləyən əməliyyat

sistemi mühitini təmin etməklə yaxşı təmin olunur. Bütün zəruri sistem yeniləmələri ilə sistemin təmin etmək vacibdir.Təcili kommunikasiya bant genişliyi təmin edilməsi və tıxacların qarşısının alınması eyni dərəcədə vacibdir. Təkrarlıq, yerinə yetirmə, RAID hətta hardware problemləri meydana gəldikdə ciddi nəticələrə gətirib çıxara bilər. Məlumatın itirilməsinə və ya əlaqələrdə kəsilmələrə qarşı qorunması təbii fəlakətlər və yanğın kimi gözlənilməz hadisələri ehtiva etməlidir. Belə hadisələrdən məlumatların itirilməsini maneə törətmək üçün ehtiyat nüsxə coğrafi cəhətdən izolyasiya edilmiş bir yerdə, hətta yanmaz, suya davamlı şəkildə saxlanıla bilər. Əlavə təhlükəsizlik avadanlıqları və ya firewall-lar və proxy serverləri kimi proqram və cihazlar, xidmətdən imtina (DoS) hücumları və şəbəkə müdaxilələri kimi zərərli müdaxilələrdə sistemi və onun həssas nöqtələrini qoruya bilər.

III Fəsil.Eksperimental tədqiqatların keçirilməsi metodikası.

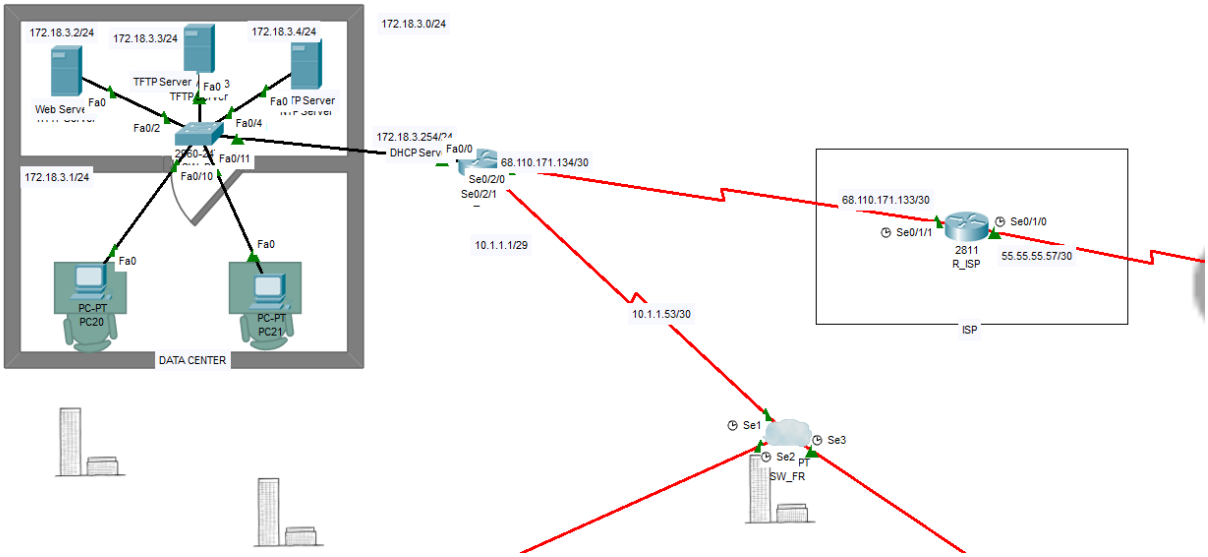
3.1 Korporativ şəbəkə modelinin şəbəkə simulyatorunda formalaşdırılması

Bu fəsildə biz bura qədər sadalanan nəzəri məlumatlardan istifadə etməklə nəzəri billikləri praktikada tətbiq edəcəyik.Cisco şirkətinin virtual şəbəkə modelinin təşkili üçün şəbəkə administratorlarının istifadəsinə verdiyi cisco packet tracer simulyatoru bu işdə bizim əsas alətimiz olacaq.Quracağımız Şəbəkə 3 fərqli cografi ərazidə olan filialdan təşkil olunub.Bu filiallar şərti olaraq Bakı filialı,Sumqayıt filialı və DataCenter-dir.Şəbəkənin ümumi görünüşü aşağıdakı kimidir.



Şəkil 4.6 Korporativ şəbəkənin tam topoloji quruluşu.

Hər üç filial (bakı filialı,sumqayıt filialı və məlumat mərkəzi) frame relay sviçinə qoşulub.Məlumat mərkəzində olan router isə internet provayderlə əlaqələnib.Default route birbaş provayder routerinə istiqamətlənib.İnternet çıxışı buradan təmin olunur.



Şəkil 4.7 Default route

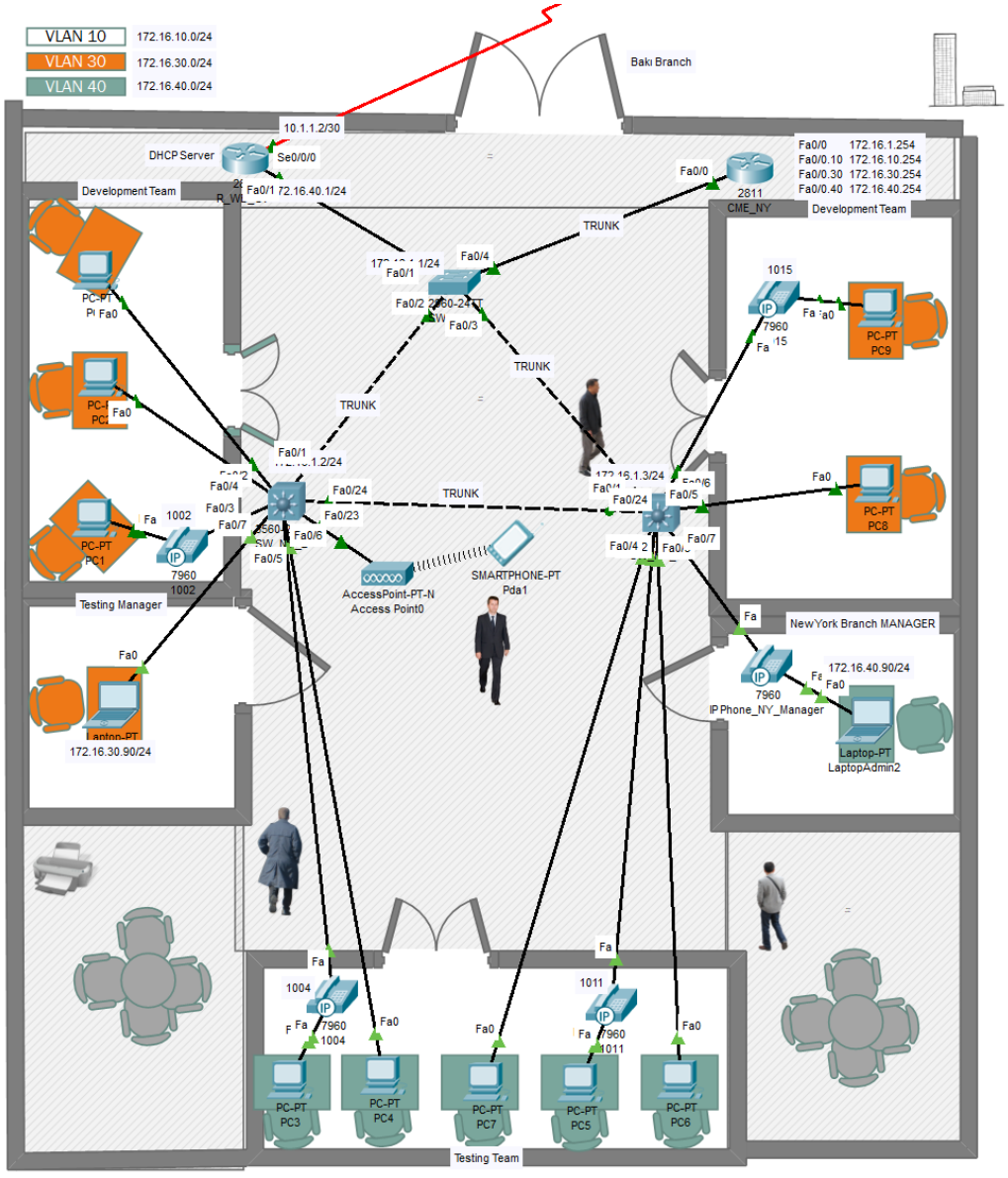
R_DC adlı router bizim məlumat mərkəzi ilə İSP (provayder) arasında internet çıxışını təmin edir və bu routerin routing cədvəli aşağıdakı kimidir.

```
R_DC#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 68.110.171.133 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/2/1.102
C       10.1.1.52 is directly connected, Serial0/2/1.103
     68.0.0.0/30 is subnetted, 1 subnets
C       68.110.171.132 is directly connected, Serial0/2/0
     172.16.0.0/24 is subnetted, 4 subnets
D       172.16.1.0 [90/2174976] via 10.1.1.2, 00:13:58, Serial0/2/1.102
D       172.16.10.0 [90/2174976] via 10.1.1.2, 00:13:58, Serial0/2/1.102
D       172.16.30.0 [90/2174976] via 10.1.1.2, 00:13:58, Serial0/2/1.102
D       172.16.40.0 [90/2172416] via 10.1.1.2, 00:13:59, Serial0/2/1.102
     172.17.0.0/24 is subnetted, 4 subnets
D       172.17.2.0 [90/2174976] via 10.1.1.54, 00:13:59, Serial0/2/1.103
D       172.17.15.0 [90/2174976] via 10.1.1.54, 00:13:59, Serial0/2/1.103
D       172.17.35.0 [90/2172416] via 10.1.1.54, 00:14:00, Serial0/2/1.103
D       172.17.45.0 [90/2174976] via 10.1.1.54, 00:13:59, Serial0/2/1.103
     172.18.0.0/24 is subnetted, 1 subnets
C       172.18.3.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 68.110.171.133
```

Burada “C” ilə göstərilən route-lar cihaza birbaş bağlı olan (connected) interfeysləri, “D” ilə göstərilən route-lar routerin EİGRP routing protokolu vasitəsi ilə öyrəndiyi şəbəkələri, “S” ilə qeyd olunan isə statik olaraq konfiqurasiya etdiyimiz şəbəkələri əks etdirir.

3.2 Şəbəkənin struktur bölmələrindəki cihaz konfiqurasiyalarının təsviri.

Əvvəlcə Bakı filialının ümumi topologiyasını gözdən keçirək.



Şəkil 4.8 Bakı filialının topologiyası

Bu filialımızda üç VLAN yaratmışıq.Vlanlar müvafiq olaraq VOICE_WB (vlan 10),DATA1_WB (vlan30) və DATA2_WB (vlan 40) adlandırılmışdırlar.

```
SW_NY_2#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Gig0/1
                                                 Gig0/2
10   VOICE_WB                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6
30   DATA1_WB                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
40   DATA2_WB                          active    Fa0/5, Fa0/6, Fa0/8
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Şəkil 4.9 Bakı filialı vlan-lar.

Vlan 1 isə sviçlər üçün management vlandır.Vlanlar üçün təyin olunmuş şəbəkələr bunlardır.

- **VLAN 1 – 172.16.1.0/24**
- **VLAN 10 -172.16.10.0/24**
- **VLAN 30 -172.16.30.0/24**
- **VLAN 40 -172.16.40.0/24**

Şəbəkənin çıxış qapısı “Baku_Router”-dir.Burada FastEthernet0/0 interfeysi sub-interfeyslərə bölünüb və sviçlərdə olan vlanlar üçün gateway bu sub-interfeyslərdir.Hər vlan öz nömrəsinə uyğun olaraq Bakı routerində formalaşdırılmış interfeyslərə tanıdılıb.Hər vlan bir broadcast domain təşkil edir.VLAN-lar şəbəkədə təhlükəsiz məlumat paylaşımı,operativlik təmini,performans yüksəldilməsi və s bu kimi faktorlara birbaşa təsir edir.Hər vlan fərqli şəbəkəni təmin etdiyi üçün onların bir birləri ilə əlaqə yaratması üçün routing funksiyasına malik bir cihaza mütləq şəkildə ehtiyac və bizim şəbəkədə bu funksiyanı bakı routeri icra edir.İndi isə bakı routerində formalaşdırdığımız sub-interfeyslərə əyani şəkildə nəzər yetirək.Qeyd etdiyimiz kimi bu interfeyslər FastEthernet0/0-ın alt interfeysləridir.

```
!
interface FastEthernet0/0
 ip address 172.16.1.254 255.255.255.0
 duplex full
 --More--
%IPPHONE-6-REG_ALARM: 24: Name=SEP001D452D50BD Load= SCCP41.8-3-3SR2S Last=Phone-Reg-Rej
 speed 100
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.254 255.255.255.0
 ip helper-address 172.16.40.1
!
interface FastEthernet0/0.30
 --More--
%IPPHONE-6-REG_ALARM: 24: Name=SEP001D452D50BD Load= SCCP41.8-3-3SR2S Last=Phone-Reg-Rej
 encapsulation dot1Q 30
 ip address 172.16.30.254 255.255.255.0
 ip helper-address 172.16.40.1
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.40.254 255.255.255.0
```

Şəkil 4.9 Bakı routerindəki interfeyslər.

Sviçlər arasındakı əlaqə kanalı trunk kanaldır.Cihazlar arası linklər access və trunk olmaqla iki qrupa bölünür.Bu tip qruplaşdırma istifadə yerinə görə dəyişir.Access linklər “end devices”-lar üçündür.Yəni bir host sviç və ya routerə qoşulduqda onlar arası xətt access adlanır.Trunk linklər isə “tağ” olunmuş və ya işarələnmiş paketlərin cihazlar arası əlaqəsini təmin edir.Bu cür paketlər müxtəlif vlan-lara aid paketlərin daşınması zamanı formalaşır.Yəni iki sviç üzərində 2 və daha çox vlan varsa biz bu sviçlər arası linklərin trunk link olmasını təmin etməliyik.Bundan sonra bu cihazlar arasında fərqli vlan paketlərinin axışı təmin olunacaq.Bundan əlavə əgər biz bu vlanların bir biri ilə əlaqəsini yaratmaq istəsək onda sviç və routerimiz arasındakı linki də trunk link kimi konfiqurasiya etməliyik.Aşağıdakı şəkildə sviçlər üzərində olan trunk portların və bu portlardan hansı vlan paketlərinin daşınmasına icazə verildiyini əyani olaraq görmək olar.

```
SW_NY_2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,30,40
Fa0/24      1,10,30,40

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,30,40
Fa0/24      1,10,30,40

SW_NY_2#
```

Şəkil 5.0 Sviç üzərindəki trunk portlar

Şəkildən də göründüyü kimi FastEthernet 0/1 və FastEthernet 0/24 portları trunk linklərdir.Bu portlar sviç2 üzərindədi.Onlardan biri sviç2 və sviç3 arasında,digəri isə sviç2 ilə sviç1 arasındakı linkdir.Burada bu portlardan keçməsinə icazə verilən vlan-lar 1-1005 kimi göstərilib.Bu rəqəm göstərilən aralıqdakı bütün vlan paketlərini daşınmasına icazə verildiyini göstərir.Ancaq qeyd edim ki, biz istədiyimiz vlanları bura əlavə edə və ya çıxara bilərik.Sviçlər üzərində VTP(vlan trunking protocol) konfiqurasiya edilib.Bu protokol sayəsində şəbəkə inzibatçılarının həm işləri daha da asanlaşmış olur və həmdə şəbəkədə performans yüksəlir.Protokolun əsas məntiqi avtomatlaşdırılmış şəkildə vlan formalaşdırmağa əsaslanır. VLAN Trunk Protokolu, mövcud VLAN-larəın silinməsi və yenidən adlandırılmasının bir tərəfdən idarə edilməsinə imkan verən bir şəbəkəyə yeni VLAN əlavə etmək üçün Cisco-a əsaslanan 2-ci Layer protokoludur. Bu protokolu istifadə edərək şəbəkə rəhbərliyi daha effektiv və asan təmin olunur. Ümumiyyətlə, VTP-nin nə olduğunu müəyyən etdikdən sonra, VTP rejimlərinə keçək. VTP 3 istifadə rejimi var:

- Server
- Client
- Transparent

Server;

Server rejimində yeni VLAN əlavə oluna bilər, mövcud VLAN silinir və dəyişdirilə bilər. Bu rejimdə istifadə ediləcək VTP versiyası (v1 və ya v2) bütün domendə vtp topologiyasının istifadəsinin olub-olmadığını müəyyən etmək üçün də istifadə edilə bilər. VTP paketləri həmin qovşaqda digər keçidlərə magistral portları və idarəetmə vlanı VLAN 1 vasitəsilə göndərilir, bu da sinxron şəkildə işləməyə imkan verir. Bu rejim Cisco açarları üçün standart rejimdir. VLAN məlumatları burada konfiqurasiya edilir və NVRAM-a saxlanılır. Bu, cihaz yenidən başlasa, VLAN məlumatlarının itirilməsinə mane olur.

Client;

VLAN məlumatı bu rejimdə yerli olaraq yaradılmır, silinir və ya dəyişdirilə bilməz.Eyni VTP domainindən alınan VLAN məlumatı və konfiqurasiya təftiş nömrəsini qeyd edir.

Transparent;

Bu rejimdə keçid heç bir server və ya müştəri rejimində keçid kimi davranmır. Bu rejimdə keçid alınan VLAN məlumatını gömrük portundan ötürür, lakin bu məlumatı VLAN məlumatında saxlamır. Yerli VLAN məlumatını yaratmaq, silə və dəyişdirə bilər, ancaq onları digər domendə digər keçidlərə köçürmür və onlardan məlumatlara uyğun olaraq işləmir. VTP protokolu hər 5 dəqiqədə VTP paketləri göndərir və ya e-server dəyişiklik kimi istifadə olunan keçid üçün formalaşdırmağa və digər dəyişənlərə yenilik etmək əsasında VLAN məlumatlarını yeniləmək üçün istifadə olunur. VTP-də Konfiqurasiya Revision nömrəsini bilmək çox vacibdir. Şəbəkə dəyişikliyi ilə, bu 32-bitlik dəyər də artır və vtp rejimində keçid, başqa cari VLAN məlumatları ilə birlikdə eyni sahədə digər keçidlərə göndərir. Sviçlər VLAN məlumatlarını ən yüksək konfiqurasiya versiyası

nömrəsinə görə yeniləyirlər. Bu sayının artırılmasının əsas məqsədi bütün keçidlərin ən müasir son cari vəziyyətə uyğun qurulmasını təmin etməkdir.

```
SW_NY_2#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : NY
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.BCDC.BD00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 172.16.1.2 on interface Vl1 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 18
MD5 digest                      : 0x5C 0xA2 0x91 0x57 0xBA 0xAB 0xF7 0xBB
                                  0xBD 0x0A 0xE1 0xE8 0xFF 0x64 0x1E 0x63
```

Şəkil 5.1 VTP statusu.

Qeyd etdiyimiz kimi şəkildə qeyd olunan sviçdə VTP sazlanıb.Bu sviç VTP server modunda fəaliyyət göstərir.Revision nömrəsi olaraq cari dəyər 18 qeyd olunub və VTP version 2 aktivdir.Bu isə cari sviçin digər sviçlər üçün server rolunu oynadığını və onlar üçün lazımı konfiqurasiya məlumatlarını təmin etdiyini göstərir.

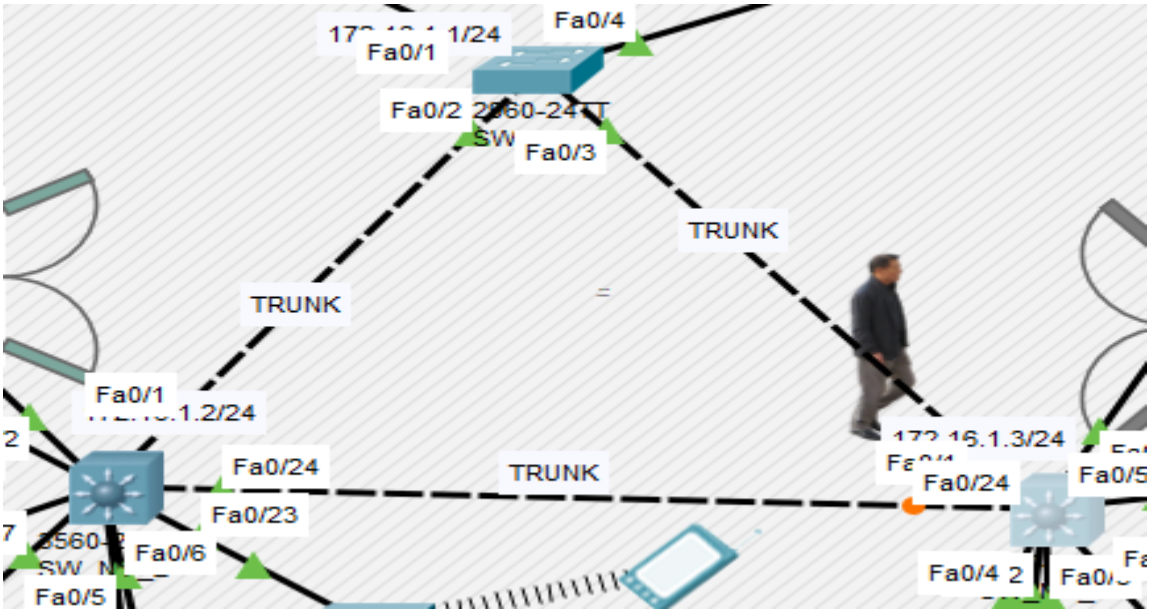
```
SW_NY_2#sh vtp password
VTP Password: cisco
SW_NY_2#
```

VTP domain-dəki digər sviçlərin bu sazlamaları qəbul etməsi və təhlükəsiz əlaqənin təmini üçün verilən şifrə CİSCO-dur.

Şəbəkəmizdə STP protokolunun tətbiqi.

Spanning Tree Protokolu (STP) hər hansı bir LAN seqmenti (toqquşma sahəsi) arasında yalnız bir aktiv əlaqə qalmaq üçün bəzi portları bloklamaq üçün kommutator daxil olmaqla bütün körpü (körpü) cihazlarında spanning ağac alqoritmini istifadə edən IEEE 802.1 standartıdır. . Həmçinin, dayanacaqlar

arasında çoxlu aktiv marşrutlar olduqda baş verə biləcək çevrələrin qarşısını alır. Spanning ağacı alqoritmi körpü və switch əsaslı şəbəkələrdə istifadə olunur və trafik üçün ən yaxşı yoldan qaynaqdan təyinata keçməyə qərar verir. Bu alqoritm bütün backup yollarını nəzərə alır və istənilən vaxt onlardan birini aktivləşdirir. Spanning tree protokolunun fəal şəkildə istifadə etdiyi şəbəkələrdə kök şəbəkəsi üçün bir kök körpü, kök kökdən hər bir kök port və bir dənə təyin olunmuş port var. Kök körpü açar şəbəkələrdə yayılmış ağac topologiyasının məntiqi mərkəzidir. Topologiya üzrə hər bir körpü digərlərinə "salam BPDU" adlı mesaj göndərərək root olduğunu iddia edir.



Şəkil 5.2 Spanning tree (stp)

Kök körpüləri hər iki saniyədə onların "salam" BPDU-lərini fəaliyyət göstərdiyini bildirmək üçün göndərir. Bütün digər keçidlər və körpülər bu BPDU-ları götürürlər. "Salam" məlumatların köçürülməsi yolu ilə gəlirsə, kök yolun hələ də ayaq üstə olduğu anlamına gəlir. "Salam" paketi qəbul etməzsə, spanning ağac prosesi yenidən başlayacaq. "Salam" BPDU, şəbəkə dəyişikliyinə cavab verərkən körpülərin gözləyəcəyi vaxtları təyin edir. Bu dövrlər; "Salam Zamanı" ən uzun gözləmə müddəti (maksimum yaş) və çatdırılma gecikməsidir.

BPDU bütün keçidlər növbəti şəbəkə konfiqurasiyasından istifadə etmək üçün kök körpünün məlumatını (Köprü id, kök yol dəyəri) dəyişir. Hər keçid qonşusunu

başqa qonşuya göndərir. Bu mərhələlər Bridge Protocol Data Unit (BPDU) çərçivələri ilə həyata keçirilir.

```
SW_NY_1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     00E0.8FE9.493D
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4097  (priority 4096 sys-id-ext 1)
              Address     00E0.8FE9.493D
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     00E0.8FE9.493D
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
              Address     00E0.8FE9.493D
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
```

Şəkil 5.3 STP konfiqurasiyası

Şəbəkədə root sviç seçimi aparılarkən ilk öncə “Bridge Priority” dəyərinə baxılır.Bu dəyər default olaraq 32769-dur.Əgər əl ilə hər hansı dəyişiklik etməmişiksə bu dəyərlər bütün sviçlərdə eyni olacaq.İkinci olaraq cihazların MAC ünvanları müqaisə olunur və ən kiçik ünvana malik cihaz root olaraq seçilir.Root olan cihazın hər iki portu aktiv halda olur.Digər cihazların ən böyük MAC-lı cihazın isə portlarından biri bloklanır və loop əngəllənir.Yuxarıdaki şəkildə (5.3) göründüyü kimi bu sviçdə priority dəyəri manual olaraq 4106 kimi verilib.Göründüyü kimi bu sviçdəki portlar forwarding moddadır.İndi isə digər portu blok olan sviçdəki stp vəziyyəti ilə tanış olaq.

```
SW3#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     00E0.8FE9.493D
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    12289  (priority 12288 sys-id-ext 1)
              Address     0060.5C1A.5433
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/24           Altn BLK 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     00E0.8FE9.493D
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    12298  (priority 12288 sys-id-ext 10)
```

Şəkil 5.4 STP konfiqurasiyası (sviç2)

Bu sviçdə priority dəyəri 12288 olaraq təyin edilib.Bu isə onun portunun bloklanmasına səbəb olub.Burada Fa0/24 interfeysi data mübadiləsi etmir və passiv durumdadır.

Şəbəkəmizdə DHCP protokolunun tətbiqi.

DHCP servisi cihazlar üçün İP ünvan paylanmasına cavabdeh servisdir.Bu funksiya üçün korporativ şəbəkəmizdə router yerləşdirmişik.Şəbəkədəki hər üç vlan (vlan 10,vlan 30 və vlan 40) bu router üzərindəki dhcp pool-dan İP alır.Sözügedən konfiqurasiyaya əyani baxaq:

```
ip dhcp excluded-address 172.16.40.1 172.16.40.100
ip dhcp excluded-address 172.16.40.240 172.16.40.254
ip dhcp excluded-address 172.16.30.1 172.16.30.100
ip dhcp excluded-address 172.16.30.240 172.16.30.254
ip dhcp excluded-address 172.16.10.240 172.16.10.254
ip dhcp excluded-address 172.16.10.1 172.16.10.100
ip dhcp excluded-address 172.16.1.1 172.16.1.100
ip dhcp excluded-address 172.16.1.240 172.16.1.254
!
ip dhcp pool FORVLAN40
 network 172.16.40.0 255.255.255.0
 default-router 172.16.40.254
 dns-server 4.2.2.2
ip dhcp pool FORVLAN30
 network 172.16.30.0 255.255.255.0
 default-router 172.16.30.254
 dns-server 4.2.2.2
ip dhcp pool FORVLAN10_VOICE
 network 172.16.10.0 255.255.255.0
 default-router 172.16.10.254
 option 150 ip 172.16.10.254
```

Şəkil 5.5 DHCP konfiqurasiyası

Vlan 40 üçün 172.16.40.0/24 şəbəkəsindən ip paylaşımı edilir.Bu şəbəkədən İP alan cihazlar üçün default çıxış nöqtəsi isə 172.16.40.254 ip-sidir.Bu ip bizim routerin sub-interfeysində vlan 40 üçün ayırdığımız İP dir.DNS (domain name server) olaraq isə cihazlara GOOGLE –a məxsus public DNS ünvanı göstərilib.Vlan 30 –a gəldikdə isə burda cihazlar 172.16.30.0/24 şəbəkəsindən İP alırlar.Onlar üçün default router 172.16.30.254 hesab olunur.Burada da DNS ünvanı olaraq GOOGLE göstərilib.Nəhayət Vlan 10 üçün isə ip 172.16.10.0/24 şəbəkəsindən paylanır.Burada isə default router 172.16.10.254-dür.Bu vlan voice vlan-dır və İP telefoniya üçün istifadə olunur.Digər vlanlardan fəqrli olaraq bu vlan konfiqurasiyasında DNS ünvanı qeyd etməməyimizin səbəbi də budur.Excluded adreslər isə rezerv olunub.Şəbəkədə routing protokolu olaraq EİGRP istifadə olunur.Hər routerdə müvafiq konfiqurasiyalar yazılıb.Onlara əyani nəzər yetirək.

```
!
router eigrp 1
 redistribute static
 network 172.18.0.0
 network 10.0.0.0
 no auto-summary
!
```

Şəkil 5.6 EİGRP konfiqurasiyası

EIGRP, IGRP protokolu yetərli olmadığından sonra, inkişaf etmiş xüsusiyyətləri sayəsində Cisco cihazları tərəfindən yaradılmış şəbəkələrdə çox üstünlük təşkil edən bir protokoldur. Bu protokola Hybrid deyilir, çünki eyni zamanda, məsafə vektoru və cari xətt özəlliklərindən istifadə xüsusiyyətləri vardır. EIGRP-də ən böyük "hop count" (paketin çatdıqları rabitə sayıları sayı) 224-dir. Metrik hesablayarkən EIGRP xətt gecikməsini, bant genişliyi, etibarlılıq və yük vəziyyəti metrik olaraq istifadə edir. Bundan əlavə, təhlükəsizlik MD5 kripto alqoritmindən istifadə edərək marşrutlaşdırıcılar arasında şifrəli identifikasiya təmin olunur. Bu protokolun ən vacib üstünlüklərindən biri alternativ marşrutlar

arasında yüksək sürətlə keçid təklif edir. EIGRP, protokol alqoritmi olaraq DUAL (Diffusing Update Algorithm - Span Update Algorithm) alqoritmini istifadə edir. Marşrutlaşdırma bu alqoritmlə hesablanır və bir problem meydana çıxarsa əvvəlcədən hesablanmış backup marşrutuna keçir. Digər marşrutlaşdırma protokollarında belə bir xüsusiyyət yoxdur. Bu EIGRP'ye böyük bir sürət verir. Bu protokolun IGRP-dən ən mühüm fərqlərindən biri, IGRP kimi dövri bir yeniləmə etməməsidir. Marşrutlaşdırma masasında bir dəyişiklik olduğunda bütün masa deyil, yalnız dəyişiklik hissəsi digər routerlərə göndərilir və şəbəkə trafiki ən azı bant genişliyi istifadə edərək sürətlənir. EIGRP bütün şəbəkə məlumatlarını qonşu marşrutlaşdırıcılara göndərmir. Hello paket adlı paket sayəsində, qonşu routerın vəziyyəti barədə məlumat veriləcəkdir. Ona göndərilən "Salam" tab paketi sözdə "qəbul etmə paketini alır və marşrutlaşdırma stolu müvafiq olaraq yenilənir. Cisco tərəfli RTP (Etibarlı Nəqliyyat Protokolu) protokolu bu əməliyyatları yerinə yetirmək üçün istifadə olunur. Şəbəkə topologiyasına (məsələn, yeni bir router əlavə etməklə) dəyişiklik edildikdə, sorğu adlı yeniləmə paketlərini istifadə edərək, yeni əlavə edilən router tezliklə RTP protokolu vasitəsilə marşrutlaşdırma tablosunu yarada bilər.

EIGRP-nin əsas xüsusiyyətləri aşağıdakılardır:

- AD (İnzibati məsafə) dəyəri 90.
- VLSM üçün dəstək.
- IP, IPX, AppleTalk protokollarını dəstəkləyir.
- Auto Summarization xüsusiyyəti.
- EIGRP protokolu Classless işləyir.

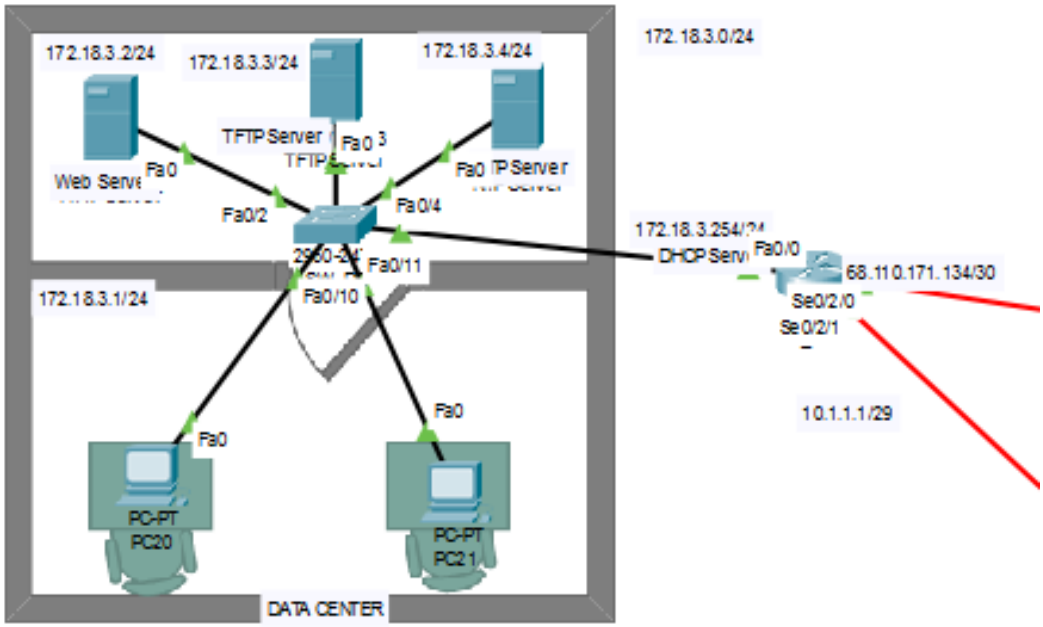
Routing haqda son olaraq qeyd edək ki internet çıxışı üçün router üzərində İSP (internet servis provider) istiqamətində statik route yazılıb.Statik route AD (administrativ distance) dəyəri 1 olan və əllə manual olaraq verilən routlardı.

```
ip route 0.0.0.0 0.0.0.0 68.110.171.133
!
```

Şəkil 5.7 Statik route

Statik routing kiçik şəbəkələrdə daha çox istifadə olunur.

Məlumat mərkəzi:



Şəkil 5.8 Məlumat mərkəzi

Məlumat mərkəzimizdə 3 əsas server fəaliyyət göstərir.Bu serverlərdən 172.18.3.2/24 İP ünvanlısı veb serverdi.Bu server üzərində bizim müəssisənin saytı yayımlanır.Bundan başqa TFTP server və NTP serverlərimiz də varki onların da hansı funksionallığa sahib olduqlarını incələyək.

TFTP server:

Az Riskli Fayl Ötürülməsi Protokolu (TFTP), FTP'nin əsas funksional forması kimi 1980-ci ildə təsbit edilən sadə bir fayl ötürülməsi protokudur. Sadə quruluşu sayəsində çox az yaddaş istehlak olunur. Bu xüsusiyyətdən ötəri, kompüterlərin fayl paylaşımı üçün heç bir yığma cihazı olmayan bir router istifadə edilmişdir. Şəbəkədə ana kompüterlər arasında kiçik faylları köçürmək üçün istifadə olunur. TFTP qismən KAP protokol qrupunun bir hissəsi olan EFTP

protokoluna əsaslanır. TCP / IP protokolu qrupunun inkişafının erkən mərhələlərində TFTP, sadəcə olaraq, yeni bir host tipində fəaliyyət göstərən ilk protokol idi.Bu sadalanan keyfiyyət və sürətinə görə tftp bugün fayl ötürülməsində geniş istifadəçi kütləsinə və rəğbətinə sahibdir.

NTP server:

Şəbəkə strukturumuzda Syslog serverləri varsa, bu serverlərə göndərilən logların vaxt məlumatı çox vacibdir. Əlavə olaraq, Router kimi cihazlarda, Time server məlumatından vaxtında məlumat almaq üçün yerli vaxtla müəyyən olunmuş vaxt məlumatlarını vaxtında müəyyənləşdirməklə daha təhlükəsiz bir üsuldur. Saat serverləri bir qaynaq kimi atom saatları və ya atom saatlərini ehtiva edən GPS-lərə əsaslanır.

- NTP Protokolu UDP, həm qaynaq, həm də hədəf portu olaraq 123 istifadə edir.
- NTP bir daxili və ya xarici mənbədən vaxt məlumatı ala bilər.
- Router və ya Switch bir NTP Server və ya NTP Client kimi konfiqurasiya edilə bilər.

Konfiqurasiya əmrləri:

Router(config)#ntp server *serverin ip adresi*

Doğrulama əmrləri:

Router(config)#show clock

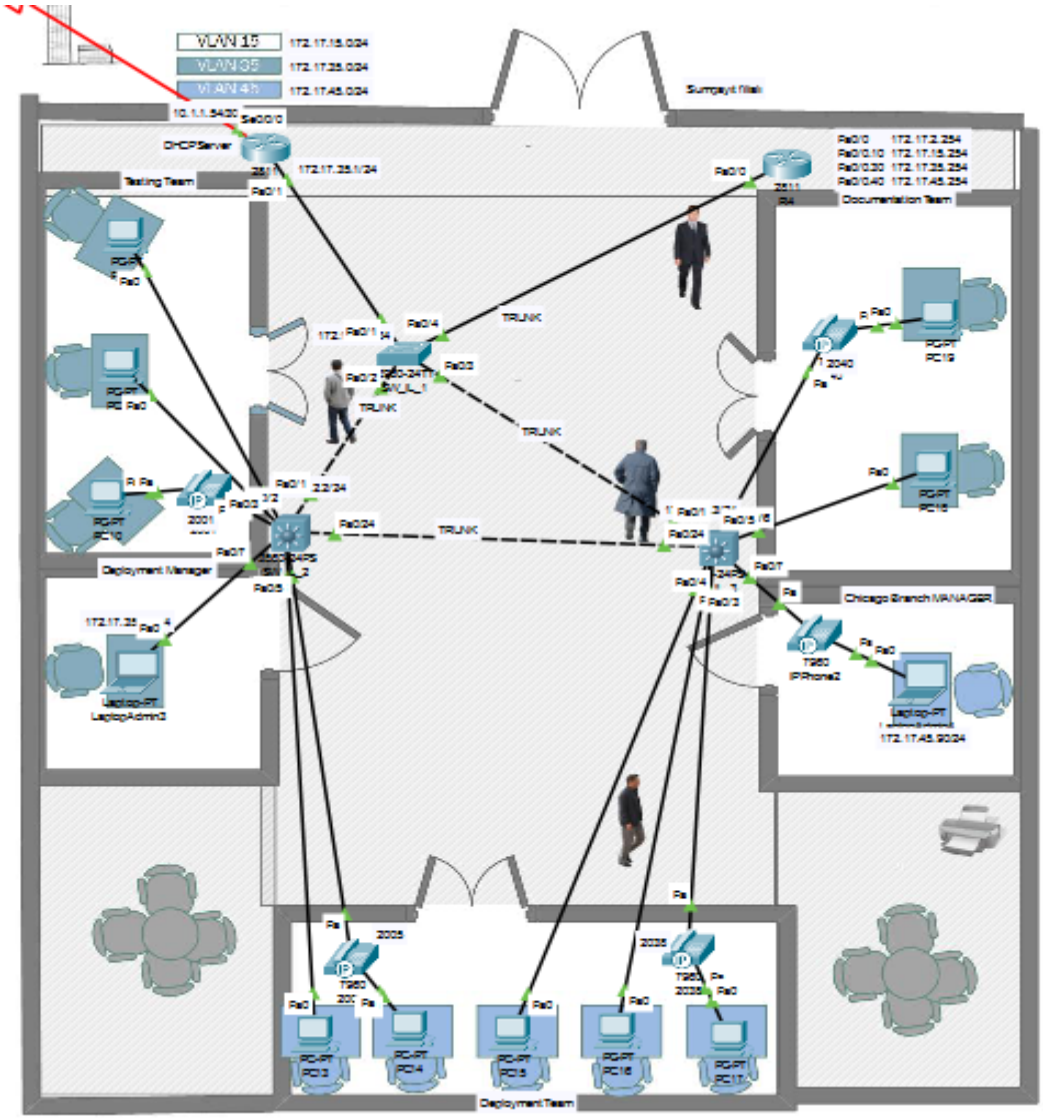
Router(config)#show ntp status

Router(config)#show ntp associations

Bizim router üzərindəki NTP server konfiqurasiyası isə belədir:

```
 login
!
!
ntp server 4.2.2.3
!
end
```

Sumqayıt filialımıza nəzər yetirək:



Şəkil 5.9 Sumqayıt filialı

Burada da Bakı filialında olduğu kimi vlanlar yaradılıb və İP telefonlar sazlanıb.Demək olarki eyni konfiqurasiyaların hamısı bu filialımız üçün də keçərlidir.Yeganə fərq vlan və subnetlərin fəqli olması göstərilə bilər.Telefoniya üçün olan vlanımız VLAN 15-dir.Digər 2 vlan isə istifadəçilər üçün nəzərdə tutulub.Bu vlanlar isə müvafiq olaraq VLAN 35 və VLAN 45 –dir.Buradakı DHCP servisi də router üzərində konfiqurasiya edilib.Aşağıdakı şəkildə bu sazlamaları aydın görə bilərik.

```
!
ip dhcp excluded-address 172.17.2.1 172.17.2.100
ip dhcp excluded-address 172.17.2.240 172.17.2.254
ip dhcp excluded-address 172.17.35.1 172.17.35.100
ip dhcp excluded-address 172.17.35.240 172.17.35.254
ip dhcp excluded-address 172.17.45.1 172.17.45.100
ip dhcp excluded-address 172.17.45.240 172.17.45.254
ip dhcp excluded-address 172.17.15.1
ip dhcp excluded-address 172.17.15.254
!
ip dhcp pool FORVLAN35
 network 172.17.35.0 255.255.255.0
 default-router 172.17.35.254
ip dhcp pool FORVLAN45
 network 172.17.45.0 255.255.255.0
 default-router 172.17.45.254
ip dhcp pool FORVOICE_15
 network 172.17.15.0 255.255.255.0
 default-router 172.17.15.254
 option 150 ip 172.17.15.254
!
```

Şəkil 6.0 DHCP servisi

Göründüyü kimi hər üç vlan üçün müvafiq İP aralıqları təyin olunub.Excluded adress əmri ilə göstərilən adreslər isə paylanacaq İP-lər içərisindən seçilmiş və rezerv olunmuş istisna ünvanlardır.Routing prosesi də bu router üzərindən təyin olunub.

```
!
router eigrp 1
 network 172.17.0.0
 network 10.1.1.54 0.0.0.0
 no auto-summary
!
router rip
!
ip classless
!
```

Sviçlər arası portlar isə trunk port olaraq təyin olunub.Bu portlar üzərindən bütün vlanlar digər sviçə göndərilə bilir.Bu konfiqurasiyaya baxaq:

```
SW_IL_2#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,15,35,45
Fa0/24      1,10,15,35,45

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,15,35,45
Fa0/24      10
```

Şəkil 6.1 Trunk portlar

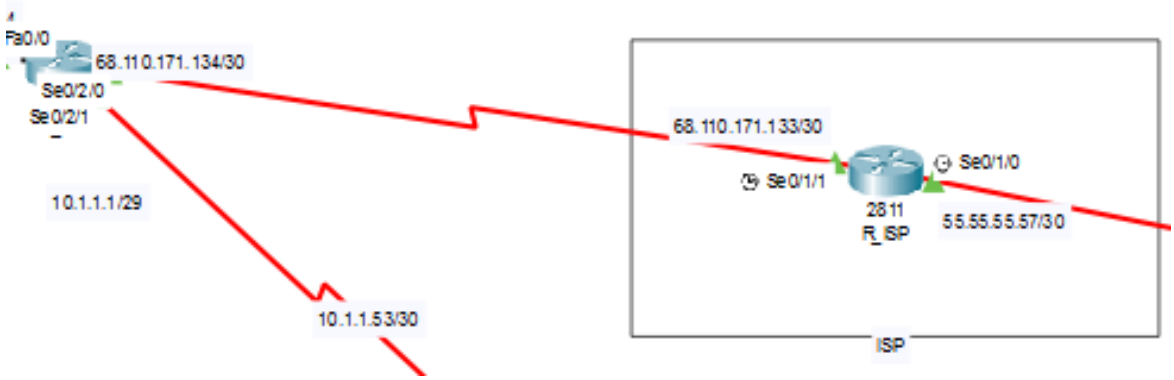
Burada Fastethernet0/1 və 0/24 cü portlar trunk link olaraq qeyd edilib.Eyni işarələmə digər sviç üzərində də aparılıb.Bu konfiqurasiya üçün əmrlər aşağıdakı kimidir.

```
Switch(config)#     interface     GigabitEthernet     0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

```
Switch(config)# interface GigabitEthernet 0/1
Switch(config-if)# switchport trunk allowed vlan
1,2,3,4
```

```
Switch# show run interface GigabitEthernet 0/1
Switch# show interface trunk
```

Bütün şəbəkənin internet çıxışı üçün olan routing statik olaraq qeyd olunub və bu bizim cihazların internetə çıxmasına şərait yaradır.Həmçinin NAT servisi də çıxış routeri ilə reallaşır.



Şəkil 6.2 İSP ilə əlaqələnmə.

Bildiyimiz kimi daxili şəbəkələrdə özəl İP-lər istifadə olunur.Ancaq internet çıxışı üçün bizə public İP lazımdır.NAT (network address translation) bu işi icra edən servisdir.Bu servis bizim daxili ip aralıqlarını bir xarici İP ilə internetə bağlanmağa yardım edir.Burada hər internetə çıxan istifadəçi üçün interfeysə verilmiş xarici İP-ə port nömrəsi əlavə edir və bu proses tamamlanmış olur.

```
!
router eigrp 1
 redistribute static
 network 172.18.0.0
 network 10.0.0.0
 no auto-summary
!
ip nat inside source list 1 interface Serial0/2/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 68.110.171.133
!
ip flow-export version 9
!
```

Şəkil 6.2 Statik route və NAT

NƏTİCƏ VƏ TƏKLİFLƏR

Hazırda təyinatından asılı olmayaraq istənilən müəssisədə müxtəlif ölçüdə korporativ internet şəbəkənin olmaması demək olar ki, imkansızdır.Çünki hazırda iş və yaşamın bir parçası olan internetə hər kəsin ehtiyacı var.İsitifadəçi sayına və təyinatına görə bu şəbəkələr də müxtəlif quruluşa malik olurlar.

Bizim formalaşdırdığımız bu korporativ şəbəkə modelində iki filialı və bir data mərkəzi olan nümunə öz əksini tapıb.Şəbəkə daxilində virtual lokal şəbəkələr (vlan),routing protokolları (eigrp,statik routing), müxtəlif internet servisləri (dhcp , dns , ntp , stp və s) konfiqurasiya edilib. Bundan əlavə şəbəkədə təkcə internet çıxışı yox həmçinin təhlükəsizlik də nəzərə alınıb və müvafiq konfiqurasiyalar (acl-access control list) edilib.

Korporativ şəbəkəmizdə data ilə yanaşı səsin də ötürülməsi və rabitə əlaqəsinin mövcudluğu qeyd oluna bilər.Bunu biz CİSCO –nun ip üzərindən səs ötürməyə imkan verən voice routeri ilə icra etmişik.

Burada layer 2 səviyyəsində təhlükəsizlik konfiqurasiyaları da mövcuddur (port security).Ancaq layer 3 təhlükəsizlik üçün bu tip şəbəkələr üçün Firewall adlanan təhlükəsizlik cihazlarına gərək duyulur.Bu cihazlar ola biləcək və risk daşıyan təhdidlərə qarşı ideal vasitədir.Bu gün istifadə olunan bu cihazlara misal olaraq cisco şirkətinin CİSCO ASA (adaptive security appliance), Palo Alto şirkətinin eyni adlı cihazını göstərmək olar.Bu cihazlar layer 3-4 və hətda layer 7 səviyyədə təhlükəsizlik təminatını qarşılaya bilir.

Bu gün informaisya qarşı olan təhdidlərin artması bu məsələnin önəmini bir daha göz önünə sərir.Bu gün ölkəmizdə bu mövzuya diqqət istənilən səviyyədə deyil.Kiber cinayətkarlıq və ondan qorunmaq üçün daha geniş maarifləndirmə aparılmasına ehtiyac var.Son olaraq mövcud şəbəkə modelimizin cari tələblərə uyğunluğunu və yüksək performanslı,itkisiz məlumat mübadiləsi etməyi və

marşurutların optimal təyininin həm filiallarda həm də məlumat mərkəzində istənilən səviyyədə olduğu qeyd oluna bilər.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT SİYAHISI

1) CCNA Security 640-554 Official Cert Guide - Keith Barker, Scott Morris, 2012
2) CCNA Data Center DCICT 200-155 Official Cert Guide - Navaid Shamsee, Ahmed Afrose, David Klebanov, Hesham Fayed, Ozden Karakok,2017
3) Voice Study Guide - Andrew Froehlich,2010
4) Routing and Switching Portable Command Guide, 4th Edition - Scott Empson 2016
5) Mulgan GJ. Communications and Control: Networks and New Economies of Communication. Oxford: Polity, 1991. P. 19.
6) .Чернавский Д.С. «Синергетика и информация». - М.: Наука, 2001; Корчагин Ю.А. Информация и человеческий капитал. Вестник ЦИРЭ «Проблемы региональной экономики».
7) Цирель. С. Экономический рост и информационные технологии: компаративистский подход ВЭ. 2004. 92-111. №11;
8) И.А. Стрелец. Новая экономика и информационные технологии. - «ЭКЗАМЕН», 2003, С.: 254; Ходжсон Док. Социально-экономические последствия прогресса знаний и нарастания сложности // Вопросы экономики. 2001. №8. С.34;
9) Курицкий А. Интернет-экономика: закономерности формирования и функционирования. СПб.: Издательство СПбГУ, 2000.
10) Карр Н.Д. Блеск и нищета информационных технологий. - М.: Секрет фирмы, 2005.

Elektron ədəbiyyat:

www.cisco.com

www.paloaltonetwork.com

www.cozumpark.com.tr

www.ilkaddimlar.com

http://www.anilkutman.com

https://rutracker.org

http://www.ciscotr.com

S U M M A R Y

The computer network consists of a series of computers and a peripheral equipment system with communication lines and special software. It is a prerequisite to have information networks, networks, and networks to provide users with the information they need. Depending on the distance, cable, telephone lines, radios, satellite communications and optical fibers are used as communication lines. The most popular computer network is the Internet.

The main components of computer networks are:

computers;

communication equipment;

network operating systems;

network applications;

contact channels.

Р Е З Ю М Е

Компьютерная сеть состоит из серии компьютеров и системы периферийного оборудования с линиями связи и специальным программным обеспечением. Обязательным условием является наличие информационных сетей, сетей и сетей для предоставления пользователям необходимой им информации. В зависимости от расстояния в качестве линий связи используются кабельные, телефонные линии, радиоприемники, спутниковая связь и оптические волокна. Самая популярная компьютерная сеть - Интернет.

Основными компонентами компьютерных сетей являются:

компьютеры;

коммуникационное оборудование;

сетевые операционные системы;

сетевые приложения;

контактные каналы.