**15. tétel**

**Hálózati ismeretek – Otthoni és kisvállalati hálózatok (3.1.1)**

Ismertesse a helyi hálózat fogalmát és jellemzőit! Mutassa be a helyi hálózatok jellemző hálózati eszközeit és azok hálózati feladatait! Beszéljen a helyi hálózatok szolgáltatásairól és mutassa be azok jellemzőit (egyenrangú, szerver-kliens)!

***Szempontok a tartalom rész értékeléséhez***

− A helyi hálózat fogalma. A helyi hálózat jellemzői: földrajzi kiterjedés, sebesség, menedzselés stb.

− A helyi hálózatok jellemző hálózati eszközei: kapcsoló, forgalomirányító, vezeték nélküli hozzáférési pont, integrált hálózati eszközök, tűzfalak

− A helyi hálózatok jellemző hálózati eszközeinek feladata: kapcsoló: OSI modell 2. réteg béli eszköz, kliensek és egyéb hálózati eszközök csatlakoztatása a hálózathoz, 2. réteg béli biztonsági funkciók

**forgalomirányító:** OSI modell 3. réteg béli eszköz, forgalomirányítási feladatok, hálózatok elkülönítése, forgalomszűrési feladatok, NAT, PAT megvalósítás stb.

**hozzáférési pont:** vezeték nélküli kliensek csatlakoztatása

**integrált eszközök:** kisebb hálózatok hálózati megoldása egy eszközben

**tűzfalak:** a hálózat külső és belső támadásokkal szembeni védelme, forgalomszűrési feladatok

− A helyi hálózatok szolgáltatásai: egyenrangú és szerver-kliensszolgáltatások (fájl- és nyomtatómegosztás, webszolgáltatás, elektronikus levelezés stb.)

Megjegyzés(NF): Nem értem mit keres helyi szolgáltatásoknál webszolgáltatás és elektronikus levelezés, ha valaki elmagyarázza mit keressek azt megköszönöm…

Hálózat típusai földrajzi kiterjedés szerint:

* Személyi hálózat (az angol **P**ersonal **A**rea **N**etwork alapján **PAN** hálózatok)
* Helyi hálózat (az angol **L**ocal **A**rea **N**etwork alapján elfogadott **LAN** hálózatok)
* Városi hálózat (az angol **M**etropolitan **A**rea **N**etwork alapján **MAN** hálózatok)
* Nagy kiterjedésű hálózat (az angol **W**ide **A**rea **N**etwork alapján **WAN** hálózatok)

**Helyi hálózat fogalma:**  
LAN = Local Area Network

Kis területen elhelyezkedő több, egymással kommunikáló számítógépet és egyéb hardver egységet tartalmazó rendszer.

***Előnyök***

**Közös erőforrás-használat:**  
a hálózati összeköttetés révén a gépek a hálózat egy másik gépének bármely erőforrását használhatják, mely elsősorban a szerveren lévő eszközökre vonatkozik. Ez irányulhat az egyes gépek, illetve a szerver(ek) háttértárolójára, továbbá a rendszer   
bármely munka-állomásához illesztett nyomtató használatára  
**Osztott háttértár használat:**   
az egyes userek, munkaállomások háttértárolóján lévő könyvtára(ka)t, alkönyvtárakat kijelölhetjük - megoszthatjuk - közös használatra. A megosztást a user tulajdonosa végezheti, sőt azt is meghatározhatja, hogy a melyik user, milyen jogokkal veheti igénybe a megosztott erőforrást. Még arra is lehetőség van, hogy a megosztott erőforrás fizikai helye rejtve maradjon, hiszen egy ún. megosztási névvel hivatkozunk az adott erőforrásra.  
**Nincs feltétlenül szükség önálló háttértárolóra:**  
mivel az egyébként önálló működésre képes gépeket egy központi gép irányítja (szerver), ezért a központi gép háttértárolóit a rendszer bármelyik munkaállomása használhatja.  
**Gyors adatátvitel:**   
az adatátvitel gyakorlatilag a floppy lemezen történő adattovábbítással kezdődött. Ehhez képest a hálózati adatforgalom rendkívül nagy lépés előre, hiszen a műveleti sebességek összehasonlíthatatlanul gyorsabbak a hálózaton.  
**Nagyobb teljesítmény:**   
az önállóan működő számítógépek összekötésével, azok egy közös rendszert alkotnak, így a rendelkezésre álló erőforrások összeadódnak, vagyis a teljes hálózat egyes gépein megosztott, hozzáférhetővé tett erőforrásainak összessége.  
**Több felhasználós adatbázis használat:**   
a számítógép hálózatok alkalmazásával lehetőség van bonyolult, több gépre telepített adatbázisok, egy időben, különböző munkaállomásokról történő használatára.

***Hátrányok:***

* A központi gép(ek) (szerverek) üzemzavara a munkaállomásokat is megbéníthatja
* Közös erőforrások kiesése egyszerre több munkahelyet érint
* Ipari kémkedéssel és szándékos károkozással kapcsolatos problémák
* Vírusvédelmi problémák

**A hálózat topológiája**

Topológián a hálózat alkotórészeinek összekapcsolási módját, fizikai elrendezését értjük. A számítógépek kábelezését néhány jellegzetes mértani formával szokás jellemezni, mint csillag, sín, gyűrű. Ennek megfelelően beszélhetünk csillag, sín, gyűrű, fa topológiákról.  
  
**Sín (bus):**  
Az állomások egyetlen közös használatú kábelre (gerincvezetékre, sínre) kapcsolódnak. A sín két végét a vissza-verődések elkerülése végett illesztve zárják le. Előnye az alacsony előállítási költség, de a sín meghibásodása az egész rendszert megbízhatatlanná teszi.  
  
**Csillag (star):**  
Minden állomás a kapcsoló központhoz vagy egy csillagelosztóhoz csatlakozik. Előnye, hogy minden állomás könnyen megcímezhető, és egy-egy állomás vagy kábelszakasz meghibásodása esetén nem omlik össze a hálózat. Hátránya, hogy az előállítási költsége viszonylag magas, bővítése nehézkes, és a hálózat a kapcsoló központ meghibásodása esetén használhatatlan.  
  
**Fa (tree):**  
Olyan hierarchikus csillaghálózatot jelent, amelyben az egyes állomások helyén újabb csillaghálózatok lehetnek. Előnye, hogy a hálózat terhelése megoszlik az alhálózatokat vezérlő számítógépek között, és ezek meghibásodása esetén csak a hozzájuk tartozó alhálózat válik használhatatlanná.  
  
**Gyűrű (ring):**  
Nincs gerincvezeték, mint a sín topológiánál, mert az állomások megszakítják a kábelt. Az egyes kábelszakaszok terhelése kiegyenlített, de az adatok továbbítása lassú, mert az adó és a vevő között az adatok valamennyi állomáson áthaladnak. Ha az adatok a gyűrűben csak egy irányban haladhatnak (ez a gyakoribb), akkor egy állomás meghibásodása az egész hálózatot használhatatlanná teheti.

**A helyi hálózat elemei**

**szerver (kiszolgáló) gépek:** általában nagy teljesítményű és tárolókapacitású, folyamatos üzemű számítógépek, amelyek a hálózatba kapcsolt többi gép számára szolgáltatásokat nyújtanak. Ezek a szolgáltatások különfélék lehetnek, sőt gyakran előfordul, hogy nem egy számítógépen koncentrálódnak, hanem a hálózatban több szerver található, egy vagy több saját funkcióval.

**kliens gépek:** (munkaállomások) valamely hálózati szolgáltatást vesznek igénybe.

**hálózati adapterkártyák:** kapcsolat az adatátviteli közeg és a PC között

**a hálózati protokollok:** Protokolloknak a számítástechnikában egy pontosan, sok esetben szabványban rögzített eljárást nevezünk. Leggyakrabban az adatátvitel szabályait nevezzük protokollnak. A hálózati protokollok feladata, hogy a számítógépek közt (a fizikai eszközök, például hálózati kártya, modem, stb. segítségével) az adatokat 1.) elküldje, ill. 2.) az adatok átvitelét ellenőrizze.

**modemek:** kapcsolat telefonvonalon keresztül két gép (vagy hálózat) között

**HUB:** elosztók, a kapott jelet a megfelelő címre továbbítja (pl.: csillag topológiánál)

**bridge:** a hálózati szegmensek összekapcsolására használják, fizikailag eltérő hálózatokra is. Minden hálózat üzenetét veszi, melynek tagja, és az információt a megfelelő hálózat megfelelő címére adja tovább. Csak egy híd lehet két hálózat között, mert az üzenetek esetleg sorrendhibásak lehetnek.

**repeater:** jelismétlők, nem eltérő hálózatok között, hanem a hálózat különböző szegmensei közötti kapcsolat fenntartására szolgálnak, így nagyobb hálózatokat lehet létrehozni. Konkrétan - a megkapott jelet felerősíti (helyreállítja) az eredeti szintre és továbbítja. Az összekötött szegmenseknek ugyanolyan típusúnak kell lenniük

**router:** forgalomirányítók, melyek (két hálózat között akár több is lehet) az azonos hálózati protokollt használó hálózatok csomópontjai közötti lehetséges útvonalak közül megpróbálják a legideálisabbat kiválasztani. Az elküldött üzenet rendelkezik a tényleges címmel és  fel van tüntetve az odavezető út címsorozata is. Ez a cím folyamatosan változik, ahogy az üzenet csomópontról csomópontra halad.

**Router Típusai:**

**Szolgáltatói (ISP – Internet Service Provider)**

Az internetre csatlakozást mindig valamilyen szolgáltatón keresztül lehet megvalósítani. A szolgáltatók által üzemeltetett hálózatokat és a szolgáltatókat magukat is routerek kötik össze, általában ezeket a hálózatokat nevezhetjük az internet gerincének.

**Vállalati, nagyvállalati**

A cégek és vállalkozások mai alapvető követelménye, hogy az internetre csatlakozzanak. Ehhez is routereket használnak, azonban nagyobb vállalatok esetében szükséges lehet a hálózat tagolása, akár logikailag adminisztratív szempontból, akár fizikailag elhatárolódott, országos vagy akár kontinens méretű kiterjedés esetén. Ebben az esetben a külön egységek külön helyi hálózatokkal (LAN) rendelkeznek, melyeket routerekkel lehet összekötni, így lehetővé téve a kommunikációt közöttük.

**SOHO (Small Office, Home Office), Otthoni Irodai (kisvállalati)**

Kisebb cégek illetve otthoni felhasználók Internetre való csatlakozásához használatosak ezen routerek, melyek teljesítménye is ennek megfelelően jóval kisebb. Alapvető feladatuk a belső, saját hálózat Internetre való csatlakoztatása. Egy 2013-as vizsgálat szerint a SOHO routerek nagy részének biztonsága hagy kívánnivalót maga után. A helyi hálózat felől mind a 13 vizsgált készülék feltörhető volt.

**gateway:** egymástól teljesen különböző hálózatok összekapcsolására használt rugalmas hálózati elem, melynél a protokollok is különbözhetnek a hálózati rétegekben. A gateway minden átalakítást (üzenet-, cím- és protokoll átalakítás) elvégez a két rendszer között.

**tűzfal:** A tűzfal megpróbálja a privát hálózatot megvédeni nem kívánt támadásoktól. Szabályozza a különböző megbízhatósági szintekkel rendelkező számítógép-hálózatok közti forgalmat. Tipikus példa erre az internet, ami semmilyen megbízhatósággal nem rendelkezik és egy belső hálózat, ami egy magasabb megbízhatósági szintű zóna. Egy közepes megbízhatósági szintű zóna az ún. „határhálózat” vagy demilitarizált zóna (DMZ), amit az internet és a megbízható belső hálózat között alakítanak ki. Megfelelő beállítás nélkül egy tűzfal gyakran értelmetlenné válik. A biztonsági szabványok „alapértelmezett-letiltás” tűzfal-szabálycsoportot határoznak meg, amelyben csakis azok a hálózatok vannak engedélyezve, amiket már külsőleg engedélyeztünk. Sajnos egy ilyen beállításhoz részletesen ismerni kell a hálózati eszközöket és azokat a végpontokat, amik a vállalat mindennapi működéséhez szükségesek. Sok vállalatnál hiányzik ez az ismeret, és ezért egy „alapértelmezett-engedélyezés” szabályt alkalmaznak, amiben minden forgalom engedélyezve van, amíg konkrétan nem blokkolják. Az ilyen beállítások kéretlen hálózati kapcsolatokat és rendszer veszélyeket okoznak. A szabálymegszegéseket leszámítva, egy tűzfal funkciója nem abból áll, hogy veszélyeket felismerjen és akadályozzon. Főleg abból áll, hogy a meghatározott kommunikációs kapcsolatokat engedélyezze, a forrás- vagy célcímek és a használt szolgáltatások alapján. A támadások felkutatásáért az ún. behatolás-felismerő rendszerek a felelősek, amelyet akár a tűzfalra is lehet telepíteni, de ezek nem tartoznak a tűzfalhoz.

**Csomagszűrés**

**(angolul *packet-filter firewall*)**

Az adatcsomagok egyszerű szűrése a cél-port, valamint forrás- és célcím, egy a tűzfal-adminisztrátor által már definiált szabályrendszer alapján történik. Ez minden hálózati-tűzfal alapfunkciója. A vizsgálat eredményeképp a csomagokat megsemmisíti vagy továbbítja. A fejlett tűzfalak csendben dobják el a csomagokat, azaz az érintett kapcsolat egyszerűen nem jön létre/megszakad, de nincs konkrét visszajelzés. Ez egy gyors és univerzális megoldás, viszont jelentős háttérismeretet, a hálózati és alkalmazási protokollok ismeretét igényli. Ez a tűzfalak leggyakrabban használt fajtája, ezekkel az alapvető szűrésekkel rendelkezik manapság a legtöbb router, és vállalati switchek.

### Állapot szerinti szűrés

Ez a csomagszűrés egy kibővített formája, ami a 7. OSI-rétegen egy rövid vizsgálatot hajt végre, hogy minden hálózati-csomagról egyfajta állapottáblát hozzon létre. Ezáltal felismeri ez a tűzfal a csomagok közti összefüggéseket és az aktív kapcsolathoz tartozó munkafolyamatokat leállíthatja. Így sikerül ennek felismerni egy kapcsolat felépítése után, hogy a belső kliens a külső célrendszerrel mikor kommunikál, és csak akkor engedélyezi a válaszadást. Amikor a célrendszer olyan adatokat küld, melyeket a belső kliens nem kért, akkor a tűzfal már önmaga blokkolja az átvitelt a kliens és a célrendszer között fennálló kapcsolatnál. Ez különbözteti meg ezt a tűzfalat egy szokásos csomagszűréstől. Egy proxy-val ellentétben a kapcsolat itt önmagában nem befolyásolt.

**Szolgáltatások**

**Fájlmegosztás** segítségével a hálózatban lévő fájlokat lehet a hálózat elemei között elérhetővé tenni.

**Nyomtatómegosztás** lehetőségét akkor válasszuk, ha szeretnénk egy olyan nyomtatót létrehozni, ami az adott hálózat összes gépéről elérhetővé szeretnénk tenni. 2 lehetőséget különböztetünk meg:

* PC-re kötött nyomtató esetén, csak akkor érjük el az adott eszközt, ha az adott PC is elérhető.
* Külön hálózati kártyával rendelkező nyomtató esetén, elég ha a nyomtató az adott hálózatban van, onnan bárki használatba veheti, aki csatlakozott ahhoz.

További linkek: <https://www2.akg.hu/info/erettsegi/szobeli/08.html>