**Şəbəkələrin əsasları imtahan sualları – cavabları**

**Sual 1. OSI modelinin ümumi quruluşunu və funksional təyinatını izah edin.**

**Cavab:** OSI modelinin əsas məqsədi müxtəlif istehsalçıların avadanlıq və protokollarının bir-biri ilə işləməsinə imkan verməkdir.

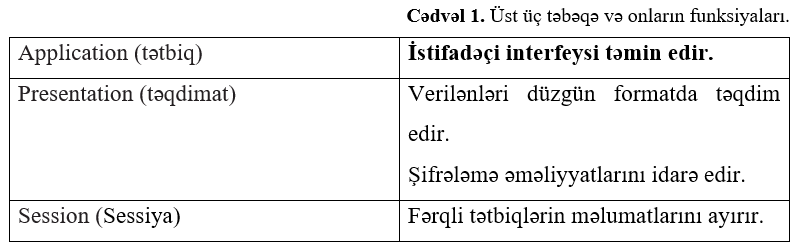
OSI təbəqələşmiş modelindən istifadə etməyin bəzi vacib üstünlüklərinin siyahısı:

* Şəbəkə ünsiyyəti prosesini daha kiçik və sadə komponentlərə ayırır, bu da komponentlərin inkişafını, dizaynını və problemlərin həllini asanlaşdırır.
* Şəbəkə komponentlərinin standartlaşdırılması vasitəsilə çoxsaylı istehsalçıların inkişafını təmin edir.
* Modelin hər təbəqəsində hansı funksiyaların həyata keçirildiyini açıq şəkildə müəyyən edərək, sənaye standartlarını təşviq edir.
* Müxtəlif növ şəbəkə avadanlığı və proqram təminatının bir-biri ilə ünsiyyət qurmasına imkan verir.
* Bir təbəqədəki dəyişikliklərin digər təbəqələrə təsir etməsinin qarşısını alır, beləliklə inkişafı sürətləndirir.

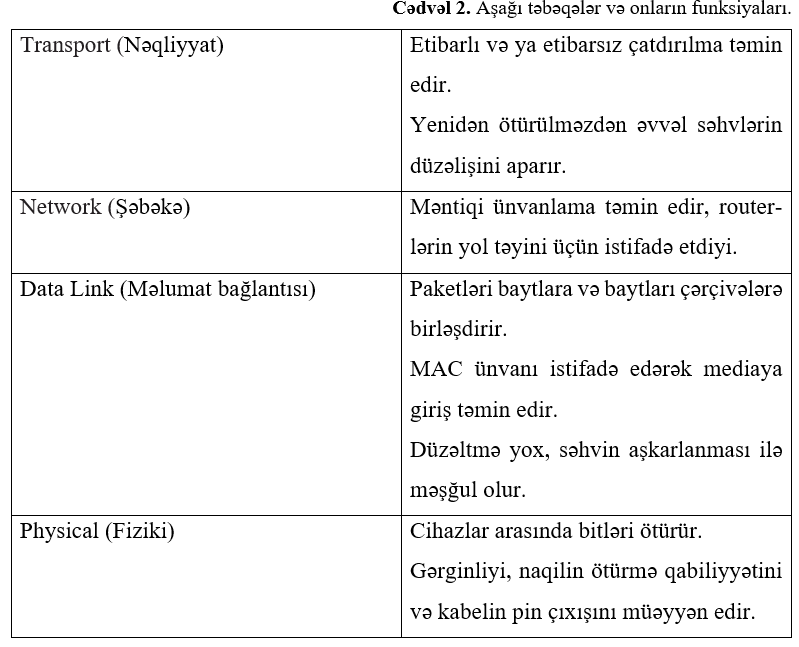
OSI referans modeli

OSI spesifikasiyalarının bizə verdiyi ən yaxşı üstünlüklərdən biri fərqli əməliyyat sistemləri (Unix hostları, Windows maşınları, Mac-lar, smartfonlar və s.) üzərində işləyən müxtəlif hostlar arasında məlumat ötürülməsini asanlaşdırmaqdır.

Yadda saxlayın ki, OSI məntiqi bir modeldir, fiziki deyil. Əsasən, şəbəkə üzərində işləyəcək tətbiqləri yaratmaq və tətbiq etmək üçün istifadə edilə bilən bir sıra rəhbər prinsiplərdir. Eyni zamanda, şəbəkə standartlarını, cihazları və sxemlərini yaratmaq və tətbiq etmək üçün bir çərçivə təmin edir.

OSI-nin yeddi fərqli təbəqəsi var və bunlar iki qrupa bölünür. Üst üç təbəqə, son cihazlar arasındakı tətbiqlərin bir-biri ilə və istifadəçilərlə necə ünsiyyət quracağını müəyyən edir. Aşağıdakı dörd təbəqə isə məlumatın son nöqtədən son nöqtəyə necə ötürüldüyünü müəyyən edir.

Cədvəl 1.- dən məlum olur ki, istifadəçilərin kompüterlə **tətbiq təbəqəsində** qarşılıqlı əlaqə qurduğunu və yuxarı təbəqələrin hostlar arasında tətbiqlərin ünsiyyətini təmin etməkdən məsul olduğunu başa düşmək vacibdir. Yuxarı təbəqələrin heç biri şəbəkə və ya şəbəkə ünvanları haqqında məlumat bilmir, çünki bu, dörd alt təbəqənin məsuliyyətidir.

Cədvəl 2.- də, dörd alt təbəqə və onların funksiyaları göstərildiyi kimi, bu dörd alt qatın fiziki mediada, məsələn, kabel, optik lif, sviç və router- lər vasitəsilə məlumatın ə ötürüləcəyini müəyyən etdiyini görə bilərsiniz.

Bu alt təbəqələr həmçinin məlumat axınının ötürən hostdan təyinat hostunun tətbiqinə necə bərpa olunacağını müəyyən edir. Aşağıdakı şəbəkə avadanlıqları OSI modelinin yeddi təbəqəsində işləyir:

* Şəbəkə idarəetmə stansiyaları (NMS)
* Veb və tətbiq serverləri
* Qapılar (default qapılar deyil)
* Serverlər
* Şəbəkə hostları.

Əsasən, ISO şəbəkə protokol dünyasının Emily Post-u kimidir. Necə ki, xanım Post insan sosial qarşılıqlı əlaqələri üçün standartları və ya protokolları müəyyənləşdirmək üçün kitab yazmışdı, ISO da açıq şəbəkə protokol dəsti üçün precedent və rəhbər olaraq OSI istinad modelini inkişaf etdirdi. Ünsiyyət modellərinin etiketini təyin edərək, bu gün protokol dəstləri üçün müqayisə edilən ən populyar vasitə olaraq qalır.

**Sual 2. Şəbəkə avadanlıqlarının nəzəri analizi və təbəqə əsaslı fərqləndirilməsi.**

**Cavab:** Şəbəkə Avadanlıqları və Qısa Məlumatları:

1. Router:
   * Funksiya: Fərqli şəbəkələr arasında məlumat paketlərini yönləndirir. Məlumatları IP ünvanlarına əsaslanaraq doğru ünvana yönəldir.
   * Təbəqə: 3-cü təbəqə (Şəbəkə təbəqəsi).
2. Siviç:
   * Funksiya: Eyni şəbəkə daxilində cihazlar arasında məlumat ötürür. MAC ünvanları əsasında məlumatı yönləndirir.
   * Təbəqə: 2-ci təbəqə (Data Link təbəqəsi).
3. Hub:
   * Funksiya: Şəbəkə daxilində məlumatı bütün cihazlara eyni anda ötürür. Sadə və passiv cihazdır.
   * Təbəqə: 1-ci təbəqə (Fiziki təbəqə).
4. Firewall:
   * Funksiya: Şəbəkə təhlükəsizliyini təmin edir, şəbəkəyə daxil olan və çıxan məlumatları analiz edərək müəyyən şəbəkə qaydalarına əsasən məhdudiyyətlər qoyur.
   * Təbəqə: 3-cü və 4-cü təbəqələr (Şəbəkə və Nəqliyyat təbəqələri).Yeni nəsil olanlar 7- ci təbəqədə işləyir.
5. Modem:
   * Funksiya: İnternet bağlantısını təmin edən avadanlıqdır, analog siqnalları rəqəmsal siqnallara çevirir və əksinə.
   * Təbəqə: 1-ci təbəqə (Fiziki təbəqə).
6. Access Point (AP):
   * Funksiya: Şəbəkə cihazlarına naqilsiz əlaqə təmin edir, şəbəkəyə naqilsiz qoşulma imkanı yaradır.
   * Təbəqə: 2-ci təbəqə (Data Link təbəqəsi).
7. Bridge:
   * Funksiya: Eyni şəbəkə daxilində məlumat ötürür və şəbəkələr arasında əlaqə yaradır. Trafiki azaldır və şəbəkə hissələrini birləşdirir.
   * Təbəqə: 2-ci təbəqə (Data Link təbəqəsi).
8. Repeater:
   * Funksiya: Siqnalları gücləndirərək uzun məsafələrə ötürməyə imkan verir, məlumatın keyfiyyətini artırır.
   * Təbəqə: 1-ci təbəqə (Fiziki təbəqə).
9. Gateway:
   * Funksiya: Fərqli şəbəkə protokollarını birləşdirərək əlaqə qurur, məsələn, bir şəbəkənin protokolunu başqa bir şəbəkəyə çevirir.
   * Təbəqə: 3-cü təbəqə (Şəbəkə təbəqəsi) və daha yüksək təbəqələr.

### Təbəqə Əsaslı Fərqləndirmə:

#### **OSI Modeli l:**

1. **Fiziki təbəqə / Physical Layer**: Hub-lar və kabellər (1-ci təbəqə).
2. **Məlumat bağlantısı təbəqəsi / Data Link Layer**: Keçidlər (Switch-lər) (2-ci təbəqə).
3. **Şəbəkə təbəqəsi / Network Layer**: Yönləndiricilər (Router-lər) (3-cü təbəqə).
4. **Nəqliyyat təbəqəsi / Transport Layer**: TCP, UDP (4-cü təbəqə).
5. **Sessiya təbəqəsi / Session Layer**: Şəbəkə əlaqəsinin idarə olunması (5-ci təbəqə).
6. **Təqdimat təbəqəsi / Presentation Layer**: Məlumatın formatlanması və sıxılması (6-cı təbəqə).
7. **Tətbiq Təbəqəsi / Application Layer**: HTTP, FTP, DNS kimi protokollar (7-ci təbəqə).

#### **TCP/IP Modeli / TCP/IP Model:**

1. **Tətbiq təbəqəsi / Application Layer**: HTTP, FTP, DNS (Application Layer).
2. **Nəqliyyat təbəqəsi / Transport Layer**: TCP, UDP (Transport Layer).
3. **İnternet təbəqəsi / Internet Layer**: IP (Internet Layer).
4. **Giriş və ya bağlantı təbəqəsi / Link Layer**: Ethernet, fiziki və şəbəkə bağlantıları (Link Layer).

**Sual 3. Ethernet texnologiyasının əsas anlayışlarını izah edin. Ethernet standartının nə olduğunu və hansı sürət dərəcələrində istifadə olunduğunu izah edin. MAC ünvanı nədir, necə formalaşır və şəbəkə cihazlarının identifikasiyasında hansı rolu oynayır?**

**Cavab:** Ethernet texnologiyası IEEE standartlarına əsaslanan bir şəbəkə texnologiyasıdır və Data Link Layer-də iki alt təbəqəyə bölünür: MAC (Media Access Control) və LLC (Logical Link Control). MAC alt təbəqəsi paketlərin mediaya necə yerləşdirildiyini, fiziki ünvanlamanı və məntiqi topologiyaları müəyyən edir. Bu təbəqə həmçinin xətt intizamı, çərçivələrin ardıcıl çatdırılması və opsional axın nəzarətini təmin edir. LLC alt təbəqəsi isə şəbəkə təbəqəsinin protokollarını müəyyənləşdirir və onları kapsul halına gətirir.

Ethernet standartı IEEE tərəfindən müəyyən edilir və Cisco imtahan məqsədləri üçün yalnız IEEE Ethernet standartları əsas götürülür. Ethernet texnologiyası fiziki ulduz topologiyası və məntiqi bus marşrutu ilə işləyir, bu isə onu hibrid topologiya edir.

MAC ünvanı, Data Link Layer-də istifadə olunan hardware ünvanıdır və hər bir cihazın yerli şəbəkədə unikal identifikasiyası üçün istifadə olunur. Sviçlər və körpülər bu MAC ünvanlarına əsasən çərçivələri yönləndirir və cihazların yerini təyin edir. MAC ünvanı sayəsində layer 2 cihazları fərdi cihazları müəyyən edə bilir və onların trafikinə yön verir. Bu ünvanlar filter cədvəllərində qeyd olunur və bu cədvəllər vasitəsilə şəbəkə daxilində məlumatların düzgün istiqamətdə hərəkəti təmin edilir.

**Ethernet texnologiyası müxtəlif sürət dərəcələrində istifadə olunur**:

* **10 Mbps (Ethernet)**: Ən ilkin Ethernet sürəti olub, çox vaxt köhnə şəbəkələrdə istifadə edilir.
* **100 Mbps (Fast Ethernet)**: Bu sürət daha yeni şəbəkələrdə daha geniş istifadə edilir, xüsusilə ofis şəbəkələrində.
* **1 Gbps (Gigabit Ethernet)**: Bu sürət daha yüksək bant genişliyi tələb edən şəbəkələrdə istifadə olunur və çox vaxt müasir ofis və məlumat mərkəzlərində yaygındır.
* **10 Gbps (10-Gigabit Ethernet)**: Böyük şəbəkələr və data mərkəzlərində yüksək performans tələb edən tətbiqlər üçün istifadə olunur.
* **Yüksək sürətlər (40 Gbps, 100 Gbps və daha çox)**: Bu sürətlər böyük müəssisələr və təchizatçıların xidmət göstərdiyi yüksək bant genişliyi tələb edən şəbəkələrdə istifadə olunur.

Bu sürətlər, Ethernet texnologiyasının inkişafı ilə birlikdə daha yüksək performans və genişlənmə imkanları təmin edir. Hər bir sürət dərəcəsi müvafiq cihazlar və şəbəkə infrastrukturuna uyğun şəkildə təyin edilir.

**Sual 4. Ethernet çərçivəsinin quruluşu və kapsullaşdırma prosesi haqqında geniş izahat verin. Ethernet çərçivəsinin sahələrini (destination MAC, source MAC, type/length, payload, FCS və s.) izah edin və hər sahənin funksiyasını nəzəri şəkildə açıqlayın. Kapsullaşdırma nədir və məlumat OSI modelində hansı ardıcıllıqla kapsullaşdırılır? Ethernet çərçivəsinin OSI modelinin hansı təbəqəsində formalaşdığını və bu təbəqənin digər təbəqələrlə əlaqəsini izah edin.**

**Cavab:** Ethernet çərçivəsinin sahələri və funksiyaları:

Destination MAC Address: Ethernet çərçivəsinin ilk sahəsidir və 6 baytdan ibarətdir. Bu sahə çərçivənin göndərildiyi cihazın MAC ünvanını saxlayır. Yəni məlumatın hansı cihaz üçün nəzərdə tutulduğunu göstərir.

Source MAC Address: Növbəti 6 bayt mənbə MAC ünvanını ehtiva edir. Verilənləri göndərən cihazın fiziki (MAC) ünvanını göstərir.

Type/Length: Bu sahə 2 baytdır. Əgər dəyəri 1500-dən kiçikdirsə, bu zaman sahə çərçivədəki məlumatın uzunluğunu göstərir. Əgər 1500-dən böyükdürsə, o zaman bu sahə yuxarı təbəqənin hansı protokoldan istifadə etdiyini göstərir (məsələn, IPv4 – 0x0800, ARP – 0x0806).

Payload (Məlumat hissəsi): Ethernet çərçivəsinin əsas məlumat hissəsidir. Uzunluğu 46 ilə 1500 bayt arasında dəyişir. Əgər məlumat 46 baytdan azdırsa, boşluq (padding) ilə doldurulur.

Frame Check Sequence (FCS): Bu sahə 4 baytdır və səhv aşkarlama üçün CRC (Cyclic Redundancy Check) üsulundan istifadə olunur. Məlumat ötürülməsində səhvləri aşkar etmək üçün istifadə olunur.

Kapsullaşdırma nədir və OSI modelində necə həyata keçirilir?

Kapsullaşdırma — məlumatın OSI modelində yuxarıdan aşağıya doğru ötürülərkən hər təbəqədə uyğun başlıq (və ya sonluq) əlavə olunması prosesidir. Hər bir təbəqə öz funksiyasına uyğun məlumatı əlavə edir və nəticədə çərçivə əmələ gəlir.

OSI modelində kapsullaşdırma ardıcıllığı:

**Application Layer → Transport Layer → Network Layer → Data Link Layer → Physical Layer**

Ethernet çərçivəsinin OSI modelində formalaşdığı təbəqə və əlaqələr:

Ethernet çərçivəsi Verilənlərin ötürülməsi təbəqəsində (Data Link Layer) formalaşır. Bu təbəqə yuxarı təbəqədən (Network Layer) aldığı IP paketinə MAC başlıqları əlavə edir və çərçivəni yaradır.

Daha sonra bu çərçivə Fiziki təbəqəyə (Physical Layer) ötürülür və burada bit axını şəklində fiziki mühitə göndərilir.Beləliklə:

* Layer 3 (Network): IP ünvanları ilə işləyir.
* Layer 2 (Data Link): MAC ünvanları və çərçivə quruluşunu təmin edir.
* Layer 1 (Physical): Bitlər səviyyəsində ötürülmə baş verir.

**Sual 5. Ethernet şəbəkələrində çətinlik yaradan əsas problemləri izah edin. Collision domain və broadcast domain anlayışlarını izah edin, bu anlayışların şəbəkə performansına necə təsir etdiyini nəzəri şəkildə izah edin. Şəbəkədə yayımlanan (broadcast) trafik nədir və bu trafikin şəbəkə resurslarına təsirini izah edin.**

**Cavab:** Ethernet şəbəkələrində ən çox rast gəlinən problemlər toqquşmalar (collisions) və broadcast storm-dur. Toqquşmalar xüsusilə köhnə hub əsaslı şəbəkələrdə yarım-dupleks rejimində baş verir. Bu zaman iki və ya daha çox cihaz eyni anda məlumat göndərməyə çalışdıqda siqnallar bir-biri ilə toqquşur və beləliklə paket itkisi baş verir. Bu problemin həlli üçün əsas üsul switchlərin istifadəsidir. Switchlər hər bir port üçün ayrı-ayrı collision domain yaradaraq toqquşmaların qarşısını alır və full-duplex ünsiyyətə imkan yaradır.

Broadcast storm isə şəbəkədə çox sayda broadcast paketlərinin yayılması nəticəsində yaranır. Bu paketlər (ARP, DHCP kimi) şəbəkənin bütün cihazlarına çatdığı üçün lazımsız şəkildə bant genişliyini sərf edir və CPU yükünü artırır. Bu problemin həlli üçün ən effektiv üsul VLAN texnologiyasının tətbiqidir ki, bu da broadcast domainləri kiçiltməyə kömək edir. VLAN texnologiyası şəbəkəni məntiqi baxımdan bölünmüş kiçik hissələrə bölür. Bundan əlavə, routerlar hər bir interface üçün ayrı broadcast domain yaratmaqla bu problemin qarşısını almaqda kömək edir.

Broadcast domain, şəbəkədə bir cihazın göndərdiyi broadcast paketinin çata biləcəyi bütün cihazların olduğu məntiqi sahədir. Məsələn, bir switchə qoşulmuş bütün cihazlar tək bir broadcast domain təşkil edir. Bu o deməkdir ki, hər hansı bir cihazın göndərdiyi broadcast paketi (məsələn, ARP sorğusu) şəbəkənin bütün digər cihazlarına çatacaq.

**Broadcast trafikinin şəbəkəyə əsas təsirləri üç qrupa bölünə bilər:** Birincisi, bant genişliyinin səmərəsiz istifadəsinə səbəb olur, çünki lazım olmayan cihazlara çatan paketlər şəbəkə resurslarını boşa sərf edir. İkincisi, bütün qəbuledicilərin bu paketləri emal etmə zərurəti CPU yükünü qeyri-mütənasib şəkildə artırır. Üçüncüsü və ən kritiki olaraq, ARP spoofing kimi kiberhücumlar üçün potensial təhlükəsizlik boşluğu yaradır. Bu faktorlar birgə şəbəkə performansının aşağı düşməsinə və sistem təhlükəsizliyinin zəifləməsinə gətirib çıxarır ki, bu da xüsusilə böyük şəbəkələrdə ciddi problemlər yarada bilər.

### **Collision Domain və Onun Təsiri**

Collision domain anlayışı Ethernet şəbəkələrində xüsusi əhəmiyyət kəsb edir. Bu, eyni şəbəkə seqmentində olan və bir-biri ilə toqquşa bilən cihazlar qrupudur. Köhnə hub əsaslı şəbəkələrdə bütün portlar tək bir collision domainə daxil idi, bu da şəbəkə performansını ciddi şəkildə məhdudlaşdırırdı. Müasir switchlər isə hər bir port üçün ayrı collision domain yaradaraq bu problemi aradan qaldırır. Bu yanaşma şəbəkənin ümumi performansını xeyli artırır və full-duplex ünsiyyətə imkan yaradır.

**Sual 6. TCP/IP modelinin ümumi quruluşunu və əsas funksiyalarını izah edin. TCP/IP modelindəki təbəqələrin adlarını sadalayın və hər bir təbəqənin şəbəkə fəaliyyətindəki rolunu qısa şəkildə izah edin. TCP/IP modeli ilə OSI modeli arasında əsas fərqlər hansılardır?**

**Cavab:** TCP/IP modelinin ümumi quruluşu və əsas funksiyaları:

TCP/IP modeli açıq standartlara əsaslanan və müxtəlif növ şəbəkə sistemlərinin qarşılıqlı əlaqəsini təmin edən protokollar dəstidir. Bu model kompüterlər arasında məlumatların etibarlı və düzgün ötürülməsini təmin etmək məqsədilə yaradılmışdır. TCP/IP protokol dəsti həm kiçik, həm də böyük ölçülü şəbəkələrdə istifadə olunur və internet şəbəkəsinin əsasını təşkil edir. TCP/IP modeli müxtəlif istehsalçıların avadanlıqları və proqram təminatları arasında qarşılıqlı əlaqəni təmin edir.

TCP/IP modelindəki təbəqələrin adları və şəbəkə fəaliyyətindəki rolları:

1. Tətbiq (Application) təbəqəsi: Bu təbəqə istifadəçilərə şəbəkə xidmətlərinə çıxış imkanı verir. Elektron poçt, fayl ötürülməsi və uzaqdan giriş kimi xidmətlər bu təbəqədə həyata keçirilir.
2. Nəqliyyat (Transport) təbəqəsi: Bu təbəqə iki son nöqtə arasında etibarlı və ardıcıl məlumat ötürülməsini təmin edir. TCP (Transmission Control Protocol) və UDP (User Datagram Protocol) bu təbəqəyə aiddir.
3. Şəbəkə (Internet) təbəqəsi: Bu təbəqənin əsas funksiyası məlumat paketlərinin mənbədən təyinat nöqtəsinə çatdırılması üçün marşrutlaşdırmanın həyata keçirilməsidir. IP (Internet Protocol) bu təbəqədə əsas rol oynayır.
4. Şəbəkə giriş (Network Access) təbəqəsi: Bu təbəqə fiziki mühit üzərindən məlumatların ötürülməsi və qəbul edilməsini təmin edir. Buraya həm fiziki (hardware) həm də əlaqə səviyyəsindəki protokollar daxildir.

TCP/IP modeli ilə OSI modeli arasındakı əsas fərqlər:

1. TCP/IP modeli dörd təbəqədən ibarətdir: tətbiq, nəqliyyat, şəbəkə və şəbəkə giriş təbəqəsi. OSI modeli isə yeddi təbəqədən ibarətdir: fiziki, əlaqə, şəbəkə, nəqliyyat, sessiya, təqdimat və tətbiq təbəqəsi.
2. TCP/IP modeli real şəbəkələrdə geniş istifadə olunur, OSI modeli isə nəzəri model kimi qəbul edilir və əsasən şəbəkə arxitekturasını izah etmək üçün istifadə olunur.
3. TCP/IP modelində tətbiq təbəqəsi OSI modelindəki tətbiq, təqdimat və sessiya təbəqələrinin funksiyalarını özündə birləşdirir.
4. TCP/IP modeli əvvəlcə konkret protokolların işlənib hazırlanması üçün yaradılıb, OSI modeli isə konseptual çərçivə kimi hazırlanmışdır.

**Sual 7. TCP/IP yığınına daxil olan əsas protokolları və onların funksiyalarını izah edin.**

**Cavab: TCP/IP yığını** — kompüter şəbəkələrində məlumatların necə ötürüldüyünü və qəbul edildiyini tənzimləyən bir sıra protokollardan ibarətdir. Bu model əsasən dörd təbəqədən ibarətdir: Şəbəkə girişi (Network Access), İnternet (Internet), Nəqliyyat (Transport) və Tətbiq (Application) təbəqələri. Hər bir təbəqə öz funksiyasına uyğun olaraq müxtəlif protokollardan istifadə edir və bu protokollar birlikdə internetin və digər şəbəkələrin işləməsini təmin edir.

### **1. Şəbəkə Girişi Təbəqəsi (Network Access Layer)**

Bu təbəqə məlumatların kompüterdən fiziki şəbəkə üzərindən digər cihazlara necə göndərildiyini müəyyənləşdirir. Əsas məqsəd məlumatların düzgün şəkildə paketlənməsi və fiziki mühitə ötürülməsidir.

**Ethernet** protokolu bu təbəqədə ən çox istifadə edilən texnologiyalardan biridir və məlumatların lokal şəbəkədə (LAN) ötürülməsini təmin edir. Həmçinin, **Wi-Fi**, **Frame Relay**, **ATM** kimi texnologiyalar da bu təbəqəyə aiddir. Bu təbəqədə MAC ünvanı istifadə olunur və məlumat çərçivə (frame) şəklində ötürülür.

### **2. İnternet Təbəqəsi (Internet Layer)**

Bu təbəqənin əsas funksiyası məlumat paketlərinin müxtəlif şəbəkələr arasında marşrutlaşdırılmasını (routing) təmin etməkdir. Bu təbəqə mənbədən təyinat nöqtəsinə qədər məlumatların necə çatdırılacağını müəyyən edir.

Bu təbəqənin əsas protokolu **IP (Internet Protocol)**-dur. IP protokolu məlumatları paketlərə bölür və onların düzgün ünvanlara çatdırılmasını təmin edir. IP iki əsas versiyada mövcuddur: IPv4 və IPv6.

**ICMP (Internet Control Message Protocol)** protokolu da bu təbəqəyə daxildir və şəbəkədə baş verən xətalar haqqında məlumat ötürür. Məsələn, "ping" əmri ICMP protokolundan istifadə edərək iki cihaz arasındakı əlaqəni yoxlayır.

**ARP (Address Resolution Protocol)** isə IP ünvanlarını fiziki MAC ünvanlarına çevirmək üçün istifadə olunur. Bu, bir cihazın digərini lokal şəbəkədə tanıması üçün vacibdir.

### **3. Nəqliyyat Təbəqəsi (Transport Layer)**

Nəqliyyat təbəqəsi məlumatın tətbiqlər arasında etibarlı və düzgün ardıcıllıqla ötürülməsini təmin edir. Burada məlumat segmentlərə bölünür və çatdırılarkən yenidən birləşdirilir.

Bu təbəqənin iki əsas protokolu var: **TCP (Transmission Control Protocol)** və **UDP (User Datagram Protocol)**.

**TCP** protokolu əlaqə yönümlü (connection-oriented) protokoldur və məlumatların ardıcıl və itkisiz ötürülməsini təmin edir. Məsələn, veb səhifələrin yüklənməsi və e-poçt göndərilməsi TCP ilə həyata keçirilir.

**UDP** isə əlaqəsiz (connectionless) protokoldur və məlumatı daha sürətli ötürür, amma məlumatın çatıb-çatmadığını yoxlamır. Canlı video yayımı və onlayn oyunlar kimi real vaxt tələb edən tətbiqlər UDP protokolundan istifadə edir.

### **4. Tətbiq Təbəqəsi (Application Layer)**

Bu təbəqə istifadəçilərin qarşılıqlı əlaqədə olduğu səviyyədir və müxtəlif internet xidmətlərinin həyata keçirilməsi üçün cavabdehdir. Bu təbəqədə bir çox protokol mövcuddur və onların hər biri konkret bir tətbiq növünə xidmət edir.

**HTTP (HyperText Transfer Protocol)** – veb səhifələrin serverdən brauzerə ötürülməsi üçün istifadə olunur.  
**HTTPS** – HTTP-nin şifrələnmiş və daha təhlükəsiz versiyasıdır.  
**FTP (File Transfer Protocol)** – faylların bir serverdən digər kompüterə ötürülməsi üçün istifadə olunur.  
**SMTP (Simple Mail Transfer Protocol)** – e-poçt göndərmək üçün istifadə olunur.  
**POP3 və IMAP** – e-poçtların serverdən oxunması üçün istifadə olunan protokollardır.  
**DNS (Domain Name System)** – domen adlarını (məsələn, www.example.com) IP ünvanlarına çevirir ki, kompüterlər bir-birini tapa bilsin.

TCP/IP protokol yığını internet və lokal şəbəkələrdəki bütün rabitənin əsasını təşkil edir. Bu yığının hər təbəqəsi və onun protokolları öz funksiyalarını dəqiq şəkildə yerinə yetirərək məlumatların düzgün, təhlükəsiz və etibarlı şəkildə ötürülməsini təmin edir. TCP/IP yığınına daxil olan protokollar bir-biri ilə qarşılıqlı əlaqə quraraq həm texniki, həm də istifadəçi səviyyəsində tam funksional bir şəbəkə mühiti yaradır.

**Sual 8. Alt şəbəkə nədir və hansı şəbəkə problemlərini həll etmək üçün istifadə olunur?**

**Cavab:** Alt şəbəkə (və ya subnet) – bir IP şəbəkəsinin daha kiçik hissələrə bölünməsi ilə yaranan ayrı ayrı şəbəkə seqmentləridir. Bu prosesə alt şəbəkələmə (subnetting) deyilir. Alt şəbəkələmə şəbəkə mühəndislərinə böyük və mürəkkəb şəbəkələri daha səmərəli, təhlükəsiz və idarəolunan şəkildə təşkil etməyə imkan verir. Məsələn, bir təşkilatda minlərlə cihaz ola bilər və bu cihazların hamısının eyni IP şəbəkəsində yerləşməsi ciddi texniki və inzibati problemlər yarada bilər. Bu səbəbdən şəbəkəni kiçik hissələrə – alt şəbəkələrə bölmək daha məntiqli və faydalı olur.

Alt şəbəkələmənin əsas məqsədi IP ünvan məkanının daha səmərəli istifadə olunmasıdır. IPv4 ünvanları məhduddur və bu ünvanları ehtiyaclara uyğun bölmək vacibdir. Alt şəbəkələmə vasitəsilə hər bir alt şəbəkəyə yalnız ehtiyacı qədər IP ünvan ayrılır. Bu isə ünvan israfının qarşısını alır və ünvan məkanının uzun müddət yetərli olmasına kömək edir.

Alt şəbəkələmə həmçinin şəbəkə trafikinin idarə olunması baxımından da çox vacibdir. Bütün şəbəkə vahid bir seqmentdə olduqda, bütün trafik hər yerdən keçməli olur. Bu isə şəbəkə performansını azaldır və ləngimələrə səbəb olur. Alt şəbəkələrdə isə trafik əsasən lokal olaraq qalır. Məsələn, bir şöbənin kompüterləri öz alt şəbəkəsində olduqda onların arasındakı trafik digər şöbələrə təsir etmir. Bu, trafikin lokal saxlanmasına və ümumi şəbəkə yükünün azalmasına səbəb olur.

Təhlükəsizlik baxımından da alt şəbəkələmə əhəmiyyətlidir. Fərqli şöbələr və ya istifadəçi qrupları üçün ayrı alt şəbəkələr yaradıldıqda, onların bir-birinə giriş imkanları nəzarət altında saxlanıla bilər. Məsələn, İT şöbəsinin alt şəbəkəsinə digər istifadəçilərin birbaşa çıxışı məhdudlaşdırıla bilər. Bu isə şəbəkə təhlükəsizliyinin artırılması deməkdir.

Bundan əlavə, alt şəbəkələmə idarəetməni sadələşdirir. Şəbəkə inzibatçıları hər bir alt şəbəkəni ayrıca nəzarətdə saxlayaraq daha rahat diaqnostika və konfiqurasiya edə bilirlər. Eyni zamanda, marşrutlaşdırma cədvəlləri sadələşir, çünki alt şəbəkələr üçün xüsusi marşrutlar təyin etmək mümkündür.

Nəticə olaraq, alt şəbəkələmə şəbəkənin daha çevik, təhlükəsiz, e ektiv və idarəolunan olmasını təmin edən əsas texnologiyalardan biridir. Bu üsul həm IP ünvanlarının düzgün bölgüsünü təmin edir, həm də böyük şəbəkələrdə performans və təhlükəsizlik problemlərini həll etməyə kömək edir. Şəbəkə dizaynında alt şəbəkələmə anlayışını düzgün tətbiq etmək müasir şəbəkələrin e ektiv idarə olunmasında mühüm rol oynayır.

**Alt Şəbəkələşdirmə Nümunələri**

**Nümunə 1: Şəbəkənin Alt Şəbəkələşdirilməsi**

Tutaq ki, bizdə 192.168.10.0/24 şəbəkəsi var və bu şəbəkəni 4 alt şəbəkəyə bolmək istəyirik.Addım-addım hesablamalar:- Şəbəkənin əvvəlki (default) maskası: /24 → 255.255.255.0- 4 alt şəbəkə yaratmaq uçun bizə 2 əlavə bit lazımdır: 2^2 = 4 alt şəbəkə- Yeni subnet maskası: /26 → 255.255.255.192- Hər alt şəbəkədə movcud olacaq host sayı: 2^6 - 2 = 62 host

**Sual 9. Alt şəbəkə maskasının nə olduğunu və IP ünvanının hansı hissəsinin şəbəkəyə, hansının hostlara aid olduğunu necə müəyyən etdiyini izah edin. CIDR (Classless Inter-Domain Routing) anlayışını və ənənəvi sinif əsaslı alt şəbəkə ilə fərqlərini müqayisəli şəkildə izah edin. CIDR istifadəsinin ünvan qənaətində və marşrutlama cədvəllərinin sadələşdirilməsində rolunu izah edin.**

**Cavab:** Alt şəbəkə maskası IP ünvanının şəbəkə və host (qovşaq) hissələrini ayırmağa xidmət edən **32-bitlik** bitlər ardıcıllığıdır. O, IP-ünvanla birlikdə işlənərək ünvanın hansı bitlərinin şəbəkəyə, hansı bitlərinin isə hosta aid olduğunu göstərir. Maskadakı 1 bitləri şəbəkə identifikatorunu, 0 bitləri isə host (qovşaq) identifikatorunu göstərir. Məsələn, 255.255.255.0 maskasında ilk üç bayt şəbəkə hissəsi, son bayt host hissəsi üçün nəzərdə tutulur. Şəbəkə avadanlıqları IP-ünvanı və maskanı Bitwise AND əməliyyatı ilə birləşdirərək həmin IP-ünvanın şəbəkə nömrəsini hesablayır. Bitwise AND zamanı hər iki bit 1 olduqda nəticə 1, başqa hallarda 0 olur. Beləliklə, IP-ünvanın maska ilə Bitwise AND əməliyyatının nəticəsi şəbəkə ünvanını verir, qalan bitlər isə host ünvanını təmsil edir.

**CIDR (Sinifsiz Domenlərarası Marşrutlaşdırma) anlayışı**

CIDR (“Classless Inter-Domain Routing”) sinif əsaslı (classful) ünvanlamanı əvəz edən **sinifsiz** ünvаnlama metodudur. Bu metoda görə şəbəkə hissəsinin ölçüsü / prefiks uzunluğu ilə göstərilir (məs., 192.168.1.0/24), sinif anlayışı tətbiq edilmir. CIDR şəbəkələri VLSM (variyabll uzunluqlu subnet maskası) texnikası əsasında qurulur ki, bu da ehtiyaca uyğun müxtəlif ölçülü alt şəbəkələrin yaradılmasına imkan verir.

**CIDR ilə sinif əsaslı ünvanlama arasındakı fərqlər**

Sinif əsaslı ünvanlamada IPv4 ünvanları sabit siniflərə (A, B, C, …) bölünür və hər sinif üçün şəbəkə-maskası əvvəlcədən müəyyənləşdirilir. CIDR-də isə belə sinif məhdudiyyəti yoxdur – şəbəkə bitlərinin sayı istənilən olur və ünvan prefiksi (/sayı) ilə bildirilir.

**• Ünvan paylanması:** Sinif əsaslı ünvаnlamada ünvanlar siniflərə görə A/B/C bloklarından verilir, CIDR-də isə istənilən uzunluqlu prefiksdən ibarət ip-blokları təyin oluna bilər. Bu o deməkdir ki, şəbəkə və host sahələrinin bölünməsi yalnız sinifdən asılı deyil, / prefiksi ilə elastik şəkildə müəyyən edilir.

**• Subnet maskası:** Klassik sinif metodunda A sinfi üçün default 255.0.0.0, B üçün 255.255.0.0, C üçün 255.255.255.0 kimi sabit maskalar var. CIDR-də isə maska dəyişkən olub istənilən bayt sərhədində olmaya bilər; məsələn, 255.224.0.0 və ya hətta 255.255.248.0 kimi maskalar da mümkündür. Bu, alt şəbəkələrin ölçüsünü daha dəqiq tənzimləməyə imkan verir.

**• Ünvan israfı**: Sinifli sistemdə tələbatdan çox böyük bloklar alınması ünvanların boş yerə israfına səbəb olurdu. CIDR-də isə ünvanlar ehtiyaca uyğun ölçüdə verilə bilir. Klass A/B/C blokları kimi **böyük kvotalar tələb olunmur, bu da ünvan məhdudiyyətini azaldır.**

**• VLSM dəstəyi:** Sinifli ünvаnlamada VLSM dəstəklənmirdi, CIDR isə tamamilə VLSM üzərində qurulub. Bu da müxtəlif ölçülü alt şəbəkələrin (subnet) yaradılmasına, marşrutizasiyada daha elastik idarəetməyə imkan verir.

**Marşrut cədvəllərinin sadələşdirilməsi**

CIDR marşrut cədvəllərinin ölçüsünü xeyli azaldır. Sinifsiz ünvanlama eyni prefiksli bir neçə şəbəkəni supernet (ümumi şəbəkə) halında birləşdirməyə imkan verir. Məsələn, ardıcıl IP blokları ən yaxın / prefiks altında birləşdirilərək tək marşrut olaraq elan oluna bilər. Bu yolla routerlərin yaddaşında saxlanan marşrut qeydləri sayı azalır. IETF məlumatına görə, CIDR sinifli ünvanlama məhdudiyyətini götürməklə marşrut cədvəllərinin sürətli böyüməsini ləngidib və ünvan sahəsinin tükənməsinin qarşısını almağa kömək edir. Nəticədə, internet marşrutlaşmasında daha az sayda qovşağa daha geniş ünvаn blokları elan edilə biləcəyindən, marşrutlaşdırma cədvəlləri daha yığcam olur.

**Sual 10. Alt şəbəkə dizaynının prinsiplərini və mümkün çətinliklərini izah edin. Alt şəbəkə tətbiq olunarkən nəzərə alınmalı olan vacib dizayn prinsiplərini (şəbəkə ölçüsü, host sayı, gələcək genişlənmə və s.) nəzəri şəkildə təsvir edin. Alt şəbəkələşmə zamanı rast gəlinə biləcək ümumi problemləri (overlapping subnets, mask uyğunsuzluğu və s.) izah edin. Effektiv alt şəbəkə dizaynının real şəbəkə planlamasına necə töhfə verdiyini və planlaşdırma prosesində hansı qərarların vacib olduğunu izah edin.**

**Cavab: Alt şəbəkə dizaynının əsas prinsipləri:**

1. **Şəbəkə ölçüsü və host sayı:**
   * Alt şəbəkə planlaşdırılarkən hər alt şəbəkədə neçə cihazın (hostun) olacağı müəyyən edilməlidir.
   * Gərəksiz dərəcədə böyük subnetlər ünvan israfına səbəb olur; çox kiçik subnetlər isə genişlənməyə mane olur.
2. **Gələcək genişlənmənin nəzərə alınması:**
   * Şəbəkə gələcəkdə böyüyə bilər. Buna görə alt şəbəkə planı genişlənməni nəzərə alaraq tərtib edilməlidir.
   * Əlavə host və ya subnetlər üçün yer saxlanmalıdır.
3. **Subnet maskın düzgün seçimi:**
   * CIDR (Classless Inter-Domain Routing) üsulu ilə mask seçilərək daha çevik və qənaətcil alt şəbəkələşmə mümkündür.
   * Məsələn: /24 maskı ilə 256 ünvan, /26 ilə 64 ünvan ayrılır.
4. **Loji və fiziki topologiyaya uyğunluq:**
   * Alt şəbəkələr coğrafi və funksional bölmələrə əsasən dizayn olunmalıdır.

**Alt şəbəkələşmə zamanı rast gəlinə biləcək problemlər:**

1. **Overlapping subnets (örtüşən alt şəbəkələr):**
   * Eyni IP aralığının fərqli subnetlərdə istifadə olunması marşrutlaşdırma problemlərinə səbəb olur.
2. **Mask uyğunsuzluğu:**
   * Yanlış subnet maskı nəticəsində cihazlar bir-birini eyni şəbəkədə və ya xarici şəbəkədə görə bilmir.
3. **Broadcast trafikinin artması:**
   * Alt şəbəkələr düzgün planlanmazsa, broadcast domenləri çox böyük ola bilər.
4. **Statik marşrutlar və ACL-lərdə uyğunsuzluq:**
   * Əgər düzgün subnet tətbiq olunmazsa, marşrutlaşdırma və filtrasiya qaydaları işləməyə bilər.

**Effektiv dizaynın faydaları:**

* **Təhlükəsizlik:** Şəbəkə seqmentləşməsi ilə trafik və girişi daha asan nəzarət etmək mümkündür.
* **Performans:** Kiçik subnetlərdə broadcast azalar, şəbəkə yüklənməz.
* **Asan idarəetmə:** Hər bölmənin IP planı aydın və strukturlaşdırılmış olur.
* **Marşrutlaşdırma optimallaşması:** Daha az və effektiv marşrut yazıları.

**Sual 11. Cisco IOS əməliyyat sisteminin əsas funksiyalarını və məqsədini izah edin.**

**Cavab: Cisco IOS Əməliyyat Sisteminin Əsas Funksiyaları və Məqsədi**

**Cisco IOS** (Internetwork Operating System) — **Cisco** şirkətinin yönləndiricilər (routers) və keçidlər (switches) üçün hazırladığı xüsusi **əməliyyat sistemidir**. Bu sistem Cisco avadanlıqlarının idarə olunması, şəbəkə bağlantılarının qurulması və təhlükəsizliyin təmin olunması üçün istifadə olunur.

**Cisco IOS-un əsas məqsədi:**

Cisco IOS-un əsas məqsədi şəbəkə avadanlıqlarının **idarə olunmasını** və onların **şəbəkədə düzgün işləməsini təmin etməkdir**.

**Cisco IOS-un əsas funksiyaları:**

1. **Şəbəkə interfeyslərinin idarəsi**  
   – Cisco IOS cihazdakı bütün şəbəkə portlarını və interfeysləri idarə edir. Hansı portun aktiv və ya deaktiv olduğunu müəyyən edir.
2. **Yönləndirmə (Routing)**  
   – Məlumat paketlərinin bir şəbəkədən digərinə düzgün şəkildə ötürülməsi üçün yönləndirmə protokollarından istifadə edir (məsələn, RIP, OSPF, EIGRP).
3. **Təhlükəsizlik (Security)**  
   – Cisco IOS müxtəlif təhlükəsizlik funksiyalarını dəstəkləyir: parollar, ACL-lər (Access Control List), VPN və s. Bu da şəbəkəni icazəsiz girişdən qoruyur.
4. **İstifadəçi interfeysi**  
   – Cisco IOS-da cihazları konfiqurasiya etmək üçün komanda sətri interfeysi (CLI) var. Administrator bu interfeys vasitəsilə cihazı quraşdırır və idarə edir.
5. **QoS – Xidmət keyfiyyəti (Quality of Service)**  
   – Cisco IOS bəzi məlumat növlərinə (məsələn, video və ya səs) daha çox önəm verərək şəbəkə performansını tənzimləyir.
6. **Diagnostika və monitorinq**  
   – Cisco IOS şəbəkədəki problemləri müəyyən etmək və izləmək üçün müxtəlif komandalardan istifadə etməyə imkan verir (məsələn, ping, traceroute, show komandaları).

Cisco IOS şəbəkə avadanlıqlarının "beyni" kimi işləyir. O, cihazın düzgün işləməsini təmin edir, şəbəkəni qoruyur və əlaqəni sabit saxlayır. Bu sistem şəbəkə inzibatçıları üçün çox vacibdir və şəbəkənin güclü, təhlükəsiz və effektiv olmasına kömək edir.

**Sual 12. User EXEC və Privileged EXEC rejimləri arasında fərqləri izah edin, hər rejimin funksiyalarını nəzəri olaraq açıqlayın. Global Configuration rejiminin məqsədini və bu rejimdə görülən əsas konfiqurasiya işlərini izah edin. IOS interfeysində istifadə olunan köməkçi əmrlər və kontekstə əsaslanan yardım funksiyasının (context-sensitive help) rolu barədə məlumat verin.**

**Cavab: User EXEC və Privileged EXEC rejimləri arasında fərqlər:**

1. **User EXEC rejimi:**
   * **Funksiyalar:** Bu rejim istifadəçiyə cihazın müəyyən məlumatlarını yoxlamağa imkan verir, amma konfiqurasiya dəyişiklikləri etmək mümkün deyil. Yalnız oxuma əmrləri icra edilə bilər.
   * **Əmr simvolu:** Router> (və ya cihazın adından sonra > işarəsi).
   * **Məqsəd:** Bu rejim əsasən cihazın vəziyyətini izləmək və sadə əməliyyatlar həyata keçirmək üçün istifadə olunur. Misal olaraq, cihazın şəbəkə interfeysləri haqqında məlumatları yoxlamaq üçün bu rejimdən istifadə edilir.
2. **Privileged EXEC rejimi:**
   * **Funksiyalar:** Bu rejimdə cihazın konfiqurasiyasını dəyişdirmək mümkündür. Dəyişiklik etmək, cihazın bütün parametrləri ilə işləmək və sistemin dərin konfiqurasiyasını icra etmək üçün lazım olan bütün əmrləri bu rejimdə icra etmək olar.
   * **Əmr simvolu:** Router# (və ya cihazın adından sonra # işarəsi).
   * **Məqsəd:** Cihazın idarə edilməsi və konfiqurasiyasının aparılması üçün daha geniş imkanlar təqdim edir. Bu rejim cihazın administrativ idarə edilməsində əsas rol oynayır.

**Global Configuration rejimi və məqsədi:**

* **Məqsəd:** Global Configuration rejimi, cihazın şəbəkə parametrlərini dəyişdirmək və tənzimləmək üçün istifadə edilir. Bu rejimdə global (ümumi) konfiqurasiyalar aparılır ki, onlar cihazın bütün sisteminə təsir edir.
* **Əmrlər:** Bu rejimə daxil olduqda, istifadəçi müxtəlif konfiqurasiya əmrlərini icra edə bilər. Məsələn, şəbəkə interfeyslərinin, yönləndirmə protokollarının, şifrələrin təyin edilməsi və s.
* **Əmr simvolu:** Router(config)#.

**Global Configuration rejimində əsas konfiqurasiya işləri:**

1. **İnterfeys konfiqurasiyası:** Şəbəkə interfeyslərinin (Ethernet, serial və s.) ünvanlandırılması, aktivləşdirilməsi və digər parametrlərin təyin edilməsi.
2. **Yönləndirmə protokollarının konfiqurasiyası:** OSPF, RIP və s. kimi yönləndirmə protokollarının aktivləşdirilməsi.
3. **Şifrələrin təyin edilməsi:** Cihazın müxtəlif rejimləri və interfeysləri üçün şifrələr təyin etmək.
4. **QoS və təhlükəsizlik ayarları:** Keyfiyyət təminatı (QoS) və təhlükəsizlik parametrlərinin təyin edilməsi.

**Köməkçi əmrlər və kontekstə əsaslanan yardım funksiyası:**

* **Köməkçi əmrlər (Help commands):** IOS əmrlərini daha yaxşı başa düşmək üçün istifadəçilərə kömək edən əmrlərdir. Məsələn, ? simvolu ilə əmrlərin siyahısını görmək və ya xüsusi bir əmr haqqında ətraflı məlumat əldə etmək mümkündür.
* **Kontekstə əsaslanan yardım (Context-sensitive help):** Bu xüsusiyyət istifadəçiyə əmrlərin nə zaman və necə istifadə olunacağı barədə məlumat verir. Məsələn, əgər istifadəçi yalnız əmrin bir hissəsini yazarsa və sonra ? istifadə edərsə, IOS həmin kontekstə uyğun əmrləri və ya variantları göstərəcək. Bu, istifadəçinin əmrləri düzgün yazmasına kömək edir.

User EXEC rejimi istifadəçiyə sadə məlumatları oxumağa, Privileged EXEC rejimi isə cihazın daha geniş idarə edilməsinə imkan verir. Global Configuration rejimi isə cihazın konfiqurasiyasını dəyişmək üçün nəzərdə tutulub. Köməkçi əmrlər və kontekstə əsaslanan yardım funksiyaları, istifadəçilərin IOS əmrlərini daha effektiv və doğru şəkildə istifadə etmələrinə kömək edir.

**Sual 13. Cisco cihazlarında istifadə olunan yaddaş növləri (RAM, ROM, NVRAM, Flash) haqqında geniş izah verin və bu yaddaşların IOS sistemindəki rollarını qeyd edin. Running-config və startup-config fayllarının fərqlərini və bu faylların yaddaş növlərində yerləşdirilmə prinsiplərini nəzəri şəkildə izah edin. IOS fayl sisteminin strukturu, fayl adlandırma qaydaları və konfiqurasiya saxlanması prinsipləri barədə ətraflı izahat verin.**

**Cavab:** Cisco cihazlarında istifadə olunan yaddaş növləri şəbəkə cihazlarının düzgün işləməsini təmin etmək üçün çox vacibdir. Bu yaddaş növləri RAM, ROM, NVRAM və Flash-dan ibarətdir və hər birinin fərqli funksiyaları və IOS sistemindəki xüsusi rolları vardır.

**RAM (Random Access Memory)** müvəqqəti yaddaş növüdür. Cihaz işləyərkən bütün aktiv əməliyyatlar və müvəqqəti məlumatlar bu yaddaşda saxlanılır. **Running-config** faylı RAM-da saxlanır və bu fayl cihazın cari konfiqurasiyasını göstərir. Running-config faylında edilən dəyişikliklər dərhal tətbiq olunur və cihazın fəaliyyətinə təsir edir. Ancaq cihaz yenidən başladıqda, RAM-da saxlanılan bütün məlumatlar itir, çünki RAM yalnız müvəqqəti məlumatları saxlamaq üçün nəzərdə tutulub. RAM həmçinin şəbəkə trafikinin işlənməsi, yönləndirmə cədvəllərinin saxlanması və digər müvəqqəti əməliyyatlar üçün istifadə olunur.

**ROM (Read-Only Memory)** sabit yaddaş növüdür və burada yalnız oxunabilən məlumatlar saxlanır. ROM, cihazın başlama proqramını (boot loader) və hardware diaqnostika testlərini saxlayır. Cihaz işə düşdükdə, ROM-da saxlanılan yükləyici proqram (boot loader) ilk növbədə işləyir və cihazın əməliyyat sistemini yükləməyə başlayır. ROM-da olan məlumatlar dəyişdirilə bilməz, bu da onun cihazın əsas işləmə prosesləri üçün vacib olduğunu göstərir.

**NVRAM (Non-Volatile Random Access Memory)** elektrik kəsilsə belə məlumatları saxlayan yaddaş növüdür. NVRAM, cihazın açılışında istifadə ediləcək olan **startup-config** faylını saxlayır. Startup-config faylı cihazın açılışında tətbiq olunan sabit konfiqurasiyanı ehtiva edir. Cihaz işə düşəndə, startup-config faylı NVRAM-dan RAM-a yüklənir və bu konfiqurasiya cihazın işini idarə edir. NVRAM, cihazın açılışında istifadə olunan məlumatların qorunmasını təmin edir, beləliklə cihaz hər dəfə başladıqda sabit və əvvəlki konfiqurasiya ilə işləyir.

**Flash** yaddaşı daimi yaddaş növüdür və burada **IOS əməliyyat sistemi** və digər fayllar saxlanır. Flash yaddaşı cihazın əsas əməliyyat sistemini və konfiqurasiya fayllarını saxlamaq üçün istifadə olunur. Cihaz başladıqda, Flash yaddaşında saxlanılan IOS faylı RAM-a yüklənir və cihazın işləməsini təmin edir. Flash yaddaşı, cihazın əməliyyat sisteminin saxlanması və mütəmadi olaraq yenilənməsi üçün geniş yer təklif edir. IOS-un müxtəlif versiyaları və digər fayllar Flash yaddaşında saxlanır və cihazın bu faylları yükləyərək işləməsi təmin edilir.

**Running-config** və **startup-config** fayllarının fərqləri var. **Running-config** faylı RAM-da saxlanır və cihazın o anki konfiqurasiyasını göstərir. Bu fayl cihaz işləyərkən edilən bütün dəyişiklikləri əks etdirir və dəyişikliklər dərhal tətbiq olunur. Ancaq cihaz yenidən başladıqda, running-config faylı itir, çünki RAM-da saxlanır. **Startup-config** faylı isə NVRAM-da saxlanır və bu fayl cihazın açılışında tətbiq olunan sabit konfiqurasiyanı ehtiva edir. Startup-config faylında edilən dəyişikliklər yalnız "copy running-config startup-config" əmri ilə startup-config faylına kopyalanarsa, gələcəkdə tətbiq olunur.

**IOS fayl sistemi** Cisco cihazlarında Flash yaddaşında yerləşir və burada IOS əməliyyat sistemi və digər fayllar saxlanır. IOS fayllarının adları adətən cihazın modelini və versiyasını göstərir.. Fayl adında cihazın modeli, IOS funksiyaları və versiyası əks olunur. IOS fayl sistemi Cisco cihazlarının əməliyyat sistemini düzgün şəkildə yükləyib işlətmək üçün vacibdir.

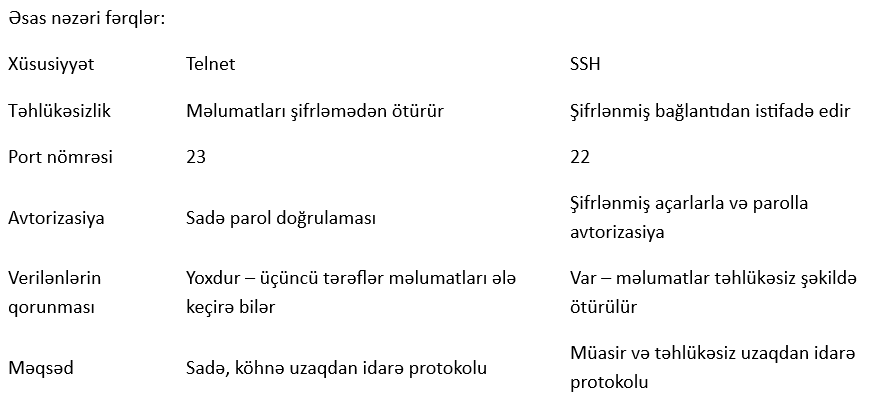
Cihazın fayl sistemi ilə işləmək üçün müxtəlif əmrlər mövcuddur. Məsələn, dir flash: əmri ilə Flash yaddaşındakı fayllar göstərilə bilər, copy running-config startup-config əmri ilə running-config faylı startup-config faylına kopyalanır. Bu əmrlər faylların idarə edilməsini və konfiqurasiyanın saxlanmasını asanlaşdırır.

Cisco cihazlarının yaddaş növləri (RAM, ROM, NVRAM, Flash) və onların IOS sistemindəki rolları şəbəkə cihazlarının konfiqurasiyasını idarə etməyə və əməliyyatların düzgün işləməsinə kömək edir. Hər bir yaddaş növü cihazın fərqli funksiyalarını və konfiqurasiya saxlanmasını təmin edir, bununla da cihazın performansı və sabitliyi artır.

**Sual 14. Telnet və SSH protokolları arasında nəzəri fərqləri sadalayın və onların təhlükəsizlik baxımından müqayisəsini verin. Hansı hallarda Telnet əvəzinə SSH istifadə edilməlidir və bunun üstünlükləri nədir?**

**Cavab: Telnet və SSH protokolları arasında nəzəri fərqlər:**

Telnet və SSH (Secure Shell) protokolları uzaqdan sistemlərə daxil olmaq üçün istifadə olunur, lakin aralarında təhlükəsizlik və funksionallıq baxımından əhəmiyyətli fərqlər mövcuddur.

****

**Təhlükəsizlik baxımından müqayisə:**

* **Telnet** – istifadəçi adı, parol və bütün məlumatlar açıq mətn (plain text) şəklində göndərilir. Bu da onu kibertəhlükələrə (sniffing, man-in-the-middle) qarşı həssas edir.
* **SSH** – bütün trafik şifrlənmiş formada ötürülür, buna görə təhlükəsizlik baxımından üstünlük təşkil edir.

Telnet əvəzinə SSH hansı hallarda istifadə olunmalıdır?

**Hər hansı bir ictimai və ya müdafiəyə ehtiyacı olan şəbəkə üzərindən uzaqdan qoşulma həyata keçiriləcəksə, SSH mütləq Telnet əvəzinə istifadə edilməlidir.**

SSH istifadə olunmasının üstünlükləri:

* Məlumatların şifrlənməsi və qorunması
* İki mərhələli autentifikasiya və açar əsaslı giriş imkanı
* Trafik izlənməsinin və dəyişdirilməsinin qarşısını alır
* Müasir sistemlər və şəbəkə təhlükəsizliyi standartları ilə uyğunluq

**Sual 15. SNMP protokolunun əsas komponentlərini (agent, manager, MIB) nəzəri baxımdan izah edin və onların şəbəkə monitorinqindəki funksiyalarını göstərin. Syslog sisteminin şəbəkə cihazlarında hadisələrin qeydi və mərkəzi loqlama baxımından əhəmiyyətini nəzəri şəkildə izah edin. Hər iki protokolun idarəetmədə istifadəsini müqayisəli şəkildə izah edin. NTP (Network Time Protocol) protokolunun şəbəkədə vaxt sinxronizasiyasında rolu və əhəmiyyəti nədir?**

**Cavab: SNMP protokolunun əsas komponentləri və funksiyaları**

SNMP (Simple Network Management Protocol) şəbəkə idarəçiliyi üçün istifadə olunan əsas protokollardan biridir. Onun üç əsas komponenti var: agent, manager və MIB. Agent şəbəkə cihazlarında (router, switch, server) quraşdırılan proqramdır və cihaz haqqında məlumat toplayaraq SNMP Manager-ə göndərir. Manager (Network Management System) isə agentlərdən məlumat alıb təhlil edən mərkəzi sistemdir. MIB (Management Information Base) isə cihazların idarə oluna bilən parametrlərinin məlumat bazasıdır və OID (Object Identifier) adlı unikal identifikatorlarla işləyir. SNMP şəbəkə monitorinqində performans izləmə, səhv aşkarlama, konfiqurasiya idarəetmə və həddindən artıq yüklənmə hallarında bildiriş göndərmə kimi funksiyaları yerinə yetirir.

**Syslog sisteminin rolu və əhəmiyyəti**

Syslog şəbəkə cihazlarında baş verən hadisələri qeyd edən standart loqlama protokoludur. Bu sistem cihazlarda baş verən bütün vacib hadisələri (səhvlər, uğursuz giriş cəhdləri, konfiqurasiya dəyişiklikləri) qeyd edir və bu loqları mərkəzi serverə göndərir. Syslog-un əsas üstünlüyü ondadır ki, o, problemlərin tez aşkarlanmasına, təhlükəsizlik auditlərinin aparılmasına və qanuni tələblərə uyğunluğun təmin edilməsinə kömək edir. Hadisələr prioritet səviyyələrinə görə çeşidlənir (Emergency, Error, Warning, Informational), bu da problemlərin təciliyyətini müəyyən etməyə imkan verir.

**SNMP və Syslog-un müqayisəli təhlili**

SNMP və Syslog şəbəkə idarəetmədə müxtəlif funksiyaları yerinə yetirir. SNMP daha çox real vaxt rejimində cihazların monitorinqi və idarə edilməsi üçün nəzərdə tutulub. O, CPU, yaddaş və bant genişliyi istifadəsi kimi statistik məlumatları toplayır və proaktiv idarəetməyə imkan verir. Syslog isə daha çox hadisələrin qeyd edilməsi və sonradan təhlili üçün nəzərdə tutulub. O, problemlərin araşdırılması, təhlükəsizlik hadisələrinin analizi və audit məqsədləri üçün vacibdir. Praktikada bu iki protokol bir-birini tamamlayır - SNMP problemləri real vaxt rejimində aşkar edir, Syslog isə onların səbəblərini müəyyən etməyə kömək edir.

**NTP protokolunun rolu və əhəmiyyəti**

NTP (Network Time Protocol) şəbəkədəki bütün cihazların vaxtının dəqiq sinxronizasiyasını təmin edir. Bu protokol xüsusi əhəmiyyət kəsb edir, çünki şəbəkə idarəçiliyinin bir çox aspektləri dəqiq vaxt tələb edir. Bu, çox sadə görünsə də, çox vacibdir, çünki bu gün edilən bir çox əməliyyat zaman və tarix möhürü ilə qeyd olunur. Verilənlər bazalarını düşünün — bir server, ona qoşulmuş maşınlarla saniyəlik belə bir uyğunsuzluqla sinxronlaşdırılmadıqda çox pis bir şəkildə pozula və hətta çökə bilər. Məsələn, bir maşın tərəfindən səhər saat 1:50-də daxil edilmiş bir əməliyyat server tərəfindən saat 1:45-də qeydə alındığında, bu əməliyyatın qeydə alınması mümkün olmaz. Loqların düzgün təhlili üçün bütün cihazlarda vaxtın sinxron olması vacibdir. NTP mərkəzi server vasitəsilə bütün şəbəkə cihazlarına vaxt təyin edir və bu, təhlükəsizlik auditlərinin etibarlılığını, həmçinin qanuni tələblərə uyğunluğu təmin edir. Vaxt sinxronizasiyası olmadan SNMP və Syslog kimi sistemlərin düzgün işləməsi mümkün deyil.

**Sual 16. Cisco IOS-da istifadə olunan fayl sisteminin strukturunu (direktoriyalar, fayl adları, fayl tipləri) izah edin. Faylların silinməsi, saxlanması və bərpası üçün nəzərdə tutulmuş əməliyyatları(copy, delete, write və s.) izah edin. Fayl sisteminin düzgün idarəsinin təhlükəsizlik və konfiqurasiya sabitliyi baxımından əhəmiyyətini nəzəri olaraq izah edin.**

**Cavab:** Cisco IOS-da istifadə olunan fayl sisteminin strukturu:

Cisco IOS-un fayl sistemi müxtəlif direktoriyalar və bu direktoriyalarda yerləşən fayllardan ibarətdir. Fayl sistemi istifadəçiyə şəbəkə cihazındakı fayllara baxmaq, onları idarə etmək və dəyişikliklər etmək imkanı verir. Fayl adları müəyyən qaydalara əsaslanır və müxtəlif tip fayllar (məsələn, konfiqurasiya faylları, image faylları) bu struktura uyğun saxlanılır. Fayl sistemi içində istifadəçi fərqli direktoriyalara keçə bilər, direktoriyaların məzmununu siyahıya sala bilər və konkret fayllarla işləyə bilər. Bu, həmçinin müxtəlif əməliyyatların icrası üçün lazım olan çevikliyi təmin edir.

Faylların silinməsi, saxlanması və bərpası üçün əməliyyatlar:

**Copy:** Faylların bir mənbədən digərinə kopyalanmasını təmin edir. Məsələn, konfiqurasiya faylını flash yaddaşdan TFTP serverə və ya əksinə kopyalamaq üçün istifadə olunur.

**Delete:** İstifadəçi artıq lazım olmayan və ya köhnəlmiş faylları silmək üçün bu əmrdən istifadə edir.

**Write:** Konfiqurasiya dəyişikliklərinin yadda saxlanması üçün işlədilir ki, dəyişikliklər cihaz yenidən başladıldıqda itməsin.

Bu əmrlər Cisco IOS-un çevik idarəetməsini və fərqli vəziyyətlərə uyğunlaşmasını təmin edir.

Fayl sisteminin düzgün idarəsinin təhlükəsizlik və konfiqurasiya sabitliyi baxımından əhəmiyyəti:

Fayl sisteminin düzgün idarəsi şəbəkənin təhlükəsizlik səviyyəsinin qorunması üçün vacibdir. Autentifikasiya və istifadəçi identifikasiyası prosesləri icazəsiz girişlərin qarşısını alır və yalnız yetkili şəxslərin cihazda dəyişiklik etməsinə imkan verir. Bundan əlavə, konfiqurasiya və digər vacib faylların düzgün saxlanması şəbəkə fəaliyyətinin sabitliyi üçün önəmlidir. Əks halda, səhv silinmiş və ya itirilmiş fayllar cihazın işində pozuntuya, hətta şəbəkənin dayanmasına səbəb ola bilər. Fayl sisteminin səliqəli idarəsi həmçinin kritik vəziyyətlərdə sürətli bərpa və ehtiyat nüsxələrinin istifadəsi üçün şərait yaradır.

**Sual 17. Statik və dinamik marşurutlama anlayışlarını müqayisə edin. Dinamik marşurutlama protokollarını (məsələn RIP, OSPF) geniş formada izah edin. Statik marşurutlamanın təhlükəsizlik və idarəetmə baxımından hansı üstünlükləri və çatışmazlıqları ola bilər.**

**Cavab:** Statik və dinamik marşrutlaşdırma kompüter şəbəkələrində məlumat paketlərinin düzgün istiqamətə yönləndirilməsi üçün istifadə olunan iki əsas üsuldur. Onların hər biri fərqli vəziyyətlər üçün üstünlüklərə və çatışmazlıqlara malikdir. Aşağıda bu anlayışların geniş müqayisəsi, dinamik marşrutlaşdırma protokollarının izahı və statik marşrutlaşdırmanın təhlükəsizlik və idarəetmə baxımından təhlili verilmişdir.

### **1.Statik və Dinamik Marşrutlaşdırmanın Müqayisəsi**

**Statik marşrutlaşdırma** — şəbəkə administratoru tərəfindən əl ilə təyin olunan və dəyişməyən marşrutlardır. Hər bir marşrut konkret şəkildə yazılır və cihazlarda sabit olaraq qalır. Əgər şəbəkədə hansısa dəyişik baş verərsə (məsələn, bir marşrut kəsilərsə), bu zaman administrator həmin marşrutu yenidən əl ilə dəyişməlidir. Bu səbəbdən statik marşrutlaşdırma adətən kiçik və sabit şəbəkələrdə istifadə olunur.

**Dinamik marşrutlaşdırma** isə marşrutlaşdırıcılar arasında avtomatik məlumat mübadiləsi ilə işləyir. Burada xüsusi protokollar (məsələn, RIP və OSPF) vasitəsilə şəbəkənin topologiyası öyrənilir və ən optimal marşrutlar müəyyən edilir. Bu üsul xüsusilə iri və dəyişkən şəbəkələrdə daha uyğun hesab olunur, çünki şəbəkədə baş verən dəyişikliklərə tez və avtomatik reaksiya verir.

### **Əsas Müqayisə Bəndləri üzrə Təsvir:**

1. **Qurulma üsulu:**
   * Statik marşrutlaşdırmada marşrutlar administrator tərəfindən əl ilə yazılır.
   * Dinamik marşrutlaşdırmada isə marşrutlaşdırıcılar öz aralarında avtomatik məlumat mübadiləsi aparır.
2. **Şəbəkə dəyişikliklərinə uyğunlaşma:**
   * Statik marşrutlar dəyişikliklərə avtomatik uyğunlaşmır. Əgər bir əlaqə pozularsa, məlumatın hara yönəldiləcəyi əvvəlcədən müəyyən olunmadığı üçün trafik itə bilər.
   * Dinamik marşrutlaşdırma isə dəyişiklikləri dərhal aşkar edir və yeni optimal marşrutlar müəyyən edir.
3. **İdarəetmə rahatlığı:**
   * Kiçik və dəyişməyən şəbəkələrdə statik marşrutlaşdırma sadə və effektivdir.
   * Böyük və daimi dəyişən şəbəkələrdə isə dinamik marşrutlaşdırma idarəetməni xeyli asanlaşdırır.
4. **Təhlükəsizlik baxımından:**
   * Statik marşrutlar dəyişməz olduğu və protokol məlumat mübadiləsi aparmadığı üçün daha təhlükəsiz hesab olunur. Xaricdən müdaxilə ehtimalı azdır.
   * Dinamik marşrutlaşdırma protokolları məlumat yaydığı üçün bu məlumatlar ələ keçirilə və marşrutlar manipulyasiya oluna bilər.
5. **Rəqəmsal resurs istifadəsi:**
   * Statik marşrutlar üçün cihazlar çox az yaddaş və CPU istifadə edir.
   * Dinamik marşrutlaşdırma isə mütəmadi hesablama və təhlil apardığı üçün daha çox resurs tələb edir.
6. **Texniki bacarıq tələbi:**
   * Statik marşrutlaşdırma üçün administratorun şəbəkənin strukturunu tam bilməsi vacibdir.
   * Dinamik marşrutlaşdırma quraşdırıldıqdan sonra daha az texniki müdaxilə tələb edir
   * Sonda qeyd etmək olar ki, **statik marşrutlaşdırma** daha çox **sabit, sadə və təhlükəsiz şəbəkələrdə**, **dinamik marşrutlaşdırma** isə **mürəkkəb, dəyişkən və böyük şəbəkələrdə** tətbiq olunmalıdır. Hər iki üsulun özünəməxsus üstünlükləri və çatışmazlıqları vardır və konkret şəbəkə ehtiyaclarına əsasən seçilməlidirlər.

### **2. Dinamik Marşrutlaşdırma Protokolları**

Dinamik marşrutlaşdırma protokolları şəbəkə marşrutlaşdırıcılarının bir-biri ilə əlaqə quraraq optimal marşrutları avtomatik müəyyən etməsinə imkan verir. Bu protokollar iki əsas kateqoriyaya bölünür:

#### **A. Distance Vector Protokolları (Məsafə və istiqamətə əsaslanır)**

##### **RIP (Routing Information Protocol)**

* **Əsas xüsusiyyətləri:**
  + Hər marşrutun dəyəri (metric) hop sayı ilə ölçülür (maksimum 15 hop).
  + 16 hop isə əldə olunmaz (unreachable) marşrut sayılır.
  + Marşrut məlumatları 30 saniyədən bir yayılır (broadcast).
* **Üstünlükləri:**
  + Sadə və asan tətbiq olunur.
  + Kiçik şəbəkələr üçün uyğundur.
* **Çatışmazlıqları:**
  + Yavaş konvergensiya (dəyişikliklərə cavab gecdir).
  + Dəqiq marşrut seçimi yoxdur (yalnız hop sayına əsaslanır).
  + Yalnız kiçik ölçülü şəbəkələrdə effektiv işləyir.

#### **B. Link-State Protokolları (Hər interfeysin vəziyyətinə əsaslanır)**

##### **OSPF (Open Shortest Path First)**

* **Əsas xüsusiyyətləri:**
  + Marşrut seçimini Dijkstra alqoritmi ilə həyata keçirir.
  + Şəbəkə topologiyası haqqında daha ətraflı məlumat toplayır.
  + Böyük şəbəkələr üçün zonalara (areas) bölünərək idarə olunur.
* **Üstünlükləri:**
  + Sürətli konvergensiya.
  + Metrika bir çox faktoru nəzərə alır (bandwidth, cost və s.).
  + Böyük və mürəkkəb şəbəkələrdə yüksək performans göstərir.
* **Çatışmazlıqları:**
  + Quraşdırılması və idarə edilməsi RIP-ə nisbətən daha çətindir.
  + Daha çox yaddaş və CPU resursları tələb edir.

### **3. Statik Marşrutlaşdırmanın Təhlükəsizlik və İdarəetmə Baxımından Təhlili**

#### **Üstünlükləri:**

1. **Təhlükəsizlik:**
   * Dinamik protokollarda olduğu kimi məlumat yayımı olmadığı üçün şəbəkənin marşrut strukturu gizli qalır.
   * Hücumçular dinamik protokolları manipulyasiya etməklə marşrut dəyişdirə bilməz.
   * Daha stabil və proqnozlaşdırıla bilən davranış sərgiləyir.
2. **İdarəetmə:**
   * Kiçik şəbəkələr üçün idarəetməsi daha sadədir.
   * Marşrutlar administratorun nəzarətində olduğu üçün dəyişikliklər tam istəyə uyğun aparılır.
   * Resurs istifadəsi çox azdır – RAM və CPU-ya təsiri minimaldır.

#### **Çatışmazlıqları:**

1. **Mərkəzləşdirilmiş dəyişiklik tələbi:**
   * Şəbəkədə bir dəyişiklik olduqda (məsələn, bir yol kəsilərsə), administrator bütün əlaqəli marşrutlaşdırıcılarda əl ilə düzəliş etməlidir.
   * Bu isə vaxt aparır və səhvlərə səbəb ola bilər.
2. **Çeviklik yoxdur:**
   * Şəbəkə dinamik olaraq dəyişirsə (yeni cihazlar qoşulursa və ya əlaqələr dəyişirsə), statik marşrutlar buna uyğun dəyişmir və məlumat itkiləri baş verə bilər.
3. **Böyük şəbəkələr üçün uyğunsuzluq:**
   * Şəbəkə böyüdükcə marşrutların sayı da artır və bunların hamısını əl ilə idarə etmək çox çətinləşir.

Statik marşrutlaşdırma daha təhlükəsiz və resurs baxımından az tələbkar olsa da, geniş və dəyişkən şəbəkələr üçün əlverişli deyil. Dinamik marşrutlaşdırma isə daha çevik və funksional olsa da, müəyyən təhlükəsizlik riskləri və konfiqurasiya çətinlikləri yarada bilər. Bu üsulların hər biri şəbəkənin ölçüsünə, strukturuna və dəyişkənliyinə əsasən seçilməlidir.

**Sual 18. Marşurutlama cədvəli nədir və hansı əsas hissələrdən (network prefix, next hop, metric və s.) ibarətdir? Marşrut seçimi zamanı router hansı kriteriyalara (administrative distance, metric, longest match) əsasən qərar verir? Eyni şəbəkəyə aid birdən çox marşrut mövcud olduqda bu marşrutların necə qiymətləndirildiyini və hansı qaydalarla tətbiq edildiyini nəzəri şəkildə izah edin.**

**Cavab: Marşrutlama Cədvəli və Marşrut Seçimi Prinsipləri**

Marşrutlama cədvəli (Routing Table), bir marşrutlayıcının və ya hostun şəbəkədə məlumatların dogru istiqamətdə oturulməsi uçun istifadə etdiyi əsas strukturdur. Routerlər bu cədvələ əsasən paketləri yonləndirir və optimal marşrut seçimi edir. Effektiv marşrutlama şəbəkənin umumi performansına və məlumat oturulməsinin surətinə birbaşa təsir gostərir.Marşrutlama şəbəkələrin duzgun işləməsi uçun vacibdir. Routerlər marşrut seçimində **ən uzun uyğunluq, idarəetmə məsafəsi və metrik** kimi kriteriyalara əsaslanırlar. Eyni şəbəkəyə aid birdən çox marşrut olduqda isə **spesifiklik, protokol etibarlılığı və metrikə görə** seçim edilir.

**Marşrutlama Cədvəlinin Əsas Hissələri**

Marşrutlama cədvəlində marşrut seçimində muhum rol oynayan aşagıdakı elementlər movcuddur:

**1. Şəbəkə Prefiksi (Network Prefix)** – Marşrutun aid oldugu şəbəkəni muəyyənləşdirən IP unvanı. Məsələn, 192.168.1.0/24, konkret bir şəbəkəni ifadə edir. Routerlər marşrut seçərkən prefiksin dəqiqliyinə baxırlar.

**2. Növbəti Addım (Next Hop)** – Paketin hədəfə çatmaq uçun gondəriləcəyi novbəti marşrutlayıcı. Routerlər birbaşa baglı olmayan şəbəkələrə paket gondərərkən əvvəl başqa bir routerə yonləndirirlər.

**3. Metrik (Metric)** – Marşrutun keyiyyətini muəyyən edən dəyərdir. Daha az metrikə malik olan marşrut daha ustun hesab edilir. RIP protokolunda hop sayına, OSPF-də isə bandwidth və gecikmə dəyərlərinə əsasən metrik hesablanır.

**4. İnterfeys (Interface)** – Routerin paketi gondərdiyi şəbəkə interfeysi. Hər bir marşrut muəyyən interfeysə baglıdır.

**5.İdarəetmə Məsafəsi (Administrative Distance - AD)** – Muxtəlif marşrutlaşdırma protokollarının etibarlılıq səviyyəsini muəyyən edən dəyərdir. Kiçik AD daha etibarlı marşrut deməkdir.

**Routerin Marşrut Seçimində İstifadə Etdiyi Kriteriyalar**

Router marşrut seçərkən aşagıdakı uç əsas kriteriyaya əsaslanır:

**1. Ən Uzun Uyğunluq (Longest Match)** – Router, ən spesfik şəbəkə prefiksinə malik olan marşrutu seçir. Məsələn:

* 192.168.1.0/24 preiksi 192.168.0.0/16 ilə muqayisədə daha spesfikdir və ustunluk təşkil edir.

**2. İdarəetmə Məsafəsi (Administrative Distance - AD)** – Muxtəlif marşrutlaşdırma protokollarından gələn marşrutlar arasında seçim edərkən router bu dəyərə baxır.

**3. Metrik (Metric)** – Eyni protokoldan olan marşrutlar arasında ən aşagı metrikə malik olan marşrut seçilir.

Birdən Çox Marşrut Mövcud Olduqda Seçim Prosesi

Əgər eyni şəbəkəyə bir neçə marşrut varsa, router bu marşrutları aşagıdakı qaydalara əsasən qiymətləndirir:

* **Ən uzun prefiksə malik olan marşrut seçilir.**
* **Eyni idarəetmə məsafəsinə malik marşrutlar arasında ən aşağı metrik seçilir.**
* **Eyni metrikə malik marşrutlar varsa, yük balanslaşdırma (load balancing) tətbiq edilə bilər.**

**Marşrutlama Protokolları və Onların Təsnifatı**

Marşrutlama protokolları iki əsas kateqoriyaya bolunur:

**1. Daxili Marşrutlama Protokolları (Interior Gateway Protocol - IGP)**

Bu protokollar bir şirkət və ya təşkilatın daxili şəbəkəsində işləyir:

**1. RIP (Routing Information Protocol)**

RIP, ən kohnə və sadə Daxili Marşrutlama Protokollarından (IGP) biridir və distance vector metodundan istifadə edir. Bu protokol hop sayına əsasən marşrut seçir və maksimum 15 hop məhdudiyyətinə malikdir.

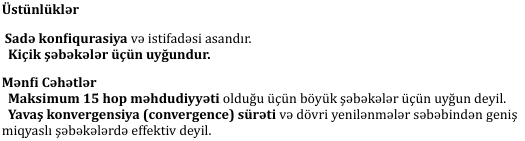
**Əsas Xüsusiyyətlər:**

**Distance-Vector:** Marşrut seçimində hop sayına əsaslanır.

**Maksimum Hop Sayı**: 15-dən boyuk hop olan marşrutlar istifadəyə yararsız sayılır.

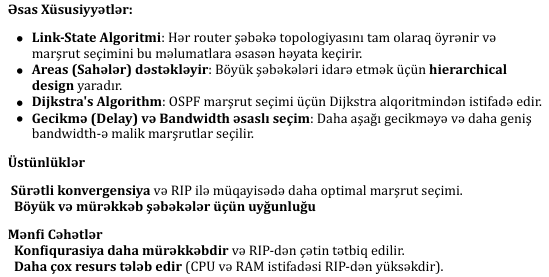
**Periodic Updates:** Şəbəkə marşrutlarını 30 saniyədə bir yeniləyir.

**UDP Port 520:** RIP mesajlarının oturulməsi uçun istifadə edilir.

****

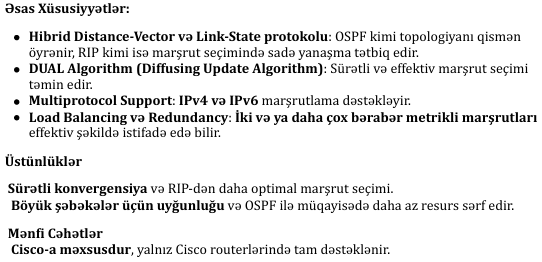
**2. OSPF (Open Shortest Path First)**

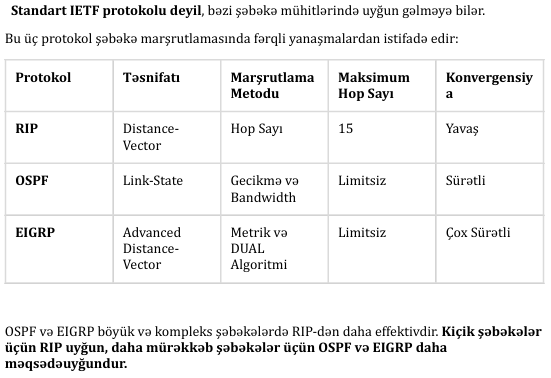
OSPF, link-state protokoludur və RIP-dən fərqli olaraq hop sayına deyil, yolun ümumi keyiyyətinə əsasən marşrut seçir. OSPF hər routerin şəbəkə topologiyasını tam bilməsinə əsaslanır və daha optimal marşrutlama təmin edir.

****

**3. EIGRP (Enhanced Interior Gateway Routing Protocol)**

EIGRP, Cisco tərəindən yaradılmış hibrid (Advanced Distance-Vector) marşrutlama protokoludur. O, distance-vector və link-state yanaşmalarını birləşdirir, daha surətli və optimal marşrutlama təmin edir.

****

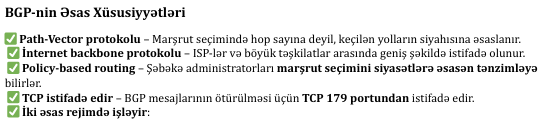
****

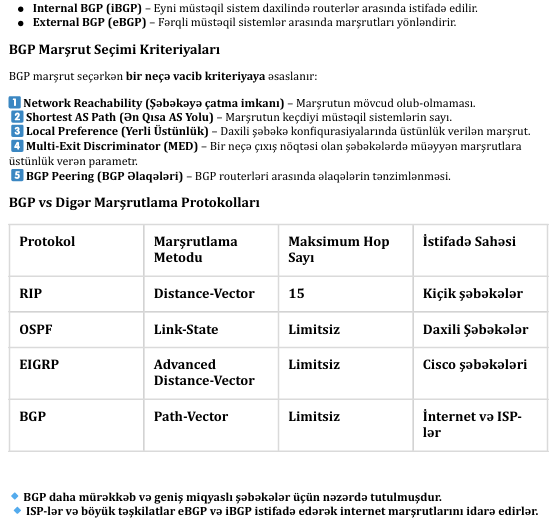
**2. Xarici Marşrutlama Protokolları (Exterior Gateway Protocol - EGP)**

Bu protokollar muxtəlif şəbəkələr arasında işləyir:

**BGP (Border Gateway Protocol) – İnternetin Marşrutlama Protokolu**

BGP (Border Gateway Protocol), İnternetin əsas marşrutlama protokolu olub, müstəqil sistemlər (Autonomous Systems - AS) arasında marşrutları idarə etmək uçun istifadə edilir. BGP, path-vector marşrutlama protokolu olaraq, marşrut seçimində hər bir şəbəkənin keçdiyi yolları nəzərə alır.BGP İnternet marşrutlamasında fundamental rol oynayan protokoldur. O, marşrut seçimində path-vector yanaşmasını tətbiq edir və mustəqil sistemlər arasında əlaqəni təmin edir. Kiçik şəbəkələr uçun uygun olmasa da, ISP-lər, böyük korporativ şəbəkələr və məlumat mərkəzləri üçün vazgeçilməzdir.

****

****

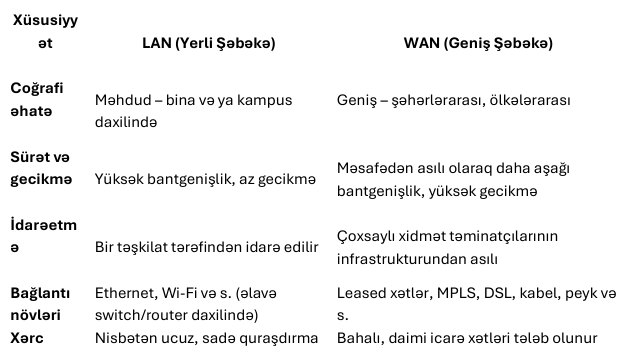
**Sual 19. WAN nədir və LAN-dan əsas nəzəri fərqləri hansılardır? WAN bağlantılarında istifadə olunan əsas texnologiyaları (məsələn: leased line, MPLS, DSL) nəzəri olaraq izah edin.**

**Cavab: WAN (Geniş Sahə Şəbəkəsi) nədir?**

Geniş Sahə Şəbəkəsi (WAN ) böyük coğrafi əraziləri əhatə edən telekommunikasiya şəbəkəsidir. WAN bir neçə məntəqəni – məsələn müxtəlif şəhər və ya ölkələrdə yerləşən ofislərin LAN-larını – birləşdirərək uzaq məsafələrdə məlumat mübadiləsini təmin edir. WAN bağlantıları adətən ictimai telekommunikasiya infrastrukturu üzərindən qurulur: şirkətlər icarəyə götürülmüş xüsusi xətlərdən (leased lines), virtual özəl şəbəkələrdən (VPN) və ya xüsusi IP-tünellərdən istifadə edərək şəbəkələri bir-birinə bağlayırlar. Nəzəri cəhətdən internet özü də ən böyük WAN nümunəsi sayılır. LAN-dan fərqli olaraq, WAN şəbəkələri fərqli provayderlərin infrastrukturu üzrə qurulduğu üçün bir neçə inzibatçı və xidmət təminatçısı iştirak edə bilər. WAN texnologiyaları geniş məsafəni əhatə etdiyinə görə məlumat ötürülməsində əlavə gecikmələr və bantgenişliyi məhdudiyyətləri ilə xarakterizə olunur, lakin uzaq məntəqələri bir-birinə bağlamaq qabiliyyətinə malikdir.

**WAN ilə LAN arasındakı əsas nəzəri fərqlər**

LAN məhdud bir ərazidə (məsələn, bina daxilində) yüksək sürət və aşağı gecikmə ilə işləyir; WAN isə şəhərlərarası və ölkələrarası məsafələri birləşdirir və bir neçə LAN-ı əhatə edir. LAN-larda əlaqənin idarə olunması və təhlükəsizliyi adi halda həmin təşkilatın özünə məxsus şəbəkə avadanlıqları (marşrutlaşdırıcı, switch) ilə həyata keçirilir. WAN-lar isə çox zaman telekommunikasiya şirkətlərinin icarəyə verdiyi xətlərə və xidmətlərə əsaslanır, yəni birdən çox provayder infrastrukturu üzrə qurulur.

****Aşağıdakı cədvəldə WAN və LAN arasındakı əsas fərqlər xülasə olunub:

**WAN bağlantılarında istifadə olunan əsas texnologiyalar**

Geniş sahə şəbəkələrində müxtəlif fiziki və protokollu texnologiyalar tətbiq olunur. Aşağıda LAN-ları uzaq məsafələrdə birləşdirmək üçün istifadə edilən əsas WAN texnologiyalarının nəzəri izahı verilmişdir:

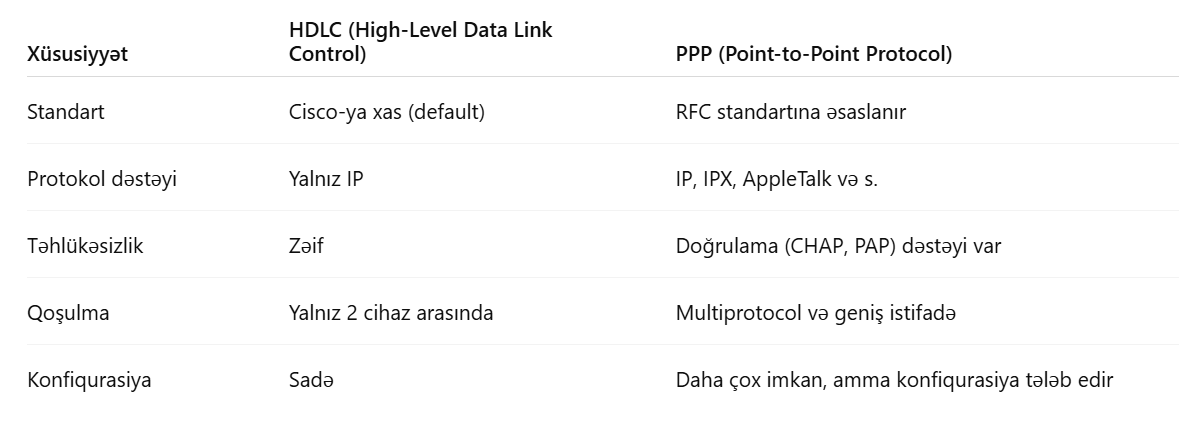
• Xəttlərin icarəsi (Leased Lines): Bu, iki məntəqə arasında daimi həsr olunmuş (point-to-point) fiziki bağlantıdır. Təşkilat hər ay telekommunikasiya provayderindən müəyyən bantgenişlikli xətti icarəyə götürür. Bu xəttlər daimi açıq bağlantı təmin etdiyi üçün səs, video və məlumat üçün ən sabit şəbəkə tipidir.Leased line-ların üstünlüyü ondadır ki, bantgenişlik statikdir və gecikmə/jitter çox azdır, lakin elastikliyə malik deyildir (əlavə bant üçün provayder müdaxiləsi tələb olunur).

• MPLS (MultiProtocol Label Switching): MPLS yüksək performanslı, çoxprotokollu yönləndirmə texnologiyasıdır. Bu texnologiya paketləri yönləndirmək üçün IP ünvanlarından çox, verilən qısa etiketlərə əsaslanır. Hər bir paketə etiket əlavə olunur və marşrutlaşdırıcılar bu etiketi oxuyaraq növbəti məntəqəni müəyyənləşdirir.

• DSL (Rəqəmsal Abunə Xətti): DSL cari telefon xətlərindən istifadə edərək yüksək sürətli məlumat ötürmə imkanı verən texnologiyadır. Xəttin abunəçi tərəfində DSL modem şəbəkədən gələn Ethernet siqnalını DSL siqnalına çevirir və telefon infrastrukturu üzrə mərkəzi ofisə ötürür.

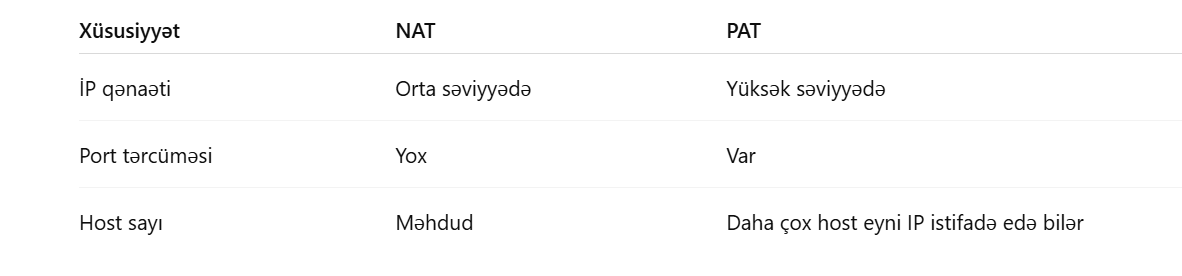
Bunlardan başqa Kabel (Coaxial broadband) Simsiz texnologiyalar (Wi-Fi, Mobil şəbəkələr) Ethernet WAN (Metro Ethernet) kimidə texnologiyalar mövcuddur.

**Sual 20. HDLC və PPP protokollarının WAN bağlantılarında istifadəsini və funksional fərqlərini nəzəri olaraq müqayisə edin. NAT (Network Address Translation) və PAT (Port Address Translation) texnologiyalarının IP ünvan qənaətində rolunu və aralarındakı nəzəri fərqləri izah edin. WAN dizaynında bu texnologiyaların təhlükəsizlik və marşrutlaşdırma baxımından necə istifadə olunduğunu izah edin.**

**Cavab:**

**NAT və PAT texnologiyalarının izahı və fərqləri:**

* **NAT (Network Address Translation):**
  + Daxili şəbəkədəki lokal IP ünvanlarının bir ictimai IP ünvanı ilə dəyişdirilməsi.
  + Məsələn, 192.168.1.2 → 203.0.113.5
* **PAT (Port Address Translation):**
  + Bir ictimai IP ünvanı üzərindən bir neçə lokal IP ünvanının port nömrələri ilə ayırd edilməsi.
  + Məsələn, 192.168.1.2:3000 və 192.168.1.3:3001 → 203.0.113.5:3000, 3001



**WAN dizaynında bu texnologiyaların rolu:**

* **Təhlükəsizlik:**
  + Daxili şəbəkə gizlədilir; xarici hostlar birbaşa daxili sistemə çıxış edə bilmir.
  + TCP/UDP portlarına əsaslanan NAT/PAT konfiqurasiyası ilə əlaqə daha sərt şəkildə idarə olunur.
* **Marşrutlaşdırma:**
  + Daxili IP-lərin marşrutlaşdırılması tələb olunmur; sadəcə NAT/PAT qovşağından keçərək çevrilir.
  + WAN yönləndiricilərində NAT tabeləri saxlanılaraq şəbəkə idarəsi asanlaşdırılır.

**Sual 21. Aşağıdakı şəbəkə topologiyalarını təsvir edin və hər birini izah edin.**

**a. Ulduz (Star)**

**b. Halqa (Ring)**

**c. Şin (Bus)**

**Cavab:**

a)Ulduz (Star) Topologiyası

Təsviri:

* Bütün cihazlar mərkəzi qurğuya (switch, hub, router) qoşulur.
* Hər cihaz ayrıca kabel ilə bağlanır.
* Topologiyanın forması ulduza bənzəyir.
* Məlumat mərkəzi qurğu üzərindən ötürülür.
* Əsasən Ethernet şəbəkələrində istifadə olunur.

Üstünlükləri:

1. Asan idarəetmə – Mərkəzi qurğu şəbəkəyə nəzarəti sadələşdirir.
2. Nasazlıq aşkarlanması – Problemli cihazı tez tapmaq olur.
3. Rahat genişlənmə – Yeni cihaz əlavə etmək çox asandır.
4. Yaxşı performans və təhlükəsizlik – Switch istifadə olunarsa, məlumatlar yalnız təyinat cihazına gedir.

Çatışmazlıqları:

1. Mərkəzi qurğuya asılılıq – O sıradan çıxarsa, şəbəkə dayanır.
2. Yüksək kabelləşmə xərci – Hər cihaz üçün ayrı kabel tələb olunur.
3. Fiziki məkan problemi – Kabellər çox olduqda idarə çətinləşir.

Nəticə:

* Sadə, güclü və genişlənə bilən bir topologiyadır.
* Mərkəzi qurğu vacib rol oynayır.
* Müasir şəbəkələrdə tez-tez istifadə olunur.
* Performans və təhlükəsizlik baxımından əlverişlidir.

b)Halqa (Ring) Topologiyası

Təsviri:

* Cihazlar dairəvi şəkildə bir-birinə bağlanır.
* Hər cihaz yalnız iki qonşu cihazla əlaqəlidir.
* Məlumat bir istiqamətdə və ya iki istiqamətdə dövr edir.
* Məlumat hər cihazdan keçərək təyinat nöqtəsinə çatır.

Üstünlükləri:

1. Sadə struktur – Kiçik şəbəkələr üçün əlverişlidir.
2. Nizamlı məlumat axını – Trafik nəzarəti asanlaşır.
3. Mərkəzi qurğuya ehtiyac yoxdur – İdarəetmə daha sadədir.
4. Balanslı mühit – Bütün cihazlar eyni hüquqa malikdir.

Çatışmazlıqları:

1. Nasazlığa həssaslıq – Bir problem bütün şəbəkəyə təsir edir.
2. Gecikmə riski – Məlumat bir neçə cihazdan keçməli olur.
3. Çətin genişlənmə – Yeni cihaz əlavə etmək çətindir.
4. Tez-tez texniki baxım – Sistem daimi nəzarət tələb edir.

Nəticə:

* Kiçik və orta ölçülü şəbəkələr üçün uyğundur.
* Müasir tələblərə görə daha az istifadə olunur.
* Sadə və balanslı olsa da, nasazlığa qarşı dayanıqsızdır.
* Bəzi xüsusi hallarda hələ də tətbiq edilir.

c)Şin (Bus) Topologiyası

Təsviri:

* Şəbəkə cihazları tək bir kabelə (backbone) qoşulur.
* Məlumat bu kabel üzərindən ötürülür.
* Yalnız təyinat cihazı məlumatı qəbul edir.
* Digər cihazlar məlumatı oxumur.
* Sadə quruluşu ilə kiçik şəbəkələr üçün uyğundur.

Üstünlükləri:

1. Sadə və ucuz – Az kabel və avadanlıq tələb edir.
2. Asan genişlənir – Yeni cihaz əlavə etmək rahatdır.
3. Mərkəzi cihaz tələb etmir – İdarəetmə sadə və ucuzdur.

Çatışmazlıqları:

1. Siqnal toqquşmaları – Eyni anda göndərişlər toqquşa bilər.
2. Kabel nasazlığı – Əsas kabel sıradan çıxsa, şəbəkə dayanır.
3. Gecikmələr – Uzaq məsafələrdə siqnal zəifləyir.
4. Terminator vacibdir – Siqnalın əksini və itkisinin qarşısını alır.

Nəticə:

* Şin topologiyası sadə və ucuzdur.
* Ancaq nasazlıqlara qarşı həssasdır.
* Müasir şəbəkələrdə nadir hallarda istifadə olunur.
* Tədris və təcrübə məqsədilə hələ də faydalıdır.

**Sual 22. Ofis şəbəkəsində iki kompüter bir-biri ilə əlaqə qura bilmir. Hər iki cihaz eyni sviçə qoşulub. Problemi diaqnostika etmək üçün hansı 3 addımı yerinə yetirməlisiniz?**

**Cavab:**

1. Fiziki bağlantını və avadanlığın vəziyyətini yoxlayın

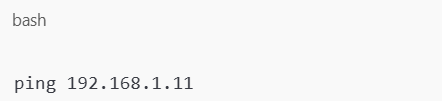
* Hər iki kompüterin şəbəkə kabelləri düzgün qoşulubmu?
  + Kabel zədəlidirsə və ya portlara tam oturmamışsa, əlaqə qurulmaya bilər.
* Sviçin port göstərici işıqlarını (LED) yoxlayın:
  + Portda kabel qoşulubsa, normalda yaşıl və ya narıncı işıq yanmalıdır.
* Sviçin və kompüterlərin şəbəkə kartlarının işlək olduğunu təsdiqləyin.
  + Kompüterlərin şəbəkə adapterlərinin deaktiv olub-olmadığını yoxlayın.
* Mümkünsə, kabeli dəyişdirin və ya başqa portdan istifadə edin.

2. IP ünvan konfiqurasiyasının və ARP cədvəlinin yoxlanılması (Layer 3 – Network Layer)

* Hər iki kompüterin IP ünvanını yoxlayın:
  + Windows-da: ipconfig
  + Linux/macOS-da: ifconfig və ya ip a
* Hər iki kompüter eyni şəbəkə daxilində olmalıdır.
  + Məsələn:
    - Kompüter 1 → 192.168.1.10
    - Kompüter 2 → 192.168.1.11
    - Subnet mask: 255.255.255.0  
      ✅ Bu halda hər iki kompüter eyni şəbəkədədir və əlaqə qura bilməlidir.
  + Əgər biri 192.168.1.10, digəri isə 10.0.0.5 ünvanına malikdirsə — ❌ bu artıq fərqli şəbəkədir və əlaqə qura bilməzlər.
* Subnet mask və default gateway-in düzgün təyin olunduğuna əmin olun.

3. Əlaqəni yoxlamaq üçün testlər və təhlükəsizlik maneələrini analiz edin

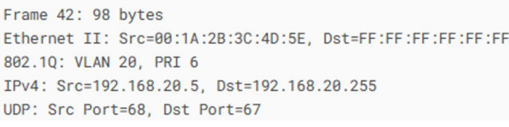
* ping əmri ilə bir kompüterdən digərinin IP ünvanına siqnal göndərin:



* + Əgər cavab gəlirsə → əlaqə var.
  + Əgər cavab gəlmirsə → əlaqə problemi mövcuddur.
* Əlavə analiz:
  + Kompüterdə firewall aktivdirsə, bu ping və digər əlaqə cəhdlərini bloklaya bilər.
  + Antivirus və ya təhlükəsizlik proqramları da şəbəkə əlaqəsinə mane ola bilər.
* arp -a əmri ilə digər kompüterin MAC ünvanını ARP cədvəlində görürsünüzmü?
  + Görünmürsə, bu layer 2 (Data Link layer) problemi ola bilər (kabel, sviç və s.)

İki kompüter arasında əlaqə problemi zamanı aşağıdakı 3 əsas diaqnostika addımı yerinə yetirilməlidir:

1. Fiziki bağlantılar və avadanlıqlar yoxlanmalıdır (kabel, port, sviç, adapterlər)
2. IP ünvanları və şəbəkə konfiqurasiyası yoxlanmalıdır (eyni subnetdə olmaları şərtdir)
3. Əlaqə testləri (ping) aparılmalı və firewall və ya digər proqram maneələri analiz edilməlidir

**Sual 23. Wireshark-da tutulmuş çərçivəni analiz edib sualları cavablandırın.**

**a) Bu hansı növ trafikdir? (DHCP, ARP, DNS?)**

**b) Niyə hədəf MAC FF:FF:FF:FF:FF:FF-dir?**

**c) PRI 6 nəyi göstərir?**

**Cavab:**

**a)** **Cavab: DHCP trafikidir.**

**Səbəb:**

* **UDP portlarına baxdıqda:** 
  + Mənbə portu (SRC Port) = 68 (DHCP Client portu)
  + Təyinat portu (Dst Port) = 67 (DHCP Server portu)
* DHCP mesajları üçün bu portlar standartdır. Bundan əlavə, IP ünvanı 192.168.20.255 (broadcast ünvanı) və MAC ünvanı FF:FF:FF:FF:FF:FF (broadcast MAC) istifadə olunması DHCP-nin kəşfiyyat (Discover) və ya sorğu (Request) mərhələlərinə uyğundur.

**b)** **Cavab: DHCP mesajı şəbəkədəki bütün qurğulara çatmaq üçün broadcast kimi göndərilib.**

**Səbəb:**

* DHCP protokolunda client (məsələn, yeni qoşulan kompüter) ilkin olaraq server tapmaq üçün broadcast istifadə edir (DHCP Discover/Request mesajları).
* FF:FF:FF:FF:FF:FF MAC ünvanı bütün şəbəkə qurğularına mesajın çatdırılmasını təmin edir. DHCP serveri bu mesajı aldıqdan sonra cavab verir (unicast və ya broadcast ilə).

**c)** **Cavab: Prioritet (Priority) 6 göstərir ki, bu çərçivəyə yüksək prioritet təyin edilib.**

**Səbəb:**

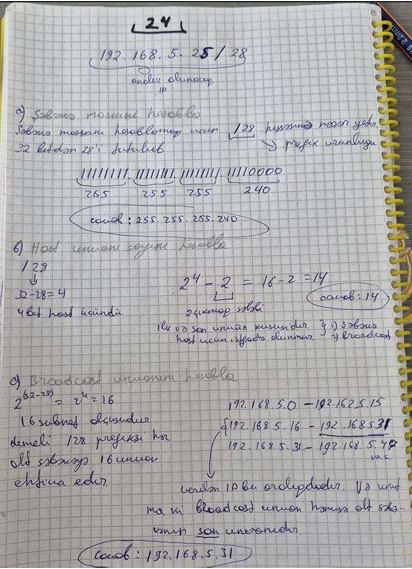
* 802.1Q teqində PRI (Priority) sahəsi 3 bitlik bir dəyərdir (0–7 aralığında). Bu, IEEE 802.1p standartına əsasən trafikə prioritet təyin edir.
* Dəyər 6 (ikilik sistemdə 110) "Critical Applications" kateqoriyasına uyğundur (məsələn, VoIP, DHCP kimi vacib şəbəkə trafiki). DHCP-nin
* prioritetli ötürülməsi onun şəbəkə üçün vacib olması ilə əlaqədardır.

**Sual 24. Aşağıdakı IP ünvanını analiz edib sualları cavablandırın: 192.168.5.25/28**

**a) Bu ünvanın alt şəbəkə maskını hesablayın**

**b) Bu alt şəbəkədə neçə host ünvanı var?**

**c) Bu alt şəbəkənin broadcast ünvanı nədir?**

**Cavab:**

**Sual 25. Bir şirkətin Ethernet şəbəkəsində yalnız Layer 2 sviçlərdən istifadə edirlər, həmin şirkətdə aşağıdakı problemlər yaşanır:**

* **Bəzən şəbəkədə broadcast storm (yayğın siqnal fırtınası) olur.**
* **Şəbəkədə loop yaranır və cihazlar cavab vermir.**
* **Bütün cihazlar birdən performans problemi yaşayır.**

**Yuxarıdakıları nəzərə alaraq, aşağıdakı tapşırıqları yerinə yetirin.**

**a) Bu problemlərin səbəbi nə ola bilər? Ən azı 2 səbəb konkret olaraq yazın.**

**b) Bu cür problemlərin qarşısını almaq üçün hansı protokolu aktivləşdirməlisiniz? (protokolun adını və qısa izahını verin.)**

**c) Sviçdə hansı əmri işlədərək bu problemi minimuma endirə bilərsiniz? (Cisco IOS əmri ilə yazın.)**

**Cavab**:

Ethernet Şəbəkə Problemləri və Həll Yolları

a) Problemlərin Səbəbləri:

1. Şəbəkədə loop (döngü) olması: Layer 2 sviçlər arasında birdən çox yol olması və bunun nəticəsində broadcast paketlərinin sonsuz dövr etməsi.

2. Spanning Tree Protocol (STP)-nin aktiv olmaması: Loop-ların qarşısını alan STP protokolunun konfiqurasiya edilməməsi və ya söndürülməsi.

b) Problemin Qarşısını Almaq Üçün Aktivləşdirilməli Protokol:

Spanning Tree Protocol (STP) - Bu protokol şəbəkədə loop-ların qarşısını almaq üçün işlədilir. STP, şəbəkədəki bütün keçidləri tarayaraq ən optimal yolu seçir və digər yolları ehtiyat (blocking) vəziyyətində saxlayır.

c) Sviçdə Problemi Minimuma Endirmək Üçün Cisco IOS Əmri:

Spanning-tree mode rapid-pvst

Bu əmr Rapid Per-VLAN Spanning Tree (RPVST+) modunu aktivləşdirir ki, bu da STP-nin daha sürətli versiyasıdır və hər VLAN üçün ayrı-ayrı spanning tree hesablayır.

**Sual 26. Wireshark-da tutduğunuz TCP əlaqəsində aşağıdakı seq/ack nömrələri vardır, bunları nəzərə alıb tapşırığı yerinə yetirin:**

****

**a. Növbəti data paketinin seq/ack nömrələri nə olar?**

**b. 150 bayt data göndərildikdə nömrələr necə dəyişər?**

**Cavab:**

Nəqliyyat təbəqəsində əlaqə (ünsiyyət) “bağlantılı” və ya “bağlantısız” ola bilər. Verilən sualda əks olunan əlaqə bağlantılıdır. Bağlantılı əlaqənin baş tutması üçün ilkin olaraq ünsiyyət qurmaq istəyən hər iki cihaz (əsasən “client” və “server”) bir-biri ilə bağlantılı ünsiyyət sessiyası qurmalıdır. Bu prosesə üçtərəfli əl sıxma (three-way handshake) deyilir. Bu sessiya qurulduqdan sonra 2 cihaz arasında məlumat mübadiləsi baş tuta bilər. Sualda qoşa nöqtədən əvvəlki hissə prosesi, sonrakı hissə isə həmin proses zamanı göndərilən paketləri göstərir. Üç tərəfli əl sıxma prosesində 3 tip proses vardır:

**SYN -** “Client” “Server” ilə sinxronizasiya edə bilmək üçün sorğu göndərir.

**SYN-ACK -** “Server” sorğunu qəbul edir və sinxronizasiyanın baş tutduğunu bildirmək üçün yenidən “Client”-a təsdiq sorğusu ötürür.

**ACK -** “Client” “Server”-in göndərdiyi sorğunu qəbul edir və sinxronizasiya baş tutur.

Bu proses baş tutduqdan sonra 2 cihaz arasında məlumat mübadiləsi yarana bilər.

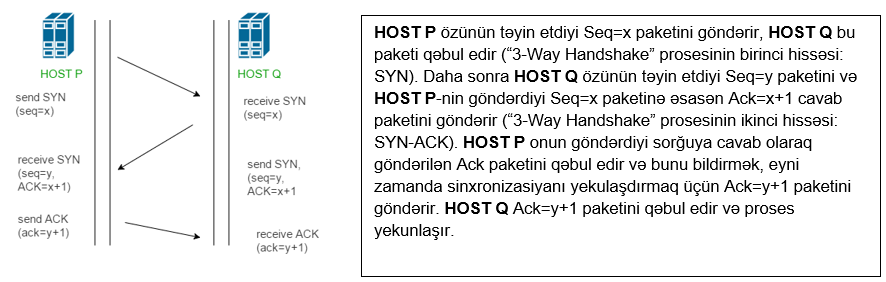
**SYN -** “Synchronize” ifadəsinin qısaltmasıdır.

**ACK -** “Acknowledgment” ifadəsinin qısaltmasıdır.

Bununla yanaşı üç tərəfli əl sıxma prosesində 2 tip paket var:

**Seq –** sorğuların göndərilməsi üçün. SYN prosesində “Client” bu paketi ilkin olaraq Seq=1000 olaraq təyin edib. “Server” isə bu paketə ilkin olaraq Seq=5000 dəyərini verib.

**Ack –** göndərilən sorğuya verilən cavabdır. “Client” tərəfindən göndərilən sorğuda Seq=1000 olduğu üçün cavab olaraq göndərilən paket Ack=1001 olacaqdır. Çünki göndərilmə zamanı Seq paketidə özüdə 1 seqment istifadə edir (TCP spesifikasiyasına əsasən:RFC 793 —> Ack=Seq+1). Bu səbəbdən cavab paketi məhz 1000 yox 1001 dəyərini alır. Eyni şəkildə “Server”-in göndərdiyi Seq=5000 paketinə də “Client” tərəfi Ack=5001 cavabını göndərir.



a. Artıq sinxronizasiya yekunlaşdığı üçün hər iki tərəf məlumat ötürə bilər. Ona görə də bu sualın cavabı növbəti paketi kimin göndərəcəyindən asılıdır.

1. “Client” göndərərsə:

Seq=1001

Ack=5001

2. “Server” göndərərsə:

Seq=5001 (“Client” Ack=5001 paketi ilə “Server”-dən Seq=5001 dəyərini gözləyir)

Ack=1001 (“Client”-in göndərdiyi Seq dəyərinə bərabərdir. SYN prosesi olmadığı üçün Ack=Seq+1 qaydasını tətbiq etmək lazım deyil. Sinxronizasiyadan sonra tətbiq olunan qayda Ack=Seq+Data olur. Heç bir məlumat ötürülmədiyi üçün Ack=Seq olaraq qalır.)

b. Bu sualın cavabı da məlumatı hansı tərəfin göndərdiyindən asılı olaraq dəyişir.

1. ”Client” göndərərsə:

Seq=1001+150=1151

Ack=5001 (Bu dəyər eyni qalır çünki “Server” yeni sorğu göndərməyib)

2. “Server” göndərərsə:

Seq=5001+150=5151

Ack=1001 (Bu dəyər eyni qalır çünki “Client” yeni sorğu göndərməyib)

**Sual 27. TCP/IP paketinin aşağıdakı sahələri verilib, aşağıdakı tapşırıqları yerinə yetirin:**

**a) Bu paket hansı xidmətə yönəlib? (xidmət adını qeyd edin)**

**b) Həmin xidmət hansı təbəqədə (OSI və TCP/IP modelinə görə) işləyir? (hər iki modelə görə yazın)**

**c) TCP protokolunun burada istifadə edilməsinin səbəbini izah edin (yəni niyə TCP istifadə olunur, UDP deyil?)**

**Cavab:**

a) Bu paket hansı xidmətə yönəlib? (xidmət adını qeyd edin)

Destination Port: 80 olduğu üçün bu paket HTTP xidmətinə yönəlib.

### b) Həmin xidmət hansı təbəqədə (OSI və TCP/IP modelinə görə) işləyir?

OSI modelinə görə: Application Layer (Tətbiq Təbəqəsi)

TCP/IP modelinə görə: Application Layer (Tətbiq Təbəqəsi)

HTTP xidməti hər iki modeldə də tətbiq səviyyəsində işləyir.

### c) TCP protokolunun burada istifadə edilməsinin səbəbini izah edin (yəni niyə TCP istifadə olunur, UDP deyil?)

TCP istifadə olunur, çünki:

HTTP xidməti etibarlı məlumat ötürülməsi tələb edir.

TCP əlaqə yönümlüdür və məlumatların ardıcıllığını, bütövlüyünü və çatdırılmasını zəmanət altına alır.

UDP isə etibarsız, əlaqəsiz bir protokoldur və belə xidmətlər üçün uyğun deyil (məs. video yayımı, DNS sorğuları üçün istifadə olunur).

**Sual 28. Bir şəbəkədə TCP/IP protokolları ilə işləyən cihazlar arasında DNS və DHCPxidmətləri düzgün işləmir. Bəzi kompüterlər IP ünvanı almır, bəziləri isə veb səhifələrə adla (məsələn, www.test.com) daxil ola bilmir. Şəbəkə tədqiqatında aşkar edilir ki, DHCP server çalışır, lakin bəzən IP ünvanı vermir və DNS server IP-sinə ping atmaq olur, amma ad çevrilməsi (resolve) işləmir. Bunları nəzərə alaraq aşağıdakı tapşırıqları yerinə yetirin.**

**a) DHCP problemi üçün hansı ilk 2 praktiki addımı atmalısınız? (konkret əmrlər və ya yoxlamalar)**

**b) DNS problemi üçün hansı əsas yoxlamanı etməlisiniz? (konkret texniki addım və səbəb yazın)**

**c) DHCP və DNS serverlərin şəbəkə üzrə necə paylanmasının daha düzgün olacağını izah edin. (məsələn, redundansı necə təmin edərdiniz?)**

**Cavab:**

Bir şəbəkədə TCP/IP protokolları ilə işləyən cihazlar arasında DNS və DHCPxidmətləri düzgün işləmir. Bəzi kompüterlər IP ünvanı almır, bəziləri isə veb səhifələrə adla (məsələn, www.test.com) daxil ola bilmir. Şəbəkə tədqiqatında aşkar edilir ki, DHCP server çalışır, lakin bəzən IP ünvanı vermir və DNS server IP-sinə ping atmaq olur, amma ad çevrilməsi (resolve) işləmir. Bunları nəzərə alaraq aşağıdakı tapşırıqları yerinə yetirin.

a) DHCP problemi üçün hansı ilk 2 praktiki addımı atmalısınız? (konkret əmrlər və ya yoxlamalar)

1. DHCP müştəri cihazında IP ünvanı təyin olunub-olunmadığını yoxlamaq:  
    Əmr: ipconfig /all  
    Bu əmr vasitəsilə kompüterin IP ünvanı, DHCP serverin ünvanı və DHCP aktiv olub-olmadığı yoxlanılır. Əgər “Autoconfiguration IP Address” (169.x.x.x) görsənirsə, bu, DHCP serverdən IP alınmadığını göstərir.
2. DHCP serverdən yenidən IP ünvanı almağa çalışmaq:  
    Əmr: ipconfig /release və sonra ipconfig /renew  
    Bu əmrlərlə müştəri əvvəlki IP-ni buraxır və DHCP serverdən yenisini tələb edir. Əgər bu uğursuz olursa, DHCP serverin cavab vermədiyi və ya şəbəkədə çatım problemi olduğu ehtimal olunur.

b) DNS problemi üçün hansı əsas yoxlamanı etməlisiniz? (konkret texniki addım və səbəb yazın)

DNS serverin ad çevirmə (name resolution) funksiyasını yoxlamaq:  
 Əmr: nslookup [www.test.com](https://www.test.com) Bu əmr DNS serverə sorğu göndərərək [www.test.com](http://www.test.com/) ünvanının IP ünvanını alıb-almadığını göstərir. Əgər cavab gəlmirsə, deməli DNS server ad çevrilməsi funksiyasını düzgün yerinə yetirmir. Bu halda DNS serverdə konfiqurasiya və ya əlaqə problemi ola bilər.

c) DHCP və DNS serverlərin şəbəkə üzrə necə paylanmasının daha düzgün olacağını izah edin. (məsələn, redundansı necə təmin edərdiniz?)

Redundant (təkrarlayıcı) DHCP və DNS serverlər yerləşdirilməlidir:  
 1) Şəbəkədə bir neçə DHCP və DNS server yerləşdirilərsə, biri sıradan çıxanda digər serverlər işləməyə davam edər.  
 2) DHCP üçün “failover” və ya “load balancing” mexanizmlərindən istifadə etmək olar.  
 3) DNS üçün isə “primary” və “secondary” DNS serverlər təyin olunmalıdır. Müştərilərdə hər iki DNS ünvanı qeyd edilməlidir ki, biri cavab vermədikdə digəri istifadə olunsun.  
 4) Serverlər fərqli şəbəkə seqmentlərində yerləşdirilərsə, şəbəkə nasazlığı halında belə xidmətlərin fasiləsizliyi təmin olunar.

**Sual 29.** 192.168.10.0/24 şəbəkəsini 4 bərabər alt şəbəkəyə bölərkən, yeni alt şəbəkə maskasını və hər bir alt şəbəkənin IP aralığını (şəbəkə ünvanı və yayım ünvanı) hesablayın.

**Cavab:**

192.168.10.0/24 şəbəkəsini 4 bərabər alt şəbəkəyə bölmək üçün aşağıdakıları hesablayırıq:

* **Yeni Alt Şəbəkə Maskası**

Əsas şəbəkə: **192.168.10.0/24**

4 bərabər alt şəbəkə yaratmaq üçün:

≥ 4 ⇒ n=2 bit əlavə

Yeni prefix:

/24+2=/26

Yeni şəbəkə maskası:

255.255.255.192

Çünki 192 🡪 11000000 (ilk 2 bit "1")

* **Hər alt şəbəkədə neçə IP ünvanı olur?**

/26 → 32-dən 26 bit şəbəkə üçün → 6 bit host üçün qalır:

IP ünvanı

Bu 64 ünvanın:

* 1-i **şəbəkə ünvanı**
* 1-i **yayım ünvanı**  
  qalır **62 usable host** ünvanı.

Alt şəbəkələr 64 ünvanlıq bloklarla irəliləyir (0, 64, 128, 192). Gəlin hər bir alt şəbəkəni ayrıca yazaq:

**Alt şəbəkə 1:**

* **Şəbəkə ünvanı:** 192.168.10.0
* **Yayım ünvanı:** 192.168.10.63
* **İstifadə edilə bilən host IP aralığı:** 192.168.10.1 – 192.168.10.62

**Alt şəbəkə 2:**

* **Şəbəkə ünvanı:** 192.168.10.64
* **Yayım ünvanı:** 192.168.10.127
* **İstifadə edilə bilən host IP aralığı:** 192.168.10.65 – 192.168.10.126

**Alt şəbəkə 3:**

* **Şəbəkə ünvanı:** 192.168.10.12
* **Yayım ünvanı:** 192.168.10.191
* **İstifadə edilə bilən host IP aralığı:** 192.168.10.129 – 192.168.10.190

**Alt şəbəkə 4:**

* **Şəbəkə ünvanı:** 192.168.10.192
* **Yayım ünvanı:** 192.168.10.255
* **İstifadə edilə bilən host IP aralığı:** 192.168.10.193 – 192.168.10.254

**Sual 30. Sizə 10.0.0.0/8 şəbəkəsi verilib və bu şəbədə 1000 cihazın yerləşəcəyi alt şəbəkələr yaratmaq istəyirsiniz. Aşağıdakı tapşırıqları nəzərə alaraq həll edin. a) Hər alt şəbəkədə ən azı 1000 cihazı yerləşdirmək üçün minimum alt şəbəkə maskası nə olmalıdır? b) Hər alt şəbəkənin neçə IP ünvanı olacaq?**

**Cavab:** Bu tip suallar alt şəbəkələşdirmə (subnetting) mövzusuna aiddir və əsas məsələ — 1000 cihaz yerləşdirmək üçün uyğun subnet maskası tapmaqdır. Gəlin ardıcıl şəkildə həll edək.

## Verilənlər:

* Verilən şəbəkə: 10.0.0.0/8 (bu, Class A şəbəkəsidir, default mask: 255.0.0.0)
* Hər alt şəbəkədə ən azı 1000 cihaz yerləşməlidir.

## a) Minimum subnet mask nə olmalıdır?

### 1. 1000 cihaz üçün neçə IP ünvan lazımdır?

IP ünvanlar aşağıdakı qayda ilə hesablanır:

*2h−2≥1000*

burada *hh*h — host (cihaz) bitlərinin sayı, "-2" isə şəbəkə və yayım ünvanı üçündür.

İndi baxaq hansı *hh*h bu şərti ödəyir:

* *29=512*  → azdır
* *210=1024*  → uyğundur

### 2. Host hissəsi 10 bit olmalıdır → 32 - 10 = 22 bit şəbəkə hissəsi

Cavab a): Minimum subnet mask: /22  
 Yəni, 255.255.252.0

## b) Hər alt şəbəkədə neçə IP ünvanı olacaq?

Subnet maskı /22 olduğuna görə host hissəsi 10 bitdir:

*210=1024*  IP u¨nvanı

Bu IP-lərdən:

* 1-i şəbəkə ünvanı
* 1-i yayım ünvanı üçün istifadə olunur

Cavab b): 1024 IP ünvanı (1000-dən çox cihaz üçün uyğundur)  
 İstifadə edilə bilən cihaz (host) sayı: 1022

**Sual 31. Sizə 172.16.0.0/16 şəbəkəsi verilib. Siz 5 alt şəbəkə yaratmalı və hər alt şəbəkədə ən azı 10.000 host ünvanı dəstəklənməli olduğunu nəzərə alaraq aşağıdakı tapşırıqları həll edin.**

**a) Hansı alt şəbəkə maskası istifadə olunmalıdır?**

**b) İlk 3 alt şəbəkənin şəbəkə ünvanlarını və yayım ünvanlarını yazın.**

**a) Hostların sayı formulu:**

Burada h — host üçün ayrılmış bitlərdir.

Burada “-2” biri şəbəkə ünvanı, biri də yayım ünvanı üçün çıxılır.

İndi h-nı tapaq:

- 2 = 8192 - 2 = 8190 → azdır.

- 2 = 16384 - 2 = 16382 → uyğundur

Deməli, bizə 14 bit host üçün lazımdır.

Maskanı tapırıq:

IPv4 ünvanı 32 bitlikdir.Eger 14 bit host uçün saxalyırıqsa,şebeke üçün

32−14=18

**Cavab a): Alt şəbəkə maskası /18 (və ya 255.255.192.0) olmalıdır.**

**b) /18 şəbəkəsində hər alt şəbəkədə:**  
 Host sayı: 2¹⁴ - 2 = 16,382  
 Addım: == 16,384 ünvan → Yəni şəbəkə blokları 16,384 IP fərqi ilə artır

1-ci alt şəbəkə:  
 Şəbəkə ünvanı: 172.16.0.0/18  
 Yayım ünvanı: 172.16.63.255

2-ci alt şəbəkə:  
 Şəbəkə ünvanı: 172.16.64.0/18  
 Yayım ünvanı: 172.16.127.255

3-cü alt şəbəkə:  
 Şəbəkə ünvanı: 172.16.128.0/18  
 Yayım ünvanı: 172.16.191.255

**Sual 32. Sizə 192.168.5.0/24 şəbəkəsi verilib və bu şəbəkəni 8 bərabər alt şəbəkəyə bölərkən, aşağıdakıları hesablayın**

**a) Yeni alt şəbəkə maskası nə olacaq?**

**b) Hər alt şəbəkədə neçə usable IP ünvan olacaq?**

**Cavab:**

a) Yeni alt şəbəkə maskası nə olacaq?

Addım 1: Mövcud şəbəkə maskası

* Verilən: /24, yəni 255.255.255.0
* Bu maska 256 IP ünvanı verir (2⁸ = 256)

Addım 2: Alt şəbəkə sayı → 8 bərabər hissə

* 8 alt şəbəkə üçün neçə bit əlavə etmək lazımdır?
  + 2ⁿ ≥ 8 → n = 3 (çünki 2³ = 8)

Addım 3: Yeni maska

* Əlavə 3 bit istifadə edirik: /24 + 3 = /27
* Yeni alt şəbəkə maskası: /27 və ya 255.255.255.224

b) Hər alt şəbəkədə neçə usable IP ünvan olacaq?

/27 maskasında:

* Hər alt şəbəkədə ümumi IP sayı = 2^(32 - 27) = 32 IP
* Usable (istifadə edilə bilən) IP = 32 - 2 = 30 IP
  + 1-i şəbəkə ünvanı
  + 1-i broadcast ünvanı
* Yeni alt şəbəkə maskası: 255.255.255.224 və ya /27
* Usable IP sayı hər alt şəbəkədə: 30 IP ünvanı

**Sual 33. Sizə 172.30.0.0/16 şəbəkəsi verilib və ən azı 500 cihaz yerləşdirə biləcəyiniz alt şəbəkələr yaradarkən, aşağıdakıları hesablayın.**

**a) Minimum hansı subnet mask istifadə olunmalıdır?**

**b) Bir alt şəbəkənin şəbəkə ünvanı və yayım ünvanını yazın.**

**Cavab:**

**a)** **Cavab: /23 subnet maskı (yaxud 255.255.254.0) istifadə olunmalıdır.**

**Hesablama:**

* /16 şəbəkəsi (172.30.0.0/16) 65,534 host ünvanı verir (2¹⁶ – 2).
* 500 cihaz üçün lazım olan host sayı:
  + Host sayı = 2ⁿ – 2 ≥ 500 → n = 9 bit (çünki 2⁹ – 2 = 510 ≥ 500).
* **Subnet mask:** 
  + Əsas şəbəkə /16 olduğundan, host üçün 9 bit ayırırıq:
    - Yeni prefix uzunluğu = 32 – 9 = /23 (yaxud 255.255.254.0).

**Yoxlama:**

* /23 şəbəkəsində 510 host mümkündür (2⁹ – 2), bu da 500-dən çoxdur.
* /22 (1022 host) də istifadə oluna bilər, lakin minimum /23 tələbə cavab verir.

**b) Nümunə alt şəbəkə:** **172.30.0.0/23**

* **Şəbəkə ünvanı (Network Address):** **172.30.0.0**
* **Yayım ünvanı (Broadcast Address): 172.30.1.255**

**Broadcast (yayım) ünvanını hesablamaq üçün:**

* 172.30.0.0/23 deməkdir ki, ilk 23 bit şəbəkə prefiksidir
* Son 9 bit host hissəsidir
* Broadcast ünvanı əldə etmək üçün host bitlərinin hamısını 1-ə çevirməliyik

**Hesablama:**

1. **/23 blokunda ünvan aralığı:**
   * Host ünvanları üçün son 9 bit sərbəstdir.
   * **172.30.0.0/23** üçün:
     + Şəbəkə ünvanı: **172.30.0.0** (bütün host bitləri 0).
     + Broadcast ünvanı: **172.30.1.255** (**son 9 bit 1, yəni .00000001.11111111**).
2. **Növbəti alt şəbəkə:**
   * **172.30.2.0/23** (hər alt şəbəkə 512 ünvanlıq blok tutur, lakin 510 host üçün istifadə olunur).

**Beləliklə:**

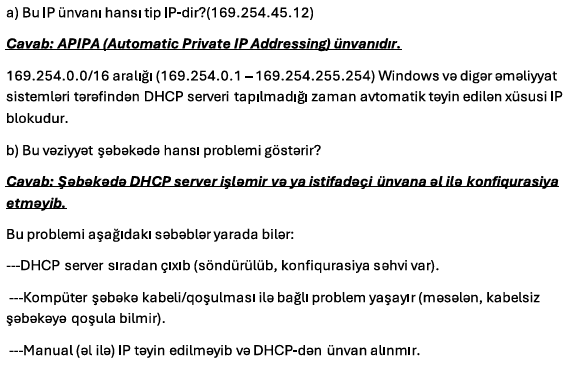
* **Şəbəkə ünvanı: 172.30.0.0/23**
* **Broadcast ünvanı: 172.30.1.255/23**

**Sual 34. Siz bir kompüterdə IP ünvanı: 169.254.45.12 və alt şəbəkə maskasını: 255.255.0.0 kimi görürsünüzsə, aşağıdakı tapşırıqları yerinə yetirin:**

**a) Bu IP ünvanı hansı tip IP-dir?**

**b) Bu vəziyyət şəbəkədə hansı problemi göstərir?**

**Cavab:**

****

**Sual 35. Siz bir kompüterdən ping 8.8.8.8 (Google DNS server) əmrini işlədirsiniz və cavab alırsınız. Amma ping www.google.com əmri cavabsız qalır. Şəbəkədə hansı problem var? Problemi necə diaqnoz edərdiniz? (ən azı 2 praktiki addım yazın)**

**Cavab:**

DNS Problem Diaqnozu və Həll Yolları

Problem:

- Ping 8.8.8.8 (Google DNS server) işləyir, yəni İnternet bağlantısı var və şəbəkə marşrutizasiyası düzgündür.

- Ping [www.google.com](http://www.google.com**) işləmir, yəni DNS çevirmə problemi var (domain adı IP-ə çevrilmir).

Problemin Səbəbləri:

1. DNS server düzgün konfiqurasiya edilməyib (məsələn, səhv DNS server ünvanı verilib və ya DNS server cavab vermir).

2. DNS cache problem (keşlənmiş qeydlər səhvdir və ya korlanıb).

3. Firewall/Bloklama (DNS sorğuları bloklanıb).

Diaqnoz Addımları (Praktiki Yoxlamalar):

1. DNS Serverı Yoxlamaq (nslookup/dig ilə test etmək)

* Windows üçün:

```cmd

Nslookup [www.google.com](http://www.google.com)

```

Əgər ”Server: UnKnown” və ya ”DNS request timed out” xətası verirsə, DNS server problemlidir.

* Linux/macOS üçün:

```bash

Dig [www.google.com](http://www.google.com)

```

Əgər ”connection timed out” və ya ”SERVFAIL” cavabı alırsınız, DNS işləmir.

2. Alternativ DNS Serverı Sınamaq (8.8.8.8 və ya 1.1.1.1 istifadə etmək)

* Əgər default DNS işləmirsə, əl ilə Google DNS (8.8.8.8) qeyd edib test etmək:

```cmd

Nslookup [www.google.com](http://www.google.com) 8.8.8.8

```

- Əgər bu işləyirsə, deməli yerli DNS server problemlidir (ISP DNS-i sıradan çıxıb).

- Əgər yenə işləmirsə, o zaman Firewall/Bloklama problemi ola bilər.

Həll Yolları:

DNS serverı dəyişmək (8.8.8.8 və ya 1.1.1.1 istifadə etmək)

DNS cache təmizləmək(Windows: `ipconfig /flushdns`, Linux/macOS: `sudo systemd-resolve –flush-caches`)

Firewall/proxy yoxlamaq (DNS portu 53 bloklanmayıb?)

Nəticə:

-Ping IP işləyir, domain işləmir → DNS problemi.

- Diaqnoz üçün: `nslookup/dig` və alternativ DNS sınaqla yoxlamaq ən sürətli üsuldur.

**Sual 36. Siz bir şəbəkədə kompüterin şəbəkəyə qoşula bilmədiyini görürsünüz. Əsas ehtimal olunan problemi tapıb, problemin həlli üçün hansı 3 konkret addımı reallaşdırılmalıdır? Tapşırığın həll edilməsi üçün aşağıdakı diaqnostika addımlarını izləyin:**

* **ipconfig əmri nəticəsində IP ünvanı düzgün görünür (192.168.1.55/24).**
* **ping 192.168.1.1 (router IP) uğurlu deyil.**
* **ping 127.0.0.1 (localhost) uğurludur.**
* **ping digər kompüterlərə də uğursuzdur.**

**Cavab:** Problemin müəyyən həllərini müəyyən etməmişdən öncə diaqnostika nəticəsində əldə etdiyimiz nəticələrə nəzər yetirməliyik.

* ipconfig əmri nəticəsində IP ünvanı düzgün görünür (192.168.1.55/24):

Bu o deməkdir ki komputer düzgün şəkildə IP ünvanı almışdır və DHCP server düzgün işləyir.

* ping 192.168.1.1 (router IP) uğurlu deyil:

Yerli routera əlaqə yoxdur. Fiziki əlaqə problemləri (kabel, wi-fi), ARP problemləri, ya da routerın söndürülməsi kimi problemlərə işarə edir. Problem şəbəkə adapteri ilə router arasındadır.

* ping 127.0.0.1 (localhost) uğurludur:

Bu test kompüterin özü ilə kommunikasiya qurub-qura bilmədiyini yoxlamaq üçün istifadə olunur. Burada 127.0.0.1 ünvanı loopback adlanır və fiziki şəbəkə kartından asılı olmayaraq, kompüterin özü ilə əlaqəni simulyasiya edir. Şəbəkə protokollarının düzgün quraşdırılıb-quraşdırılmadığını (TCP/IP) yoxlayır. Network adapterinin (şəbəkə kartının) driverinin düzgün işləyib-işləmədiyini və Firewall/Antivirusun ICMP (ping) sorğularını bloklamadığını yoxlayır. Əgər lokal ping işləyirsə, problem xarici şəbəkədədir.

* ping digər kompüterlərə də uğursuzdur:

Yerli şəbəkədə heç bir cihazla əlaqə yoxdur. Ya ümumi şəbəkə problemi var, ya da kompüterin şəbəkə siyasəti/konfiqurasiyası problemlidir. Təkcə routerla deyil, bütün şəbəkə ilə əlaqə problemi var.

Diaqnostika əsasında reallaşdırılması lazım olan 3 konkret addım:

1.Fiziki Əlaqəni Yoxlamaq (Kabel/Wi-Fi)

2.ARP Cədvəlini və MAC Ünvanını Yoxlayın

3.Router/İnterfeys Konfiqurasiyasını Sıfırlayın

**Sual 37. Cisco router-ə qoşularkən konfiqurasiyanı görmək və əsas əmrləri yoxlamaq üçün hansı Cisco IOS əmrlərindən istifadə edilir? (ən azı 2 əmr yazın)**

**Cavab:**

bunlardan 3 ve ya 4 denesini oyrensez besdir (sualda en az 2 dene isteyir)

|  |  |
| --- | --- |
| show running-config | Hazırda işləyən konfiqurasiyanı göstərir. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| show startup-config | | | | | | | | Yaddaşda saxlanılan (boot zamanı yüklənəcək) konfiqurasiyanı göstərir. | | | | | | | | | | | | | |
| show ip interface brief | | | | | | | | | | Bütün interfeyslərin IP ünvanı və statusunu qısa formada göstərir. | | | | | | | | | | |
| show interfaces | | | | İnterfeyslərin texniki vəziyyətini (trafik, error, duplex və s.) göstərir. | | | | | | | | | | | | | | |
| show version | | Router-in modeli, IOS versiyası, uptime və s. haqqında məlumat verir. | | | | | | | | | | | | | | | |
| show protocols | Hər interfeys üzrə IP protokolunun vəziyyətini göstərir. | | | | | | | | | | | | | |
| show ip route | | | | Routing cədvəlini göstərir (hansı şəbəkəyə necə çatmaq olar). | | | | | | | | | | | |
| show arp | | | IP və MAC ünvanları arasında əlaqə cədvəlini göstərir (ARP table). | | | | | | | | | | | | | |
| show vlan | | | VLAN-ların siyahısını göstərir (switch-lərdə). | | | | | | | | |
| show mac address-table | | | | | | | | | MAC ünvan cədvəlini göstərir (switch-lərdə). | | | |
| show cdp neighbors | | | | | | | Qoşulmuş Cisco cihazlarını göstərir (CDP – Cisco Discovery Protocol). | | | | | | | | | | | | |
| show clock | | | | | Sistemin saat və tarixini göstərir. | | | | | |
| show users | | | | | | Sistemdə hal-hazırda kimlərin qoşulu olduğunu göstərir. | | | | | | | |

**Sual 38. Cisco router-də bir interfeysi (GigabitEthernet0/1) aktivləşdirmək üçün lazım olan əmrləri addım-addım yazın ki, interfeys "up" vəziyyətinə gəlsin.**

**Cavab:** Cisco router-də bir interfeysi (GigabitEthernet0/1) aktivləşdirmək üçün lazım olan əmrləri addım-addım yazın ki, interfeys "up" vəziyyətinə gəlsin.

1. İstifadəçi rejimindən imtiyazlı rejimə keç:

Router> enable

1. Qlobal konfiqurasiya rejiminə daxil ol:

Router# configure terminal

1. İnterfeys rejiminə daxil ol:

Router(config)# interface GigabitEthernet0/1

1. İnterfeysi aktivləşdir:

Router(config-if)# no shutdown

1. (Əgər şəbəkə IP ünvanı verilməyibsə, interfeysə IP ünvan da təyin oluna bilər.)

Router(config-if)# ip address 192.168.1.1 255.255.255.0

1. Əlavə olaraq interfeysin "up" olub-olmadığını yoxlamaq üçün:

Router# show ip interface brief

**Sual 39. Yeni bir Cisco router-in interfeysinə (GigabitEthernet0/0) IP ünvan (IP: 192.168.100.1/24) təyin edib, şəbəkə interfeysini aktivləşdirmək üçün lazım olan IOS əmrlərini ardıcıl yazın.**

**Cavab:** Cisco router-də GigabitEthernet0/0 interfeysinə IP təyin edib aktivləşdirmək üçün əmrlər:

1. Privileged EXEC mode-a keç:

enable

1. Global Configuration mode-a daxil ol:

configure terminal

1. İnterfeysi seç:

interface GigabitEthernet0/0

1. IP ünvanı və subnet mask təyin et:

ip address 192.168.100.1 255.255.255.0

1. İnterfeysi aktivləşdir:

no shutdown

1. Konfiqurasiyadan çıx:

end

1. Yoxlamaq üçün:

show ip interface brief

*(GigabitEthernet0/0 yanında "up" statusu görsənməlidir)*

1. Konfiqurasiyanı qeyd et:

copy running-config startup-config

**Sual 40.** Siz yeni bir Cisco router-ə qoşulub onu konfiqurasiya etməlisiniz. Konfiqurasiya edərkən ilk öncə təhlükəsizlik üçün router-ə console portdan giriş üçün parol cisco123, enable rejimə keçid üçün isə parol adminpass və routerin adı BranchRouter təyin edilməlidir. Siz bu sazlama işlərini görərkən yerinə yetirilməli olan bütün IOS əmrlərini ardıcıllıqla yazın.

**Cavab:** Bu tapşırıqda Cisco router-i konfiqurasiya etmək üçün console portuna giriş parolu, enable rejimə keçid parolu və cihaz adı (hostname) təyin edilməlidir. Aşağıda sənə lazım olan bütün IOS əmrlərini ardıcıllıqla verirəm.

## Cisco Router üçün konfiqurasiya əmr ardıcıllığı:

Router> enable

Router # configure terminal

Router(config) # hostname BranchRouter

BranchRouter(config) # enable secret adminpass

BranchRouter(config) # line console 0

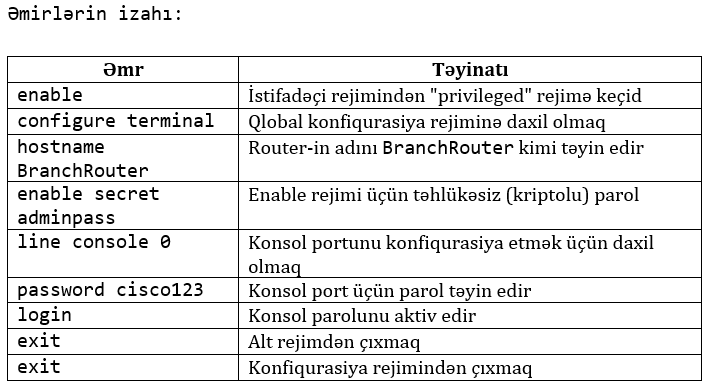
BranchRouter(config-line) # password cisco123

BranchRouter(config-line) # login

BranchRouter(config-line) # exit

BranchRouter(config) # exit

BranchRouter



**Sual 41. Cisco routerlə birbaşa əlaqədə olan zaman onun bütün aktiv interfeyslərinin IP ünvanlarını və statuslarını görmək üçün hansı Cisco IOS əmri işlədilməlidir?**

**Cavab:** Cisco routerlə birbaşa əlaqədə olanda onun bütün aktiv interfeyslərinin IP ünvanlarını və statuslarını görmək üçün aşağıdakı Cisco IOS əmri istifadə olunur:

* show ip interface brief

Bu əmr interfeyslərin adını, IP ünvanını, statusunu (up/down) və protokol vəziyyətini qısa şəkildə göstərir

Əgər interfeyslər haqqında daha ətraflı məlumat istəyiriksə, bu əmrdən istifadə edə bilərik;

* show interfaces

**Sual 42. Şəbəkədə monitorinq və troubleshooting üçün Cisco router üzərində real vaxt rejimində hansı hadisələrin (interfeys up/down olur, yeni cihaz qoşulur və ya kəsilir) baş verdiyini izləmək və bu məlumatları fayla yazmaq istəyiriksə hansı əmrlərdən istifadə edilməliyik?**

**Cavab:**

### 1. Hadisələrin real vaxtda izlənməsi üçün:

### terminal monitor

Bu əmr Telnet və ya SSH ilə qoşularkən real vaxt mesajlarını (məsələn, interfeys up/down, cihaz qoşulması/kəsilməsi) ekranda görmək üçün aktiv edilir.

Router# terminal monitor

2. Göstərilən mesajları fayla (log-a) yazmaq üçün:

a) Logging aktiv etmək:

Router(config)# logging buffered 4096

Bu, mesajların RAM-də saxlanmasını təmin edir. (4096 — bufer ölçüsüdür, istəyə görə dəyişə bilər.)

b) Göstərilən log mesajlarını yoxlamaq üçün:

Router# show logging

Bu əmr RAM-ə yazılmış bütün log mesajlarını göstərir.

**Sual 43. Siz Cisco router və ya sviçdə yeni konfiqurasiya dəyişiklikləri etdiniz və istəyirsiniz ki, bu dəyişikliklər cihaz restart edildikdən sonra itməsin. Dəyişiklikləri hansı əmr vasitəsilə yaddaşa yazırsınız?**

**Cavab:** **Cisco router və ya switch-də konfiqurasiya dəyişikliklərini yaddaşa yazmaq üçün istifadə olunan əmr:**

* copy running-config startup-config

Bu əmr cihazının aktiv konfiqurasiyasını (RAM-da olan "running-config") yaddaşa (NVRAM-da olan "startup-config") yazır. buna görə, cihaz restart dəyişikliklər itməyəcək.

* Qısa forması: copy run start

**Sual 44. Siz Cisco routerdə konfiqurasiya faylını başqa bir serverə ötürmək istəyirsiniz (məsələn, backup üçün). Server TFTP serverdir. Hansı əmrlə routerin konfiqurasiya faylını TFTP serverə göndərə bilərsiniz? (Sadəcə əmri nümunə IP ünvanı ilə yazın, məsələn: TFTP server IP-si 192.168.1.100)**

**Cavab: Cisco routerdə konfiqurasiya faylını TFTP serverə ötürmək üçün istifadə olunan əmr:**

* copy running-config tftp

Əmr daxil olduqdan sonra router sizdən TFTP serverin IP ünvanını istəyəcək. Məsələn, əgər TFTP serverin IP-si 192.168.1.100-dürsə, əmr kimi belə olacaq:

copy running-config tftp:

Address or name of remote host []? 192.168.1.100

Bu əmrlə konfiqurasiya faylı TFTP serverə ötürüləcək.

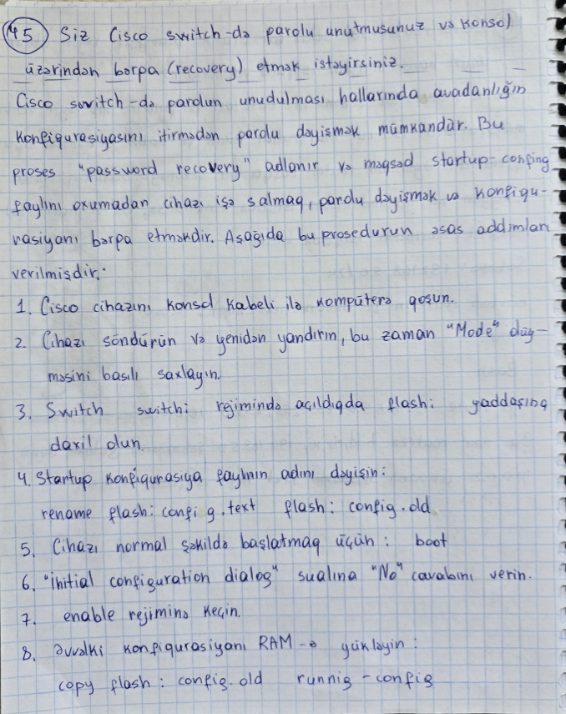
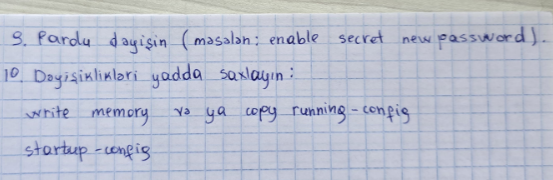
* Qısa forması: copy running-config tftp://192.168.1.100/router-config.cfg

Bu əmrlər edir:

* running-config faylını (hazırda RAM-da olan aktiv konfiqurasiya)
* 192.168.1.100IP-li TFTP serverə
* router-config.cfgadlı fayl kimi ötürür.

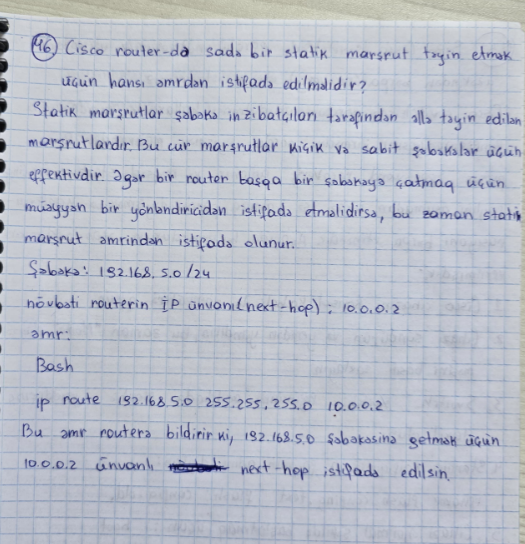
**Sual 45. Siz Cisco sviçdə parolu unutmusunuz və konsol üzərindən bərpa (recovery) etmək istəyirsiniz. Sizin məqsədiniz: cihazı reboot etmək, startup-config faylını oxumadan cihazı başlatmaq, parolu dəyişmək və konfiqurasiyanı bərpa etməkdir. Cisco cihazında parol bərpa prosedurunun əsas addımlarını sıralayın.**

**Cavab:**

**** ****

**Sual 46. Cisco router-də sadə bir statik marşrut təyin etmək üçün hansı əmri istifadə edilməlidir? (İstədiyiniz şəbəkə: 192.168.5.0/24, növbəti routerin IP ünvanı (next-hop): 10.0.0.2)**

**Cavab:**

****

**Sual 47. Şəbəkənizdə çoxlu routerlər var və siz dinamik marşrutlaşdırma üçün OSPF protokolundan istifadə etmək üçün hansı əmrləri yazmalısınız? (Routerdə şəbəkə: 192.168.10.0/24, OSPF proses ID: 1, router-in interfeysində IP ünvan: 192.168.10.1)**

**Cavab:**

Router> enable

Router# configure terminal

Router(config)# router ospf 1

Router(config-router)# network 192.168.10.0 0.0.0.255 area 0

Router(config-router)# exit

Router(config)# exit

Router# write memory

Əmrlərin izahı:

* router ospf 1 – OSPF marşrutlaşdırma prosesini 1 nömrəli proses ID ilə işə salır.
* network 192.168.10.0 0.0.0.255 area 0 – 192.168.10.0/24 şəbəkəsini OSPF-ə daxil edir və onu əsas (backbone) area 0-a təyin edir.
* 0.0.0.255 – bu wildcard maskdır və 255.255.255.0 maskasına uyğundur.
* write memory – konfiqurasiyanı yadda saxlamaq üçün istifadə olunur.

**Sual 48. Şəbəkəmizdə bir-biri ilə birbaşa bağlı A və B routerlərimiz vardır. Biz bu routerləri dinamik marşurutlama protokolu olan EIGRP- ilə əlaqələndirərkən hər iki routerdə hansı əmrləri yazmalıyıq? (Router A: 192.168.1.0/24, Router B: 192.168.2.0/24)**

**RouterA> enable**

**RouterA# configure terminal**

**RouterA(config)# router eigrp 1**

**RouterA(config-router)# network 192.168.1.0 0.0.0.255**

**RouterA(config-router)# network 10.0.0.0 0.0.0.3 ! <-- Əgər A ilə B arasında bağlantı 10.0.0.0/30-dursa**

**RouterA(config-router)# no auto-summary**

**RouterA(config-router)# exit**

**RouterA(config)# exit**

**RouterB> enable**

**RouterB# configure terminal**

**RouterB(config)# router eigrp 1**

**RouterB(config-router)# network 192.168.2.0 0.0.0.255**

**RouterB(config-router)# network 10.0.0.0 0.0.0.3 ! <-- Eyni bağlantı interfeysi**

**RouterB(config-router)# no auto-summary**

**RouterB(config-router)# exit**

**RouterB(config)# exit**

* router eigrp 1 — burada 1 EIGRP AS (Autonomous System) nömrəsidir. Hər iki routerdə bu eyni olmalıdır.
* network əmrində **wildcard mask** istifadə olunur (məsələn, 0.0.0.255 əvəzinə).
* no auto-summary — EIGRP-nin köhnə davranışında avtomatik classful şəbəkə kəsimlərinin qarşısını almaq üçün istifadə olunur. İndiki dövrdə bunu əlavə etmək tövsiyə olunur.
* A və B routerləri arasındakı birbaşa əlaqə üçün istifadə olunan interfeysin IP aralığı mütləq EIGRP konfiqurasiyasında göstərilməlidir ki, marşrutlama məlumatları ötürülsün.

**Sual 49. İki Cisco routeri birbaşa serial kabel ilə birləşdirilib (Serial0/0/0 interfeysi istifadə olunur) PPP (Point-to-Point Protocol) WAN bağlantısı qurmaq istəyirsiniz. PPP protokolunu aktivləşdirmək üçün hansı IOS əmrlərini işlədəcəksiniz? (Serial interfeysi üçün)**

**Cavab:**

* İki ədəd Cisco router var.
* Bu routerlər Serial 0/0/0 interfeysləri ilə birbaşa serial kabel vasitəsilə bir-birinə qoşulub.
* Routerlər arasında PPP protokolu ilə WAN bağlantısı qurmaq lazımdır.

Bu ssenaridə məqsəd: HDLC əvəzinə PPP protokolunu aktivləşdirməkdir.

### **1. İdarəetmə rejiminə keç**

Router> enable

Router# configure terminal

Burada **konfiqurasiya rejiminə** keçilir ki, interfeys dəyişə bilsin.

### **2. Serial interfeysə keç**

Router(config)# interface Serial 0/0/0

Bu əmr ilə **Serial 0/0/0 interfeysi** aktiv şəkildə konfiqurasiya edilir.

### **3. PPP protokolunu aktivləşdir**

Router(config-if)# encapsulation ppp

Bu əsas addımdır. **Encapsulation** (qablaşdırma) üsulunu dəyişərək **PPP** təyin edilir.

### **4. IP ünvanı təyin et**

Router A:

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router B:

Router(config-if)# ip address 192.168.1.2 255.255.255.0

**Eyni subnet** daxilində IP ünvanları verilməlidir ki, əlaqə mümkün olsun.

### **5. Interfeysi aktivləşdir**

Router(config-if)# no shutdown

Bu əmrlə interfeysi **aktiv (UP)** vəziyyətə gətirilir. Əgər bu verilməzsə, bağlantı qurulmaz.

### 6. (Əgər lazım olsa) Clock rate ver

Əgər routerlərdən biri **DCE** interfeysə sahibdirsə:

Router(config-if)# clock rate 64000

Bu əmr yalnız **DCE ucunda** verilir və **data ötürmə sürətini** təyin edir.

Nəticə:

Bu əmrləri hər iki routerdə işlədəndən sonra:

* Routerlər arasında PPP bağlantısı qurular.
* Bunu test etmək üçün bir routerdən digərinə ping ataraq yoxlaya bilərik:

RouterA# ping 192.168.1.2

Əlavə izah.

**Hər bir routerdə aşağıdakı addımları yerinə yetirin:**

**Router> enable**

**Router# configure terminal**

**Router(config)# interface serial0/0/0**

**Router(config-if)# encapsulation ppp**

**Router(config-if)# ip address <IP\_ADDRESS> <SUBNET\_MASK> ! Hər router üçün uyğun IP**

**Router(config-if)# no shutdown**

**Router(config-if)# exit**

**Router(config)# exit**

**Misal üçün:**

**RouterA(config)# interface serial0/0/0**

**RouterA(config-if)# encapsulation ppp**

**RouterA(config-if)# ip address 10.0.0.1 255.255.255.252**

**RouterA(config-if)# no shutdown**

**RouterB(config)# interface serial0/0/0**

**RouterB(config-if)# encapsulation ppp**

**RouterB(config-if)# ip address 10.0.0.2 255.255.255.252**

**RouterB(config-if)# no shutdown**

* Əgər **authentication** (məsələn, PAP və ya CHAP) istifadə ediləcəksə, əlavə konfiqurasiya da tələb olunur.
* encapsulation ppp əmri default HDLC protokolunu dəyişərək PPP-ni aktiv edir.
* PPP daha çevik və geniş imkanlara malikdir, məsələn, autentifikasiya, sıxılma, səhv yoxlaması və s.

**İki router birbaşa serial kabel** (məsələn, Serial0/0/0) ilə birləşdirilibsə və bu interfeyslər üzərindən **point-to-point** bir əlaqə qurulursa, **IP ünvanlar eyni şəbəkədən təyin edilməlidir.**

**Sual 50. Bir Cisco routerdə iki ofis arasında serial bağlantı qurmusunuz. İndi istəyirsiniz ki, Serial0/0/0 interfeysi üzərində istifadə olunan bandwidth dəyərini 128 kbps təyin edəsiniz (default 1544 kbps əvəzinə) və bu dəyişiklik dinamik marşrutlama protokolları (məsələn, EIGRP və ya OSPF) üçün düzgün hesablama təmin etsin. İnterfeysin bandwidth dəyərinin dəyişdirilməsi üçün lazım olan əmrləri yazın.**

**Cavab:** Bandwidth əmri **gerçək sürəti dəyişmir**, sadəcə **routerin məlumatına** təsir edir ki, dinamik protokollar düzgün yol seçə bilsin.

### 1. **Routerə daxil ol**

Router> enable

Bu əmr ilə **privileged exec** rejiminə keçirsən.

### 2. **Global konfiqurasiya rejiminə keç**

Router# configure terminal

### 3. **Serial interfeysi seç**

Router(config)# interface Serial 0/0/0

İndi Serial0/0/0 interfeysini konfiqurasiya edirsən.

### 4. **Bandwidth dəyərini təyin et**

Router(config-if)# bandwidth 128

Bu əmr:

* Bandwidth dəyərini **128 kbps** olaraq təyin edir.
* Diqqət: bu **kbps** ilədir, amma əmr daxilində **rəqəm sadəcə ədəddir**, yəni 128 yazılır.

Bu əmrdən sonra:

* EIGRP bandwidth-i metric hesablamasında istifadə edir:  
  metric = (10^7 / bandwidth) + delay
* OSPF isə bandwidth əsasında cost hesablayır:  
  cost = reference\_bandwidth / interface\_bandwidth

Yəni bu dəyişikliyin məqsədi routing qərarlarının düzgün verilməsi üçündür.