**Şəbəkələrin əsasları imtahan sualları – cavabları**

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

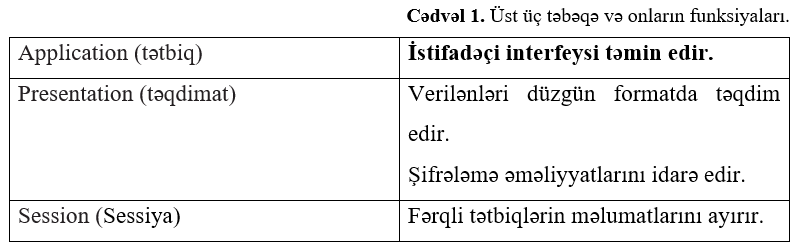
**Cavab:** OSI modelinin əsas məqsədi müxtəlif istehsalçıların avadanlıq və protokollarının bir-biri ilə işləməsinə imkan verməkdir.

OSI təbəqələşmiş modelindən istifadə etməyin bəzi vacib üstünlükləri bunlardır:

Şəbəkə ünsiyyəti modeli şəbəkəni daha sadə hissələrə bölərək inkişafı və problemlərin həllini asanlaşdırır. Standartlaşdırma sayəsində fərqli istehsalçılar uyğun avadanlıq və proqram təminatı yarada bilir. Hər təbəqənin funksiyası aydın şəkildə müəyyən olunur, bu da sənaye standartlarını təşviq edir. Müxtəlif sistemlər bir-biri ilə uyğun işləyə bilir və bir təbəqədəki dəyişiklik digər təbəqələrə təsir etmir.

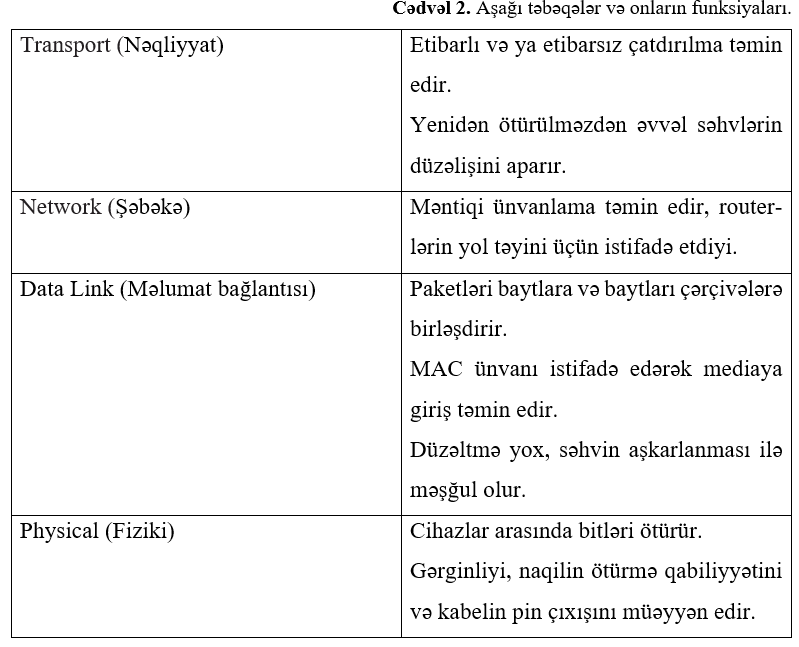
OSI referans modeli

OSI modeli müxtəlif əməliyyat sistemləri arasında məlumat ötürülməsini asanlaşdırır. Bu, fiziki deyil, məntiqi modeldir və şəbəkə tətbiqlərinin və standartlarının hazırlanması üçün rəhbər prinsiplər və çərçivə təqdim 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, yuxarı üst 3 təbəqə istifadəçi ilə tətbiq arasında əlaqə yaradır, məlumatın formatlanması, şifrələnməsi və sessiyanın idarəsini təmin edir. Bu təbəqələr istifadəçi proqramlarının şəbəkəyə çıxışını təmin edir və insan-kompüter əlaqəsini qurur. Şəbəkə ünvanlarını tanımır, sadəcə məlumatın necə təqdim olunacağını və ötürüləcəyini müəyyən edir.

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.

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

Şəbəkə avadanlıqları şəbəkənin düzgün işləməsi üçün müxtəlif funksiyalar həyata keçirir və OSI modelinin fərqli təbəqələrində fəaliyyət göstərirlər. Əsas avadanlıqlara router, switch, hub, firewall, modem, access point, bridge, repeater və gateway daxildir.

\*\*Router\*\* fərqli şəbəkələr arasında məlumat paketlərini IP ünvanlarına əsaslanaraq yönləndirir və OSI modelinin 3-cü təbəqəsində (Şəbəkə təbəqəsi) işləyir. \*\*Switch\*\* isə eyni şəbəkə daxilində cihazlar arasında məlumat ötürür, MAC ünvanlarına əsaslanır və 2-ci təbəqədə (Data Link) fəaliyyət göstərir. \*\*Hub\*\* məlumat paketlərini şəbəkədəki bütün cihazlara eyni anda göndərir, lakin məlumatı yönləndirmir və fiziki təbəqədə (1-ci təbəqə) işləyir.

\*\*Firewall\*\* şəbəkə təhlükəsizliyini təmin edir, məlumatların giriş-çıxışını analiz edir və 3-cü və 4-cü təbəqələrdə (Şəbəkə və Nəqliyyat) fəaliyyət göstərir. Yeni nəsil firewall-lar isə tətbiq təbəqəsində (7-ci təbəqə) də işləyə bilər. \*\*Modem\*\* internet bağlantısını təmin edir, analoq siqnalları rəqəmsal siqnallara çevirir və fiziki təbəqədə fəaliyyət göstərir.

\*\*Access Point\*\* cihazların şəbəkəyə simsiz qoşulmasını təmin edir və data link təbəqəsində işləyir. \*\*Bridge\*\* fərqli şəbəkə seqmentlərini birləşdirir, trafiki azaldır və 2-ci təbəqədə fəaliyyət göstərir. \*\*Repeater\*\* siqnalları gücləndirir, məsafəni artırır və fiziki təbəqədədir. \*\*Gateway\*\* fərqli şəbəkə protokollarını uyğunlaşdırır və daha yüksək təbəqələrdə işləyir.

Bu avadanlıqlar OSI modelinin müxtəlif təbəqələrində şəbəkə əlaqəsinin qurulması, idarə olunması və təhlükəsizliyini təmin edir. TCP/IP modelində isə bu funksiyalar tətbiq, nəqliyyat, internet və bağlantı təbəqələrinə bölünür. Şəbəkə avadanlıqlarının düzgün seçilməsi və istifadəsi şəbəkənin effektiv və təhlükəsiz işləməsi üçün vacibdir.

**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.**

Ethernet şəbəkələrində əsas problemlər toqquşmalar (collisions) və broadcast storm-dur. Toqquşmalar köhnə hub əsaslı şəbəkələrdə, yarım-dupleks rejimində baş verir; cihazlar eyni anda məlumat göndərərkən siqnallar toqquşur və paket itkisi olur. Bu problemi switchlər həll edir, çünki onlar hər port üçün ayrı collision domain yaradaraq toqquşmaların qarşısını alır və full-duplex ünsiyyətə imkan verir.

Broadcast storm çoxlu broadcast paketlərinin yayılmasıdır (məsələn, ARP, DHCP), bu isə bant genişliyini və CPU yükünü artırır. VLAN texnologiyası bu problemi azaldır, çünki şəbəkəni məntiqi kiçik hissələrə bölür və broadcast domainləri kiçildir. Routerlar da hər interface üçün ayrı broadcast domain yaradır.

Broadcast domain — bir cihazın göndərdiyi broadcast paketlərinin çatdığı bütün cihazların məntiqi sahəsidir. Məsələn, bir switchə qoşulmuş bütün cihazlar tək broadcast domain təşkil edir. Bu, bant genişliyinin itirilməsi, CPU yükünün artması və kiberhücumlara (məsələn, ARP spoofing) yol açır.

Collision domain isə toqquşmaların baş verə biləcəyi cihazlar qrupudur. Köhnə hub-larda bütün portlar tək collision domain idi və bu, şəbəkə performansını azaldırdı. Müasir switchlər isə hər portu ayrı collision domain kimi idarə edərək performansı artırır və full-duplex ünsiyyətə şərait 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.**

TCP/IP yığını kompüter şəbəkələrində məlumatların ötürülməsini tənzimləyən protokollar toplusudur və dörd əsas təbəqədən ibarətdir:

Şəbəkə Girişi Təbəqəsi (Network Access Layer)

Bu təbəqə məlumatların fiziki şəbəkə üzərindən ötürülməsini təmin edir. Burada məlumatlar çərçivə (frame) şəklində paketlənir. Ən çox istifadə edilən protokollar Ethernet, Wi-Fi, Frame Relay və ATM-dir. MAC ünvanı bu səviyyədə cihazları identifikasiya edir.

İnternet Təbəqəsi (Internet Layer)

Bu təbəqə məlumat paketlərinin şəbəkələr arasında düzgün marşrutlaşdırılmasına cavabdehdir. Əsas protokol IP-dir (IPv4 və IPv6 versiyaları mövcuddur). Bundan əlavə, ICMP şəbəkədəki xətalar və əlaqənin yoxlanması üçün, ARP isə IP ünvanlarını fiziki MAC ünvanlara çevirmək üçün istifadə olunur.

Nəqliyyat Təbəqəsi (Transport Layer)

Bu təbəqə məlumatların etibarlı və ardıcıl şəkildə tətbiqlər arasında ötürülməsini təmin edir. İki əsas protokol var:

TCP (əlaqə yönümlü, məlumat itkisinə yol vermir, məsələn, veb səhifə yüklənməsi və e-poçt üçün),

UDP (əlaqəsiz, sürətli, lakin məlumatın çatmasını təmin etmir, məsələn, canlı video yayımı və onlayn oyunlar üçün).

Tətbiq Təbəqəsi (Application Layer)

İstifadəçi ilə birbaşa əlaqədə olan səviyyədir. Burada müxtəlif xidmət protokolları fəaliyyət göstərir:

HTTP/HTTPS – veb səhifələrin ötürülməsi,

FTP – fayl ötürülməsi,

SMTP – e-poçt göndərilməsi,

POP3 və IMAP – e-poçtların oxunması,

DNS – domen adlarının IP ünvanlara çevrilməsi.

Nəticə olaraq, TCP/IP yığını internet və lokal şəbəkələrdə məlumat mübadiləsinin düzgün, təhlükəsiz və etibarlı olmasını təmin edən əsas strukturdur. Hər təbəqə öz rolunu oynayır və protokollar birlikdə işləyərək şəbəkənin funksionallığını təmin edir.

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

Alt şəbəkə (subnet) — bir IP şəbəkəsinin daha kiçik və idarəolunan hissələrə bölünməsi nəticəsində yaranan seqmentlərdir. Bu proses alt şəbəkələmə (subnetting) adlanır və əsas məqsədi IP ünvanlarının daha səmərəli istifadəsini təmin etmək, şəbəkəni sadələşdirmək və təhlükəsizliyi artırmaqdır. Böyük təşkilatlarda bütün cihazların eyni şəbəkədə olması texniki problemlərə səbəb olur. Alt şəbəkələmə bu problemlərin qarşısını alır.

IPv4 ünvanları məhdud olduğuna görə, alt şəbəkələmə ilə hər bölməyə yalnız ehtiyac qədər IP ünvan verilir və ünvan israfı azalır. Bu, IP resurslarının uzunmüddətli istifadəsinə imkan yaradır. Eyni zamanda, alt şəbəkələmə şəbəkə trafikini daha yaxşı idarə etməyə kömək edir. Trafik əsasən lokal alt şəbəkədə qalır, bu isə performansı artırır və digər bölmələrə təsiri azaldır.

Təhlükəsizlik baxımından, müxtəlif şöbələr üçün ayrı alt şəbəkələrin yaradılması onların bir-birinə girişini məhdudlaşdırmağa imkan verir. Məsələn, İT şöbəsinə digər istifadəçilərin çıxışı məhdudlaşdırıla bilər. Bu, daxili şəbəkənin daha təhlükəsiz olmasına səbəb olur.

Alt şəbəkələmə həmçinin idarəetməni asanlaşdırır. Hər alt şəbəkə ayrıca izlənilə və konfiqurasiya oluna bilər. Marşrutlaşdırma cədvəlləri də sadələşir, çünki hər alt şəbəkə üçün ayrıca marşrut təyin etmək mümkündür.

Nəticə olaraq, alt şəbəkələmə şəbəkənin daha effektiv, təhlükəsiz və çevik idarə olunmasını təmin edir. Bu yanaşma IP ünvan bölgüsünü optimallaşdırır və böyük şəbəkələrin idarəsini asanlaşdırır.

**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.**

Alt şəbəkə maskası — IP ünvanını şəbəkə və host hissələrinə ayırmağa kömək edən 32-bitlik ardıcıllıqdır. Maskadakı 1-lər şəbəkə, 0-lar isə host hissəsini göstərir. Məsələn, 255.255.255.0 maskasında ilk üç bayt şəbəkəyə, sonuncusu isə hostlara aiddir. Şəbəkə avadanlıqları IP ünvan və maskanı Bitwise AND əməliyyatı ilə birləşdirərək şəbəkə ünvanını müəyyən edir.

CIDR anlayışı (Classless Inter-Domain Routing) – sinifli ünvаnlamanı əvəz edən, daha elastik və effektiv sinifsiz ünvanlama metodudur. CIDR-də IP ünvanlar prefiks uzunluğu ilə göstərilir (məsələn, /24) və VLSM (dəyişkən uzunluqlu maska) dəstəklənir.

CIDR ilə sinifli ünvаnlamanın fərqləri:

Şəbəkə ölçüsü: Sinifli sistemdə sabit A/B/C sinifləri var, CIDR-də isə şəbəkənin ölçüsü istənilən prefiks ilə təyin olunur.

Subnet maskası: Sinifli metodda maskalar sabitdir, CIDR-də isə maskalar daha çevikdir (məs., 255.255.248.0).

Ünvan israfı: Sinifli sistemdə ünvanlar çox vaxt ehtiyacdan böyük verilir, CIDR ünvanları ehtiyaca uyğun ayırmağa imkan verir.

VLSM: CIDR VLSM-i dəstəkləyir, bu da müxtəlif ölçülü alt şəbəkələr yaratmağa imkan verir.

Marşrutlaşdırma cədvəllərinə təsiri:

CIDR supernetting vasitəsilə bir neçə şəbəkəni birləşdirib marşrutları sadələşdirir. Bu, routerlərdə daha az marşrut qeydinin saxlanmasına, yaddaş yükünün və internet trafikinin optimallaşdırılmasına səbəb olur. CIDR sayəsində ünvan məkanı daha səmərəli idarə olunur və şəbəkənin genişlənməsi daha asan 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.**

User EXEC və Privileged EXEC rejimləri Cisco cihazlarında fərqli idarəetmə səviyyələri təqdim edir. User EXEC rejimi əsasən istifadəçiyə cihazın vəziyyəti haqqında məlumatları oxumaq imkanı verir, lakin burada konfiqurasiya dəyişiklikləri etmək mümkün deyil. Bu rejimin əmr simvolu Router> şəklində olur. Bu rejimdən əsasən şəbəkə interfeysləri və digər sadə yoxlamalar üçün istifadə olunur.

Privileged EXEC rejimi isə cihazın tam idarəsini təmin edir. Bu rejimdə istifadəçi cihazın bütün parametrlərini dəyişə və dərin sistem əmrlərini icra edə bilər. Əmr simvolu Router# olur və bu rejim cihazın administrasiyası üçün əsasdır.

Global Configuration rejimi isə cihazın qlobal şəbəkə parametrlərinin dəyişdirilməsi üçün istifadə edilir. Burada şəbəkə interfeyslərinin ünvanlandırılması, yönləndirmə protokollarının aktivləşdirilməsi, şifrələrin təyin olunması və təhlükəsizlik parametrlərinin konfiqurasiyası kimi əməliyyatlar aparılır. Bu rejimdə əmr simvolu Router(config)# olur.

İstifadəçilərə əmrləri düzgün öyrənmək və tətbiq etməkdə kömək edən “köməkçi əmrlər” və “kontekstə əsaslanan yardım” funksiyaları mövcuddur. Məsələn, ? işarəsi ilə mövcud əmrlərin siyahısını və ya xüsusi əmrin izahını görmək mümkündür. Bu xüsusiyyətlər istifadəçilərin əmrləri doğru və səmərəli şəkildə istifadə etməsini təmin edir.

Nəticədə, User EXEC rejimi yalnız məlumat əldə etmək üçün, Privileged EXEC rejimi cihazın idarəsi və konfiqurasiyası üçün, Global Configuration rejimi isə sistem parametrlərinin dəyişdirilməsi üçün nəzərdə tutulub. Köməkçi əmrlər isə əmrlərin istifadəsini asanlaşdırır və idarəetmədə səhvlərin qarşısını alır.

**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 RAM, ROM, NVRAM və Flash yaddaş növləri müxtəlif funksiyalar üçün istifadə olunur və cihazın düzgün işləməsini təmin edir.

RAM — müvəqqəti yaddaşdır. Cihaz işləyərkən cari konfiqurasiya (running-config) və digər müvəqqəti məlumatlar burada saxlanılır. Dəyişikliklər dərhal tətbiq olunur, amma cihaz söndükdə RAM məlumatları itir.

ROM — daimi və yalnız oxunabilən yaddaşdır. Burada boot loader və cihazın işə düşməsi üçün zəruri proqramlar saxlanır. ROM məlumatları dəyişdirilə bilməz.

NVRAM — elektrik kəsilsə belə məlumatları saxlayan yaddaşdır. Startup-config faylı burada yerləşir və cihaz açılarkən bu konfiqurasiya RAM-a yüklənir. Startup-config sabit konfiqurasiya kimi işləyir və dəyişikliklərin qalıcı olması üçün running-config-dən startup-config-ə köçürülməsi tələb olunur.

Flash — cihazın əməliyyat sistemi (IOS) və digər faylların saxlandığı daimi yaddaşdır. IOS burada saxlanılır və cihaz işə düşərkən RAM-a yüklənir. Flash yaddaşı əməliyyat sisteminin yenilənməsi üçün də istifadə olunur.

Running-config və startup-config faylları arasındakı fərq: Running-config RAM-da müvəqqəti saxlanır və dəyişikliklər dərhal təsir edir, lakin cihaz yenidən başladıqda itir. Startup-config isə NVRAM-da saxlanır və cihazın açılışında istifadə olunur. Dəyişikliklərin qalıcı olması üçün running-config startup-config-ə kopyalanmalıdır.

Cisco cihazlarında Flash yaddaşındakı faylları idarə etmək üçün əmrlər mövcuddur, məsələn, dir flash: əmri faylları göstərir, copy running-config startup-config əmri isə konfiqurasiyanı yadda saxlayır.

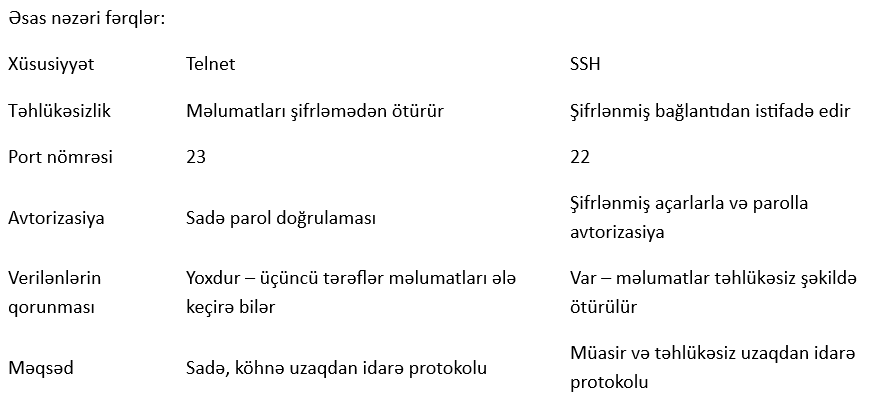
Beləliklə, bu yaddaş növləri Cisco cihazlarının performansını və sabitliyini təmin edir, konfiqurasiyaların idarə edilməsində vacib rol oynayır.

İstəsəniz, daha da qısalda və ya genişləndirə bilərəm.

**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?**

SNMP protokolunun əsas komponentləri və funksiyaları:

SNMP (Simple Network Management Protocol) şəbəkə idarəçiliyi üçün istifadə olunur. Üç əsas komponenti var:

Agent — şəbəkə cihazlarında işləyən proqram, cihaz haqqında məlumat toplayır və SNMP Manager-ə göndərir.

Manager — mərkəzi sistem, agentlərdən məlumatları alır və təhlil edir.

MIB (Management Information Base) — idarə olunan parametrlərin məlumat bazasıdır, OID-lərlə unikal identifikasiya təmin edir.

SNMP performans izləmə, səhvlərin aşkarlanması, konfiqurasiya idarəsi və bildiriş göndərmə funksiyalarını yerinə yetirir.

Syslog sisteminin rolu və əhəmiyyəti:

Syslog şəbəkə cihazlarında hadisələri (səhvlər, uğursuz girişlər, konfiqurasiya dəyişiklikləri) qeydə alan standart protokoldur. Hadisələr prioritet səviyyələrinə görə təsnif olunur və mərkəzi serverə göndərilir. Syslog problemlərin tez aşkarlanması, təhlükəsizlik auditi və qanuni tələblərə uyğunluq üçün vacibdir.

SNMP və Syslog-un müqayisəsi:

SNMP daha çox real vaxt monitorinqi və idarəetmə üçün, Syslog isə hadisələrin qeyd olunması və sonradan təhlili üçün istifadə olunur. SNMP cihazların performansını izləyir, Syslog isə problemlərin səbəblərini araşdırmağa kömək edir. Hər iki sistem bir-birini tamamlayır.

NTP protokolunun rolu və əhəmiyyəti:

NTP (Network Time Protocol) şəbəkə cihazlarının vaxtını dəqiq sinxronlaşdırır. Vaxt sinxronizasiyası loqların düzgün təhlili, təhlükəsizlik auditləri və qanuni tələblərin yerinə yetirilməsi üçün vacibdir. Vaxt uyğunsuzluğu verilənlərin itirilməsinə və sistem problemlərinə səbəb ola bilər. SNMP və Syslog kimi sistemlərin düzgün işləməsi üçün NTP-nin fəaliyyəti zəruridir.

**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.**

Statik və dinamik marşrutlaşdırma kompüter şəbəkələrində məlumat paketlərinin düzgün istiqamətə yönləndirilməsi üçün istifadə olunan iki əsas üsuldur. Hər iki üsulun fərqli üstünlükləri və çatışmazlıqları vardır və onların seçimi şəbəkənin ölçüsünə, mürəkkəbliyinə və ehtiyaclarına görə dəyişir.

Statik marşrutlaşdırma, administrator tərəfindən əl ilə təyin olunan və dəyişməyən marşrutlardan ibarətdir. Bu marşrutlar cihazlarda sabit qalır və şəbəkədə dəyişiklik olarsa, administrator onları əl ilə yeniləməlidir. Bu səbəbdən statik marşrutlaşdırma əsasən kiçik və sabit şəbəkələrdə istifadə olunur.

Dinamik marşrutlaşdırma isə marşrutlaşdırıcılar arasında avtomatik məlumat mübadiləsi yolu ilə işləyir. Xüsusi protokollar, məsələn RIP və OSPF vasitəsilə şəbəkənin topologiyası öyrənilir və ən optimal marşrutlar müəyyən edilir. Bu üsul iri və tez-tez dəyişən şəbəkələr üçün daha əlverişlidir, çünki şəbəkədə baş verən dəyişikliklərə sürətlə və avtomatik reaksiya verir.

Statik marşrutlaşdırmada marşrutlar əl ilə qurulur və dəyişikliklərə uyğunlaşmır, buna görə əlaqə pozulanda trafik itkisi ola bilər. Dinamik marşrutlaşdırma isə şəbəkə dəyişikliklərini dərhal aşkar edir və yeni marşrutları avtomatik müəyyən edir.

Kiçik və sabit şəbəkələrdə statik marşrutlaşdırma daha sadə və effektivdir, lakin böyük və dinamik şəbəkələrdə idarəetmə üçün dinamik marşrutlaşdırma daha uyğundur.

Təhlükəsizlik baxımından, statik marşrutlar məlumat yaymadığı üçün daha təhlükəsiz sayılır və xarici müdaxilə ehtimalı azdır. Dinamik marşrutlaşdırma protokolları isə məlumat mübadiləsi apardığından manipulyasiya riski yarana bilər.

Statik marşrutlar az yaddaş və CPU resursu tələb edir, dinamik marşrutlaşdırma isə davamlı hesablama və analiz tələb etdiyi üçün daha çox resurs sərf edir.

Statik marşrutlaşdırmada administrator şəbəkənin tam strukturunu bilməli və hər dəyişiklikdə müdaxilə etməlidir, dinamik marşrutlaşdırma isə bir dəfə qurulduqdan sonra daha az texniki müdaxilə tələb edir.

Dinamik marşrutlaşdırma protokolları iki növə bölünür: distance vector protokolları (məsələn, RIP) və link-state protokolları (məsələn, OSPF). RIP daha sadədir və kiçik şəbəkələr üçün uyğundur, amma yavaş reaksiya verir və məhdudiyyətləri var. OSPF isə daha mürəkkəb, sürətli və böyük şəbəkələr üçün daha effektivdir, lakin daha çox resurs tələb edir.

Ümumiyyətlə, statik marşrutlaşdırma sabit və təhlükəsiz kiçik şəbəkələrdə, dinamik marşrutlaşdırma isə mürəkkəb və dinamik böyük şəbəkələrdə daha uyğundur. Hər iki üsulun tətbiqi konkret şəbəkənin ehtiyaclarına uyğun olmalıdır.

**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.

Marşrutlama cədvəli şəbəkədə məlumat paketlərinin düzgün istiqamətə göndərilməsi üçün istifadə olunan əsas məlumat bazasıdır. Routerlər bu cədvəldə saxlanılan məlumatlara əsaslanaraq paketlərin hansı interfeys vasitəsilə və hansı növbəti marşrutlayıcıya göndəriləcəyinə qərar verirlər. Cədvəldə əsasən şəbəkə prefiksi, növbəti addım, metrik, interfeys və idarəetmə məsafəsi kimi məlumatlar olur.

Şəbəkə prefiksi marşrutun aid olduğu IP ünvan aralığını göstərir. Növbəti addım paketin hədəfə çatmaq üçün göndəriləcəyi növbəti routerin ünvanıdır. Metrik marşrutun keyfiyyətini göstərir və daha aşağı metrik daha üstün sayılır. İnterfeys paketin göndəriləcəyi şəbəkə portunu bildirir. İdarəetmə məsafəsi isə fərqli marşrutlaşdırma protokollarının etibarlılıq səviyyəsini göstərir; kiçik dəyər daha etibarlı marşrut deməkdir.

Routerlər marşrut seçərkən əsasən üç kriteriyaya diqqət yetirirlər. Əvvəlcə ən uzun uyğunluq prinsipi ilə ən spesifik prefiksi seçirlər. Daha sonra idarəetmə məsafəsinə baxırlar; ən aşağı dəyər üstünlük təşkil edir. Əgər idarəetmə məsafələri bərabərdirsə, metrik dəyərlərə baxılır və ən aşağı metrikli marşrut seçilir. Eyni şəbəkəyə aid bir neçə marşrut varsa, bu qaydalara əsasən seçim edilir. Əgər bütün dəyərlər eynidirsə, router yük balanslaşdırma funksiyasını tətbiq edə bilər.

Marşrutlama protokolları daxili və xarici olmaqla iki qrupa bölünür. Daxili protokollar şirkət və təşkilat daxilində istifadə olunur. Məsələn, RIP hop sayına əsaslanan distance-vector protokoldur və kiçik şəbəkələr üçün uyğundur. OSPF link-state protokolu olub, şəbəkənin topologiyasını öyrənərək daha optimal marşrut seçir. EIGRP Cisco tərəfindən yaradılmış hibrid protokoldur. Xarici protokol BGP isə internetdə müstəqil sistemlər arasında marşrutların idarə olunması üçün istifadə olunur və marşrutların keçdiyi yolları nəzərə alır.

Bu prinsiplər şəbəkənin sürətli, dayanıqlı və təhlükəsiz işləməsini təmin edir. Marşrutlama cədvəllərinin düzgün qurulması və marşrut seçimi zamanı routerlərin kriteriyalara əsaslanması məlumatların vaxtında və səmərəli çatdırılmasına kömək edir. Bu da şəbəkə performansını artırır və idarəetməni asanlaşdırır.

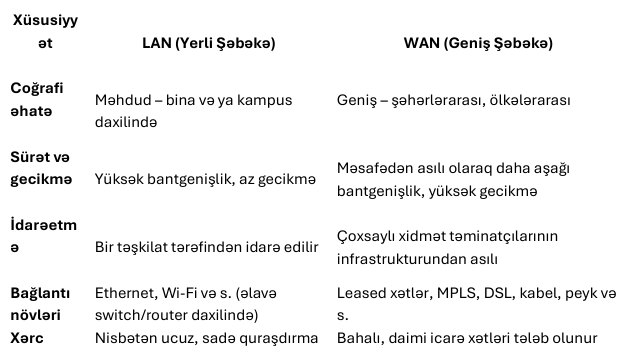
**Sual 19. WAN nədir və LAN-dan əsas nəzəri fərqləri hansılardır? WAN bağlantılarında istifadə olunan əsas texnologiyaları (məsələn: leased line, MPLS, DSL) nəzəri olaraq izah edin.**

Geniş Sahə Şəbəkəsi (WAN) böyük coğrafi əraziləri əhatə edən və uzaq məsafələrdə yerləşən müxtəlif şəbəkələri, məsələn, şəhərlər və ölkələrdəki ofislərin LAN-larını birləşdirən telekommunikasiya şəbəkəsidir. WAN əlaqələri adətən ictimai telekommunikasiya infrastrukturundan istifadə etməklə qurulur. Şirkətlər bu əlaqələr üçün xüsusi icarəyə götürülmüş xətlər, virtual özəl şəbəkələr (VPN) və ya IP-tünellərdən yararlanırlar. İnternet də ən böyük WAN nümunəsi kimi qəbul edilir. WAN-lar fərqli provayderlərin infrastrukturu üzərində qurulduğu üçün idarə edilməsi daha mürəkkəbdir və gecikmə ilə bantgenişliyi LAN-lara nisbətən daha məhduddur.

WAN və LAN arasındakı əsas fərq əhatə etdiyi ərazi və əlaqə sürətindədir. LAN məhdud ərazidə, məsələn, bina daxilində yüksək sürət və aşağı gecikmə ilə işləyir, WAN isə geniş coğrafi məsafələri əhatə edərək bir neçə LAN-ı birləşdirir. LAN-larda əlaqə əsasən təşkilatın öz avadanlıqları ilə idarə olunur, WAN-larda isə telekommunikasiya şirkətlərinin təmin etdiyi xidmətlərdən istifadə edilir.

WAN bağlantılarında istifadə olunan əsas texnologiyalara leased line, MPLS və DSL daxildir. Leased line — iki məntəqə arasında daimi və stabil bağlantı təmin edən icarəyə götürülmüş xəttdir, bantgenişliyi sabit və gecikməsi aşağıdır. MPLS isə paketləri IP ünvanları yerinə qısa etiketlər əsasında yönləndirən yüksək performanslı texnologiyadır. DSL isə mövcud telefon xətlərindən istifadə edərək internet bağlantısı yaradır. Bundan başqa, coaxial kabel, simsiz şəbəkələr və Metro Ethernet kimi digər texnologiyalar da WAN-larda tətbiq olunur.

Bu texnologiyalar uzaq məsafələrdə məlumat mübadiləsini mümkün edir və şəbəkələrin etibarlı, sürətli və dayanıqlı işləməsinə yardımçı olur.

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

**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.**

HDLC və PPP protokolları WAN bağlantılarında məlumatların ötürülməsi üçün istifadə olunan əsas protokollardır, lakin funksional olaraq fərqlidirlər. HDLC (High-Level Data Link Control) daha sadə və əsasən serial əlaqələrdə standart protokol kimi tətbiq olunur. O, əsasən nöqtədən nöqtəyə əlaqə qurur və yalnız bir protokol növünü dəstəkləyir, yəni çox protokollu dəstək vermir. PPP (Point-to-Point Protocol) isə daha inkişaf etmişdir və müxtəlif şəbəkə protokollarını (məsələn, IP, IPX) daşıya bilir, həmçinin autentifikasiya, xəta aşkarlanması və bağlantının idarə olunması kimi əlavə funksiyalar təklif edir. PPP WAN bağlantılarında daha çevik və təhlükəsiz əlaqə qurmağa imkan verir, xüsusilə modem və DSL kimi texnologiyalarda geniş istifadə olunur.

NAT (Network Address Translation) və PAT (Port Address Translation) IP ünvanlarının qənaətli istifadəsində mühüm rol oynayan texnologiyalardır. NAT şəbəkədəki daxili IP ünvanları ilə ictimai IP ünvanları arasında çevirmə aparır, bu yolla bir neçə daxili cihazın tək bir və ya məhdud sayda ictimai IP vasitəsilə internetə çıxışı təmin edilir. PAT isə NAT-ın daha inkişaf etmiş formasıdır və eyni ictimai IP ünvanı üzərindən müxtəlif daxili cihazların fərqli port nömrələrini istifadə edərək əlaqə qurmasına imkan verir. Bu, IP ünvanlarının daha effektiv istifadəsini təmin edir və şəbəkə resurslarının qənaətini artırır.

WAN dizaynında HDLC və PPP protokolları, həmçinin NAT və PAT texnologiyaları təhlükəsizlik və marşrutlaşdırma baxımından əhəmiyyətlidir. PPP protokolunun autentifikasiya imkanları şəbəkənin təhlükəsizliyini artırır və istifadəçilərin düzgün identifikasiyasını təmin edir. NAT və PAT isə daxili şəbəkəni birbaşa internetdən gizlətməklə, əlavə müdafiə qatları yaradır, həmçinin IP ünvanlarının çatışmazlığı problemini aradan qaldırır. Marşrutlaşdırma zamanı NAT və PAT şəbəkə trafikinin düzgün yönləndirilməsinə kömək edir və şəbəkənin genişlənməsinə şərait yaradır. Bu texnologiyalar birgə istifadə edilərək WAN şəbəkələrinin həm effektiv, həm də təhlükəsiz işləməsi təmin olunur.

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

a. Ulduz (Star) b. Halqa (Ring) c. Şin (Bus)

Ulduz topologiyası (star)-Bu topologiyada bütün cihazlar mərkəzi bir cihaz məsələn switch və ya hub vasitəsilə bir-birinə qoşulur hər cihaz mərkəzə ayrıca kabel ilə bağlanır. forması ulduza bənzədiyinə görə bu topologiyaya ulduz topologiyası deyilir Burada məlumatlar mərkəzi qurgu tərəfindən digər komputerlərə ötürülür.Ethernet şəbəkələrində istifadə olunur.

Üstün cəhətləri-Nasaz cihazları aşkar etmək daha asandır, Asan idarəetməsi var cünki mərkəzi qurgu ilə idarə olunur, yeni cihazları əlavə etmək rahatdır, təhlükəsizlik və perfromans cəhətdən yaxşıdır

Catışmayan cəhətləri:Şəbəkənin işi mərkəzi qurgudan asılıdır o sıradan cixarsa şəbəkə dayanır,Kabellərin cəkilməsi üçün cox vəsait tələb olunur,kabellər cox olanda idarə olunma cətinləşir

Halqa topologiyası(ring)-Cihazlar bir-biri ilə dairəvi şəkildə halqa formasında birləşdirilir. məlumatlar bir istiqamətdə bəzi hallarda iki istiqamətdə cihazdan cihazara ötürülür, məlumat bütün cihazlardan keçərək təyinat nöqtəsinə çatır.

Üstün cəhətləri- Bütün cihazlar eyni səviyyədə olur, burada mərkəzi qurğuya ehtiyac yoxdu, trafikə nəzarət etmək daha asandır, kicik şəbəkələr üçün daha yaxşıdır

Catışmayan cəhətləri- Bir cihazın sıradan cıxması bütün şəbəkəyə təsir edir ,məlumat bir neçə cihazdan keçməli olur,bu topologiyada şəbəkəyə yeni cihaz əlavə etmək cox çətindi.tez-tez texniki baxım tələb edir

Şin topologiyası (Bus Topology)- Bütün cihazlar bir tək kabelə (şin) birləşdirilir. Məlumat bu kabel üzərində ötürülür və bütün cihazlara göndərilir, amma yalnız ünvanlanan cihaz onu qəbul edir.

Üstün cəhətləri-daha az kabel və avandanlıq işlədir,asan genişlənir,cihaz əlavə etmək daha rahatdır,bu topologiyada mərkəzi cihaz tələb olunmur

Catışmayan cəhətləri-siqnallarda toqquşmalar ola bilir,uzaq məsafəyə siqnal göndərəndə zəifləyir,kabel sıradan çıxsa, şəbəkə dayanır.

**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:

Ilk olaraq baglantılar yoxlanmalıdır kabellərin və digər cihazların qoşulu oldugundan əmin olmaq lazımdır.Əgər kabellərdə bir problem olarsa bu zaman komputerlər arasındakı əlaqə olmayacaq

Sviçin led ışıqlarının yandıgından əmin olmaq lazımdır əgər hər hansı bir porta kabel qoşulubsa o yaşıl rəngdə normalda isə narıncı rəngdə olmalıdır.alınırsa portları dəyişin

Şəbəkə adapterlərinin aktiv olub-olmadığını yoxlayın.Daha sonra komputerlərin ip lərini yoxlamaq lazımdır

Hər iki kompüterin ip ünvanını yoxlayın:

oWindows-ipconfig

oLinux- ifconfig və ya ip a

Hər iki kompüter eyni şəbəkə daxilində olmalıdır.

Kompüter 1 -- 192.168.1.55 Kompüter 2 -- 192.168.1.57

Subnet mask -- 255.255.255.0

Komputerlərdən biri 192.168.1.55 digəri isə 10.0.0.6 ip olarsa onda bu iki komputer əlaqə qura bilməz

Subnet mask və default gateway in doğruluğuna baxın

Komputerlərə ping göndərərək bağlantını yoxlayın

Ping 192.168.1.55 cavab gəlirsə bağlantı var deməkdir amma cavab gəlməsə deməli nəsə problem var Bundan əlavə əgər kompüterdə firewall aktivdirsə bu ping i bloklaya biler

Antivirus və ya təhlükəsizlik proqramları da şəbəkə əlaqəsinə mane ola bilər.

arp -a ilə digər kompüterin MAC ünvanını ARP cədvəlində yoxlamağa calışın

Mac ünvanı görünməsə deməli problem layer 2 də ola bilər.

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

Cavab:

a) Cavab-DHCP trafikidir.

Izahı-Bu trafikin DHCP oldugunu bilmək üçün standart portlara baxmaq lazımdır.UDP portlarına baxanda SRC(port68-Client portu) və Dst(port67-Server portu) portlarını görə bilərik

Bunlar DHCP də standart portlardır. Bundan əlavə, IP ünvanı 192.168.20.255 (broadcast ünvanı) və MAC ünvanı FF:FF:FF:FF:FF:FF olması DHCP-nin discover və request mərhələlərinə uyğundur.

b) Cavab-DHCP mesajı şəbəkədəki bütün qurğulara çatsın deyə broadcast kimi yollanıb.

İzah-DHCP protokolunda client ilk dəfə server tapmaq üçün broadcast istifadə edir (DHCP discover/request mesajları). FF:FF:FF:FF:FF:FF ünvanı bütün şəbəkə qurğularına mesajı çatdırma işini görür DHCP serveri bu mesajı alır və sonra cavab verir (unicast ilə).

c) Cavab: Prioritet (PRI) 6, bu çərçivəyə yüksək prioritet təyin olundugunu göstərir.

İzahı- 802.1Q teqində PRI sahəsinin dəyəri 3 bitdir (0–7 aralığı),IEEE 802.1p standartına görə trafikə prioritet təyin edir.

Dəyər 6 "Critical applications" kateqoriyasına uyğun gəlir ( VIP, DHCP).

DHCP-nin prioritetli ötürülməsi onun şəbəkə üçün vacib olmasını göstərir

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

a) Bu ünvanın alt şəbəkə maskını hesablayın-Bunun üçün /28 hissəsinə nəzər yetirmək lazımdır.Biz bilik ki ip 32 bitdən ibarət olur və 32 bitdən 28 i istifadə olunub burada

11111111.11111111.11111111.11110000 Buradakı bitləri 10 luq say sistemində hesablayanda 255.255.255.240 alırıq CIDR formatında /28 — bu o deməkdir ki ilk 28 bit şəbəkə hissəsinə aiddir IP ünvanlar 32 bitlikdir deməli qalan 4 bit hostlar üçün qalır.

b) Bu alt şəbəkədə neçə host ünvanı var?

Subnet maskı /28, yəni 32 - 28 = 4 bit host üçün qalır.

Host ünvanlarının sayı: 2⁴ = 16 ünvan

Amma 1-i şəbəkə ünvanı, 1-i isə broadcast üçün istifadə olunur.

16 - 2 = 14 istifadə oluna bilən host ünvanı Cavab:14

c) Bu alt şəbəkənin broadcast ünvanı nədir-Əvvəlcə şəbəkə ünvanını tapaq.Subnet mask /28 --- hər alt şəbəkə 16 IP ünvanından ibarətdir.

Alt şəbəkələr 192.168.5.0/28 192.168.5.16/28 192.168.5.32/28

192.168.5.25 → 192.168.5.16/28 alt şəbəkəsindədir. Bu alt şəbəkə:

Şəbəkə ünvanı: 192.168.5.16

Broadcast ünvanı: son ünvan = 192.168.5.31 CAVAB: 192.168.5.31

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

Cavab:

a) Problemin səbəbləri:

Şəbəkədə loop varsa deməli layer 2 sviçdər arasında birdən çox yol var və buna görə də broadcast paketləri şəbəkə daxilində sonsuz dövr edir

STP-nin aktiv olmaması-bu protokol loopların qarşısını alan protokoldur STP protokolunun sönülu olması və yaxud quraşdırılmamasına görə bu problem yarana bilər

b) Problemin qarşısını almaq üçün protokol:

STP (Spanning tree protocol) - Bu protokol şəbəkədə loop ların qarşısını almaq üçün istifadə olunur. STP şəbəkədəki bütün keçidləri axtarır və ən qısa yolu seçir,digər yolları işlətmədən ehtiyatda saxlayır

c) Sviçdə problemi minimuma endirmək üçün cisco IOS əmri

spanning-tree mode rapid-pvst

Bu əmr vasitəsiylə Rapid Per-VLAN Spanning Tree modu işə düşür bu isə STP-nin daha sürətli versiyasıdır və hər vlan üçün ayrı-ayrı spanning tree hesablayır.

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

Nəqliyyat qatında ünsiyyət iki cür olur- bağlantılı və ya bağlantısız. Bu sualda göstərilən ünsiyyət bağlantılıdır yəni client və server arasında əvvəlcədən əlaqə qurulmalıdır bu əlaqə qurmaq üçün "üçtərəfli əl sıxma" prosesi aparılır əvvəlcə hər iki cihaz bir-birinə siqnal göndərir və cavab alır bu baş verdikdən sonra məlumat ötürülməsi mümkündür Bu prosesdə 3 əsas addım var:

SYN – Client server-ə qoşulmaq istədiyini bildirir, sinxronizasiya üçün siqnal göndərir.

SYN-ACK – Server həmin siqnalı qəbul edir və cavab olaraq həm SYN, həm də ACK siqnalı göndərir.

ACK – Client serverin cavabını qəbul edir və sinxronizasiya başa çatır.

Bu üç addım tamamlandıqdan sonra məlumat göndərmək mümkündür.SYN “synchronize”, ACK isə “acknowledgment” sözlərinin qısaldılmış formasıdı.Əl sıxma prosesi zamanı 2 növ paket olur:

Seq – göndərilən sorğunun sıra nömrəsini bildirir.

Ack – qəbul olunan sorğuya cavab verir.

Məsələn client ilk SYN paketində Seq=1000 göndərir. Server bu paketi qəbul edib öz cavabında Seq=5000 təyin edir Eyni zamanda server Ack=1001 göndərir. Bu da ona görədə Seq=1000 olan paket 1 seqment sayılır deyə cavab olaraq +1 artırılır (RFC 793 qaydasına əsasən). Sonra client serverə cavab verir və Ack=5001 göndərir çünki serverin Seq=5000 idi ona görə +1 edilir

A) Bu sualın cavabı növbəti paketi kimin göndərəcəyindən asılıdır.

Client göndərirsə:Seq=1001,Ack=5001 Server göndərirsə: Seq=5001 Ack=1001

B) Yenə də sualın cavabı da məlumatı hansı tərəfin göndərdiyindən asılıdır

Client göndərərsə: Seq=1001+150=1151 Ack=5001

Server göndərərsə:Seq=5001+150=5151 Ack=1001

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

Cavab:

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

Destination port=80 olduğuna görə bu paket HTTP -ə yönəlib

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

HTTP xidməti hər iki modeldə də tətbiq səviyyəsində(Application layer) 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 üçündür,TCP əlaqə yönümlüdür və məlumatların ardıcıllığını, bütövlüyünü və çatdırılmasını zəmanət altına alır.UDP isə daha cox video ,dns sorguları üçün istifadə olunur.etibarsız protokoldur və belə xidmətlər üçün uyğun deyil

**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.**

Cavab:

a) DHCP müştəri cihazında ipünvanını yoxlamaq lazımdırki görək işləyirmi : ipconfig /all

Bu əmr vasitəsilə kompüterin ip ünvanı və DHCP serverin ünvanı və DHCP aktiv olub-olmadığı yoxlanılır. Əgər “Autocnfiguration ip address” görsənirsə DHCP serverdən ip alınmayıb

DHCP serverdən yenidən ip almaq- ipconfig /release və ipconfig /renew

Bu əmrdən sora köhnə ip buraxılır və serverdən yeni ip tələb olunur. Yenə alınmasa deməli bu şəbəkədə çatım problemi mövcuddur

b) DNS serverin ad çevirmə funksiyasını yoxlayaq- nslookup www.test.com

Əmr serverə sorğu göndərərək www.test.com ünvanının IP ünvanının olub olmamasına baxır əgər cavab gəlmirsə, onda deməli cevrilmə düzgün yerinə yetirilmir və bu zaman yenidən konfiquryasiya etmək lazım ola bilər

c)Təkrarlayəcı DHCP və DNS serverlər yerləşdirilməlidir:

1) Əgər şəbəkədi bir neçə DNS server olarsa onda bunlardan biri sıradan çıxarsa digəri işə düşməlidir

2) DHCP üçün load balancing və ya failover mexanizmlərindən istifadə eləmək

3) DNS üçün isə birinci və ikinci DNS serverlər təyin olunmalıdır ki biri cavab vermədikdə digəri işləsin

4) Şəbəkədəki serverlər fərqli seqmentlərdə olsa bu onlardan biri sıradan çıxan zaman digərlərinin fasiləsiz işləməsinin təmin edir

**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:

Gəlin 192.168.10.0/24 şəbəkəsini 4 bərabər alt şəbəkəyə bölək.Əvvəlcə biz baxırıqki burada /24 var yəni bu şəbəkənin maskası 255.255.255.0 dır,ümumi olaraq 256 ip(0-255) ünvanı vardır.Biz bunu 4 bərabər hissəyə bölməliyik ilk öncə hesablayaq ki hər alt şəbəkəyə neçə İP düşür

256/4=64(hər alt şəbəkədə 64 ip ünvanı olacaq)

İndi isə şəbəkənin yeni subnet maskını hesablamaq lazımdır:

4 bərabər alt şəbəkə yaradacıqsa 2n >=4 n=2 yeni prefix 24+2= /26 olacaq

Yeni şəbəkə maskası -- 255.255.255.192

ŞƏBƏKƏLƏR

1) Şəbəkə ünvanı:192.168.10.0/26 broadcast ünvanı: 192.168.10.63

ip aralıgı :192.168.10.1-62

2) Şəbəkə ünvanı:192.168.10.64/26 broadcast ünvanı: 192.168.10.127

ip aralıgı :192.168.10.65-126

3) Şəbəkə ünvanı:192.168.10.128/26 broadcast ünvanı: 192.168.10.191

ip aralıgı :192.168.10.129-190

4) Şəbəkə ünvanı:192.168.10.192/26 broadcast ünvanı: 192.168.10.255

ip aralıgı :192.168.10.193-254

**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:

İlk öncə bizdən tələbolunanları yazaq 1000 cihazın yerləşəcəyi bir alt şəbəkə lazımdır.

10.0.0.0/8 şəbəkəsinin subnet maskı 255.0.0.0(A class şəbəkəsidir)

a)Minimum subnet mask nə olmalıdır?

Şəbəkədə olacaq İP ləri hesablayaq: 2^n -2= 1000 n=10

Deməli minimum subnet 32-10 =22 olmalıdır ki bu da 255.255.252.0 olacaq

b) Hər alt şəbəkədə neçə İP unvanı olacaq?

İP unvanı sayı 2^10=1024 dür lakin bunlardan biri şəbəkə ünvanı , biri isə broadcast ünvanı olmalıdır.ona görədə istifadə edilə bilən host sayı 1024-2=1022 olacaq

Cavab=1022

**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.

Cavab:

172.16.0.0/16 şəbəkəsini 5 alt şəbəkəyə ayırmalıyıq və hər şəbəkədə 10000 ip ünvanı olmalıdır

a) Hansı alt şəbəkə maskası istifadə olunmalıdır?

Şəbəkə maskını tapmaq üçün 2^n-2>=10000 düsturunu yazırıq buradanda n=14 olur bu da 16384 ip ünvanı edir.Bundan 2 çıxaraq hostların istifadəsi üçün olan 16382 ip ünvanını tapırıq

Deməli 14 bit hostlar üçün lazımdır.Yerdə qalan 32-14 = 18 bir isə bizim şəbəkə maskamız olacaq yəni 255.255.192.0 alt şəbəkə maskası oldu

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

İlk 3 şəbəkənin şəbəkə və yayım ünvanları

ALTŞƏBƏKƏ 1- Şəbəkə ünvanı 172.16.0.0/18 | Broadcast ünvanı- 172.16.63.255

ALTŞƏBƏKƏ 2- Şəbəkə ünvanı 172.16.64.0/18 | Broadcast ünvanı- 172.16.127.255

ALTŞƏBƏKƏ 3- Şəbəkə ünvanı 172.16.128.0/18 | Broadcast ünvanı- 172.16.191.255

**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:

192.168.5.0/24 Şəbəkəsini 8 bərabər alt şəbəkəyə ayırmaq lazımdır

a) Yeni alt şəbəkə maskası nə olacaq?

/24 =255.255.255.0 deməkdir bu da onu göstərir ki son 8 bit hostlar üçündür

Deməli 2^n >=8 n=3 olur

Biz yeni subnet mask; tapmaq üçün köhnənin üzərinə 3 gəlməliyiy 24+3= 27

Deməli alt şəbəkələrin subnet maskı 27 yəni 255.255.255.224 olur.

b) Hər alt şəbəkədə neçə usable IP ünvan olacaq?

Alt şəbəkədəki usable ip sayını tapmaq üçün 32 bitlik hissədən 27 ni cıxırıq

32-27=5 daha sonra 2^5=32 cavabını alırıq

Amma bu 32 ip ünvanından birincisi şəbəkə ünvanı olur sonuncusu isə broadcast ünvanı ona görə də aldıgımız cavabdan 2 cıxaraq nəticəni əldə edirik

32- 2= 30 Cavab: 30 usable IP ünvanı var

**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) Minimum hansı subnet mask istifadə olunmalıdır?

Minimum subnet mask –ı tapmaq üçün( 2^n)-2>=500 düsturunu yazaraq n=9

cavabını alırıq. Deməli 9 bit host ip üçün istifadə olunur Bilirik ki ip 4 ədəd 8 bitlik hissədən yəni 32 bitdən ibarət olur.32-9=23 olduguna görə deməli artıq subnet maskı hesablaya bilərik

Yeni subnet mask /23 255.255.254.0 olur

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

Bu alt şəbəkələrdən birinin şəbəkə ünvanını və broadcast ünvanını yazaq

ALTŞƏBƏKƏ – Şəbəkə ünvanı – 172.30.0.0 Broadcast ünvanı—172.30.1.255

Qeyd bu altşəbəkədə 2^9 yəni 512 ip unvanı var lakin onlardan ilki şəbəkə ünvanına təyin olunur sonuncusu isə yayım ünvanı(broadcast) kimi təyin olunur və cihazlar üçün 510 usable ip ünvanı qalır

**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:

a) Bu IP ünvanı hansı tip IP-dir?

Bu ip ünvanı APİPA(Automatic Private İP Addressing) tiplidir.

Cünki 169.254.0.0/16 aralıgında ip lər o zaman təyin olunurki DHCP serveri ip ünvanı təyin etmir və o zaman avtomatik olaraq bu aralıqda ip ünvanı alınır

b) Bu vəziyyət şəbəkədə hansı problemi göstərir?

Bu problemin səbəbi Şəbəkədə DHCP serverin işləməməsi və yaxud istifadəcini ip unvanını əl ilə daxil etməsinin unutdugunu göstərir.

Problemi aradan qaldırmaq üçün DHCP serveri yenidən config etmək və yaxud manual olaraq əl ilə İP ünvanı təyin etmək lazımdır

**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:

Problem-- Ping 8.8.8.8 dns işləyir, yəni bağlantısı var və şəbəkə düzgün qurulub.ping www.google.com işləmir yəni yəni bu da o deməkdirdi domein adı İP ə cevrilmir(dns serverdə problem var) Bəs buna nə səbəb ola bilər

DNS serveri düzgün config edilməyəndə məsələn DNS server ünvanı səhv veriləndə və ya DNS server cavab vermirsə bu zaman problem yarana bilər.Həmçinin Dns serverda keşlənmiş qeydlərdə problem olanda yəni cache problemi ola bilər

Firewall dns sorgularını blokladıgı üçündə bu problem yarana bilər

Gəlin yoxlamaları edək:

nslookup www.google.com yazıb DNS serveri yoxlayırıq əgər server unknown və ya request timed out xətası versə deməli DNS serverdə problem var

Bu zaman alternativ DNS serveri sınamaq olar (8.8.8.8 və ya 1.1.1.1)

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

Cmd də bunu yazıb yoxlayırıq-- nslookup www.google.com 8.8.8.8

- Əgər işləsə deməli onda yerli DNS serverdə problem var

- Əgər işləməsə Firewall/Bloklama problemi ola bilər.

Həll yolları:

DNS cache təmizləmək--- ipconfig /flushdns yazaraq edə bilərik

DNS serverı dəyişək 8.8.8.8 və ya 1.1.1.1 olaraq təyin edək

Firewall/proxy yoxlamaq dns 53 portu bloklanıbsa deməli problem oradadır

Nəticə:

-Ping IP işləyir, domain işləmirsə --- DNS problemi.

- Diaqnoz üçün: nslookup/dig və alternativ DNS sınaqla yoxlamaq ən yaxşı üsuldur

**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:

Əlimizdə olan nəticələrdən bilirik ki ipconfig ımri nəticəsində İP ünvanı düzgün görünür.Bu da onu göstərir ki DHCP server düzgün işləyir

Ping 192.168.1.1 yəni router ip si uğurlu deyil.Routerlə əlaqə yoxdur bun kabellərdə və yaxud routerin özündə fiziki bir problem ola biləcəyini göstərir.Problem router ilə şəbəkə adapteri arasındadır.

ping 127.0.0.1 (localhost) uğurludur yəni komputer localhostda özü ilə əlaqə qura bilir 127.0.0.1 ünvanı loopback adlanır və hec nədər asılı olmayaraq komputerin özü ilə əlaqəni simulyasiya edir.Şəbəkə protokollarının düzgün işləyib işləmədiyini yoxlayır və firewall in ping sorgularını bloklayır

Digər komputerlərdə ping ugursuzdursabu onu göstrərirki yerli şəbəkədə digər cihazların heç biri ilə əlaqə yoxdur

Problemin həlli yolları:

1.Fiziki əlaqələri yəni kabelləri və wifi –ni yoxlamaq lazımdır.

2.ARP cədvəli və mac ünvan yoxlanmalıdır

3.routerin konfiquryasiyalarını resetləmək lazımdır

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

Cavab

Cisco routerlərindı confiquryasiyaları görmək üçün müxtəlif əmrlər mövcuddur.Gəlin bunlardan bir neçəsinə baxaq:

1.show running-config ---- Hala hazırda işləyəm konfiquryasiyanı göstərəcək

2.show startup-config ---- Yaddaşda saxlanılan yəni boot da yüklənən configi göstərir

3.show ip interface brief ---- bütün interfacelərin ip ünvanın və statusunu göstərir

4.show interfaces ---- interfacelərn texniki vəziyyətini göstərir

5.show version ---- routerin modeli ,ios versiyası və s haqqında məlumat verir

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

Cavab:

Gəlin addımları bir bir izahlı şəkildə yazaq:

1.Router> enable --- imtiyazlı(privileged) rejimə keçmək üçündür

2.Router# configure terminal --- qlobal configuryasiya rejiminə keçir

3.Router(config)# interface GigabitEthernet0/1 --- interface secirik

4.Router(config-if)# ip address 192.168.1.1 255.255.255.0 --- interface ə ip ünvanı təyin edirik

5.Router(config-if)# no shutdown --- interface i aktivləşdiririk

6.Router(config-if)# exit --- configuration rejimindən cixmaq üçündür

7.Router# show ip interface brief --- interfacein up olun olmadıgını yoxlayırıq

**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:

1.Enable

2.Configure terminal

3.Interface GigabitEthernet0/0

4.Ip address 192.168.100.1 255.255.255.0

5.No shutdown

6.Exit

7.Show ip interface brief

8.Copy running-config startup-config

**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:

1.enable --- imtiyazlı rejimə keçmək üçündür

2.configure terminal --- qlobal configuryasiya rejiminə keçir

3.hostname BranchRouter --- router adını BranchRouter olaraq təyin edir

4.enable secret adminpass --- enable rejimi üçün təhlükəsizlik paroludur

5.line console 0 --- kosol portunu config etmək üçündür

6.password cisco123 --- konsol portuna parol təyin edir

7.login --- konsol portunu aktiv edir

8.exit --- alt rejimdədn cıxır

9.exit --- configuration rejimindın çıxır

**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 vasitəsiylə biz interfacelərin adını ,statusunu,ip ünvanını və protokol vəziyyətini görə bilirik

İnterfeyslər haqqında daha ətraflı məlumat istəsək onda bu əmri işlətməliyiy

show interfaces

**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:

router#terminal monitor

2. Mesajları bir fayla yəni LOG –a yazmaq üçünbunları etməliyik:

a) Logging in aktivləşdirilməsi

router(config)# logging buffered 4096

Bu əmr mesajların RAM da saxlanmasını reallaşdırır (4096 –buferin ölcüsüdür onu öz istəyimizə görə də təyin edə bilərik.)

b) Göstərilən log mesajlarını yoxlamaq üçün:

router# show logging

Bu əmr RAM-a yazılmış log mesajlarını göstərir.

**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:

Routerdə və ya switchdə edilən dəyişikləri yaddaşda saxlamaq üçün aşağıdakı əmrlərdən istifadə olunur

Copy running-config startup-config

Bu əmr hal hazırda edilən konfiquryasıyanı yəni ramda olan configi NVRAM-a yükləyir və bu configlər boot zamanı avtomatik olaraq yüklənir

Bunun yerinə alternativ olaraq:

write memory yazmaq olar

**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 bütün əmrləri və cavabları ardıcıl və tam şəkildə aşağıdakı kimi yazmalıyıq

Router# copy running-config tftp:

Address or name of remote host []? 192.168.1.100

Destination filename [running-config]? backup-config

Bu əmrlər nə edir?

copy running-config tftp: — aktiv konfiqurasiya faylını TFTP serverə göndərmək əmri.

192.168.1.100 — TFTP serverin IP ünvanı.

backup-config — TFTP serverdə faylın saxlanacağı ad.

**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:

Switch də parolun unudması zamanı switch in konfiquryasiyalarnı itirmədən parolun bərbası mümkündür.Bu proses password recovery adlanır Burada biz elə etməliyik ki switch startup confiquryasiyasını oxumadan cihaz işə düşsün və biz parolu dəyişərək onu bərpa edək

1.İlk olaraq Cisco cihazını konsol kabeli vasitəsiylə komputerə qoşun

2.Cihazı söndürün və yenidən yandırın,bunu edən zaman cihazın üzərində olan MODE düyməsini 10-15 saniyə basılı saxlayın

3.Switch: rejimi açıldıqda flash yaddaşa daxil olun

4.Startup konfiquryasiya faylının adını dəyişin

5.Rename flash:config.text flash:config.old

6.Cihazı normal şəkildə başlatmaq üçün “Initial configuration dialog sualına NO cavabını verin

7.Enable yazaraq imtiyazlı rejimə keçin

8.əvvəlki configuryasiyanı RAM –a yükləyin

9.copy flash: config.old running-config

10.enable sevret password yeniparol

11.write memory