Szabványok és protokollok

A szabványok és protokollok kiemelkedően fontosok a számítástechnikában és a hálózati kommunikáció területén. Ezek a normák meghatározzák, hogyan kell működniük az egyes komponenseknek és rendszereknek ahhoz, hogy kompatibilisek legyenek és kommunikálni tudjanak egymással. „A szabványok az definiálják, ami az együttműködéshez (interoperability) kell: se többet se kevesebbet” (A.S. Tannenbaum). A szabványok lényegében meghatározzák azokat a minimális követelményeket, amelyek az eszközöknek és rendszereknek tudniuk kell ahhoz, hogy gond nélkül kommunikálni tudjanak egymással. A szabványok pontosan meghatározzák az ilyen együttműködéshez szükséges alapvető feltételeket, mint az adatok formátumát, az adatközlés módját, és más ilyen technikai részleteket. Ezekre a szabványokra azért van szükség, hogy a különböző gyártoktól származó eszközök és rendszerek összekapcsolódjanak és együttműködjenek anélkül, hogy mélyrehatóbban ismerni kellene a másik rendszer belső felépítését és működését. A szabványok segítenek az iparág fejlődésében, az innovációt létrehozásában. Ezáltal a felhasználók számára nagyobb választékot és rugalmasságot biztosítanak, miközben garantálják a különböző rendszerek és eszközök zökkenőmentes együttműködését.

A szabványokat két csoportra lehet osztani, de facto és de jure. A „de facto” szabványok olyan szabványok, amelyek a gyakorlatban alakultak ki és váltak elfogadottá, enélkül, hogy valamilyen szabványügyi szervezet ált volna a szabvány létrejötte mögött. Ezeket a szabványokat a piaci erők, az iparági szokások tették széles körben elfogadottá és alakultak ki. A de facto szabványok jellemzően azáltal váltak elfogadottá, hogy sokan használják, mivel rendelkeznek egy előnyös tulajdonsággal, vagy könnyebb implementációs előnyökkel. A de facto szabványok jelentősége, hogy gyakran sokkal jobban és gyorsabban kielégítik a piac igényeit, mint a, de jure szabványok. De facto szabványok például az MP3 (MPEG Layer 3), formátum a WAV (Waveform Audio File Format) alternatívájaként indult az internetes zenei terjesztésben, majd felváltotta azt. Ma már a legtöbb zenelejátszó média támogatja. Egy másik ilyen szabvány az Ethernet, magas megbízhatósága és könnyű telepítése miatt vált a helyi hálózatok közkedvelt szabványává.

A de jure szabványok olyan hivatalos szabványok, amelyeket szabványügyi hivatalok hoztak létre, fejlesztettek ki a hivatalos eljárások mentén. Ezek a szabványok jól dokumentált és rögzített dokumentumok, melyek teljes mértékben megmagyarázzák a szabvány használatát az adott területen. A de jure szabványok létrejöttéért, egy vagy több szabványügyi szervezet munkája szüksége, legyen az államközi vagy önkéntes szervezet. A legismertebb szabványosítási szervezetek közé tartozik az ISO (International Standart Organization), az ITU (International Telecommunication Union), az IETF (Internet Engineering Task Force) vagy az IEEE (Institute of Electrical and Electronics Engineers) vagy más iparági vagy regionális szervezetek. Ezek a szabványok gyakran hivatkozási pontot jelentenek a termékek, szolgáltatások vagy folyamatok minőségének és megfelelőségének mérésében és értékelésében. De jure szabvány például az IEEE 802.11, amely a vezetéknélküli hálózatok kialakításához és működtetéséhez szükséges szabványt írja le, amit az IEEE fejlesztett ki és írt le ezzel meghatározva a Wi-Fi technológiát. Egy másik példa az ISO 18000, ami az RFID (Radio-Frequency Identification) technológiát, írja le, ami egy fontos szerepet tölt be az azonosítás és nyomkövetés terén.

A protokoll szabályok összesége, amelyek az adatok formázására és feldolgozására vonatkoznak. A protokoll a számítógépes hálózatokban az úgynevezett „közös nyelv”, melynek segítségével tudnak a számítógépek kommunikálni egymással. Ahhoz, hogy egy protokoll működhessen mind a két félnek ismernie kell a protokollt a sikeres kommunikációnak, ez nagyban hasonlít ahhoz mikor két teljesen más anyanyelvet ismerő ember, tételezzük fel, hogy egy német ajkú és egy japán anyanyelvet beszélő ember ahhoz, hogy egymással kommunikálni tudjanak az angol, mint közös nyelvet használják, feltételezve, hogy mind a ketten ismerik az angol nyelvet, tudnak beszélgetni. Ebben a példában a protokoll az angol nyelv. Ilyen protokollra számos példát lehet keresni az internet világában, mint a TCP, UDP protokollok, melyekről a későbbiekben még szó lesz.

<https://www.cloudflare.com/learning/network-layer/what-is-a-protocol>

Internet

Az "internet" egy globális hálózat, amely különböző számítógépeket és hálózati eszközöket kapcsol össze szerte a világon. Az internet lehetővé teszi az adatok cseréjét, kommunikációt, információhoz való hozzáférést és az online tartalmak megosztását.

Az internet a következő fő jellemzőkkel rendelkezik:

1. Globális elérhetőség: Az internet egy világméretű hálózat, amelyen keresztül a felhasználók bármely részén könnyen elérhetik az információkat és szolgáltatásokat.
2. Számítógépek és eszközök hálózata: Az interneten keresztül számítógépek, okostelefonok, táblagépek, szerverek és más hálózati eszközök kapcsolódnak egymáshoz.
3. Protokollok és szabványok: Az internet működését különböző protokollok és szabványok szabályozzák, például a TCP/IP (Transmission Control Protocol/Internet Protocol), amely az adatátvitelt és az adatok csomagolását kezeli.
4. Weboldalak és alkalmazások: Az interneten található weboldalak, alkalmazások, szolgáltatások és tartalmak sokféle témában érhetők el, beleértve az információkeresést, a közösségi médiát, az online vásárlást, az oktatást és még sok mást.
5. Elektronikus levelezés: Az internet lehetővé teszi az elektronikus levelezést (e-mail), amely egy gyors és hatékony kommunikációs eszköz.
6. Online kapcsolatok: Az internet lehetővé teszi az emberek számára, hogy online kapcsolatba lépjenek másokkal, például közösségi média platformokon vagy online csevegőszolgáltatásokon keresztül.

Az internet elindítása és fejlesztése a múlt század közepén kezdődött, és azóta folyamatosan bővül és fejlődik. A közös szabványok és protokollok révén az internet összekapcsolja a világ számítógépes rendszereit és eszközeit, létrehozva a digitális információs és kommunikációs kor egyik kulcsfontosságú alapját.

**OSI modell**

Az OSI (Open System Interconnection) modell egy ISO alapján szabványosított különböző rétegeket használt hivatkozási modell.



ábra 1 OSI modell 7 rétege

Az OSI modellnek 7 különálló rétege van, 5 felosztási elvet követnek:

1. A rétegek különböző absztrakciós szinteket képviselnek
2. Minden réteg jól definiált feladatot hajt végre
3. A rétegek feladatának definiálásakor a nemzetközileg szabványosított protokollokat kell figyelembe vennie
4. A rétegek határait úgy kell meghatározni, hogy a rétegek közötti információcsere minimális legyen
5. A rétegek számának elég nagynak kell lennie ahhoz, hogy eltérő feladatok ne kerüljenek szükségtelenül ugyanabba a rétegbe, viszont elég kicsinek kell lennie ahhoz, hogy az architektúra ne váljon kezelhetetlenné.

Az OSI modell 7 rétegét úgy szabványok, mint protokollok alkotják. Minden egyes rétegnek megvan a maga protokollja, ami szerint tud megtörténni a kommunikáció. Röviden részletezni fogjuk mind a 7 réteg tulajdonságát.

Az OSI modell első rétege a fizikai réteg (Physical Layer) dolgozik a hardware-hez legközelebb mivel a bitek fizikai átvitelével, az átviteli közeggel foglalkozik. Meghatározza a fizikai közeg jellemzőit, mint az elektromos jellemzők vagy a fényimpulzusok. Az adatok átvitele történhet fizikai kábeleken, mint a sodrott érpár, vagy koaxiális kábel, vagy történhet vezeték nélkül is, mint a rádióhullámos átvitel. Főbb protokolljai RJ45, DSL (Digital Subscriber Line), 802.11.

Az adatkapcsolati réteg (Data Link Layer), mint a modell második rétege, fő feladata biztosítani, hogy az adatok a megfelelő képpen megérkezzenek a közegen kereszül egyik eszközről a másik eszközre, a megfelelő sorrend biztosítása az átvitel során. Kezeli az adatok összecsomagolását és kicsomagolását. A két legfőbb protokollja ennek a rétegnek a MAC és az LLC. Még megemlíthető a 802.11 vagy az Ethernet protokollok.

A 3. réteg a hálózati réteg (Network Layer), feladata a csomagok eljuttatása a forrástól a célállomásra. A réteg meghatározza és kijelöli az útvonalat, az összeköttetést megadott kritériumok szerint, feladata az optimális út kiválasztása. Másik feladata az egyszerre történő túl sok adat által okozott torlódások megakadályozása és vagy kezelése. IGP (Interior Gateway Protocol), ICMP (Internet Control Message Protocol), IP (Internet Protocol), csak néhány az ehhez a réteghez tartozó protokollokból.

A szállítási réteg (Transport Layer) az OSI modell következő rétege, mely feladata a hosztok közötti adatátvitel. Fontos része a címzések kezelése, forrás cél összeköttetések meghatározása és annak felügyelése. Mivel a forrás és a célállomás gyakran nagy távolságra vannak egymástól, ezért a küldeni kívánt adat több csomóponton is át kell menjen. A réteg másik feladata ennek kezelés és annak a megvalósítása, hogy a két hoszt csak egy pont-pont összeköttetésnek lássa az adatküldést. Az ehhez a réteghez tartozó protokollok az UDP (User Datagram Protocol), TCP (Transmission Control Protocol), SSL (Secure Socket Layer).

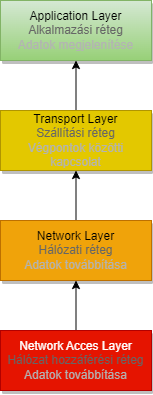
A következő réteg az úgynevezett viszony réteg (session layer), szokás még együttműködési rétegnek is nevezni, mely fenntartja a kapcsolatot a két gép között, illetve lebontja a kapcsolatot mikor az már nem használatos. Beiktat ellenőrző pontokat mivel, hogy ne keljen a meghibásodott adatokat teljesen az elejétől újra küldeni, hanem csak a meghibásodás előtti ponttól A réteg másik nagyon fontos feladata, minden adatcsomag és berendezés szinkronban tartása. Néhány fontosabb protokoll, ami ebben a rétegben található: TCP, SIP (Session Initiation Protocol), RTP (Real Time Transport Protocol).

A 6.-ik réteg a megjelenítései réteg (presentation layer), feladata a bitek által küldött adatcsomagok lefordítását, szükséges kódkonverzió mint például az ASCII (American Standard Code for Information Interchange) vagy más formátumra. Egységes absztrakt adatstukturákat alakít ki és kezeli azokat. Feladata közé tartozik az adatok tömörítése a kisebb méret és így könnyebb kezelhetőség miatt, például videóbeszélgetés során. A fontos adatok titkosítása is ebben a rétegben valósul meg. Főbb protokolljai: HTML (HyperText Markup Language), MPEG (Moving Picture Experts Group), JPEG (Joint Photographic Experts Group) stb.

Az OSI modell utolsó rétege a megjelenítési réteg (Presentation layer), a felhasználóhoz ez a réteg áll a legközelebb mivel a végfelhasználó ez a réteg által nyújtott felületet lássa. A megjelenítési réteg az adatokat jeleníti meg különböző protokollokat használva. Ez a réteg határozza meg melyik protokollt használja a megjelenítés során, mint az FTP (File Transfer Protocol) vagy a HTTP (HyperText Transfer Protocol), mely lekéri a weboldal adatait és megjeleníti azokat egy web böngésző segítségével.

**TCP/IP modell**

A TCP/IP modell megvalósulásának egyik fő oka, hogy a hálózat terjeszkedésével a régebbi protokollok nem, vagy csak alig tudtak működni az új technológiákkal, mint a műholdas vagy rádiós kommunikáció. A modellt úgy alkották meg, hogy minden szempontból lehetővé tegye a hálózatok zökkenőmentes összekapcsolását. Ennek kiküszöbölésére jött létre egy új modell, amit a két legfőbb protokollról neveztek el, amit elsőként Cerf és Kahn [1974] definiált. A másik fő szempont, amit a modellel alkottak meg, hogy ha a végpontok közötti kapcsolat megvan akkor az egy alhálózat meghibásodása ne tudja tönkre tenni a teljes kapcsolatot.



ábra 2 TCP/IP modell 4 rétege

A TCP/IP protokollcsomagnak több kulcsfontosságú szolgáltatása van a hálózati kommunikációja során. Néhány ezek közül:

1. Logikai címzés: A TCP/IP protokollcsomag lehetővé teszi a logikai címzést azáltal, hogy minden eszköznek a hálózatban egyedi, úgynevezett IP címet rendel hozzá. Az IP cím az azonosításban és kommunikációban van fontos szerepe
2. Útválasztás: A TCP/IP protokollcsomag lehetővé teszi az útválasztást, vagyis az adatok továbbítását a hálózaton belül egy adott útvonalat kijelölve és azt használva
3. Névfeloldás: A TCP/IP protokollcsomag lehetővé teszi a névfeloldást, ami az IP címeket egy emberek által könnyebben megjegyezhető formára alakítsa át és fordítva, például a DNS (Domain Name System) segítségével.
4. Hibakezelés és folyamatszabályozás: A TCP/IP protokollcsomag biztosítja a megfelelő hibakezelést és folyamatszabályozást a hálózaton belül, amely így egy megbízhatóbb hálózatot eredményez.
5. Alkalmazások támogatása: A TCP/IP protokollcsomag lehetővé teszi számos alkalmazás használatát a hálózaton, mint az email küldés fogadás, böngészést, fájlmegosztást, videó streamingolást és sok más alkalmazást, amely lehetővé teszi az adatok hatékony és megbízható átvitelét a hálózaton.

A TCP/IP modell tervezésének kulcsfontosságú előnyei közé tartozik:

* Univerzalitás: A TCP/IP protokollokat az interneten és a legtöbb hálózati környezetben használják, így a modell egyetemes elfogadottságat élvez.
* Szabványosítás: A modell segít létrehozni és fenntartani szabványokat a hálózati kommunikációhoz, amelyek segítik az interoperabilitást különböző eszközök és rendszerek között.
* Rugalmas skálázhatóság: A négy réteg modellje lehetővé teszi az egyszerűsített fejlesztést, bővítést és konfigurációt a hálózati rendszerek számára.

A TCP/IP modell legalsó rétege a hálózat hozzáférési réteg (Network Access Layer) lehetővé teszi az adatok továbbítását egyik hosztól a másik fele. Mivel a TCP/IP modell megalkotásánál a fő szempont a különböző átviteli közegek és protokollok használata volt, ezért ez a réteg képes kezelni úgy a vezetékes, mint a vezeték nélküli protokollokon alapuló átviteli technikákat. Más szóval ez a réteg független a bármilyen konkrét hálózati átviteli technológiától.

A modell második rétege a hálózati réteg (Network Layer), hasonló feladatokat lát el, mint az OSI modell hálózati rétege Feladata az adatok eljuttatása, az eljuttatni kívánt adatok kezelése, mivel az adatok nem kell az elküldés sorrendjében megérkezzenek ezért a modell feladata az adatok újra sorba rendezése. A réteg másik feladata az adatok csomagolása és a különböző elválasztási funkciók ellátása. Az ebben a rétegben használt legfontosabb protokollok az IP lásd később, az ARP (Address Resolution Protocol), mely felelős az internet rétegben lévő hardware címek felderítésében, és az ICMP mely diagnosztikai funkciókat lát el, mint mikor egy csomag nem érkezik meg a cél állomásra az ICMP protokoll megkeresi és felderíti a hiba okát.

A szállítási réteg (Transport Layer), felelős az hosztok közötti párbeszéd megvalósítására, adatok eljuttatása a forrástól a célállomás felé. Az ebben a rétegben használt két legfontosabb protokoll a TCP és az UDP protokollok, melyek segítenek az adatok eljuttatásában. A TCP egy az egyhez kapcsolatot hoz létre figyeli az adatcsomagokat, az esetleges adat meghibásodásokat kezeli és vagy javítja őket. Ezzel szemben az UDP protokoll egy az egyhez vagy egy a többhöz kapcsolatokat alakít ki, az adatcsomagok elküldése után már nem foglalkozik többet velük.

A TCP/IP protokoll utolsó rétege az alkalmazási réteg (Application Layer), mely feladata az adatok kezelése és megjelenítése a végfelhasználó számára. Biztosítja a többi réteghez való hozzáférést. Főbb protokolljai a HTTP, FTP, DNS stb.

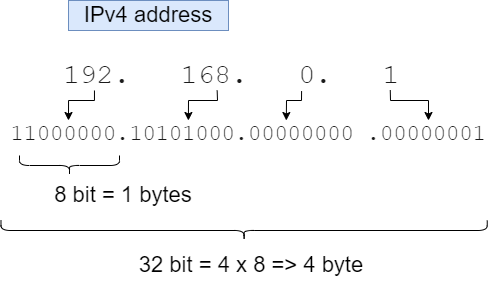
**Az IP (Internet Protocol) protokoll**

Az "IP protokoll" vagy az "Internet Protocol" egy olyan protokoll, amely a hálózatokban történő adatátvitelért felelős. Az IP egy alapvető eleme a TCP/IP hálózati modellnek, és az interneten és más hálózatokban a leggyakrabban használt protokoll.

Az IP protokoll fő feladata a csomagok (packets) címzése és továbbítása a hálózaton keresztül. Az IP címkék segítségével azonosítja az adatok forrását és célját. Az IP címek hierarchikus rendszert alkotnak, amelyek segítik az útvonalazási folyamatot.

Az IP-t két verzióban használják széles körben:

IPv4 (Internet Protocol version 4): Ez a régebbi verzió, amely négy bájtos (32 bites) IP címeket használ. Az IPv4 címek például 192.168.0.1 formátumban jelennek meg. Az IPv4 címtartomány korlátozott, és a világ gyors növekedése miatt a rendelkezésre álló IP címek száma kimerült.



ábra 3 IPv4 képzése

IPv6 (Internet Protocol version 6): Az IPv6 a következő generációs IP protokoll, amely 128 bites IP címeket használ. Ez jelentősen megnöveli az elérhető címek számát, így kevésbé lesz kimerülés a címtartományban. Az IPv6 címek például

2001:0db8:0000:0000: 0000:7a6e: 0680:9668 formátumban jelennek meg.



ábra 4 IPv6 képzése

Az IP protokoll együttműködik más protokollokkal a TCP/IP hálózati modellben. Például az IP és a TCP (Transmission Control Protocol) együttműködik a megbízható adatátvitelért, míg az IP és az UDP (User Datagram Protocol) a gyors, megbízhatatlan adatátvitelért felelős.

**A TCP Protokoll**

A TCP (Transmission Control Protocol) egy megbízható, kapcsolatorientált protokoll, amelyet a TCP/IP hálózati modell transzport rétegében használnak az adatok megbízható továbbítására. A TCP a számítógépek közötti adatkommunikáció egyik alapvető építőköve, és az interneten és más hálózatokon általánosan alkalmazott. A protokoll figyeli az adatok áramlását a hálózaton, és az esetleges hibákat kijavítja vagy újra küldi figyeli az adatok megérkezési sorrendjét és ha szükséges akkor újra rendezi azokat.

A TCP protokoll fő jellemzői:

1. Megbízhatóság: A TCP megbízható adatátvitelt biztosít. Ez azt jelenti, hogy az adatokat az egyik végpontról a másikig megbízhatóan és sorrendben továbbítja, és gondoskodik arról, hogy az adatok a célpontnál épségben megérkezzenek.
2. Kapcsolatorientált: A TCP kapcsolatot hoz létre a kommunikáló felek között, mielőtt adatokat küldenének. Ez a kapcsolat biztosítja a megbízható adatátvitelt, és mindkét fél szinkronizálva tartja az adatforgalmat.
3. Áramlásszabályozás: A TCP áramlásszabályozást alkalmaz, amely szabályozza a küldő és a fogadó oldal közötti adatátvitelt, és csökkenti a túlzott terhelést vagy adatvesztést a hálózaton.
4. Kézbesítési visszaigazolások: A TCP visszaigazolásokat küld az adatok érkezéséről. Ha az adatok nem érkeznek meg, vagy hibásak, a TCP újra küldi azokat.
5. A TCP és az IP (Internet Protocol) együtt alkotja a TCP/IP protokollcsaládot, amely a legtöbb modern hálózati kommunikáció alapját képezi, beleértve az interneten történő adatátvitelt is. A TCP a magasabb rétegek számára biztosít megbízható adatátvitelt, míg az IP az alacsonyabb rétegeken az adatok csomagolásáért és továbbításáért felel.

**Az UDP Protokoll**

Az UDP (User Datagram Protocol) egy másik transzport rétegű protokoll a TCP/IP hálózati modellben. Az UDP kevésbé komplex és kevésbé megbízható, mint a TCP, de gyorsabb és könnyebb. Míg a TCP célja a megbízható adatátvitel és a kapcsolatfenntartás, az UDP a gyors és hatékony adatátvitelt preferálja, anélkül, hogy megbizonyosodna az adatok sorrendjéről vagy épségéről.

Az UDP protokoll fő jellemzői:

1. Nem kapcsolatorientált: Az UDP nem hoz létre kapcsolatot a kommunikáló felek között, mielőtt adatokat küldene. Ez azt jelenti, hogy nincs olyan megbízhatóságot biztosító kapcsolat, mint a TCP esetében.
2. Nincs kézbesítési visszaigazolás: Az UDP nem küld visszaigazolásokat az adatok sikeres kézbesítéséről. Ha az adatok elvesznek vagy sérülnek, az UDP nem próbálja meg újra küldeni őket.
3. Nincs áramlásszabályozás: Az UDP nem tartalmaz áramlásszabályozási mechanizmust, így nincs olyan funkció, amely megfékezi az adatküldést, ha a fogadó oldal túlterhelt.
4. Gyors és könnyű: Az UDP kevesebb protokollinformációt tartalmaz a fejlécében, ami csökkenti az adatátviteli késleltetést és a hálózati terhelést.

Az UDP-t olyan alkalmazások használják, amelyeknél a késleltetés és a könnyedség fontosabb, mint a megbízhatóság. Példák közé tartozik a hang- és videóstreaming, a játékokhoz használt adatkommunikáció, a DNS (Domain Name System) kérések stb.

**Router**

Az útválasztó (router) egy hálózati eszköz, amely az adatcsomagok útját irányítja a különböző hálózatok között. A router egy eszköz, ami összekapcsol 2 vagy több csomag kapcsolt hálózatot vagy alhálózatot. A routerek az OSI modell 3. rétegében (Layer 3) működnek. A szakirodalomban a routereke az ábra 1.1 jelöli. Két fő funkciót lát el: a hálózatok közötti forgalom kezelése az adatcsomagok továbbításával a kívánt IP-címekre, valamint annak lehetővé tétele, hogy több eszköz is használhassa ugyanazt az internetkapcsolatot. A routerek lehetővé teszik az eszközök számára, hogy kommunikáljanak egymással, még akkor is, ha különböző hálózatokon vannak. [1]



ábra 5 Router ikonja

A routerek általában két vagy több hálózati interfésszel rendelkeznek. Minden interfész egy adott hálózathoz csatlakozik. A routerek az adatcsomagokat az egyik interfészről a másikra továbbítják a célhálózat felé.

A routerek különböző módon határozhatják meg az adatcsomagok útját.

* Az egyik lehetőség az, hogy a routerek az adatcsomagok IP-címét használják.
* Egy másik lehetőség az, hogy a routerek a hálózatok közötti útvonalakat tárolják egy útválasztási táblázatban.

A routerek fontos szerepet játszanak az internet hálózatokban. Az interneten a routerek az adatcsomagokat az internetszolgáltatók hálózatai között továbbítják. A routerek különböző típusai léteznek, beleértve a vezetékes routereket, a vezeték nélküli routereket és a mobil routereket.

1. Vezetékes routerek

A vezetékes routerek vezetékes hálózatokhoz csatlakoznak. A vezetékes routerek általában Ethernet-kábellel csatlakoznak a számítógépekhez és más eszközökhöz

1. Vezeték nélküli routerek

A vezeték nélküli routerek vezeték nélküli hálózatokhoz csatlakoznak. A vezeték nélküli routerek általában Wi-Fi-vel csatlakoznak a számítógépekhez és más eszközökhöz.

1. Mobil routerek

A mobil routerek mobil hálózatokhoz csatlakoznak. A mobil routerek általában mobil adatcsomaggal csatlakoznak az internethez.

A routerek előnyei

* + A routerek számos előnnyel járnak, beleértve:
  + Az eszközök közötti kommunikáció lehetővé tétele különböző hálózatokon
  + Az adatcsomagok útjának optimalizálása
  + A hálózat biztonságának javítása

A router hátrányai

A routereknek néhány hátránya is van, beleértve:

* + A routerek költségesek lehetnek
  + A routerek telepítése és konfigurálása bonyolult lehet
  + A routerek meghibásodhatnak, ami a hálózat leállását okozhatja

Hogyan is működik egy útválasztó (router)?

Gondoljuk a routerre úgy, mint egy légiforgalmi irányító központra. Az adatok a repülőgépek a cél állomás pedig a reptér. Minden repülőgépnek egyedi célállomása van és egyedi útvonalon halad, úgy kell minden adatcsomagot a lehető leghatékonyabban a célállomásra eljuttatni. Ebben a szerepkörben a router a forgalomirányító és ő felel azért, hogy mindenki eljusson a célállomásra anélkül, hogy elveszne vagy ütközések történjenek az út során. A csomagok hatékony irányításához az útválasztó egy belső útválasztási táblázatot használ – a különböző hálózati célállomások elérési útvonalainak a listáját. A router leolvassa a csomag fejlécében, hogy hova is tart, majd megkeresi az útválasztási táblázatból (routing table), a célállomáshoz vezető leghatékonyabb utat. Ezután a csomagot továbbítja a következő hálózat felé. [1]

[1] <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-router/>

**Switch**

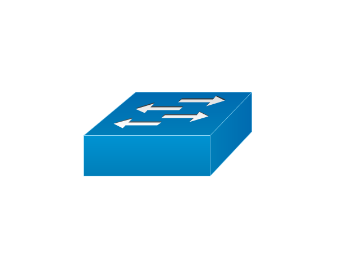
Mi is az a hálózati kapcsoló?

A hálózati kapcsoló (a következőkben swich) összekapcsolja az eszközöket egy hálózaton (gyakran helyi hálózaton, LAN) belül, és továbbítja az adatcsomagokat az eszközök között. Az útválasztóval ellentétben a kapcsoló csak a neki szánt egyetlen eszköznek (amely lehet egy másik kapcsoló, útválasztó vagy a felhasználó számítógépe) küld adatokat, több eszközből álló hálózatoknak nem. Ethernet használatával működik a helyi hálózatokban. MAC-cím (Media Access Control) alapján határozza meg, hogy hova továbbítsa tovább a bejövő üzeneteket. A switch az OSI-modell adatátviteli rétegén 2. rétegében működik (Layer 2).

Milyen típusú switch-ek vannak?

Virtual switches – kizárólag szoftveres kapcsoló, amit szoftver környezeten belül határozunk meg

* **Routing switches** – LAN-ok összekapcsolása. Az OSI 3. réteg útválasztási funkcióit is ellátja és a forgalmat a csomagokban szereplő IP cím alapján is képes a csomagok továbbítására
* **Managed switches** – lehetővé teszi, hogy a switch minden egyes portját be lehessen állítani. Lehetővé teszi a konfigurálást és a felügyeletet
* **Unmanaged switches** – biztosítja az Ethernet eszközök számára az adatok automatikus átvitelét az autonegotáció segítségével, amely meghatározza az olyan paramétereket, mint például az adatátviteli sebesség. A konfiguráció rögzített
* **Smart switches** – konfigurálható, hogy nagyobb ellenőrzést tegyenek lehetővé az adatátvitel felett, de a managed switch-hez képest több korlátozással rendelkeznek
* **Stackable switches** – olyan kapcsolók, amelyek egy hátlapi interfészen keresztül csatlakoztathatok egymáshoz, hogy két vagy több fizikai kapcsolóból egyetlen logikai kapcsolót alkossanak
* **Modular switches** – kapcsolókártyákkal való bővíthetőséget tesz lehetővé, két vagy több fix formátumú kártya befogadására alkalmas switch. Ez a fajta kapcsoló biztosítja a legnagyobb rugalmasságot és frissíthetőséget.



ábra 6 Switch ikonja

<https://www.techtarget.com/searchnetworking/definition/switch>

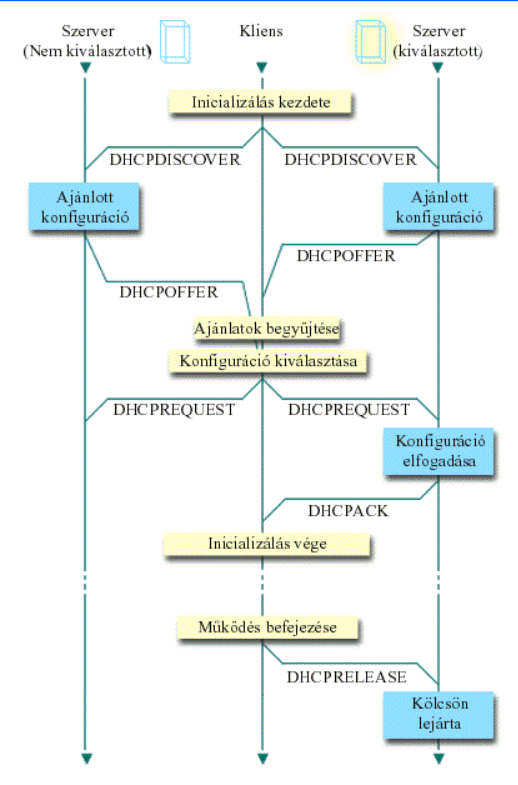
**DHCP**

Minden számítógép rendelkezni a hálózati kártyába épített adatkapcsolati réteggel de IP-címmel nem. Nagy hálózatokon belül nagyon problémás minden végberendezésnek külön - külön megadni az IP-címét, anélkül, hogy valami hiba csúszna belé. Erre a problémára ad megoldást a DHCP. A DHCP (Dynamic Host Configuration Protocol) egy olyan hálózati protokoll, amely az IP-hálózatokon lévő eszközök konfigurálásának automatizálását valósítja meg. DHCP alkalmazás esetén minden hálózat kell rendelkezzen egy DHCP szerverrel A végberendezés adatszórással kér IP-címet a hálózaton belül, ezt DHCP felfedezés csomag küldésével teszi [2]. Amikor a DHCP szerver megkapja a kérést kioszt egy szabad IP-címet a végberendezésnek. Azért, hogy a DHCP szerver IP-cím nélkül ezt meg tudja tenni a végberendezést az Ethernet címével másik nevén MAC címével azonosítja, amit a DHCP felfedezés csomag tartalmaz. De mi van akkor, ha a végberendezés megszűnik, olyankor a kiosztott IP-címmel mi történik? Ilyen esetekre találták ki a lízingelés módszerét, ami annyit takar, hogy a kiosztott IP-cím egy adott időre szól. Az IP-cím lízingelése egy dinamikus folyamat, ahol a DHCP szerver egy ideiglenes IP-címet kioszt egy végberendezésnek. A lízingelési idő egy meghatározott időintervallumba, amelyet a DHCP szerver állít be. Amikor a lízingelési idő közel jár a lejáráshoz, a végberendezés automatikusan megpróbálja megújítani az IP-cím lízingét a DHCP szerverrel. A DHCP szerver ekkor eldönti, hogy további lízingidőt biztosít vagy egy új IP-címet kínál. Ha a végberendezés nem válaszol a lízingmegújítási kérésre, a DHCP szerver újra elérhetővé teheti az adott IP-címet más eszközök számára.

DHCP Folyamat lépései:

1. DHCP Felfedezés (DHCP Discover): Amikor egy eszköz (pl.: számítógép, mobiltelefon) csatlakozik a hálózathoz, és nincs neki konfigurált IP-címe, DHCP felfedezés csomagot küld a hálózaton. Ez a csomag általában a kliens egyedi azonosítóját (jellemzően a MAC címét) tartalmazza. Az üzenet üzenetközvetítés útján kerül kiküldésre. Ha a hálózatban vannak routerek, akkor azokat úgy kell konfigurálni, hogy a DHCP szerver felé továbbítsák a DHCP felfedezés csomagot.
2. DHCP Kínálat (DHCP Offer): A hálózati eszköz által küldött felfedezési csomagot a hálózati eszközökön kívül lévő DHCP szerver észleli. A DHCP szerver válaszként kínálatot (offer) küld vissza a szabad IP-címek közül, amelyeket a végberendezés használhat. Ha a DHCP nem küld vissza a kliensnek kínálat üzenetet, a leggyakoribb okok lehetnek, hogy minden rendelkezésre álló cím ki van osztva, nincs szabad IP cím, a kliens nincs támogatva.
3. DHCP Kérelem (DHCP Request): A végberendezés kiválasztja a kapott kínálatból az egyik IP-címet, majd DHCP kérelmet küld, amelyben elfogadja az ajánlatot és jelzi, hogy melyik általa kiválasztott IP címet kívánja használni. Ezt az üzenetet a teljes hálózat számára elküldi, hogy mindegyik DHCP szerver értesüljön a kiválasztott IP címről.
4. DHCP Nyugtázás (DHCP Acknowledge): A DHCP szerver megkapva a kérelmet, visszaigazolásként (acknowledge) elküldi a végberendezésnek a kiválasztott IP-címet, valamint a hálózati beállításokat. A kliens mostantól használhatja a kapott IP címet.
5. DHCP lízing meghosszabbítása (DHCP kérelem, DHCP Nyugtázás): A lízing idő lejárta elött a kliens megkísérli meghosszabbítani DHCP kérelem üzenet küldésével. Ha a szerver elfogadja a kérést, visszaküld egy nyugtázás üzenetet. Ha a szerver nem válaszol a kliens használhass a bérlési idő lejártáig a kapott IP címet. Mindaddig amig a bérlés él a kliens és a szerver nem kell felfedezés és kínálat üzeneteket folytassanak.
6. DHCP Befejezés (DHCP Release): A kliens befejezi a bérlést befejezés üzenet küldésével, ekkor a szerver visszahelyezi az IP címet a kiosztható címek közé.

A ábra 3 szemlélteti a teljes adatfolyamot egy kliens és szerver között.



ábra 7

[2] Számítógép hálózatok A.S.Tannenbaun

**Internet sebesség mérése**

Az internet sebesség mérése egy alapvető módja az internet tesztelésének. Amikor internetet használunk és az nem működik megfelelően akkor az első dolog, amit csinálunk, hogy fellépünk egy internet sebesség mérésére kitalált oldalra és megmérjük a jelenlegi le és feltöltési gyorsaságát az internetünknek. Az internet sebessége nagyon sok tényezőtől függ, beleértve a szerver sebességét, egyszerre hányan használják az internetet, mit csinálunk, amikor használjuk az internetet stb. Elsőként a kiszolgáló feltérképezi a jelenlegi helyzetünket és a legközelebbi tesztkiszolgálót. A teszt kiszolgáló egy egyszerű jelet (ping) küld a tesztkiszolgálónak és az válaszol. Az üzenet küldése és válasza között eltelt időt ms-ban méri le a rendszer. A ping befejezése után, a letöltési fázis következik. A kiszolgáló egyszerre több kapcsolaton próbál kis mennyiségű adatot letölteni a teszkiszolgálótól.

<https://www.ookla.com/articles/introducing-loaded-latency>

De mennyi is a „jó internet sebesség?” A Federal Communications Commission (FCC) szerint a szélessávú internet minimum követelményei:

25Mbps-os letöltési sebesség és 3Mbps feltöltési sebesség. Az internet sebességét bit/szekundumban mérik, amin a bitek másodpercenkénti sebességét értik, így a Mbps a bit milliomodszorosát értik. A letöltési sebességen azt értik, hogy milyen gyorsan áramlik át az információ a hálózaton keresztül a számítógépre. A feltöltési sebesség méri, hogy milyen gyorsan áramlik át az információ a számítógépről a hálózatra. A késleltetés (latency) azt az időt jelenti, ami alatt a számítógép kapcsolatba lépik az internet szolgáltatóval és az internet szolgáltatótól visszatér a kapcsolat.

A leggyakrabban használt internet sebesség mérő oldalak a fast.com, Speedtest.net, CloudFlare.

<https://www.forbes.com/home-improvement/home/how-to-test-your-internet-speed/>

**Cisco Packet Tracer**

A Cisco Packet Tracer egy olyan szoftver, amelyet a Cisco Systems fejlesztett ki, és célja a hálózati tervezés, szimuláció és gyakorlás elősegítése. A Packet Tracer lehetővé teszi a diákoknak, hálózati szakembereknek és tanároknak, hogy virtuális hálózattokat hozzanak létre és működtessenek, szimulálva valós hálózati környezeteket. A cisco packet tracer képes logikai és fizikai nézetben mutatni a hálózat felépítését. A logikai nézet az általunk felépített hálózat logikai felépítését, eszközöket és az eszközök közötti felépítést mutatja meg. A fizikai nézet megmutatja a logikai hálózat fizikai megvalósítását, az üzenetek áramlását a forrástól a célállomás fele. A cisco packet tracer képes számos a hálózatokban használt protokollok megvalósítására lásd Kép 1

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

Kép 1 A cisco packet tracer által támogatott protokollok

**Tűzfal**

A tűzfal (firewall) egy olyan biztonsági eszköz vagy szoftver, amely védelmet nyújt a számítógépes hálózatok és rendszerek számára, megakadályozva vagy ellenőrizve a nem kívánt hozzáférést és adatáramlást. A tűzfalak fontos szerepet játszanak a hálózati biztonság fenntartásában, és segítenek megelőzni a jogosulatlan hozzáféréseket, a rosszindulatú támadásokat és a biztonsági fenyegetéseket.

A tűzfalaknak két fő típusa létezik:

1. Hardveres tűzfal (Hardware Firewall): A hardveres tűzfal egy önálló eszköz, amelyet a hálózati infrastruktúrába integrálnak. Ezek gyakran különálló eszközök, például tűzfalas routerek, amelyek a hálózati forgalmat ellenőrzik és szűrik. A hardveres tűzfalak fizikai eszközként működnek a hálózat és a külvilág között.
2. Szoftveres tűzfal (Software Firewall): A szoftveres tűzfal egy számítógépes program vagy alkalmazás, amely a számítógépen fut, és ellenőrzi a szoftveres rendszerből származó adatokat. A szoftveres tűzfalak hatékonyan védenek egyetlen számítógépet vagy eszközt, és általában testre szabhatók a felhasználói igények szerint.

A tűzfalak általában a következő funkciókat látják el:

* Állapotellenőrzés (Stateful Inspection): A tűzfal figyeli az átmenő forgalmat és döntéseket hoz annak alapján, hogy milyen állapotban van az adatkapcsolat.
* Csomagszűrés (Packet Filtering): A tűzfal szűri az adatcsomagokat a megengedett és tiltott típusok szerint.
* Proxy szolgáltatások: A tűzfal proxyként működhet, ahol közvetítőként működik az átmenő forgalom és a hálózati erőforrások között.
* Hálózati tervezés (Network Address Translation - NAT): A tűzfal általában NAT-t használ, hogy elrejtse a belső hálózatok IP-címeit a külvilág elől.
* Hozzáférési vezérlés (Access Control): A tűzfal meghatározza, hogy milyen hozzáférést engedélyez vagy tilt meg a hálózati erőforrásokhoz.

A tűzfalak alkalmazásának célja a hálózati biztonság megerősítése és a jogosulatlan hozzáférés, támadások és károkozások minimalizálása. Mint ilyenek, a tűzfalak a felhasználói hozzáférés-szabályozás tágabb kategóriájának egyik biztonsági eszköze. Ezeket a korlátokat jellemzően két helyen állítják fel: a hálózat dedikált számítógépein vagy magukon a felhasználói számítógépeken és más végpontokon (hosztokon).