**1.2 fejezet**

**A HÁLÓZAT RÉSZEI**

* + - 1. **állomások**
* minden olyan számítógépet állomásnak nevezünk, amely csatlakozik a hálózathoz és közvetlenül részt vesz a hálózati kommunikációban
* más néven: végberendezés vagy host, de bizonyos eszközök esetében client vagy ügyfél a neve
* a kommunikációs cél értekében IP (Internet Protocol) címet kap [az IP cím meghatározza az állomást és a hálózatot, amelyhez csatlakozik]
* a nyomtató és a szerver (kiszolgáló, információt biztosít más végberendezések számára pl.: e-mail, http, DNS szerver, fájl is lehet) is egy végponti állomás
* a kliensek szoftverekkel rendelkeznek a szervertől kapott információk kéréséhez és megjelenítéséhez pl. Chrome webböngésző is egy kliensprogram
  + - 1. **egyenrangú hálózatok** (peer to peer hálózat)
* a kliens és a szerver programok általában külön számítógépen futnak, de az egyenrangú hálózatok esetében egy számítógép egyszerre tölti be ezt a két szerepet pl. kisvállalati, otthoni hálózatok esetében
* például: két gépnek vannak fájljai, amit szeretne nyomtatni, nincs kitüntetett kiszolgáló szerep mindenki tud nyomtatni és mindenki kliens is egyben

|  |  |
| --- | --- |
| előnyei:   * könnyen konfigurálható, * kevésbé összetett * alacsonyabb költségű, mert hálózati eszközökre és dedikált kiszolgálókra nincs szükség * egyszerű feladatok elvégzésére pl. fájlátvitel, nyomtatómegosztás alkalmas | hátrányai:   * nincs központosított adminisztráció * nem biztonságos * nem skálázható * minden eszköz működhet egyszerre kliensként és kiszolgálóként is, ami csökkentheti a teljesítményüket |

* + - 1. **végberendezések** (a hálózat végpontjai)
* a végberendezések megkülönböztetésére mindegyiknek hálózati címet kell adni
* amikor egy végberendezés kommunikációt kezdeményez, a célállomás címével határozza meg, hogy hova kell az üzenetet továbbítani. Tehát a végberendezés (telefon vagy számítógép) vagy a forrása vagy a célállomása a hálózaton átvitt üzeneteknek.
  + - 1. **közvetítő eszközök** (ezek az eszközök nem végpontok)
* az egyes végberendezéseket csatlakoztatják a hálózathoz
* biztosítják az összeköttetést és az adatáramlást a hálózaton
* több különálló hálózatot is egymáshoz köthetnek (ezek neve: internetwork)
* a céleszköz címének és a hálózati kapcsolatokról való saját információik alapján határozzák meg az üzenetek útvonalát a hálózaton
* közvetítő eszköz például

wireless router: pl. otthoni router (SOHO-hálózatban)

közvetítő eszköz és forgalomirányító eszköz is lesz a funkciója függvényében

1. LAN Switch – elosztja a hálózatot
2. Router
3. Multilayer Switch
4. Firewall appliance

A közvetítő eszközök feladatai (a felsoroltak egy részét vagy akár mindegyiket elláthatják):

* kommunikációs jelek újragenerálása (távolsággal gyengül a jel, erősíteni kell) és továbbítása (routing),
* hálózaton belüli és a hálózatok közti különböző útvonalak információinak karbantartása,
* értesítési funkció: más eszközök értesítése a hibákról és a kommunikáció sikertelenségéről
* kapcsolati hiba esetén alternatív útvonalak biztosítása
* üzenetek osztályozása és továbbítása prioritásuk alapján
* az adat továbbításának engedélyezésére vagy megtagadása a biztonsági beállítások alapján

|  |
| --- |
| összefoglalva  hálózati eszköz:   * végpont: PC, laptop, szerver, * közvetítő: switch * forgalomirányító: router |

1. **hálózati átvételi közeg** (4-es fejezet FIZIKAI RÉTEG c. részletesen foglalkozik vele)

* a kommunikáció egy átviteli közegen (csatornán) halad a hálózaton, célja, hogy az üzenet eljusson a forrástól a célállomásig
* 3 fajtája van:
  + - 1. fémdrót kábelben (rézkábel): az adat elektromos impulzusokká kódolva halad
      2. üveg- vagy műanyag szálak kábelben(üvegszálas vagy optikai kábel): az adat fényvillanások formájában halad
      3. vezeték nélküli átvitel: az adatokat az elektromágneses hullámok bizonyos frekvenciáinak modulációjával kódolják
* átviteli közeg kiválasztásakor az alábbi szempontokat kell figyelembe venni:

az adott közeg milyen távolságra képes elvinni a jelet

milyen környezetbe lesz telepítve a közeg

mennyi adatot és milyen sebességgel kell továbbítani

mennyibe kerül a közeg és a telepítése

**1.3.1., 1.3.2 HÁLÓZAT MEGJELENÍTÉSE ÉS A TOPOLÓGIAI ÁBRÁK**

eszközök és közegek nevei:

1. **Network interface Card** (NIC):  a hálózati kártya fizikailag csatlakoztatja a végberendezést a hálózathoz.
2. **Fizikai port** : aljzat vagy csatlakozó egy hálózati eszközön, ide csatlakozik egy végberendezéshez vagy egy másik hálózati eszközhöz vezető kábel.
3. **Interfész**: speciális port a hálózati eszközön, amely más hálózatokhoz csatlakozik. Mivel a routerek hálózatokat kötnek össze, ezért a router portjait hálózati interfészeknek nevezzük.

topológiai ábrák: vizuális térképet adnak a hálózat csatlakozásairól

2 fajtája van:

* FIZIKAI TOPOLÓGIAI ÁBRA (fatopológia, csillagtopológia): szemléltetik a közvetítő eszközök fizikai helyét és a kábeltelepítést,valamint hogy melyik helyiségben vannak az eszközök.
* LOGIKAI TOPOLÓGIAI ÁBRA:  hálózat eszközeit, portjait és címzési sémáját ábrázolja, valamint hogy melyik végberendezés melyik közvetítő eszközhöz csatlakozik, milyen átviteli közeggel.

**1.4 HÁLÓZAT TÍPUSOK**

Különböző méretű hálózatok léteznek:

1. kisméretű otthoni hálózatok (PAN): néhány számítógépet kapcsol össze egymással és az internettel.

Egy eszköz és a perifériái (telefon és bluetooth fülhallgató) tartoznak bele. IP címezés nem lesz köztük, csak USB vagy bluetooth lesz a kapcsolat. Ez egy állomásnak minősül hálózati szempontból,

1. **kisvállalati és otthoni irodai hálózatok (SOHO): a**z otthoni vagy távoli iroda számítógépeit kapcsolja össze a céges hálózattal, vagy központi, megosztott erőforrások elérését teszi lehetővé. Több gépet, több végpontot, routert kapcsol össze,
2. közepes és nagy hálózat (LAN) például vállalati vagy iskolai hálózatok, sok helyszínen, több száz vagy ezer számítógépet kapcsolnak össze.

Sok végpont van, és szerver mindenképpen van. A szerver adja ki az IP címet, több épület is lehet összekötve, kialakítható álhálózat is,

1. világméretű hálózat (WAN): a hálózatok hálózata, ami több száz millió számítógépet kapcsol össze világszerte. Sok LAN összekapcsolva

A hálózatokat több szempont szerint osztályozzuk:

* lefedett terület mérete,
* kapcsolódott felhasználók száma
* az elérhető szolgáltatások száma és típusa,
* felelősség mértéke

1. PAN: személyi hálózat egy gép és a perifériák.
2. SOHO: otthoni hálózat (small office, home office) soho router és kevés végpont (PC, telefon, mosógép). Kívülről korlátozottan elérhető, belülről induló kérdésekre és az érkező válaszokra válaszol a soho router.

A hálózati infrastruktúrák két leggyakoribb típusa a helyi hálózat (LAN) és a nagy kiterjedésű hálózat (WAN). A LAN olyan hálózati infrastruktúra, amely kis földrajzi elhelyezkedésű területen biztosít összeköttetést felhasználók és végberendezések számára. A LAN lehet egy vállalat egy részlege, egy otthoni vagy egy kisvállalati hálózat. A WAN olyan hálózati infrastruktúra, amely más hálózatokhoz biztosít hozzáférést nagyobb földrajzi területen, jellemzően egy nagyobb vállalat vagy távközlési szolgáltató a tulajdonosa és karbantartója. Az ábra WAN-hoz csatlakoztatott LAN-okat mutat

1. LAN: helyi hálózat. Kis földrajzi területet lefedő hálózat. egy korlátozott nagyságú területen (pl.: otthon, az iskolában, egy irodaépületben vagy az egyetemi kampuszon) kapcsol össze végberendezéseket.Egy épület számítógépes hálózata, sok végpont van, routerek, szerverek, több alhálózatot is tartalmazhat. Egy személy vagy szervezet felügyeli. Nagy sávszélességet biztosít a belső végberendezéseknek és a közvetítő eszközöknek
2. MAN: városi hálózat

két fajtája van:

1. LAN-ok összekötése pl. posta

2. internet szolgáltató területi hálózata

1. WAN: egy ország, kontinens törzshálózata (tenger alatti üvegszálas-kábelek). A WAN nagy földrajzi területet lefedő hálózati infrastruktúra. Például egy országban két iroda összekötése (direkt kiépített vonal). Ezeket a hálózatokat nem a kormányok felügyelik. A WAN hálózatokat általában szolgáltatók vagy internetszolgáltatók (ISP, Internet Service Provider) üzemeltetik.

jellemzői:

* biztosítja a nagy földrajzi területeket (pl.: városokat, államokat, tartományokat, országokat vagy kontinenseket) lefedő összeköttetést a LAN-ok között,
* rendszerint több szolgáltató biztosítja,
* lassabb összeköttetést biztosít, mint a LAN.

1. SAN: szerverfarm

**INTERNET**

* az internet egymással összekapcsolt hálózatok világméretű halmaza,
* egymással összekapcsolt LAN-okból és WAN-okból áll (az internet a végpontja a soho vagy a lan hálózat, az utolsó router lesz a végpontja)
* a WAN-ok rézvezetékeken, optikai kábeleken és vezeték nélküli átvitelen keresztül kapcsolódhatnak az internet nincs egyetlen személy vagy csoport tulajdonában. A különböző hálózatok közti hatékony adatkommunikáció egységes és következetes szabványok alkalmazását igényli, egyben számos rendszerfelügyeleti szervezet együttműködését is feltételezi. Vannak olyan szervezetek, amelyek az internetes protokollok és folyamatok formai követelményeire és szabványosítására felügyelnek. Ezen szervezetek közé tartozik az Internet (IETF), az Internet Corporation for Assigned Names and Numbers (ICANN), az Internet Architecture Board (IAB). (nonprofit szervezetek).

**INTRANET**

* egy szervezet LAN-jai és WAN-jai közti privát kapcsolatra használják (helyi hálózat, eléred a serveren a belső tárhelye, de otthonról már nem tudod elérni
* csak a szervezet tagjai, alkalmazottai vagy más, engedéllyel rendelkező személyek férhetnek hozzá.

**EXTRANET**

* egy szervezet használja, hogy biztonságos és megbízható hozzáférést biztosítson a saját hálózata eléréséhez más szervezetek dolgozói számára is. A helyi hálózat része, dekívülről is elérhető Például:

- egy cég hozzáférést biztosít külső beszállítói és alvállalkozói számára,

- egy kórház időpont-foglalási rendszert biztosít az orvosok számára, akik így találkozókat egyeztethetnek a betegeikkel.

- egy oktatásügyi helyi kirendeltség költségvetési és személyzeti adatokat szolgáltat a kerületi iskolákról.

**1.5.1 Internet hozzáférési technológiák**

Az otthoni felhasználók, a távmunkások (távoli dolgozók), és a kis irodák jellemzően egy ISP-hez csatlakoznak, hogy elérjék az internetet. Az elérhető csatlakozási lehetőségekben nagy különbségek találhatók az internetszolgáltatók és földrajzi területek között. Népszerű csatlakozási lehetőség a szélessávú kábel, a szélessávú digitális előfizetői vonal (DSL), a vezeték nélküli WAN és a különböző mobil szolgáltatások.

A szervezeteknek jellemzően más vállalati telephelyekhez és az internethez történő hozzáférésre van szükségük. Gyors kapcsolat szükséges olyan üzleti szolgáltatások támogatására, mint az IP-telefonok, videokonferencia megoldások és az adatközponti tárolás. A szolgáltatók (SP, service provider) vállalati szintű összeköttetéseket kínálnak. Népszerű vállalati szintű szolgáltatás az üzleti DSL, a bérelt vonal és a Metro Ethernet.

**1.5.2. Otthoni és kisvállalati internetkapcsolatok**

* **kábeles, kábeltévés** : kábeltévé szolgáltatók nyújtanak ilyen szolgáltatást, az internet adatjelei ugyanazon a kábelen haladnak, mint a kábeltévé adás. Nagy sávszélesség, magas rendelkezésre állás jellemzi, állandó kapcsolatot biztosít.
* **DSL** (Digital Subscriber Line): nagy sávszélességet, magas rendelkezésre állást és folyamatos internetkapcsolatot nyújt. A DSL telefonvonalon működik. A kisvállalati és otthoni felhasználók aszimmetrikus DSL (ADSL) használatával csatlakoznak, Ez azt jelenti, hogy a letöltési sebesség gyorsabb, mint a feltöltési sebesség.
* **Mobilnetes**: mobilnet vagy mobil adatkapcsolat (angol megfelelője: cellular) a mobilhálózatot használja. Ahol van mobilhálózati jel, ott internetezni is lehet. A teljesítmény függ a telefon képességeitől és attól, hogy épp milyen adótoronyhoz csatlakozik.
* **Műholdas**: a műholdas internet előnye az, hogy olyan helyeken is rendelkezésre áll, ahol semmilyen más internetkapcsolat nincs. A parabola antennának rá kell látnia a műholdra.
* **Betárcsázós**: a modemes vagy betárcsázós internethez egy bármilyen telefonvonal és egy modem kell, ez egy olcsó megoldás. A modem alacsony sávszélessége nagy adatok átvitelére nem alkalmas, de utazás közbeni mobil használatra hasznos.

A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvénye.

**1.5.3 Vállalati internetkapcsolatok**

A vállalatok csatlakozási lehetőségei különböznek az otthoni felhasználók lehetőségeitől. A vállalatok nagyobb és dedikált sávszélességet, valamint menedzselt szolgáltatásokat igényelnek. A csatlakozási lehetőségek eltérőek attól függően, hogy hány szolgáltató működik a vállalat közelségében.

* **Dedikált bérelt vonal**: a szolgáltató hálózatának fenntartott vonala, amellyel földrajzilag távol levő irodákat lehet összekötni hang- és/vagy adatkapcsolat céljából. A bérelt vonalat havi vagy éves díjszabással adják bérbe.
* **Metro Ethernet** : Ethernet WAN néven is hívják. LAN hozzáférési technológiákkal valósít meg WAN-t. Az Ethernet egy LAN-technológia.
* **Üzleti DSL**: Sok változata van. A legnépszerűbb változat a szimmetrikus digitális előfizetői vonal (SDSL), amely hasonló az aszimmetrikus digitális előfizetői vonalhoz (ADSL), de ugyanakkora feltöltési és letöltési sebességet biztosít.
* **Műholdas**: műholdas szolgáltatást ott is lehet nyújtani, ahol vezetékes megoldás nincs.

A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei.

**1.5.4. Konvergáló hálózat**

**Hagyományos különálló hálózatok**

Egy harminc évvel ezelőtt épült iskolában a tantermek külön kábelezést használtak az adathálózathoz, a telefonhálózathoz és a televíziókhoz használt videohálózathoz. Ezek a különálló hálózatok nem tudtak kommunikálni egymással. Minden hálózat különböző technológiákat használt a kommunikációs jel hordozásához. Mindegyik hálózatnak saját szabályai és szabványai voltak a kommunikáció sikeres lebonyolításához. Több szolgáltatás futott több hálózaton.

**Konvergált hálózatok**

Ma a különálló adatok, telefon- és videóhálózatok kezdenek összeolvadni. A dedikált hálózatokkal ellentétben a konvergált hálózatok adat-, hang- és videojelet is képesek átvinni ugyanazon a hálózaton, különböző típusú eszközök között. Ez a hálózati infrastruktúra már ugyanazokat a szabályokat, megállapodásokat és megvalósítási szabványokat használja. A konvergált adathálózat több szolgáltatást nyújt egy hálózaton.

**1.6.MEGBÍZHATÓ HÁLÓZATOK**

**1.6.1. HÁLÓZATI ARCHITEKTÚRÁK**

Ahhoz, hogy a hálózatok hatékonyan működhessenek, egész hálózatot egy szabványos hálózati architektúra alapján kell kiépíteni.

A hálózatok számos alkalmazást és szolgáltatást támogatnak, ugyanakkor a fizikai infrastruktúrát alkotó különböző kábelekkel és eszközökkel is együtt kell működniük. A hálózati architektúra kifejezés ebben az összefüggésben azokra a technológiákra utal, amelyek támogatják azt az infrastruktúrát, valamint a különböző programozott szolgáltatásokat és szabályokat (más néven protokollokat), amelyek adatokat küldenek a hálózaton keresztül.

A hálózatok fejlődésével kialakult az a négy alapvető jellemző, amelyet a hálózat tervezőjének meg kell valósítania, ha teljesíteni szeretné a felhasználók elvárásait:

* hibatűrés
* skálázhatóság
* szolgáltatás minősége (QoS)
* biztonság

**HIBATŰRÉS**

Egy hibatűrő hálózat hiba előfordulása esetén minimalizálni tudja az érintett eszközök számát. A hiba után gyors helyreállítást tesz lehetővé. Az ilyen hálózatok azon alapulnak, hogy az üzenet forrása és a célja között több útvonal is létezik. Ha egy útvonal megszakad, az üzeneteket azonnal egy másik kapcsolaton továbbítják. **Redundanciának** hívják azt, amikor egy célállomáshoz több út is vezet.

A csomagkapcsolt hálózat megvalósítása egy lehetséges módja annak, hogy a megbízható hálózatok redundanciát biztosítsanak. A csomagkapcsolás a forgalmat szétdarabolja és egy megosztott hálózaton át továbbítja. Ilyenkor egyetlen üzenet (pl.: egy e-mail vagy videófolyam) több üzenetblokkra, úgynevezett csomagokra lesz bontva. Minden csomag rendelkezik a szükséges címzési információkkal az üzenet forrásáról és céljáról. A hálózat routerei a hálózat állapota alapján irányítják a csomagokat. Ez azt jelenti, hogy egy üzenet darabjai egészen különböző úton érhetik el ugyanazt a célt. Az ábrán azt látjuk, hogy a felhasználó tudta és befolyása nélkül fogja a router másfelé irányítani a csomagot egy kapcsolat hibája esetén.

**SKÁLÁZHATÓSÁG**

A skálázható hálózatot nagyon gyorsan lehet bővíteni az új felhasználók és alkalmazások támogatásához. Ezt anélkül lehet megvalósítani, hogy a jelenlegi felhasználók által igénybe vett szolgáltatások teljesítménye csökkenne. Az ábra azt mutatja, hogyan lehet egy új hálózatot könnyen hozzáadni egy meglévő hálózathoz. Ezek a hálózatok azért skálázhatók, mert a tervező követi az elfogadott szabványokat és protokollokat. Ez lehetővé teszi, hogy a szoftver- és hardvergyártók a termékek és szolgáltatások fejlesztésére összpontosítsanak anélkül, hogy új szabályokat kellene kidolgozniuk a hálózaton belüli működéshez.

**SZOLGÁLTATÁSMINŐSÉG**

A szolgáltatás minősége (QoS) egyre erősebb követelmény a jelenlegi hálózatokban. Egyre újabb hálózati alkalmazások állnak a felhasználók rendelkezésére, mint például az élő hang- és videoközvetítési szolgáltatások, és ezek egyben magasabb minőségi elvárásokat is támasztanak. Mivel az adat-, hang- és videotartalom ugyanazon a hálózaton utazik, a QoS az elsődleges módszer a torlódások kezelésére és a megbízható kézbesítés megvalósítására a felhasználók számára.

Torlódás akkor alakul ki, ha a sávszélességigény magasabb, mint amennyi rendelkezésre áll. A hálózati sávszélesség az egy másodperc alatt átvihető bitek száma, vagyis a mértékegysége a bit per másodperc (bps). Ha egyszerre több kommunikáció használja a hálózatot, akkor előfordulhat, hogy az összesített igény meghaladja a rendelkezésre álló hálózati sávszélességet, vagyis torlódás alakul ki.

Ha a forgalom nagyobb, mint amennyit át lehet vinni a hálózaton, az eszközök a memóriában tárolják a csomagokat addig, amíg nem tudják továbbítani. Az ábrán egy felhasználó weboldalt tölt le, egy másik pedig telefonbeszélgetést folytat. Egy QoS-házirenddel konfigurált router képes az adat- és hangforgalom kezelésére úgy, hogy a hang alapú kommunikációnak elsőbbséget biztosít hálózati torlódás esetén.

**HÁLÓZATBIZTONSÁG**

A hálózati infrastruktúra, a különböző szolgáltatások és a hálózatra csatlakoztatott eszközökön átmenő adatforgalom létfontosságúakká váltak a személyes és az üzleti világban. Két típusú hálózatbiztonsági probléma létezik: a hálózati infrastruktúra biztonsága és az információbiztonság.

A hálózati infrastruktúra biztosítása magában foglalja a kapcsolatokért felelős eszközök fizikai biztonságának a megteremtését, valamint ezen eszközök felügyeleti szoftvereihez történő illetéktelen hozzáférés megakadályozását is

* 1. **FIZIKAI RÉTEG CÉLJA**

**4.1.1. FIZIKAI KAPCSOLAT**

Mielőtt bármilyen hálózati kommunikációt folytatnánk, a fizikai kapcsolatot kell kialakítani a helyi hálózaton. A kapcsolat lehet vezetékes vagy vezeték nélküli, attól függően, hogy kábelt vagy rádióhullámokat használunk az átvitelhez.

A fizikai kapcsolat típusa a hálózat kialakításától függ. Például számos vállalati irodában az alkalmazottak asztali és hordozható számítógépei egyaránt kábellel csatlakoznak egy switch-hez. Ez a beállítás vezetékes hálózatot jelent. Az adatok továbbítása fizikai kábelen keresztül történik.

A vezetékes összeköttetés mellett számos vállalat kínál vezeték nélküli kapcsolatot laptopok, táblagépek és okostelefonok számára. Vezeték nélküli eszközök esetében az adatok továbbítását rádióhullámok végzik. A vezeték nélküli kapcsolatok is egyre terjednek, mivel az egyéni és vállalati felhasználók egyaránt felfedezik annak előnyeit. A vezeték nélküli hálózat eszközeit olyan vezeték nélküli hozzáférési ponthoz (AP) vagy vezeték nélküli routerhez kell csatlakoztatni.

**VEZETÉKES KAPCSOLAT VEZETÉK NÉLKÜLI ROUTERHEZ**

A hálózati kártyák (NIC) eszközöket csatlakoztatnak a hálózathoz. Az Ethernet kártyák vezetékes, míg a WLAN kártyák vezeték nélküli kapcsolatok létrehozására használhatók. A végfelhasználói eszközökben a két típus legalább egyike megtalálható. Ha egy hálózati nyomtató például csak Ethernet csatlakozóval rendelkezik, akkor a hálózathoz csak kábel használatával tud kapcsolódni. Más eszközök, például a táblagépek és az okostelefonok, csak WLAN adapterrel rendelkeznek, így csak vezeték nélküli kapcsolatot képesek létesíteni.

**VEZETÉKES KAPCSOLAT ETHERNET HÁLÓZATI KÁRTYA HASZNÁLATÁVAL**

Hálózati kapcsolódás esetén nem minden fizikai kapcsolat egyenértékű a teljesítmény tekintetében.

**4.1.2.FIZIKAI RÉTEG**

Az OSI modell fizikai rétege biztosítja a adatkapcsolati réteg kereteit alkotó bitek továbbítását a hálózati közegen. Ez a réteg egy teljes keretet fogad az adatkapcsolati rétegtől, és olyan jelek sorozatává alakítja, amelyek továbbíthatók az átviteli közegen. A keretet alkotó bitek származhatnak végberendezéstől vagy közvetítő eszköztől egyaránt.

A beágyazási folyamat utolsó része a fizikai közegen keresztül küldött biteket mutatja. A fizikai réteg kódolja a kereteket és létrehozza azokat az elektromos, optikai vagy rádióhullámú jeleket, amelyek a keret bitjeinek felelnek meg. A jelek ezután egyesével elküldésre kerülnek az átviteli közegen. A célállomás fizikai rétege fogadja ezeket a jeleket, bitekké alakítja őket, majd a biteket teljes keretként továbbítja az adatkapcsolati rétegnek.

1. rézkábel: minden impulzusban más-más feszültség megy át ,
2. optikai kábel: impulzus formában megy az átvitel
3. vezeték nélküli: AM, FM

SÁVSZÉLESSÉG: adott másodperc alatt mennyi adatot tudsz átvinni a kábelen

1. késleltetés: valós idő, ami alatta az az adatmennyiség átjut
2. átbocsátóképesség: adott idő alatt, hány bit jut át, ez valós, tényleges adat
3. hasznos átbocsátóképesség: speed test

**4. 3 RÉZKÁBELEK**

JELLEMZŐI

A rézkábelek a leggyakrabban használt kábeltípusok a mai hálózatokban. A rézkábel valójában nem csak egyfajta kábeltípust jelent. Három különböző típusa létezik, amelyek mindegyike meghatározott körülmények között használható.

A hálózatokban azért használunk rézkábelt, mert olcsó, könnyen telepíthető és kicsi az ellenállása az elektromos árammal szemben. Hátránya viszont, hogy korlátozott a kábelhossz és érzékeny az interferenciára.

A rézkábelben az adatok elektromos impulzusok formájában továbbítódnak. A vevőkészülék hálózati interfészének érzékelője fogadja azokat a jeleket, amelyekből sikeresen vissza tudja állítani az elküldött jelet. Azonban minél távolabbra jut el a jel, annál inkább gyengül. Ezt nevezik jelcsillapításnak. Emiatt minden réz alapú kábelnél be kell tartani a szabványokban meghatározott szigorú hosszúsági korlátozásokat.

Az elektromos impulzusok időzítési és feszültségértékei két forrásból származó interferenciára érzékenyek:

* **Elektromágneses interferencia (EMI) vagy rádiófrekvenciás interferencia (RFI)**: az EMI és RFI jelek torzíthatják és meghamisíthatják a réz alapú adathordozók által továbbított adatjeleket. A jellemző zavarforrások közé tartoznak a rádióhullámok és az elektromágneses eszközök, például a fluoreszkáló lámpák vagy az elektromos motorok.
* **Áthallás:** ha egy vezetéken haladó jel elektromos vagy mágneses mezője által keltett zavar átterjed a szomszédos vezetéken található jelre. Telefonvonalakon az áthallás következménye lehet, hogy halljuk egy szomszédos vonalon zajló másik beszélgetés részleteit. Tehát amikor egy vezetéken elektromos áram folyik keresztül, a huzal körül kis méretű, körkörös mágneses mező alakul ki, amely a szomszédos vezetékre is kifejti hatását.

Az EMI és az RFI negatív hatásainak ellensúlyozására néhány rézkábel típusban fémes árnyékolást alkalmaznak és előírják a kapcsolat megfelelő földelését.

Az áthallás negatív hatásainak csökkentése érdekében bizonyos rézkábel fajtákban az ellentétes áramköri érpárokat összesodorják, ezzel tudnak hatékonyan fellépni ellene.

A rézkábel elektromos zajokra való érzékenysége az alábbi tényezők használatával korlátozható:

* az adott hálózati környezetben leginkább alkalmazható kábel típusának vagy kategóriájának kiválasztása
* kábelezési terv készítése az ismert és az előre látható interferencia források elkerülésére.
* kábelek megfelelő kezelésére és lezárására vonatkozó kábelezési technikák használata.

TÍPUSAI

1. **árnyékolatlan csavart érpár (UTP)**

Az árnyékolatlan csavart érpáras kábel (UTP) a leggyakrabban használt hálózati átviteli közegtípus. Az UTP kábelek RJ-45-ös csatlakozókban végződnek, hálózati állomások és hálózati eszközök (pl. switch-ek és routerek) közötti összeköttetés létrehozására használják.

A helyi hálózatokban használt UTP kábel négy pár, színkóddal jelölt, egymással összecsavart vezetékből áll, amely rugalmas műanyag köpenybe van befoglalva a fizikai károsodástól történő védelem miatt. A vezetékek csavarása a más vezetékekről származó jelinterferencia elleni védelemre szolgál.

A színkódok az egyes vezetékpárok és a párokban található vezetékek azonosítására szolgálnak, valamint segítenek a kábelek végződtetéseinek létrehozásában.

1. **árnyékolt csavart érpár (STP)**

Az árnyékolt csavart érpáras kábel (STP) jobb zaj elleni védelmet biztosít, mint az UTP kábel. Viszont az UTP-hez hasonlítva az STP kábel lényegesen drágább, és nehezebb is telepíteni. Az UTP-hez hasonlóan RJ-45-ös csatlakozót használ.

Az STP kábelek az EMI és az RFI ellen használt árnyékolási technikákat kombinálják az áthallás elleni védelmet szolgáló vezetékcsavarással. A teljes értékű árnyékolás eléréséhez az STP kábelek speciálisan árnyékolt STP csatlakozókban végződnek. Ha a kábel nem megfelelően van leföldelve, az árnyékolás antennaként viselkedve összegyűjtheti a nemkívánatos jeleket.

Az STP kábel négy érpárat használ. Ezek mindegyike fóliaárnyékolással van borítva, amelyek aztán még egy fémhálóval vagy fóliával is be vannak burkolva.

1. **Koaxiális kábel**

A koaxiális kábel - vagy röviden koax - elnevezés a vezeték szerkezetéből származik, mivel két vezető egy közös tengelyen (axis) osztozik. A koaxiális kábel az alábbi részekből áll:

* egy rézvezető, amely az elektronikus jelek továbbítását végzi,
* a rézvezetőt körülvevő rugalmas műanyag szigetelőréteg,
* szigetelőanyagot beborító rézfonat vagy fémfólia, amely az áramkör második vezetékeként és a belső vezető árnyékolójaként működik. Ez a második réteg (más néven árnyékolás) a külső elektromágneses interferencia hatását is csökkenti.
* a kisebb fizikai sérülések elleni védelem érdekében az egész kábel egy borítással van bevonva.

A koaxiális kábelhez különböző típusú csatlakozók használhatók. A bajonett Neill—Concelman (BNC), N és F típusú csatlakozók.

A mai modern Ethernet hálózatokban az UTP kábel lényegében felváltotta a koax kábelt, a koax kábelnek a következő felhasználási területei léteznek:

* **Vezeték nélküli berendezések**: a koaxiális kábel antennákat kapcsol össze vezeték nélküli eszközökkel. A kábel hordozza a rádiófrekvenciás (RF) energiát az antennák és a rádiós berendezés között.
* **Kábelnetes berendezések** : a kábelnetes szolgáltatók úgy biztosítják az internetkapcsolatot az ügyfelek számára, hogy a koax kábel egyes részeit és az erősítő elemeket optikai kábellel helyettesítik. Az ügyfél telephelyén azonban még mindig koax kábelt használnak.

**4. 4. UTP KÁBEL**

TULAJDONSÁGAI

Az UTP kábelt a helyi hálózatokban történő használatra szabványosították.

Hálózati átviteli közegként használva az árnyékolatlan csavart érpár (UTP) négy pár, színkóddal jelölt, egymással összecsavart vezetékből áll, amelyek rugalmas műanyag köpenybe vannak befoglalva. Kis mérete előnyös lehet a telepítés során.

Az UTP kábel nem használ árnyékolást az EMI és az RFI hatásainak kivédésére. A kábeltervezők ehelyett felismerték, hogy mivel tudják ellensúlyozni az áthallás negatív hatásait:

* **Kioltás:** a tervezők a vezetékpárokat egy áramkörként hozzák létre. Ha az áramkörben ezt a két vezetéket közel helyezzük el egymáshoz, a két vezeték által keltett mágneses mező pontosan ellentétes irányú lesz. Emiatt a két mágneses mező kioltja egymást, valamint a külső forrásból származó EMI és RFI jeleket is.
* **A vezetékpárok csavarásszámának változtatása:** a kioltási effektus hatásának fokozása érdekében eltérő számú csavarást alkalmaznak az egyes vezetékpárokban. UTP kábel használatakor szigorú előírásokat kell követni a méterenkénti csavarások számát illetően. A narancs/narancs-fehér vezetékpár kevésbé csavart, mint a kék/kék-fehér pár. Mindegyik színezett vezetékpár eltérő számú csavarást tartalmaz.

Az UTP kábel kizárólag a vezetékek csavarásából eredő kioltási hatásra támaszkodik a jelromlás csökkentésének érdekében, valamint hatékonyan biztosítja a vezetékpárok önárnyékolását a közegen belül.

UTP KÁBELEZÉSI SZABVÁNYOK ÉS CSATLAKOZÓK

Az UTP kábel a TIA/EIA által közösen összeállított szabványokban foglaltaknak felel meg. Pontosabban a TIA/EIA-568 szabvány az, amely meghatározza a LAN hálózatok kábelezési előírásait, és a leggyakrabban előforduló LAN kábelezési szabványnak számít. Néhány, a szabványban definiált elem a következő:

* kábeltípusok,
* kábelhosszak,
* csatlakozók,
* kábelvégződés,
* kábeltesztelési módszerek

A rézkábel elektromos jellemzőit a mérnököket egyesítő nemzetközi szervezet, az IEEE határozza meg. Az IEEE az UTP kábeleket a teljesítményük alapján minősíti. Kategóriákba sorolja őket aszerint, hogy mekkora adatátviteli sebességre képesek. Az 5-ös kategóriájú kábelt például a 100BASE-TX FastEthernet típusú megvalósításoknál használják. A további kategóriák közé tartozik a továbbfejlesztett 5-ös kategóriájú, 6-os kategóriájú és a 6a kategóriájú kábel is.

A magasabb kategóriájú kábelek nagyobb adatátviteli sebességeket támogatnak. Az új, gigabites sebességű Ethernet technológiák bevezetésével az 5e kategória kevésbé elfogadott kábeltípussá vált, helyette a 6-os kategória használata javasolt új kábelezések kiépítésekor.

UTP kábel három kategóriája:

* a 3-as kategóriát eredetileg hangátvitelre használták telefonvonalakon, de később adatátvitelre is alkalmazták,
* az 5 és 5e kategóriákat adatátvitelre használják. Az 5-ös kategória 100 Mbps, az 5e kategória pedig 1000 Mbps adatátviteli sebességet támogat,
* a 6-os kategóriában minden vezetékpár között található egy elválasztó rész a nagyobb átviteli sebesség támogatása érdekében. Ez a kategória legfeljebb 10 Gbps-ot támogat,
* a 7-es kategória szintén támogatja a 10 Gbps-ot,
* a 8-as kategória képes a 40 Gbps adatátviteli sebességre is.

Néhány gyártó a 6a kategória követelményeit túlteljesítő kábeleit 7-es kategória jelzővel látja el.

is.

Az UTP kábel végződéseit általában RJ-45 csatlakozóval zárjuk le. A TIA/EIA-568 szabvány az Ethernet kábelben található vezetékek színkódjait és az aljzatok bekötését (lábkiosztást) írja le.

Az RJ-45 csatlakozó a kábel végére szorított (krimpelt) dugaszt jelenti.

**RJ-45 UTP csatlakozók:** acsatlakozóaljzat a konnektor (anya) típusú összetevőt jelenti, amelyet hálózati eszközbe, falba, kabinszerű munkahelyi fülkékbe vagy patch panelbe szerelnek bele. Minden egyes helytelenül szerelt csatlakozó potenciális forrása lehet a fizikai jelek teljesítménycsökkenésének.

**RJ-45 UTP aljzatok**

**helytelenül lezárt utp kábel**: a hibás csatlakozó olyan vezetékeket tartalmaz, amelyek kilógnak, a csavarásuk ki van bontva, és a burkolat nem teljesen fedi őket.

EGYENES – ÉS KERESZTKÖTÉSŰ UTP KÁBEL

Különböző helyzetek különböző szabványú UTP kábelbekötések használatát követelik meg. Ez azt jelenti, hogy az egyes vezetékeket a kábelben különböző sorrendben kell csatlakoztatni az RJ-45 csatlakozó különböző érintkezőihez.

A kábelezési szabványoknak megfelelően a fő kábeltípusok az alábbiak:

* **egyeneskötésű Ethernet kábel:** a leggyakrabban használt hálózati kábeltípus. Általában állomás és switch, valamint switch és router közötti összeköttetéseknél használjuk,
* **keresztkötésű Ethernet kábel:** hasonló eszközök összekapcsolására használjuk. Összeköthetünk vele például switch-et switch-el, állomást állomással vagy routert routerrel. A keresztkötésű kábelek azonban már elavultnak számítanak, mivel a hálózati kártyák az automatikus közegfüggő interfész fordítás (automatic medium-dependent interface crossover, Auto-MDIX) segítségével automatikusan felismerik a kábel típusát és létrehozzák a kapcsolatot,
* egy másik kábeltípus is létezik, az úgynevezett **rollover kábel**, amely a Cisco saját tervezésű kábele. Használatával a routerek vagy switch-ek konzolportjához lehet csatlakozni egy munkaállomásról.

A kereszt- vagy egyeneskötésű kábelek helytelen használata nem károsítja az eszközt, ilyen esetben viszont nem jön létre az eszközök közötti kapcsolat és adatkommunikációra sem kerül sor. Ez gyakori hibának számít, ezért ha a kapcsolat nem elérhető, a hibaelhárítás első lépéseként az eszközök összeköttetéseinek helyességét kell ellenőrizni.

|  |  |  |
| --- | --- | --- |
| kábeltípus | szabvány | alkalmazás |
| egyeneskötésű Ethernet kábel | mindkét végén T568A vagy T568B szabványú | Egy hálózati állomást csatlakoztat egy hálózati eszközhöz, például switch-hez vagy hub-hoz. |
| keresztkötésű Ethernet kábel | az egyik vége T568A, a másik vége T568B szabványú | Két hálózati állomást vagy két közvetítő eszközt kapcsol össze (switch-et switch-hez vagy routert routerhez). |
| rollover kábel | a Cisco saját fejlesztésű protokollja | A munkaállomás soros portját csatlakoztatja egy router konzolportjához adapter használatával. |

**4.5. OPTIKAI KÁBELEK**

TULAJDONSÁGAIK

A magas ára miatt nem olyan elterjedt a használata, mint a különböző típusú rézkábeleké. Az optikai kábel viszont bizonyos tulajdonságai alapján a legjobb választást jelentheti adott helyzetekben.

Bármely más hálózati közeghez képest nagyobb távolságú és nagyobb sávszélességű adatátvitelt tesz lehetővé. A réz vezetékekkel ellentétben az optikai kábel kisebb csillapítással képes a jeltovábbításra, valamint teljesen érzéketlen az EMI és az RFI okozta zavarokra. Az optikai szálakat általában hálózati eszközök összekapcsolására használják.

Az optikai szál egy rugalmas, de rendkívül vékony, átlátszó anyagú nagyon tiszta üvegszál, amely nem sokkal vastagabb az emberi hajszálnál. A bitek fényimpulzusként jelennek meg rajta. A száloptikai kábel hullámvezetőként vagy '"fénycsőként" viselkedik, amikor minimális veszteséggel továbbítja a fényt két végpont között.

Ennek analógiájaként képzeljünk el egy üres papírtörlő tekercset, amelynek belseje tükörrel van bevonva. Ezer méter hosszú, és egy kis lézermutatót használnak Morse kódjelek fénysebességgel történő küldésére. A száloptikai kábel lényegében így működik, kivéve, hogy kisebb az átmérője és kifinomultabb fény alapú technológiákat használ.

TÍPUSAI

két csoportba sorolhatók:

1. Egymódusú kábel (Single-mode fiber, SMF)

**egymódusú szál:** nagyon vékony magból áll, valamint lézeres technológiát használ a fénysugár elküldésére. Főleg az egymástól nagy távolságra, akár több száz kilométerre lévő helyek összekötésére használják, például hosszútávú telefonos és kábeltelevíziós felhasználás során.

1. Többmódusú kábel (Multimode Fiber, MMF)

**Többmódusú szál:** nagyobb a mag átmérője, és LED fényforrást használ a fényimpulzusok kibocsátására. A LED-ből származó fény különböző szögekben léphet be a szál belsejébe. Helyi hálózatokban népszerű, mivel alacsony költségű LED-ekkel üzemel. Akár 10 Gb/s adatátviteli sebességet is elérhetünk vele, a maximális 550 méteres kábelhosszon.

Az MMF és SMF közötti legnagyobb különbségek egyike a szóródás (diszperzió) mértéke. A szóródás arra utal, hogy a fényimpulzus mennyire terjed szét egy bizonyos idő eltelte után. A nagymértékű szóródás a jelerősség fokozottabb gyengülését is jelenti. A többmódusú szálnak nagyobb a diszperziója, mint az egymódusúnak. Ezért egymódusú szál esetén a jelet csak 500 méter távolságig lehet továbbítani veszteség nélkül.

FELHASZNÁLÁSI TERÜLETEI

* **vállalati hálózatok**: gerinchálózat kábelezése és a hálózat infrastruktúráját alkotó eszközök összekötése.
* **üvegszál az otthonig (Fiber-to-the-home, FTTH)**: folyamatos szélessávú kapcsolatot biztosít az otthoni és kisvállalati felhasználók számára.
* **nagytávolságú hálózatok**: szolgáltatók használják országok és városok összekötésére.
* **tenger alatti kábelhálózatok**: nagy sebességet és kapacitást biztosít akár óceánnyi távolságok áthidalására is, valamint képes ellenállni a tengerek alatt lévő körülményeknek.

OPTIKAI CSATLAKOZÓK

Az optikai csatlakozók az optikai szálak végződéseit zárják le. Ezeknek számos típusa elérhető. A fő különbség közöttük a méretből és a kapcsolódás módjából adódik. Annak kiválasztása, hogy a különböző típusok közül melyik kerül felhasználásra, a vállalat eszközeitől függ.

Egyes switchek és routerek olyan portokkal rendelkeznek, amelyek támogatják az SFP (small form-factor pluggable) típusú optikai csatlakozókat.

optikai csatlakozók fajtái:

* ST (Straight-Tip) csatlakozó: az egyik legkorábban használt csatlakozótípus. A csatlakozót fel- és lecsavarható (twist-on/twist-off) bajonettzáras módszerrel lehet biztonságosan rögzíteni
* SC (Subscriber Connector) csatlakozók: négyzetes vagy szabványos csatlakozónak is nevezik. Széles körben elterjedt LAN és WAN hálózati csatlakozótípus, amely megnyom-kihúz (push-pull) típusú mechanizmust használ a biztos csatlakozás érdekében. Egy- és többmódusú kábelek esetében egyaránt használják ezt a típust.
* Szimplex LC (Lucent connector) csatlakozó:a szimplex LC csatlakozók az SC csatlakozó kisebb változatai. A kicsi vagy helyi csatlakozó néven is említett típus gyors népszerűségre tett szert a kis mérete miatt.
* Többmódusú duplex LC csatlakozók:Hasonló a szimplex LC-csatlakozóhoz, de duplex csatlakozót használ.

A közelmúltig a fényt csak egy irányban lehetett továbbítani az optikai szálon keresztül. A teljes duplex működés megvalósításához két szálra volt szükség. Az optikai lengőkábelek (patch kábelek) emiatt két optikai szálat foglalnak magukban, a végződésüket pedig szabványos optikai csatlakozópárral valósítják meg. Bizonyos optikai csatlakozók, amelyeket duplex csatlakozó néven ismerünk, képesek a küldő és a fogadó szálat egy csatlakozóba bekötni, ez duplex többmódusú LC csatlakozó néven látható az ábrán. A BX szabványok (például a 100BASE-BX) különböző hullámhosszakat használnak egyetlen szálon keresztül történő küldéshez és fogadáshoz.

OPTIKAI PATCH KÁBELEK

Az optikai patch kábelt a hálózatok gerincét alkotó eszközök összekötésére használják. Az egy- és többmódusú kábelek között a kábel színe tesz különbséget. A sárga szín az egymódusú, a narancssárga (vagy kék) pedig a többmódusú kábeleket jelöli.

típusai:

* SC-SC többmódusú patch kábel
* LC-LC egymódusú patch kábel
* ST-LC többmódusú patch kábel
* SC-ST egymódusú patch kábel

**RÉZ – ÉS AZ OPTIKAI KÁBELEK ÖSSZEHASONLÍTÁSA**

Az optikai kábel használatának számos előnye van a rézkábelekhez képest.

Napjainkban az optikai kábelt vállalati környezetben elsősorban gerinchálózati kábelezésnél használják különböző létesítmények nagyforgalmú pont-pont összeköttetéseinek megvalósításakor. Emellett egyetemi kampuszokon is használható az egyes épületek összekötésére. Az optikai kábel remekül alkalmazható ezen célokra, mivel nem vezeti az elektromosságot és kicsi a jelvesztesége.

|  |  |  |
| --- | --- | --- |
| **Felhasználás tényezői** | **UTP kábel** | **Optikai kábel** |
| Támogatott sávszélesség | 10 Mb/s - 10 Gb/s | 10 Mb/s - 100 Gb/s |
| Hatótávolság | Viszonylag kicsi (1 - 100 méter) | Viszonylag nagy (1 - 100 000 méter) |
| EMI és RFI elleni védettség | Alacsony | Magas (teljesen védett) |
| Elektromos veszélyekkel szembeni védettség | Alacsony | Magas (teljesen védett) |
| Vezetékek és csatlakozók költségei | Legalacsonyabb | Legmagasabb |
| Telepítéshez szükséges ismeretek | Legalacsonyabb | Legmagasabb |
| Biztonsági óvintézkedések | Legalacsonyabb | Legmagasabb |

**4.6. VEZETÉK NÉLKÜLI ÁTVITEL**

JELLEMZŐI

A vezeték nélküli közegek rádió- vagy mikrohullámok használatával továbbítják az elektromágneses jeleket, amelyek az adatkommunikáció bináris számjegyeinek felelnek meg.

A vezeték nélküli átvitel biztosítja a legnagyobb mobilitást az összes közegtípus közül, emellett a vezeték nélküli eszközök száma is folyamatosan növekszik. Mostanra a felhasználók leginkább vezeték nélkül csatlakoznak az otthoni és vállalati hálózatokhoz.

A vezeték nélküli átvitel korlátai:

* **Lefedettségi terület** : vezeték nélküli adatátviteli technológiák kiválóan működnek szabadtéren. Ugyanakkor az épületekben használt egyes építési anyagok és a helyi földrajzi viszonyok korlátozzák a tényleges lefedettséget.
* **Interferencia**: vezeték nélküli átvitel érzékeny az interferenciára, és olyan hétköznapi eszközök is zavarhatják az átvitelt, mint például a vezeték nélküli telefonok, bizonyos fénycsőtípusok, mikrohullámú sütők és más vezeték nélküli eszközök.
* **Biztonság**: a lefedettségi területen belül nem kell fizikailag a közeghez kapcsolódni annak használatához. Emiatt az erre nem jogosult eszközök és felhasználók is hozzáférhetnek a hálózathoz. A hálózatbiztonság a vezeték nélküli hálózatok felügyeletének egyik fő összetevője.
* **Osztott átviteli közeg**: a WLAN-ok fél-duplex módban működnek, ami azt jelenti, hogy egyidejűleg csak egy eszköz végezhet adatküldést vagy fogadást. A vezeték nélküli közeg az összes vezeték nélküli felhasználó között meg van osztva. Ha a WLAN-hoz egyszerre több felhasználó is hozzáfér, akkor az minden felhasználó számára csökkenti a sávszélességet.

Habár a vezeték nélküli technológia egyre népszerűbb a kis távolságú összeköttetések esetében, a legnépszerűbb fizikai közegnek még mindig a réz- és optikai kábel számít a közvetítő eszközökkel (mint routerek és switchek ) megvalósított hálózatokban.

TÍPUSAI

A vezeték nélküli átvitelre vonatkozó IEEE és ipari távközlési szabványok mind az adatkapcsolati, mind pedig a fizikai rétegre kiterjednek. Ezen szabványok mindegyikének a fizikai rétegre vonatkozó specifikációja a következő területeket foglalja magában:

* az adatok rádiójelekké történő átalakítása,
* átviteli frekvencia és teljesítmény
* a jel vételére és dekódolására vonatkozó követelmények
* antennák tervezése és kivitelezése

A vezeték nélküli szabványok a következők:

* **Wi-Fi (IEEE 802.11)** : vezeték nélküli LAN (WLAN) technológia, közismert nevén Wi-Fi. A WLAN-ok egy versengés alapú protokollt használnak, amelyet vivőjel-érzékeléses többszörös hozzáférés ütközéselkerüléssel (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA) néven ismerünk. A vezeték nélküli hálózati kártyának küldés előtt figyelnie kell a csatornát annak megállapítására, hogy az szabad-e. Ha éppen egy másik vezeték nélküli eszköz végez továbbítást, akkor a hálózati kártyának várnia kell, amíg a csatorna szabaddá nem válik. A Wi-Fi védjegy tulajdonosa a Wi-Fi Szövetség (Wi-Fi Alliance). A Wi-Fi megnevezés azokra a tanúsított WLAN eszközökre vonatkozik, amelyek a 802.11 szabványok alapján működnek.
* **Bluetooth (IEEE 802.15)**: ez egy vezeték nélküli személyes hálózati (WPAN) szabvány, amelynek közismert neve „Bluetooth”. Társított eszközpárok közötti kommunikációra alkalmas maximum 100 méter távolságig.
* **WiMAX (IEEE 802:16)**: pont-multipont topológiát használ a szélessávú vezeték nélküli hozzáférés biztosításához, közismert neve WiMAX (Worldwide Interoperability for Microwave Access).
* **Zigbee (IEEE 802.15.4)**: egy olyan szabvány, amelyet alacsony adatsebességű és kis energiaigényű kommunikációhoz használunk. Olyan alkalmazásokhoz készült, amelyek rövid hatótávolságot, alacsony adatátviteli sebességet és hosszú akkumulátor-élettartamot igényelnek. A Zigbee-t jellemzően ipari és IoT (Internet of Things) környezetekben használják, például vezeték nélküli villanykapcsolóknál és orvostechnikai eszközök adatgyűjtésénél.

Más vezeték nélküli technológiák, például a mobil és a műholdas kommunikáció szintén nyújthat adathálózati kapcsolatot.

VEZETÉK NÉLKÜLI LAN

A vezeték nélküli hálózat közös adatátviteli közege lehetővé teszi az eszközök számára, hogy vezeték nélkül csatlakozzanak egymáshoz egy LAN-on keresztül. Egy WLAN általában a következő hálózati eszközök használatát követeli meg:

* **Vezeték nélküli hozzáférési pont (Access Point, AP)**: fogadja a felhasználók vezeték nélküli jeleit, és csatlakozik a meglévő rézvezetékes hálózathoz, például az Ethernethez. Az otthoni és kisvállalati környezetben használt vezeték nélküli router egy eszközben tartalmazza a router, a switch és a hozzáférési pont funkcióit.
* **Vezeték nélküli hálózati adapterek**: vezeték nélküli kommunikáció képességét biztosítják a hálózati állomásoknak.

A technológia fejlődésével számos Ethernet alapú WLAN szabvány alakult ki. Vezeték nélküli eszközök vásárlásakor meg kell győződni annak kompatibilitási és az együttműködési képességeiről. A vezeték nélküli kommunikáció előnyei nyilvánvalóak, különösen ha a költséges kábelezés megtakarításáról és a hordozhatóságból adódó kényelemről beszélünk. A hálózati rendszergazdának úgy kell megalkotnia és alkalmaznia a szigorú biztonsági szabályokat, hogy a vezeték nélküli LAN védve legyen az illetéktelen hozzáférésektől és támadásoktól.

**PRTOKOLLOK ÉS MODELLEK**

**3.1.2. KOMMUNIKÁCIÓS ALAPOK**

Minden kommunikációs módszerben van három közös alkotóelem.

1. **az üzenet forrása (küldő, feladó)**: az üzenetek forrásai emberek vagy elektronikus eszközök, amelyeknek üzenetet kell küldeniük más személyeknek vagy eszközöknek.
2. **az üzenet célja (címzett, fogadó)**: a célállomás fogadja és értelmezi az üzenetet.
3. **csatorna**: az a közeg (média) alkotja, amely azt az utat biztosítja, amelyen az üzenetek haladnak a forrástól a célig

KOMMUNIKÁCIÓS PROTOKOLLOK

Egy üzenet küldését szabályok irányítják, amiket protokolloknak nevezünk. Ezek a protokollok a használt kommunikációs módtól függnek. A hétköznapi személyes kommunikációnkban azok a szabályok, amelyeket egy adott közegben használunk (mint például egy telefonhíváskor), nem feltétlenül egyeznek meg azokkal a protokollokkal, amelyeket más közegben használunk (például levélküldéskor).

|  |  |
| --- | --- |
| **analógia** | **hálózat** |
| A kommunikáció előtt meg kell egyezniük a részt vevő feleknek, hogy miként fognak kommunikálni. Ha a kommunikáció beszéddel történik, akkor először meg kell állapodni a nyelvben. Ezután ha van egy megosztandó üzenet, akkor képesnek kell lenniük arra, hogy érthetően megformázzák.  Például, ha valaki az angol nyelvet használja, de rossz a mondat szerkezete, az üzenet könnyen félreérthető lesz. Mindezek a feladatok jellemzik azokat a protokollokat, amelyeket a kommunikáció megvalósításához használni kell. | Ez a számítógépes kommunikációra is igaz. A világ mindenfajta kommunikációs módját rengeteg különféle szabály és protokoll irányítja. |

SZABÁLYOK KIALAKÍTÁSA

A hatékony kommunikációhoz szükséges szabályok (azaz protokollok) használatával kellene megírni.

A protokolloknak a következő követelményeket kell figyelembe venniük a vevő által érthető üzenet sikeres kézbesítéséhez:

* azonosított küldő és fogadó,
* közös nyelv és nyelvtan,
* a kézbesítés sebessége és időzítése,
* megerősítési vagy nyugtázási követelmények.

HÁLÓZATI PROTOKOLL KÖVETELMÉNYEI

A hálózati kommunikációban használt protokollok sok ilyen alapvető tulajdonsággal rendelkeznek. Amellett, hogy azonosítják a forrást és a célt, a számítógépes és hálózati protokollok meghatározzák annak részleteit, hogyan kell egy üzenetet továbbítani a hálózaton keresztül. A leggyakoribb számítógépes protokollok a következő követelményeket teljesítik:

* az üzenet kódolása,
* az üzenet formázása és beágyazása,
* az üzenet mérete,
* az üzenet időzítése,
* az üzenet szállítási feltételei.

ÜZENET KÓDOLÁSA

Egy üzenet elküldésének egyik első lépése a kódolás. A kódolás az, amikor egy információt egy másik, a továbbításhoz megfelelő formába alakítunk át. A dekódolás ennek a fordítottja.

|  |  |
| --- | --- |
| **analógia** | **hálózat** |
| Egy személy felhívja a barátját, hogy megvitassa egy gyönyörű naplemente részleteit.  Az üzenet közléséhez gondolatait egy elfogadott nyelvre alakítja át. Beszéd közben a nyelv hangjait használva küldi el az üzenetet. A barátja meghallgatja a leírást, és dekódolja a hangokat, hogy megértse a kapott üzenetet. | Az állomások közti kódolásnak a közeghez kell alkalmazkodnia. A hálózaton küldött üzenetet a küldő állomás először bitekké konvertálja. Minden bit rézhuzalok feszültségmintázatára, optikai szálakban lévő infravörös fényre vagy vezeték nélküli rendszerekhez tartozó mikrohullámokra van kódolva. A célállomás megkapja és dekódolja a jeleket, hogy megértse az üzenetet. |

ÜZEMET FORMÁZÁSA ÉS BEÁHGYAZÁSA

Amikor egy üzenetet küldünk a forrástól a célig, megfelelő formátumot vagy szerkezetet kell használni. Az üzenet formátuma, formája az üzenet típusától és az átvitelhez használt csatornától függ.

|  |  |
| --- | --- |
| **analógia** | **hálózat** |
| Egy levél elküldése.  A borítékon szerepel a küldő és a fogadó címe, mindegyik a megfelelő helyen. Ha a célcím vagy a formátum helytelen, a levelet nem tudják kézbesíteni.  Beágyazásnak hívjuk azt a folyamatot, amikor egy üzenetformátumot (levél) egy másik üzenetformátumba (boríték) helyezünk. Ennek a fordítottja, a kicsomagolás az, amikor a címzett kiveszi a levelet a borítékból | A levélküldéshez hasonlóan a számítógép-hálózaton küldött üzenet is egy speciális formázási szabályt követ, hogy elszállítsák és feldolgozzák.  Az Internet Protocol (IP) egy olyan protokoll, amely hasonló a boríték példájához. Az Internet Protocol 6-os verziójának (IPv6) csomagjának mezői azonosítják a csomag forrását és célját. Az IP-cím felelős az üzenetforrásból a célba küldött üzenetek küldéséért egy vagy több hálózaton keresztül. |

ÜZENET MÁRETE

|  |  |
| --- | --- |
| **analógia** | **hálózat** |
| Amikor az emberek egymással kommunikálnak, a küldendő üzenetet általában kisebb részekre, rendszerint mondatokra tördelik. A mondatok méretét korlátozza az, hogy a fogadó személy mennyit képes egyszerre feldolgozni. Megkönnyíti az olvasást és a megértést is. | A számítógépes kommunikációban is történik kódolás.  Az állomások közti kódolásnak a közeghez kell alkalmazkodnia. A hálózaton küldött üzenetet a küldő állomás először bitekké konvertálja. Minden bitet hangmintákká, fény- vagy elektromos impulzusokká kódolunk, attól függően, hogy milyen hálózati közegen fogjuk a biteket továbbítani. A célállomás megkapja és dekódolja a jeleket, hogy megértse az üzenetet. |

ÜZENET IDŐZÍTÉSE

Az üzenet időzítése szintén nagyon fontos a hálózati kommunikációban. Az üzenet időzítése a következőket jelenti:

* **adatfolyam-vezérlés:** az adatátvitel sebességének kezelése. Az adatfolyam-vezérlés meghatározza, hogy mennyi információt küldhetünk el és milyen sebességgel, hogy sikeresen célba érjen. Például, ha egy ember túlságosan gyorsan beszél, a többieknek nehéz meghallani és megérteni az üzenetet. A hálózati kommunikációban vannak olyan hálózati protokollok, amelyeket a forrás- és céleszközök használnak az információ áramlásának egyeztetésére és kezelésére.
* **válaszidő-túllépés:** ha valaki feltesz egy kérdést, és nem hallja a választ elfogadható időn belül, akkor feltételezi, hogy már nem is jön válasz, és ennek megfelelően reagál. Lehet, hogy megismétli a kérdést, de az is lehet, hogy folytatja a párbeszédet. A hálózati állomásoknak szintén vannak szabályaik, amik meghatározzák, hogy mennyit kell várni a válaszra, és mit kell csinálni, ha válaszidő-túllépés történik.
* **hozzáférési mód:** meghatározza, hogy mikor küldhet valaki üzenetet. Ha ketten egyszerre beszélnek, "információütközés" lép fel, ezért mindkettőjüknek be kell fejezniük, majd újra kell kezdeniük az egészet. Hasonlóképpen, ha egy eszköz vezeték nélküli LAN-on szeretne továbbítani, a WLAN hálózati interfész kártyának (NIC) meg kell állapítania, hogy a vezeték nélküli közeg rendelkezésre áll-e.

ÜZENET SZÁLLÍTÁSI FELTÉTELEI

|  |  |
| --- | --- |
| **analógia** | **hálózat** |
| Vannak olyan helyzetek, mikor csupán egyetlen emberrel szeretnénk valamilyen információt megosztani. Máskor előfordulhat, hogy emberek egy csoportjával, vagy akár egy adott területen lévő összes emberrel szeretnénk egyszerre közölni valamit | Háromféle adatkommunikációt szoktunk megkülönböztetni:   * **Unicast (egyedi üzenet)**: az információt egyetlen eszköz kapja meg. * **Multicast (csoportos üzenet)**: az információt egy vagy több eszközre továbbítják. * **Broadcast (szórás)**: az információt mindenki megkapja. |

3.2 PROTOKOLLOK

A HÁLÓZATI PROTOKOLLOK ÁTTEKINTÉSE

Az eszközök közti üzenettovábbítás közös formátumát és szabályrendszerét a hálózati protokollok határozzák meg. A protokollokat végberendezések és közvetítő eszközök valósítják meg szoftveresen, hardveresen vagy mindkettő módon. Minden hálózati protokoll saját funkcióval, formátummal és kommunikációs szabályokkal rendelkezik.

A táblázat felsorolja azokat a protokollokat, amelyek egy vagy több hálózaton keresztül történő kommunikáció sikerességéhez szükségesek.

|  |  |
| --- | --- |
| **protokoll típusa** | **leírás** |
| **Hálózati kommunikációs protokollok** | Lehetővé teszik, hogy két vagy több eszköz kommunikáljon egy vagy több hálózaton keresztül. Az Ethernet család számos protokollt foglal magában, ilyenek az IP, a Transmission Control Protocol (TCP), a HyperText Transfer Protocol (HTTP), és még sok más. |
| **Hálózatbiztonsági protokollok** | Ezek a protokollok az adatok biztonságával kapcsolatosak, hitelesítést, az adatok integritását és adattitkosítást biztosítanak. A biztonsággal kapcsolatos protokollok közé tartozik például a Secure Shell (SSH), a Secure Sockets Layer (SSL) és a Transport Layer Security (TLS). |
| **Irányító protokollok** | Ezek a protokollok lehetővé teszik routerek közt az útvonalinformációk cseréjét, az útvonalinformációk összehasonlítását, majd a célhálózat legjobb elérési útjának kiválasztását. Irányító protokoll például az Open Shortest Path First (OSPF) és a Border Gateway Protocol (BGP). |
| **Szolgáltatásfelderítési protokollok** | Ezeket a protokollokat eszközök vagy szolgáltatások automatikus észlelésére használják. A szolgáltatásfelderítési protokollok közé tartozik például a Dynamic Host Configuration Protocol (DHCP), amely az IP-címkiosztási szolgáltatásokat fedezi fel, valamint a nevek és IP-címek közötti fordításhoz használt Domain Name System (DNS). |

HÁLÓZATI PROTOKOLLOK FUNKCIÓI

A hálózati kommunikációs protokollok felelősek a végberendezések közötti hálózati kommunikációhoz szükséges különböző funkciókért.

A számítógépek és a hálózati eszközök közös protokollokat használnak a kommunikációhoz. A táblázat felsorolja a protokollok funkcióit.

|  |  |
| --- | --- |
| **funkció** | **leírás** |
| **Címzés** | Azonosítja az üzenet küldőjét és címzettjét egy meghatározott címzési rendszer szerint. Címzést biztosító protokoll például az Ethernet, az IPv4 és az IPv6. |
| **Megbízhatóság** | ez a funkció szállítási mechanizmusokat biztosít abban az esetben, ha az üzenetek elvesznek vagy megsérülnek a továbbítás során. A TCP biztosít garantált kézbesítést. |
| **Adatfolyam-vezérlés** | Ez a funkció biztosítja, hogy az adatok hatékony sebességgel áramoljanak két kommunikáló eszköz között. A TCP adatfolyam-vezérlési szolgáltatásokat is nyújt. |
| **Sorrendhelyes kézbesítés** | Minden továbbított adatszegmens saját azonosítót kap. A fogadó eszköz az azonosítási információkat használja az információ megfelelő módon történő újbóli összeállításához. Akkor hasznos, ha elvesznek vagy rossz sorrendben érkeznek az adatszegmensek. A TCP azonosítást és sorba rendezést is biztosít. |
| **Hibafelismerés** | Ez a funkció annak meghatározására szolgál, hogy az adatok megsérültek-e az átvitel során. Hibadetektálást biztosít többek között az Ethernet, az IPv4, az IPv6 és a TCP. |
| **Alkalmazás interfész** | Ez a funkció a hálózati alkalmazások közötti folyamat-folyamat közti kommunikációhoz használt információkat tartalmazza. Weboldal elérésekor például HTTP vagy HTTPS protokollokat használnak a kliens és a szerver webes folyamatai közötti kommunikációra. |

A PRTOKOLLOK EGYÜTTMŰKÖDÉSE

A számítógépes hálózaton keresztül küldött üzenet általában több protokoll használatát igényli, amelyek mindegyike saját funkciókkal és formátummal rendelkezik. Hálózati protokollok, amelyeket akkor használunk, amikor egy eszköz lekéri egy webszerver weboldalát:

* Hypertext Transfer Protocol (HTTP): ez a protokoll felelős a webszerver és a kliens kommunikációjáért. A http leírja a kliens és a szerver közötti kérések és válaszok formáját és tartalmát. A http-t mind a kliens, mind pedig a webszerver szoftvere használja. A http más prokollokra bízza, hogy az üzenetek szállítása hogyan történjen a kliens és a szerver között.
* Transmission Control Protocol (TCP): létrehozza az egyedi párbeszédeket. A TCP megbízható kézbesítést garantál, emelett adatfolyam-vezérlést is biztosít.
* Internet Protocol (IP) végzi az üzenetek továbbítását a küldőtől a címzettig. AZ IP segítségével továbbítják a routerek az üzeneteket több hálózaton keresztül is.
* Ethernet: ez a prokoll az azonos Ethernet LAN-on elhelyezkedő eszközök hálózati interfészei között továbbítja az üzenetet

3.4 SZABVÁNYÜGYI SZERVEZETEK

NYÍLT SZABVÁNYOK

Mivel számos gyártó készít hálózati berendezéseket, fontos, hogy ugyanazokat a szabványokat használják. A hálózati szabványokat nemzetközi szabványügyi szervezetek fejlesztik ki.

A nyílt szabványok elősegítik az együttműködést, a versenyt és az innovációt. Azt is garantálják, hogy egyetlen cég ne sajátíthassa ki a piacot, vagy szerezhessen tisztességtelen előnyt a versenyben.

A nyílt szabványok teszik lehetővé azt is, hogy egy Apple OS X operációs rendszert futtató kliens egy Linuxot futtató webszervertől kérjen le egy weboldalt. Ez azért lehetséges, mert mindkét operációs rendszer ugyanazokat a nyílt protokollokat valósítja meg, a TCP/IP protokollcsalád elemeit.

A szabványügyi szervezetek általában gyártófüggetlen, non-profit szervezetekként jönnek létre, hogy fejlesszék és támogassák a nyílt szabványok koncepcióját. Ezek a szervezetek fontosak az internet nyitottságának fenntartásában, szabadon hozzáférhető előírásokat és protokollokat készítenek, amelyeket minden gyártó alkalmazhat.

Egy szabványügyi szervezet magától is kidolgozhat egy szabályrendszert, vagy bizonyos esetekben kiválaszthat egy zárt protokollt is, ami majd az alapját képezheti a szabványnak. Ha egy gyártóspecifikus protokollt használ, ez általában annak a gyártónak a bevonásával történik, aki a protokollt megalkotta.

INTERNETES SZABVÁNYOK

A különböző szervezeteknek különböző felelőssége van az internet és a TCP/IP protokoll szabványainak előmozdítása és létrehozása terén. Ilyen szervezetek például, az ISOC, az IAB, az IETF és az IRTF.

A TCP/IP fejlesztésével és támogatásával foglalkozó szabványszervezetek az IANA és az ICANN.

ELEKTRONIKAI ÉS KOMMUNIKÁCIÓS SZABVÁNYOK

Más szabványügyi szervezetek az IP-csomagok vezetékes vagy vezeték nélküli közegen, elektromos jelként történő szállításához használt elektronikus és kommunikációs szabványok terjesztéséért és létrehozásáért felelnek. Ezek a szervezetek a következők:

* **Institute of Electrical and Electronics Engineers**(**IEEE**): elektronikai, elektrotechnikai szervezet, technológiai újításokat és új szabványokat dolgoznak ki nagyon széles körben az energiaellátástól, az egészségügyön át, a telekommunikációig és a hálózatokig. Fontos IEEE hálózati szabvány a 802.3 Ethernet és a 802.11 WLAN.
* **Electronic Industries Alliance (EIA):** a szervezet legismertebb szabványai a vezetékezéshez, csatlakozókhoz és a hálózati eszközök beszereléséhez használt 19 colos szekrényekhez kapcsolódnak.
* **Telecommunications Industry Association (TIA):** kommunikációs szabványokat fejlesztenek számos területen: rádióátvitel, mobil adótornyok, VoIP eszközök, műholdas kommunikáció.
* **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T**): az egyik legnagyobb és legrégebbi kommunikációs szabványügyi szervezet. Az ITU-T olyan területek számára ír elő szabványokat, mint a videótömörítés, az IPTV (Internet Protocol Television) és a szélessávú kommunikáció (pl.: DSL).

3.5. REFERENCIAMODELLEK

RÉTEGMODELLEK ELŐNYEI

A hálózat egyes műveleteit lebontjuk és kezelhetőbb rétegekbe rendezzük, ez lesz a rétegmodell. A rétegmodellnek számos előnye van a hálózati protokollok és műveletek leírása során:

* segít a protokollok tervezésében, mert egy adott rétegben működő protokoll esetén egyértelműen meghatározza, hogy mit kell tennie, és hogyan kapcsolódik az alatta és felette lévő rétegekhez,
* elősegíti a versenyt, mert a különböző gyártóktól származó termékek képesek lesznek együttműködni,
* megakadályozza, hogy az egyik réteg technológiájának vagy adottságainak változásai hatással legyenek az alatta és felette levő rétegekre,
* közös nyelvet biztosít a hálózat működésének és képességeinek leírásához,

Két rétegmodellt használunk a hálózati műveletek leírására:

* Open System Interconnection (OSI) referenciamodell
* TCP/IP referenciamodell

AZ OSI REFERENCIAMODELL

* az OSI-modell részletes listát ad valamennyi réteg funkcióiról és szolgáltatásairól. Ez a modell az egységességet biztosítja hálózati protokollok és szolgáltatások valamennyi típusán belül azzal, hogy leírja, mit kell tenni egy bizonyos rétegben, de nem írja elő, hogy miként kell azt megvalósítani,
* leírja továbbá a rétegek kölcsönhatását a közvetlenül alattuk és felettük lévő rétegekkel. Az ebben a tanfolyamban tárgyalt TCP/IP protokollok mind az OSI, mind a TCP/IP modellek köré szerveződnek.

|  |  |
| --- | --- |
| OSI-modell réteg | leírás |
| **7 Alkalmazási** | Az alkalmazási réteg folyamat-folyamat közti kommunikációhoz használt protokollokat tartalmaz. |
| **6 Megjelenítési** | A megjelenítési réteg az alkalmazási rétegbeli szolgáltatások közt átvitt adatok közös ábrázolását valósítja meg. |
| **5 Viszony** | A viszony réteg a megjelenítési réteg számára biztosít szolgáltatásokat párbeszédek megvalósításához és adatok cseréjéhez. |
| **4 Szállítási** | A szállítási réteg a végberendezések közti kommunikáció adatainak szegmentálását, szállítását és összeillesztésével kapcsolatos szolgáltatásokat nyújt |
| **3 Hálózati** | A hálózati réteg végberendezések közti egyedi adatelemek cseréjét megvalósító szolgáltatásokat biztosít. |
| **2 Adatkapcsolati** | Az adatkapcsolati réteg protokolljai adatkeretek továbbítását végzik egy közös közegen elhelyezkedő eszközök között. |
| **1 Fizikai** | A fizikai rétegbeli protokollok mechanikai, elektromos, funkcionális és folyamatbeli módszerekkel foglalkoznak, melyek hálózati eszközről induló vagy oda megérkező bitsorozatokat továbbító fizikai kapcsolatok aktiválás |

A TCP/IP modell rétegeire főleg a nevükkel hivatkozunk, az OSI-modell hét rétegét gyakrabban emlegetjük a számuk alapján. Például a fizikai réteget az OSI-modell első rétegének, az adatkapcsolatit a második rétegnek hívjuk, és így tovább.

TCP/IP PROKOLLMODELL

A TCP/IP protokollmodellt a hálózatközi kommunikációhoz hozták létre a 1970-es években, néha internetmodellnek is nevezik. Ez a modell szorosan illeszkedik egy bizonyos protokollkészlet szerkezetéhez. A TCP/IP azért protokollmodell, mivel a TCP/IP protokollkészletben lévő protokollok valamennyi rétegének funkcióit leírja. A TCP/IP referenciamodellként is használható.

|  |  |
| --- | --- |
| **TCP/IP modell réteg** | **leírás** |
| **4 - Alkalmazási** | Adatok megjelenítése a felhasználónak, ezen kívül kódolás és párbeszédek vezérlése. |
| **3 - Szállítási** | Különböző eszközök közötti kommunikáció különböző hálózatokon keresztül. |
| **2 - Internet** | Meghatározza a hálózaton keresztül a legjobb elérési utat. |
| **1 - Hálózatelérési** | A hálózatot alkotó hardvereszközök és közegek. |

A szabvány és a TCP/IP protokollok definícióját egy nyilvános fórum tárgyalja, és nyilvánosan elérhető RFC-kben vannak meghatározva. Az RFC-ket a hálózatépítő mérnökök alkotják, és megküldik más IETF-tagoknak észrevételek céljából.

**OSI ÉS A TCP/IP MODELL ÖSZEHASONLÍTÁSA**

A TCP/IP protokollkészlet protokolljai leírhatók az OSI-referenciamodellből kiindulva is. Az OSI-modellben a TCP/IP modell hálózatelérési és alkalmazási rétege további részekre van felosztva, hogy leírják a rétegekben előforduló különálló funkciókat.

A hálózatelérési rétegben a TCP/IP protokollkészlet nem határozza meg, hogy mely protokollokat kell használni egy fizikai közegen való továbbításkor, hanem csak azok átadását írja le az internet rétegből a fizikai hálózati protokollok felé. Az OSI 1. és 2. rétege tárgyalja a közeghozzáféréshez szükséges eljárásokat és a hálózaton keresztül történő adattovábbítás fizikai eszközeit.

A hálózatelérési rétegben a TCP/IP protokollkészlet nem határozza meg, hogy mely protokollokat kell használni egy fizikai közegen való továbbításkor, hanem csak azok átadását írja le az internet rétegből a fizikai hálózati protokollok felé. Az OSI 1. és 2. rétege tárgyalja a közeghozzáféréshez szükséges eljárásokat és a hálózaton keresztül történő adattovábbítás fizikai eszközeit.

A legfontosabb hasonlóságok a szállítási és hálózati rétegekben vannak, azonban a két modell különbözik abban, hogy miként viszonyulnak a felsőbb és alsóbb rétegekhez:

* az OSI 3. rétege, a hálózati réteg megfelel a TCP/IP internet rétegének. Ez a réteg olyan protokollokat ír le, amelyek címzéssel és az üzenetek hálózatok közti irányításával foglalkoznak,
* az OSI 4. rétege, a szállítási megfelel a TCP/IP szállítási rétegének. Ez a réteg általános szolgáltatásokat és funkciókat tartalmaz, amelyek sorrendhelyes és megbízható átvitelt tesznek lehetővé az adatforrástól a címzettig,
* TCP/IP alkalmazási rétege számos protokollt tartalmaz, ezek a felhasználói alkalmazások számos fajtájának nyújtanak specifikus szolgáltatásokat. Az OSI-modell 5., 6. és 7. rétegei az alkalmazások fejlesztőinek biztosítanak referenciát a hálózatokon kommunikáló alkalmazások tervezése során.
* a TCP/IP és az OSI-modellt egyaránt gyakran használjuk, amikor bizonyos rétegek protokolljaira szeretnénk hivatkozni. Mivel az OSI-modell elkülöníti az adatkapcsolati réteget a fizikaitól, ha ezekre a rétegekre szeretnénk hivatkozni, akkor általában ezt a modellt használjuk.

**6.1.2. IEEE 802 LAN/MAN adatkapcsolati alrétegek**

Az IEEE 802 szabványcsalád LAN/MAN szabványai az Ethernet LAN-okra, a vezeték nélküli LAN-okra (WLAN), a vezeték nélküli személyes hálózatokra (WPAN) és a helyi és nagyvárosi hálózatok egyéb típusaira vonatkoznak.

Az IEEE 802 LAN/MAN adatkapcsolati rétege a következő két alrétegből áll:

* **logikai kapcsolatvezérlés (Logical Link Control, LLC)**: ez az alréteg kommunikál a felsőbb rétegek hálózati szoftverei és az alsóbb rétegek hardverei között. Információkat helyez el a keretben annak a hálózati rétegbeli protokollnak az azonosítására, amelyik a keretet használni fogja. Ez az információ lehetővé teszi, hogy több 3. rétegbeli protokoll (pl. IPv4 és IPv6) is ugyanazt a hálózati interfészt és közeget használja.
* **közeghozzáférés vezérlés (Media Access Cotrol, MAC)**: ezt az alréteget (IEEE 802.3, 802.11 vagy 802.15) hardveres formában valósítják meg. Az adatbeágyazásért és a közeghozzáférés vezérlésért felelős. Az adatkapcsolati réteg címzését biztosítja, és a különböző fizikai rétegbeli technológiákkal építették egybe.

Az LLC-alréteg fogadja a hálózati protokoll adatait (ami jellemzően egy IPv4 vagy IPv6 csomag ) és olyan 2. rétegbeli vezérlő információkkal látja el, amelyek segítik a csomag célállomáshoz történő eljuttatását.

A MAC alréteg vezérli a hálózati kártyát és más hardvereket, amelyek a vezetékes vagy vezeték nélküli LAN/MAN közegen történő adatküldésért és fogadásért felelősek.

A MAC alréteg biztosítja az adatbeágyazást:

* **Kerethatárolás**: a keretezési folyamat fontos határolókat biztosít a kereten belüli mezők azonosításához. Ezek a határoló bitek biztosítják a szinkronizációt az adó és a vevő csomópontok között.
* **Címzés**: biztosítja a forrás- és célcímeket a 2. rétegbeli keret továbbításához a megosztott közeg eszközei között.
* **hibadetektálás**: tartalmaz egy keret lezáró részt, amelyet az átviteli hibák észlelésére használnak.

A MAC alréteg közeghozzáférés-vezérlést is biztosít, amely több eszköz számára is lehetővé teszi egy megosztott (fél-duplex) közegen keresztül történő kommunikációt. A teljes duplex kommunikáció nem igényel hozzáférés-vezérlést.

**6.1.3. Közeghozzáférés biztosítása**

A csomagok a helyi állomástól a távoli állomás felé tartó útjuk során számos, különböző tulajdonságokkal rendelkező hálózati környezettel találkozhatnak. Az Ethernet hálózat például az átviteli közeg használatáért versengő állomásokból áll. A MAC alréteg végzi ennek megvalósítását.

Soros kapcsolatok esetén a hozzáférési mód mindössze két eszköz (általában routerek) közötti közvetlen összeköttetésből áll. Ezért itt nincs szükség az IEEE 802 MAC alrétegben alkalmazott technikákra.

A router interfészei a megfelelő keretbe ágyazzák be a csomagot. Mindegyik összeköttetéshez a neki megfelelő közeghozzáférés-vezérlési módszer van használatban. A hálózati rétegbeli csomagok továbbítása során többször változhat az adatkapcsolati réteg és az átviteli közeg.

A router a következő 2. rétegbeli funkciókat hajtja végre minden egyes ugrásnál az útvonal mentén:

1. fogadja a keretet a közegtől,
2. kibontja a keretet,
3. a csomagot egy új keretbe ágyazza be.
4. továbbítja az új keretet a hálózati szegmens közegének megfelelő formában.

A router Ethernet interfésze egy LAN-hoz, a soros interfésze pedig egy WAN hálózathoz csatlakozik. A router a keretek feldolgozásakor az adatkapcsolati réteg szolgáltatásaira támaszkodik, amikor fogadja a keretet az egyik közegtől, kibontja a keretből a 3. rétegbeli adategységet, újra keretbe ágyazza azt, majd az új keretet a kimeneti vonal közegére helyezi.

**6.2.2 WAN TOPOLÓGIÁK**

* 1. pont-pont (Point to point): ez a legegyszerűbb és leggyakoribb WAN topológia. Két végpont közötti állandó kapcsolatból áll.
  2. csillagpont (Hub and Spoke): a csillag topológia WAN változata, amelyben egy központ pont-pont kapcsolatok használatával köti össze a telephelyeket. A telephelyek csak a központon keresztül cserélhetnek adatokat egymással.
  3. hálós (mesh): ez a topológiatípus nagyfokú rendelkezésre állást biztosít, viszont megköveteli, hogy minden végrendszer mindegyik másikkal össze legyen kapcsolva. Emiatt a fenntartási és kivitelezési költségek magasak lehetnek. Minden egyes kapcsolat egy pont-pont összeköttetést jelent valamely másik csomóponttal.

A hibrid topológiát ezen topológiák variációja vagy kombinációja alkotja. A részleges háló például egy hibrid topológia, amelyben néhány, de nem az összes végberendezés kapcsolódik egymáshoz.

**Pont-pont WAN topológia**

A fizikai pont-pont összeköttetések közvetlenül két végpontot kapcsolnak össze egymással. Ebben az elrendezésben a két végpontnak nem kell más állomásokkal megosztozniuk a közegen. Továbbá, soros kommunikációs protokoll, például pont-pont protokoll (Point-to-Point Protocol, PPP) használatakor az állomásnak nem kell eldöntenie, hogy a beérkező keretet neki vagy egy másik csomópontnak szánták. Emiatt a logikai adatkapcsolati protokollok nagyon egyszerű felépítésűek is lehetnek, hiszen a keretek csak a két állomás egyikének lehetnek címezve vagy csak tőlük származhatnak. A kereteket a pont-pont kapcsolat egyik végén az állomás ráhelyezi a közegre, majd a túlsó végén lévő másik állomás leveszi azokat.

Etherneten keresztül történő pont-pont kapcsolat használatakor az eszköznek meg kell határoznia, hogy a bejövő keretet neki címezték-e.

A forrás- és célállomás közvetve, nagy földrajzi távolságok áthidalásával kapcsolódik egymáshoz számos közvetítő eszköz használatával. A hálózatban használt fizikai eszközök nincsenek befolyással a logikai topológiára. Az ábrán új közvetítő fizikai kapcsolatok hozzáadása nem változtatja meg a logikai topológiát. A logikai pont-pont kapcsolat ugyanaz marad.

**LAN topológiák**

A többes hozzáférésű helyi hálózatokban a végberendezések (azaz csomópontok) csillag- vagy kiterjesztett csillag topológiákkal vannak összekapcsolva. Az ilyen típusú topológiában a végberendezések egy központi közvetítő eszközhöz csatlakoznak, ebben az esetben egy Ethernet switch-hez. Egy **kiterjesztett csillag** topológia több Ethernet switch összekapcsolásával bővíti ezt ki. A csillag és kiterjesztett csillag topológiák telepítése egyszerű, nagymértékben méretezhetők (könnyedén hozzáadhatunk és eltávolíthatunk végberendezéseket), valamint hibaelhárításuk is egyszerűen elvégezhető. A korai csillag topológiáknál a végberendezések Ethernet hub használatával kapcsolódtak egymáshoz.

Időnként előfordulhat, hogy csak két eszköz csatlakozik az Ethernet hálózaton. Például két egymással összekapcsolt router. Ez egy példa l az Etherneten használt pont-pont topológiára.

**Régi LAN topológiák**

A korai Ethernet és a régi vezérjeles gyűrű (Token Ring) LAN technológiák két másik topológia típust tartalmaztak:

* **Busz**: az állomások egymás után vannak láncolva és valamilyen formában a lánc mindkét vége le van zárva. A végberendezések összekapcsolásához nincs szükség (a kapcsolóhoz hasonló) hálózati eszközökre. Az Ethernet korábbi változataiban busz topológiát használtak koax kábellel, az alacsony ára és könnyű telepíthetősége miatt.
* **Gyűrű**: az állomások a megfelelő szomszédaikkal összeköttetésben állva alkotnak egy gyűrűt. A busz topológiával ellentétben a gyűrűt nem kell lezárni. A gyűrű topológiát az FDDI hálózatok korábbi változataiban és a vezérjeles gyűrűben használták.

**FÉL-ÉS TELJES DUPLEX KOMMUNIKÁCIÓ**

A LAN topológiák tekintetében fontos a duplex kommunikáció megértése, mivel az két eszköz közötti adatátvitel irányára utal. A duplex kommunikációnak két általános módja van.

**FÉLDUPLEX KOMMUNIKÁCIÓ**

Mindkét eszköz képes adatküldésre és -fogadásra a közegen, de nem egyidejűleg. A WLAN-ok és a korai Ethernet hubokkal rendelkező busztopológiák félduplex módot használnak. A félduplex mód egyszerre csak egy eszköz számára teszi lehetővé a küldést vagy a fogadást egy megosztott közegen.

**TELJES DUPLEX KOMMUNIKÁCIÓ**

Mindkét eszköz egyidejűleg képes adatküldésre és -fogadásra a megosztott közegen. Az adatkapcsolati réteg feltételezi, hogy a közeg bármikor elérhető mindkét állomás számára. Az Ethernet kapcsolók alapértelmezés szerint teljes duplex üzemmódban működnek, de félduplex módban is működhetnek, ha olyan eszközhöz csatlakoznak, mint például az Ethernet hub.

Összefoglalva, a félduplex kommunikáció egyszerre egy irányba korlátozza az adatküldést. A teljes duplex az adatok egyidejű küldését és fogadását teszi lehetővé. Fontos, hogy két összekapcsolt interfész, például egy állomás hálózati kártyája és egy switch Ethernet interfésze ugyanazt a duplex módot használja. Ellenkező esetben eltérés lesz a duplexitásban, ami teljesítménycsökkenést és késleltetést eredményez a kapcsolaton.

**6.3.1 ADATKAPCSOLATI KERET**

A kerethez csatolt információkat a használt protokoll határozza meg. Az adatkapcsolati réteg egy fejléccel és utótaggal ellátott keretbe ágyazza be az adatot (általában IPv4 vagy IPv6-csomagot), ezzel készíti elő azt a közegen való továbbításra.

Az adatkapcsolati protokoll felelős az ugyanazon hálózaton belül található hálózati kártyák egymás közti kommunikációjáért. Annak ellenére, hogy számos különböző adatkapcsolati protokoll létezik az adatkapcsolati keretek leírására, mindegyik kerettípus három fő részből áll:

* fejléc,
* adatrész,
* utótag.

A többi beágyazást végző protokolltól eltérően az adatkapcsolati réteg a keret végéhez is csatol információkat egy utótag formájában.

Az adatkapcsolati rétegben található protokollok mindegyike a keret adat mezőjébe ágyazza be a felsőbb rétegbeli adatokat. A keret felépítése, valamint a fejlécben és az utótagban található mezők viszont protokollonként eltérőek lehetnek.

Olyan keretszerkezet nem létezik, amely mindenféle átviteli közegre kielégítené az összes adattovábbítási igényt. A keretben lévő vezérlési információk mennyisége a környezettől függően változik, amiatt, hogy megfeleljen a közeg és a logikai topológia hozzáférési követelményeinek. A WLAN keretnek például tartalmaznia kell az ütközések elkerülésére szolgáló eljárásokat, ezért további vezérlési információkat igényel az Ethernet kerethez képest.

Érzékeny környezetben több ellenőrzésre van szükség a kézbesítés biztosításához. A fejléc és utótag mezők nagyobb méretűek, mivel több ellenőrzési információra van szükség.

A KERET MEZŐI

A keretezéssel olyan csoportokra bontjuk a bitfolyamot, amelyeknek fejlécében és utótagjában megtalálható vezérlőinformációk különböző adatmezők értékeiként jelennek meg. Ez a formátum egy olyan szerkezetet ad a jelsorozatnak, amelyet a fogadó állomás felismer és képes belőle visszaalakítani az adatcsomagokat.

Nem minden protokoll tartalmazza ezen mezők mindegyikét. Az adatkapcsolati protokollok szabványai határozzák meg a tényleges keretformátumot.

A keret mezői a következőket tartalmazzák:

* **keretkezdet és vége jelzők**: keret kezdetének és végének azonosítására szolgál,
* **címzés**: a közegen található forrás- és célállomásokat jelzi,
* **típus**: a 3. rétegbeli protokollt azonosítja az adatmezőben,
* **vezérlés**: speciális adatfolyam szolgáltatásokat azonosít, mint például a szolgáltatásminőség (QoS). A QoS bizonyos típusú üzenetek számára elsőbbséget biztosít a továbbítás során. Például az IP alapú hangtovábbítás (VoIP) keretei általában elsőbbséget élveznek, mert érzékenyek a késleltetésre,
* **adat**: a keret adatrészét tartalmazza (azaz a csomag fejrészt, a szegmens fejrészt és az adatot)
* **hibaellenőrzés**: az adatrész után található, az utótagot alkotja.

Az adatkapcsolati protokoll minden keret végéhez egy utótagot ad hozzá. A hibakeresésnek nevezett folyamat során az utótag határozza meg, hogy a keret hibamentesen érkezett-e meg. A keretet alkotó bitek logikai vagy matematikai összegzését helyezi el az utótagba. Azért az adatkapcsolati rétegben történik a hibadetektálás, mert a közegen továbbított jelek interferencia, torzítás vagy veszteség következtében jelentős mértékben megváltoztathatják az általuk ábrázolt bitek értékét.

A továbbítást végző csomópontok készítik el a keret tartalmának logikai összegzését, amelyet ciklikus redundancia-ellenőrzésnek (Cyclic redundancy check, CRC) hívunk. A kiszámított értéket a keretellenőrző összeg (Frame Check Sequence, FCS) mezőbe helyezik, hogy a keret tartalmát képviselje. Az Ethernet utótagban az FCS egy módszert biztosít a fogadó csomópont számára a keret átviteli hibáinak megállapítására.

**7.1. ETHERNET KERETEK**

ETHERNET BEÁGYAZÁS

Az Ethernet a manapság használt két LAN-technológia egyike, a másik a vezeték nélküli LAN (WLAN). Az Ethernet vezetékes kommunikációt használ, csavart érpárat, száloptikai kapcsolatokat és koaxiális kábeleket.

Az Ethernet az OSI-modell két rétegében működik: az adatkapcsolati és a fizikai rétegben. Hálózati technológiák egész családját jelenti, amelyeket az IEEE 802.2 és 802.3 szabványok határoznak meg. Az Ethernet a következő sávszélességeket támogatja:

* 10 Mbit/s,
* 100 Mbit/s,
* 1000 Mbit/s (1 Gbit/s),
* 10 000 Mbit/s (10 Gbit/s),
* 40 000 Mbit/s (40 Gbit/s),
* 100 000 Mbit/s (100 Gbit/s).

Az Ethernet szabványok meghatározzák mind a 2. rétegbeli protokollokat, mind pedig az 1. rétegbeli technológiákat

AZ ADATKAPCSOLATI RÉTEG ALRÉTEGEI

Az IEEE 802 LAN/MAN protokollok, beleértve az Ethernetet is, az adatkapcsolati réteg két különálló alrétegét használják a működéshez. Ezek a logikai kapcsolatvezérlési (LLC) és a közeghozzáférés-vezérlési (MAC) alrétegek.

Az LLC és a MAC a következő szerepekkel rendelkezik az adatkapcsolati rétegben:

* **LLC alréteg**: ez az IEEE 802.2 alréteg biztosítja a kommunikációt a felső rétegek hálózati szoftverei és az alsó rétegek eszközhardverei között. Információkat helyez el a keretben annak a hálózati rétegbeli protokollnak az azonosítására, amelyik a keretet használni fogja. Ez az információ lehetővé teszi, hogy több 3. rétegbeli protokoll (pl. IPv4 és IPv6) is ugyanazt a hálózati interfészt és közeget használja,
* **MAC-alréteg**: ez az alréteg (például IEEE 802.3, 802.11 vagy 802.15) a hardverben valósul meg, és felelős az adatbeágyazásért és a közeghozzáférés-vezérléséért. Biztosítja az adatkapcsolati réteg címzését, és együttműködik a különböző fizikai rétegbeli technológiákkal.

MAC ALRÉTEG: a MAC-alréteg felelős az adatbeágyazásért és a közeghez való hozzáférésért.

**Adatbeágyazás**

Az IEEE 802.3 adatbeágyazás a következőket tartalmazza:

* **Ethernet keret**: az Ethernet keret belső szerkezete,
* **Ethernet címzés**: az Ethernet keret forrás- és cél MAC-címet is tartalmaz, hogy a keretet az egyik Ethernet hálózati kártyától egy másik Ethernet hálózati kártyához ugyanazon a LAN-on keresztül továbbítsa.
* **Ethernet hibajelzés**: az Ethernet keret tartalmaz egy hibaészleléshez használt keret-ellenőrző bitsorozat utótagot (Frame Check Sequence, FCS).

**Közeghozzáférés**

Az IEEE 802.3 MAC-alréteg tartalmazza az Ethernet kommunikációs szabványok specifikációit a különböző típusú adathordozókhoz, beleértve a réz és üvegszál alapú közegeket is

A korai Ethernet busz topológiát vagy hub-okat használt, és megosztott, fél-duplex közegen működött. Az Ethernet a fél-duplex közegen egy ütközés-alapú hozzáférési módszert használ, a vivőjel érzékeléses többszörös hozzáférésű ütközésérzékelést (CSMA/CD). Ez biztosítja, hogy egyszerre csak egy eszköz továbbítson adatot. A CSMA/CD lehetővé teszi, hogy több eszköz ugyanazon a fél-duplex közegen osztozzon, és észlelje az ütközést, amikor egynél több eszköz egyszerre próbál kommunkálni. Ezenkívül egy visszalépéses algoritmust is biztosít az újraküldéshez. A mai Ethernet LAN-ok olyan switch-eket használnak, amelyek teljes duplex módban működnek. Az Ethernet switch-ekkel megvalósított teljes duplex kommunikáció nem igényel CSMA/CD hozzáférés-vezérlést.

AZ ETHERNET KERETEK MEZŐI

Az Ethernet keret mérete minimum 64 bájt, maximum 1518 bájt. Ez magában foglalja az összes bájtot a cél MAC-cím mezőtől kezdve a keret ellenőrző összeg mezőig (Frame Check Sequence, FCS). Az előtag és a keretkezdő mezőket nem vesszük figyelembe, amikor megadjuk a keret méretét.

Minden keretet, ami kevesebb, mint 64 bájt hosszúságú, ütközési töredéknek (runt) nevezünk. Ezeket a fogadó állomás automatikusan eldobja. A több mint 1500 bájt adattal rendelkező kereteket „jumbo” vagy „óriás" kereteknek hívjuk.

Ha egy átvitt keret mérete kisebb, mint a minimális vagy nagyobb, mint a maximális érték, a fogadó készülék eldobja azt. Az eldobott keretek valószínűleg ütközések vagy más, nem kívánt jelenségek eredményei, ezért érvénytelennek minősülnek. A jumbo kereteket azonban a legtöbb Fast Ethernet és Gigabit Ethernet switch és hálózati kártya támogatja.

|  |  |
| --- | --- |
| **mező** | **leírás** |
| Előtag és keretkezdő mezők | Az előtag (Preamble, 7 bájt) és a keretkezdő (Start Frame Delimiter, SFD, 1 bájt) mezők szinkronizálásra szolgálnak a küldő és fogadó készülékek között. A keretnek ezt az első nyolc bájtját használják arra, hogy a fogadó csomópont figyelmét felhívják a keret érkezésére. Lényegében az első néhány bájt azt mondja a vevőnek, hogy álljon készen az új keret fogadására. |
| Cél MAC-cím mező | Ez a 6 bájtos mező azonosítja a címzettet. Ezt a címet használja a második réteg, hogy segítse az eszközöket a nekik szóló keretek meghatározásában. A keretben lévő címet a készülék összehasonlítja a saját MAC-címével. Ha egyezés van, az eszköz elfogadja a keretet. Lehet unicast, multicast vagy broadcast cím is, |
| Forrás MAC-cím mező | Ez a 6 bájtos mező a keretet küldő hálózati kártyát vagy interfészt azonosítja. |
| Típus/Hossz mező | Ez a 2 bájtos mező azonosítja az Ethernet keretbe ágyazott felsőbb rétegbeli protokollt. Gyakori hexadecimális értékek: 0x800 (IPv4), 0x86DD (IPv6) és 0x806 (ARP).: Ezzel a mezővel EtherType néven is találkozhatunk. |
| Adat mező | Ez a mező (46-1500 bájt) tartalmazza a magasabb rétegbeli beágyazott adatokat, amely egy általános 3. rétegbeli PDU, például egy IPv4-csomag. Minden keretnek legalább 64 bájt hosszúnak kell lennie. Ha egy kis csomagot ágyaznak be, akkor további biteket, úgynevezett kitöltést (pad) használnak, hogy megnöveljék a keret méretét a minimális méretre. |
| Keretellenőrző mező | A keretellenőrző (Frame Check Sequence, FCS) mezőt (4 bájt) a hibák észlelésére használják a keretben. Ez a ciklikus redundancia-ellenőrzést (CRC) használja. A küldő készülék beleteszi a CRC-számítás eredményét a keret FCS-mezőbe. A fogadó készülék megkapja a keretet, és szintén kiszámít egy CRC-t a hibakereséséhez. Ha a számítások megegyeznek, nem történt hiba. Ha a számított értékek nem egyeznek, az azt jelzi, hogy az adat megváltozott, ezért a keretet el kell dobni. Az értékben bekövetkezett változás annak a következménye lehet, hogy a biteket leíró elektromos jelekben zavar keletkezett. |

**7.2. ETHERNET MAC-címek**

A hálózatkezelésben a bináris IPv4-címeket a tízes számrendszer segítségével ábrázolják. Az IPv6-címek és az Ethernet-címek a hexadecimális alapú, vagyis tizenhatos számrendszerbeli értékként jelennek meg. A hexadecimális rendszer a 0-9 számokat és az A-tól F-ig terjedő betűket használja.

Az Ethernet MAC-cím 48 bit bináris értékből áll. Az Ethernet-cím hexadecimális számjegyei egyenként négy bitet jelölnek. Ezért a 48 bites Ethernet MAC-cím mindössze 12 hexadecimális számjeggyel kifejezhető.

Mivel 8 bit alkot egy bináris csoportot (vagy bájtot), a bináris 00000000-11111111 közti értékeket a hexadecimális 00-tól FF-ig terjedő tartománnyal lehet kifejezni.

Hexadecimális ábrázolást használva a vezető nullákat is mindig megjelenítjük a teljes 8 bites kiírásnál. Például a 0000 1010 bináris értéket hexadecimális 0A-ként írjuk le.

A hexadecimális számokat gyakran a **0x** (pl. 0x73) előzi meg, hogy megkülönböztessék a decimális és hexadecimális értékeket a dokumentációban.

A hexadecimális értéket képviselheti egy alsó indexbeli 16-os, vagy a hexadecimális számot követő H betű is (pl. 73H).

Előfordulhat, hogy decimális és hexadecimális értékek között kell konvertálnunk. Ha ilyen átalakítások szükségesek, általában könnyebb a decimális vagy hexadecimális értéket binárissá átalakítani, majd azután a bináris értéket konvertálni át decimális vagy hexadecimális értékké.

Egy Ethernet LAN-ban minden hálózati eszköz ugyanahhoz a megosztott közeghez csatlakozik. A MAC-cím a helyi hálózati szegmens forrás- és céleszközeinek (hálózati kártya, NIC) fizikai azonosítására szolgál. A MAC-címzés az OSI-modell adatkapcsolati rétegében biztosítja az eszközök megkülönböztethetőségét.

Az Ethernet MAC-cím egy 48 bites érték, amelyet 12 hexadecimális számjegy használatával írunk le. Mivel egy bájt 8 bitnek felel meg, azt is mondhatjuk, hogy a MAC-cím 6 bájt hosszúságú.

Minden MAC-címnek egyedinek kell lennie az Ethernet eszközre vagy az Ethernet interfészre nézve. Ennek biztosítása érdekében minden, Ethernet-eszközt értékesítő gyártónak regisztrálnia kell az IEEE-nél, hogy kapjon egy egyedi, 6 hexadecimális jegyből álló (azaz 24 bites vagy 3 bájtos) kódot, amelyet egyedi szervezetazonosítónak (Organizatonally Unique Identifier, OUI) neveznek.

Amikor egy gyártó MAC-címet rendel egy eszközhöz vagy Ethernet interfészhez, a következőket kell tennie:

* a kapott OUI-t használja az első 6 hexadecimális számjegyként,
* egyedi értéket ad az utolsó 6 hexadecimális számjegyhez.

Ezért az Ethernet MAC-cím egy 6 jegyű, hexadecimális gyártói OUI-kóddal kezdődik, amelyet egy 6 hexadecimális jegyből álló, gyártó által generált érték követ.

Például, a Ciscónak egyedi MAC-címet kell hozzárendelnie egy új eszközhöz. Az IEEE által a Cisco-hoz rendelt egyik OUI a**00-60-2F**. A Cisco ezután konfigurálhatja a készüléket egy egyedi gyártói kóddal, mint például **3A-07-BC.** Ezért az eszköz Ethernet MAC-címe 00-60-2F-3A-07-BC lesz. **00-60-2F-3A-07-BC.**

A gyártó felelőssége annak biztosítása, hogy egyik eszköze sem kapja ugyanazt a MAC-címet. Lehetséges azonban, hogy azonos MAC-címek keletkeznek a gyártás során elkövetett hibák, a virtuális gépek megvalósítási módszereiben rejlő algoritmusok vagy valamely szoftvereszköz egyikével végrehajtott módosítások miatt. Mindegyik esetben a MAC-címet módosítani kell szoftver segítségével vagy egy új NIC beépítésével.

A KERET FELDOLGOZÁSA

A MAC-címet gyakran nevezik beégetett címnek (Burned-In Addresss, BIA), mert régen ezt a címet fixen beprogramozták a hálózati kártya ROM-jába). Ez azt jelenti, hogy a cím véglegesen bele lett kódolva a ROM-chipbe - nem lehetett szoftveresen megváltoztatni.

A modern operációs rendszerek és a hálózati kártyák esetén szoftveresen is meg lehet változtatni a MAC-címet. Ez akkor hasznos, ha olyan hálózathoz próbálunk hozzáférni, amely a BIA alapján szűr. Következésképpen a forgalom MAC-cím alapján történő szűrése vagy ellenőrzése már nem olyan biztonságos.

A számítógép elindulásánál a NIC első teendője, hogy bemásolja a MAC-címet a ROM-ból a RAM-ba. Amikor egy eszköz üzenetet továbbít egy Ethernet hálózatra, az Ethernet fejléc a következőket tartalmazza:

* **forrás MAC-cím**: ez a forrás állomás hálózati kártyájának MAC-címe,
* **cél MAC-cím**: ez a céleszköz hálózati kártyájának MAC-címe.

Amikor egy hálózati kártya Ethernet keretet kap, összehasonlítja a benne levő cél MAC-címet a RAM-ban tárolt fizikai MAC-címmel. Ha nincs egyezés, akkor a készülék eldobja a keretet. Ha egyezik, akkor átadja a keretet a felsőbb OSI-rétegeknek, ahol a kibontási folyamat megtörténik.

Az Ethernet hálózati kártya akkor is elfogadja a kereteket, ha a cél MAC-cím szórásos vagy olyan csoportos címzésű, amelynek az állomás tagja.

Minden eszköz, amely a forrása vagy célja egy Ethernet keretnek, rendelkezik egy Ethernet hálózati kártyával, és ezért egy MAC-címmel is. Ide tartoznak a munkaállomások, a kiszolgálók, a nyomtatók, a mobileszközök és a routerek.

EGYEDI CÍMZÉSŰ MAC-CÍM

Az Etherneten belül különböző MAC-címeket használunk az egyedi címzésű, a szórásos és a csoportos kommunikációra.

1. Egyedi címzésű (unicast) MAC-címet használunk, amikor egy keretet egyetlen cél eszközre küldünk.

A példában a 192.168.1.5 (forrás) IP-című állomás lekér egy weboldalt a 192.168.1.200 IP-című szervertől. Ahhoz, hogy egyedi címzésű csomagot küldhessünk és fogadhassunk, a cél IP-címnek szerepelnie kell az IP-csomag fejlécében. A megfelelő cél MAC-címnek szintén benne kell lennie az Ethernet keret fejlécében. Az IP-cím és a MAC-cím együttesen kézbesíti az adatokat egy adott célállomáshoz.

Az a folyamat, amelyet a forrásállomás használ az IPv4-címhez társított cél MAC-cím meghatározásához, az úgynevezett címfeloldási protokoll (ARP). Az a folyamat, amelyet a forrásállomás használ az IPv6-címhez társított cél MAC-cím meghatározásához, a szomszédfelderítés (Neighbor Discovery, ND). A forrás MAC-címnek mindig egyedi címzésűnek kell lennie.

1. Szórásos MAC-cím: az Ethernet LAN minden eszköze megkapja és feldolgozza az Ethernet szórásos kereteket (broadcast).

Az Ethernet szórás jellemzői a következők:

* a cél MAC-cím FF-FF-FF-FF-FF-FF-FF-FF hexadecimálisan (48 darab egyes binárisan),
* kiküldésre kerül az összes Ethernet switchporton, kivéve a bejövő portot (elárasztás).
* a routerek nem továbbítják ezt a forgalmat.

Ha a beágyazott adat egy IPv4 szórásos csomag, akkor a csomag célcímként egy olyan IP-címet tartalmaz, amiben csupa 1-es áll az állomásazonosító részben. Ennek következtében a helyi hálózat összes gépe (a szórási tartomány) fogadja és feldolgozza a csomagot.

A forrásállomás IPv4 szórási csomagot küld a hálózat összes eszközének. Az IPv4-célcím egy szórási cím: 192.168.1.255. Amikor az IPv4 szórásos csomag az Ethernet keretbe van ágyazva, a cél MAC-cím az FF-FF-FF-FF-FF-FF hexadecimális (48 bináris egyes) szórási cím.

Az IPv4 DHCP példa egy olyan protokollra, amely Ethernet- és IPv4-szórási címeket használ.

Azonban nem minden Ethernet szórás hordoz IPv4 szórásos csomagot. Az ARP-kérések például nem használnak IPv4-et, de az ARP-üzenetet Ethernet-szórásként küldik el.

1. Csoportos címzésű MAC-cím: az Ethernet csoportos címzésű kereteket (multicast) a LAN azon eszközcsoportjai fogadják és dolgozzák fel, amelyek ugyanahhoz a csoporthoz tartoznak. Az Ethernet csoportos küldés jellemzői a következők:

* a cél MAC-cím 01-00-5E, ha a beágyazott adat egy IPv4 csoportos küldésű csomag, illetve 33-33, ha a beágyazott adat IPv6 csoportos küldésű csomag.
* vannak más fenntartott csoportos címzésű cél MAC-címek is, amikor a beágyazott adat nem IP, hanem például STP (Spanning Tree Protocol) vagy LLDP (Link Layer Discovery Protocol),
* a bejövő port kivételével az összes Ethernet switchporton kiküldésre kerül (kivéve, ha a switch multicast snooping-ra van konfigurálva)
* a router nem továbbítja (kivéve, ha csoportos címzésű csomagokat is továbbít).

Ha a beágyazott adat egy IP multicast csomag, akkor a csoporthoz tartozó eszközöknek csoportos IP-címe van. Az IPv4 multicast címek tartománya 224.0.0.0 - 239.255.255.255. Az IPv6 csoportos címzésű címek tartománya ff00።/8. Mivel egy multicast cím a címek egy csoportját jelenti (néha állomás-csoportnak is hívják), csak csomagok célcímeként használható. A forrásnak mindig egyedi címe van.

Ugyanúgy, mint az egyedi vagy szórási címek esetében, a csoportos címekhez is szükség van egy megfelelő csoportos MAC-címre, hogy kézbesíteni lehessen a kereteket a helyi hálózaton. A csoportos címzésű MAC-cím az IPv4 vagy IPv6 csoportos küldési címhez van társítva.

Az útválasztási és más hálózati protokollok csoportos címzést használnak. A videó- és képkezelő szoftverek is alkalmazhatnak multicast címzést, bár ezek nem túl gyakoriak.

7.3.1 A KAPCSOLÁS ALAPJAI

Hogyan használja egy switch ezeket a címeket a keretek továbbítására (vagy eldobására) a hálózat más eszközei felé. Ha egy switch továbbítana minden megkapott keretet az összes portjára, akkor hálózati torlódás keletkezne, és valószínűleg teljes leállás következne be.

Egy 2. rétegbeli Ethernet switch a 2. rétegbeli MAC-címeket használja a továbbítási döntések meghozatalához. Nem foglalkozik a keret adatrészével (protokoll), például az IPv4-csomagokkal, ARP-üzenetekkel vagy IPv6 ND-csomagokkal. A switch a továbbítási döntéseket kizárólag a 2. rétegbeli Ethernet MAC-címek alapján hozza meg.

Minden egyes keret esetén megvizsgálja a MAC-címtáblát, hogy továbbítási döntést hozzon, ellentétben az Ethernet hubokkal, amelyek a bejövő port kivételével az összes portra kiküldik a biteket. Switch bekapcsoláskor a MAC-címtábla még üres, mert a switch még nem tanulta meg a csatlakoztatott számítógép MAC-címét.

A MAC-címtáblát gyakran nevezik CAM-táblázatnak is (Content Addressable Memory, tartalom szerint címezhető memória).

A SWITCH TANULÁSI ÉS TOVÁBBÍTÁSI FOLYAMATAI

A switch a bejövő keretek forrás MAC-címét megvizsgálva dinamikusan építi fel a MAC-címtáblát. A kereteket úgy továbbítja, hogy egyezést keres a keretben lévő cél MAC-cím és a MAC-címtábla bejegyzései között.

1. A FORRÁS MAC-CÍM VIZSGÁLATA

Minden beérkező keret ellenőrzésre kerül, hogy van-e benne új információ a switch számára. A switch megvizsgálja a keret forrás MAC-címét és a port számát, ahol a keret belépett. Ha a forrás MAC-cím nincs benne a táblázatban, akkor a bejövő portszámmal együtt hozzáadásra kerül. Ha a forrás MAC-címe létezik, a switch frissíti az adott bejegyzéshez tartozó időzítőt. Alapértelmezés szerint a legtöbb Ethernet switch 5 percig tart meg egy bejegyzést a táblázatban.

Ha a forrás MAC-cím létezik a táblázatban, de egy másik porton, a switch ezt új bejegyzésként kezeli. A bejegyzést ugyanazzal a MAC-címmel, de az aktuális portszámmal helyettesíti.

1. A CÉL MAC-CÍM MEGTALÁLÁSA

Ha a cél MAC-cím egy unicast cím, a switch egyezést keres a keret cél-MAC-címe és a MAC-címtábla egy bejegyzése között. Ha a cél MAC-cím szerepel a táblázatban, akkor továbbítja a keretet a megadott portra. Ha a cél MAC-cím nem szerepel a táblázatban, a switch a keretet az összes portján keresztül kiküldi, kivéve azt a portot, amelyen az beérkezett. Ezt nevezik ismeretlen unicast-nek vagy elárasztásnak.

Ha a cél MAC-cím szórásos vagy csoportos, a keretet kiküldi az összes portra, kivéve a bejövő portot.

**11. fejezet IPv4-címzés (forrás:ppt)**

**IPv4**

* 32 bites cím, egyesekből és nullákból álló sorozat
* IPv4-es címeket pontozott decimális formátumban használjuk
  + minden bájt (oktet) 0 és 255 közötti lehet
  + egy IPv4 cím 4 bájt (4 oktet) = 32 bit

11000000.10101000.00100010.00011001

192.168.34.25

**alhálózati maszk**

* egy IP cím két részből áll, hálózatot azonosító rész és állomást azonosító rész
* elkülönítése binárisan történik, a 32 bit első része adja a hálózatot azonosító részt (egyesek), a második része az állomást azonosító részt (nullák)

|  |  |  |  |
| --- | --- | --- | --- |
| 192 | 168 | 10 | **10** |
| 255 | 255 | 255 | 0 |
| 11111111 | 11111111 | 11111111 | **00000000** |

**hálózati előtag (prefix):**

* prefix az alhálózati maszk megadásának másik formája
* az alhálózati maszk egyeseinek a száma
* Megadása:/[egyesek száma]   
   /8 /16 /24

255.255.0.0 = /16

11111111.11111111.00000000.00000000

**hálózatcím:**

* hálózatcím: a hálózatra való hivatkozás, az IPv4-es hálózaton az első cím
* megadásának módja: cím + alhálózati maszk vagy cím + prefix
* nem lehet állomás IP-je.

192.168.20.0 255.255.255.0

192.168.20.0 /24

**állomáscím:**

* állomáscím: a végberendezéseket azonosító cím. A hálózati cím és a szórásicím (broadcast cím) között lévő címek.

Hálózatcím:192.168.20.0 /24  
Broadcast cím: 192.168.20.255  
Első host: 192.168.20.1  
Utolsó host: 192.168.20.254

10.0.0.0 /8

172.16.0.0 /16

**szórási cím:**

* szórási cím: egy speciális címe az alhálózatoknak, amelynek segítségével minden állomással egyszerre kommunikálhatunk.
* Hálózat utolsó címe.

192.168.20.0 /24

192.168.20.255

**IPv4 címek osztályai:**

* A, B, C, D és E osztályokra osztja az IPv4 címeket
* A, B, C kiosztható (kivételeitől eltekintve)
* D = multicast osztály
* E = kisérleti osztály

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Osztályok | Kezdete | Vége | Alapértelmezett  alhálózati maszk | Prefix |
| A | 0.0.0.0 | 127.255.255.255 | 255.0.0.0 | /8 |
| B | 128.0.0.0 | 191.255.255.255 | 255.255.0.0 | /16 |
| C | 192.0.0.0 | 223.255.255.255 | 255.255.255.0 | /24 |
| D | 224.0.0.0 | 239.255.255.255 | Nem definiált | /4 |
| E | 224.0.0.0 | 239.255.255.255 | Nem definiált | /4 |

**speciális használatú címek**

* **alapértelmezett útvonal címe** (default route)  
  ha semmilyen más útvonal nem megfelelő, ezt alkalmazzuk.  
  0.0.0.0 /8
* **visszacsatolási cím** (loopback)  
  olyan cím, amelyet a hostok használnak, hogy a forgalmat visszairányítsák saját maguknak

127.0.0.0 /8 hálózati cím

Loopback cím: 127.0.0.1

* **Link-local cím** (Adatkapcsolati szinten helyi címek)  
  ezeket a címeket az operációs rendszer automatikusan a helyi géphez rendeli akkor, amikor nincs beállított vagy elérhető IP konfiguráció.

abban az esetben is használatos, ha nincs elérhető DHCP.

169.254.0.0 /16

* **Test-net cím:** oktatási és tanulási célokra fenntartott.  
  192.0.2.0 /24
* **Multicast cím:** teljes D osztály
* **Kisérleti cím:** teljes E osztály

**Publikus és privát címek**

* Publikus címek: internetre kötött hálózatokban használt címek. A teljes A, B és C osztály (kivételek és privát címek nélkül)
* Privát címek: az internethozzáférés nélküli vagy korlátozott hozzáférésű hálózatokban használt címek.(LAN és SOHO)

**privát címtartományok**

* 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
* 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
* 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

**16. HÁLÓZATBIZTONSÁG (forrás jegyzet)**

BAHATOLÁS CÉLJA:

1. információlopás pl. bankszámladatok megszerzése, facebook jelszavak, e-mail címek
2. adatvesztés és manipuláció pl. adatbázis manupulálása, adatok törlése
3. azonosító lopás: felhasználónév, jelszó megszerzése, bankkártya-adatok ellopása
4. szolgáltatás megszakítása: annyi kérést küld a szerver felé, hogy nem tudja kiszolgálni a felhasználokat, pl. DoS-olás, vonalat is le lehet terhelni, amivel a servert éred el

SEBEZHETŐSÉGI TÍPUSOK (milyen gyenge pontok vannak)

* technológiai: harward,softvert,hálózatot,OP rendszert
* konfigurációs biztonsági részek:

1. rendszergazda hagyott benne hibát pl. nem biztonságos felhasználói fiók,
2. nem http-protokollal van védve, nincs titkosítva,
3. rosszul konfigurált internetes szolgáltatások,
4. nem biztonságos alapértelmezett beállítások,
5. rosszul konfigurált hálózati berendezések: jelszavazási hiba történt, port bekapcsolva maradt, MAC-cím szűrés

* házirend biztonsági rései: melyik mappába melyik felhasználó mit csinálhat

1. írásbeli biztonsági szabályzat hiánya: hány karakteres jelszó
2. politika
3. hitelesítés szabályozásának hiánya: erős jelszó legyen, fél évente új
4. hozzáférés-vezérlés nem kielégítő: naplózás kell, hogy jogosult volt-e, vagy sem, inkognító ablak
5. szoftver és hardvertelepítés és a módosítások nem követik a házirendet
6. nincs katasztrófa utána helyreállítási terv: biztonsági mentés

FIZIKAI BIZTONSÁG:

* hardver fenyegetések: szétverik a gépet,
* környezeti fenyegetés: szélsőséges hőmérséklet, páratartalom,
* elektromos veszélyek: alacsony feszültség,
* karbantartási veszélyek: hibás kábelezés.

HÁLÓZATI TÁMADÁSOK

KÁRTEVŐ TÍPUSOK: ezek program kódok

1. VÍRUS: kell neki egy gazdatest, vagyis számítógépes környezet (program vagy állomány)  
   vírustámadás az emberi hanyagság miatt következik be, a közvetítő az ember lesz (e-mail melléklet malware)

terjedéséhez beilleszti saját másolatát egy másik programba, és így annak szerves része lesz

ez nem önálló fájl, beépül valahova

1. FÉREG: hálózatnak, illetve a számítógépnek a kiskapuit keresi és úgy jut be, hálózati résekből, hálózati réseken át terjed el (másolatot készít saját magáról). Nem kell programhoz kapcsolódnia, hogy belépjen egy számítógépbe. Fertőzés esetén mindenképpen a gépeket kell leválasztani a hálózatról (azonosítókat is lop).
2. TRÓJAI: van egy program, ami valaminek látszik, de ő egy rosszindulatú program (toolbar, játékok) ahova bejut meg akarja szerezni a címlistákat, mindenképpen tovább akarja küldeni magát (sms, email).

cél, hogy megtalálják a rendszer gyenge pontját

1. **felderítéses támadások**

* internetes lekérdezések: hálózati domain megkeresése
* ping pásztázás: melyik IP cím aktív, mik vannak kiosztva
* port pásztázás: innen már ki tudja találni a hecker, hogy melyik a szerver

1. **hozzáférési támadások**: lop vagy manipulál adatot

* jelszó elleni támadás

1. nyers erő támadás (5ször próbálkozás a jelszóval)
2. trójai támadás: a trójai gyűjthet adatokat is
3. protokollelemző alkalmazások

* bizalom kihasználás: nincs a B hálózat lejelszavazva, és be tud jutni az A-ba is a hacher
* port irányítás: SSH-támadás, bármilyen szolgáltatás egy másik portra van irányítva, abba a hálózatba ellehetetleníti a szolgáltatást (összekeveri a portokat)
* közbeékelődés: a felhasználó weboldalt kér, de a támadó számítógépre irányul (más lesz a domain) – megtévesztő weboldalak

1. **szolgáltatásmegtagadási támadások**: szerver túlterhelés

* DoS: túl sok pingeléssel leterheli a szervert
* DDoS: a két végponttal próbál forgalmat irányítani és így leterheli a szervert

BIZTONSÁGI MENTÉSEK

* gyakran
* többszörösen, redundánsan menteni
* erős jelszóval mentett

FRISSÍTÉS ÉS HIBAJAVÍTÁS

* win update: javításokat is tartalmaz
* hibajavítást az op rendszer gyártó cég megoldja

3-a modell: AAA: ki léphet be hova és mit csinálhat (naplózás is benne van)

TŰZFAL: megakadályozza a külső behatolást, belülről kifelé kiengedi és engedi válaszolni, a kívül érkező kéréseket nem engedi be (lehet szoftveres, hardveres is)