

A hálózat jelene

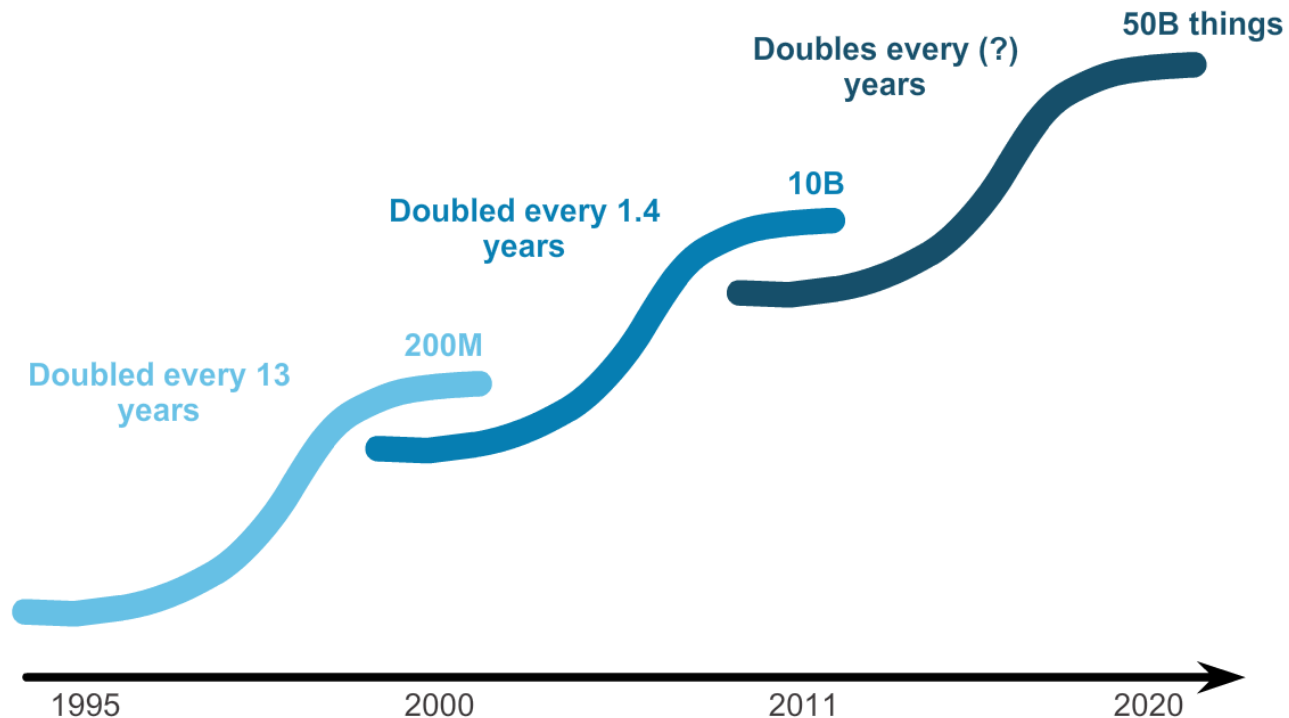
Hálózatok a mindennapokban

"Fixed" Computing
(You go to the device)

Mobility/BYOD
(The device goes with you)

Internet of Things
(Age of Devices)

Internet of Everything
(People, Process, Data, Things)



A hálózat jelene

Hálózatok hatása a mindennapokban

- A hálózat hatása a tanulás folyamatára

Virtual Classrooms



Collaborative Learning Spaces



Networks support the way we learn ...



On-demand Video



Mobile Learning

A hálózat jelene

Hálózatok hatása a mindennapokban

■ A hálózat hatása a kommunikáció folyamatára

Instant Messaging



Instant messaging is everywhere and can include audio and video conversations. IM can send text messages to mobile phones.

Weblog



You can express your thoughts online, share your photos, and join a community of fellow thinkers.

Podcasting



You can listen to your favorite radio show on your portable audio player whenever you have the time and wherever you are. Every time a new show becomes available, it can be automatically downloaded.

- Azonnali üzenetküldés (IM) / szöveges üzenetküldés
- Közösségi portálok
- Csoportmunka
- Weblogok (blogok) –
- Wikik
- Podcasting
- Peer-to-peer (P2P) fájlmegosztás
- Szociális hálózatok

A hálózat jelene

Hálózatok hatása a mindennapokban

A hálózat hatása a munkavégzés folyamatára

- saját pénzügyi és egyéb adatok információk tárolására és az ezekhez való hozzáférésre
- Cégen belüli és cégek közötti e-mail, videó, üzenetküldés és a telefonos kommunikáció.
- Távmunka, videokonferencia,
- eredményes és költséghatékony munkavállalói tanfolyamok területén
- az időigényes és költséges utazásokat szükségszerűségének csökkentése



A hálózat jelene

Hálózatok hatása a mindennapokban

A hálózat hatása, a szórakozási szokásainkra

Online Interest Groups



Online Gaming



Online Entertainment



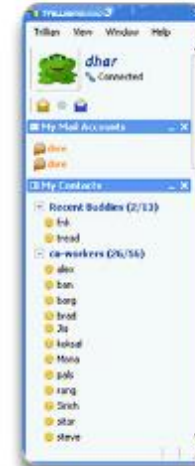
Online Shopping



Onboard Data Networks



Instant Messaging



The way we play is supported by services delivered by the data network.

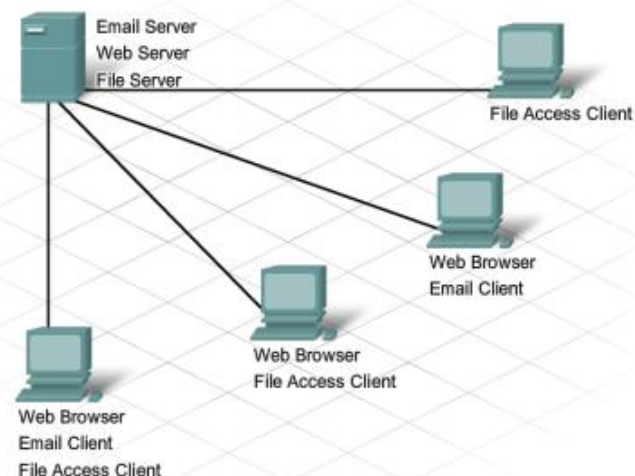
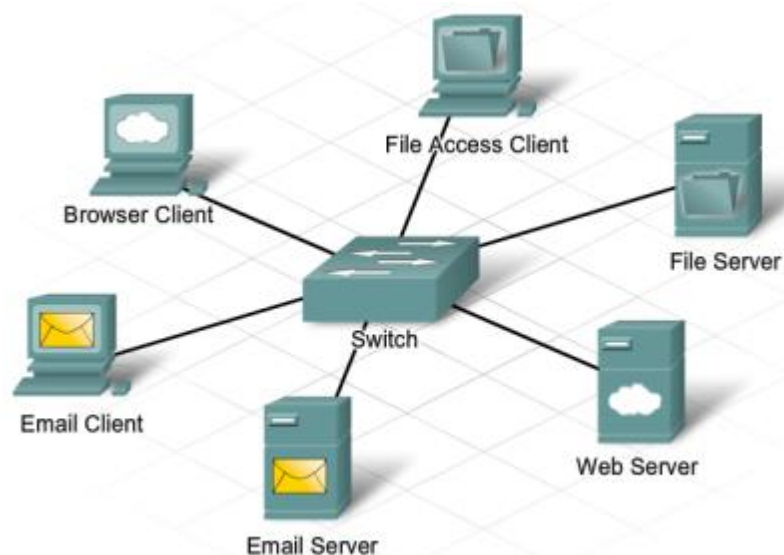
Erőforrások biztosítása egy hálózaton

Kliensek és szerverek

- **Állomásnak (host) vagy végberendezésnek:** nevezünk minden hálózatra csatlakoztatott számítógépet, eszközt, gépet, amelyek közvetlenül részt vesznek a hálózati kommunikációban.

Az állomásokat működésük szerint két nagy csoportba sorolhatjuk:

- **1. Szervereknek** nevezzük azokat az állomásokat, amelyeknek a feltelepített programjai más hálózati állomások számára információt szolgáltatnak, szolgáltatásokat biztosítanak. (pl.: elektronikus levelezés vagy weboldalak formájában, távoli fájllelés, -átvitel.)
- **2. Klienseknek** nevezzük azokat az állomásokat, amelyeknek telepített programjai lehetővé teszik, hogy szerverektől információkat kérjenek és azokat megjelenítsék, használják. Igénybe vegyék szerverek szolgáltatásait. A kliensprogramra példák a Firefox böngésző vagy az Outlook levelező kliens



Erőforrások biztosítása egy hálózaton

Hálózatok típusai

- Azon felépítésű hálózatokat, ahol az egyes számítógépek szerepeik szerint jól elkülöníthetők **kliens-szerver** hálózatoknak nevezzük.
- Ilyenek tipikusan vállalati, iskolai, ... stb. hálózatok. (lásd előző dia)
- Azokat a kisvállalati és otthoni hálózatokat, amelyekben egy állomás egyszerre szerverként és kliensként is szolgál **egyenrangú (peer-to-peer)** hálózatnak nevezzük.



-
- Előnyök - hátrányok egyenrangú hálózatok esetén:

előny	hátrány
könnyű beállítani	központilag nem tartható karban
egyszerű felépítés	nem biztonságos
alacsony költség, nem szükséges dedikált szerver	nehezen skálázható
egyszerű fájlmozgatás, és megosztott nyomtatás	minden állomás lehet egyszerre kliens és szerver is, ami rontja a teljesítményt

A hálózati infrastruktúra elemei:

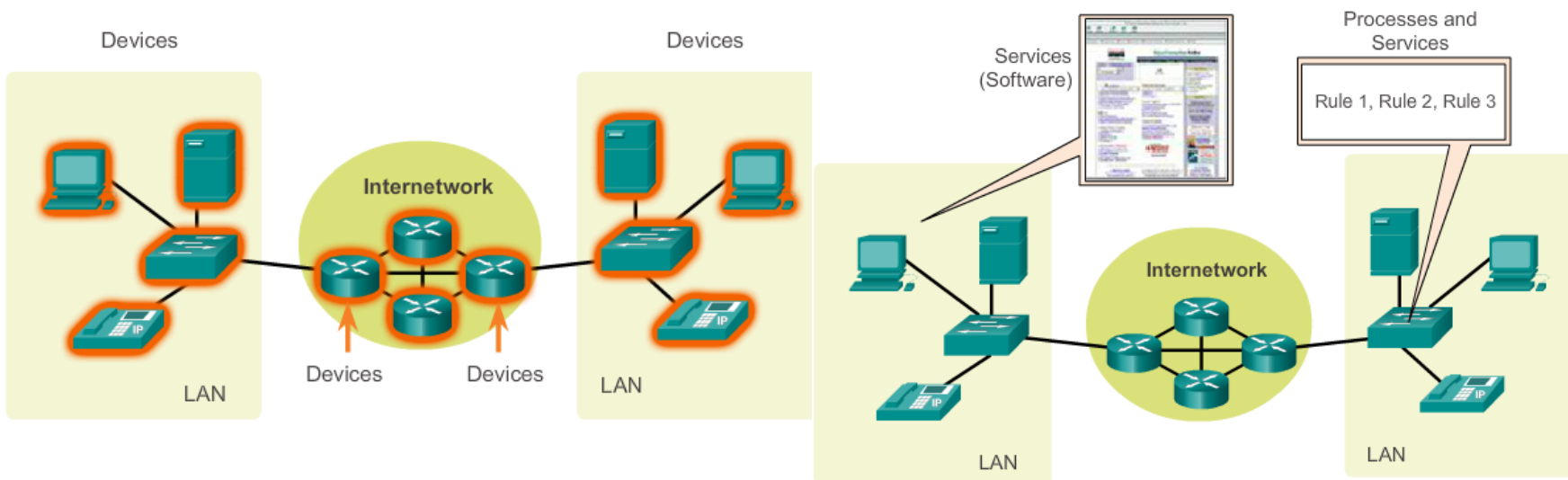
■ Eszközök

Végberendezések, állomások: A végberendezés forrása vagy célállomása is lehet a hálózati kommunikációnak. Emiatt minden állomást a hálózaton egy egyedi címmel kell azonosítanunk a hálózaton. (számítógépek, mobil telefonok, nyomtatók, IP kamerák, ...)

közvetítőhálózati eszközök: A közvetítő hálózati eszközök kapcsolják össze a végberendezéseket. (switchek, routerek, AP-k, tűzfalak, ...)

Ezen közvetítő eszközök feladatai: adatjelek továbbítása, [újra]generálása, forgalomirányítás, hibajavítás, QoS, szűrés

■ Szolgáltatások (programok, amik szolgáltatásokat nyújtanak - HTTP, FTP, VoIP, DNS, ...)



A hálózati infrastruktúra elemei:

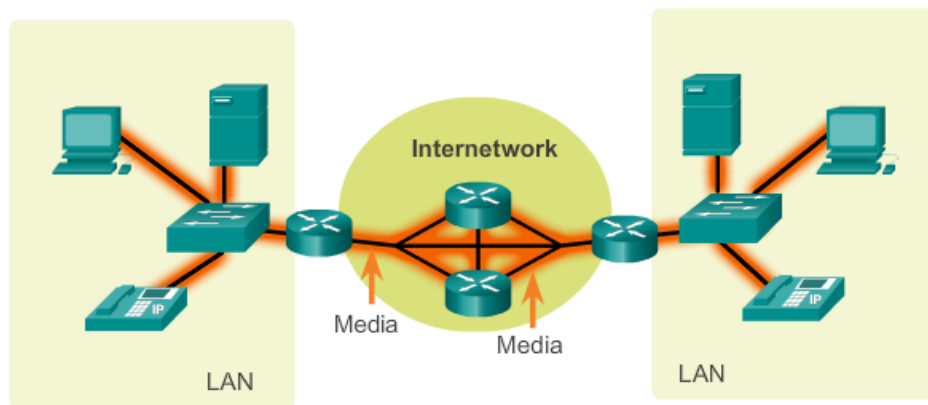
■ Információhordozó közeg vagy média:

ez biztosítja az összeköttetést (csatornát) az eszközök között, amelyen keresztül az üzenet eljut a forrástól a célállomásig.

Lehet: kábelezés (réz (elektromos impulzus), optika (fény impulzus)) ; levegő (EM hullám))

A választásnál az alábbi szempontok fontosak:

- jeltovábbítási távolság
- a környezeti lehetőségek
- átvitendő adatok mennyisége, átviteli sebesség
- telepítési költségek



Copper



Fiber Optic

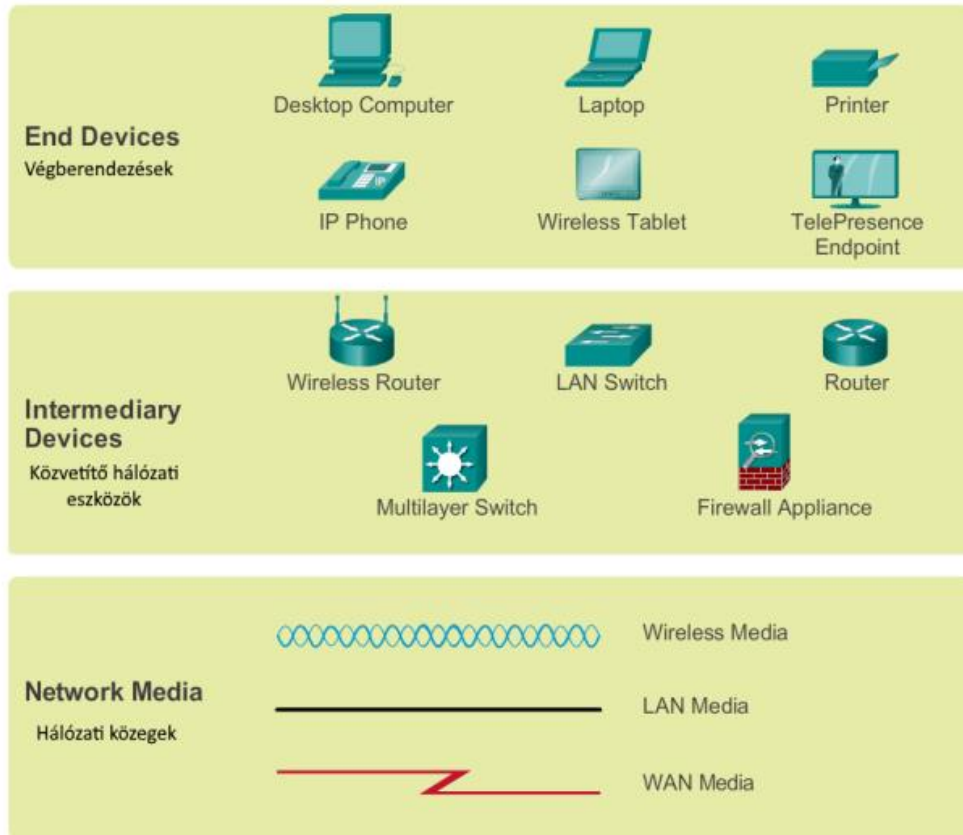


Wireless



A hálózat elemei

A hálózatok elemek megjelenítése



Hálózati kártya (NIC, Network Interface Card) - Ez az az eszköz, amely biztosítja a PC-k vagy más állomások számára a hálózathoz történő fizikai kapcsolódást. Gyakran hívják NIC-nek, vagy LAN adapternek. A PC és a hálózat közti átviteli közeg közvetlenül a NIC-be csatlakozik.

Fizikai port - Egy hálózati eszközön a csatlakozást biztosító aljzat, ehhez csatlakozik az átviteli közegen keresztül egy állomás vagy egy másik hálózati eszköz.

Interfész - Speciális port egy hálózati eszközön, amely saját hálózatokhoz csatlakozik. Mivel a forgalomirányítók kötik össze a hálózatokat, ezért a forgalomirányító portjait nevezzük interfészeknek.

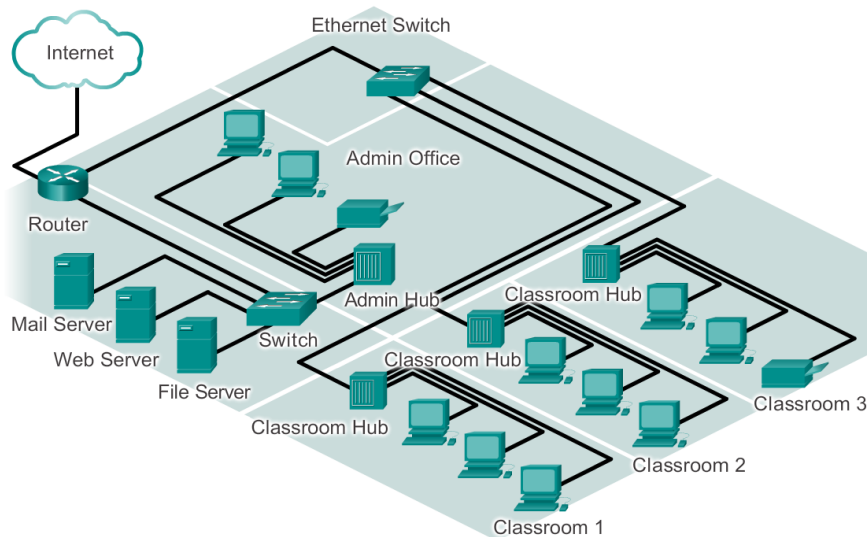
A hálózat elemei

Topológiai ábrák

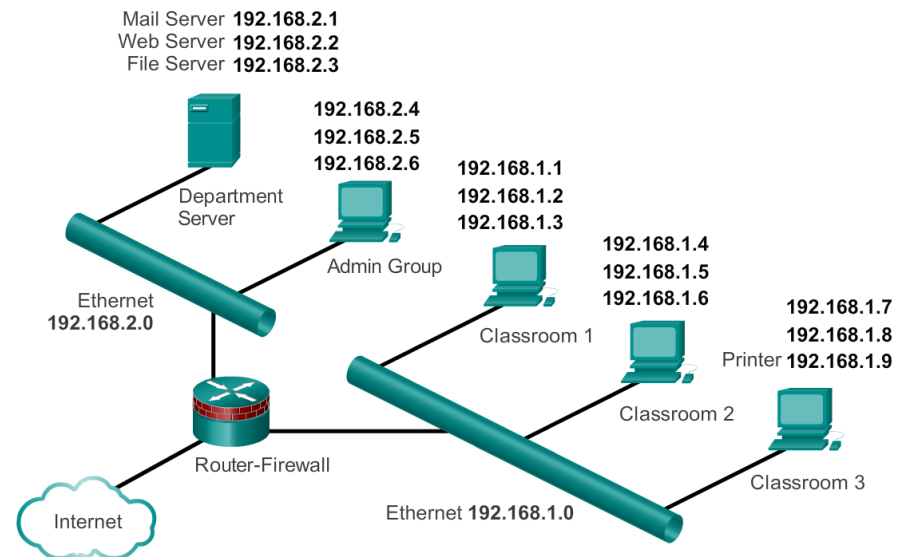
A topológiai ábrák biztosítják a hálózati összeköttetések vizuális térképét. Kétféle topológiai ábra létezik:

- **Fizikai topológiai ábra** - Ez mutatja meg a közvetítő eszközök, a használt portok és a kábelezés fizikai elhelyezkedését.
- **Logikai topológiai ábra** - Ez azonosítja az eszközöket, a portokat és az IP-címzési rendszert.

Physical Topology



Logical Topology



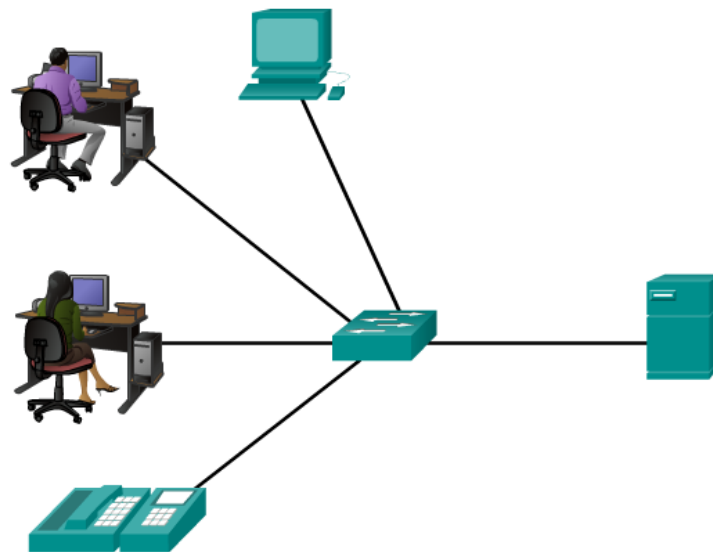
Hálózattípusok – Helyi hálózat

A **hálózati infrastruktúrák** nagyban eltérnek egymástól a következőkben:

- a lefedett terület mérete,
- kapcsolódott felhasználók száma,
- az elérhető szolgáltatások száma és típusa.

1. Helyi számítógép-hálózat (LAN, Local Area Network)

- amely kis földrajzi elhelyezkedésű területen biztosít összeköttetést a felhasználók és a végberendezések számára, mint például az otthonok, az iskolák, az irodaépületek vagy az egyetemi kampuszok.
- egyetlen szervezet vagy egy magánszemély felügyeli. Az adminisztratív feladatok közé tartozik többek között a hálózati szintű biztonsági és hozzáférési házirendek alkalmazása.
- nagy sávszélességet biztosítanak a belső végberendezéseknek és hálózati közvetítő eszközöknek.

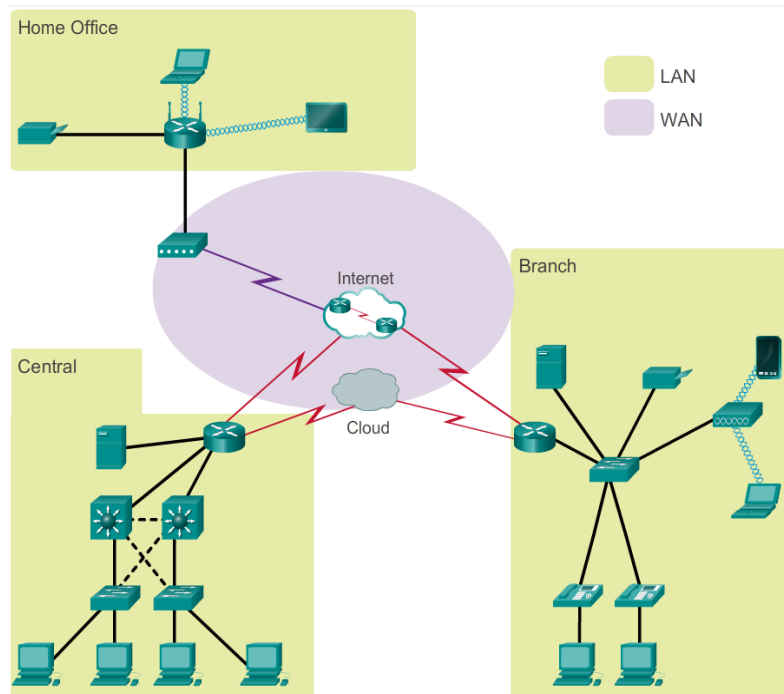


A network serving a home, building, or campus is considered a LAN.

LAN és WAN

Nagyvárosi és nagy távolságú hálózatok

2. Nagyvárosi hálózat (MAN, Metropolitan Area Network) - Olyan hálózati infrastruktúra, amely egy LAN-nál nagyobb, de egy WAN-nál kisebb fizikai területet fed le (pl. egy város területe). A MAN hálózatokat gyakran egyetlen szervezet működteti, például egy nagyvállalat.

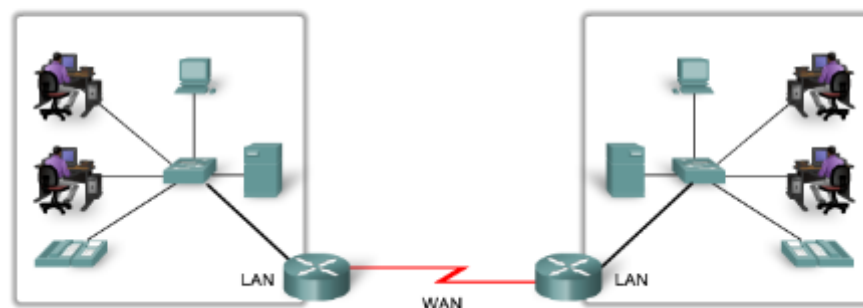


3. Nagy távolságú hálózat (WAN, Wide Area Network) - A nagy távolságú hálózatok (WAN, Wide Area Network) nagy földrajzi területeket fednek le. A WAN hálózatokat általában szolgáltatói szervezetek, vagy internet szolgáltató cégek (ISP, Internet Service Provider) biztosítják.

A WAN hálózatok sajátosságai a következők:

- A WAN-ok biztosítják az összeköttetést a LAN-ok között olyan nagy földrajzi területeket átfogva, mint városok, államok, tartományok, országok vagy kontinensek.
- A WAN hálózatokat rendszerint több szolgáltató biztosítja.
- A WAN-ok jellemzően lassabb összeköttetést biztosítanak, mint a LAN-ok.

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



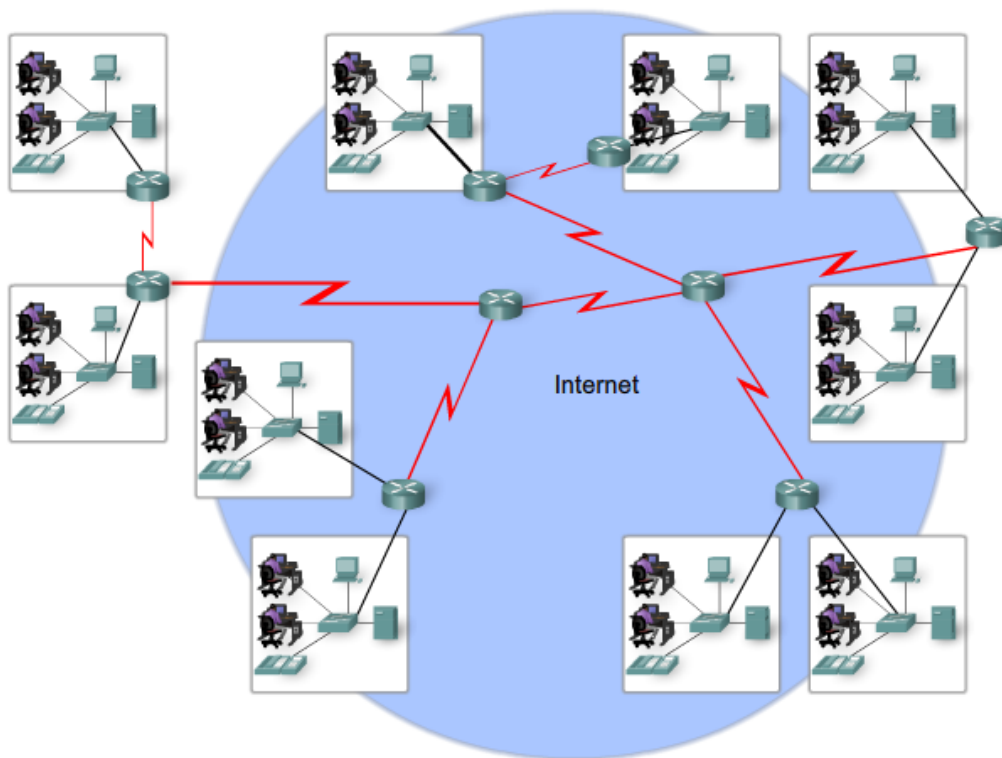
LAN, WAN és az internet

Az internet

internet - Az internet a hálózatoknak olyan halmaza, amelyet nem birtokol egyetlen magánszemély vagy csoportosulás sem.

Megjegyzés: Az internet szót (kisbetűs "i"-vel) a többszörösen összekapcsolt hálózatokra használják. Amikor a globális hálózati rendszerre hivatkozunk, mint például a World Wide Web-re, akkor nagybetűs "I"-vel is írhatjuk az internetet.

LANs and WANs may be connected into internetworks.

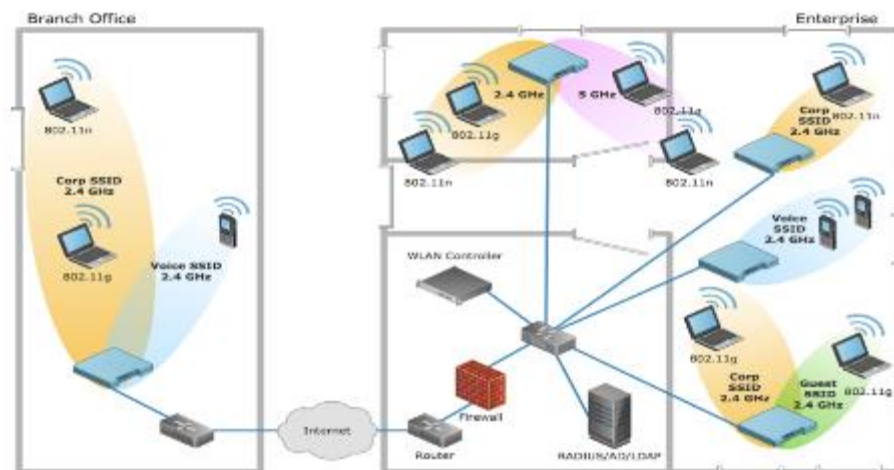
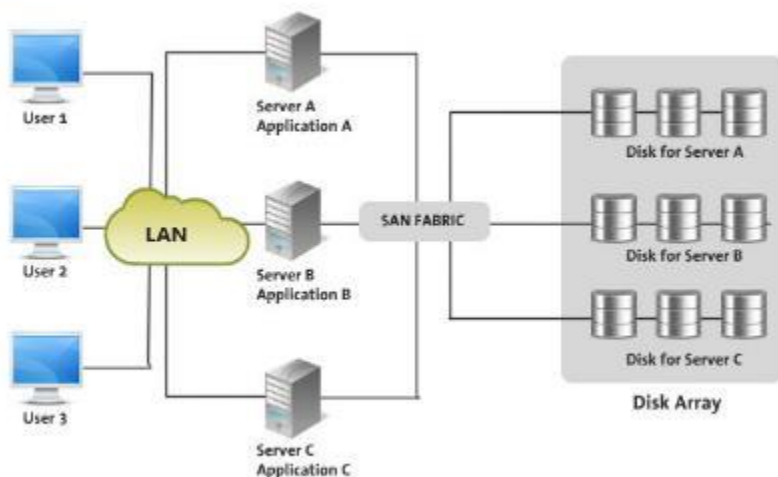


LAN, WAN és az internet

Egyéb hálózat típusok

Adattároló hálózat (SAN, Storage Area Network) - Ezt a hálózati infrastruktúrát fájlserverek támogatására tervezték, biztosítja az adatok tárolását, visszakereshetőségét és mentését. Modern servereket, több lemezből álló adattárolókat (úgynevezett blokkokat) és Fibre Channel összeköttetéseket magában foglaló hálózat

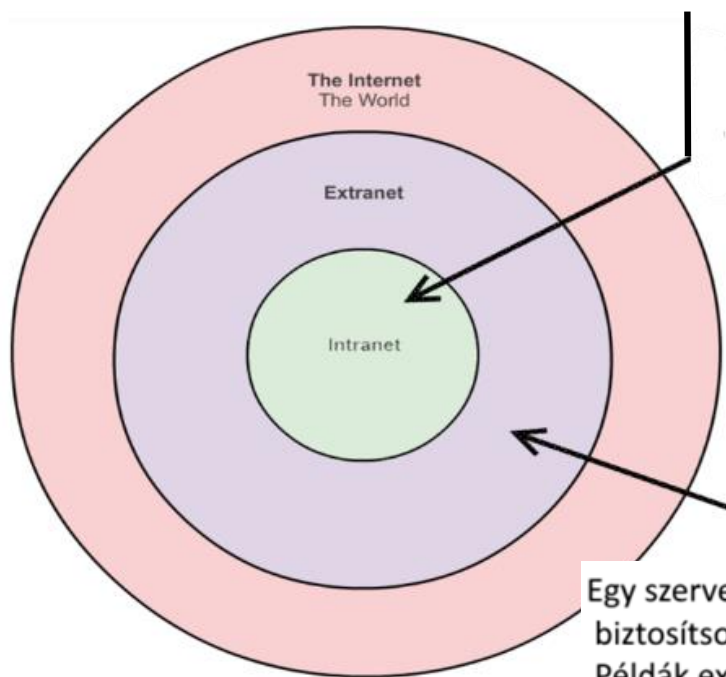
Vezetéknélküli LAN (WLAN, Wireless LAN) - Hasonló a LAN-hoz, de vezeték nélkül köti össze a felhasználókat és a végpontokat egy kis földrajzi területen.



LAN, WAN és az internet

Intranet és extranet

Az **Intranet** azon privát LAN és WAN hálózati összeköttetések összesége, amelyek egy szervezethez tartoznak, és csak a szervezet tagjai, munkavállalói vagy meghatalmazott külső személyek használhatják. Az intranet alapvetően, olyan internet amely általában csak egy szervezeten belülről érhető el.



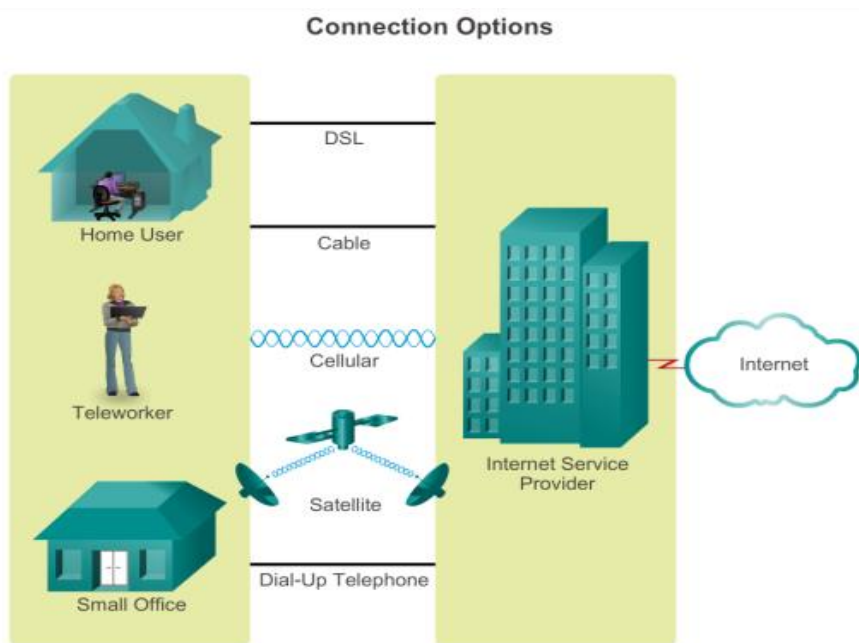
Egy szervezet használhat **Extranet-et** hogy biztonságos és megbízható hozzáférést biztosítson a saját hálózata eléréséhez más szervezetek dolgozói számára is.

Példák extranet-re a következők:

- Egy cég hozzáférést biztosít külső beszállítóik / vállalkozóik számára.
- Egy kórház foglalási rendszert biztosít az orvosok számára, akik így találkozókat egyeztethetnek a betegeikkel.
- Egy oktatásügyi helyi kirendeltség költségvetési és személyi adatokat szolgáltat a kerületi iskolákról.

Távoli felhasználók internet csatlakozása

- **Kábel** - Általában kábeltelevíziós szolgáltatók kínálják, az internetes adatjelek és a kábeltévé jeleinek szállítása ugyanazon a koaxiális kábelon történik. Nagy sávszélességű és állandó internetkapcsolatot biztosít. Egy speciális kábelmodem választja el az internetes adatok jeleit a többi jeltől, és ez az eszköz biztosítja az Ethernet kapcsolatot a számítógép vagy a LAN felé.
- **Mobilhálózatok** - A mobil internet a mobiltelefonos összeköttetést használja csatlakozásra. Ahol a rádiójelek elérhetők, ott lehet mobil internet-hozzáférés is. A teljesítményt korlátozhatják a telefon, vagy a csatlakozást biztosító adótorony (bázisállomás) képességei. Azokon a helyeken előnyös a mobil internet használata, ahol egyébként nem lehet máshogy internet kapcsolatot biztosítani, vagy ahol a felhasználók folyton mozgásban vannak.



DSL - Nagy sávszélességű és állandó internetkapcsolatot biztosít. Szükséges hozzá egy speciális nagy sebességű modem, amely elválasztja a DSL jeleit a telefonos jelektől, és egy Ethernet kapcsolatot biztosít a számítógép vagy a LAN felé. A DSL a telefonvonalat használja, amit három különböző csatornára oszt szét.

- Az első csatorna szolgál a telefonhívásokra. Ez a csatorna teszi lehetővé, hogy az előfizető anélkül fogadjon telefonhívásokat, hogy bontania kellene az internet kapcsolatát.

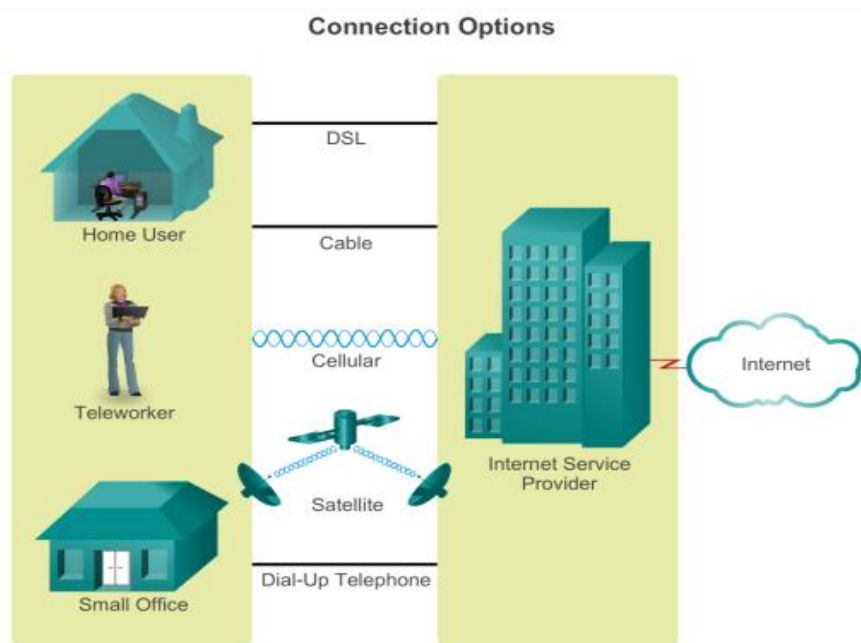
- A második csatorna egy gyorsabb letöltési csatorna, ezen keresztül érkeznek az adatok az internet felől.

- A harmadik csatorna küldésre vagy feltöltésre használható. Ez a csatorna általában valamivel lassabb, mint a letöltési csatorna.

A DSL minősége és a sebessége nagyban függ a telefonvonal minőségétől és a telefonos cég szolgáltató központjának távolságától. Minél messzebb van ettől a központtól az előfizető, annál lassabb lesz a kapcsolata

Távoli felhasználók internet csatlakozása - 2

- **Modemes behívás** A modemes betárcsázás egy nem túl költséges, telefonvonal és modem használatával megvalósított internet elérési módszer. Az internetszolgáltatóhoz való kapcsolódáshoz a felhasználónak fel kell hívnia a szolgáltató elérési számát. A modemes behívás alacsony sávszélessége rendszerint nem elegendő a nagy adatátviteli műveletekhez, bár hasznos mobil hozzáférést biztosít utazás közben. A modemes behívás csak akkor jöhet számításba, ha nagyobb sebességű kapcsolat nem áll rendelkezésre.



Műhold - A műholdas szolgáltatás egy jó lehetőség azon otthonok vagy irodák számára, amelyek nem tudnak hozzáférni a DSL vagy a kábeles szolgáltatásokhoz. A parabola antennának tiszta rálátás szükséges a megfelelő műholdra, így ez a szolgáltatás nem mindig érhető el sűrű erdős, vagy más akadályokkal teli területen. A műholdas szolgáltatásnál alapvetően jó sávszélesség áll rendelkezésre, de a konkrét sebesség a választott szerződés függvénye. A berendezés- és telepítési költségek magasak lehetnek, ezek mellett a havi díjak már mérsékeltebbek. A műholdas internet-hozzáférés ott előnyös igazán, ahol nincs más mód a csatlakozásra.

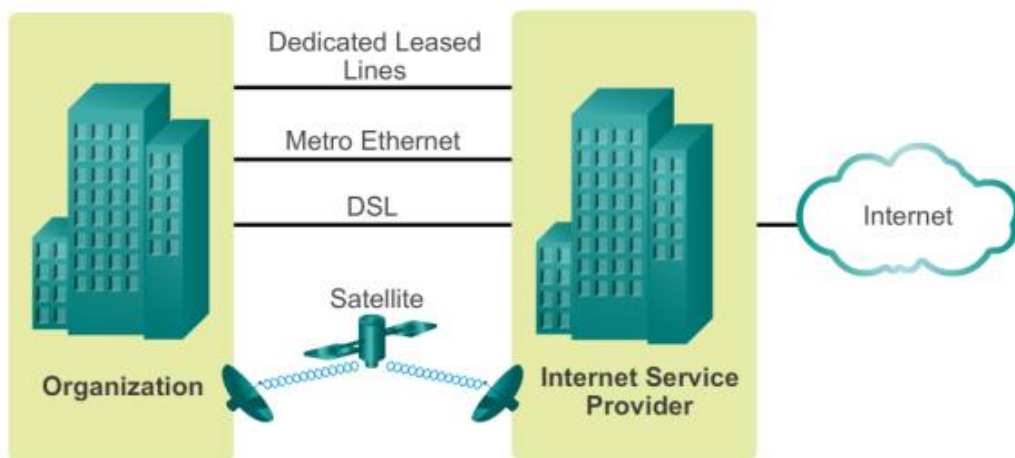
Optikai vonalak: Sok otthon és kisebb iroda egyre gyakrabban használ közvetlen optikai vonalat a csatlakozásra. Ez lehetővé teszi az internetszolgáltatók számára, hogy a nagyobb sávszélesség mellett egyszerre több szolgáltatást is biztosítsanak, úgymint internet, telefon és TV.

Vállalatok internet csatlakozása

A vállalatok nagyobb és dedikált sávszélességet, valamint menedzselt szolgáltatásokat igényelnek. A csatlakozási lehetőségek nagyban eltérőek attól függően, hogy hány szolgáltató működik a vállalat közelségében.

Dedikált bérelt vonal - Ez egy dedikált kapcsolat a szolgáltató és az ügyfél telephelyei között. A bérelt vonalak valóban saját használatú távközlési áramkörök, amelyek földrajzilag távol levő irodák saját hang- és/vagy adathálózatát biztosítják. A vonalakat általában bérlik viszonylag magas havi vagy éves díj ellenében. Észak-Amerikában gyakori bérelt vonali áramkörök a T1 (1,54 Mb/s) és a T3 (44,7 Mb/s) T4 (275Mb/s), T5(400Mb/s) míg a világ más részein az E1 (2 Mb/s) és az E3 (34 Mb/s) E4(160 Mb/s) kapcsolatok állnak a vállalatok rendelkezésére.

Connection Options

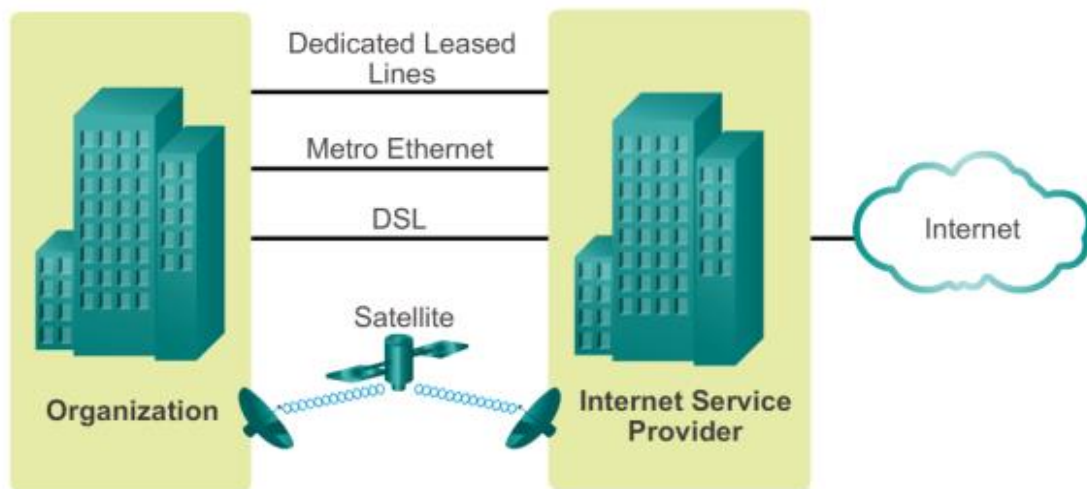


- **Metro Ethernet** - A Metro Ethernet általában közvetlen réz- vagy optikai kapcsolaton keresztül érhető el a szolgáltatótól, a biztosított sávszélesség pedig 10 Mb/s és 10 Gb/s között van. Sok esetben a réz alapú Ethernet (EOC, Ethernet over Copper) sokkal gazdaságosabb, mint az optikai Ethernet szolgáltatás, mert meglehetősen széles körben áll rendelkezésre, és sávszélessége elérheti akár a 40 Mb/s-ot is. A réz alapú Ethernet használata ugyanakkor függ a távolságtól. Az optikai Ethernet szolgáltatás biztosítja a leggyorsabb és ár-érték arányban a leg gazdaságosabb kapcsolatot. Sajnos még sok olyan terület van, ahol ez a szolgáltatás nem érhető el.

Vállalatok internet csatlakozása - 2

- **DSL** - Az üzleti DSL több változatban létezik. A legnépszerűbb változat a szimmetrikus digitális előfizetői vonal (SDSL), amely hasonló az aszimmetrikus digitális előfizetői vonalhoz (ADSL), de ugyanazt a feltöltési és letöltési sebességet biztosítja. Az ADSL-t úgy tervezték, hogy különböző nagyságú legyen a letöltési és feltöltési sáv szélesség. Például egy ügyfél internet-hozzáférése letöltési irányban 1,5-9 Mb/s lehet, míg a feltöltési irány 16-640 Kb/s. Az ADSL átvitel 18000 láb (5488 méter) távolsáig működik egy réz alapú csavart érpáron.

Connection Options



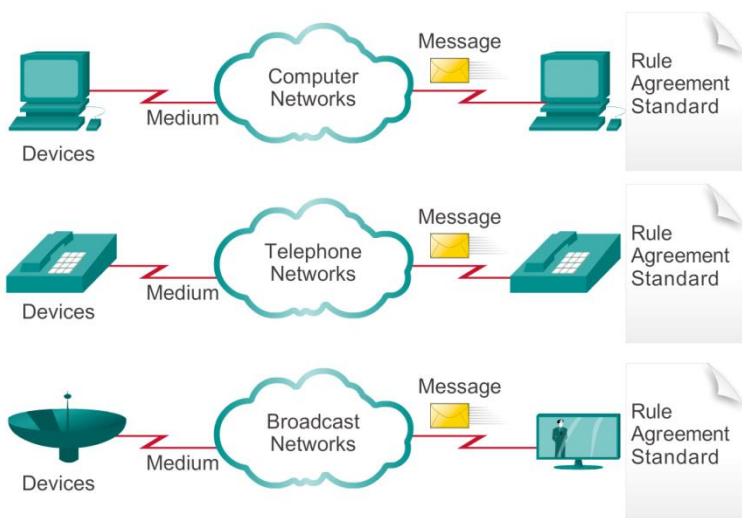
Műhold - Műholdas szolgáltatást ott is lehet nyújtani, ahol a vezetékes megoldások nem állnak rendelkezésre. A parabola antennáknak szükséges a tiszta rálátás a műholdra. A berendezés- és telepítési költségek magasak lehetnek, de emellett a havi díjak már mérsékeltebbek. A kapcsolatok általában lassabbak és kevésbé megbízhatóak, mint a földi versenytársakéi, így ez a lehetőség kevésbé vonzó, mint a többi alternatíva.

Konvergált hálózatok

A konvergáló hálózat

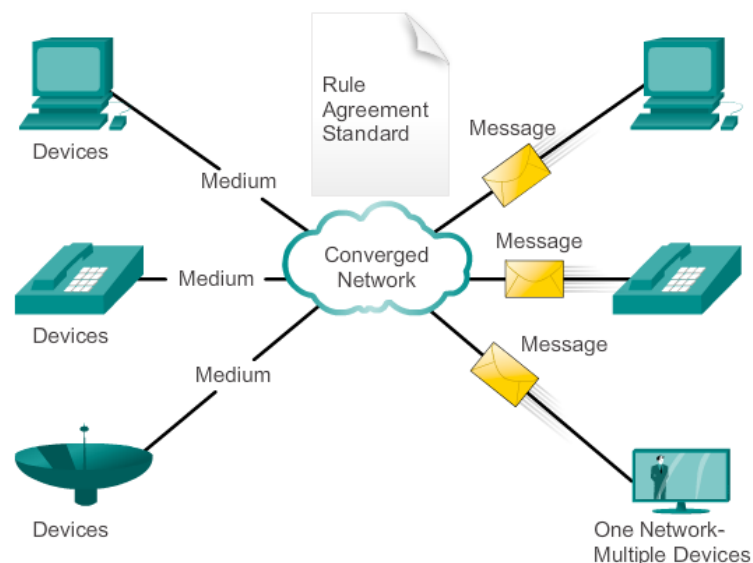
Konvergált hálózat:A konvergált hálózatok sok különböző típusú eszköz között, de ugyanazt a közeget/kommunikációs csatornát használva egyszerre átvinni hang- és videojelet, valamint szöveg és képi jellegű adatokat

Multiple Networks



Multiple services are running on multiple networks.

Converged Networks



Converged data networks carry multiple services on one network.

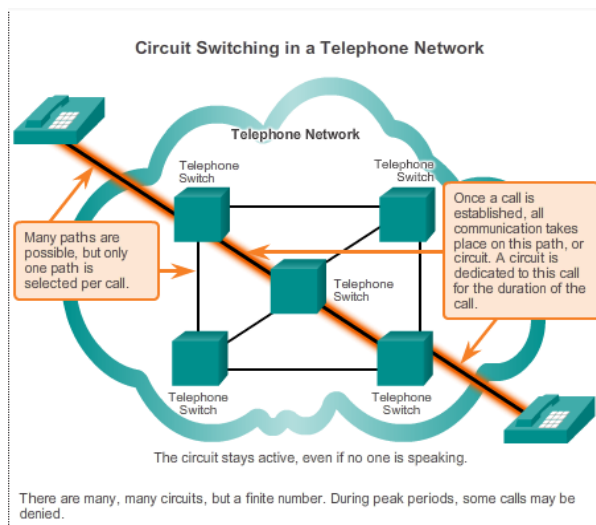
Megbízható hálózat

A hálózati architektúra

A megbízható hálózatok főbb jellemzői:

- hibatűrés
- skálázhatóság
- a szolgáltatás minősége (QoS, Quality of Service)
- Biztonság

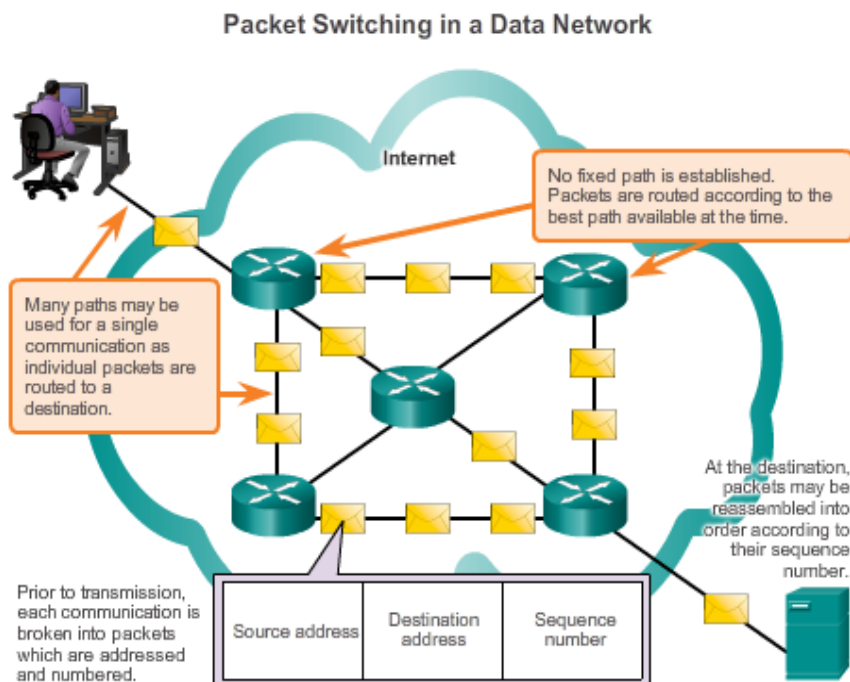
- **1. Hibatűrő hálózat:** Az a hibatűrő hálózat, amely képes korlátozni egy hálózati kiesés hatását, vagyis hogy minél kevesebb eszköz legyen érintve a hibában.
- Az ilyen hálózatokban az üzenet forrása és a célja közötti több útvonal is létezik. Ha egy útvonal megszakad, az üzeneteket azonnal egy másik kapcsolaton továbbítódnak. *Redundanciának* hívjuk, ha a forrásállomástól egy célállomáshoz egyszerre több út is vezet.



- *vonalkapcsolt hálózatokban (pl.: telefonhálózatok)*
- A hívásnak először fel kellett épülnie, ami egy vonal a hívó fél (forrás) és a fogadó fél eszköze (célállomás) között. Ha bármelyik eszköz tönkremegy vagy kapcsolat megszakad, az egész hívás sikertelenné válik. Újrakapcsolódás esetén pedig egy teljesen új hívást kellett kezdeményezni, új vonalak használatával. Ezt a kapcsolódási formát vonalkapcsolásnak nevezzük,

Csomagkapcsolt hálózatok

- csomagkapcsolt hálózatokban: A csomagkapcsolt hálózatokban az üzeneteket kisebb egységekre (csomag, keret) lehetett bontani, az egységek mindegyike tartalmazza a szükséges címezési információkat, vagyis a küldő és a fogadó állomás címét. A csomagokat a forrástól a cél állomás felé különböző útvonalakon is el lehet küldeni, majd a célállomáson vissza lehet állítani a csomagokból az eredeti üzenetet



During peak periods, communication may be delayed, but not denied.

A működés során, ha egy korábban használt útvonal már nem érhető el, akkor a következő legjobb útvonal dinamikusan kerül kiválasztásra a forgalomirányítás révén.

Mivel az üzeneteket nem egyben, hanem darabokban küldik el, ezért ezt a néhány csomagot esetleg elveszik, egy másik útvonalon újra el lehet küldeni célállomásnak.

Megbízható hálózat

Skálázható hálózatok

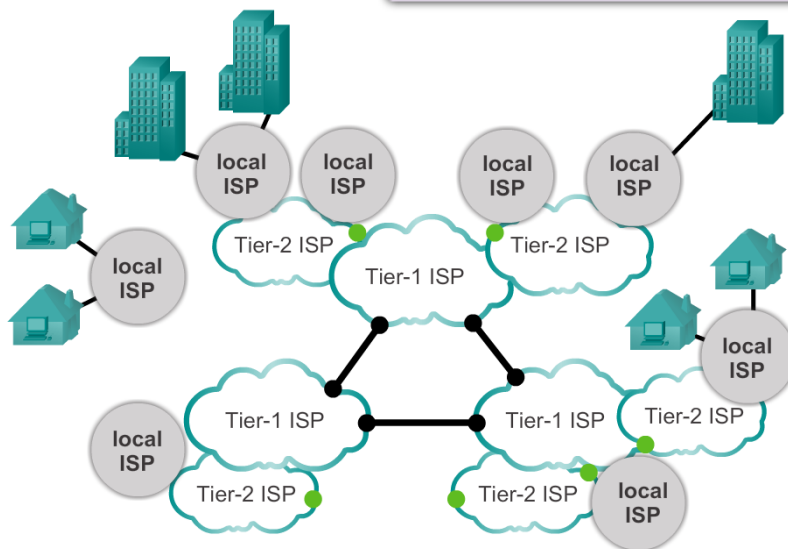
Skálázhatóság, méretezhetőség:

A skálázható hálózatokat gyorsan lehet bővíteni anélkül, hogy az befolyásolná a már meglévő felhasználók számára nyújtott szolgáltatások tulajdonságait, teljesítményét.

At the center of the Internet, Tier-1 ISPs provide national and international connections. These ISPs treat each other as equals.

Tier-2 ISPs are smaller and often provide regional service. Tier-2 ISPs usually pay Tier-1 ISPs for connectivity to rest of the Internet.

Peer connections between networks at the same level provide direct connections, bypassing longer routes and preventing congestion on the backbone.

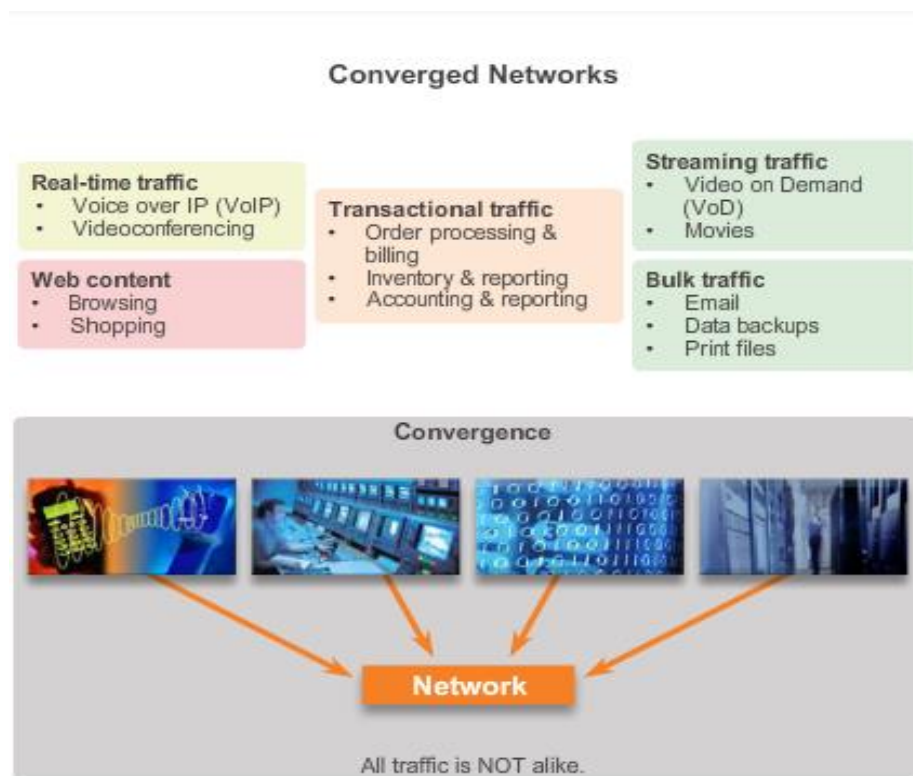


Tier-3 ISPs are the local providers of service directly to end users. Tier-3 ISPs are usually connected to Tier 2 ISPs and pay Tier 2 providers for Internet access.

Szolgáltatás minőség - QoS biztosítása

Szolgáltatás minősége(QoS): A hálózatoknak kiszámítható, mérhető és szükség esetén garantált szolgáltatásokat kell biztosítaniuk adott típusú kommunikációk (hang, video, http, ftp ...) részére.

Ha egyszerre több kommunikáció használja a hálózatot, akkor előfordulhat, hogy az összesített igény meghaladja a rendelkezésre álló hálózati sávszélességet, vagyis torlódás* alakul ki. A hálózatnak egyszerűen több bitet kell ilyenkor továbbítania, mint amit a kommunikációs csatorna *sávszélessége*** lehetővé tenne.



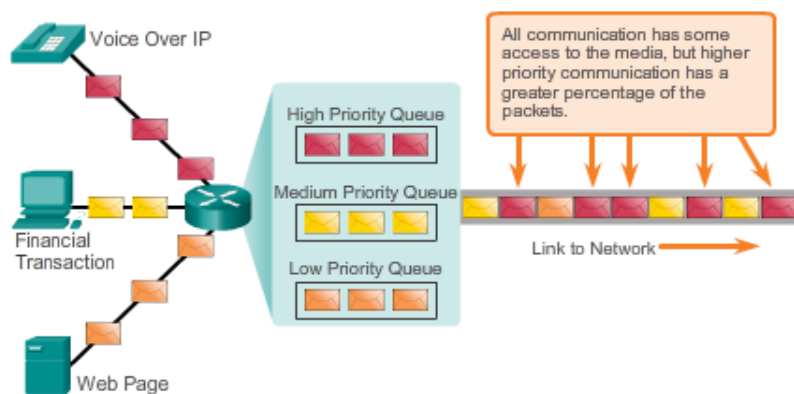
Megoldás = QoS: Az adatok a kommunikáció jellegének és az adott alkalmazáshoz rendelt relatív fontosságnak kombinációját használva osztályokba (QoS osztályokba) kell sorolni. Ezt követően az egy osztályba sorolt adatokat ugyanolyan szabályokat követve kell feldolgozni.

*A **torlódás** A legtöbb esetben, amikor a csomagok mennyisége nagyobb, mint amit a hálózat képes lenne kezelni, az eszközök a memóriába beolvasott csomagokat késleltetnek, várakozási sorba állítják azokat. Ezek a sorban álló csomagok késedelmet okoznak, mivel addig nem lehet új csomagot továbbítani, amíg a korábbi csomagok nem kerültek feldolgozásra. Ha a sorban álló csomagok száma folyamatosan növekszik, a memória egy idő után megtelik és az újonnan érkező csomagok eldobásra kerülnek.

A **hálózati sávszélesség az egy másodperc alatt átvihető bitek számát adja meg. A mértékegysége a bit per másodperc (bps).

Szolgáltatás minőség - QoS biztosítása

Using Queues to Prioritize Communication



Queuing according to data type enables voice data to have priority over transaction data, which has priority over web data.

A prioritások felállításakor a következőkre érdemes figyelni:

- Időérzékeny kommunikáció - A kiemelt szolgáltatások prioritásának növelése (például hang vagy videó továbbítása esetén).
- Nem időérzékeny kommunikáció - Csökkentsük a prioritásokat olyan esetekben, mint a weboldalak böngészése vagy az e-mail kommunikáció.
- Rendkívül fontos a szervezet részére - Növeljük a prioritásokat a termelés szabályozásához, illetve az üzleti tranzakciókhoz szükséges forgalmak esetén.
- Nemkívánatos kommunikáció - Csökkentsük a prioritását a különböző kéretlen alkalmazásoknak, mint például a peer-to-peer fájlcsere-lő vagy valós idejű szórakoztató alkalmazások adatai.

Megbízható hálózat

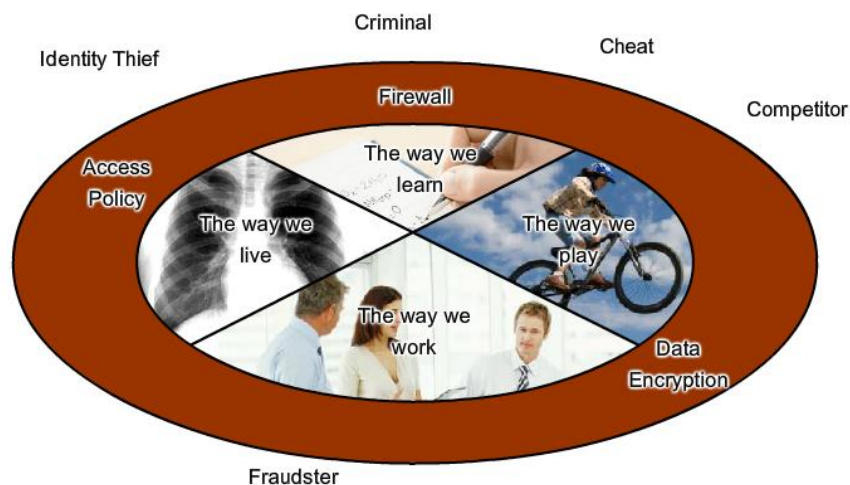
Hálózatbiztonság

Két típusú hálózati biztonsági probléma létezik, amelyekkel foglalkozni kell:

1. *a hálózati infrastruktúra biztonsága*
2. *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. Az *információbiztonság* azt jelenti, hogy szükséges védeni az adatokat tartalmazó csomagok továbbítását, valamint a különböző hálózati eszközökön történő tárolásukat is. A biztonsági intézkedéseknek magukban kell foglalniuk a következő biztonsági veszélyek megakadályozását:

- az információk illetéktelenül történő nyilvánosságra hozatalát,
- az információ eltulajdonítását
- az illetéktelenül történő adatmódosítást,
- szolgáltatás-megtagadási (Denial of Service, DoS) támadást.



The communication and information that we would like to be private is protected from those who would make unauthorized use of it.

Hálózatbiztonság -2

A hálózati biztonsággal szemben támasztott követelmények:

Adatok bizalmas kezelése (confidentiality) - Az adatok bizalmas kezelése azt jelenti, hogy csak a kívánt és felhatalmazott címzettek - egyének, folyamatok vagy eszközök - képesek elérni és olvasni az adatokat.

Ez úgy érhető el, hogy egy erős felhasználói hitelesítést kell használni, vagyis nehezen kitalálható jelszavakat kell beállítani és gyakran kell azokat változtatni. Az adatok titkosítása is része azok bizalmas kezelésének, használatával valóban csak a címzett lesz képes elolvasni az adatokat.

A kommunikáció integritásnak megtartása (integrity)- Az adat integritásáról akkor beszélünk, ha biztosítani tudjuk, hogy az adatokat senki sem tudja módosítani a küldő és a célállomás közti átvitel során.

Az adatok integritása veszélybe kerülhet, ha az információ - szándékosan vagy véletlenül - valahol megsérül. Az adatok integritása a küldő fél hitelesítésén és azokon a folyamatokon alapul, amelyekkel meg lehet bizonyosodni arról, hogy a kapott csomagokat nem változtatták meg az átvitel során.

Elérhetőség biztosítása (Availability)- Az elérhetőség azt jelenti, hogy biztosítjuk a jogosult felhasználók számára a naprakész és megbízható adathozzáférést.

Hálózati tűzfal eszközök, valamint az asztali és szerveroldali víruskereső szoftverek biztosíthatják a rendszer megbízhatóságát az ilyen jellegű támadások felderítésével, kezelésével és kivédésével. Teljesen redundáns hálózati infrastruktúra kiépítésével csökkenthetjük ezeknek a veszélyeknek a hatásait.

Új hálózati trendek

Új trendek

Néhány a legismertebb trendek közül:

- minden eszközhöz, minden tartalomhoz és mindenhol csatlakozhatunk,
- online csoportmunka,
- videó,
- felhő alapú számítástechnika (Felhő alapú szolgáltatások).

BYOD: "Hozd a saját eszközödet":

A BYOD lehetővé teszi a felhasználók számára, hogy akár a saját privát eszközeik használatával érjenek el információkat, vagy kommunikáljanak másokkal egy szervezet hálózatán belül.



Online csoportmunka

A csoportmunka eszközök által a munkavállalók, diákok, tanárok, ügyfelek és a partnerek képessé válnak az azonnali kapcsolatfelvételre, együttműködésre, üzleti tevékenység folytatására, valamint céljaik elérésére - bármilyen kommunikációs csatornát is részesítsenek előnyben.

Az új és fejlődő csoportmunka eszközök lehetővé teszik az egyén számára, hogy gyorsan és egyszerűen, függetlenül a fizikai elhelyezkedéstől képes legyen együttműködni valaki mással.

Collaboration



IP Communication



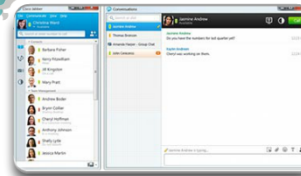
Mobile Applications



Telepresence



Online Conferencing



Messaging

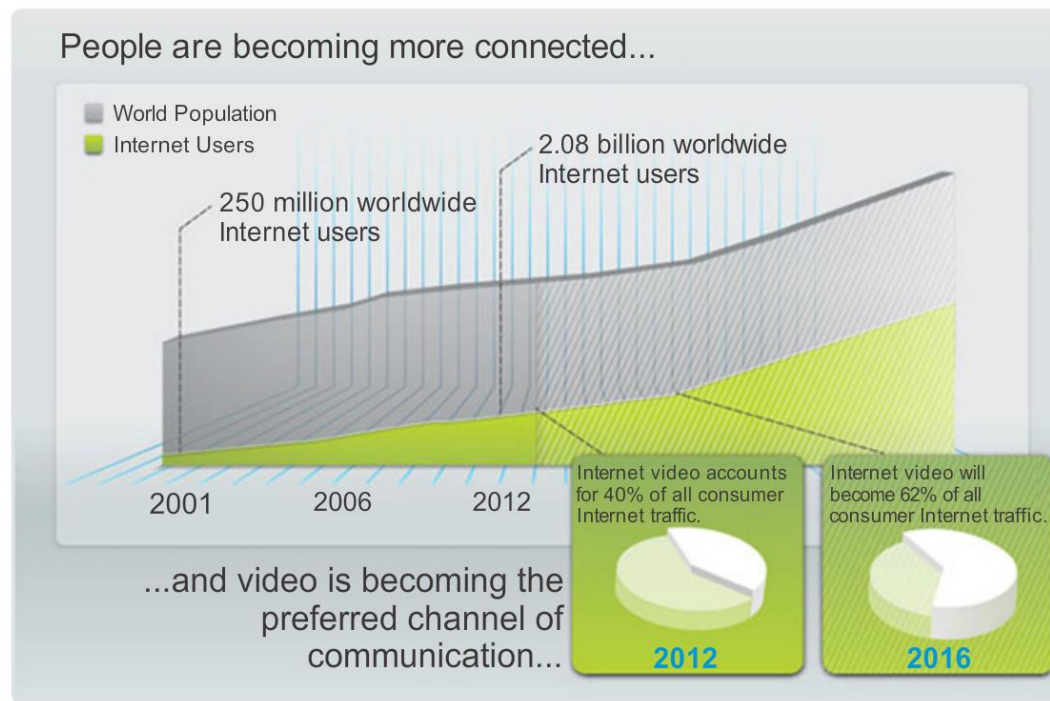
Hálózati trendek

Videó kommunikáció

A videohívások elősegítik a kommunikációt a humán hálózatokban. Egy internetkapcsolat segítségével bárholnan lehet videohívást kezdeményezni és fogadni is, akár otthonról vagy akár a munkahelyről is.

A videó versenyelőnyt biztosít a vállalkozásoknak, csökkenti a költségeket, és a kevesebb utazás révén csökkenti a környezetre gyakorolt hatást is.

- Telepresence, videokonferencia
- digitális videótár (video-on-demand)
- élő videóközvetítések (streaming video).



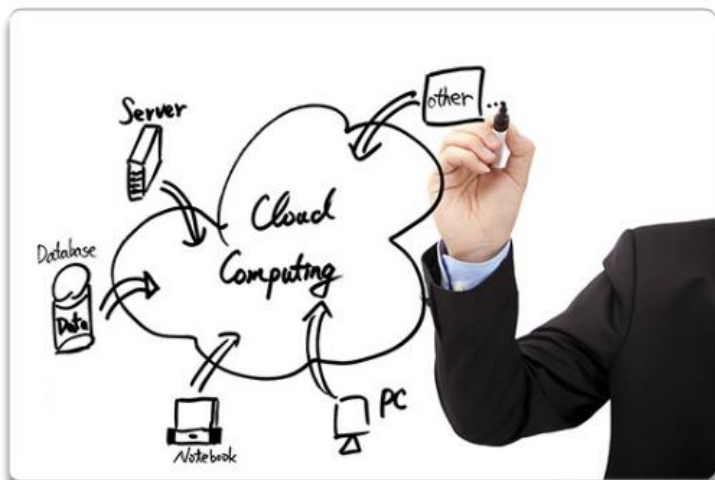
Felhő alapú szolgáltatások

A **felhő alapú szolgáltatások (cloudcomputing)** használatával a hálózaton keresztül szolgáltatásként vehetünk igénybe számítógépes hardver- és szoftvererőforrásokat. Egy vállalat szolgáltatási díj ellenében használhatja a felhőben lévő hardver- és a szoftvererőforrásokat.

A felhő megnöveli a vállalkozások informatikai lehetőségeit anélkül, hogy új infrastruktúrába kellene beruházni, új embereket kellene kiképezni, vagy éppen új szoftverlicenceket vásárolni.

A felhő alapú szolgáltatások a következő előnyöket nyújthatják:

- Szervezeti rugalmasság* - A felhasználók egy webböngésző segítségével bármikor és bárhol hozzáférhetnek az információkhoz.
- Agilitás és gyors megvalósítás* - A gyors megvalósítás mellett az informatikai részleg olyan eszközök kifejlesztésére is összpontosíthat, amelyek által az adatbázisokból, a fájlokból vagy a felhasználói tevékenységekből kinyerhető adatok és tudás könnyebben értékelhetőbbé, elemezhetőbbé és megoszthatóbbá válik.
- Kisebb infrastruktúra költségek* - A technológia átkerül a felhasználói helyszínről a felhőbe, ezáltal csökken a helyi hardverhez és szoftverhez társítható költségigény.
- Az IT-erőforrások átcsoportosítása* - A hardver és szoftver jellegű költségmegtakarítást máshol fel lehet használni.
- Új üzleti modellek létrehozása* - Az alkalmazások és erőforrások könnyebben elérhetővé válnak, így a vállalatok gyorsabban tudnak reagálni az ügyfelek igényeire. Ez segíthet új innovatív stratégiák felállításában, vagy új potenciális piacokra való belépésben.



Adatközpontok

Adatközpontok: A felhő alapú szolgáltatások terjedése az adatközpontok miatt vált lehetségessé. Az adatközpont egy olyan létesítmény, amely fogadja a számítógépes rendszereket és a következő kapcsolódó elemeket:

- Redundáns adatkommunikációs kapcsolatok
- Nagy sebességű virtuális szerverek (néha ezt szerverfarmoknak, vagy szerver-klasztereknek hívják)
- Redundáns tárolórendszerek (általában SAN technológiát használnak)
- Redundáns vagy tartalék tápegységek
- Környezeti hatások elleni védelem (pl. klíma, tűzoltó rendszer)
- Biztonsági berendezések



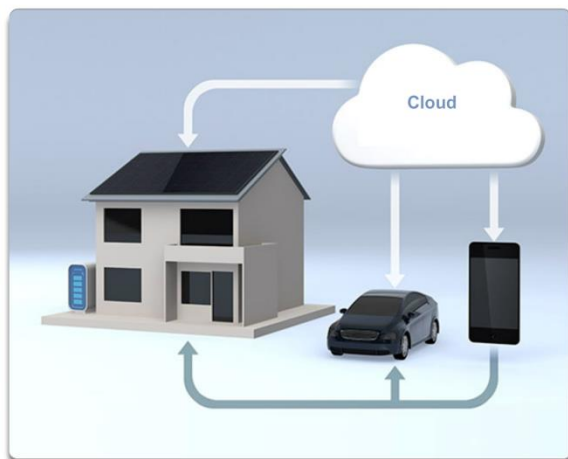
A modern adatközpontok teszik lehetővé, hogy a számítási felhő és a virtualizáció akár nagy méretű és tömeges adatátvitelt is hatékonyan tudjon kezelni.

A **virtualizáció** valamilyen erőforrás virtuális változatának a létrehozását jelenti, ami lehet egy hardver platform, operációs rendszer (OS), tárolóeszköz, vagy akár hálózati erőforrás is. Az adatközpontokat általában nagyon drága felépíteni és fenntartani. Emiatt csak a nagy szervezetek tehetik meg, hogy saját adatközpontot építsenek és nyújtsanak általuk szolgáltatásokat a felhasználóik számára.

Például egy nagy kórház rendelkezhet egy saját adatközponttal, amelyen az elektronikus betegnyilvántartási rendszere fut.

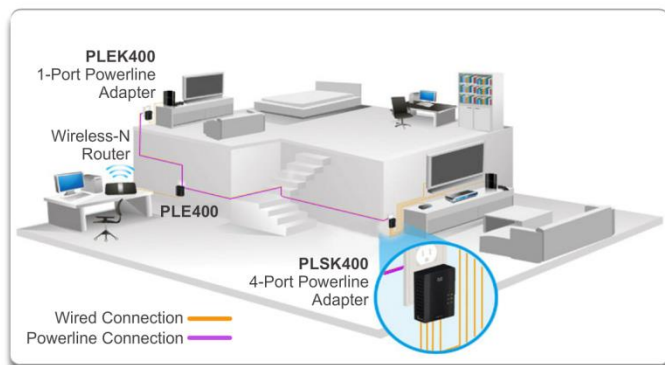
Technológiai trendek az otthonunkban

Smart Home Technology



"intelligens otthoni technológia,,: Az intelligens otthon technológiája egy olyan technológia, amely beépül a nap mint nap használt készülékeinkbe, lehetővé téve, hogy azok más eszközökkel kapcsolódjanak össze, ezáltal "intelligensebbé" vagy automatizáltabbá téve azokat. (hűtőszekrény, sütő, fűtési rendszer, stb ...)

Powerline Networking



powerlinenetwork: A már meglévő elektromos hálózatot használó adathálózat . Az adatkommunikáció és az áramellátás ugyanazt a vezetéket használja, csak a powerline hálózat az adatokat más frekvencián küldi, hasonlóan, mint ahogy azt a DSL-hálózatok teszik. A powerline hálózat különösen akkor hasznos, ha a vezeték nélküli hozzáférési pontok nem használhatóak, vagy nem tudjuk megoldani a kábelezést a házban.

Vezeték nélküli szélessávú hozzáférés

Wireless Broadband Service



Vezeték nélküli internetszolgáltató:

- A vezeték nélküli internetszolgáltató (Wireless Internet Service Provider, WISP) egy olyan szolgáltató, amely az otthoni WLAN hálózatokhoz hasonló technológiát alkalmazva csatlakoztatja az előfizetőket egy kijelölt hozzáférési ponthoz vagy hot spot-hoz. Az előfizető és az ISP közötti kapcsolat a fizikai kábel helyett vezeték nélküli átvitellel van megoldva. (ANet- Antenna Hungária)

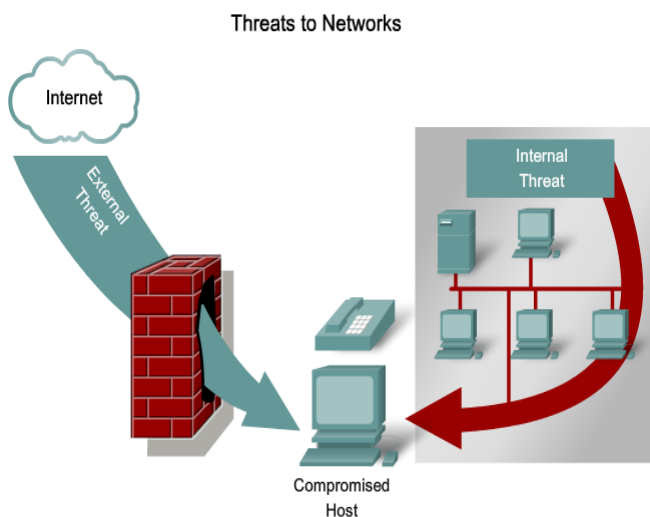
A vezeték nélküli szélessávú szolgáltatás:

- Az otthoni és kisvállalkozások számára egy másik vezeték nélküli megoldás a vezeték nélküli szélessávú hozzáférés. Ez ugyanazt a mobil technológiát használja az internet elérésre, mint egy okostelefon vagy egy tablet. A házon kívül egy antenna kerül telepítésre, amely a házon belüli eszközöknek vezeték nélküli vagy akár vezetékes csatlakozást is biztosíthat.

Hálózati biztonság

A biztonsági fenyegetések

Hálózati Biztonság: hálózat biztonságossá tétele és a fenyegetések kivédése speciális protokollok, technológiák, eszközök és technikák használatával érhető el. Napjainkban számos külső hálózati biztonsági fenyegetés terjed az interneten.



Vírusok, férgek és trójai lovak - rosszindulatú szoftverek vagy bármilyen kód elemek, amelyek egy felhasználói eszközön futnak.

Kémprogram- és reklámprogram (spyware és adware) - egy olyan telepített szoftver a felhasználó eszközén, amely titokban információkat gyűjt a felhasználóról.

Nulladik napi támadások, más néven nulladik órák támadások - a sebezhetőség felfedezésének első napján történő támadások.

Hacker támadások - egy hozzáértő személy által elindított támadás egy eszköz, vagy hálózati erőforrás ellen.

Szolgáltatásmegtagadási támadások (Denial of Service, DoS) - a támadások célja, hogy lelassítsanak, vagy elérhetetlenné tegyenek hálózati eszközön futó alkalmazásokat és folyamatokat.

Adatlehallgatás és a lopás - egy támadás, amelynek célja, hogy egy szervezet hálózatáról személyes információkhoz férjenek hozzá.

Személyazonosság-lopás - egy támadás, amely a személyes adatainkhoz használt felhasználói belépési azonosítók ellopására irányul. A leggyakoribb külső hálózati fenyegetések a következők:

Hálózati biztonság

Biztonsági megoldások

Számos tanulmány kimutatta, hogy az adatokkal történő visszaélések leggyakrabban a hálózat belső felhasználói miatt történnek. Ez az elvesztett vagy ellopott eszközöknek, az alkalmazottak véletlen visszaélésének, vagy üzleti környezetben akár még a rosszindulatú alkalmazottaknak is tulajdonítható.

Egyetlen **megoldás** nem képes megvédeni a hálózatot a különböző fenyegetésektől. A biztonságot emiatt több rétegben, több biztonsági megoldást is alkalmazva kell megvalósítani.

- *Egy otthoni vagy kisvállalati hálózatban* minimum a következő biztonsági elemeknek kell jelen lenniük:

Vírus-és kémprogramvédelem - a felhasználói eszközök rosszindulatú szoftverekkel szembeni védelme érdekében.

Tűzfal szűrés - hogy blokkolja a jogosulatlan hozzáférést a hálózathoz. Ez lehet egy munkaállomás alapú tűzfalrendszer, vagy az otthoni forgalomirányító.

- A nagyobb hálózatoknak és a vállalati hálózatoknak gyakran más biztonsági követelményeik vannak:

Dedikált tűzfalrendszerek - hogy a fejlettebb tűzfal képességek miatt az eszköz képes legyen akár jelentős mértékű forgalom mellett is részletesebb szűréseket végezni.

Hozzáférés-szabályozó listák (ACL) - szűrési feltételek a hozzáférésről és a forgalom továbbításáról.

Behatolás-megelőző és detektáló rendszerek (IPS/IDS IntrusionPrevention/Detection System) - azonosítani olyan gyorsan terjedő fenyegetéseket, mint például a nulladik napi vagy nulladik órás támadások, illetve detektálni azokat ha már megelőzni nem sikerült őket.

Virtuális magánhálózatok (Virtualprivatenetworks, VPN) - biztonságos hozzáférés kialakítása a távoli dolgozók részére.