SZÁMÍTÓGÉPES HÁLÓZATOK

Szabó Bálint – Márföldi Endre

MÉDIAINFORMATIKAI KIADVÁNYOK

SZÁMÍTÓGÉPES HÁLÓZATOK

Szabó Bálint – Márföldi Endre

Eger, 2011

Lektorálta:

CleverBoard Interaktív Eszközöket és Megoldásokat Forgalmazó és Szolgáltató Kft.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Felelős kiadó: dr. Kis-Tóth Lajos
Készült: az Eszterházy Károly Főiskola nyomdájában, Egerben
Vezető: Kérészy László
Műszaki szerkesztő: Nagy Sándorné

Kurzusmegosztás elvén (OCW) alapuló informatikai curriculum és SCORM kompatibilis tananyag-fejlesztés Informatikus könyvtáros BA, MA lineáris képzésszerkezetben
TÁMOP-4.1.2-08/1/A-2009-0005

Tartalom

1. Bevezetés 10
1.1 Célkitűzés 10
1.2 A kurzus tartalma 11
1.3 Kompetenciák és követelmények 11
1.4 Tanulási tanácsok, tudnivalók 11
2. hálózati alapismeretek 12
2.1 Célkitűzés 12
2.2 A lecke témakörei 12
2.3 A számítógépes hálózat 12
2.3.1 A számítógépes hálózat fogalma 12
2.3.2 Hálózatok és operációs rendszerek 13
2.3.3 A hálózatok alkalmazásának előnyei 13
2.3.4 A hálózatok alkalmazásának hátrányai 14
2.3.5 A hálózatok csoportosítása 14
2.3.5.1 Kiterjedés szerinti csoportosítás 15
2.3.5.2 Hálózati topológia szerinti csoportosítás 16
2.3.5.3 Erőforrásokhoz való hozzáférés módja szerinti csoportosítás 20
2.3.5.4 Nyilvánosság szerinti csoportosítás 21
2.3.5.5 Az adattovábbítás módja szerinti csoportosítás 21
2.3.5.6 Közeghozzáférési mód szerinti csoportosítás 22
2.3.5.7 Az átviteli módszer alapján történő csoportosítás 23
2.3.5.8 Kommunikáció iránya szerinti csoportosítás 23
2.3.6 A hálózatok egyéb jellemzői 24
2.4 Összefoglalás 25
2.5 Önellenőrző kérdések 25
3. A hálózati architektúrák 27
3.1 Célkitűzés 27
3.2 A lecke témakörei 27
3.3 A hálózati feladatok 27
3.3.1 A hálózati feladatok rétegekre osztása 27
3.3.2 Hálózati protokollok, architektúrák 28
3.3.3 Hálózati szabványok 28
3.3.4 Az OSI modell 29
3.3.5 A TCP/IP modell 31
3.3.6 Beágyazás (Encapsulation) 33
3.3.7 Az Ethernet 33
3.3.8 Az Ethernet keretek felépítése 34
3.4 Összefoglalás 35
3.5 Önellenőrző kérdések 36
4. hálózati eszközök 37
4.1 Célkitűzés 37

4.2 Tartalom 37
4.3 Hálózati eszközök 37
4.3.1 Az aktív és passzív eszközök 37
4.3.2 A hálózati kártya 38
4.3.3 A repeater 38
4.3.4 A hub 39
4.3.5 A bridge 39
4.3.6 Switch 40
4.3.7 A router 40
4.3.8 Gateway 41
4.3.9 Az Acces Point 41
4.3.10 Az UTP 41
4.3.11 Optikai kábelek 42
4.4 Összefoglalás 44
4.5 Önellenőrző kérdések 45

5. Az internet működése 46
5.1 Célkitűzés 46
5.2 Tartalom 46
5.3 Az internet 46
5.3.1 Az internet története 46
5.3.2 Az internet és a TCP/IP kapcsolata 49
5.3.3 Az internet működése 50
5.3.4 Az IP címek 51
5.3.5 Az IPv4 51
Különlegességek az IPv4-ben 53
5.3.6 IPv6 53
Különlegességek az IPv6-ban 54
5.3.7 Az IPv6 előnyei az IPv4-hez képest 54
5.3.8 Kompatibilitás 55
5.3.9 Az internet szállítási protokolljai 55
5.3.10 Az internet vezérlő protokolljai 56
5.4 Összefoglalás 56
5.5 Önellenőrző kérdések 58

6. Irodai hálózat, otthoni hálózat 59
6.1 Célkitűzés 59
6.2 Tartalom 59
6.3 Az internet kapcsolat megosztása és annak eszközei 59
6.3.1 A DSL-kapcsolatok 59
6.3.2 Kábelmodemes kapcsolatok 60
6.3.3 A SOHO switchek 61
6.3.4 A routerek 61
6.3.5 Vezeték nélküli eszközök 62
6.3.6 A vezeték nélküli hálózatok biztonsága 63
6.3.7 Tűzfalak 64

6.3.8 VPN és más kiegészítő szolgáltatások a routerekben 65
6.4 Összefoglalás 66
6.5 Önellenőrző kérdések 67

7. A Domain Name System 69
7.1 Célkitűzés 69
7.2 A lecke témakörei 69
7.3 Szolgáltatások az interneten 69
7.3.1 A szerver 70
7.3.2 A kliens 70
7.3.3 A protokoll 70
7.4 Az IP címek és gépnevek használata, névfeloldás 71
7.5 A Domain Name System 72
7.6 A Domain Name Service 74
7.7 A DNS IP címének megadása 75
7.8 Szervezetek domain neveinek kiosztása 75
7.9 Összefoglalás 76
7.10 Önellenőrző kérdések 76

8. Telnet, SSH, Távoli asztal 77
8.1 Célkitűzés 77
8.2 A lecke témakörei 77
8.3 A Telnet szolgáltatás 77
8.3.1 A Telnet használatának feltételei 78
8.3.2 A Telnet szolgáltatás lehetőségei 78
8.3.3 Gépek távoli vezérlése a Telnet kapcsolattal 79
8.4 Biztonságos kommunikáció 80
8.4.1 A biztonságos kommunikáció alapelvei 80
8.4.2 Nyilvános kulcsú kódolás 81
8.5 Az SSH 82
8.5.1 Az SSH használatának feltételei 82
8.5.2 Az SSH kapcsolat 82
8.6 A távoli asztal 83
8.6.1 A Távoli asztal lehetőségei 83
8.6.2 A Távoli asztal szolgáltatás használatának feltételei 84
8.6.3 A Távoli asztal kapcsolat felépítése 84
8.7 Összefoglalás 85
8.8 Önellenőrző kérdések 85

9. Az FTP szolgáltatás 86
9.1 Célkitűzés 86
9.2 A lecke témakörei 86
9.3 Az FTP szolgáltatás 86
9.4 Kapcsolat az ügyfél és a kiszolgáló között 87
9.5 Az FTP használatának feltételei: 88
9.6 Jogosultságok 88
9.7 Ftp kliensek 88

9.8 Munka karakteres FPT klienssel 88
9.8.1 A kliens indítása, bezárása 89
9.8.2 Kapcsolat kialakítása, bejelentkezés 89
9.8.3 Az átviteli mód beállítása 90
9.8.4 Könyvtár tartalomjegyzékének megtekintése 90
9.8.5 Fájlok átvitele 91
9.8.6 Néhány egyéb hasznos parancs 92
9.8.7 A kapcsolat bontása 92
9.9 A biztonságos FTP 92
9.10 Grafikus felületű FTP ügyfelek 93
9.10.1 Kapcsolódás az FTP szerverhez 93
9.10.2 Fájlok átvitele 93
9.10.3 Kapcsolat bontása 93
9.11 Összefoglalás 94
9.12 Önellenőrző kérdések 94

10. Az elektronikus levelezés 95

10.1 Célkitűzés 95
10.2 A lecke témakörei 95
10.3 Az elektronikus levelezés lehetőségei 95
10.4 Az elektronikus levelezés címezési rendszere 96
10.5 Az elektronikus levelezés működése 96
10.6 Az elektronikus levelezés feltételei 98
10.7 Az elektronikus levél felépítése 98
10.8 Elektronikus levelezés különböző hálózatokból 99
10.8.1 Levél küldése a szolgáltató SMTP szerverével 100
10.8.2 Levél küldése tunnelinggel 100
10.8.3 Jelszóval védett SMTP szerver 101
10.9 Az elektronikus levelező kliensek szolgáltatásai 101
10.9.1 Konfigurálhatóság 101
10.9.2 Levelek írása, elküldése, letöltése 101
10.9.3 Archiválás 102
10.9.4 Levelezési szabályok 102
10.10 Levelezés és biztonság 102
10.10.1 Informatikai támadások 102
10.10.2 Hogyan védekezzünk? 102
10.11 Összefoglalás 103
10.12 Önellenőrző kérdések 104

11. A World Wide Web 105

11.1 Célkitűzés 105
11.2 A lecke témakörei 105
11.3 A WWW története 106
11.3.1 A World Wide Web születése 106
11.3.2 A World Wide Web 106
11.3.3 A WWW korszakai 107

11.4 A WWW elemei 108
11.4.1 Webszerver 108
11.5 Statikus és dinamikus weblapok 112
11.6 Összefoglalás 112
11.7 Önellenőrző kérdések 113

12. Összefoglalás 114

12.1 A kurzusban kitűzött célok összefoglalása 114
12.2 A tananyagban tanultak részletes összefoglalása 114
12.2.1 Hálózati alapismeretek 114
12.2.2 Hálózati architektúrák 114
12.2.3 Hálózati eszközök 114
12.2.4 Az Internet működése 114
12.2.5 Irodai és otthoni hálózatok 115
12.2.6 A Domain Name System 115
12.2.7 Telnet, SSH, Távoli asztal 115
12.2.8 Az FTP szolgáltatás 115
12.2.9 Az elektronikus levelezés 115
12.2.10 A World Wide Web 115

13. Kiegészítések 116

13.1 Irodalomjegyzék 116
13.1.1 Könyv 116
13.1.2 Elektronikus dokumentumok / források 116

14. Ábrajegyzék 117

15. Médiaelemek 118

16. Tesztek 120

16.1 Próbateszt 120
16.2 Záróteszt A. 122
16.3 Záróteszt B. 124
16.4 Záróteszt C. 127

1. BEVEZETÉS

A sci-fi műfaja megosztja az olvasást kedvelők táborát. Vannak, akik szeretik, sőt olvasmányaik nagy részét e körből választják, míg mások inkább csak mosolyognak rajta. Akár egyik akár másik táborhoz tartozunk is, Isaak Asimovnak, a tudományos fantasztikus irodalom egyik klasszikusának nevét valószínűleg hallottuk már. Asimov az „Alapítvány és Föld" c. regényében olvashatunk a Gaia nevű bolygóról, ahol az emberek különös módon élnek. Tudatuk nem egymástól független lények idegrendszerének elszigetelt termékeként működik, hanem egy egységes, az egész homo-szféráját behálózó, elsöprő erejű, tudású, és akaratú lélekké egyesül. Minden ember éli saját autonóm életét, érzékel, érez, tapasztal, tanul, szeret, vagy gyűlöl. Egyéni élete, tapasztalásai, megszerzett tudása azonban részévé válik egy globális szellemi erőnek, amely magasabb szinten, működik, értékel, dönt és a bolygónyi tudat érdekeit figyelembe véve irányít.

Ha olvastuk az említett könyvet, valószínűleg megegyezik majd a véleményünk abban, hogy Gaia élete egyszerre fenséges és egyszerre hátborzongatóan taszító. Csodálatos, hiszen az egyes bolygólakók szellemi erejét megsokszorozva olyan tudat jön létre, amelynek ereje úgy mérhető az egyén tudatához, mint az emberi agy működése egyetlen emberi idegsejt erejéhez. Elborzasztó azonban abban az értelemben, hogy az autonomitást, az önállóságot, a szabad döntést háttérbe szorítva az egyént, a globális tudat érdekei alá rendeli.

Asimov vízióján most, a Web 2.0 korszak delén, a Web 3.0, és 4.0 hajnalán elgondolkodva rádöbbenünk, hogy nem csak azt nem látjuk, mi felé tartunk, hanem sokszor az sem teljesen világos mi vesz körül már most bennünket.

Tudjuk-e miként lehetséges, hogy egy új-zélandi szerveren tárolt weblap szövege és képei másodpercek alatt megjelennek képernyőnkön. Belegondoltunk-e, hogyan lehet, hogy bár ugyanazon a tengeralatti kábelen, amin az említett oldal bájtjai érkeznek, még milliónyi fájl, e-mail, MSN üzenet, és egyéb adat halad a nap minden egyes másodpercében, mégis minden bit pontosan eljut címzettjéhez.

Ismerjük-e annak az informatikai rendszernek a működését, amelyről Bill Gates azt mondta, hogy jelenlegi állapotát, képességeit a Ford T-modellhez hasonlíthatjuk, azaz elkövetkező néhány év olyan hatalmas fejlődést idéz majd elő, mint amekkora a T-modell és egy mai, F1-es versenyautó között mérhető le? Ha ez a fejlődés valóban ilyen dinamikusnak mutatkozik, akkor nem tehetjük meg, hogy nem foglalkozunk a hálózatokkal, különben az élet versenyautója elszáguld mellettünk, mi pedig a múlt szomorúan groteszk mementójaként álldogálunk majd tovább az információs szupersztráda szélén.

Tananyagunkban arra vállalkozunk, hogy megismertetjük az olvasót e fantasztikus világ működésével.

1.1 CÉLKITŰZÉS

Tananyagunk célja, hogy az olvasó megismerkedjen a hálózati alapfogalmakkal, megismerje a hálózati adatcsere feladatrendszerének rétegeit, megértse a hálózati architektúra jelentését.

Könyvünk áttanulmányozása után Ön tisztában lesz a számítógépes hálózatok felépítésének és osztályozásának legfontosabb fogalmaival, a hálózatok ismérveivel. Megismeri a számítógép hálózatok előnyeit, képes lesz a hálózati ismeretek gyakorlati alkalmazására.

Meg fogja ismerni napjaink legelterjedtebb hálózati architektúráját, a TCP/IP-t, és annak legfontosabb szolgáltatásait.

1.2 A KURZUS TARTALMA

1. Hálózati alapismeretek
2. Hálózati architektúrák
3. Hálózati eszközök
4. Az Internet működése
5. Irodai és otthoni hálózatok
6. A Domain Name System
7. Telnet, SSH, Távoli asztal
8. Az FTP szolgáltatás
9. Az elektronikus levelezés
10. A World Wide Web

1.3 KOMPETENCIÁK ÉS KÖVETELMÉNYEK

A tananyag elsajátítása után Önnek ismernie kell, és helyesen kell használnia a hálózati alapfogalmakat. A legfontosabb ismérvek alapján képesnek kell lennie hálózattípusok elkülönítésére, meg kell ismernie a hálózati architektúrákra jellemző rétegek, protokollok, és entitások fontosságát. Meg kell értenie a TCP/IP architektúra fölépítését, tisztában kell lennie az IP alapú hálózatok csomagirányításával.

Meg kell ismernie az internet címzési rendszereit, illetve a Telnet, az SSH, e-mail, FTP, és a WWW szolgáltatások működését. Képesnek kell lennie az alapvető internet-szolgáltatások használatára.

1.4 TANULÁSI TANÁCSOK, TUDNIVALÓK

A könyv 10 leckéje felöleli mindazokat az ismereteket, amelyekre Önnek szüksége van. A leckék nem csupán száraz tananyagot tartalmaznak, hanem megpróbálnak együttgondolkodni az olvasóval. Problémákat, kérdéseket vetnek fel, példákat mutatnak be, feladatokat fogalmaznak meg. Minden lecke végén önellenőrző kérdések segítik az olvasót abban, hogy felmérje saját tudását. Kérjük, alaposan olvasson el mindent, kövesse a könyv tanácsait, próbáljon válaszokat keresni a felvetett és az önmaga által megfogalmazott kérdésekre.

2. HÁLÓZATI ALAPISMERETEK

2.1 CÉLKITŰZÉS

Kezdetben a számológépek és a korai számítógépek közötti utasítások továbbítását maguk az emberek végezték. Napjainkban, miközben az internetet használva végezzük munkánkat, napi gyakorlattá válik a hálózatok, a hálózati szolgáltatások növekvő méretű használata. Ebben a leckében megismerheti a számítógépes hálózat felépítését, fogalmát. Megtudhatja miért előnyös a használata, és milyen szempontok alapján csoportosíthatja, valamint megismerkedhet legfontosabb jellemzőivel.

2.2 A LECKE TÉMAKÖREI

- A számítógépes hálózat fogalma
- A hálózatok építőelemei, felépítése
- Az operációs rendszerek és hálózatok kapcsolata
- Az alkalmazásának előnyei
- Csoportosítása
- Lényeges jellemzői

2.3 A SZÁMÍTÓGÉPES HÁLÓZAT

Arról, hogy mi is a számítógépes hálózat, természetesen minden kedves olvasónak van elképzelése. Sejtjük, hogy itt számítógépek egymással való összekapcsolásával kialakított rendszerről van szó. Ha azonban pontosan szeretnénk meghatározni a hálózat fogalmát, akkor definíciónkban pontosabban kell fogalmaznunk.

2.3.1 A számítógépes hálózat fogalma

Az informatika robbanásszerű fejlődése a számítógépek elterjedésével és a felhasználók számának gyors növekedésével járt együtt. A számítógépek összekötése iránti igény először akkor merült fel, amikor egyes csoportok ugyanazt a háttértárolót, nyomtatót, adatbázist vagy programot közösen szerették volna használni. Ehhez a számítógépek fizikai összekapcsolására volt szükség, valamint néhány olyan gépre, amely rendelkezett ezekkel az erőforrásokkal, és így ezeket a csoport minden tagja ugyanolyan formában tudta használni.

A felhasználók igényei egyre nőttek. Lehetővé kellett tenni az üzenetek, elektronikus levelek, valamint nagy mennyiségű adat gyors és megbízható továbbítását akár nagy távolságok között is. Ugyancsak célszerűnek látszott a drága szuperszámítógépek kapacitását megosztani, hogy ne csak a rákapcsolt gépekről lehessen őket használni, hanem megfelelő jogosultság esetén a világ távoli pontjairól is hozzájuk lehessen férni. Ezek ismét a számítógép-hálózatok kialakítását tették szükségessé.

Ezek után tisztázzuk a számítógépes hálózat fogalmát:

A hálózatok önállóan is működőképes számítógépek elektronikus összekapcsolása, ahol az egyes gépek külső beavatkozás nélkül képesek kommunikációra.

A számítógépes hálózat olyan függőségben lévő vagy független számítógépek egymással összekapcsolt együttese, amelyek abból a célból kommunikálnak egymással, hogy bizonyos erőforrásokon osztozkodhassanak, egymásnak üzeneteket küldhessenek, illetve terhelésmegosztást vagy megbízhatóság-növekedést érjenek el.

2.3.2 Hálózatok és operációs rendszerek

A hálózatok általános felépítése kapcsán feltétlenül meg kell említenünk, hogy a fenti feltételek megléte még nem elegendő ahhoz, hogy a fizikailag kialakított hálózat „lélegezni kezdjen" azaz szolgáltatásokat nyújtson. A számítógép-hálózat használatát olyan programok biztosítják, amelyek a meglévő fizikai lehetőségek felhasználásával, képesek egymással kommunikálni. Napjaink operációs rendszerei beépített hálózatkezelési lehetőséggel rendelkeznek.

2.3.3 A hálózatok alkalmazásának előnyei

Amennyiben a kedves olvasónak már volt szerencséje hálózatos környezetben dolgozni, minden bizonnyal tapasztalta azokat a lehetőségeket, amelyeket a hálózat alkalmazásával kihasználhatunk. Gondoljunk csak az egy iroda több gépét kiszolgáló nyomtatóra, vagy az elektronikus levelezésre. Jelen fejezetben a hálózatok nyújtotta lehetőségeket, előnyöket foglaljuk össze.

1. **Erőforrás-megosztás** Az erőforrás-megosztás fogalmának megértéséhez először is lássuk, mit értünk erőforrás alatt. Az informatikában az erőforrás egy rendszer olyan összetevőjét jelenti, amely a rendszer teljesítményét, szolgáltatásait, lehetőségeit meghatározza. Egy számítógép esetén beszélhetünk hardver és szoftver erőforrásokról. Előbbiek közé olyan hardverelemek tartoznak, mint például a processzor, a memóriák, a háttértárak, nyomtatók, kommunikációs eszközök. Ezek mind jelentősen meghatározzák egy számítógép teljesítményét. Hajlamosak vagyunk az erőforrás fogalmát ezekre a hardver erőforrásokra leszűkíteni. Fontos azonban tudni, hogy a hardveres összetevőkön kívül a gép által felhasználható különböző szoftvereknek is fontos szerepük van a teljesítmény és a képességek meghatározásában.

   A számítógép-hálózatba kötött gépek a hálózat segítségével képesek lehetnek arra, hogy saját erőforrásaikat a hálózat más gépei számára is elérhetővé, használhatóvá tegyék.

Ha nem egészen világos előttünk, hogy milyen jelentősége van az erőforrás-megosztásnak, gondoljunk a nyomtatóra, mint erőforrásra. Tegyük fel, hogy egy kisebb irodában dolgozunk, ahol több számítógép helyezkedik el. Minden gépen keletkeznek nyomtatási munkák. Ha lehetővé akarjuk tenni, hogy bármelyik gép felhasználója tudjon nyomtatni, akkor minden géphez külön-külön nyomtatót kell vásárolnunk. Ha azonban számítógépeink hálózatot alkotnak, akkor elég egyetlen géphez nyomtatót vásárolni, majd osztott erőforrássá tenni azt. Ezzel lehetővé válik, hogy több gép használhassa ugyan azt a nyomtatót.

2. **Költségkímélés:** Ez a lehetőség egyenesen következik az erőforrás-megosztásból. Ha elég egyetlen nyomtatót vásárolnunk a hálózat minden gépének kiszolgálására, akkor gépenként megtakarítjuk egy nyomtató árát. Hálózat alkalmazásával tehát

elegendő a megosztható erőforrásokat kis példányszámban megvásárolni, majd azokat osztott erőforrásként több más gép számára használhatóvá tenni.

3. **Osztott munkavégzés:** A költségkíméléshez hasonlóan az osztott munkavégzés lehetősége is az erőforrás-megosztáson alapszik. A hálózatokon fájlok, adatbázisok is megoszthatók. Egy adatbázis megosztásával lehetővé tehető, hogy többen dolgozzanak egyazon adatbázis tábláinak, rekordjainak kezelésén, azaz ugyanazt a munkát többen végezzék. Ilyenkor osztott munkavégzésről beszélünk.
4. **Adatvédelem:** A hálózati szoftver képes az egyes felhasználók megkülönböztetésére (felhasználónévvel és jelszóval) és ennek függvényében az adatokhoz való hozzáférés differenciálására. (Például egy iskolában nem lenne jó, ha a diákok hozzáférnének a tanár által megírt, a hálózaton tárolt dolgozati kérdésekhez.)
5. **Megbízhatóság, biztonság:** Minden állomány két vagy több gépen is jelen lehet, így ha pl. hardverhiba következtében valamelyik állomány elérhetetlenné válik az egyik gépen, akkor annak másolata egy másik gépen még hozzáférhető marad. Egyszerre több CPU (központi egység) alkalmazása is növelheti a megbízhatóságot. Az egyik CPU leállása esetén a többi még átveheti a kiesőre jutó feladatokat, így a teljes rendszer üzemképes marad (bár csökken a teljesítmény). A működés folyamatos fenntartása kulcsfontosságú a katonai, banki, a légi irányítási és más egyéb alkalmazások esetén is.
6. **Kommunikáció:** Napjaink egyik legszélesebb körben használt hálózata az Internet, amely számos szolgáltatást biztosít felhasználói számára. Ezen szolgáltatások többsége a számítógépek mellett ülők adatcseréjét, ismeretek átadását, és átvételét, azaz a kommunikációt teszi lehetővé. Sokan felróják, hogy a számítógép elidegeníti egymástól az embereket, interakcióik beszűkülését, egyfajta virtuális világba való menekülést eredményez. Nos a számítógép-hálózatok nyújtotta kommunikációs lehetőségek, és azok egyre szélesebb körben történő elterjedése látványos cáfolata ezen véleményeknek.

2.3.4 A hálózatok alkalmazásának hátrányai

A számítógépes hálózatok gyors elterjedése az előnyös tulajdonságok mellett hátrányokat is hordozhatnak.

1. **Illetéktelen hozzáférés:** Az adatokat olyanokkal is megoszthatjuk, akikkel nem szeretnénk. (Például bankszámlához való hozzáférés, kódfeltörések, személyes adatokkal való visszaélés, ipari kémkedés stb.)
2. **Vírusok gyorsabb elterjedése:** A gyors adatátvitel és kommunikáció révén a vírusok gyorsabban megfertőzhetik a hálózatba kötött gépeket, így nagyobb veszélyben vannak a gépek és a rajtuk tárolt adatok.
3. **Kommunikációs problémák:** felléphetnek olyan kommunikációs akadályok is, amelyek teljesen megbéníthatják a rendszer működését.

2.3.5 A hálózatok csoportosítása

Az előző szakaszokban azokat a tulajdonságokat vizsgáltuk meg, amelyek minden hálózatra egyaránt jellemzőek. Most arra keresünk választ, hogy melyek azok a tulajdonsá-

gok, amelyek alapján csoportokba sorolhatjuk a számítógép-hálózatokat. Felállítjuk azokat a kategóriákat, amelyek segítenek majd abban, hogy megismerjük és megértsük az általunk használt vagy egy újonnan megismert hálózat működését.

2.3.5.1 Kiterjedés szerinti csoportosítás

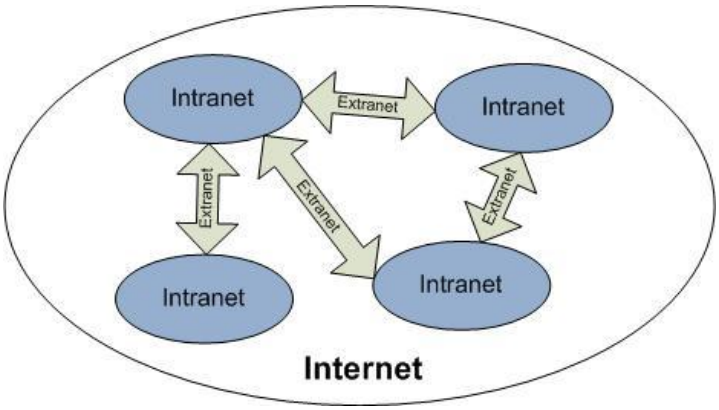
A számítógép-hálózat általában egy térben jó körülhatárolható területen elhelyezkedő gépeket köt össze. Amikor a hálózat kiterjedéséről beszélünk, akkor valójában azt fogalmazzuk meg, hogy mekkora területen helyezkednek el az egymással összekapcsolt hostok. Kiterjedés alapján három csoportot állíthatunk fel.

1. **LAN** (Local Area Network)**:** E kategóriába a legkisebb hálózatok tartoznak. A hálózat által összekapcsolt hostok[1] egy teremben, vagy egy épület helyiségeiben, esetleg egymástól néhány kilométernyi távolságra helyezkednek el.
2. **MAN** (Metropolitan Area Network)**:** A nagyvárosi hálózat méretét az elnevezés is sugallja. Általában néhány tíz kilométeres sugarú körben elhelyezkedő hálózatok.
3. **WAN** (Wide Area Network)**:** A széles vagy nagykiterjedésű hálózatok csoportja. Olyan hálózatok tartoznak ide, amelyek több, esetleg eltérő földrészeken elhelyezkedő ország gépeit kapcsolják hálózatba. Kiterjedése pár kilométertől kezdve az egész Földre is kiterjedhet. Jobbára több szervezet birtokában van.
4. **GAN** (Global Area Network): Az egész világot átölelő hálózat.

A hálózatok kiterjedtségével kapcsolatban gyakran használatosak még az alábbi elnevezések és fogalmak is:

1. **Internet:** az egész Földet átfogó hálózat, mint ilyen a WAN-ok közé tartozik
2. **Intranet:** internetes technológiát alkalmazó zárt, kisebb kiterjedésű (általában vállalati) hálózatok. Az intranetek hozzáférhetővé teszik az arra felhatalmazott felhasználók számára a szervezet belső LAN-ját. Az intranetes webkiszolgálók abban különböznek a nyilvános webkiszolgálóktól, hogy kívülállók csak a szükséges engedélyek és jelszavak birtokában érhetik el.
3. **Extranet:** Az intézményi intraneteket szabályozottan – azaz megfelelő hozzáférési-biztonsági megszorításokkal – összekapcsoló hálózatszakaszok. Két vagy több intranet stratégiai kiterjesztése, amely biztonságos kommunikációt tesz lehetővé a résztvevő vállalatok és intraneteik között. A hozzáférés általában jelszavakkal, felhasználó-azonosítókkal, illetve egyéb, alkalmazási szintű biztonsági funkciókkal valósul meg.

[1] A kifejezés egy olyan végfelhasználói számítógépet jelöl, amely a hálózathoz csatlakozik, és a felhasználók számára különböző adatszolgáltatásokat nyújt, illetve vezérlési feladatokat is ellát. A gazdagép az Interneten egy adattovábbítás végpontjaként szerepelhet, ez lehet személyi számítógép, munkaállomás vagy nagyszámítógép.



1. ábra Az internet intranet extranet viszonya

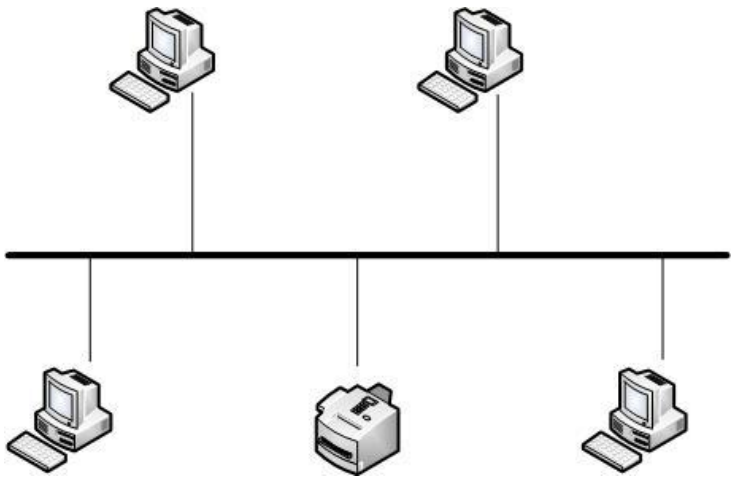
2.3.5.2 Hálózati topológia szerinti csoportosítás

A számítógép-hálózatokban a hostok és az azokat összekötő kommunikációs csatornák kapcsolódásának rendszerét topológiának nevezzük.

A topológia egyik összetevője a fizikai topológia, amely a vezeték vagy az átviteli közeg tényleges elrendezése. A másik része a logikai topológia, amely azt határozza meg, hogy hogyan érik el az állomások az átviteli közeget adatküldés céljából.

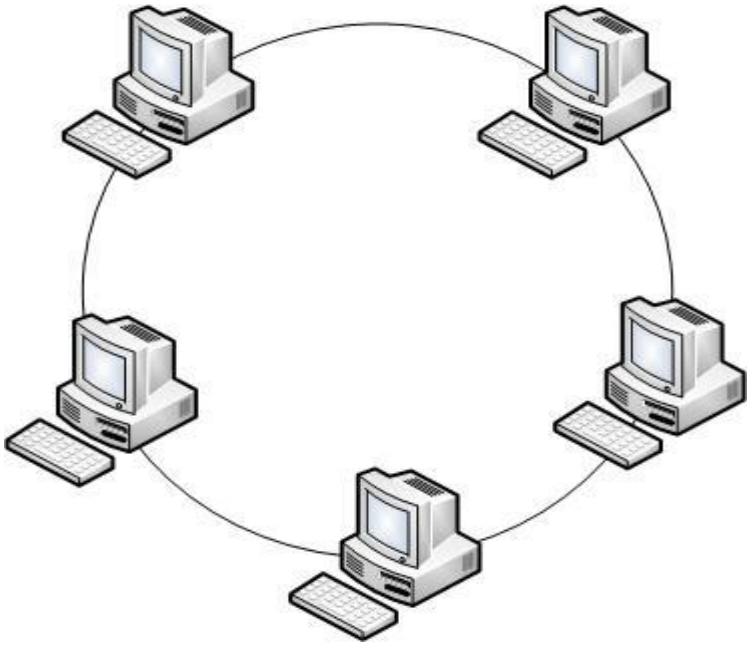
A következők a leggyakoribb fizikai topológiák:

1. A busz topológiában egyetlen, mindkét végén lezárt gerinckábelt használnak. Minden állomás közvetlenül ehhez a gerinchez kapcsolódik.



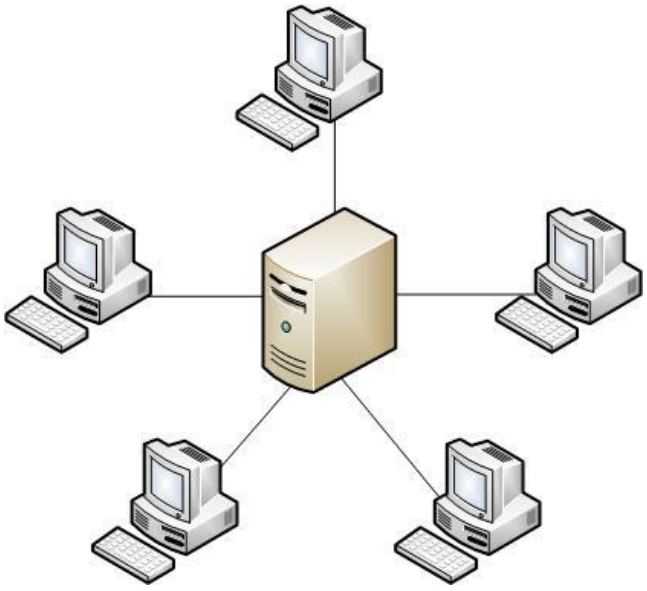
2. ábra A busz topológia

2. A gyűrű topológiában minden állomás a következőhöz csatlakozik, az utolsó pedig az elsőhöz. Ezzel a kábel fizikailag gyűrűt formál.



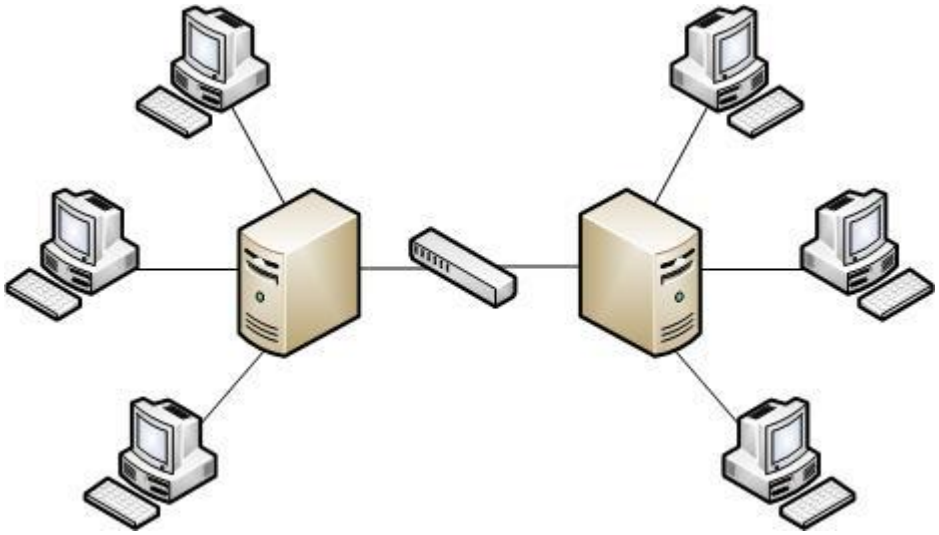
3. ábra A gyűrű topológia

3. A csillag topológiában minden kábel egy centrális ponthoz csatlakozik.



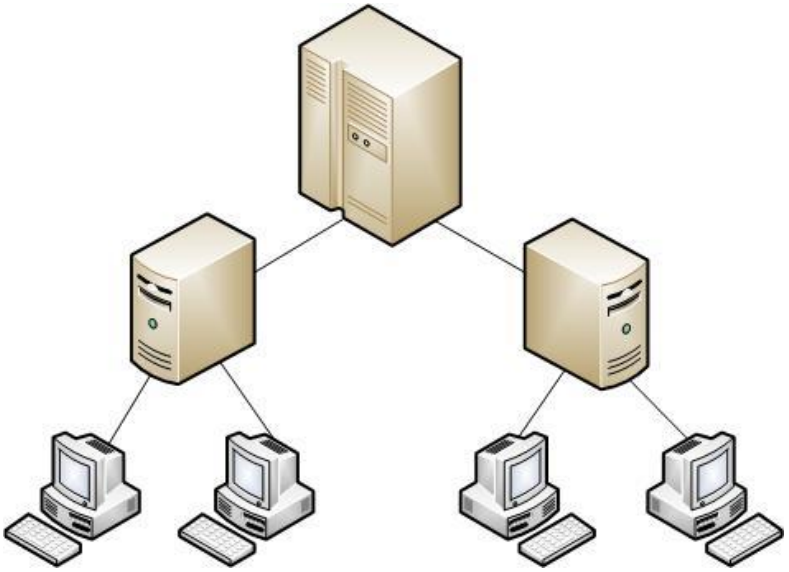
4. ábra A csillag topológia

4. A kibővített csillag topológiában az egyes csillagok hubok vagy a kapcsolók összekapcsolásával vannak összekötve. Ezzel a topológiával kiterjeszthető a hálózat hatóköre és a lefedettség mértéke.



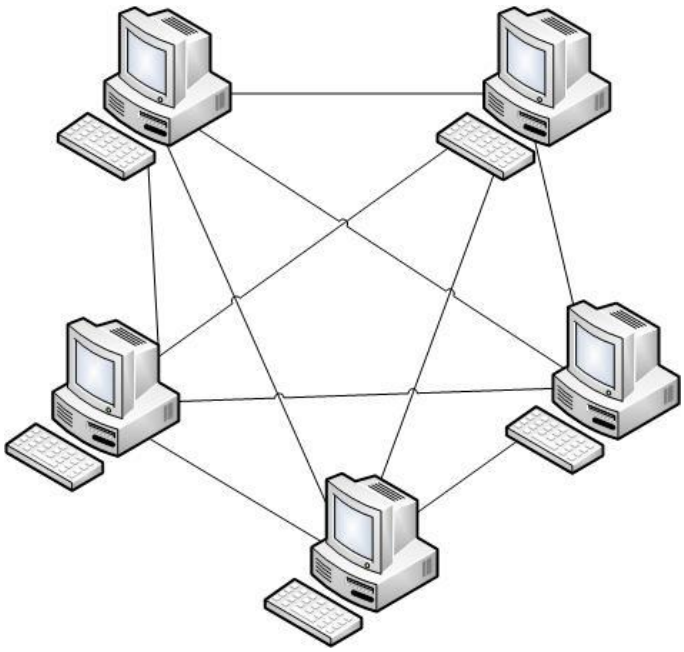
5. ábra A kibővített csillag topológia

5. A fa (tree) vagy hierarchikus topológia hasonlít a kibővített csillagra. Ebben azonban nem a hubok vagy a kapcsolók vannak összekötve, hanem a rendszer egy számítógéphez csatlakozik, amely vezérli a topológián belül zajló forgalmat. Bármely két összekötött gép között egy és csak egy útvonal van.



6. ábra A fa topológia

6. A háló topológiát akkor szokás alkalmazni, ha a lehető legnagyobb mértékű védelmet kell elérni az esetleges szolgáltatás kimaradással szemben. Például az atomerőművek hálózatos vezérlőrendszerében alkalmazható háló topológia. Az internet ugyan minden helyet több útvonallal tud elérni, mégsem teljes háló topológia.



7. ábra A háló topológia

A hálózat logikai topológiája azt határozza meg, hogy miként kommunikálnak egymással az állomások. A két legelterjedtebb logikai topológia a szórásos és a vezérjeles topológia.

1. A szórásos topológia esetében az állomások minden adatot elküldenek minden, a hálózati közeghez csatlakozó állomásnak. Az állomásoknak semmilyen sorrendet sem kell betartaniuk a hálózat használatában. Így működnek az Ethernet hálózatok, amelyek a tananyagban részletesebben bemutatásra kerülnek.
2. A másik logikai topológia a vezérjeles. Az ilyen topológiában sorban minden állomás megkap egy elektronikus vezérjelet. Amikor egy állomás megkapja a vezérjelet, megkapja a jogot arra, hogy adatokat küldjön a hálózatban. Ha az állomás nem akar adatokat küldeni, átadja a vezérjelet a következő állomásnak, a folyamat pedig megismétlődik.

2.3.5.3 Erőforrásokhoz való hozzáférés módja szerinti csoportosítás

Az **egyenrangú hálózatokban** a hálózatba kapcsolt számítógépek egymással egyenrangú partnerekként viselkednek. Az egyenrangú állomások ügyfél és kiszolgáló szerepet egyaránt felvehetnek.

A hálózat felhasználói rendelkeznek saját erőforrásaik felett. Önállóan dönthetik el, hogy mely fájljaikat osztják meg más felhasználókkal. A felhasználók jelszó megadásához is köthetik a saját erőforrásaikhoz való hozzáférést. Mivel ezeket a döntéseket az egyéni felhasználók hozzák meg, a hálózatnak nincs központi felügyeleti pontja. Emellett a biztonsági mentésekről is a felhasználóknak kell gondoskodniuk, ha azt akarják, hogy meghibásodás esetén az adatokat helyre lehessen állítani. Ha egy számítógép kiszolgáló szerepet játszik, használója a teljesítmény csökkenését tapasztalhatja, hiszen gépe a más rendszerekről származó kérések teljesítésével is foglalkozik.

Az egyenrangú hálózatok telepítése és üzemeltetése viszonylag egyszerű. A számítógépekre megfelelő operációs rendszert kell telepíteni, más eszközre nincs szükség.

A hálózatok növekedésével az egyenrangú kapcsolatok egyre nehezebben tarthatók kézben. A számítógépek erőforrásaihoz való hozzáférés szabályozása az egyéni felhasználók feladata, ami biztonsági szempontból erősen megkérdőjelezhető. Az egyenrangú hálózatok korlátait az ügyfél-kiszolgáló hálózati modell segítségével lehet átlépni.

Ügyfél-kiszolgáló elrendezésnél a hálózati szolgáltatásokat egy **kiszolgáló**nak (server) nevezett számítógép futtatja. A kiszolgáló feladata a válaszadás az ügyfelek kéréseire. A kiszolgáló olyan központi számítógép, amely folyamatosan rendelkezésre áll az ügyfelektől érkező szolgáltatásokra vonatkozó kérések fogadására. A legtöbb hálózati operációs rendszer az ügyfél-kiszolgáló modellt követi. A munkaállomások általában ügyfél szerepet játszanak, a nagyobb kapacitással és speciális szoftverekkel rendelkező számítógépek pedig a kiszolgálók.

Mielőtt egy ügyfél hozzáférhetne valamelyik erőforráshoz, azonosítási és jogosultságellenőrzési eljáráson kell átesnie. A biztonsági szolgáltatásoknak és a hozzáférésvezérlésnek a központosításával, vagyis a kiszolgáló alapú modellt követve leegyszerűsödik a nagyméretű hálózatok felügyelete.

A hálózati erőforrások (fájlok, nyomtatók, alkalmazások) kiszolgálókon való koncentrálása megkönnyíti az adatok karbantartását és biztonsági mentését. Az erőforrások dedikált, speciális kiszolgálókra helyezve könnyebben elérhetők. A legtöbb ügyfél-kiszolgáló rendszer arra is biztosít lehetőséget, hogy új szolgáltatások bevezetésével növeljük a hálózat hasznosságát.

Számos előnyük mellett néhány hátrányuk is van. A kiszolgáló központi helyzetéből következően növelhető a biztonság, könnyebb a hozzáférés, a meghibásodása azonban a teljes hálózat üzemképtelenné válásával jár. Működő kiszolgáló hiányában a hálózat sem tudja ellátni feladatát. A kiszolgálók kezeléséhez és karbantartásához jól képzett szakemberekre van szükség, ami növeli a hálózat üzemeltetésével kapcsolatos kiadásokat. További költségelemet jelent a speciális kiszolgáló számítógépek és célszoftverek megvásárlása.

2.3.5.4 Nyilvánosság szerinti csoportosítás

A zárt hálózatok olyan rendszerek, amelyek felépítése nem publikus, azt a hálózat gyártója és felhasználója titokként kezeli, nem hozza nyilvánosságra. A külső felhasználó számára nem ismert a hálózathoz való csatlakozás feltételrendszere, a hálózat működése, sem szolgáltatásai. A zárt rendszerek tipikusan banki, katonai rendszerek, olyan hálózatok, amelyek üzemeltetője nem tartja kívánatosnak külső felhasználók csatlakozását.

A nyílt rendszerek felépítése, működése, használatának hardver és szoftver feltételei megismerhetők a nagyközönség számára, azaz teljesen nyilvánosak. Nyitott mivoltuk természetesen nem csupán megismerhetőségükben nyilvánul meg, hanem abban is, hogy e megismerhetőség révén adott a lehetősége annak, hogy a nyitott rendszerhez más hálózatokat kapcsoljanak. Ilyen nyitott rendszer például az Internet is. Az Internet minden egyes összetevőjének specifikációja megtalálható az úgynevezett RFC [2]-kben.

2.3.5.5 Az adattovábbítás módja szerinti csoportosítás

Minden hálózat működése a hálózatot alkotó hostok kommunikációján alapul. A hálózat gépei különböző hosszúságú üzeneteket küldenek egymásnak. Az esetek többségében az feladó nem a vele közvetlen kapcsolatban lévő gépnek, hanem egy távolabbi címzettnek küld üzenetet. Ilyen esetben az adó és a vevő között több gép helyezkedik el, és az üzenetnek ezen közbülső gépek közvetítésével kell eljutniuk a címzetthez. A hálózatokat aszerint is megkülönböztetjük, hogy hogyan kapcsolódik össze az adó és a vevő, illetve milyen módon jut el az üzenet a kiindulási állomásról a célba.

1. A **vonalkapcsolás** esetén az adó és a vevő is egy központhoz kapcsolódik. Amikor az adó kapcsolatot kíván létesíteni a vevővel, jelzi ezt a szándékát a központnak, amely felépíti a kapcsolatot, „fémesen” összekapcsolja a két számítógépet, azaz zárt áramkört alakít ki közöttük. Ezután a gépek folyamatos használhatják adatküldésre a csatornát mindaddig, míg egyikük meg nem szakítja a kapcsolatot. Jó példa erre a telefon.
2. **Üzenetkapcsolás**t elsősorban teljes vagy részleges topológiák esetén alkalmaznak. Ilyenkor a két egymással üzenetet váltó gép általában nincs egymással közvetlen kapcsolatban. Az üzenet az adó gép felől gépről gépre továbbítva a „tárol” és „továbbít” elv szerint halad a cél felé. Az üzenet küldése előtt az adó gép felépíti a csatornát, így jelzi ilyen irányú igényét az általa kiválasztott szomszédos gépnek. Az ismét felveszi a kapcsolatot egy vele szomszédságban lévő hosttal. Ez a folyamat mindaddig tart, amíg a csatorna, az úgynevezett virtuális áramkör ki nem alakul az adó és a vevő között. Amikor ez megtörtént, a teljes üzenet az így kialakított útvonalon halad majd a cél felé. Az üzenet hossza nem korlátozott. Leginkább a postai csomagküldéshez hasonlít.

[2] Request for Comments, egy olyan dokumentum, mely egy új Internet-szabvány beiktatásakor adnak közre. Az új szabvány első tervezete saját számmal kerül a nyilvánosság elé, egy adott időtartamon belül bárki hozzászólhat. Ezeket a hozzászólásokat rendszerezik, majd többszöri módosítás után a szabványtervezetet elfogadják vagy eldobják. Pl.: RFC793: Transmission Control Protocol (TCP)

3. A **csomagkapcsolás** a legrugalmasabb adatátviteli forma, amely szintén teljes vagy részleges topológiák esetén használható. Az üzenetkapcsoláshoz hasonlóan, az üzenet küldője és fogadója között gépről gépre, a „tárol" és „továbbít" technikával haladnak az adatok. Az egy egységben elküldhető adatmennyiség hossza azonban pontosan meghatározott, ami az jelenti, hogy a teljes üzenet általában nem egyetlen egységként, hanem kisebb darabokra, úgynevezett csomagokra bontva halad a címzett felé. A feladó gép tehát először csomagokra szabdalja az üzenetet, külön-külön címmel látja el azokat, majd kiválasztja az általa legrövidebbnek vélt útvonalra eső szomszédját. Az első csomagot elküldi ennek a gépnek, amely megvizsgálja a címzettet, majd egy ismételt útvonalválasztás után továbbküldi az adatokat. A további csomagok haladhatnak ezen az úton is, de mivel minden csomagküldést útvonalválasztás előz meg, akár egészen másfelé is eljuthatnak a címzetthez. Az üzenet tehát szabadon választott útvonalakon haladó csomagok formájában jut el a címzetthez, amely az összes csomag beérkezése után összeilleszti azokat az eredeti üzenetté. A csomagkapcsolás számunkra kiemelkedően fontos adattovábbítási mód, ugyanis az Interneten is ilyen módon továbbítódnak az üzenetek.

2.3.5.6 Közeghozzáférési mód szerinti csoportosítás

A fentiekből megtudhattuk, hogy hálózatba kötött számítógépeink különböző topológiáknak megfelelően csatlakozhatnak egymáshoz.

- Pont-pont kapcsolat: Ha az információközlés csak két pont (egy adó és egy vevő) között zajlik, akkor pont-pont kapcsolatról beszélünk.
- Többpontos kapcsolat, üzenetszórás: Többpontos kapcsolatról akkor beszélünk, ha egy adó egyszerre több vevőt lát el információval. Az üzenetszórás olyan többpontos kapcsolat, ahol az adótól egy bizonyos hatósugáron belül minden vevő megkapja az információt (pl. rádiós műsorszórás).

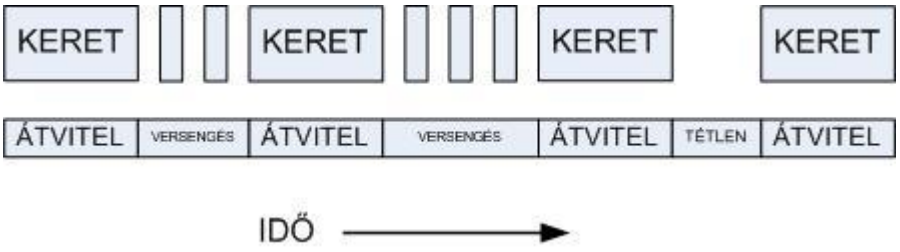
Akár pont-pont, akár üzenetszórásos azonban a topológia, mindenképpen szükség van egy a hálózat minden gépe által alkalmazott szabályrendszerre, ami meghatározza, hogy egy gép a csatornát mikor használhatja adás küldésére, azaz mikor férhet hozzá az átviteli közeghez. E szabályok nélkül könnyen előfordulhatna az, hogy a gépek egyszerre próbálnak üzenetet küldeni ugyanazon a csatornán, vagy az, hogy egy gép olyankor próbál üzenetet küldeni, amikor annak továbbítására a csatorna éppen nem alkalmas.

> Az átviteli közeghez való hozzáférést meghatározó szabályokat átvitel-vezérlésnek nevezzük.

Az átvitelvezérléseket három nagy csoportra bontjuk.

1. **Véletlen átvitelvezérlés**: Ha szabad a hálózat, akkor bármelyik állomás leadhat jelet. A véletlen átvitelvezérlés esetében minden állomás (számítógép) maga dönti el, hogy mikor kísérli meg az üzenet elküldését, éppen ezért megtörténhet, hogy két gép egy időben próbál meg adást küldeni a közösen használt csatornán. Ilyen

esetben ütközésről beszélünk. Ha két üzenet ütközik, akkor mindkettő elvész, éppen ezért a véletlen átvitelvezérlések esetén az adó gépnek mindenképpen értesülnie kell az esetleges ütközésről, hogy az üzenet küldését megismételhesse.
Tipikus megvalósítása a CSMA/CD (Carrier Sense Multiple Access with Collision Detection), azaz csatorna figyelő többszörös hozzáférés ütközés detektálással. Elsősorban busz topológiájú hálózatokban használják, s mint azt látni fogjuk ez az igen népszerű Ethernet hálózatokban alkalmazott átvitelvezérlés is.



8. ábra CSMA/CD protokoll állapotai.

2. **Osztott átvitelvezérlés**: Azt jelenti, hogy egy közösen használt szabály pontosan rögzíti, hogy melyik időpillanatban melyik gép használhatja a csatornát, azaz csak egy állomásnak van joga jelet adni.
3. **Központosított átvitelvezérlés:** E vezérlési forma elsősorban a csillag topológiákhoz kötött, ugyanis itt van egy központi szerepet betöltő gép (server), amely vezérli a hálózat többi hostját, azaz megmondja, hogy melyik host mikor küldhet adást.

2.3.5.7 Az átviteli módszer alapján történő csoportosítás

1. Alapsávú (Baseband)**:** Modulálatlan jeleket továbbít, tehát az átviteli közegben haladó jel frekvenciája közel azonos a bitsorozat frekvenciájával. Telepítése olcsó. Rövid távra alkalmazható. Általában LAN-okhoz használják.
2. Szélessávú (Broadband)**:** Az adatátvitel modulált, tehát a vivő frekvenciája jóval nagyobb, mint a bitsorozat frekvenciája. Az átvitelre használható sávot több logikai csatornára osztják.

2.3.5.8 Kommunikáció iránya szerinti csoportosítás

- szimplex: a hálózati kommunikáció egyirányú / Az egyik állomás csak az adó a másik csak a vevő. Ilyen például a televízió. /
- fél duplex: a hálózati kommunikáció váltakozó irányú / Az adatátvitel mindkét irányban megengedett, de egy időben csak az egyik irányban élhet. Ilyen például a CB rádiózás./
- duplex: a hálózati kommunikáció kétirányú**.** / Mindkét állomás egyszerre lehet adó és vevő is. Ilyen például a telefonálás. /

2.3.6 A hálózatok egyéb jellemzői

Sebesség: A hálózatok igen fontos jellemzője a sebesség, amely azt határozza meg, hogy a hálózat átviteli közegén – kommunikációs csatornáján – időegység alatt mekkora adatmennyiség vihető át. Mivel az adatmennyiség alapvető mértékegysége a bit, az átviteli sebesség mértékegysége a bit/secundum, amit gyakran rövidítenek bps-ként.

Digitális hálózatok esetén a hálózatra (pontosabban a kommunikációs csatornára) jellemző legnagyobb adatátviteli sebességet nevezik sávszélességnek. A sávszélesség minden átviteli eszköz jellemző mennyisége (hálózati kártya, modem, hálózati vonal). Sok esetben a szolgáltatók két sávszélességi adatot adnak meg. Más sebességgel történhet a letöltés, mint a feltöltés. Pl.: 768/128 kbps. Az átvitel sávszélességét mindig a leglassabb elem sebessége határozza meg (pl.: egy nagysebességű hálózatra kapcsolt modem esetén a modem, telefonvonal esetén a telefonvonal sebessége). A kommunikációs csatornák esetében a sebesség szó szinonimájaként gyakran használják a sávszélesség kifejezést.

Átviteli közeg: A hálózat állomásait kommunikációs csatornák kötik össze. Ezeket a csatornákat más néven átviteli közegeknek nevezzük. Az adatátvitelhez többféle fizikai közeg használható.

Vezetékes rendszerek: Az ilyen rendszerekben valóban elektromos, vagy fény impulzusok továbbítására alkalmas kábelek kötik össze a számítógépeket. Fizikai felépítése alapján több fajtát különböztetünk meg. Ezek fizikai tulajdonságai erőteljesen befolyásolják alkalmazhatóságukat. A különféle hálózati megvalósításokban háromféle kábeltípussal találkozhatunk:

1. **Koaxiális kábel**: Felépítése megegyezik a televíziózásban használt koaxiális kábelekével. A 80-as, 90-es évek elején használták helyi hálózatok kiépítésére. Alacsony adatátviteli sebessége és sérülékenysége miatt az új hálózatokban már nem használják.
2. **Csavart érpár:** Egy kábel általában több érpárt tartalmaz. Ha az érpárokat árnyékoló fémburkolat takarja, Shielded Twisted Pair-ról (STP), azaz árnyékolt sodrott érpárról beszélünk, az árnyékolás hiánya esetén a kábelt Unshielded Twisted Pairnak (UTP), árnyékolatlan sodrott érpárnak nevezzük. Az UTP napjaink legelterjedtebb kábele.
3. **Optikai kábel:** Az optikai, vagy üvegszálas kábelek nem elektromos, hanem fényimpulzusok segítségével továbbítják az üzenetek bitjeit.

Az UTP kábelekről, és az optikai kábelekről a későbbiekben bővebben lesz szó.

Vezeték nélküli rendszerek: A vezetékes rendszerek kiépítése nem mindig megoldható. Ilyenkor vezeték nélküli technológiák közül lehet választanunk. Jellemzői:

1. infravörös kommunikáció kisebb távolságra
2. rövidhullámú, rádiófrekvenciás átvitel (WiFi, Bluetooth) kisebb távolságra

3. mikrohullámú átvitel, mely működésének feltétele, hogy a két antennának látnia kell egymást
4. lézer
5. műholdas átvitel.

2.4 ÖSSZEFOGLALÁS

A számítógépek egymás közötti kommunikációját egy speciális rendszer a számítógép-hálózat biztosítja. A számítógépek kommunikációja megvalósulhat akár valamilyen közös hardver buszrendszeren keresztül, akár a nyilvános telefonhálózaton keresztül: a lényeg az, hogy a kommunikáló felek megértsék egymást. A számítógépes hálózatok fejlődésének legfőbb ösztönző ereje gazdaságosságuk. Ezen kívül még számos előnyük megemlíthető: az erőforrás-megosztás, az osztott munkavégzés, a kommunikációs lehetőségek.

A számítógépes hálózatokat többféle szempont szerint csoportosíthatjuk. Kiterjedés alapján megkülönböztetjük a LAN, a MAN, és a WAN hálózatokat. Fizikai topológiájuk szerint busz, gyűrű, fa, csillag, kibővített csillag, hierarchikus és háló; logikai topológia szerint szórásos és vezérjeles hálózatokat. A hálózatok lehetnek zártak, melyek felépítése nem publikus, és nyíltak melyek felépítése és működése megismerhető. Csoportosíthatóak ezen kívül az adattovábbítás módja szerint, azaz hogyan kapcsolódik össze az adó és a vevő, illetve milyen módon jut el az üzenet a feladótól a vevőig. Eszerint lehet vonal, üzenet és csomagkapcsolásos. Az átvitelvezérlés is megkülönbözteti a hálózatokat. Itt megismertük, a véletlen az osztott és a központosított átvitelvezérléseket. Ezeken kívül még csoportosítottuk a hálózatokat az átvitel módszere alapján alap és szélessávúaknak, illetve a kommunikáció iránya szerint egyirányú (szimplex), váltakozó irányú (half-duplex) és kétirányú (duplex) hálózatoknak.

A jellemzői között megismerhettük a sebességet, ami az időegység alatt átvihető adatmennyiséget jelöli. Mértékegysége a bit/s. Valamint a sávszélességet, ami kommunikációs csatornák esetében a sebesség szinonimája.

A hálózatok másik jellemzője, hogy az adatátvitelre milyen közeget használ. A vezetékes rendszerek koaxiális, csavart érpár, és optikai kábeleket használnak. Alkalmazhatóságukat fizikai tulajdonságaik erősen befolyásolják. A vezeték nélküli rendszerek kisebb távolságoknál használhatnak infravörös, vagy rövidhullámú rádiófrekvenciás átvitelt (Wi-Fi, Bluetooth), nagyobb távolságoknál megoldást jelenthet mikrohullámú átvitel, mely működésének feltétele, hogy a két antennának látnia kell egymást; a lézer illetve a műholdas átvitel.

2.5 ÖNELLENŐRZŐ KÉRDÉSEK

(Igaz vagy hamis?)

1. A kibővített csillag topológiát akkor szokás alkalmazni, ha a lehető legnagyobb mértékű védelmet kell elérni az esetleges szolgáltatás kimaradással szemben.
2. A legtöbb hálózati operációs rendszer az ügyfél-kiszolgáló modellt követi.
3. A hálózati erőforrások (fájlok, nyomtatók, alkalmazások) kiszolgálókon való koncentrálása megnehezíti az adatok karbantartását és biztonsági mentését.

4. Ha a külső felhasználó számára nem ismert a hálózathoz való csatlakozás feltételrendszere, a hálózat működése, akkor nyilvánosság szerint zárt hálózatról beszélünk.
5. Ethernet hálózatokban a véletlen átvitelvezérlés az alkalmazott.
6. A vonalkapcsolás esetén az adó és a vevő is egy központhoz kapcsolódik.
7. Half-duplex kommunikációnál a hálózati kommunikáció kétirányú.
8. Az átvitel sávszélességét mindig a leggyorsabb elem sebessége határozza meg.
9. A csavart érpáras kábelek közül az STP az elterjedtebb.
10. A mikrohullámú átvitel működésének feltétele, hogy a két antennának látnia kell egymást.

3. A HÁLÓZATI ARCHITEKTÚRÁK

3.1 CÉLKITŰZÉS

A mai számítógépek már nem csak önálló eszközök, hanem többnyire egy hálózat részei. Ahhoz azonban, hogy ezekhez a hálózatokhoz csatlakozni tudjunk, és szolgáltatásait igénybe tudjuk venni, a hálózattervezésnek szigorúan strukturáltnak kell lennie, azaz a hálózat egymásra épülő részeit rétegekbe kell sorolni. A rétegek feladataira, felosztásukra hálózati referenciamodellt és szabványokat kellett létrehozni, mely biztosítja a kommunikációs folyamatok felépíthetőségét.

Ebben a leckében bemutatásra kerülnek a hálózati feladatok rétegei, és az hogy ezek a rétegek milyen módon kommunikálnak egymással. Megismerheti a két legjelentősebb referenciamodellt az OSI és a TCP/IP modellt.

A lecke segít megérteni a szabványok jelentőségét az informatikában, és bemutat néhányat a létrehozó szervezetek közül.

A lecke végén megismerheti az Ethernetet, a mai LAN hálózatok legelterjedtebb technológiáját.

3.2 A LECKE TÉMAKÖREI

- A hálózati feladatok részekre bontása
- Protokollok, architektúrák
- Referencia modellek
- Hálózati szabványok
- Ethernet

3.3 A HÁLÓZATI FELADATOK

Ma már nem létezik olyan cég, amely egyszerre lenne képes gyártani mindent a számítógép hálózathoz beleértve a szoftver és hardver elemeket. A legáltalánosabban elterjedt megoldás, hogy csak egy vagy esetleg néhány területre szakosodnak. Ilyenkor azonban kapcsolódási pontokat (interface-ket) kell pontosan definiálni.

Mindennapi munkafolyamatok esetében megfigyelhető a feladatok részekre bontása. A részfeladatokat különböző emberek valósítják meg, tehát házon belül is megjelenik az interface probléma.

3.3.1 A hálózati feladatok rétegekre osztása

A hálózatokat a tervezés és megvalósítás könnyítésének érdekében tehát rétegekre (layer) osztják. A rétegekre a következő megállapítások érvényesek:

1. se túl sok, se túl kevés réteg ne legyen
2. a rétegek határai határozottak, könnyen definiálhatók legyenek
3. hasonló feladatok elvégzését azonos szint végezze
4. egy szint belső változásai ne érintsék a többi szintet.

3.3.2 Hálózati protokollok, architektúrák

Egymással kommunikálni csak az azonos szintek rétegei tudnak. Ennek a kommunikációnak a szabályai a protokollok.

A teljes átvitelben több ilyen is részt vesz, ezek egymást követő halmazát nevezzük protokoll veremnek (stack). Az elküldött üzenet egy ilyen protokoll vermen megy végig, amíg elér az átvivő közeghez. Minden egyes protokoll kiegészíti az áthaladó csomagot a saját információival. A felsőbb réteg használja az alatta lévő réteg szolgáltatásait. A rétegek közötti elemi műveleteket egy interface definiálja.

Egy hálózat rétegeinek és protokolljainak halmazát hálózati architektúrának hívjuk.

A tényleges hálózati megvalósítások meghatározó jellemzője, hogy azokban milyen rétegek, és a rétegek között milyen protokollok vannak meghatározva.

3.3.3 Hálózati szabványok

Mindaddig, amíg egy technológia egyetlen országban létezik csak, nem kell azzal foglalkozni, hogy más országokban annak milyen megvalósításait dolgozzák ki. Manapság azonban a távközlés, de természetesen más iparágak területén is nagyfokú globalizációnak vagyunk tanúi. Ilyen körülmények között természetes az a törekvés, hogy az egyes országok törekszenek egy-egy tervezett termék, vagy technológia kapcsán véleményüket, elképzelésüket, szakmai érveiket egyeztetni, azaz olyan közös szabályokat kidolgozni, amelyekhez igazodva biztosítani lehet a különböző államokban megvalósított rendszerek kompatibilitását, egymáshoz illeszthetőségét. E törekvés szabályrendszerek, szabványok kidolgozásában, elfogadásában, illetve alkalmazásában nyilvánul meg.

A több gyártó által elfogadott, alkalmazott technológiákat, illetve szabványügyi szervezetek által kidolgozott ajánlásokat szabványoknak nevezzük. A következő néhány sorban röviden áttekintjük a szabványügyi szervezeteket.

1. **International Standards Organization (ISO)** A Nemzetközi Szabványügyi Szervezet legnagyobb, 89 állam szabványügyi szervezeteit tömörítő szerveződés. A legkülönfélébb szabványok megalkotásán fáradozik. A csavarok menetemelkedésének szabványától kezdve a hálózati kommunikáció szabályrendszereinek kidolgozását végzi. Az ISO néhány említésre méltó tagszervezete az ANSI (Egyesült Államok), DIN (Németország), BSI (Nagy Britannia), AFNOR (Franciaország). A szabványok kidolgozása egy ország szervezetének javaslata alapján indul meg. Az ISO munkacsoportot alakít, amely bizottsági javaslatot készít (Commite Draft). A CD-t minden tagszervezet véleményezi, majd ez alapján nemzetközi szabványtervezet készül (Draft International Standard, DIS). A DIS ismételt közös véleményezése, majd elfogadása után alakul ki a Nemzetközi Szabvány (International Satandard IS).
2. **International Telecommunication Union (ITU)** Nemzetközi Távközlési Egyesülés, 1865-ben alakult szervezet, amely kezdetben a távíró, később a telefon nem-

zetközi szabványosításával foglakozó szervezet, amelynek jelentőségét tovább növelte, hogy 1947-ben az ENSZ ügynöksége lett. Három ágazata a távközlés különböző területeivel foglakozik:

- ITU-R, rádiókommunikáció
- ITU-D, fejlesztés
- ITU-T távközlés.

A számítógép-hálózatokkal kapcsolatos szabványok kidolgozásáért az ITU-T felelős. Ezt az ágazatot nevezték 1956-1993 között CCITT-nek (Comité Consultatif International Télégraphique at Telefhonique), napjainkban azonban, visszatértek az ITU-T elnevezéshez. Az ITU-T telefon, távíró, és egyéb adatátviteli eszközökkel kapcsolatos szabványok kidolgozásán fáradozik. Szabványaik elnevezései egy betűből és egy a ponttal (.) elválasztott számból állnak (X.25 felhasználói rendszerek hálózati összekapcsolása dedikált vonalú csomagkapcsolt rendszereken segítségével). A betűk különböző szabványsorozatokat, a számok pedig a sorozaton belüli szabványokat jelölik.

3. **Institute of Electrical and Electronics Engineers (IEEE)** Villamos- és Elektronikai Mérnökök Szervezete villamosmérnöki és informatikai témákat dolgoz fel. Több egyéb szabvány kidolgozása mellett jelentős szerepe volt az Ethernet szabványosításában is.
4. **American National Standards Institute (ANSI)** Az Amerikai Egyesült Államok számára ipari szabványokat kidolgozó nonprofit szervezet. Informatikában például az ASCII karakterkészlet köthető hozzá. / www.ansi.org /

Amint látjuk, több szabványügyi szervezet létezik, amelyek egyrészt saját szabványokat dolgoznak ki, másrészt lépéseket tesznek más szabványügyi szervezetek szabványainak saját rendszerükbe való beillesztésébe.

3.3.4 Az OSI modell

Nyitott, más hálózatokról hozzáférhető rendszerek kialakítása során, gondoskodni kell a kommunikációs feladatok rendszerezéséről, rétegekbe rendezéséről. A világcégek többsége megalkotta saját hálózati architektúráját, de az eltérések miatt ezeket egységesíteni kellett, amit csak nemzetközi szinten lehetett megoldani. Ezt a feladatot az **ISO** (International Standards Organization – Nemzetközi Szabványügyi Szervezet) szakemberei végezték el.

A hálózatokra vonatkozó rétegmodell megfogalmazására 1980-ban került sor **OSI** (Open System Interconnection) néven.

> Fontos tudni, hogy maga a modell nem szabvány, tehát nem egy ténylegesen megvalósítandó hálózat pontos leírása, csupán egy ajánlás, amely rögzíti, és rétegekbe rendezi a hálózati kommunikáció során megvalósítandó feladatokat.

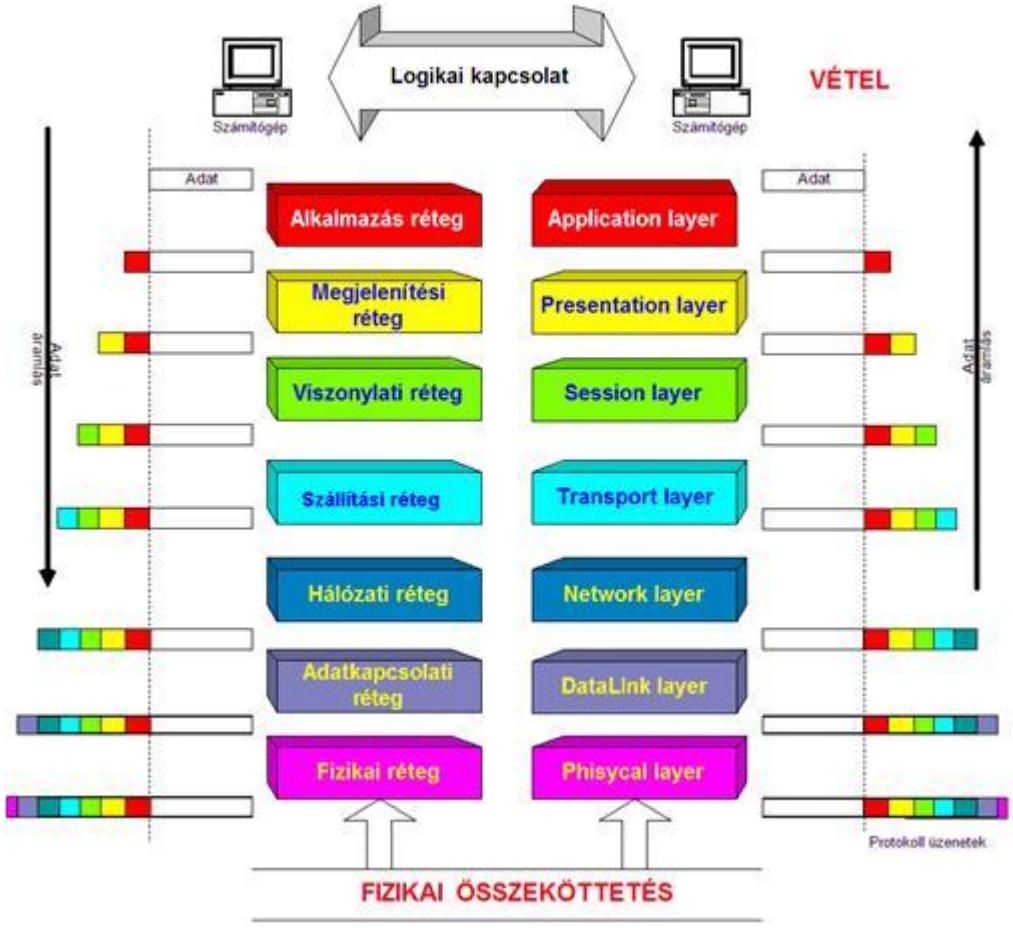
Az OSI modell egyfajta „kályha” amelytől elindulva ki lehet dolgozni az egyes hálózati megvalósítások pontos rendszerét. Betartása nem kötelező. A megvalósított rendszerekben egyes rétegei szinte teljesen üresek maradnak, míg másoknál további osztásokra lett szükség zsúfoltságuk miatt. Hiányosságai ellenére a mai napig alapnak tekintik a gyártók.

Az OSI referencia modell szerint egy hálózatot 7 rétegre osztunk.
Az adatátvitellel foglalkozó rétegek:

1. **A fizikai réteg (physical layer)** A fizikai réteg a legalsó réteg, ezen zajlik a tényleges adatátvitel. Feladata a bitek hibamentes átvitele, azaz biztosítja, hogy az adó által küldött jeleket a vevő is azonosként értelmezze.
2. **Az adatkapcsolati réteg (data link layer)** Az adatkapcsolati réteg feladata az adatok kisebb egységekre, úgynevezett adatkeretekre (data frame) darabolása, és a keretek hibamentes célbajuttatása. Ezt úgy éri el, hogy a csomagokban adathalmazát egységnyi darabokra vágja, és majd minden kereten elvégez egy bonyolult matematikai műveletet, amelynek eredményét a keret végéhez illeszti. Ezt a számot CRC-nek (ciklikus redundancia control) nevezzük. A fogadó gép, miután megkapott egy keretet, ugyanazt a matematikai műveletet végzi el vele, mint a feladó gép. Saját eredményét összehasonlítja a keret végén található CRC-vel. Ha az elküldött, illetve a vevő oldalon számított eredmény megegyezik, akkor a vevő gép adatkapcsolati rétege egy úgynevezett nyugtakeretet küld a küldő gép adatkapcsolati rétegének, jelezve, hogy a keret hibamentesen megérkezett. Ha a küldő gép bizonyos időn belül nem kap nyugtakeretet, akkor az adatkeretet elveszettnek minősíti, és ismételten elküldi azt, forgalomszabályozást is végezve. A hibátlanul megérkező adatkereteket az adatkapcsolati réteg csomaggá illeszti össze, majd továbbítja azt a hálózati rétegnek.
3. **A hálózati réteg (network layer)** Vezérli a kommunikációs alhálózatok működését, legfontosabb feladata az útvonalválasztás a forrás és célállomás között. Ha az útvonalban eltérő hálózatok is vannak, akkor protokollátalakítást, -tördelést (fragmentation) is végez. Fontos megjegyezni, hogy míg az adatkapcsolati réteg az egymással kommunikáló távoli gépek között tartja a kapcsolatot és nem vesz tudomást az „útközben” elhelyezkedő gépekről, addig a hálózati réteg mindig csak egy szomszédos hosttal van kapcsolatban.
4. **A szállítási réteg (transport layer)** A végpontok közötti hibamentes adatátvitel biztosításáért felelős. A topológiát már nem ismeri, csak a két végpontban van rá szükség. Feladatai: összeköttetések felépítése, bontása, csomagok sorrendbe állítása, hibaérzékelés, helyreállítás és az adatáramlás vezérlése.

A logikai összeköttetéssel foglalkozó rétegek:

5. **A viszonyréteg (session layer)** Megteremti annak a lehetőségét, hogy két számítógép felhasználói kapcsolatot létesítsenek egymással, azaz a programok, pontosabban folyamatok összekapcsolását végzi el. Feladata az alkalmazások közti viszonyok felépítése, kezelése és lebontása.
6. **A megjelenítési réteg (presentation layer)** A fogadó rendszer számára biztosítja az adatok olvashatóságát. A megjelenítési réteg feladatai közé tartozik az adatok titkosítása, és visszafejtése is. A rétegek közül az egyetlen, amely megváltoztathatja az üzenet tartalmát.
7. **Az alkalmazási réteg (application layer)** Az alkalmazások számára biztosít hálózati szolgáltatásokat. Az adó oldalon elfogadja és feldolgozza a felhasználó által továbbítandó adatokat, a vevő oldalon pedig gondoskodik azok felhasználó felé történő továbbításáról. Pl.: fájlok gépek közötti másolása.



9. ábra Az ISO/OSI modell rétegei adatáramlás

3.3.5 A TCP/IP modell

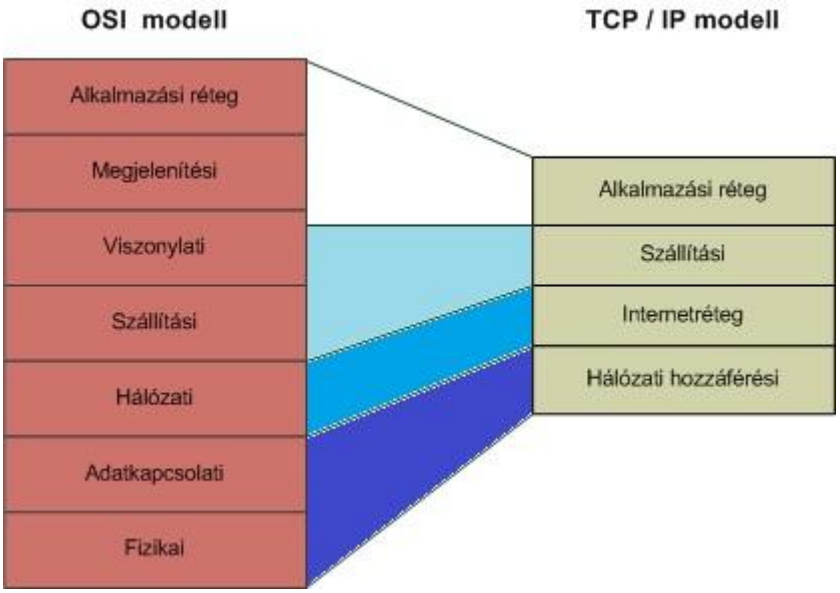
A számítógépek kommunikációjának leírására alkalmas másik modellt az Amerikai Védelmi Minisztérium definiálta. Célja olyan hálózatot megtervezése, amely minden körülmények között működőképes marad. A jól körülhatárolt feladatokat megvalósító hálózati rétegeket és a közöttük használható protokollokat definiálja. A TCP/IP-t nyílt szabványként alakították ki, vagyis mindenki szabadon használhatja. Felépítése hasonlít az OSI modelléhez, de egyszerűbb annál, mindössze négy réteget tartalmaz. Bár elnevezésükben találhatóak azonosságok, a modellek között mégsem felelnek meg egymásnak pontosan a két modell rétegei.

A TCP/IP modell a következő négy rétegből áll:

1. **Állomás hálózat közötti réteg** A legalsó réteg, amely valójában az OSI modell fizikai és adatkapcsolati rétegének feladatait tartalmazza. A TCP/IP tulajdonképpen nem is foglalkozik e réteg pontos leírásával, csak azt határozza meg, hogy ebben a rétegben kell megvalósulnia a szomszédos gépek közötti tényleges adatátvitelnek.

Ide tartozik minden olyan fizikai és logikai összetevő, amely a fizikai összeköttetés felépítéséhez szükséges. Hogy a bitek átvitele hogyan zajlik, azzal a modell egyáltalán nem törődik.

2. **Internet réteg** Az OSI modell hálózati rétegének felel meg. Feladata, hogy a felsőbb rétegektől kapott csomagokat, az Interneten alkalmazott címzés, az IP cím alapján továbbküldje a cél felé, vagyis csomagokra bontsa a TCP-szegmenseket, és elküldje őket bármely hálózatról. Az internet réteg a szállítási rétegtől kapott minden egyes csomag elküldése előtt megvizsgálja, hogy a csomagot milyen útvonalon kell továbbítani. Az útvonal megválasztása után pedig továbbítja csomagot a megfelelő állomás internet rétegének. Amikor az internet réteg az alatta elhelyezkedő állomás és hálózat közötti rétegtől kap csomagot, akkor megvizsgálja, hogy az a saját gépnek érkezett-e. Ha igen, akkor saját gép szállítási rétegének, ha pedig nem, akkor egy ismételt útválasztás után valamelyik szomszéd gépnek továbbítja azt. Az internet réteg protokollja az IP (Internet protokoll).
3. **Szállítási réteg** A TCP/IP szállítási rétege az egymásnak üzenetet küldő két végpontot összekötő réteg. Nem vizsgálja a végpontok közötti állomásokat, csak azzal foglalkozik, hogy a végpontok között megvalósuljon az adatátvitel. A szolgáltatás minőségi kérdései tartoznak ide: a megbízhatóság, az adatfolyam-vezérlés és a hibajavítás. Két protokollal is rendelkezik, az egyik a TCP (Transmission Control Protokoll), a másik az UDP (User Datagram Protokol).
4. **Alkalmazási réteg** Megfigyelhetjük, hogy a TCP/IP modell nem tartalmazza az OSI modell viszony- és megjelenítési rétegeit. Ez azért van, mert az interneten ezen rétegek feladatát az alkalmazási réteg látja el. Kezeli a megjelenítés, a kódolás és a párbeszédvezérlés kérdéseit. Az alkalmazási rétegben az Interneten egymással kommunikáló alkalmazások, illetve ezek protokolljai foglalnak helyet.



10. ábra OSI és TCP/IP modell

3.3.6 Beágyazás (Encapsulation)

A hálózaton minden kommunikáció egy forrás és egy cél között jön létre. A hálózaton át küldött információt adatnak vagy adatcsomagnak nevezzük.

Ha egy gép adatot akar küldeni egy másik számítógépnek, akkor a küldendő adatokat be kell csomagolnia. Ezt a folyamatot beágyazásnak nevezzük.

A referenciamodellek közül bármelyikre elmondható, hogy a hálózat rétegei a következő öt lépéssel ágyazzák be és továbbítják az adatokat:

1. Adattá alakítják a képeket és a szövegeket.
2. Szegmensekbe csomagolják az adatokat.
3. A forrás- és a célállomás címét tartalmazó csomagba ágyazzák az adatszegmenst.
4. A következő közvetlenül csatlakozó készülék MAC-címét tartalmazó keretbe ágyazzák a csomagot.
5. Átalakítják a keretet az átviteli közegen továbbítható egyesek és nullák (bitek) sorozatává.

1. Beágyazás folyamata

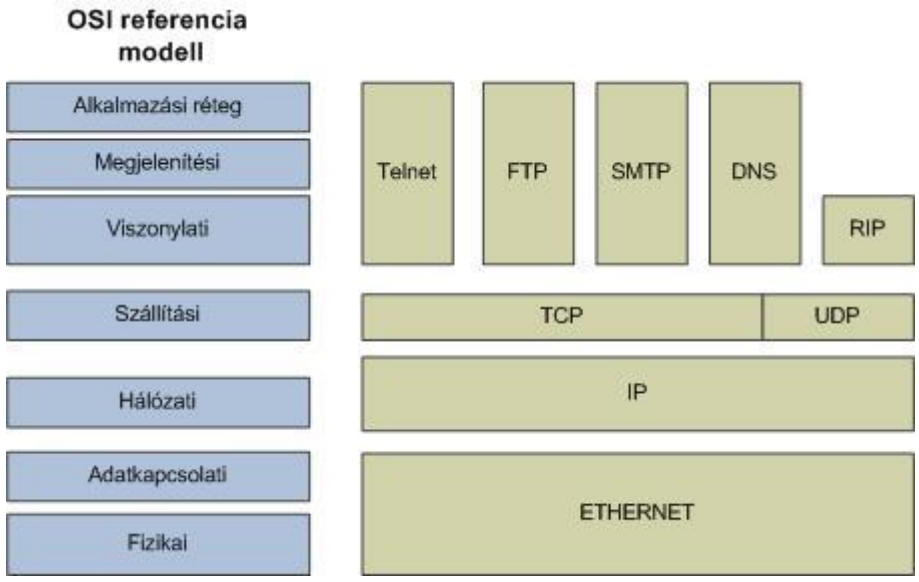
A beágyazás folyamatát a 2. animáció mutatja be.

3.3.7 Az Ethernet

Napjaink legszélesebb körben használt LAN technológiája az Ethernet. Első megvalósítását, a Digitalt, az Intelt és a Xeroxot összefogó csoport, a DIX készítette el. A DIX hozta létre az első Ethernet LAN specifikációkat is, amelyek alapján az IEEE 1980-ban összeállította a 802.3 szabványt. Az IEEE szándéka az volt, hogy szabványai kompatibilisek legyenek a Nemzetközi Szabványügyi Hivatal (ISO) szabványaival és az OSI modellel. Ennek érdekében az IEEE 802.3 szabvány az OSI modell első rétegét, illetve második rétegének alsó felét fedi le.

Az Ethernet szabvány alapján készült első termékek az 1980-as évek elején jelentek meg. Ekkor az ethernet legfeljebb 10 Mbit/s sebességű adatátvitelre volt képes vastag koaxiális kábelen keresztül, legfeljebb 2 km-es távolságra. A 10 Mbit/s-os sávszélesség az 1980-as évek lassú személyi számítógépei számára több mint elegendő volt. Az 1990-es évek elejére azonban a számítógépek gyorsabbak lettek, a fájlok mérete megnőtt, és az adattovábbítás során egyre többször jelentkeztek torlódások. Ezeket a legtöbb esetben a szűkös sávszélesség okozta. Ezért 1992-ben létrehoztak a 802.3 minden egyéb előírását megtartva egy új szabványt egy gyorsabb LAN-ra, melyet 802.3u-nak, gyors ethernetnek (fast ethernet) neveztek el, majd 1995-ben létrejött a 802.3z szabvány, ami a gigabites ethernet jelöli.

Az a protokoll, amely 1973-ban még 3 Mbit/s sebességgel továbbította az adatokat, most akár 10 Gbit/s-ra is képes, miközben az eredeti Ethernet szabvánnyal gyakorlatilag kompatibilis maradt. Működőképes az a rendszer is, amelyben egy Ethernet keret elhagy egy régebbi, koaxiális kábelre csatlakozó, 10 Mbit/s sebességű hálózati kártyát, áthalad egy 10 Gbit/s sebességű, optikai szálas Ethernet összeköttetésen, továbbhalad egy 100 Mbit/s sebességű kapcsolón, majd egy 1000 Mbit/s sebességű hálózati kártyába fut be. Amíg a keret valamilyen Ethernet hálózaton marad, addig nem változik meg.



11. ábra Az OSI modell a TCP/IP protokollok és az Ethernet

3.3.8 Az Ethernet keretek felépítése

Az ethernet hálózatokon az adatok keretekben jutnak el a címzettől a feladóig. A keretek valójában nem mások, mint mezőkre osztott bitsorozatok. A mezőkben a következők szerepelhetnek:

1. Az előtag (preamble)váltakozva tartalmaz egyeseket és nullákat. 7 darab 10101010 tartalmú bájtból álló sorozat. A 10 Mbit/s-os és kisebb sebességű Ethernet-megvalósításoknál az órajel szinkronizálása ennek a mezőnek a segítségével történik. Az Ethernet gyorsabb változatai szinkron működésűek, ezeknél időzítési információkra nincs szükség; ennek ellenére, a kompatibilitás érdekében a mező megmaradt.
2. Az előtagot egy egyoktetből álló mező a keretkezdő (start frame delimiter) követi, amely az időzítési információk végét, a keret tényleges kezdetét jelzi. Tartalma az 10101011 bitsorozat.
3. Ezután a cél (destination) és küldő (source) állomás 48-bites címei következnek. Az Ethernet hálózaton minden állomást egy egyedi, 48-bites (6 bájtos) ún. MAC (Media Access Control) cím azonosít. Ezen címek kiosztását az IEEE kontrollálja.
4. A hossz/típus mezőt kétféle célra lehet használni. Ha értéke a decimális 1536-nál, vagyis a hexadecimális 0×600-nál kisebb, akkor a benne szereplő érték hosszt ad meg, egyébként típus értékként azt adja meg, hogy az Ethernet folyamatainak lezárulása után melyik felsőbb rétegbeli protokoll fogja kapni az adatokat. A hossz a mezőt követő adatrészben található bájtok számát adja meg.
5. Az adat mező és a szükség szerinti kitöltés hossza tetszőleges lehet, azonban a keret mérete nem haladhatja meg a felső mérethatárt. A maximális átviteli egység

(maximum transmission unit, MTU) az Ethernet esetében 1500 oktett, az adatok mérete tehát ezt nem haladhatja meg. A mező tartalma nincs meghatározva. Ha nincs elég felhasználói adat ahhoz, hogy a keret mérete elérje a minimális kerethosszt, akkor előre meg nem határozott mennyiségű adat kerül beillesztésre, közvetlenül a felhasználói adatok mögé. Ezt a többletadatot nevezzük kitöltésnek. Az Ethernet keretek hosszának 64 és 1518 oktett között kell lennie.

6. A keret végén szereplő FCS (Frame Check Sequence – Keret Ellenőrző Sorozat) mezőben egy 4 bájton CRC ellenőrző összeg helyezkedik el. Ha a vevő által számolt és a keretben lévő összeg nem egyezik, a keret eldobásra kerül.

12. ábra Az Ethernet keret

3.4 ÖSSZEFOGLALÁS

A számítógépek közötti kommunikáció leírására a rétegek fogalmát használjuk, mely segítséget nyújt a hálózatok tervezésében és megvalósításában. Azonos szintű rétegek csak egymással kommunikálhatnak, szabályai a protokollok. A rétegek és protokollok halmaza a hálózati architektúra.

Nyílt és más rendszerekből is hozzáférhető rendszerek létrejöttéhez szükség volt nemzetközileg elfogadott egységes rétegmodellek létrehozására. Az OSI hivatkozási modell hét, sorszámmal azonosítható rétegből áll, amelyek mindegyike egy adott hálózati funkciót valósít meg: fizikai, adatkapcsolati, szállítási, hálózati, viszony, megjelenítési és alkalmazási rétegből. A TCP/IP modell négy rétegből áll: alkalmazási, szállítási, internet és hálózatelérési.

Bár neveikben találunk azonosságot, a két modell rétegei mégsem egyeznek meg pontosan. A TCP/IP alkalmazási rétege az OSI alkalmazási, megjelenítési és viszonyrétegének felel meg. A TCP/IP modell a hálózatelérési rétegben vonja össze az OSI modell adatkapcsolati rétegét és fizikai rétegét. Mindkettőre elmondható, hogy minden réteg az adat továbbítása előtt beágyazza a felette levő rétegtől kapott információt.

Ahhoz, hogy a különböző földrajzi helyeken létrehozott rendszerek kompatibilitása és egymáshoz illeszthetősége megmaradjon szabályrendszerek, szabványok létrehozására volt szükség. Néhány jelentősebb szabványügyi szervezet: **International Standards Organization (ISO), International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI).**

A Digitalt, az Intelt és a Xeroxot összefogó csoport, a DIX készítette el napjaink legszélesebb körben használt LAN technológiájának, az Ethernetnek az első megvalósítását. Az

IEEE 1980-ban összeállította a 802.3 szabványt, mely tartalmaz az erre vonatkozó specifikációkat. 1992-ben jelent meg továbbfejlesztése a 802.3u (fast ethernet), majd 1995-ben a 802.3z szabvány mely a gigabites ethernet szabványt jelöli. Az újabb szabványok megőrizték kompatibilitásukat az eredeti ethernet szabvánnyal.

Az ethernet keretek mezőkre osztott bitsorozatok. A mezőkben a következők szerepelhetnek: előtag, 7db 10101010 tartalmú bájtból álló sorozat; keretkezdő, amely az időzítési információk végét, a keret tényleges kezdetét jelzi, tartalma az 10101011 bitsorozat; a cél és küldő állomás 48-bites címei. A hossz/típus mező, mely vagy a mezőt követő adatrészben található bájtok számát adja meg, vagy típus értékként azt adja meg, hogy az Ethernet folyamatainak lezárulása után melyik felsőbb rétegbeli protokoll fogja kapni az adatokat. Az adat mező és a szükség szerinti kitöltés hossza tetszőleges lehet, azonban a keret mérete nem haladhatja meg a felső mérethatárt, mely ethernet esetében 1500 oktett. A keretet egy 4 bájton elhelyezkedő CRC ellenőrző összeg zárja, az FCS mezőben.

3.5 ÖNELLENŐRZŐ KÉRDÉSEK

1. A hálózatokat a tervezés és megvalósítás könnyítésének érdekében rétegekre (layer) osztják.
2. Egy hálózat rétegeinek és protokolljainak halmazát hálózati architektúrának hívjuk.
3. Az OSI referencia modell szerint egy hálózatot 6 rétegre osztunk.
4. Az OSI modell hálózati rétege a végpontok közötti hibamentes adatátvitel biztosításáért felelős.
5. A TCP/IP modell szállítási rétege az egymásnak üzenetet küldő két végpontot összekötő réteg.
6. A TCP/IP modell tartalmazza az OSI modell viszony- és a megjelenítési rétegeit.
7. Ha egy gép adatot akar küldeni egy másik számítógépnek, akkor a küldendő adatokat be kell csomagolnia. Ezt a folyamatot beágyazásnak nevezzük.
8. A több gyártó elfogadott, alkalmazott technológiákat, illetve szabványügyi szervezetek által kidolgozott ajánlásokat szabványoknak nevezzük.
9. Napjaink legszélesebb körben használt WAN technológiája az Ethernet.
10. A maximális átviteli egység (maximum transmission unit, MTU) az Ethernet esetében 1536 oktett.

4. HÁLÓZATI ESZKÖZÖK

4.1 CÉLKITŰZÉS

A hálózatokba kötött számítógépek között az átviteli közeg feladata, hogy biteket juttasson egyiktől a másikig. A gépeket hálózattá összekötő közeg azonban sokféle lehet.

Ebben a leckében megismeri az aktív és passzív eszközök fogalmát. Megismerkedik a hálózati kártya, a repeater, a hub, a bridge, a switch, a router és a gateway szerepével a hálózatok felépítésében.

Megtudja mi az az Access Point. És megismerkedik napjain leggyakrabban használt hálózati kábeltípusaival.

4.2 TARTALOM

- Az aktív és passzív eszközök
- A hálózati kártya
- A repeater
- A hub
- A bridge
- A switch
- A router
- A gateway
- Az access Point
- Az UTP
- Optikai kábelek

4.3 HÁLÓZATI ESZKÖZÖK

A hálózati eszközök olyan szoftver- és hardver eszközök, amelyek segítségével a hálózat fizikailag megvalósítható. Jelenleg több gyártó különféle eszköze áll a hálózatot kiépíteni szándékozók rendelkezésére. Az utóbbi évtizedben ezek az eszközök is ugrásszerű fejlődésen mentek át, például az átlagos átviteli sebességük (10-ről 1000 Mb/s-ra) nőtt, és megjelentek az vezeték nélküli hálózathoz szükséges ún WLAN vagy Wi-Fi eszközök is, amelyek akár 300 Mb\s sávszélességet is képesek biztosítani[3].

4.3.1 Az aktív és passzív eszközök

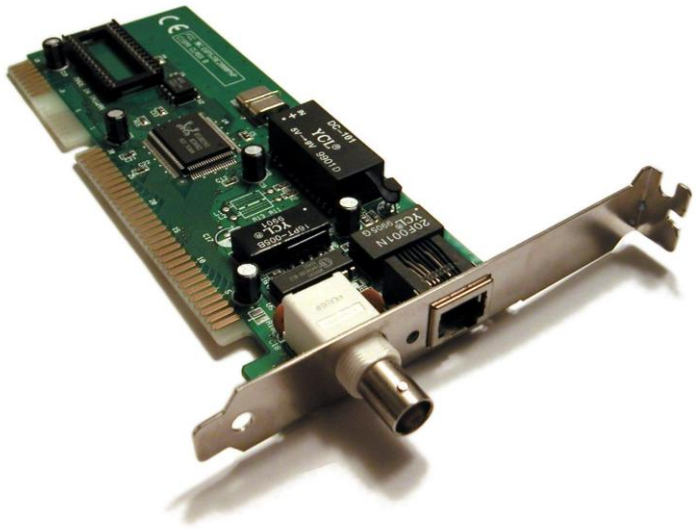
Tekintsük át, mit jelent az aktív és a passzív eszközök fogalma. Egy jel megy a kábelen. Elérkezik egy eszközhöz, ami ezeket a jeleket szétosztja. Ez az eszköz lehet aktív és passzív abból a szempontból, hogy a rajta átfolyó jelekkel mit csinál. Ha csak simán továbbadja/szétosztja, akkor passzív eszköz, mert nem csinál mást, mint továbbítja a bemenetén kapott jelet. Amennyiben ezen jeleket erősíti is, akkor már aktív. Jelerősítés akkor lehet

[3] Akár több gigabites sávszélességű vezeték nélküli hálózati kapcsolatok építhetők fel a jövőben Wi-Fi technológiával, a 802.11b/g/n szabványok és a WiGig technológia kereszteződése révén.

fontos, ha a hálózat szegmense túl nagy ahhoz, hogy a jelek biztonságosan (jelveszteség nélkül) eljussanak a célállomásra. A jelvesztés akkor fordul elő, amikor túl hosszú a kábel a célállomás felé. Ilyen esetben van szükség erősítőre, jelismétlőre.

4.3.2 A hálózati kártya

A számítógépek hálózatra kapcsolódását és az azon történő kommunikációját lehetővé tevő bővítőkártyát nevezzük hálózati kártyának. Minden kártyához tartozik egy úgynevezett **MAC cím**, ami a hálózatban a használt protokolltól függetlenül **egyértelműen azonosítja a kártyát**. A mai korszerű számítógépeken már nem külön kártya, hanem az alaplapra integrált eszköz. Hordozható számítógépek esetében vagy magába a számítógépbe van beépítve, vagy apró PCMCIA „Personal Computer Memory Card International Association” kártyaként.



Hálózati kártya

4.3.3 A repeater

A hálózati szegmensek fizikai méretkorlátainak feloldására szolgáló legegyszerűbb eszköz a jelismétlő (Repeater). Feladata, **újragenerál**ni az átvitel közbeni csillapítás miatt eltorzult analóg vagy digitális **jeleket.** Olyankor használjuk, amikor egy hálózati szegmens már elérte a maximális hosszát, de a hálózatot tovább szeretnénk bővíteni/ 3. animáció /. Mivel a repeater csak a bitek jeleinek erősítésével foglalkozik, kijelenthetjük, hogy ez az eszköz az **OSI modell fizikai** szintjén működik. A jelismétlőket elterjedten a busz topológiájú LAN-oknál használják. Felhasználásánál mindkét hálózati szegmensnek ugyanolyan típusúnak kell lennie. Forgalomirányítást nem végez.

Ismétlő

4.3.4 A hub

A **hálózati kapcsolatokat összefog**ó eszköz a hub. Kicsit másképp fogalmazva a hub a készülékek egy csoportját egyetlen készülékként láttatja a hálózat számára. Ez passzívan megy végbe, anélkül, hogy ténylegesen változtatna a rajta áthaladó adatforgalmon.

Három típust különböztethetünk meg. A passzív hub: csupán fizikai összekötő pontként szolgál, nem módosítja vagy figyeli a rajta keresztülhaladó forgalmat, tápellátást nem igényel. Az aktív az állomások összefogásán kívül a jeleket is újragenerálja, ehhez tápellátást igényel. Az intelligens hubok aktív hubként üzemelnek, mikroprocesszorral és hibakereső képességekkel rendelkeznek. A hubokat néha koncentrátoroknak is hívják, mert az Ethernet LAN-ok központi csatlakozási pontjaként szolgálnak.

HUB

4.3.5 A bridge

A hálózati híd (bridge) a **LAN**-ok **összekapcsolás**át végzi. Az eltérő hálózati adatformátumokat átalakítja, és alapszintű adatátvitel-kezelést végez. Ellenőrzi is az adatokat, hogy megállapítsa, valóban át kell-e haladniuk a hídon. Az **OSI modell adatkapcsolati** rétegében működnek.

4.3.6 Switch

A munkacsoportos kapcsolók (switchek) többnyire az **OSI modell adatkapcsolati** rétegében dolgozó, a hídnál intelligensebb adatátvitel-kezelést megvalósító eszközök. Meg tudják állapítani, hogy a LAN-on kell-e maradniuk az adatoknak, és a MAC címek vizsgálatával képesek közvetlenül a célnak megfelelő portra továbbítani az adott keretet. Felfoghatjuk gyors működésű, **többportos hálózati híd**nak is, a kapcsoló azonban nem alakítja át az adatátviteli formátumot. A switch az aktív hubbal szemben csak arra a kábelre teszi ki a kereteket, amelyeken a címzett gép található. A többi kábeleken lévő hostokkal nem keletkezhet ütközés. A switch további jellemzője, hogy az egymással kommunikáló szegmenseket „fémesen" összekapcsolja, lehetővé téve ezzel a gyors adatátvitelt. A kapcsolók a hidaknál jóval nagyobb sebességgel működnek, emellett további szolgáltatásokat is biztosíthatnak, például virtuális LAN szolgáltatást.

Switch

4.3.7 A router

A forgalomirányító (router) az eddig felsorolt eszközök tulajdonságaival együttesen rendelkezik. Tud jelet erősíteni, kapcsolatokat összefogni, adatkonverziót végezni és kezeli az a adatátvitelt. A nagyobb, csomagkapcsolt hálózatokban szükség van arra, hogy egy csomag elküldését megelőzően kiválasszuk a megfelelő útvonalat. Ezt a feladatot is az **OSI modell hálózati réteg**ében működő routerek látják el. Ezen kívül WAN-hoz tud kapcsolódni, aminek köszönhetően egymástól nagy távolságra lévő LAN-ok összekapcsolására is alkalmas. A routerek típusai:

- Szolgáltatói (ISP – Internet Service Provider)
- Vállalati, nagyvállalati
- SOHO (Small Office, Home Office), Otthoni-Irodai (kisvállalati)

Router

4.3.8 Gateway

A legbonyolultabb hálózat-összekapcsolási módszer a hálózati zsilip (gateway). Hálózati zsilipet az egymástól teljes mértékben különböző hálózatok összekapcsolására alkalmaznak. Ha eltérő hálózati architektúrákat használnak, a protokollok különbözhetnek bármelyik vagy minden hálózati rétegen. A hálózati zsilip minden átalakítást elvégez, ami az egyik protokollkészletből a másikba való átmenet során szükséges (üzenetformátum-átalakítás, címátalakítás, protokoll-átalakítás). A TCP/IP elterjedése miatt gyakorlatilag megszűnt.

4.3.9 Az Acces Point

A vezeték nélküli hálózatok építőkövei az úgynevezett hozzáférési pontok (AP, Access Point), amelyek a WLAN infrastruktúra módban üzemelő készülékek számára központi hubként szolgálnak. Ezek sugározzák az SSID (Service Set Identifier, beállított szolgáltatóazonosító) csomagokat, amelyek alapján a kliensek csatlakozni tudnak a hálózathoz. Az AP kábellel csatlakozik a vezetékes LAN-hoz, így kapcsolódási lehetőséget vagy akár internetelérést biztosít a vezeték nélküli készülékek számára. Az AP-k saját antennával rendelkeznek, kapcsolódási lehetőséget pedig meghatározott területen nyújtanak, amit cellának nevezünk. A cella méretét döntően befolyásolja az antenna mérete és teljesítménye. Nagyobb terület lefedéséhez, több AP telepítésére van szükség átfedésekkel.

Access Point

4.3.10 Az UTP

Az Ethernet hálózatokon manapság leggyakrabban az Unshielded Twisted Pair (UTP) árnyékolatlan, csavart érpáras hálózati kábeltípust használják. Az UTP kábel 4 érpárból álló réz alapú átviteli közeg, mind a 8 vezetéke szigetelőanyaggal van körülvéve, emellett a vezetékeket párosával összesodorják, így csökkentve az elektromágneses és rádiófrekvenciás interferencia jeltorzító hatását. Az árnyékolatlan érpárok közötti áthallást úgy csök-

kentik, hogy az egyes párokat eltérő mértékben sodorják. Maximális átviteli távolsága 100 m.

Viszonylagos olcsósága, könnyű telepíthetősége tette rendkívül népszerűvé az évek során. Előnyeként szolgál kis átmérője, mely által kevesebb helyet foglal a kábelcsatornákban. Hátrányaként említhető külső interferencia-források elleni viszonylagos védtelensége, valamint kis átviteli távolsága.

A kábel végein 8P8C (gyakran RJ-45-nek nevezett) csatlakozók találhatók, amellyel a hálózati interfészekhez csatlakozik. A kábeleket kategóriákba sorolják és CAT+szám típusú jelzéssel látják el.

- CAT1 – telefonkábel (hangátvitel, 2 érpár).
- CAT2 – maximum 4 Mb/s adatátviteli sebesség érhető el vele.
- CAT3 – 10 Mb/s az adatátviteli sebessége. Csillag topológiánál alkalmazzák, ethernet hálózatokban (Legacy Ethernet[10MB/s-os] közege).
- CAT4 – max. 20 Mb/s adatátviteli sebességű.
- CAT5 – 100 Mb/s adatátviteli sebességű, csillag topológiánál alkalmazzák, ethernet hálózatokban.
- CAT5e, CAT6 – 1000 Mb/s átviteli sebesség.

A 10Base-T és 100Base-TX kábelek átvitelkor csak az 1, 2 (küldésre) és a 3, 6 (fogadásra) érpárokat alkalmazzák. 1000Base-TX szabványú átvitel esetén mind a 4 érpár részt vesz az adatátvitelben. Egy vezetéken maximum 125 Mb/s átviteli sebesség érhető el.

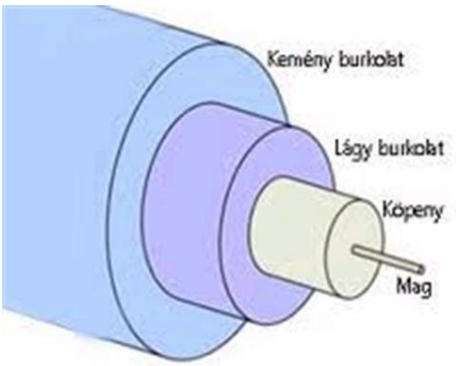
UTP kábel csatlakozóval szerelve

A felsőbb kategóriás kábelek visszafelé kompatibilisek.

4.3.11 Optikai kábelek

A számítógép-hálózatok építésének kábelei közül az optikai szálak rendkívül alkalmasak digitális információ-továbbításra. Az optikai szál információtovábbító képessége azon alapul, hogy a nagy tisztaságú optikai szálban a szálirányban besugárzott fény igen jó mi-

nőségben terjed. Az optikai szál a magból, a magot körülvevő optikai árnyékoló közegből és a mechanikai védelmet szolgáló borításból áll.



13. ábra Az optikai kábel felépítése

A fényvezető kábelek ára a technikai fejlődés során folyamatosan csökken, s így a lehetséges alkalmazások köre is egyre bővül. A fényimpulzusoknak köszönhetően hatékonyabbak, mint a hagyományos rézvezetőjű csavart érpáras UTP-kábelek.

Minden hálózati célra alkalmazott optikai kábel két üvegszálból áll, ezek külön burkolattal rendelkeznek. Az egyik szál A készülék felől B készülék felé, a másik pedig ellenkező irányba továbbítja az adatokat. Ezzel a megoldással duplex kommunikációs csatornát nyerünk. A réz csavart érpáras kábelekben külön érpár szolgál az adásra és a vételre. Az optikai szálas hálózatokban egy szálat adásra, egyet pedig vételre használunk. Az optikai kábelekben általában nagyobb számú érpárt találni. Egy-egy kábel 2-48, esetleg ennél is több szálat tartalmaz. A rézkábeleknél minden áramkör számára külön UTP kábelt kell kihúzni. Az optikai szál a réznél jóval nagyobb sebességgel, és sokkal nagyobb távolságra képes továbbítani a jeleket. Működésük szerint a fényvezető kábeleket a multimódusú (MM) illetve monomódusú (SM) kategóriákba sorolhatjuk. Az olcsóbb, multimódusú szálakra épülő rendszereket rövidebb távolságok (max. 2 km) áthidalásánál használják. Az igényesebb megoldást jelentő monomódusú rendszerek építése nagy távolságú, nagy sávszélességű adatátviteli csatornák esetén indokolt.

2. A multimódusú (MM) illetve monomódusú (SM) optikai szálak

Monomódusú vagy egymódusú optikai szál (single-mode fiber): Olyan optikai szál, mely csak egy adott frekvencián – és annak közvetlen környezetében – képes a fény átvitelére, más frekvenciákon a szál csillapítása igen erős.

Optikai kábel csatlakozóval szerelve

Az egymódusú szálak valamivel nagyobb sávszélességen képesek jelátvitelre, mint a multimódusú szálak. Monomódusú optikai szálak esetén a sávszélesség korlátlannak tekinthető. Az átvitel sebességének egyetlen korlátozó tényezője az aktív eszközök jelenlegi fejlettségi szintje. Ezért a ma installált optikai kábel akár évtizedekre megoldhatja az információs átviteli igényeket, nincs szükség drága és időt rabló újrakábelezésre.

A ma élvonalbelinek számító ún. „Fiber-to-the-Desk" rendszerekben például az üvegszálak közvetlenül a felhasználó számítógépéig futva biztosítják a magas szintű integrált hang adat és képátviteli szolgáltatást. Optikai szálakon – szabványos, piacon elérhető végberendezésekkel – biztosítható a 10Gb/s átviteli sebesség.

Adatvédelmi szempontból is tökéletes, hisz az üvegszál nem hallgatható le, s így titkos, vagy nem publikus adatokkal dolgozó, azokat feldolgozó rendszerekben biztonságosan alkalmazható, pl. katonai célú felhasználásra vagy bankok, vállalatok adatkezelő rendszereiben.

4.4 ÖSSZEFOGLALÁS

A hálózati eszközöket, aszerint hogy a rajtuk átfolyó jelet erősítik, vagy csak továbbítják, aktív illetve passzív eszközöknek nevezzük.

Az ismétlő (repeater) a jelek újragenerálására használt eszköz, mely a forgalomirányítótól eltérően intelligens forgalomirányítást nem végez.

A Hub a hálózati kapcsolatok összefogására szolgáló eszköz. Az aktív hubok a passzívaktól eltérően a jeleket is újragenerálják. Az intelligens hubok aktív hubként üzemelnek, mikroprocesszorral és hibakereső képességekkel is rendelkeznek.

A hálózati híd (bridge) a hálózatok között teremt kapcsolatot. Átalakítja a hálózati adatformátumokat, és alapszintű adatátvitel-kezelést végez. Ellenőrzi is az adatokat, hogy át kell e haladniuk a hídon, amivel segíti a különböző hálózati részek hatékonyságát.

A hálózati kapcsoló (switch) aktív hálózati eszköz, mely többnyire az OSI-modell adatkapcsolati rétegében dolgozik. A MAC címek vizsgálatával képesek közvetlenül a célnak megfelelő portra továbbítani az adott keretet; tekinthetők gyors működésű, több portos hálózati hídnak is. A kapcsoló nem alakítja át az adatátviteli formátumot.

A forgalomirányító (router) az eddig felsorolt eszközök minden tulajdonságával rendelkezik. Ezen kívül tud WAN-hoz kapcsolódni, mellyel nagy távolságú LAN-okat képes összekötni.

A hálózati zsilip (gateway)egymástól teljes mértékben különböző hálózatok összekapcsolására alkalmas. Az eltérő hálózati architektúrák használatánál, a protokollok különbözhetnek bármelyik vagy minden hálózati rétegen. A hálózati zsilip minden átalakítást elvégez, ami az egyik protokollkészletből a másikba való átmenet során szükséges (üzenetformátum-átalakítás, címátalakítás, protokoll-átalakítás).

A hozzáférési pont (Access Point, vagy röviden AP) kapcsolódási lehetőséget nyújt a vezeték nélküli készülékek számára. A LAN-okhoz vezetékkel kapcsolódik, és megoldja a különböző gyártók hálózati csatolóinak kompatibilitási problémáit. Saját antennával rendelkezik, és az ezzel lefedett területen nyújt kapcsolódási lehetőséget, amit cellának hívunk.

Az ethernet hálózatok legelterjedtebb vezetéktípusa a 8 érből álló UTP (Unshielded Twisted Pair) kábel. A vezetékek szigetelőanyaggal van körülvéve, emellett a vezetékeket párosával összesodorják, így csökkentve az elektromágneses és rádiófrekvenciás interferencia jeltorzító hatását. A kábelek végein 8P8C-s csatlakozók találhatók. A kábeleket kategóriákba sorolják és CAT+szám típusú jelzéssel látják el. A CAT5-ös kábel – 100 Mb/s adatátviteli sebességű, csillag topológiánál alkalmazzák, ethernet hálózatokban. A CAT5e, CAT6 jelölésűek- 1000 Mb/s átviteli sebességre képesek.

Az optikai szálak rendkívül alkalmasak digitális információ-továbbításra, így a számítógépes-hálózatok fontos építőelemei. Az optikai szál információtovábbító képessége azon alapul, hogy a nagy tisztaságú optikai szálban a szálirányban besugárzott fény igen jó minőségben terjed. Az optikai szál a magból, a magot körülvevő optikai árnyékoló közegből és a mechanikai védelmet szolgáló borításból áll. Működésük szerint a fényvezető kábeleket a multimódusú (MM) illetve monomódusú (SM) kategóriákba sorolhatjuk.

4.5 ÖNELLENŐRZŐ KÉRDÉSEK

1. A passzív eszköz nem csinál mást, mint továbbítja a bemenetén kapott jelet.
2. A számítógépek hálózatra kapcsolódását és az azon történő kommunikációját lehetővé tevő bővítőkártyát nevezzük hálózati hídnak.
3. Minden hálózati kártyához tartozik egy úgynevezett MAC cím.
4. A hálózati szegmensek fizikai méretkorlátainak feloldására szolgáló legegyszerűbb eszköz a jelismétlő (Repeater).
5. A hálózati híd (bridge) a LAN-ok összekapcsolását végzi.
6. A munkacsoportos kapcsolók (switchek) többnyire az OSI modell fizikai rétegében dolgozó, a hídnál intelligensebb adatátvitel-kezelést megvalósító eszközök.
7. A nagyobb, csomagkapcsolt hálózatokban szükség van arra, hogy egy csomag elküldését megelőzően kiválasszuk a megfelelő útvonalat.
8. Hálózati zsilipet az egymással teljes mértékben megegyező hálózatok összekapcsolására alkalmaznak.
9. Az UTP kábel mind a 6 vezetéke szigetelőanyaggal van körülvéve, emellett a vezetékeket párosával összesodorják, így csökkentve az elektromágneses és rádiófrekvenciás interferencia jeltorzító hatását.
10. Működésük szerint a fényvezető kábeleket a multimódusú (MM), illetve monomódusú (SM) kategóriákba sorolhatjuk.

5. AZ INTERNET MŰKÖDÉSE

5.1 CÉLKITŰZÉS

Napjainkban felhasználók millióit köti össze a „hálózatok hálózatának” nevezett internet. Az egész világot körülölelő számítógép-hálózat olyan hatalmas rendszer, amely kisebb számítógép-hálózatokat kapcsol össze. Az internet olyan gyorsan növekszik, hogy minden erre vonatkozó számadat pár hónap alatt elavul.

Az internetes technológiák beépülnek életünkbe. Az internetet használhatjuk személyes, illetve üzleti célokra, például információkeresésre, szolgáltatások és áruk megrendelésére, kapcsolattartásra, szórakozásra stb.

A leckéből megismerheti kialakulásának történetét és ismereteket szerezhet működéséről.

Tudni fogja az IP címek jelentőségét, megismeri ezek jelenlegi és jövőbeni formáját.

5.2 TARTALOM

- Az internet története
- Az internet felépítése
- Az IPv4-es címzési mód
- Az IPv6-os címzési mód
- A címzési módok összehasonlítása
- Kompatibilitás a címzési módok között
- Az internet szállítási protokolljai
- Az internet vezérlő protokolljai

5.3 AZ INTERNET

Az Internet nyílt architektúrájú, technikai szempontból számítógépek és számítógép-hálózatok központ nélküli, összekapcsolt hálózata.

5.3.1 Az internet története

A számítógépes hálózatok rohamos fejlődésének eredményeképpen létrejött a világ egészére óriási hatást gyakorló Internet, vagyis a számítógépes világhálózat. Története az 1960-as évekre nyúlik vissza. Az 1960-as években az Egyesült Államokban is uralkodott a hidegháborús hangulat. A háttérben zajló háborús készülődés, a fegyverkezési verseny nem kerülhette el az informatikát sem. Ebben az időszakban még nem beszélhettünk személyi számítógépekről, a különböző oktatási, ipari, és kormányzati intézményekben nagygépek helyezkedtek el. Felmerült azonban az igény arra, hogy ezeket az egyébként egymástól gyakran nagy távolságra elhelyezkedő számítógépeket kommunikációs csatornákkal kössék össze annak érdekében, hogy a gépek képesek legyenek az egymással való kommunikációra. Kezdetben erre a hagyományos telefonvonalakat használták, hiszen ez a lehetőség kínálkozott a legolcsóbbnak. Olcsósága és egyszerű mivolta mellett azonban ez a technológia számos hiányossággal rendelkezett. Ezek közül éppen a hidegháborús hangulat

világított rá arra a problémára, hogy a telefonhálózat központokhoz kötött kommunikációt tesz lehetővé, vonalkapcsolt adattovábbításra ad lehetőséget. Ez igen sebezhetővé teszi a rendszert. Tekintve, hogy egy telefonközpont akár több egymással kommunikáló számítógép párt is összeköthet, egy ilyen csomópont esetleges sérülése, a teljes kommunikáció megbénulásához vezethetne. Ezért az Egyesült Államokban felvetődött egy újabb, csomópontoktól mentes, decentralizált hálózat kiépítésének gondolata.

A hálózat kialakításban az alábbi szempontokat tartották szem előtt:

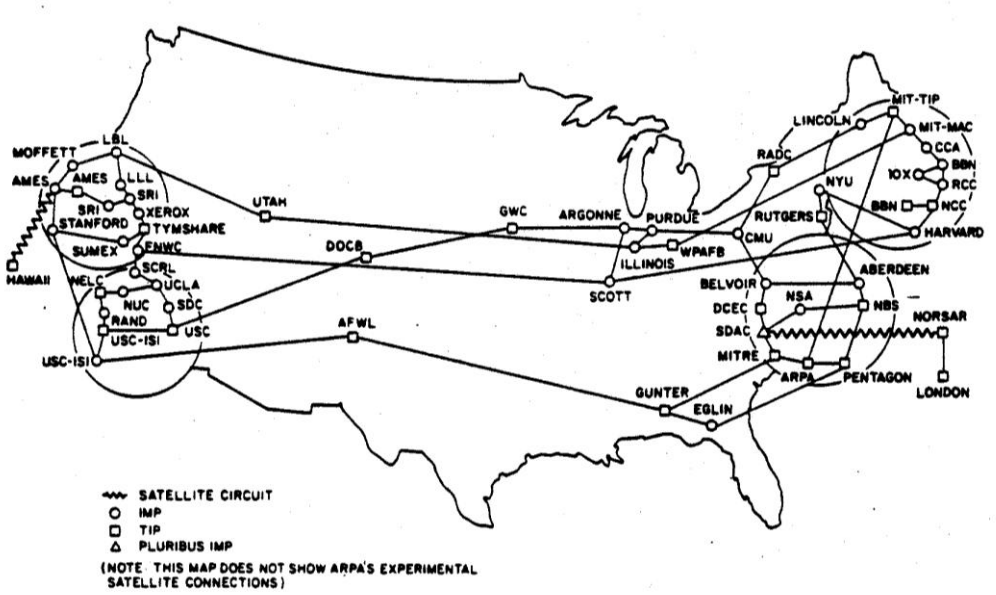
- A hálózat legyen központoktól mentes.
- A hostok ne csak egy, hanem több csatornát is használhassanak az egymással való kommunikációhoz.
- A hálózat legyen garanciamentes, azaz a hostok ne feltételezzék hibátlan működését, hanem ők maguk gondoskodjanak az ellenőrzésről.
- A hálózat ne végezzen az adatokkal különböző kódolási, átalakítási műveleteket – azt végezze el az adatot küldő és fogadó állomás – csupán adattovábbítással foglalkozzon.
- A továbbított üzenetek ne egyetlen adatfolyamként, hanem kisebb egységekre, csomagokra tagolva haladjanak rendeltetési helyük felé.
- Az üzenet csomagjai akár egymástól eltérő útvonalon is eljuthassanak a címzett számítógéphez.

Természetes, hogy egy ilyen hálózat kialakítása komoly anyagi befektetést igényel, de mivel katonai jelentősége nem volt megkérdőjelezhető, az Egyesült Államok Védelmi Minisztériuma támogatta a kezdeményezést. Az elmélet az anyagi lehetőségek megteremtődésével valóra válhatott, megkezdődhetett az Internet elődjének az ARPANET-nek a felépítése. Az alábbiakban áttekintjük a hálózat kialakulásának legfontosabb lépéseit:

- 1969: Létrejön az **ARPANET**, amely egyelőre 4 számítógépet köt össze egymással.
- 1971: Az ARPANET már 15 nagyszámítógép hálózata.
- 1972: Az év második felében 37 gép alkotja a hálózatot. Ezekhez a csomóponti gépekhez később további hostokat is kapcsolnak, amelyek így részei lesznek az ARPANET-nek. A csomóponti gépek alkotta hálózatot gerinchálózatnak, az azokhoz csatlakozó hostok alkotta helyi hálózatokat pedig alhálózatoknak kezdték nevezni.

1974: Az ARPANET-et alkotó gépek egyre különbözőbb hardverrel rendelkeznek, és gyakran egymástól eltérő szoftvereket futtatnak. A különböző „nyelveken beszélő” gépek kommunikációjának összehangolása egyre nagyobb nehézségeket jelent, ezért szükségessé válik egy új, minden ARPANET-hez csatlakozó gépre érvényes kommunikációs szabvány bevezetése. Ebben az évben dolgozzák ki és vezetik be a TCP/IP-t, ami valójában egy OSI modellhez hasonló rendszer, azzal a különbséggel, hogy ez nem csupán ajánlás, hanem ténylegesen megvalósított, működő rendszer. A TCP/IP hálózati feladatokat megvalósító rétegek és a közöttük használt protokollok halmaza, azaz hálózati architektúra. Ezen túl az ARPANET gépei a TCP/IP hálózati architektúránk megfelelően kommunikálnak egymás-

sal. A TCP/IP bevezetése magában hordozza egy egységes címzési rendszer, az IP címek bevezetését is.



ARPANET architektúra 1976

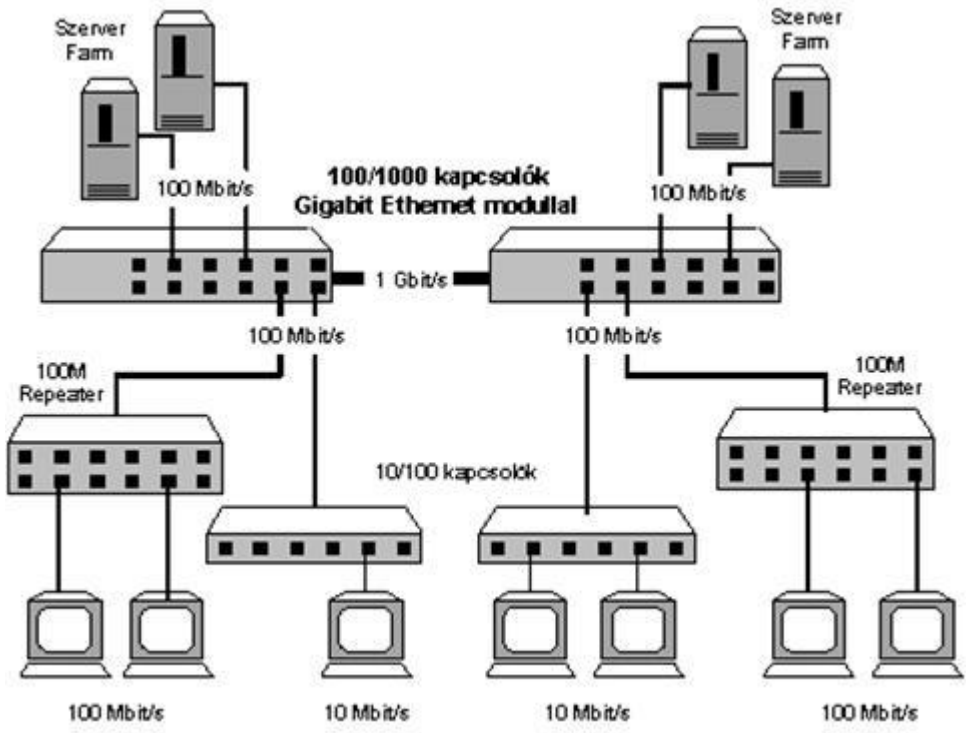
- 1983: Az ARPANET-et egyre több polgári felhasználó szeretné alkalmazni, a hálózat katonai jellege azonban gátat szab ennek. Az ARPAnet mellett létrehozták a hasonló technológiával működő MILnet (Military Network) hálózatot, és ebben az évben a két hálózatot összekapcsolták. Az ARPANET-hez ezután több hálózat is hozzákapcsolódott; pl. a MInet (a MILnet európai megfelelője), a SATnet és WIDEBAND (műholdas hálózatok), az NFSnet (National Science Foundation Network), a BITnet (Because It's Time Network), a USEnet stb.
- 1980-as évek közepe: A hálózat olyan méreteket ölt, hogy ésszerűnek látszik a hostok különböző csoportokba rendezése. Kialakítják, illetve bevezetik az úgynevezett Domain Naming Systemet (területi elnevezési rendszer), ahol a domainek (területek) azonos témakörökkel foglakozó számítógépek csoportjai. Az egyes domaineket három karakteres domain azonosítóval látják el. A különböző domainekbe tartozó gépek az IP cím mellett alfanumerikus nevet is kapnak, amelyben megjelenik a domain azonosító is – www.ektf.hu –. Később az Internet kialakulásakor a felhasználási terület szerinti domainek kevésnek bizonyulnak, így bevezetik a földrajzi területekhez kötött domaineket. Ezek már két karakteresek, és az egyes országokat azonosítják. Magyarország domain azonosítója tehát a HU.
- 1989: A Pentagonnak már nem érdeke az ARPANET fenntartása, ezért beszünteti a hálózat támogatását. Ez első pillantásra a hálózatvégét is jelenthetné, azonban erre az időre, az ARPANET mintájára már számos országban létrehoztak olyan hálózatokat, amelyek a tudományos kutatás céljait szolgálták, és amelyek saját ge-

rinchálózattal rendelkeztek. Ilyen hálózat az Egyesült Államokban a Nemzeti Kutatási Alap (U.S.National Fundation Found, NSF) által létrehozott NSFNET, illetve a néhány évvel később Magyarországon létrehozott HUNGARNET. Az egyes országok gerinchálózatát egymással összekapcsolva egy globális, világméretű hálózat jött létre, amit Internetnek nevezünk.

- 1990-es években már a nagy számítógépes kereskedelmi szolgáltató központok (CompuServe, America Online, stb.) is elérhetőek az Interneten keresztül és az üzleti alkalmazások köre azóta is rohamosan bővül.

5.3.2 Az internet és a TCP/IP kapcsolata

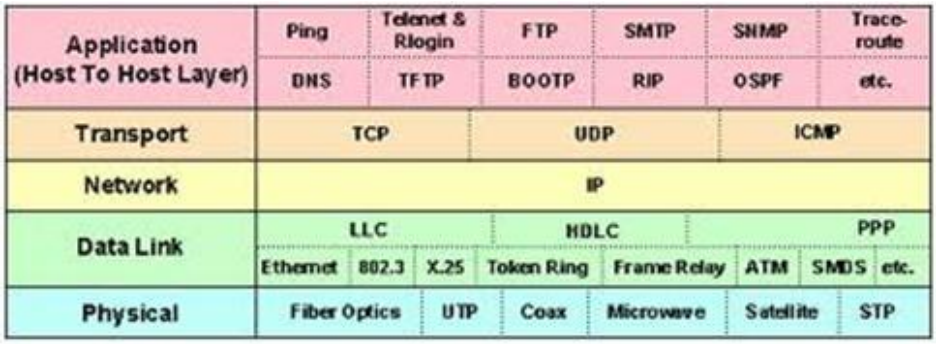
Az internet technológiai célja: az egymástól eltérő fizikai architektúrájú hálózatok összekapcsolása annak érdekében, hogy a hálózatban szereplő gépek egymással kommunikálni tudjanak.



14. ábra Eltérő technológiák kapcsolódása

Ahhoz, hogy a hálózat gépei együtt tudjanak működni, szabványosítani kellett a kommunikáció módját. A TCP/IP nem más, mint egy protokollkészlet, amelyet arra dolgoztak ki, hogy hálózatba kapcsolt számítógépek megoszthassák egymás között az erőforrásaikat.

Az Internet alapvetően a TCP/IP rétegmodellre épül. Az egyes rétegekben működő protokollok áttekintését a15. ábrán láthatjuk. A protokollok listája nem teljes, csak néhány jellegzetes elemet tartalmaz.



15. ábra TCP/IP protocol stack

5.3.3 Az internet működése

A hálózatban egyedi, egymástól független adatcsomagok haladnak, melyeknek a célhoz vezető útvonalát a csomagban lévő cím alapján keressük.

Nem biztos, hogy ilyen útvonal van, vagy ha létezik, akkor biztosan megtaláljuk meghatározott időn belül!

A hálózat csomópontjain forgalomirányítók (routerek) vannak, melyek táblázatokat (Routing tables) tartanak fenn a célokhoz vezető útvonalakról. A routing táblázat egy kis adatbázis a routeren belül, ami segítségével az eldöntheti, hogy egy adott csomagot merre továbbítson. Belátható, hogy elegendő azoknak a szomszédos csomópontoknak a tárolása, ami a célhoz vezet, nem kell a teljes útvonalat tárolni.

Az IP Routing olyan folyamat, amelynek segítségével egy több hálózati interfésszel rendelkező host eldönti, hogy a kapott IP csomagokat merre továbbítsa / 5. animáció /.

3. Az útvonal meghatározása (IP routing)

Képzeljünk el egy kisebb céget, amelynek van egy routere, amely két Ethernet interfésszel rendelkezik a cég két alhálózatához, és egy interfésszel az Internet felé. Amikor a router kap egy csomagot valamelyik interfészén keresztül, a routing az a mechanizmus, amelynek segítségével eldönti, hogy melyik interfészén kell tovább küldenie.

A további útvonal meghatározása a következő router feladata. A szolgáltatás datagram[4] jellegű, a csomagok ezért

- elveszhetnek,
- többszöröződhetnek,
- beérkezési sorrendjük megváltozhat.

A biztonságos átvitelről a felettes rétegeknek kell gondoskodni.

[4] Csomagkapcsolt hálózatokon továbbított adatcsomag, amelynek sem érkezési sorrendje, sem maga érkezése a célállomásra nem garantált.

5.3.4 Az IP címek

Ahhoz, hogy az Interneten egy adatcsomag elérhesse célját, szükség van arra, hogy a csomagban szerepeljen a cél host egyedi, őt minden más géptől megkülönböztető címe. Az Interneten alkalmazott TCP/IP modell erre az úgynevezett IP címet használja. A hálózati végpontok (számítógépek, kamerák, nyomtatók, mobil eszközök stb.) azonosítására szolgáló egyedi azonosító jelenleg a negyedik generációját éli, innen ered a neve IPv4 (Internet Protocol version 4). Az Ipv4-es címek használata azonban több problémát is felvet. Ezért készült el az Internet Protocol újabb verziója az IPv6, mely hosszú távú megoldást kínál a felmerült problémákra.

A címeket egy amerikai szervezet, a NIC (Network Information Center) osztja ki, de általában nem közvetlenül, hanem területi megbízottjain keresztül. Egy vállalat vagy szervezet internetszolgáltatójától mindig címtartományt kap, amelyen belül szabadon jelölheti ki gépeinek címét.

> Az alkalmazási rétegben elhelyezkedő, hálózati kommunikációt kiszolgáló programok ettől eltérő címzési rendszereket is használhatnak.

5.3.5 Az IPv4

Az IPv4-es cím egy 32 bites, azaz 4 bájtos azonosító, amelyben a bájtok értéke 0-255 közé esik. A 4 bájtos cím bájtjait pontokkal választjuk el egymástól (pl. 192.168.50.100). Ebben a formában minden egyes tag 8 bitet jelöl, és minden bit kétféle értéket mutathat (0-t és 1-et), vagyis egy tag 2^8-féle alakot vehet fel. Így ez a fajta számozás 2^{32} mennyiségű különböző IP-címet tud megkülönböztetni.

Az IP címek öt, az ABC betűivel jelzett kategóriába, úgynevezett címosztályba sorolhatók. A vállalatok vagy szervezetek méretüknek megfelelően háromféle címtartományt (címtípust) kaphatnak. A címtartomány típusát az IP-cím első bitjei jelzik. Ezután következik a hálózat azonosítására szolgáló bitsor (NetID), majd a hálózaton belül a gépek azonosítására szolgáló szakasz (HostID). Annak meghatározására, hogy melyik rész hány bitből áll, a netmaszkot használjuk. A netmaszk egy 32 bites szám, amelynek 1-es bitjei mondják meg, hogy meddig tart a hálózat címe, és hol kezdődik a gép címe.

Egy példán ábrázolva könnyebben megértjük:

Host cím: 192.168.1.7

Host cím(binárisan): 11000000 10101000 00000001 00000111

Netmaszk: 255.255.254.0

Netmaszk (binárisan): 11111111 11111111 11111110 00000000

A példánkból láthatjuk, hogy a netmaszk 32 bitjéből 23 az 1 értéket vette fel míg 9 a 0 értéket. Ez azt jelenti, hogy netmaszk 23 bitje írja le a hálózatot, míg 9 bitje a hálózaton szereplő gépek maximális számát adja meg. Kettes számrendszerben 9 biten a legnagyobb szám az 511, tehát elmondhatjuk, hogy a példánkban szereplő hálózat megfelel a 192.168.0.0/23 jelöléssel leírható hálózatnak, amely maximálisan 512 IP címet képes fenntartani.

A címosztályok kialakítására azért volt szükség, mert vannak nagyon sok gépből és vannak viszonylag kevés hostból álló hálózatok is. Az IP címnek, viszonylag kevés kihasználatlan bitet hagyva, a lehető legtöbb host azonosítására kell alkalmasnak lennie.

- A osztályú IP cím: Az A osztályú IP címeket olyan hálózatoknak osztják ki, amelyek nagyon sok gépből épülnek fel. Mivel az ilyen hálózatokból viszonylag kevés van, a hálózat azonosítására csak az első bájt 7 legalacsonyabb helyi értékű bitjét használják fel, a legmagasabb helyi értékű bit mindig 0. A host azonosítása az első bájtot követő három bájton történik. Az A osztályú IP címek első bájtja 1-126 közötti, míg az azt követő bájtok 0.0.1-255.255.254értéket vehetnek fel. A osztályú hálózatból tehát 126 létezhet, de ezek mindegyike közel 16 millió gépet tartalmazhat.
- B osztályú IP cím: A B osztályú IP címeket kisebb gépszámmal rendelkező hálózatokban használják. Ilyen hálózatból jóval több van, mint A osztályúból, ezért a hálózat megjelölésére itt az első két bájtot használják, de az első bájt 8. bitje mindig 1, a 7. bitje pedig mindig 0.A hostokat az utolsó két bájt azonosítja. A használható legkisebb hálózati cím a 128.0, a legmagasabb pedig a 191.255. A hosztok címe a 0.1-255.254 tartományba kell, essen. Összesen tehát hozzávetőleg 16 ezer B osztályú hálózat létezhet, amelyek mindegyikét kb. 65 ezer host alkothatja.
- C osztályú IP cím: A fenti logikát követve hamar rájöhetünk, hogy a C osztályú hálózatok a legkisebbek, azonban ezekből van legtöbb az Interneten. Az ilyen hálózatok azonosítására az IP cím első három bájtját használják, úgy, hogy az első bájt legfelső két bitje 1, az azt követő bit mindig 0 értékű. A hálózat hostjainak címét az utolsó bájt lehetséges értékei adhatják. A legkisebb hálózati cím a 192.0.0, a legnagyobb pedig a 223.255.255, C osztályú hálózatból tehát kb. 2 millió lehet. A hosztok címe 1-254 közé kell, hogy essen, ami azt jelenti, hogy egy ilyen hálózatot mindössze 254 gép alkothat.
- D osztályú IP címek: A D osztályú címzéseket arra használják, hogy egyszerre több hosthoz juttassanak el csomagokat. Az ilyen címek első bájtjának legfelső három bitje 1, az azt követő bit pedig mindig 0 értékű.
- E osztályú IP címek: Az E osztályt, amelyben az IP cím első négy bitje midig 1, később meghatározandó célokra tartják fent.

Az IPv4-cím beállítása kétféle módon történhet:

- automatikusan kapjuk a beállításokat: a gép DHCP[5] segítségével kéri le a hálózati beállításokat. A DHCP kiszolgáló adja meg a gép IP-címét és más konfigurációs beállításait, legtöbb esetben a DNS kiszolgáló automatikus lekérése mellett.

Ha az IP-cím kezdő száma 169.xxx.xxx.xxx, akkor a DHCP kiszolgáló nem megfelelően osztotta ki a címet vagy a hálózaton nincs engedélyezve a DHCP.

[5] A dinamikus állomáskonfiguráló protokoll (angolul Dynamic Host Configuration Protocol, rövidítve DHCP) egy számítógépes hálózati kommunikációs protokoll. Ez a protokoll azt oldja meg, hogy a TCP/IP hálózatra csatlakozó hálózati végpontok (például számítógépek) automatikusan megkapják a hálózat használatához szükséges beállításokat. Ilyen szokott lenni például az IP-cím, hálózati maszk, alapértelmezett átjáró stb.

- statikusan akarjuk beállítani azt – ekkor sorra meg kell adni az ip címet (pontozott decimális formában), az alhálózati maszkot (hasonló formában) és az alapértelmezett átjárót. (Az ismeretlen IP című csomagok fognak ide továbbítódni.) / 1, 11. videó /

Különlegességek az IPv4-ben

- Ahogy a fenti címkiosztásból látható, a 127.0.0.0/255.0.0.0-es címtartomány kimaradt. Az ilyen címek speciális, úgynevezett loopback címek. A loopback egy olyan áleszköz, ami a saját számítógépünket jelenti. Bármelyik cím a 127.0.0.0 tartományon belül a saját számítógépünkkel kommunikál.

- Ha egy IP cím, hostokat címző része csak 1-esekből áll, az hálózat összes gépének címzését jelenti. Az ilyen címet broadcast (műsorszórás) címnek nevezik. Ezzel a címmel az összes helyi gépet megcímezhetjük, ún. körüzenetet küldhetünk ide, és azt az összes állomás venni fogja. A broadcast címnek foglalt az adott networkon megcímezhető legnagyobb hostcím. Tehát a címben a host részen csupa 1-es szerepel. Így a fenti 192.168.50.0/255.255.255.0 tartományban a broadcast számára a foglalt a 192.168.50.255 cím.

5.3.6 IPv6

Az IPv6-os cím 128 bites, azaz 16 bájtos azonosító. Ezt kettősponttal elválasztott hexadecimális számokkal írjuk le, minden szám 16 bitet reprezentál. Tehát elvileg 8 darab hexadecimális szám kettősponttal elválasztva (pl. fe80:0:0:0:2e5:fa01:125b:ef) . Egy csoportban az elöl álló nullák elhagyhatók. Az IPv4 32 bites címzése helyett az IPv6 128 bitet használ címzésre, ami elméletileg 2^{128} cím kiosztását teszi lehetővé. Lényeges, hogy megszűntek a különböző méretű hálózatokon alapuló tartományok. Az eddigi A, B és C osztályú címtartományokhoz képest jóval gazdaságosabban és a rugalmasabb címkiosztási módszerek bevezetésével lényegesen jobban lehet kihasználni a címeket.

Az IPv6-os címek, hasonlóan az 4-es IP címekhez alapvetően két részre vannak osztva. A cím áll egy hálózati részből, és egy interfész-azonosító részből. Az Ipv6-os címek három csoportba gyűjthetők az alapján, hogy a hálózaton hogyan történik egy csomag továbbküldése.

- **Egyedi (unicast) cím**: egy interfészhez rendelt cím. Az erre a címre küldött csomag az adott interfészhez lesz kézbesítve. Leginkább ez a típus hasonlít az IPv4-ben használatos címekre.
- **Bárki (anycast) cím**: interfészek egy csoportjához rendelt cím. Ezeknek azonban nem kell feltétlenül ugyanazon a gépen lenniük, sőt akár egymástól távol is lehetnek. A forgalmat, amit ilyen címre küldünk, legalább egy interfész meg fog kapni az ezzel a címmel rendelkező csoportból. Az erre a címre küldött csomag valamelyik, az útválasztás (routing) által legközelebbinek ítélt interfészhez lesz közvetítve. Fontos megjegyezni, hogy szintaktikailag az anycast cím nem különböztethető meg az unicast címtől. Mivel az unicast/anycast címek formátuma megegyezik, megkülönböztetésük csak a hálózati konfiguráció alapján lehetséges.

- **Csoport (multicast) cím**: interfészek egy csoportjához rendelt cím. Hasonlóan az anycast címekhez, azonban itt a csoport minden tagja megkapja a küldött csomagokat. IPv6-ban ilyen címeket használunk az IPv4-es broadcast címek helyett.

Különlegességek az IPv6-ban

IPv6-ban minden hálózati eszköznek több címe van:

- **globális cím:** A globális cím az egész interneten egyedi cím, aminek segítségével az eszköz, illetve gép bárhonnan megcímezhető.
- **link-local cím:** Az adott hálózaton egyedi cím. Mindig „fe80”-al kezdődik, tehát a hálózati cím fe80::/64. A cím a hálózaton kívülről nem érhető el.
- **site-local cím:** Egy olyan cím mely elérhető az adott hálózaton belül, és a többi alhálózatról, például egy szolgáltatóhoz tartozó hálózatok. Ezek a címek „fec02”-al kezdődnek.

A globális, és link-local címet általánosan használják, a site-local kevésbé elterjedt.

Speciális IPv6-címek:

- **Meghatározatlan cím:** A meghatározatlan cím (0:0:0:0:0:0:0:0 vagy ::) a cím hiányát jelöli. Megfelel az IPv4 0.0.0.0 meghatározatlan címének. A meghatározatlan cím általában forráscímként használatos az ideiglenes címek egyediségének ellenőrzését megkísérlő csomagokhoz. A meghatározatlan cím soha nincs kapcsolathoz rendelve vagy célcímként használva.
- **Visszacsatolási cím:** A visszacsatolási cím (0:0:0:0:0:0:0:1 vagy ::1) visszacsatolási kapcsolatot azonosít, lehetővé téve, hogy egy csomópont önmagának küldjön csomagokat. Megfelel az IPv4 127.0.0.1 visszacsatolási címének. A visszacsatolási címre címzett csomagokat soha nem szabad kapcsolatra küldeni vagy egy útválasztó által továbbítani.

5.3.7 Az IPv6 előnyei az IPv4-hez képest

Az IPv6 azon felül, hogy jóval nagyobb címtartománnyal rendelkezik, számos más előnnyel rendelkezik az IPv4-hez képest:

- Az IPv6 a protokollba beépítetten támogatja a multicast továbbítást, míg IPv4 esetében ez a tulajdonság opcionális.
- Az IPv6 eszközök a hálózat összes alhálózatára kapcsolt kliensnek beállítanak egy csak lokálisan elérhető és érvényes IPv6 címet, amely lehetővé teszi, hogy címkiszolgáló és útválasztó (router) jelenlététől függetlenül is kommunikálni lehessen az azonos alhálózaton lévő végpontokkal.
- Biztonsági megoldások tekintetében, az IPsec támogatás (hitelesítés és titkosítás) kötelezően része az IPv6 protokollnak, míg IPv4 esetében ez a tulajdonság opcionális.
- Mobil IPv4 protokollal ellentétben a Mobil IPv6 (MIPv6) segít elkerülni a korábban tapasztalt nem optimális útválasztást (triangular routing), illetve elérhetővé teszi a mobil (Wi-Fi – vezeték nélküli) klienseknek az új útválasztó választást a há-

lózati címek átszámozása nélkül, ami stabilabb és gyorsabb kapcsolatot eredményez, kevesebb megszakadással.

- IPv4 esetében az adatcsomagok méretének felső korlátja 64 kB (kilobyte), míg az IPv6 esetében ez 4GB (gigabyte) méretig növelhető, amely jelentősen megnövelheti az adatátviteli sebességet.

5.3.8 Kompatibilitás

Az IPv6 teljesen más csomagformátumot használ, mint az előző verzió, így gyakorlatilag egész más protokoll, TEHÁT nem kompatibilis az IPv4-el. A teljes Internet átállítása lehetetlen egyik pillanatról a másikra IPv4-ről IPv6-ra. Épp ezért nagyon fontos, hogy a két rendszer egyszerre működhessen ne csak az Interneten, hanem akár egyetlen gépen belül is. Ezt a kompatibilis címek (az IPv4 címek egyszerűen átalakíthatók IPv6-címekké), és különféle alagutak alkalmazása biztosítja. Ezen kívül a rendszer használhatnak egy *dual stack IP* (kettős protokollcsomag) nevű technikát is, amely egy időben támogatja mindkét protokollt, vagyis két teljesen különálló hálózati alrendszert használnak és a két protokollverzió semmilyen hatással nincs egymásra.

Felmerül a kérdés, hogy az IP-re épülő protokollok mit szólnak hozzá, hogy valaki lecseréli alattuk az IP-t. Elvileg a mind az UDP, mind a TCP úgy van megtervezve, hogy független legyen az alatta lévő protokolltól. Tehát nem kell (teljesen) újraírni őket. Az ezeket használó programokat viszont módosítani kell, hiszen a régi formátumú, méretű IP címekre, a régi szolgáltatásokra stb. számítanak.

> Az IPv6 nem kompatibilis az IPv4-el, de a protokollok legnagyobb részével igen (TCP, UDP, ICMP, IGMP, OSFP, BGP és DNS). A hálózat vezérlésével és a névfeloldással kapcsolatos protokollok tehát kompatibilisek.

5.3.9 Az internet szállítási protokolljai

TCP (Transmission Control Protocol). Az Internet bővülésével már számos LAN, rádiós csomagszóró alhálózat; valamint több műholdas csatorna is működött, a végpontok közötti átviteli megbízhatóság csökkent. Ezért egy új szállítási protokoll, a TCP (Transmission Control Protocol – átvitel vezérlési protokoll) került bevezetésre 1974-ben. Tervezésénél már figyelembe vették azt, hogy megbízhatatlan alhálózatokkal is tudjon együttműködni. A TCP-vel együtt fejlesztették a hálózati réteg protokollját (IP) is.

A TCP **összeköttetés orientált protokoll**. Alapvetően a 3-utas kézfogás módszerét használja. A TCP az IP hálózati protokoll (IPv4 vagy IPv6) felett fut, használja a szolgáltatásait. A TCP fogadja a tetszőleges hosszúságú üzeneteket a felhasználói folyamattól és azokat maximum 64 kbyte-os darabokra vágja szét. Ezeket a darabokat egymástól független datagramokként küldi el. A hálózati-réteg nem garantálja sem a datagramokat helyesen kézbesítését, sem a megérkezett datagramok helyes sorrendjét. A TCP feladata az, hogy időzítéseket kezelve szükség szerint újraadja őket, illetve hogy helyes sorrendben rakja azokat össze az eredeti üzenetté. Minden TCP által elküldött byte-nak saját sorszáma van. A sorszámtartomány 32 bit széles, ami elegendően nagy ahhoz, hogy egy adott byte sorszáma egyedi legyen, vagyis a kettőződést elkerüljük a többszörös beérkezések esetén.

Az **UDP** az Internet **összeköttetés nélküli** szállítási protokollja. IP datagramok küldését teszi lehetővé összeköttetés létesítése nélkül. Jóval egyszerűbb, mint a TCP.

Használata ott célszerű, ahol egy kérésre egyetlen válasz érkezik, és a nyugtázásnak nincs jelentősége.

A TCP/IP és az UDP hálózatokban egy logikai csatlakozáshoz egy port (végpont) tartozik. A portok számai a 0 és 65536 között vannak. Néhány port számot a IANA eleve kijelölt meghatározott célokra, ezeket „jól ismert” (kijelölt) portoknak nevezik.

- **0-1023:** Ide tartoznak a gyakrabban használt portok *(Well Known Ports)*.
- **1024–49151:** Az úgynevezett regisztrált portok tartoznak ebbe a tartományba.
- **49152–65535:** Dinamikus, illetve privát portszámok. Az egyes alkalmazások által véletlenszerűen választott portszámok listája. Ezek a portok nem tartoznak állandóan egy adott alkalmazáshoz.

Tehát ha egy számítógép felajánl egy szolgáltatást, amely például weboldalakat közöl, az alkalmazás megnyitja a hozzátartozó portot. Az ilyen számítógépeket hívjuk az adott szolgáltatás szerverének. Az a számítógép, mely kapcsolatot akar teremteni a szolgáltatóval (kliens) megnyitja egyik portját és csomagokat küld a szerver IP címére, a szolgáltató portjának. Például, alapbeállításként a 80-as TCP port a http szolgáltatáshoz van hozzárendelve.

5.3.10 Az internet vezérlő protokolljai

- Az **ICMP** (Internet Control Message Protocol) Internet vezérlőüzenet protokoll az Internet felügyeletét szolgálja. Összesen mintegy tucatnyi üzenetet definiáltak. Az üzeneteket főként routerek hozzák létre. A visszhang és időbélyeg kérést indíthatja egy hoszt is.
- Az **ARP** (Address Resolution Protocol, azaz címfeloldási protokoll). Egy ügyfél hardvercímének meghatározására szolgál, ha annak csak az IP-címe ismert. Minden Internetre csatlakozó gépnek van legalább egy IP címe. Az IP cím logikai cím, amit az interface hardvere nem ért meg. Az IP címeket le kell fordítanunk az adatkapcsolati réteg számára érthető fizikai címekre.
- **RARP** (Reverse Addres Resolution Protocol). A korábban tárgyalt ARP fordítottja. Fizikai címhez kereshetünk IP címet.

5.4 ÖSSZEFOGLALÁS

Az internet gyökerei az 1960-as évekig nyúlnak vissza. A fejlesztés az USA Hadügyminisztériumában kezdődött. Olyan hálózat hálózatot próbáltak meg létrehozni, mely működőképes marad egy esetleges atomtámadás esetén is. 1969-ben telefonvonalon egy kísérleti jellegű, csomagkapcsolt hálózatot hoztak létre (ARPAnet: Advanced Research Projects Agency Network) néven, mely egyelőre 4 gépet kötött össze.

1971-től több oktatási és kutatási intézmény is kapcsolódott, a csomópontok száma 15-re nőtt. A katonai felhasználásokon kívül a csomagkapcsolt adattovábbítás további kutatásra szolgált, de egyes egyetemek, katonai bázisok és kormányzati laboratóriumok kutatói is

használták elektronikus levelezésre, fájlok cseréjére és távoli bejelentkezésre egymás számítógépei között.

1972-ben megszületett az első e-mail program. 1974-ben jelent meg először az „internet" kifejezés, egy a TCP protokollról szóló tanulmányban. Az ARPANET-hez csatlakozó egyre több gép szükségessé tette egy érvényes kommunikációs szabvány bevezetését. Ebben az évben dolgozzák ki és vezetik be a TCP/IP-t.

1983-ban azután, hogy az addig szigorúan ellenőrzött ARPANET-ből MILNET (Military Network) néven leválasztották a hadászati szegmenst, megszületett a mai fogalmaink szerinti internet.

Az internet úgynevezett Internet Protocol alapú hálózat. A hálózaton áthaladó adatcsomagok útját forgalomirányítók adják meg forgalomirányítási táblázataik (routing table) segítségével. Az IP-cím (Internet Protocol-cím) egy egyedi hálózati azonosító, amelyet az Internet Protocol segítségével kommunikáló számítógépek egymás azonosítására használnak.

A jelenleg használt IPv4-es IP-címek 32 bites egész számok, amelyeket hagyományosan négy darab egy bájtos, azaz 0 és 255 közé eső, ponttal elválasztott decimális számmal írunk le a könnyebb olvashatóság kedvéért (pl.: 192.168.50.1). Az IP címek öt, az abc betűivel jelzett kategóriába, úgynevezett címosztályba sorolhatók. Különleges címei a loopback cím, ami a saját gépünkkel kommunikál, és a broadcast cím mellyel az összes helyi gépet megcímezhetjük.

Az IPv6 szabvány jelentősen kiterjesztette a címteret. Az IPv6-os címek 128 bitesek, és már nem lenne praktikus decimálisan jelölni őket, ezért kompaktabb, hexadecimális számokkal írjuk le, 16 bites csoportosításban. (Pl. 5001:650:240:11:0:0:C100:1320).

A különböző méretű hálózatokon alapuló tartományok megszűntek. Az IPv6-os címek, hasonlóan az 4-es IP címekhez alapvetően két részre vannak osztva. A cím áll egy hálózati részből, és egy interfész-azonosító részből. A hálózaton történő továbbítás alapján három féle csoportba sorolhatjuk a címeket. Az egyedi (unicast) cím egy interfészhez rendelt cím. A Bárki (anycast) cím: interfészek egy csoportjához rendelt cím. A csoport (multicast) cím: interfészek egy csoportjához rendelt cím., hasonlóan az anycast címekhez, azonban itt a csoport minden tagja megkapja a küldött csomagokat.

Az Ipv6-nál is használnak különleges címeket. Ilyen a meghatározatlan cím, amely általában forráscímként használatos az ideiglenes címek egyediségének ellenőrzését megkísérlő csomagokhoz, és a visszacsatolási cím, ami megegyezik az IPv4-es címek loopback címével.

Az IPv6 számos előnnyel rendelkezik az előző generációhoz képest: beépített multicast támogatás, szerves része az IPSec alapú titkosítás, nagyobb maximális csomagméret, lehetővé teszi, hogy egy hálózati csatolóhoz egy időben több címet rendeljünk. Az IPv6-os hálózatokban valóban működik az automatikus konfiguráció, vagyis egy újonnan telepített rendszer bármiféle kézi beállítás nélkül is beilleszkedik a (helyi) hálózatba.

Az IPv4 és az IPv6 nem kompatibilis egymással. Az áttérést többféle megoldás segíti: használhatók alagutak, kompatibilitási címek. Ezek kívül a rendszer használhat egy *dual stack IP* (kettős protokollcsomag) nevű technikát is.

Az internet szállítási protokolljai az összeköttetés alapú TCP és az összeköttetés mentes UDP. Vezérlő protokolljai: ICMP, ARP, RARP.

5.5 ÖNELLENŐRZŐ KÉRDÉSEK

1. Az Internet zárt architektúrájú, technikai szempontból számítógépek és számítógép-hálózatok központ nélküli, összekapcsolt hálózata.
2. Az Internet elődjének az ARPANET-et tekintjük.
3. A TCP/IP nem más, mint egy protokollkészlet, amelyet arra dolgoztak ki, hogy hálózatba kapcsolt számítógépek megoszthassák egymás között az erőforrásaikat.
4. A hálózatban egyedi, egymástól független adatcsomagok haladnak, melyeknek a célhoz vezető útvonalát a csomagban lévő cím alapján keressük. Ez az útvonal biztosan létezik.
5. Az IP Routing olyan folyamat, amely segítségével egy több hálózati interfésszel rendelkező host eldönti, hogy a kapott IP csomagokat merre továbbítsa.
6. Az IPv4-es cím egy 32 bites, azaz 4 bájtos azonosító, amelyben a bájtok értéke 0-257 közé esik.
7. Az IP címek beállítása csak statikusan történhet.
8. A loopback egy olyan áleszköz, ami a saját számítógépünket jelenti.
9. Az IPv4 32 bites címzése helyett az IPv6 64 bitet használ címzésre
10. Az IPv6 kompatibilis az IPv4-el

6. IRODAI HÁLÓZAT, OTTHONI HÁLÓZAT

6.1 CÉLKITŰZÉS

Jelentősen javulhat egy vállalkozás hatékonysága, vagy akár otthon is kényelmesebb lehet az Internet használata, ha meglévő hálózati kapcsolatunkat több gépen is elérhetővé tesszük. Ehhez már nem kell bonyolult és nehezen konfigurálható eszközöket beszereznünk.

A lecke megismerteti az internetre kapcsolódáshoz szükséges eszközökkel, és bemutatja a már meglévő internetkapcsolatunk megosztásának lehetőségét akár vezeték nélküli környezetben is.

A lecke végén foglalkozunk egy kiemelt jelentőségű témakörrel, a biztonsággal is.

6.2 TARTALOM

- Az internet kapcsolat megosztása és annak eszközei
- A DSL kapcsolat
- Kábelmodemes kapcsolat
- A SOHO switchek
- Routerek
- Vezeték nélküli eszközök
- A vezeték nélküli hálózatok biztonsága

6.3 AZ INTERNET KAPCSOLAT MEGOSZTÁSA ÉS ANNAK ESZKÖZEI

Az internetkapcsolat megosztásának működéséhez két kapcsolat szükséges: egy nyilvános és egy magánhálózati. A magánhálózati kapcsolatot általában egy hálózati kártya biztosítja, ez kapcsolja az internetkapcsolat megosztását biztosító számítógépet az otthoni vagy kisméretű irodai hálózat számítógépeihez. A nyilvános kapcsolat, amely általában DSL, kábel- vagy telefonmodem révén jön létre, csatlakoztatja saját hálózatunkat az internethez. Az 1990-es években a modemek 9600 bit/s sebességen működtek. 1998-ra elérték a jelenlegi szabványt, azaz az 56 000 bit/s, másképpen 56 kbit/s sebességet. A vállalati környezetben használt nagysebességű szolgáltatások, például a digitális előfizetői vonalas (DSL) és a kábelmodemes hozzáférés megjelentek az egyéni felhasználók piacán. Az ilyen szolgáltatások immár nem igényelnek drága berendezéseket, sem újabb telefonvonalat. Ezek folyamatosan működő szolgáltatások, amelyek azonnali hozzáférést biztosítanak, nem kell minden összeköttetés alkalmával új kapcsolatot létesíteni. Így fokozódott a megbízhatóság és a rugalmasság, és a kisebb munkahelyi és otthoni hálózatokon is egyszerűbbé vált az internetkapcsolat másokkal való megosztása. A továbbiakban áttekintjük az ehhez szükséges eszközöket.

6.3.1 A DSL-kapcsolatok

A DSL modemek, vagy forgalomirányítók egy ADSL (asymmetric digital subscriber line, aszimmetrikus digitális előfizetői vonal) interfésszel rendelkeznek. Ha egy forgalom-

irányító ADSL portjához ADSL vonalat szeretnénk csatlakoztatni, a következőket kell tennünk:

- Csatlakoztassuk a telefonkábelt a forgalomirányító ADSL portjához.
- A kábel másik végét csatlakoztassuk a telefonos aljzathoz.

A forgalomirányító és a DSL szolgáltatás kapcsolatának létrehozásához RJ-11-es csatlakozókkal ellátott kábelt kell használni. A DSL-kapcsolatok normál telefonvonalakon működnek, és a szabványos RJ-11-es csatlakozók 3-as és 4-es érintkezőit használják.

Az ADSL kapcsolaton a teljes sávszélességet nem egyenlő arányban osztják fel a letöltési és feltöltési irányok között, hanem – a tipikus kliens-oldali forgalom jellemzőit figyelembe véve – előbbit részesítik előnyben utóbbival szembe. Így az ADSL vonalakon az elméleti maximális letöltési sebesség sokszor többszöröse a maximális feltöltési sebességnek.

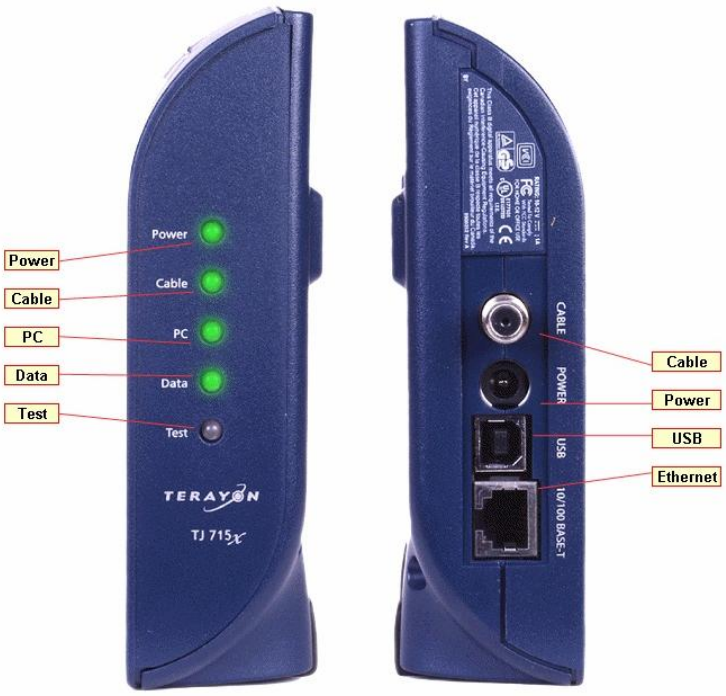
ADSL modem

6.3.2 Kábelmodemes kapcsolatok

A kábeles forgalomirányítók és modemek segítségével kisméretű irodai és otthoni (SOHO) használatra lehet nagysebességű hálózati kapcsolatokat létesíteni. Ezek az eszközök koaxiális kábelcsatlakozóval, más néven F-csatlakozóval rendelkeznek, ez az interfész közvetlenül kapcsolódik a kábelrendszerhez.

Csatlakoztatásuk a kábelrendszerhez a következő módon történik.

- Ellenőrizzük, hogy az eszköz nem kap-e tápellátást.
- Keressük meg a koaxiális kábeles (TV-s) fali aljzatból induló RF koaxiális kábelt.
- Telepítsünk jelosztót/iránycsatolót, amely a tévés és a számítógépes jeleket elkülöníti egymástól. Ha szükséges, felüláteresztő szűrő segítségével előzzük meg a tévés és a számítógépes jelek közötti interferenciákat.
- Csatlakoztassuk a koaxiális kábelt a forgalomirányító F-csatlakozójához. Szorítsuk meg (kézzel) a csatlakozót, majd fogóval további egyhatod fordulatnyit húzzunk rajta.
- Ellenőrizzük, hogy az elosztó és az eszköz között minden további koaxiális kábelcsatlakozás, köztes jelosztó, iránycsatoló és földelés csatlakozása megfelelően meg van-e húzva.



Kábelmodem

6.3.3 A SOHO switchek

Az előző két eszköz valamelyikével megoldódott az internetkapcsolat létrehozásának kérdése. Azonban a kapcsolat megosztásához, illetve a helyi hálózat kialakításához újabb eszközre van szükségünk. Ha csak vezetékes hálózatban gondolkodunk, akkor a korábbiakban ismertetett switchek egyszerűbb 4-8 portos választhatjuk. Ebben az esetben a megosztást a kábel/dsl/telefon modemmel összekötött számítógép végzi szoftveres úton, úgy, hogy több hálózati kártyával rendelkezik. Az ilyen esetben routerként viselkedő számítógép a helyi hálózatot (LAN) köti össze az Internettel (WAN). Így kívülről, az Internet felől hálózatunk egy publikus IP címmel rendelkezik (ez „azonosít" bennünket az Interneten), azonban a belső hálózatunk gépei valójában különböző, belső, nem publikus IP címekkel rendelkeznek.

6.3.4 A routerek

Az otthoni és irodai hálózat és az internet összekapcsolásának másik lehetősége az útválasztó vagy router használata. Ezek a kisteljesítményű routerek alkalmasak a hálózatok közötti adatforgalom irányítására. WAN portjuk mellett általában rendelkeznek 4-8 hálózati porttal, lehetőséget biztosítva ezzel a gyors és egyszerű hálózatépítésre. Többségük webes interfészen keresztül menedzselhető. Nem egy esetben a beállításokat „varázslók" is segítik.

Többféle funkciót kínálnak, melyek közül az internetmegosztásnál jól jöhet a Mac cím klónozása. Az internetszolgáltatók gyakran a Mac címhez kötik a szolgáltatást. Ha a router Mac címét a regisztráláskor internetre kötött gép címére módosítjuk, akkor elkerülhető az újra regisztrálás, és megoldódik a megosztás is.

6.3.5 Vezeték nélküli eszközök

Az összetett hálózati infrastruktúra kiépítéséhez szükséges erőforrások hiányában sok helyen döntenek a vezeték nélküli hálózati összeköttetés mellett, mert hatékonyan alkalmazható, olcsó, kiépítése és fenntartása pedig egyszerű. A vezeték nélküli hálózaton belül a hálózathoz csatlakoztatott számítógépek vezeték nélküli egységei és a vezeték nélküli alapegység rádióhullámok útján létesít egymással kapcsolatot.

Belső vezeték nélküli hálózati kártya

Az így kapcsolatot létesítő egységek az IEEE nevű szervezet 802.11 jelzésű rádióátviteli szabványainak egyike alapján működnek. Ezen szabványok legszélesebb körben használatos típusait gyakran Wi-Fi-nek hívják. Hálózatunkat kiterjeszthetjük Access Point telepítésével, illetve alkalmazhatunk wireless routert is, mely az előzőekben ismertetett funkciókon kívül egy AP szerepét is ellátja.

Wireless Router

SOHO környezetben a hozzáférési pontok általában körsugárzó ikerantennákat használnak, amelyek minden irányba kisugározzák ugyan a jeleket, de csak kisebb távolságra.

6.3.6 A vezeték nélküli hálózatok biztonsága

Egy rosszul beállított Wi-Fi hálózat könnyen támadható és sérülékeny lesz az illetéktelen felhasználókkal szemben. A következőkben néhány biztonságot növelő technika bemutatására kerül sor.

1. Az Access Pointok és Routerek gyári SSID elnevezéssel és jelszóval kerülnek a boltokba. Fontos ezek megváltoztatása.
2. A MAC (Media-access Control, Eszköz Hozzáférés Ellenőrzés) szűrés annyit jelent, hogy csak azt engedjük a hálózathoz kapcsolódni, akinek az azonosítója szerepel a listánkban. A Routerek beállításaiban általában így szerepel: MAC Address Filtering.
3. A WEP (Wired Equivalent Privacy, Vezetékessel Egyenértékű Titkosítás) a kezdeti WiFi szabványok biztonsági technológiája. A WEP-et eredetileg WLAN kapcsolatunk titkosítására találták ki. Az RSA által kifejlesztett RC4 titkosítást használja, szimmetrikus 64 illetve 128 bites, változó hosszúságú kulcsot használva. Ezt a kulcsot, mint sima szöveget küldik oda vissza a hálózaton a kommunikációban résztvevő eszközök, ráadásul mindegyik eszköz ugyanazt az egyetlen kulcsot használja, ezért megszerzése sajnos elég egyszerű.
4. A WPA (Wireless Protected Access, Vezeték nélküli Védett Hozzáférés) a 802.11i biztonsági szabvány része, amely 802.11x hitelesítést és TKIP (Temporal Key Integrity Protocol, Ideiglenes Kulcs Integritás Protokol) kulcskiosztást használ. A WEP leváltása céljából fejlesztették ki.
   Az IEEE 802.11i a WLAN hálózatok biztonsági szabványa, amelynek fő komponensei a 802.11x hitelesítés, a TKIP protokol és az AES (Advanced Encryption Standard, Továbbfejlesztett Titkosítási Szabvány) titkosító algoritmus.
   A WPA két működési módban alkalmazható. Az egyik a Pre-Shared Key mode (Megosztott kulcs mód), amely otthonra és kisvállalkozások számára ideális megoldás. A titkos kulcsot az Access Point adminisztrációs felületén kell megadnunk, ahogy az egyes klienseknél is. Ez első pillantásra megegyezik a WEP módszerével, a WPA azonban a kapcsolódást követően folyamatosan változtatja a titkos kulcsot, így szinte lehetetlen az éppen érvényben lévőt megfejteni. A WPA másik működési módja (Enterprise mode) nagyvállalatok számára nyújt biztonságos megoldást.
5. WPA2 A WPA tulajdonképpen még a 802.11i biztonsági szabvány végelegesítése előtt jött létre, utódja WPA2 néven már a ratifikált 802.11i szabvány szerves részeként vált ismerté, amely kötelezően tartalmazza az erősebb AES (más néven CCMP) titkosítási módszert is, lecserélve a WPA első verziója által alkalmazott (gyengébb) RC4 titkosítási algoritmust (amit a WEP is használ).

Tehát kisméretű WLAN hálózat esetében válasszuk a WPA Pre-Shared Key módot az Access Pointunk adminisztrációs felületén. Ezután válasszuk a TKIP vagy AES algoritmust a titkosításhoz, de előtte győződjünk meg arról, hogy eszközeink melyik algoritmust támogatják!

A kliens konfigurálás esetén a lényeg, hogy azonos beállításokat válasszunk, mint az Access Pointon. Meg kell adnunk az SSID-t, a WPA-PSK (WPA Pre-Shared Key) biztonsági módszert és a választott (TKIP vagy AES) titkosítást, végül a titkos kulcsot (Network Key). Ezek után már biztonságosan kapcsolódhatunk vezeték nélküli hálózatunkhoz.

6.3.7 Tűzfalak

A biztonság a legtöbb hálózatban kiemelt jelentőségű. A tűzfal (angolul firewall) célja a számítástechnikában annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Szoftver- és hardverkomponensekből áll.

Ha az internethez történő csatlakozáskor a számítógép védtelen, illetéktelen behatolók férhetnek hozzá a gépen tárolt személyes adatokhoz. Olyan kódot telepíthetnek a számítógépére, amely hibát okozhat és fájlokat törölhet. A számítógépét használva más, az internetre csatlakoztatott otthoni és vállalati számítógépeken is kárt okozhatnak. A tűzfal segítségével számos kártékony internetes tartalmat szűrhet ki, mielőtt elérnék a számítógépet.

Egyes tűzfalakkal megakadályozhatja azt is, hogy illetéktelenek a tudta nélkül, számítógépén keresztül támadjanak meg más számítógépeket. A tűzfal használata az internetcsatlakozás módjától (telefonos modem, kábelmodem, DSL- vagy ADSL-vonal) függetlenül fontos.

A tűzfal megpróbálja megóvni a privát hálózatot illetve a hálózati szegmenst a 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.

DFL-860 NetDefend Középvállalati UTM tűzfal 860

DMZ (*demilitarized zone*) A személyes vagy vállalati hálózatok megbízhatatlan külső, és a megbízható belső része között elhelyezkedő terület. A benne elhelyezkedő hálózati eszközökhöz és erőforrásokhoz a megbízható belső, és a megbízhatatlan külső területről engedélyezi a hozzáférést, de megakadályozza, hogy a külső területről bármilyen kérés vagy hozzáférési kísérlet eljusson a belső hálózatra.

Otthoni és kisirodai (SOHO) routerek is rendelkeznek DMZ funkcióval. Ilyenkor a kis hálózat szigorúan egyetlen számítógépét a tűzfalszabályok és a NAT[6]-olás elé helyezik, mintha a számítógép közvetlenül kapcsolódna az internetre. Ilyenkor sok akadály megszűnhet, mert közvetlen kapcsolatokat fogadhatunk az internet felől, de megszűnik a router mindenfajta védelmi mechanizmusa is, ezért körültekintéssel kezelendő.

A tűzfalat működésük alapján lehetnek:

- **Csomagszűrő**: 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.
- **Állapot szerinti szűrésű**: 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.
- **Alkalmazás szintű**: Egy alkalmazás-szintű tűzfal a tisztán csak a forgalomhoz tartozó, mint a forrás, cél és szolgáltatás adatokon kívül a hálózati csomagok tartalmát is figyeli.

6.3.8 VPN[7] és más kiegészítő szolgáltatások a routerekben

A kisméretű vállalatok, illetve irodai felhasználók számára is egyre fontosabbá válik a biztonságos távoli munkavégzés lehetőségének megteremtése. Jól tudják ezt a hálózati eszközök fejlesztői is, így nem csoda, ha egyre több olyan eszköz kerül forgalomba, amelyek funkcionalitása, teljesítménye és jó esetben az árazása is igazodik a kisméretű cégek igényeihez. Az ilyen eszközök jellemzője, hogy a VPN kapcsolatok létrehozását IPsec

6 Hálózati címfordítás (Network Address Translation)Lehetővé teszi belső hálózatra kötött saját nyilvános IP cím nélküli gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel. Vagyis, hogy több számítógépet egy routeren keresztül kössünk az internetre. Az elsődleges cél ez esetben az, hogy egy nyilvános IP-címen keresztül több privát IP-című (privát címtartomány: RFC 1918) számítógép csatlakozhasson az internethez.

7 A virtuális magánhálózat (VPN) olyan magánhálózat, amely nyilvános infrastruktúrán belül (például a világméretű interneten) jön létre. A VPN például arra alkalmas, hogy a távdolgozó távolról hozzáférjen a vállalatközpont hálózatához.

(Internet Protocol Security) támogatás mellett képes megvalósítani. Egy időben több párhuzamosan működő VPN csatorna kiépítését támogatja.

Az új termékekbe SPI-képes (Stateful Packet Inspection) tűzfal került, és egy DMZ port használatára és konfigurálására is van mód. Az eszköz támogatja a legfontosabb routeolási és NAT-olási funkciókat, miközben DoS elleni védelem gondoskodik az esetleges szolgáltatásmegtagadási támadások lehetőségek szerinti elhárításáról. Az új készülékek áteresztőképessége 25 megabit/másodperc.

És mit tud egy router manapság? Tulajdonképpen hálózati mindenes: 802.11n kompatibilis útválasztó, ami kicsi (legalábbis jóval kisebb, mint a mostani routerek túlnyomó többsége) beépített antennás, a házban elfér egy 2,5 hüvelykes merevlemez (hagyományos vagy SSD), az előlapon pedig egy színes 3,2” színes kijelző, hogy digitális képkeretként is funkcionáljon. Gigabites WAN és LAN portok, USB portok a nyomtatók és USB-tárolóeszközök részére, melyekkel extra tárhelyet és megosztott nyomtatót lehet szolgáltatni a hálózatra csatlakozott gépeknek. NAS szolgáltatások a beépített merevlemezhez kapcsolódóan, FTP szolgáltatás, Torrent kliens, nyomtatószerver, Samba kiszolgáló, kvótázás és webszerver, uPNP szerver és iTunes szerver képességek kapnak helyet benne, mindez párosítva a megfelelő jogosultságok kezelésével, azaz felhasználói csoportokat és/vagy felhasználókat hozhatunk létre, írás és olvasás jogokat oszthatunk ki.

Napjaink Routere

6.4 ÖSSZEFOGLALÁS

Számítógépünket analóg modem, kábel-, vagy dsl modem segítségével is kapcsolhatjuk az internethez. A csatlakoztatás után természetes igényként jelentkezik, hogy mind otthoni, mind kisirodai környezetben az internetelérést a többi gép számára is elérhetővé tegyük.

Ennek legegyszerűbb eszköze a kapcsoló (switch). Ebben az esetben a megosztást a számítógép végzi szoftveres úton.

Másik lehetőségünk az útválasztó (router) használata. A router feladata a megosztás. WAN portja mellett általában 4-8 hálózati porttal is rendelkezik.

Egyre nagyobb teret nyernek a vezeték nélküli eszközök. A vezeték nélküli hálózat kiépítése olcsó, fenntartása pedig egyszerű. Sok helyen szinte nem is adódik más lehetőség.

Ha mobil eszközöket is szeretnénk a hálózatba kötni, hozzáférési pontot (Access Point) telepítünk. Ez lehet önálló eszköz, vagy egy routerbe beépített eszköz is. Ezeket a routereket wireless routereknek nevezzük. A vezeték nélküli eszközök az IEEE nevű szervezet 802.11 jelzésű rádióátviteli szabványainak egyike alapján működnek.

Kezdetben a vezeték nélküli rendszerek biztonsági szintje nagyon alacsony volt. A WEP (Wired Equivalent Privacy, Vezetékessel Egyenértékű Titkosítás) a kezdeti WiFi szabványok biztonsági technológiája. Az RSA által kifejlesztett RC4 titkosítást használja, szimmetrikus 64 illetve 128 bites, változó hosszúságú kulcsot használva.

Könnyű feltörhetősége miatt bevezették a WPA-t (Wireless Protected Access, Vezeték nélküli Védett Hozzáférés). A 802.11i biztonsági szabvány része, amely 802.11x hitelesítést és TKIP (Temporal Key Integrity Protocol, Ideiglenes Kulcs Integritás Protokol) kulcskiosztást használ. Az IEEE 802.11i a WLAN hálózatok biztonsági szabványa, amelynek fő komponensei a 802.11x hitelesítés, a TKIP protokol és az AES (Advanced Encryption Standard, Továbbfejlesztett Titkosítási Szabvány) titkosító algoritmus.

A WPA utódja WPA2 néven már a ratifikált 802.11i szabvány szerves részeként vált ismertté, amely kötelezően tartalmazza az erősebb AES (más néven CCMP) titkosítási módszert is, lecserélve a WPA első verziója által alkalmazott (gyengébb) RC4 titkosítási algoritmust (amit a WEP is használ).

A biztonság fokozására különböző fajtájú tűzfalakat használhatunk. A legegyszerűbb és legelterjedtebb a csomagszűrő, mely az adatcsomagok egyszerű szűrését végzi a cél-port, valamint forrás- és célcím alapján. Ennek kibővített fajtája az állapot szerinti szűréssel dolgozó, ami a 7. OSI-rétegen egy rövid vizsgálatot hajt végre, hogy minden hálózaticsomagról egyfajta állapottáblát hozzon létre, így felismerve ez a csomagok közti összefüggéseket. Az alkalmazás-szintű tűzfal a tisztán csak a forgalomhoz tartozó, mint a forrás, cél és szolgáltatás adatokon kívül a hálózati csomagok tartalmát is figyeli.

A routerek legújabb generációja számos új szolgáltatást nyújt. VPN támogatás, Gigabites WAN és LAN portok. USB portok a nyomtatók és USB-tárolóeszközök részére, melyekkel extra tárhelyet és megosztott nyomtatót lehet szolgáltatni a hálózatra csatlakozott gépeknek. FTP szolgáltatás, Torrent kliens, nyomtatószerver, Samba kiszolgáló, kvótázás és webszerver, uPNP szerver és iTunes szerver képességek kapnak helyet benne, mindez párosítva a megfelelő jogosultságok kezelésével, azaz felhasználói csoportokat és/vagy felhasználókat hozhatunk létre, írás és olvasás jogokat oszthatunk ki.

6.5 ÖNELLENŐRZŐ KÉRDÉSEK

1. A DSL-kapcsolatok normál telefonvonalakon működnek.
2. A vezeték nélküli hálózaton belül a hálózathoz csatlakoztatott számítógépek vezeték nélküli egységei és a vezeték nélküli alapegység rádióhullámok útján létesít egymással kapcsolatot.
3. SOHO környezetben a hozzáférési pontok általában körsugárzó ikerantennákat használnak, amelyek csak egy irányba sugározzák a jeleket.
4. Egy rosszul beállított Wi-Fi hálózat könnyen támadható és sérülékeny lesz az illetéktelen felhasználókkal szemben.

5. A WEP-et a WPA leváltása céljából fejlesztették ki.
6. A WPA és a WPA2 ugyanazt a titkosítást használja.
7. A tűzfal (angolul firewall) célja a számítástechnikában annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.
8. A személyes vagy vállalati hálózatok megbízhatatlan külső, és a megbízható belső része között elhelyezkedő terület a DMZ.
9. Az alkalmazás szintű tűzfalaknál az adatcsomagok egyszerű szűrése a cél-port, valamint forrás- és célcím, egy a tűzfal-adminisztrátor által már definiált szabályrendszer alapján történik.
10. A fejlett tűzfalak csendben dobják el a csomagokat, azaz az érintett kapcsolat egyszerűen nem jön létre/megszakad, de nincs konkrét visszajelzés.

7. A DOMAIN NAME SYSTEM

7.1 CÉLKITŰZÉS

Az Internet és más hálózatok csupán kommunikációs közegként szolgálnak a hálózati adattovábbításban. Valójában, miközben az internetet használva végezzük napi munkánkat, nem közvetlenül a hálózatot, hanem a gépünkön futó, meghatározott kommunikációs célra (levelezésre, weblapok letöltésére, esetleg fájlok átvitelére stb.) alkalmas, hálózati szoftvereket, úgynevezett szolgáltatásokat használunk. Ebben a leckében megtanulhatja, milyen komponensek alkotják a szolgáltatásokat. Megtudhatja, mit értünk a szerver mit a kliens alatt, és mit jelent a protokoll fogalma. A lecke további részében megismerkedhet a Domain Name System rendszerrel, és a tartományneveket IP címekké feloldó Domain Name Service szolgáltatással. A lecke végére érteni fogja, hogyan lehet az IP cím az internetes csomagirányítás alapja, akkor is, ha a felhasználó sosem használja ezeket a numerikus azonosítókat hostok azonosítására.

7.2 A LECKE TÉMAKÖREI

- A szolgáltatások és azok összetevői
- Az IP címek és gépnevek használata, névfeloldás
- Tartományok az interneten, a Domain Name System
- A névszerverek hierarchikus hálózata
- Névfeloldás a Domain Name Service segítségével

7.3 SZOLGÁLTATÁSOK AZ INTERNETEN

A számítógép-hálózatok, így az internet is hostokból, kommunikációs csatornákból, és kapcsolóelemekből felépülő kommunikációs rendszerek, amelyeken az adatok automatikus továbbítását a hostokon, és kapcsolóelemeken működő programok biztosítják.

A hálózatok gépei között bármilyen digitálisan ábrázolt adat továbbítható, így egy hálózat nagyon sokféle célra használható fel.

Hasonlóan a mobiltelefon-hálózathoz, amely lehetővé teszi a beszélgetést, az SMS- és MMS-küldést, WAP-olást, illetve az adatkommunikációt, az interneten is számos különböző szolgáltatás működik.

Egy szolgáltatás a hálózat valamilyen meghatározott célú kommunikációs eszköze, amelynek működését a hálózat gépein futó programok biztosítják.

A szolgáltatás működése közben programok kommunikálnak egymással, mégpedig minden esetben pontosan meghatározott kommunikációs szabályok szerint. Amikor informatikusként egy szolgáltatásról beszélünk, egyszerre kell gondolnunk a szolgáltatás nyújtotta lehetőségekre, a szolgáltatás működését biztosító programokra, és az azok közötti kommunikációt meghatározó szabályokra.

A legtöbb szolgáltatás kliens szerver alapú, ami azt jelenti, hogy a kommunikációban kétféle szoftverkomponens szerver és kliens vesz részt.

7.3.1 A szerver

A szerverek vagy kiszolgálók legtöbbször nem a felhasználó saját számítógépén, hanem egy úgynevezett **távoli gépen** futnak. Ezek a programok általában folyamatosan üzemelő számítógépeken működnek, és biztosítják a szolgáltatás folyamatos működését. A szerver program folyamatosan „figyeli”, hogy érkezik-e a hálózaton neki szóló üzenet. Ha igen, akkor feldolgozza azt, majd pedig válaszol az üzenet küldőjének.

7.3.2 A kliens

A kliensek a felhasználó saját gépén futtatott alkalmazások, amelyek képesek a szolgáltatást biztosító szerverhez kapcsolódni, annak üzenetet küldeni. A felhasználó a kliens segítségével használja a szolgáltatást, ezért a kliensek szerepe kettős. Biztosítják felhasználó munkájához szükséges felületet, és kapcsolatot tartanak a szolgáltatást nyújtó szerverekkel.

7.3.3 A protokoll

A kliens és szerver közötti kommunikáció során a két szoftverkomponens folyamatosan üzeneteket küld egymásnak. Az üzenetek lehetséges összetételét értelmezését a szolgáltatásra jellemző kommunikációs szabályrendszerek az úgynevezett protokollok írják le.

Amikor például a népszerű Word Wide Web szolgáltatást használjuk, távoli gépeken tárolódó weblapokat töltünk le a saját gépünkre. Ehhez gépünkön egy **kliens programot**, egy úgynevezett **böngészőt** kell futtatni. A böngésző felületén be kell gépelnünk a weblap címét, amely alapján a kliens felveszi a kapcsolatot egy távoli gépen futó webszerverrel, és üzenetet, úgynevezett kérést küld a **szervernek**. Az üzenet szerkezetét a webszerverek és böngészők kommunikációját szabályozó, **http** nevű protokoll határozza meg. A szerver kiértékeli a klienstől kapott kérést, megkeresi a host könyvtárszerkezetében a kért weblapot, és válaszként elküldi azt a kliensnek. A kliens gondoskodik a weblap képernyőn történő megjelenítéséről, és további kezeléséről.

16. ábra Felhasználó-kliens–üzenet/protokoll–szerver

Egy **szolgáltatás megvalósítását végző szoftverkomponensek** a TCP/IP modell legfelső, **alkalmazási rétegében működnek**, ennek a rétegnek az entitásai.

7.4 AZ IP CÍMEK ÉS GÉPNEVEK HASZNÁLATA, NÉVFELOLDÁS

Az IP címek bevezetése után hamar kiderült, hogy bár a címzés kiválóan alkalmas gépek egyértelmű azonosítására és a csomagok irányításra, a felhasználók nehezen boldogulnak ezekkel a numerikus azonosítókkal. Az emberi agy sajátossága, hogy nehezebben memorizál számokat, mint jelentéssel bíró szavakat, szövegeket, alfabetikus azonosítókat.

Ezért a felhasználók munkáját segítendő az IP cím mellett minden gép egy egyedi, szöveges azonosítót, **gépnevet** is kapott. A gépeknek küldött **adatcsomagok változatlanul IP címeket tartalmaztak** fejléceikben, ugyanakkor **a felhasználó gépnevet használhatott** a címzésre.

Ha **192.168.1.3** IP című gép neve **iroda** volt, akkor a felhasználónak nem kellett tudnia az IP címet, címzéskor elegendő volt megadni az **iroda** szót.

Ez a megoldás azonban további problémát hordozott. Tegyük fel, hogy a felhasználó, gépnévvel (pl. **iroda**) címzi meg azt a hostot, amivel kapcsolatba akar lépni. Ilyenkor saját számítógépének valahogyan „meg kell tudnia”, hogy a használt gépnévhez, a **192.168.1.3** IP cím tartozik. Az üzenetből kialakított csomagok csak így címezhetők meg, és csak így továbbíthatók eredményesen a hálózaton. Az IP cím gépnév alapján történő meghatározása a **névfeloldás**.

Azt a műveletet, amelyben egy számítógép meghatározza egy host alfabetikus nevéhez tartozó IP címét, névfeloldásnak nevezzük.

A névfeloldás olyan adatbázis alapján történhet, amely tárolja az egyes a gépnevekhez tartozó IP címeket. Ezt kezdetben úgy oldották meg, hogy minden ARPANET-hez csatlakozó gépnek tárolnia kellett egy roppant egyszerű szerkezetű, **hosts** nevű szövegfájlt. A fájl minden egyes sora egy IP címet, és a hozzá tartozó gépnevet tárolta.

Felhasználási terület	Azonosító.
Kormányhivatalok gépei	GOV
Hálózati kapcsolatokat bonyolító gépek.	NET
Oktatásban használt gépek	EDU
Katonai felhasználású számítógépek	MIL
Non profi szervezetek gépei	ORG
Üzleti célú gépek	COM

17. ábra A hosts állomány szerkezete

Amikor a felhasználó gépnévvel címzett, a névfeloldást végző program automatikusan megkereste a **hosts** állomány megfelelő sorát, és kiolvasta belőle az IP címet.

A ’80-as évek közepe óta egy sokkal rugalmasabb rendszert használnak a névfeloldásra, de a **hosts** állományok változatlanul megtalálhatók minden internethez kapcsolódó gépen, sőt a névfeloldást végző szolgáltatás használja is ezeket a fájlokat.

Windows operációs rendszerek esetében például, a
<*Rendszerlemez*>**:\windows\system32\drivers\etc**
könyvtárban találjuk meg a **hosts.txt** fájlt. Tartalmának helyes megadásával leegyszerűsíthetjük, egy kisebb irodai, vagy otthoni hálózat gépeinek, esetleg rendszeresen használt távoli gépeknek saját gépünkről történő elérését.

Földrajzi terület	Azonosító
Magyarország	HU
Nagy-Britannia	EN
Németország	DE
...	

18. ábra Egy kitöltött hosts.txt.

7.5 A DOMAIN NAME SYSTEM

A gépnevekkel történő azonosítás egyik problémája, hogy strukturálatlan azonosítókat használva nagyobb hálózatokban lehetetlen biztosítani a nevek egyediségét. Ezen a problémán igyekszik segíteni a **Domain Name System** (tartománynév-rendszer).

A rendszer alapja, hogy a teljes hálózat gépeit saját fenntartóval rendelkező, kisebb **logikai csoportokba**, úgynevezett **domain**ekbe, területekbe sorolják. A tartományokon belül subdomainekbe, (résztartományok, al-tartomány) rendezik a tartomány gépeit. A rendszer megengedi, hogy minden tartományt további résztartományokra bontsanak[8]. Így a tartományok hierarchikus rendszerét kapjuk, amelynek tetején az úgynevezett **top-level domain**ek, legfelső szintű tartományok helyezkednek el. A top level domainekbe kezdetben felhasználási terültük, később pedig földrajzi elhelyezkedésük szerint csoportosították a subdomaineket.

A struktúrában minden domaint, (legyen az top-level domain, subdomain, vagy még kisebb terület) a befoglaló tartományon belül egyedi névvel, **domain azonosítóval** látnak el. A top-level domainek esetén a domain azonosítók az alábbi táblázatnak, vagy földrajzi terület esetén az ország név rövidítésének felelnek meg.

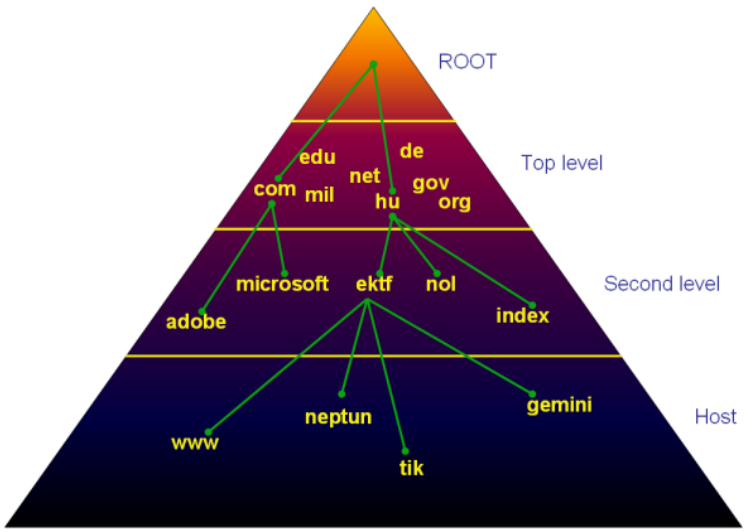
[8] A DNS a tartományok 127 szint mélységű egymásba ágyazását engedi meg. Ilyen szintű strukturálásra gyakorlatilag sosincs szükség.

Felhasználási terület	Azonosító
Kormányhivatalok gépei	GOV
Hálózati kapcsolatokat bonyolító gépek.	NET
Oktatásban használt gépek	EDU
Katonai felhasználású számítógépek	MIL
Nonprofi szervezetek gépei	ORG
Üzleti célú gépek	COM

Földrajzi terület	Azonosító
Magyarország	HU
Nagy-Britannia	EN
Németország	DE

A legfelső szintű domainek alatt lévő subdomainek, általában intézmények (egyetemek, főiskolák, cégek, szervezetek) gépeit tartalmazták, azonosítójukat pedig az intézmény határozta meg.

A **hu,** legfelső szintű domainben lévő Eszterházy Károly Főiskola tartománya, az **ektf** domain azonosítóval rendelkezik



19. ábra Domainek hierarchikus szerkezetét bemutató fa szerkezetű ábra

Mivel minden egyes terület pontosan megnevezhető, az egyes gépek azonosítására a nevükön kívül, a befogadó tartományok azonosítóit is felhasználhatjuk.

Ha egy géptől indulva, a legfelső szintű domain felé haladva, *gépnév.aldomain.domain* formában leírjuk a gép, majd minden egyes domain azonosítóját, eredményként megkapjuk a számítógép egyedi, alfabetikus azonosítóját.

A **magyar** domainben lévő **Eszterházy Károly Főiskola gemini** nevű számítógépének alfabetikus azonosítója például a **gemini.ektf.hu**

Az interneten, egy gép egyedi, alfebetikus azonosítóját úgy adjuk meg, hogy a géptől a legfelső szintű domain felé haladva, egymástól pontokkal elválasztva, leírtjuk az azonosítókat. A **Domain Name System** segítségével biztosítható, hogy a hálózat minden egyes gépe teljesen egyedi azonosítót kaphasson. Az így megadott azonosítót hívjuk a gép **domain névének**.

7.6 A DOMAIN NAME SERVICE

A **Domain Name System** megoldja a hostok teljes hálózaton érvényes egyedi elnevezését, de a domainek hierachikus rendszere önmagában még nem kezeli a névfeloldás problémáját.

Az egyedi gépeken tárolt **hosts** állományok nem alkalmasak arra, hogy a hálózat összes létező gépének domain nevét és IP címét tárolják.

A megoldást a **Domain Name Service** nevű szolgáltatás biztosítja. A szolgáltatás alapját az egyes tartományokban üzemelő, egymással (a tartományrendszernek megfelelő) hierarchikus kapcsolatban álló szerverprogramok, a Domain Name Serverek (DNS) adják. A top level domainek DNS-ei fölött még további 13, úgynevezett root (gyökér) DNS áll. Ezek nem kötődnek domainekhez, hanem a hierarchia csúcsát alkotják.

Minden egyes DNS a saját tartományába tartozó gépek IP címeit és hozzájuk kapcsolt neveket tartalmazó adatbázist kezeli. Az adatbázisok a **hosts** állományokhoz hasonlóak, de azoknál jóval összetettebb szerkezetűek. A DNS-ek ismerik a hierarchiában közvetlenül alattuk, és fölöttük lévő DNS-ek IP címét is. Minden DNS adatbázisát az adott tartomány rendszergazdái tartják karban, ők felelősek azért, hogy egy tartományban minden fontos gép domain neve és IP címe szerepeljen a DNS adatbázisában.

Ebben a rendszerben úgy történik a névfeloldás, hogy amikor egy host felhasználója domain névvel címez meg egy gépet, akkor a hoston futó, névfeloldást végző program, az úgynevezett **resolver**, a saját, közvetlen tartományának DNS-éhez fordul.

1. A resolver kérést küld saját tartománya DNS-ének, azaz a feloldás érdekében elküldi a DNS-nek a keresett domain nevet.
2. A DNS megvizsgálja, hogy adatbázisában szerepel-e a név, vagy sem.
3. Ha a kérésben kapott domain név szerepel az adatbázisban, akkor a DNS feloldja a nevet, és visszaküldi a resolvernek az IP címet.
4. Ha a név nem szerepel az adatbázisban, a DNS a vele kapcsolatban álló másik DNS címét küldi el a resolvernek, a resolver pedig a másik névszervernél újra kísérletet tesz a feloldásra.

a. Ha a keresett domain név a DNS tartományának egy résztartományában van, akkor a megfelelő résztartomány DNS-hez kerül a kérés. Ezt technikát nevezzük **delegálásnak**.
b. Ha a keresett név nem egy altartományban van, akkor a DNS a hierarchiában közvetlenül fölötte elhelyezkedő DNS-hez továbbítja a kérést. Ezt **forwarding**nak, továbbításnak nevezzük.

5. Ha egy top level domain DNS-e nem tud feloldani egy nevet, és az nem is egy saját altartományába tartozik, akkor valamelyik root DNS-nek fog forwardolni.
6. Ha egy DNS a domain név alapján sem feloldani, sem delegálni sem forwardolni nem tud, hibaüzenetet küld a resolvernek.

A Domain Name Service szolgáltatásban a DNS a szerver (általában az 53-as UDP portot használja), a resolver a kliens szerepét játssza. A szoftverkomponensek közötti szabványos kommunikációt a DNS protokoll biztosítja.

A Domain Name System struktúrája és a Domain Name Service szolgáltatás együtt teszi lehetővé, hogy a felhasználók az interneten végzett hálózati munka során IP címek helyett domain neveket használjanak a hostok azonosítására.

7.7 A DNS IP CÍMÉNEK MEGADÁSA

A további fejezetekben látni fogjuk, hogy az internetszolgáltatások általában kliens szerver alapúak. A kapcsolatfölvételt mindig a helyi gép felhasználója által elindított kliens kezdeményezi. A DNS szolgáltatás kliensének (resolver) indítása nem igényel felhasználói beavatkozást. A gép bekapcsolásakor a resolver automatikusan elindul.

A domain nevek feloldásához azonban a hostnak feltétlenül ismernie kell saját tartománya DNS-ének IP címét. A resolver csak ennek ismeretében tudja elküldeni a feloldási kéréseket.

Amikor számítógépünket internethez kapcsoljuk meg kell adnunk az egyes hálózati csatolókon történő TCP/IP alapú kommunikáció alapbeálltásait:

- a csatoló IP címét,
- a hálózati maszkot,
- az alapértelmezett átjáró címét,
- és legalább egy DNS IP címét is.

DHCP szerver használata esetén általában automatikusan kapjuk meg a fenti adatokat.[9]

7.8 SZERVEZETEK DOMAIN NEVEINEK KIOSZTÁSA

A Domain Name System kapcsán már említettük, hogy a domain azonosítóknak saját közvetlen szülőtartományukon belül egyedinek kell lenniük. Ha egy top-level domainben új tartományt hoznak létre, annak új, egyedi, mások által még nem használt nevet kell biztosítani. A nevek egyediségét minden egyes legfelső szintű domainben egy ezzel a feladattal megbízott szerveret végzi. A magyar (hu) domainben az Internet Szolgáltató Tanácsa

[9] DHCP esetén megadható, hogy automatikusan kapott, vagy pedig fix DNS címeket akarunk használni.

(ISZT) tartja nyilván a már létező aldomainek neveit. Ha egy új cég vagy szervezet saját tartományt szeretne létrehozni a magyar domainben, akkor az ISZT-től kell tartománynevet igényelnie. Az ezzel kapcsolatos szabályok és az igénylés módja a tankönyvünk megírásakor a **http://www.domain.hu** címen elérhető oldalakon olvasható.

7.9 ÖSSZEFOGLALÁS

Az internet különböző kommunikációs célokra történő felhasználását az úgynevezett szolgáltatások biztosítják. A szolgáltatások alapját általában kétféle szoftverkomponens, a kliens és a szerver teszi lehetővé. A közöttük zajló kommunikáció szabványosságát a szolgáltatás protokollja biztosítja. Az eredményes kommunikáció érdekében kliensnek és a szervernek is ugyan azt a protokollt kell betartania. A szerver biztosítja magát a szolgáltatást, a kliens pedig a felhasználó hozzáférést a szolgáltatáshoz.

Az internet az csatlakozó gépeken használt leggyakoribb szolgáltatás a felhasználó elől rejtve működik. A Domain Name Service feladata, a hostok domain nevének IP címmé alakítása, a névfeloldás. A szolgáltatás kliense a resolver, szervere a Domain Name Server. A DNS működésének alapja a Domain Name System, a hierarchikusan egymásba ágyazott domaineken alapuló elnevezési rendszer. A top level domainek aldomainekre vanak osztva, a résztartományok pedig tovább strukturálhatók. Minden terület saját azonosítóval rendelkezik. Egy hosttól a top level domain felé haladva, a gépnevet, majd a domainek azonosítóját egymástól pontokkal elválasztva, a host domain nevét kapjuk.

A DNS-rendszer hierarchikusan kialakított, osztott adatbázisának segítségével oldja fel a domain neveket. A host resolvere mindig saját tartományának DNS-éhez intézi a feloldásra vonatkozó kérést. A DNS vagy feloldja az azonosítót, vagy delegálja, vagy pedig forwardolja a kérést. Ha egy DNS sem feloldani, sem delegálni sem pedig forwardolni nem képes az azonosítót, akkor az azonosító nem oldható fel.

Ha a névfeloldás szolgáltatás nem működik, a gépünkön csak IP címeket használhatunk a címzésre. A névfeloldás helyes működéséhez internethez csatlakoztatott gépünket helyesen kell konfigurálni. Statikus beállítások esetén az IP címen, a hálózati maszkon, és az alapértelmezett átjárón kívül, be kell állítanunk a DNS IP címét is. DHCP szerver használata esetén a konfiguráció automatikus.

7.10 ÖNELLENŐRZŐ KÉRDÉSEK

1. Milyen szoftverkomponensek biztosítják egy szolgáltatás működését?
2. Mi biztosítja azt, hogy a kliens és szerver közötti üzenetek biztosan értelmezhetők legyenek a kommunikáló felek számára?
3. Milyen fogalmat takar a DNS rövidítés?
4. Mik azok a top-level domainek?
5. Hogyan nevezik el a legfelső szintű tartományokat?
6. Mi az a resolver?
7. Mi az a forwarding?
8. Mik azok a root DNS-ek?
9. Hogyan lehet Magyarországon domain nevet igényleni?
10. Hová fordul egy hoston futó resolver elsőként egy név feloldásakor?

8. TELNET, SSH, TÁVOLI ASZTAL

8.1 CÉLKITŰZÉS

A számítógép hálózatok szolgáltatásainak kialakulását és fejlődését, más szoftvereszközökhöz hasonlóan alapvetően a kor informatikai színvonala, valamint az ebből fakadó követelmények, és persze jelentős részben a felhasználói igények határozzák meg. (Kétségtelen ugyanakkor, hogy a szoftvergyárak fejlesztései is komoly hatással vannak a felhasználók elvárásaira.) Már a hálózatok fejlődésének korai szakaszában szükségesnek tartották távoli hozzáférést biztosító eszközök kifejlesztését, amelyeknek segítségével egy lokális gépről úgy lehet vezérelni egy távoli gépet, mintha a felhasználó mellette ülne.

Az első ilyen szolgás a Telnet volt, de az informatikai követelmények és a felhasználói igények később újabb, távoli elérést biztosító szolgáltatásokat is életre hívtak.

Ebben a leckében a hallgató megismerheti a Telnet, és az azt felváltó SSH szolgáltatás lényegét, de megismerheti a Windows környezetben használt Távoli asztal eszközt is.

A lecke végére tisztában lesz az egyes eszközök nyújtotta lehetőségekkel, megismerheti a Telnet és az SSH szolgáltatások közötti legfontosabb különbséget, alapvető felhasználó ismereteket szerezhet a használatukhoz szükséges kliensprogramok egyikéről.

Megismerheti a Távoli asztal szolgáltatás lehetőségeit, használatának feltételeit, megtanulhatja, hogyan érheti el otthonából munkahelyi számítógépét.

8.2 A LECKE TÉMAKÖREI

- A Telnet szolgáltatás
- A Telnet kliens használatának feltételei
- Távoli gép vezérlése Telnettel
- A biztonságos kommunikáció
- Távoli elérés biztonságos csatornán
- Távoli elérés grafikus környezetben

8.3 A TELNET SZOLGÁLTATÁS

A Telnet az egyik legrégibb Internetes szolgáltatás, amely már az ARPANET-en is használható volt. A szolgáltatást magyarul távoli bejelentkezésnek szokás nevezni.

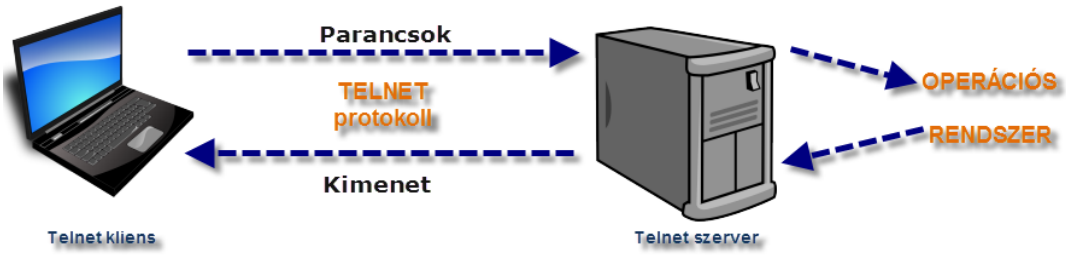
A Telnet révén távoli számítógép, és az azon futó operációs rendszer használatára nyílik lehetőség a saját gépünkről.

A személyi számítógépek megjelenése előtt gyakori volt, hogy egy szervezet (cég, intézmény) munkatársai **terminálok** segítségével kapcsolódtak a cég nagyszámítógépéhez. A nagygépen futott az összes program, és itt tárolódott minden adat. A terminálok önállóan működésképtelen, gyakorlatilag csak adat be- és kivitelre alkalmas, billentyűzetből és monitorból álló informatikai eszközök voltak. Egy-egy számítógéphez több terminál csatlakozott. Mindenki a saját terminálján dolgozhatott, de begépelt parancsai a cég nagy számítógépéhez jutottak, amely a feldolgozás után visszaküldte az eredményeket a terminál monitorára. A felhasználók egymás munkáját nem zavarták, gyakorlatilag nem is kellett

tudniuk arról, hogy ugyanazon a nagygépen dolgoznak. A Telnet szolgáltatás valójában a nagygép-terminál kapcsolat lehetőségeinek hálózati megvalósítása.

Manapság már nem terminálokon, hanem önállóan is működőképes személyi számítógépeken dolgozunk, mégis szükségünk lehet arra, hogy más gépekhez távolról kapcsolódjunk. Ezt teszi lehetővé a TELNET szolgáltatás, amely valójában terminál emulációt (utánzás) valósít meg.

A szolgáltatás szoftveres komponensei a **telnet szerver** és **telnet kliens**. A kliens terminálként működteti számítógépünket. Segítségével gépünk úgy kapcsolódhat a távoli géphez, mintha annak terminálja lenne. A kliens saját gépünk monitorán a távoli gép képernyőjének tartalmát jeleníti meg. Begépelt parancsainkat elküldi a szervernek, az pedig átadja a parancsokat a távoli gép operációs rendszerének. Az operációs rendszer válaszának megfelelő képernyőtartalmat a szerver visszaküldi a kliensnek, az pedig megjeleníti a szervertől érkező adatokat a képernyőn.



20. ábra Felhasználó–telnet kliens–üzenet–telnet szerver–operációs rendszer, majd ugyanez visszafelé

8.3.1 A Telnet használatának feltételei

A távoli gépen Telnet szervernek kell működnie ahhoz, hogy egy távoli gépet, Telnet szolgáltatással elérjünk és saját gépünkről vezéreljük. A szerver telepítése és megfelelő beállítása az ottani rendszergazda feladata. További feltétel, hogy érvényes felhasználói jogosultsággal rendelkezzünk, amit szintén a rendszergazda biztosíthat számunkra.

Saját gépünkön a szerver gép elérést biztosító hálózati kapcsolatra, és futtatható Telnet kliensre van szükségünk. A szerver és a kliens közötti **telnet** protokollt magáról a szolgáltatásról nevezték el. A telnet szerverek egyébként általában a 23-as TCP porthoz kapcsolódnak.

8.3.2 A Telnet szolgáltatás lehetőségei

A Telnet szolgáltatás lehetőségeinek megértéséhez, az alapvető célon túl (host távoli vezérlése) ismernünk kell két további fontos sajátosságot.

A Telnet **kizárólag karakteres vezérlést** tesz lehetővé, azért csak olyan operációs rendszerek esetében használható, amelyek parancssori üzemmódra is képesek.

A Telnet szerver és kliens között mindenféle **titkosítás nélküli, szöveges üzenetek** kerülnek továbbításra, azért az adatok biztonsága komoly csorbát szenved. Elsősorban ez az oka annak, hogy míg néhány éve, a Telnet, a UNIX és a Linux gépek rendszergazdáinak és

felhasználóinak alapvető eszköze volt a távoli elérésben, napjainkra a felhasználás területei erősen beszűkültek.

Hozzávetőleg egy évtizede, amikor a hálózati biztonság még nem kapott akkora hangsúlyt, mint napjainkban, az alábbi feladatokra jellemzően Telnetet használtak:

- Rendszergazdák távolról Telnet segítségével végezték a legkülönfélébb adminisztrációs feladatokat.
- A UNIX és a Linux operációs rendszereket futtató gépek felhasználói távolról bejelentkezve el tudták olvasni leveleiket, használni tudták a távoli gép erőforrásait.
- Jellemző volt a távoli gépeken működő adatbázisok, Telnet kapcsolattal történő elérése is. Különösen igaz volt ez például könyvtári adatbázisokra, katalógusokra.
- Egyes hálózati eszközök, például routerek szintén működtettek Telnet szervert. Az ilyen berendezésekre bejelentkezve lehetőség nyílt az eszköz távoli konfigurálása.

Mindezekből mára szinte csak az utolsó funkció maradt. Egyes hálózati eszközök még ma is Telnet kapcsolattal konfigurálhatók. A nem biztonságos hálózatokból elérhető gépekre a rendszergazdák már gyakran föl sem telepítik a Telnet szervert, így azok nem érhetők el Telnet kapcsolattal.

Bár a Telnetet már nagyon kevés helyen használják, az elvi lehetőség adott. A UNIX és a Linux operációs rendszerek mellett léteznek Windows operációs rendszeren telepíthető Telnet szerverek is, amelyek képesek biztosítani a Windows operációs rendszert futtató gép távoli elérését, és **parancssori** vezérlését.

A Telnettel kapcsolatos érdekesség, hogy a szolgáltatással más, karakter alapú kommunikációt folytató szerverhez is kapcsolódhatunk. Ilyenek például az elektronikus levelek letöltését biztosító SMTP szerverek, amelyek általában a 25-ös TCP porthoz kapcsolódnak. Ha egy SMTP szervert futtató számítógép 25-ös TCP portjára telnetelünk, az SMTP protokoll szerint megfogalmazott szöveges üzenetekkel vezérelhetjük a levelező szervert.

8.3.3 Gépek távoli vezérlése a Telnet kapcsolattal

Ha a fent leírtak ellenére mégis adottak egy gép Telnet elérésnek feltételei, a távoli elérés a következő lépésekben történik:

- **A kliens indítása:** Saját gépünkön el kell indítani a telnet klienst. Ha Linux operációs rendszert használunk, egyszerűen be kell gépelni a **telnet** parancsot. Windows operációs rendszer esetén meg kell nyitnunk a parancssori ablakot, és ott elvégezni a fent leírtakat. Az ezután begépelt parancsok már a klienst, illetve a kapcsolat felépítése után a távoli gépet vezérlik.
- **Kapcsolat felépítése a távoli géppel**: A kliens indulása után fel kell építeni a kapcsolatot a távoli géppel. Ez a kliensnek kiadott **open** paranccsal lehetséges. A parancs után meg kell adnunk a Telnet szervert futtató gép **ip** címét, vagy **domain** nevét. pl.: **open 192.168.1.3** A kliens a távoli gép 23-as TCP portjához próbál kapcsolódni. Ha tudjuk, hogy a szervert másik portra állították, a cím után kettőspont-tal elválasztva meg kell adnunk a portot.

- **Bejelentkezés:** Ha a szerver reagál a kliens kapcsolatkérésre, akkor megjelenik az úgynevezett *login prompt*, azaz bejelentkezési üzenet. Most kell megadnunk a távoli gépen érvényes felhasználói nevünket, majd pedig jelszavunkat. Ha a távoli gép nem érhető el, vagy a telnet szerver nem válaszol, akkor a kliens megfelelő hibaüzenetet küld.
- **Távoli gép vezérlése:** A sikeres bejelentkezés követően monitorunkon a távoli gép képernyője látszik, a képernyő alján pedig megjelenik a készenléti jel. A Telnet kliens minden ezután begépelt parancsot elküld a szervernek, az pedig a távoli gépen futó operációs rendszernek. A parancs nyomán megváltozott képernyőtartalom visszajut a saját gépünkre, és megjelenik a monitoron. Fontos tudnunk, hogy most csak a távoli gépen futó operációs rendszer parancsait használhatjuk!
- **A kapcsolat bontása:** Amikor befejeztük a munkát, ki kell jelentkeznünk a távoli gépről, és bontani kell a kapcsolatot. Ezt az **exit** parancs begépelésével tehetjük meg. Az **exit** hatására a kliens elbontja a kapcsolatot, és készen áll újabb csatlakozásra.
- **A kliens bezárása:** A kliens bezárása **quit** parancs begépelésével lehetséges.

8.4 BIZTONSÁGOS KOMMUNIKÁCIÓ

A Telnet szolgáltatás nélkülözhetetlen hálózati feladatot valósított meg, biztosította távoli gépek parancssori vezérlését. A szolgáltatás háttérbe szorulását biztonsági hiányosságai okozták.

8.4.1 A biztonságos kommunikáció alapelvei

Két fél hálózati kommunikációja akkor biztonságos, ha teljesülnek az alábbi alapelvek:

- **Bizalmas kezelés:** harmadik fél nem tudja értelmezni az üzenetet
- **Az adat sérthetetlensége:** harmadik fél nem tudja észrevétlenül megváltoztatni az üzenet tartalmát.
- **Azonosítás, hitelesítés:** A címzett képes megállapítani az üzenet származását, tudja azonosítani a feladót.
- **Letagadhatatlanság:** Bizonyítható, hogy ki a feladó. A feladó nem tudja letagadni az üzenetet.

Ezeket a feltételeket az hálózati kommunikációban kriptográfiai módszerekkel biztosítják.

A kriptográfia az alkalmazott matematika egy ága, amely az adatok biztonsági célú átalakításával, titkosításával, matematikai alapokon nyugvó „titkosírások" kidolgozásával foglalkozik. A kriptográfia a kommunikációs csatornán küldött adat sérthetetlenségének, hitelességének, bizalmas kezelésének, illetve letagadhatatlanságának biztosítására dolgoz ki eljárásokat.

Amikor két fél kriptográfiai eljárások segítségével titkosított formában kommunikál egymással, a feladó kódolja, a címzett pedig dekódolja az üzenetet.

A feladó általában valamilyen kulcsot használ a kódoláshoz. A kulcs olyan adat, amelyet egy bizonyos eljárás alkalmazásával egy másik adat kódolásához, és dekódolásához használnak.

Lássunk egy egyszerű példát:

Kódolni szeretnénk a KRIPTOGRÁFIA szót.

Egyszerű eljárást használunk: minden betűt az ABC-ben két hellyel utána következő betűre cserélünk. (A kettős betűket kihagyjuk: dz, cs, ly,ny.... Az utolsó betűk esetén az ABC elejére lépünk.)

K+2=M

R+2=T

I+2=J

P+2=R

T+2=Ú

O+2=Ö

G+2=I

R+2=T

Á+2=C

F+2=H

I+2=J

A+2=B

MTJRÚÖITCHJB

Az eljárás az ABC-beli eltolás, a kulcs pedig 2.

A címzettnek ugyan azt az eljárást és kulcsot kell használnia az üzenet dekódolásához, amit a feladó a kódoláskor használt.

A hatékony kódoláshoz és dekódoláshoz használható eljárások ismertek, ezért a kód feltörhetetlenségét mások számára ismeretlen és megismerhetetlen (vagy csak nagyon nehezen megismerhető) kulcsokkal kell megoldani. A kriptográfia alapvető problémája, hogy olyan eljárásokat és kulcsokat dolgozzon ki, amelyek biztosítják a biztonságok kommunikáció alapelveinek megvalósítását, illetve, hogy a kommunikáló felek úgy tudassák egymással a használt kulcsot, hogy azt mások ne szerezhessék meg.

8.4.2 Nyilvános kulcsú kódolás

A nyilvános kulcsú, vagy aszimmetrikus titkosítás azon alapszik, hogy léteznek olyan kulcspárok, amelyek egyike kódolásra (nyilvános kulcs), míg másik a (titkos kulcs) dekódolásra alkalmas. A nyilvános kulccsal kódolt üzenet csak a megfelelő titkos kulccsal dekódolható. Ha egy személy (vagy informatikai eszköz) rendelkezik titkos, és nyilvános kulccsal is, nyilvános kulcsát közölheti másokkal, még titkos kulcsát titokban kell tartania.

A neki szánt üzeneteket bárki kódolhatja a közzétett nyilvános kulcs segítségével, de csak ő tudja azt visszafejteni saját, titkos kulcsával.

Az informatikában leggyakrabban használt nyilvános kulcsú kódolási eljárás az RSA titkosítás, melyet 1976-ban Ron Rivest, Adi Shamir és Len Adleman fejlesztett ki.

8.5 Az SSH

Az SSH (Secure Shell) szolgáltatás és protokoll egyben. A Telnethez hasonlóan távoli számítógépek elérésére és operációs rendszerük vezérlésére fejlesztették ki 1995-ben. Az első változat megalkotója Tatu Ylönen, aki akkor Helsinki Műszaki Egyetem kutatója volt. A Telnet és az SSH közötti alapvető különbség, hogy az SSH biztonságos kommunikációs csatornát épít ki a kliens és a szerver között, mégpedig úgy, hogy nyilvános kulcsú titkosítást használ a kommunikáló gépek hitelesítésére, és az átvitt adatok bizalmasságának biztosítására. Általában távoli gépre történő belépésre és azok vezérlésére használják, a szolgáltatás azonban alkalmas fájlok biztonságos csatornán történő átvitelére is. Erről a 9. Az FTP szolgáltatás leckében olvashat.

Az SSH szerverek általában a 22-es TCP porthoz kapcsolódnak, de úgy alkották meg őket, hogy a beérkezett és dekódolt üzeneteket más portokon „figyelő” szervereknek is képesek legyenek továbbítani. Ezt a technikát nevezik tunnelingnek. A tunneling alkalmas arra, hogy egy SSH kommunikációt engedélyező tűzfalon keresztül, a tűzfal mögötti hálózat más, a tűzfalon letiltott szervereivel is kommunikálni tudjunk.

8.5.1 Az SSH használatának feltételei

Az SSH szolgáltatás használatának feltételei hasonlóak az Telnet szolgáltatásnál felsoroltakkal, azzal a különbséggel, hogy a helyi gépen SSH kliensnek, a távoli gépen SSH szervernek kell futnia. A Windows környezetben az egyik legelterjedtebb SSH kliens a PUTTY, amelyet a **www.putty.org** oldalról tölthetünk le.

8.5.2 Az SSH kapcsolat

Az SSH kapcsolat felépítése természetesen a kliens indításával történik. A PuTTY grafikus felülettel, és parancssori interfésszel egyaránt rendelkezik. Tananyagunkban a grafikus felület használatát mutatjuk be.

- A kliens indítása: A kliens a **PuTTY.exe** ikonjával történő indítás után egy párbeszédablakot jelenít meg, amelyben a Host Name szövegmezőben meg kell adnunk az SSH szervert futtató gép címét. A kapcsolat kiépítése az **Open** gombbal indul el.
- A hostok azonosítása: A kapcsolat kialakítása azzal kezdődik, hogy a kliens és szerver azonosítják egymást. Mindkét gép rendelkezik egy egyedi host azonosítóval, a szerver pedig ezen túl egy időszakonként újra generálódó szerver kulccsal. Ezek, és a kliens által a kapcsolat felépítése közben generált véletlen szám segítségével a szerver és a kliens azonosítja magát, majd megegyeznek az adatforgalom

titkosítására használt kulcsban. Ezt követően kapcsolat titkosított módon történik. Harmadik fél hiába szerzi meg az üzeneteket, azok tartalmát nem képes dekódolni.

- Bejelentkezés: A kapcsolat felépítése után a Telnethez hasonló módon történik meg a felhasználó azonosítás, de a kliens felületén begépelt azonosítók, már titkosított csatornán jutnak a szerverhez, így azokat nem lehet „ellopni”.
- Távoli operációs rendszer vezérlése: A bejelentkezést követően pontosan úgy történik, mint a Telnet esetében.
- Kapcsolat bontása: A kapcsolat bontást, az **exit** paranccsal végezhetjük el.
- Kliens bezárása: Az **exit** parancs begépelésekor a PuTTY ablaka, egyben a kliens is bezárul.

8.6 A TÁVOLI ASZTAL

A Telnet és az SSH segítségével parancssori operációs rendszerek elérésére van lehetőség[10]. A mai asztali operációs rendszerek, – de számos hálózati operációs rendszer is – általában grafikus felületet biztosítanak a felhasználói munka számára. A számítógéphasználat egyre elterjedtebbé válik az otthonokban és munkahelyeken egyaránt. A hálózati kapcsolatok számának dinamikus növekvésével párhuzamosan egyre többen szeretnék grafikus operációs rendszert futtató gépüket a hálózat segítségével, távolról használni. Ezt a feladatot valósítják meg, a különböző képernyő megosztó szolgáltatások.

A feladat megoldása valamivel bonyolultabb, de alapjaiban mégis hasonló, mint azt az előző eszközöknél láttuk. A grafikus operációs rendszerek rendelkeznek olyan ablakkezelő és beviteli eszközöket kezelő alrendszerrel, amelyek érzékelik a felhasználó billentyűzettel, egérrel végzett műveleteit, illetve grafikus felületen megjelenítik az operációs rendszer által elvégzett művelet eredményét.

A helyi gépen futó kliens érzékeli a felhasználói tevékenységet, majd azt a távoli gépen futó szerveren keresztül eljuttatja a távoli operációs rendszerhez. Az távoli operációs rendszer feldolgozza a felhasználó utasításait, elvégzi a megfelelő műveltet, majd az eredményt a lokális gép grafikus alrendszerének küldi vissza, így a kimenet a lokális gép képernyőjén jelenik meg. Az informatikában több gyártó is készített ablak megosztó alkalmazásokat. Ezek közül a legismertebbek a Linux rdesktop, az Apple Remote Desktop, és Microsoft Windows Remote Desktop szolgáltatásai. Utóbbit Távoli asztal szolgáltatásként került be a köztudatba.

8.6.1 A Távoli asztal lehetőségei

A távoli asztal szolgáltatás használatával a legalább Windows XP operációs rendszert futtató lokális számítógépünkről bejelentkezhetünk a távoli gépen futó Windows rendszerbe. A helyi gépnél ülve szinte mindent elvégezhetünk, a távoli gépen.

- Az adatbevitelhez használhatunk billentyűzetet, és pozícionáló eszközöket (pl. egér, touchpad).
- Némi korlátozással billentyűkombinációkat is alkalmazhatunk.

[10] Az állítás némi kiegészítésre szorul, az SSH ugyanis alkalmas arra is, hogy X11 kapcsolatok tunnelingjét is így alkalmas grafikus vezérlés megvalósítására is.

- Futtathatunk bármilyen, telepített alkalmazást.
- Hálózati kommunikációt indíthatunk.
- Használhatjuk a távoli gép bármilyen hardver erőforrásait.
- Lehetőségünk van a távoli gépen történő nyomtatás, helyi nyomtatóra irányítására.
- A távoli gép hangjait a lokális gépen szólaltathatjuk meg.
- A két gépen kölcsönösen használhatjuk a vágólap szöveges tartalmát.
- A távoli asztal kapcsolaton keresztül akár fájlok átvitelét is megvalósíthatjuk.

8.6.2 A Távoli asztal szolgáltatás használatának feltételei

A távolról szeretnénk használni Windows operációs rendszert használó gépünket, akkor a lokális és távoli gépen egymással kompatibilis ablakkezelő rendszert futtató operációs rendszereknek kell működniük.[11]

- A lokális gépen telepítve kell lennie a **Távoli aszal kliensnek.**
- A távoli gépen telepített **Távoli asztal szerverre** van szükség.
- Az elindított szerveren túl a távoli gépen engedélyezni kell a távoli hozzáférést, és meg kell határozni a távoli bejelentkezési joggal rendelkező felhasználók körét.
- Ha a távoli gép tűzfal mögött van, a tűzfalon engedélyezni kell a távoli asztal szerver által használt **3389**-es TCP portot.
- A távoli gépen rendelkeznünk kell a távoli bejelentkezési joggal.

8.6.3 A Távoli asztal kapcsolat felépítése

- A kliens indítása: A Távoli asztal kapcsolatot a lokális gépen, a kliens indításával kezdjük. (Windows XP esetén a Start/Programok/Kellékek/Távoli asztal kapcsolat parancsot kell használnunk).
- Alapértelmezett beállítások átírása: A kliens egy egyszerű párbeszédablakot jelenít meg, amely a **Beállítások** gombra kattintva kibővíthető. Ebben az állapotban átírhatjuk, sőt a megváltoztatott állapotban menthetjük is a kapcsolat alapértelmezett tulajdonságait.
- Ha **Beállítások** gombot nem használjuk, a kliens egy egyszerű párbeszédablakot jelenít meg, ahol csupán a távoli gép címét kell megadnunk. A kapcsolat az a **Csatlakozás** gombbal felépíthető.
- Bejelentkezés: A bejelentkezés már a távoli gépen beállított módon, a megszokott grafikus felületen történik, a felhasználói név, és a jelszó megadásával.
- Kapcsolat bontása: A kapcsolat bontásakor a távoli gép **Start/Kijelentkezés** parancsát használva a **Kapcsolat bontása** parancsot kell választanunk.

[11] Leegyszerűsítve ez azt jelenti, hogy a lokáli gépen is Windowst kell futtatnunk.

8.7 ÖSSZEFOGLALÁS

A távoli elérés szolgáltatások a számítógép hálózatok megjelenésével azonos időben keletkezett felhasználó igényt valósítanak meg. Segítségükkel helyi számítógépünket használva, úgy vezérelhetjük a távoli gép operációs rendszerét, mintha a géphez csatlakozó perifériákkal dolgoznánk.

A távoli elérést megvalósító szolgáltatások közül a Telnet az egy legrégibb alkalmazás. Karakteres felületű operációs rendszerek vezérlését teszi lehetővé. Legnagyobb hiányossága, hogy kódolatlan, karakteres adatátvitelt valósít meg. Ennek köszönhetően a Telnet protokollal továbbított adatok (már a bejelentkezéskor megadott felhasználói név és jelszó is) könnyűszerrel lehallgathatók. Hiányosságai ellenére a Telnetet még mai is használják biztonságos hálózatokon, és egyes hálózati eszközök konfigurálásakor.

Az SSH alapjaiban a Telnet funkcióit valósítja meg, a kommunikációt titkosított, biztonságos csatornán valósítja meg, a tunneling funkció segítségév el pedig alkalmas más protokollal megvalósított kommunikáció biztonságos továbbítására is.

A grafikus operációs rendszerek távoli hozzáférését olyan ablakmegosztó rendszerek biztosítják, mint az Apple Remote Desktop, vagy a Microsoft Remote Dektop, más néven Távoli asztal. Utóbbi segítségével végzett távoli munka során az sztenderd adat be- és kivitelen túl fájok, hang átvitelére, nyomtató árirányításra, vágólap tartalmának megosztásra is lehetőség nyílik

8.8 ÖNELLENŐRZŐ KÉRDÉSEK

1. Milyen funkciót biztosítanak a távoli elérés szolgáltatások?
2. Mit ért telnet szolgáltatás alatt?
3. Mik a telnet legfontosabb hiányosságai?
4. Mik a biztonságos kommunikáció legfontosabb alapelvei?
5. Mit a kriptográfia?
6. Milyen kódolást alkalmaznak az SSH kommunikációban?
7. Mit értünk tunneling alatt?
8. Milyen célt szolgálnak az ablakmegosztó szolgáltatások?
9. Van-e lehetősége a Távoli asztal szolgáltatás használatával a távoli gép perifériáinak lokális gépre történő átirányítására?
10. Lehet-e képeket vágólappal átmásolni a Távoli asztal szolgáltatásban?

9. AZ FTP SZOLGÁLTATÁS

9.1 CÉLKITŰZÉS

A távoli elérés szolgáltatások lehetővé teszik távoli gépek vezérlését, de nem mindig biztosítanak fájlátviteli lehetőségeket a helyi és a távoli számítógép között. A fájlátvitel ugyanakkor alapvető hálózati feladat. Az interneten többféle eszköz is lehetővé teszi a fájlok hostok közötti mozgatását (e-mail, WWW, azonnali üzenetküldők). Ezek között a lehetőségek között azonban mindenképpen érdemes kiemelni az FTP (File Transfer Protokoll) szolgáltatatást, amely bár az egyik legkorábban kifejlesztett fájltranszfer eszköz volt, a mai napig megőrizte fontosságát az internetes fájlátvitelben.

Ebben a leckében a hallgató megismeri az Ftp működésének alapjait, a szolgáltatás használatának feltételeit, megtanulja egy egyszerű, szinte minden internet kapcsolattal rendelkező gépen elérhető, karakteres Ftp kliens használatát, de azt is, hogyan használhatja internetes fájlátvitelre az egyik legnépszerűbb fájlkezelő programot, a Total Commander-t.

9.2 A LECKE TÉMAKÖREI

- Az Ftp lehetőségei
- Ftp szerver, Ftp kliens
- Felhasználói jogosultságok
- Karakteres Ftp kliens használata
  - Kapcsolat felépítése és bejelentkezés
  - Ftp parancsok
  - Kapcsolat bontása
- Biztonságos Ftp
- Grafikus Ftp kliensek
  - Ftp kapcsolat felépítése a Total Commanderrel
  - Fájlok átvitele
  - Kapcsolat bontása

9.3 AZ FTP SZOLGÁLTATÁS

Mielőtt hozzákezdenénk az FTP szolgáltatás használatának ismertetéséhez, tisztázzuk néhány gyakran használt kifejezés jelentését.

- **Helyi gép:** az FTP klienst futtató számítógép.
- **Távoli gép:** az FTP szervert futtató számítógép.
- **Root könyvtár**: az FTP szervert futtató számítógép fájlrendszerének az a könyvtára, amelyben szerverrel hozzáférhető adatok tárolódnak.
- **Aktuális könyvtár:** a helyi, illetve távoli gép éppen kiválasztott könyvtára
- **Letöltés:** fájl(ok) másolása az FTP szerverről a helyi gépre
- **Feltöltés:** fájl(ok) másolása a helyi gépről az FTP szerverre
- **Home directory:** az FTP szerverre saját accounttal bejelentkező felhasználó saját könyvtára.

Az FTP (File Transfer Protokoll), a TCP/IP modell alkalmazási rétegében használt protokoll, de egyben, a még manapság is, igen népszerű szolgáltatás neve is. A szolgáltatás lényege, hogy az Interneten elhelyezkedő két gép között, lehetővé teszi fájlok átmásolását. Az FTP-t használva óriási tömegű állományhoz, programhoz, dokumentumhoz juthatunk hozzá. Megszerezhetők történelmi dokumentumok másolatai éppúgy, mint számos shareware program, vagy akár egy teljes Linux disztribúció. A szolgáltatóktól kapott web területekre általában, szintén FTP-vel másolhatjuk fel a lokális gépen készített weblapjainkat.

A Telnethez hasonlóan, az FTP is kliens-szerver alapú szolgáltatás. Szerver oldali összetevője egy olyan program, ami hozzáfér az őt futtató host fájlrendszerének egy részéhez, egy a rendszergazda által kijelölt könyvtárhoz, és annak teljes tartalmához. Az FTP kliensekkel kapcsolódhatunk egy távoli gép FTP szerveréhez, és az ott található állományokat saját gépünkre másolhatjuk. A fájlok átvitele fordított irányban is megvalósítható, azaz megfelelő jogok birtokában saját gépünkről is másolhatunk fájlokat az FTP szervert futtató számítógépre.

A fájlok átvitele közben számos részfeladatot kell megoldani, amelyek végrehajtása érdekében a felhasználó parancsokkal vezéreli a helyi gépen futó klienst. Az ügyfél részben feldolgozza, részben pedig továbbítja ezeket a parancsokat szervernek. A két szoftverkomponens között tehát nem csak a le- és feltöltött adatok, hanem különböző parancsok is áramlanak.

9.4 KAPCSOLAT AZ ÜGYFÉL ÉS A KISZOLGÁLÓ KÖZÖTT

Az FTP szoftverkomponensei közötti kapcsolat némileg eltér a szokványos kliens-szerver kapcsolatoktól. A kiszolgáló és a kliens között, ugyanis **két kommunikációs csatorna** épül fel. Ez egyik a kliens és szerver közötti **parancsok átvitelére**, a másik az **adatok mozgatására** szolgál. Az FTP szerver a 20-as TCP portot figyeli, a kliens ezen a porton keresztül veszi fel vele a kapcsolatot, és építi ki a parancs csatornát.

Ezt követően kétféleképpen alakulhat ki az adatcsatorna:

1. **Alapértelmezés szerint**, a parancscsatorna felépítésekor az ügyfél saját portot nyit, és elkezdi azt figyelni. A port számát elküldi a szervernek. **Az adatcsatorna fölépítését a szerver kezdeményezi.** Saját 21-es TCP portjáról kapcsolódni próbál a kliens által megnyitott porthoz. Ez a csatorna lesz az adatcsatorna. Az adatcsatorna ilyen felépítését **aktív**, vagy **normál üzemmódnak** nevezik.
2. A másik technika, amikor a parancscsatorna fölépülése után a kliens nem küld portszámot a szervernek, hanem jelzi, hogy **passzív üzemmódban** kíván dolgozni. Ilyenkor a szerver vár (passzív), **az adatcsatorna fölépítését pedig a kliens fogja kezdeményezni**. Egy a kapcsolat idejére lefoglalt portról, a szerver 21-es portjára kapcsolódik, fölépítve ezzel az adatcsatornát.

Mivel a tűzfal beállítások általában erősen korlátozzák a bejövő kapcsolatokat, az aktív FTP üzemmód valószínűleg nem fog működni, ha tűzfallal védett hálózatból, a hálózaton kívüli FTP szerverrel próbálunk kapcsolatot létesíteni. Ilyen esetben kliensüket passzív üzemmódra kell állítani.

9.5 AZ FTP HASZNÁLATÁNAK FELTÉTELEI:

- Fájlok FTP szolgáltatással történő átviteléhez természetesen szükség van a kliens és szerver összeköttetését biztosító hálózati kapcsolatra
- A lokális gépen telepített FTP kliensnek kell lennie, amellyel a távoli gép FTP szerveréhez kapcsolódhatunk,
- A távoli gépen, amelyről fájlokat akarunk átvinni, FTP szervernek kell futnia.
- Az FTP szervert futtató gépen érvényes hozzáférési jogra, azaz accountra van szükségünk, amit a távoli gép rendszergazdájától kell igényelnünk.

9.6 JOGOSULTSÁGOK

Az FTP szerver által elérhető adatok természetesen nem minden esetben publikusak, azaz nem mindenki által hozzáférhetőek. A legtöbb FTP szerverre csak meglévő hozzáférési jogosultság birtokában jelentkezhetünk be. Accountot a Telnethez hasonlóan a távoli rendszer adminisztrátorától kaphatunk.

Az FTP kiszolgálók egy részét úgy állítják be, hogy olyan felhasználók bejelentkezését is elfogadják, akik nincsenek regisztrálva a szerveren. Az ilyen FTP kiszolgálókat anonymous FTP szervereknek nevezzük.

Az anonymous (névtelen) bejelentkezést támogató szerverek is kérnek felhasználói nevet. Ilyenkor egészen egyszerűen az anonymous nevet kell megadnunk. Jelszóként egy e-mail címet kell begépelni, de a legtöbb szerver bármilyen szöveget elfogad, amiben @ jel van. Az anonymous bejelentkezést követően egy az FTP szerver által kezelt könyvtár lesz az aktuális könyvtár, amit a távoli gép gyökérkönyvtárának látunk. Ebben a könyvtárban – korlátozott jogokkal rendelkezünk – nem írhatjuk a könyvtár tartalmát, de az ott tárolt fájlokat átmásolhatjuk saját gépünkre.

9.7 FTP KLIENSEK

FTP kliensek dolgában igen nagy a választék, lehetőség van karakteres és grafikus felületű kliensek beszerzésére, használatára. A karakteres felületű kliensek használata egy kicsit nagyobb odafigyelést igényel, de kezelésük elsajátítása után egy grafikus felület alkalmazása már gyermekjáték. Szintén a karakteres FTP ügyfélprogramok használata mellett szól, hogy ilyen alkalmazás szinte biztosan van a számítógépünkön.

A Windows operációsrendszerek tartozéka egy karakteres felületű kliens, így nem kétséges, hogy könyvünkben ismertetni fogjuk ezt a mindenki számára hozzáférhető programot. Emellett azonban bemutatjuk az egyik széles körben használt fájlkezelő program, a Total Commander FTP funkcióit is.

9.8 MUNKA KARAKTERES FPT KLIENSSEL

Egy FTP klienssel végzett munka általában a következő lépésekre bontható:

- A kliens indítása.
- Kapcsolat felvétele a szerverrel (bejelentkezés).
- Kapcsolat paramétereinek beállítása.
- Távoli és lokális könyvtárak kijelölése.

- Fájlok átvitele.
- A kapcsolat lebontása.
- A kliens bezárása.

A munka zömét az FTP kliens készenléti jelénél (prompt) begépelt parancsok segítségével végezzük el. A parancsok leírásánál

- a félkövér betűk pontosan begépelendő szavakat,
- a dőlt betűk értelemszerűen helyettesítendő szöveget,
- a szögletes zárójelek opcionálisan használható, nem kötelező paramétereket,
- a függőleges vonalak két elem közötti választási kényszert jelentenek.

Az útvonalak megadásában a UNIX/Linux operációs rendszerek esetén per (/), Windows esetén vissza per (\) jel választja el a könyvtárakat, és jelöli a főkönyvtárt.

A felhasználó saját, home könyvtárának jelölése a tilde (~) jellel történik.

Windows operációs rendszer esetén hivatkozhatunk meghajtókra, UNIX/Linux operációs rendszerben minden háttértárat egyetlen könyvtárszerkezet részeként látunk.

A karakteres felületű kliens használata közben tapasztalhatjuk, hogy minden végrehajtott parancsról egy számkóddal ellátott értesítést kapunk. Ha ezt ki szeretnénk kapcsolni gépeljük be a **verbose** (szószátyár) parancsot!

9.8.1 A kliens indítása, bezárása

A Windows terminál emulátorához hasonlóan, az FTP kliens ikonja sem szerepel a START MENÜBEN, ezért indításához célszerű a parancssori ablakot nyitnunk, majd begépelnünk az **ftp** parancsot.

A parancs hatására megjelenik a kliens készenléti jele (>). Az itt begépelt parancsot az ENTER billentyű lenyomásával küldhetjük el a szervernek. A szerver, a helyesen megadott, végrehajtható parancsokat elvégzi, egyébként pedig hibaüzenetet küld.

Az elindított klienst bezárhatjuk a **quit** paranccsal, vagy egész egyszerűen a program ablakának bezárásával.

9.8.2 Kapcsolat kialakítása, bejelentkezés

A kliens indítása még nem jelenti azt, hogy kapcsolódunk is valamilyen FTP szerverhez. A szerverrel való kapcsolatfelvétel az **open** paranccsal kezdeményezhető.

open [*gépcím***]**

A gépcím helyére a szervert futtató gép domain nevét, vagy IP címét kell begépelni. A gépnév elhagyása esetén a kliens a következő sorban rákérdez a címre.

open prometeus.ektf.hu

Ha a megadott szerver elérhető, akkor a kapcsolat felépül, ellenkező esetben hibaüzenet kapunk. Ha a kliens és a szerver közötti kapcsolatfelvétel sikeres, a kliens kérésre megadott felhasználói névvel és jelszóval azonnal be is jelentkezhetünk a távoli számítógépre.

Sikeres bejelentkezés estén (és ha a verbose mód nincs kikapcsolva) megjelenik a szerver üzenete

User *felhasználó* **loged in**
Ha a felhasználói név, vagy a jelszó hibás, a

Login incorrect
üzenetet kapjuk. Ebben az esetben a kliens és szerver között már van kapcsolat, csak a bejelentkezést kell megismételni. Erre a célra használható a **user** parancs.

user [*felhasználói_név***]**
Ha felhasználói nevet nem adjuk meg, akkor a szerver az **open** parancshoz hasonlóan megkérdezi azt.

A bejelentkezés sikere esetén a belépett felhasználó általában saját home könyvtárát látja aktuális könyvtárként.

9.8.3 Az átviteli mód beállítása

Az FTP szolgáltatás egymástól egészen eltérő operációs rendszerek közötti fájlátvitelt tesz lehetővé, ami általában nem is okoz problémát, hiszen az operációsrendszerek 8 bites bájtok formátumban tárolják a fájlok döntő többségét. A szövegfájlok azonban ebben a tekintetben kivételnek számítanak. Vannak olyan rendszerek, amelyek a szöveges állományok kezelését 7 bites ASCII kódolásnak megfelelő bájtok formájában végzik. Más rendszerek azonban a szövegeket is 8 bitenként tárolják. Ha a szerver és a kliens operációsrendszere eltérően kezeli a szövegeket, akkor az egyik rendszerről a másikra másolt szövegfájl olvashatatlan lesz. Ilyen esetben átvitel közben a kliensnek konvertálnia kell a bájtokat a fogadó operációsrendszer által használt szövegkódolásnak megfelelően. Éppen ezért, mielőtt FTP-vel átmásolunk egy fájlt, meg kell adni, hogy azt szövegként, vagy egyéb, úgynevezett bináris állományként kell-e kezelni. A **bin** paranccsal bináris, az **asc** paranccsal pedig szöveges átvitelt állíthatunk be.

Felvetődhet persze a kérdés, honnan tudjuk egy állományról, hogy binárisként, vagy szövegként kell-e lemásolnunk. A stratégia a következő lehet. Ha nem vagyunk biztosak a használandó átviteli módban, akkor egy fájl másolásakor mindig használjunk **bináris** átvitelt. Ha a letöltött állomány szöveges állomány, de letöltés után nem olvasható, vagy olvasható ugyan, de az egyébként igen hosszú szöveg egyetlen sorban jelenik meg, akkor ismételjük meg a letöltést szöveges átviteli móddal.

9.8.4 Könyvtár tartalomjegyzékének megtekintése

Az FTP szolgáltatást használva, távoli, és a lokális gép éppen kiválasztott, aktuális könyvtára között tudunk fájlokat másolni. Ha nem, tudjuk pontosan, hogy melyek az aktuális könyvtárak, a **pwd** illetve az **lcd** parancsok lehetnek segítségünkre. A **pwd** parancscsal írathatjuk ki a távoli, az **lcd** paranccsal pedig a helyi gép aktuális könyvtárának útvonalát. Az aktuális könyvtár kiválasztását más paranccsal végezzük a távoli és más paranccsal a helyi gépen.

Könyvtár kiválasztására a szerveren a **cd** parancsot alkalmazható.

cd *útvonal*

Ahol az útvonal helyén az FTP szervert futtató gép fájlrendszerének egy könyvtárának útvonalát adjuk meg.

A **cd /** parancs például a távoli gép gyökérkönyvtárát teszi aktuálissá.

A helyi gép könyvtárai közötti mozgást az **lcd [***meghajtó***][***útvonal***]** formában megadott paranccsal végezhetjük.Az elhagyható *meghajtó* paraméter egy megható azonosítója (A: B: C: …) lehet. Az *útvonal* egy a lokális gép könyvtárszerkezetében lévő valamelyik könyvtár útvonala. Az **lcd f:** parancs például az **f:** meghajtó gyökérkönyvtárát teszi aktuálissá.

A távoli gép könyvtárnak kiválasztása után, – hacsak nem ismerjük maradéktalanul –, célszerű kilistázni a tartalomjegyzéket. Erre az **ls**, vagy a **dir** parancsot használhatjuk.

9.8.5 Fájlok átvitele

A bejelentkezés, az átviteli mód beállítás és a könyvtárak kiválasztása után kezdődhet a fájlok le- vagy feltöltése. Mindkét esetben két parancs közül választhatunk aszerint, hogy csak egy, vagy esetleg egyszerre több állományt szeretnénk másolni.

Egyetlen fájlt akarunk letöltéséhez a **get [***fájlnév***]** parancsot kell használnunk, amelyben a fájlnév helyére egy, a távoli gépen éppen aktuális könyvtárban lévő fájl nevét írhatjuk be. A fájlnevet pontosan a kis- és nagybetűk megkülönböztetésével kell begépelni.

A **get level.doc** parancs például a szerver aktuális könyvtárából letölti a **level.doc** nevű állományt a helyi gép aktuális könyvtárába.

Ha egyszerre több fájlt akarunk letölteni, akkor a **get** helyett az **mget [***fájl1***] [***fájl2***] […]** parancsot kell használni. Az **mget** után, egymástól szóközzel elválasztva több fájl neve is megadható, sőt a fájlnevekben helyettesítő karaktereket (* ?) is használhatunk.

Az **mget *.doc** parancs az összes **doc** kiterjesztésű állományt letölti.

Az **mget** használata során a szerver minden állomány továbbítása előtt kiírja annak nevét, majd megkérdezi, hogy valóban le akarjuk-e tölteni azt. A válasz megadása az **Y** illetve az **N** betű lenyomásával lehetséges.

Az állományok FTP szerverre való feltöltésével kapcsolatban tudnunk kell, hogy ezt csak akkor tehetjük meg, ha a távoli gép kiválasztott könyvtárában írási jogunk van. Anonymous FTP esetén szinte teljesen biztos, hogy a szerver rendszeradminisztrátora ezt nem teszi lehetővé.

A fájlok feltöltése nagyon hasonlít a letöltéshez, de ebben az esetben a **put** és az **mput** parancsokat használhatjuk. Szintaktikájuk megegyezik a letöltés parancsaival.

put [*fájlnév***]**
mput [*fájl1***] [***fájl2***] […]**

9.8.6 Néhány egyéb hasznos parancs

A parancssori ftp kliensen még jó néhány egyéb parancs végrehatására is alkalmasak. Az alábbi távlázat ezek közül tartalmaz néhányat.

Parancs	Leírás
help [*parancs*]	Önmagában alkalmazva megjeleníti a használható parancsok listáját. Egy parancs nevével együtt begépelve rövid leírást kapunk a parancs használatáról.
prompt	Ki-, illetve bekapcsolja a másolást megerősítő kérdéseket.
hash	Hosszabb másolás esetén minden másolt 2 KB esetén egy hash (#) jelet ír a képernyőre, így a másolás folyamata nyomon követhető.
bell	Ki illetve bekapcsolja a parancsok utáni hangjelzést.
status	Kilistázza az FTP kliens pillanatnyi beállításait.

9.8.7 A kapcsolat bontása

Ha befejeztük egy FTP szerverrel a munkát, akkor illik szabályosan bontani a kapcsolatot. Erre az **close** parancs használható.

A **close** alkalmazása csak a szerverrel való kapcsolatot szünteti meg, az FTP klienst nem zárja be. Ha a klienst is be akarjuk zárni, használjuk a **bye**, vagy a **quit** parancsok valamelyikét. Ezek a parancsok a szerverrel való kapcsolatot is elbontják, de a kliens ablakát is bezárják.

9.9 A BIZTONSÁGOS FTP

A Telnettel kapcsolatban már érintettük a hálózati adatátvitel biztonság kérdéseit. Láttuk, hogy a Telnek háttérbeszorulásának egyik oka, éppen a biztonság hiánya, az adatok kódolatlan csatornán történő továbbítása. Az FTP-ről sajnos ugyanez mondható el. A szerver és kliens között áramló parancsok és az adatok mindenféle titkosítás nélkül kerülnek továbbításra. Bár az FTP szolgáltatás ennek ellenére igen népszerű a felhasználók körében, a fejlesztők nagy hangsúlyt fektetnek a biztonságos fájlátvitelt megvalósító eszközök kialakítására. Számos megoldás között például érdemes megemlíteni az SSH szolgáltatást. Ha a gépünkre telepítjük az SSH szolgáltatás szoftvereit, akkor az SSH kliens mellett, egy **psftp** nevű kliens is, amely az SSH szerverhez kapcsolódva biztonságos, kódolt csatornán keresztül képes az FTP kapcsolat lebonyolítására.

A kliens indítása után gyakorlatilag ugyan azokat a parancsokat használhatjuk, mint a parancssori FTP kliensben. A parancsok pontos listáját megtekinthetjük a **help** prancs begépelésével.

A **psftp** valójában az SSH tunneling lehetőségét használja, az FTP kapcsolat titkosított csatornán történő lebonyolítására.

Használatához az eddig megismert feltételek mellett a lokális gépen a **psftp** kliensre, SSH ügyfélre, a szerver oldalon pedig SSH szerverre, és FTP szerverre van szükség.

9.10 GRAFIKUS FELÜLETŰ FTP ÜGYFELEK

A felhasználók jelentős része kedveli a parancssorral irányítható, karakteres felületű alkalmazásokat, mert azok kiválóan alkalmasak az egyes műveletekhez tartozó opciók tömör megadására. Rendszergazdák, és informatikus beállítottságú felhasználók számára áttekinthetőbbé teszik vezérlést, és lerövidítik az arra fordított időt.

Ha azonban egy szolgáltatás kizárólag parancssori vezérlést tesz lehetővé, az a felhasználók túlnyomó többségét távol tartja az alkalmazástól. Az FTP minden bizonnyal a grafikus kliensek kifejlesztésének köszönheti fennmaradását. Számos grafikus FTP ügyfélprogram létezik, de találkozunk olyan fájlkezelő alkalmazásokkal, amelyek a helyi gép háttértárainak kezelés mellett alkalmasak FTP kapcsolat kiépítésére is. Azaz beépített FTP klienssel rendelkeznek.

Ilyen, beépített FTP klienst tartalmazó fájlkezelő a méltán népszerű Total Commander, amellyel egy távoli gép FTP szerverhez kapcsolódva majdnem úgy kezelhetjük annak könyvtárait és fájljait, mintha a lokális gépen lennének. A TC képes az FTP kapcsolat egészen precíz beállítására, de ilyenkor számos paramétert kell beállítanunk. Tananyagunkban a Total Commander 7.50 verziójának alkalmazásával a legegyszerűbb módszert mutatjuk be.

9.10.1 Kapcsolódás az FTP szerverhez

A Total Commander indítása után a **Hálózat/Új FTP kapcsolat…** paranccsal (**Ctrl+N**) jeleníthetjük meg az **ftp** párbeszédablakot, amelynek **Kapcsolódás** kombi mezőjébe az FTP szerver címét kell beírnunk. Ha saját accounttal rendelkezünk a szerveren, töröljük a **Névtelen kapcsolódás** opciót, különben a kliens **anonymous** felhasználói névvel próbál bejelentkezni. Az OK gombbal továbblépve a TC ftp kliense kapcsolódik a szerverhez, és két egymást követő párbeszédablakban beolvassa a felhasználó nevünket és jelszavunkat.

9.10.2 Fájlok átvitele

Ha mindent helyesen adtunk meg, a kapcsolat fölépül, és bejelentkezünk a szerverre. Ilyenkor az aktív panelben a távoli gép aktuális könyvtárnak tartalomjegyzéke jelenik meg, a másik panel pedig a helyi gép valamelyik könyvtárát mutatja. A TC szokásos eszközeivel mindkét gépen megváltoztathatjuk az aktuális könyvtárt, majd az egyik panelen kijelölt (jobb gombos kattintás, vagy **Insert** billentyű) fájlokat, a másik panelre másolhatjuk a Másolás gombbal, vagy az **F5** billentyűvel. Írási jog birtokában a parancssori FTP kliensekhez hasonlóan, a TC-rel is lehet fájlokat feltölteni, illetve törölni (**F8**) a szerveren, de könyvtárakat létrehozására (**F7**) és, törlésére (**F8**) is van mód.

9.10.3 Kapcsolat bontása

A fájlok mozgatását követően az eszköztár alatti **Szétkapcsolás** gombbal bonthatjuk a kliens és szerve közötti kapcsolatot. A legközelebbi kapcsolódáskor, az **ftp** párbeszédablak, **Kapcsolódás** kombi mezőjének listájából kiválaszthatjuk a korábban használt FTP szerverek nevét.

9.11 ÖSSZEFOGLALÁS

Az FTP (File Transfer Protocol) az egyik legrégebbi szolgáltatás, amely hálózatra kapcsolt gépek közötti fájlátvitelt tesz lehetővé. A szolgáltatás neve azonos a kliens és szerver kommunikációját szabványosító protokoll nevével. A két szoftverkomponens közötti kapcsolat eltér a szokványostól, amennyiben kiszolgáló és ügyfél között a parancsok és az adatok továbbítására két, külön kommunikációs csatorna alakul ki. Az első, parancsok átvitelére alkalmas csatornát mindig a kliens nyitja meg, a szerver 20-as TCP portjához kapcsolódva. Az adatcsatorna megnyitását aktív FTP esetén a szerver, passzív FTP esetén a kliens kezdeményezi. A szerver mindkét esetben a 21-es TCP porton kapcsolódik az adat csatornához.

A szolgáltatás használata során alkalmazhatunk karakteres és grafikus felületű FTP ügyfélprogramokat is. A karakteres kliensek mellett szól, hogy minden internethez kapcsolható gépen megtalálhatók, így külön telepítésükre nincsen szükség. Karakteres klienst használva parancsok (**open, close, bye, pwd, cd, lcd, ls, dir, get, mget, put, mput, help...**) begépelésével irányíthatjuk a kommunikációt. A grafikus felületű kliensek valójában csak eltakarják előlünk a kiszolgáló, és az ügyfél közötti karakteres parancsokkal és numerikus válaszkódokkal történő párbeszédet. Számos más alkalmazás mellett a Total Commander is alkalmas FTP kapcsolat grafikus felületen történő lebonyolítására.

Az FTP szolgáltatás titkosítás nélküli csatornákat használ az adatok és parancsok továbbítására. Titkosított FTP-t valósíthatunk meg az SSH szolgáltatás kiegészítéseként rendelkezésre álló, **psftp** karakteres klienssel, amely az SSH szolgáltatás tunneling lehetőségét használva bonyolítja le a kapcsolatot.

9.12 ÖNELLENŐRZŐ KÉRDÉSEK

1. Mit jelent az FTP rövidítés?
2. Sorolja fel az FTP szolgáltatás használatához szükséges feltételeket!
3. Milyen lépésekben végezheti el egy fájl letöltését?
4. Mit ért anonymous ftp alatt?
5. Melyik parancs szolgál a távoli, és melyik a helyi gép aktuális könyvtárának beállítására?
6. Mi a különbség a **get** és az **mget** parancs között?
7. Hogyan kérhet segítséget a parancsokkal kapcsolatban?
8. Hogyan tölthet fel fájlokat a szerverre?
9. Mire szolgál a **asc** és a **bin** parancs?
10. Tűzfal mögötti hálózatból, külső hálózatban elhelyezkedő szerverrel próbál FTP-zni. A kapcsolat felépítését követően a kommunikáció leáll. Mi lehet az ok?
11. Hogyan titkosíthatja az FTP csatornák kommunikációját?

10. AZ ELEKTRONIKUS LEVELEZÉS

10.1 CÉLKITŰZÉS

Az elektronikus levelezés az egyike azoknak a szolgáltatásoknak, amelyekkel szinte minden internet használó naponta dolgozik.

Az e-mail szolgáltatás annyiban hasonlít a hagyományos postai levelezéshez, hogy szöveges dokumentumok aszinkron továbbítását teszi lehetővé. Kiemelkedő népszerűsége a hagyományos levelezéshez mérten szinte hihetetlen sebességének, az elektronikus környezetben történő munkavégzés általánossá válásával, és aszinkron mivoltának köszönhető.

Ebben a leckében bemutatjuk az e-mail szolgáltatás működését. Megtanulhatja, mit jelent pontosan, és hogyan valósul meg az elektronikus levelezésben, az aszinkron üzenettovábbítás. Megismerheti a levelező kliensek, és levelező szerverek funkcióit, betekintést nyerhet az elektronikus levelezés biztonsági problémáiba.

10.2 A LECKE TÉMAKÖREI

- Az elektronikus levelezés lehetőségei
- Az elektronikus levelezés címzési rendszere
- Az elektronikus levelezés működése
- Az elektronikus levelezés használatának feltételei
- Az elektronikus levelek felépítése
- Levélküldés idegen hálózatból
- Levelező kliensek szolgáltatásai
- A levelezés biztonsági kérdései

10.3 AZ ELEKTRONIKUS LEVELEZÉS LEHETŐSÉGEI

Az elektronikus levelezés, az e-mail egyike azoknak a szolgáltatásoknak, amelyek nagyban hozzájárultak az Internet széleskörű elterjedéséhez. A felhasználók hamar felismerték, hogy ez lehetőség forradalmasítja az emberi kommunikációt. Az e-mail lényege, hogy az Internetre kapcsolt számítógépek felhasználói hálózat segítségével szöveges üzeneteket tudnak küldeni egymásnak. Népszerűségét elsősorban annak köszönheti, hogy az elektronikus levelek, szemben a hagyományos postával rendkívül nagy sebességgel jutnak el a címzetthez.

Számos további előnyének hosszas felsorolása helyett álljon itt a következő rövid lista.

- Az e-mail továbbítása fillérekbe kerül.
- A levelet nem kell borítékba rakni, a borítékot felbélyegezni, postaládába dobni.
- A telefonos kapcsolattartással szemben a levél megírásának és elküldésének pillanatában a címzettnek nem kell számítógépe mellett ülnie. Levelező programjának legközelebbi elindításakor szinte biztosan megkapja a küldeményt.
- Az e-mail küldése és a beérkezett levelek elolvasása nem helyhez kötött. Bármelyik Internethez csatlakozó gépről lehet levelet írni, vagy olvasni.

- Munkahelyünkön gyakran egész nap működik a levelező programunk. Ilyenkor a levelek folyamatosan beérkeznek számítógépünkre, de nekünk csak akkor kell őket elolvasni, amikor azt időnk megengedi.
- Könnyen készíthetünk körleveleket, amelyeket egyszerre továbbíthatunk az összes érdekeltnek.
- Bár az e-mail csupán szöveges üzenet, a levelekhez csatolva tetszőleges típusú fájlokat továbbíthatunk a címzettnek.

10.4 AZ ELEKTRONIKUS LEVELEZÉS CÍMEZÉSI RENDSZERE

Az elektronikus levelezés egyik fontos jellemzője, egyben vonzó tulajdonsága az **aszinkron kommunikáció**. Ez valójában azt jelenti, hogy a feladó nem közvetlenül a címzettnek küldi egy a levelet, hanem egy olyan levelező kiszolgálónak juttatja el, amelyhez a címzett hozzáféréssel rendelkezik. A beérkezett levelet a kiszolgáló mindaddig tárolja a címzett elektronikus postaládájában, míg az el nem olvassa, illetve nem törli a küldeményt.

Az elektronikus leveleket tehát egy szerver valamelyik felhasználójának küldjük. A felhasználónak elektronikus postaládával, mailbox-szal kell rendelkeznie a szerveren. (A mailbox általában egy könyvtár, amelyhez a szerver más felhasználói nem férnek hozzá.) A postaláda neve gyakran megegyezik a címzett felhasználói nevével[12].

A fentiekből adódódik az elektronikus levelek címzési rendszere. Egy e-mail címnek tartalmaznia kell a címzett mailboxát tároló számítógép címét, és a címzett mailboxának nevét is. Az e-mail cím tehát két részből áll:

- Az elektronikus postaláda nevéből, és
- a postaládát tároló számítógép címéből.

A címet *mailbox@gépcím* formában kell leírni, ahol a gép azonosítója lehet IP cím, vagy domain név is: **gabor@mail.nospam.hu** v. **gabor@192.168.1.2**

Az e-mail címmel kapcsolatban tudnunk kell a következőket:

- a domain névhez hasonlóan az e-mail cím sem tartalmazhat szóközöket,
- az e-mail címben megkülönböztetjük a kis és nagybetűket, tehát a **gabor@ mail.nospam.hu** nem ugyan az, mint a **Gabor@ mail.nospam.hu**.
- gyakori az olyan felhasználói név is, amelyben pont (.) található. Ez nem számít hibának: **varga.gabor@ mail.nospam.hu.**

10.5 AZ ELEKTRONIKUS LEVELEZÉS MŰKÖDÉSE

Az e-mail szolgáltatás működéséhez a korábbiakhoz hasonlóan kliens, azaz ügyfélprogramra, és szerver, kiszolgáló programokra van szükség. Azt azonban rövidesen látni fogjuk, hogy a levelezéshez két különböző szerverre is szükség van.

Az e-mail szolgáltatás kliensét egyszerűen **levelezőprogramnak** hívjuk. A levelezőprogrammal írjuk meg és küldjük el kimenő leveinket, de a klienssel kezeljük a beérkezett maileket is.

[12] A levelező szerverek képesek kezelni az úgynevezett virtuális felhasználókat. A virtuális felhasználó valójában egy valódi felhasználó alternatív neve, ami e-mail címben szerepeltethető. Ilyen például a **varga.gabor@ mail.nospam.hu** címben a **varga.gabor**, ami a **gabor** nevű valódi user virtuális neve lehet.

Levélküldéskor, a megírt, és megcímzett levelet a feladó nem közvetlenül a címzettnek, de még csak nem is a címzett mailboxát kezelő szervernek küldi el. A lokális hálózatok túlnyomó többségében üzemeltetnek levelek továbbítására alkalmas, úgynevezett **SMPT** (Simple Mail Transfer Protocol) szervert. Az SMTP szerverek egymás közötti levéltovábbításra képesek.

Amikor megírtunk egy levelet, levelező kliensünk segítségével átadjuk azt az általában saját hálózatunkban lévő SMTP szervernek. A szerver és a levelező kliens kapcsolata ezután meg is szakad, mert az „átvétel" után a szerver gondolkodik a levél továbbításáról. Elküldi azt a címben található gép SMTP szerverének, az pedig (szintén az email cím alapján) elhelyezi a küldeményt a címzett mailboxában.

A levél mindaddig a maiboxban marad, amíg a címzett saját levelező kliensével le nem tölti azt[13].

Az SMTP szerverek csak a levelek továbbítását végzik, nem képesek a maiboxokban tárolt levelek elolvasásának, és letöltésének biztosítására. Amikor egy felhasználó a postafiókjába érkezett levelekhez szeretne hozzáférni, levelező kliensével, a mailboxát tároló gép, letöltést biztosító szerveréhez kell kapcsolódnia. Többféle letöltést támogató szerver létezik, de egyelőre az úgynevezett POP3 (3-as változatú Post Office Protocol) szerverek a legelterjedtebbek.

A letöltő szerverhez felhasználói név, és jelszó megadása után lehet kapcsolódni. Ez biztosítja azt, hogy minden felhasználó csak saját postafiókjának tartalmát tudja letölteni.

A fentieket összefoglalva tehát a levelek lokális gépen történő kezelése a levelező kliensek feladata, a levelek továbbítását az SMPTP szerverek biztosítják, az elektronikus postaládában tárolódó küldemények lokális gépre történő letöltését pedig (általában) a POP3 szerverek teszik lehetővé.

Ahhoz, hogy küldeni és fogadni is tudjunk leveleket, levelező kliensünknek SMTP és POP3 szerverhez is kell kapcsolódnia. A mai levelező szerverek általában egyszerre biztosítják mindkét funkciót, ezért leveleink küldésére és fogadására a hálózatunkban lévő egyazon számítógépet használjuk.

A későbbiekben jelentőséget kap, ezért érdemes már most megjegyezni, hogy az SMTP szerverek alapbeállítás szerint nem kérnek felhasználói azonosítást, azaz bárki számára lehetővé teszik az elektronikus levelek elküldését. A POP3 szerverek mindenképpen kérnek autentikációt, így azok funkcióit csak a regisztrált felhasználók használhatják.

Szintén érdemes megemlíteni, hogy előállhat olyan eset, amikor az elküldött, SMTP szervernek átadott levél valamilyen oknál fogva nem kézbesíthető. Ezt okozhatja a címzett mailboxát kezelő gép működési zavara, de az e-mail cím hibás megadása, és számos egyéb körülmény is (például az, hogy a címzett postaládája megtelt). Amikor egy SMPTP szerver nem képes a címzett géphez eljuttatni a levelet, akkor azt visszateszi a feladó elektronikus postaládájába (a feladó címét a levélben tárolódó válaszcím alapján állapítja meg). Az SMTP szerverek által kézbesíthetetlenség miatt visszaküldött leveleket **visszapattanó levélnek** nevezzük.

[13] Ha a levelek megtekintéséhez IMAP protokollt használunk, a levelek mindig a szerveren maradnak.

10.6 AZ ELEKTRONIKUS LEVELEZÉS FELTÉTELEI

Az elektronikus levelezés szolgáltatás használatához az alábbi feltételek szükségesek:

- **Levelező kliens:** Rendelkeznünk kell a levelek megírására, elküldésére, és helyi gépen történő kezelésére alkalmas levelező klienssel. Itt kell megemlítenünk, hogy webes levelezés esetén a levelező program szerepét távoli gépen futó, web felületen elérhető programok vehetik át. Ebben az esetben saját gépünkre nem kell levelező programot telepítenünk.
- **SMTP szerver:** A levelező kliensünket futtató gépnek olyan hálózathoz kell kapcsolódnia, amelyben működik SMTP szerver.
- **Account:** Regisztrált felhasználónak kell lennünk egy elektronikus postafiókokat kezelő gépen.
- **Hálózati kapcsolat:** A levelező kliensünknek kapcsolódnia kell mailboxunkat tároló gép, postaládákat kezelő szerveréhez. Mint említettük, a mailboxok kezelését nem csak POP3 szerverek biztosíthatják. Hasonló funkciókat látnak el az úgynevezett IMAP4 (Internet Message Access Protocol) szerverek is, amelyek a levelek letöltése nélkül teremtenek lehetőséget azok olvasására és rendezésére.
- **Konfiguráció:** A levelező kliens beállításakor pontosan meg kell adnunk a levélküldéshez használt SMTP szervert, és a letöltéshez használt POP3 szervet futtató gép címét, valamint a kapcsolódás néhány paraméterét, például a felhasználói nevet.

10.7 AZ ELEKTRONIKUS LEVÉL FELÉPÍTÉSE

Az elektronikus levelezés megértéséhez ismernünk kell az e-mail szolgáltatással továbbított dokumentumok, az elektronikus levelek fölépítését.

Az elektronikus levél két részből tevődik össze. Az egyik a levél fejrésze (head), a másik pedig az úgynevezett levéltest (body). A fejben alapvetően a címzéssel, és a levél kezelésével kapcsolatos adatok tárolódnak, a testben pedig a levél szövege, és az esetleges csatolt állományok adatai találhatók.

A fej és a test egyes adatait, a levél megírásakor, a levelező kliens felületén, maga a felhasználó adja meg. Más, elsősorban adatokat a levelezőprogram automatikusan helyez el a levélben.

A levél fejrészében az alábbi általában az alábbi mezők szerepelnek:

- Címzett (To) A levél címzettjeinek e-mail címei.
- Feladó (From) A feladó email címe.
- Dátum (Date): Az üzenet elküldésének dátuma, és időpontja.
- Másolat (Cc): Azon felhasználók e-mail címe, akik másolatot kapnak a levélről.
- Titkos másolat (Bcc): Ezek a címzettek szintén másolatot kapnak a levélről, de címük az elküldött levelekben nem fog szerepelni.
- Tárgy (Subject): Rövid utalás a levél tartalmára. A levél címzettje először a feladót és tárgyat fogja majd látni. A tárgy üresen hagyása illetlenségnek számít.
- Válaszcím (Reply-To): Az az e-mail cím, ahová a feladó a választ várja.

Az elektronikus levelezést eredetileg kizárólag szövegtovábbításra tervezték. Így a levéltest eredetileg kizárólag karakterkódokat tartalmazott. Bár az üzenetek alapvetően továbbra is karakterekből épülnek fel, a levelekhez gyakran csatolunk bináris mellékleteket, képeket, hangállományokat, programfájlokat. Ezt az úgynevezett MIME (Multipurpose Internet Mail Extensions) formátum kialakítása tette lehetővé. A MIME valójában egy kódolási és dekódolási szabvány, amely lehetővé teszi, hogy az elektronikus levelekbe a szöveges szakaszok mellett a legkülönbözőbb típusú fájlok legyenek beágyazhatók. A MIME formátumú levél levélteste több szakaszból állhat, amelyek egy-egy MIME fejléccel kezdődnek. A fejléc leírja az őt követő adattok jellemzőit, és meghatározza az adatok típusát.

Amikor egy levelező program MIME formátumú levelet értelmez, a levél testben lévő MIME fejlécek alapján képes eldönteni, hogy az egyes levélszakaszok szöveget, képet, hangot, videót, valamilyen alkalmazást, vagy milyen egyéb adatot tartalmaznak. Az egyes szakaszok a felhasználó előtt megfelelő formában jelennek meg, illetve formátumuknak megfelelően lehet őket kezelni.

10.8 ELEKTRONIKUS LEVELEZÉS KÜLÖNBÖZŐ HÁLÓZATOKBÓL

A hálózati szolgáltatások fejlődésre általában erős hatást gyakorolnak a szolgáltatás népszerűvé válását kísérő biztonsági problémák. Az elektronikus levelezésre talán a spamek gyakorolták a legerősebb hatást. A spam nagy tömegben terjesztett, kéretlen levél, amely általában valamilyen terméket reklámoz. Mint tudjuk a reklám hatalmas üzlet, így a spamküldés nem egyszerű hóbort, hanem hatalmas, ugyanakkor tisztességtelen üzlet. A spamek még a napjainkra elterjedt óvintézkedések ellenére is gyakran elárasztják a felhasználókat.

Mivel a levélszemetelők kezdetben állandó címekről küldték el leveleiket, a spamek eredete behatárolható volt. A spamek feladóiról adatbázisokat kezdetek vezetni, és a hálózatokat védő tűzfalakat, SMTP szervereket úgy állították be, hogy ne továbbítsák a feketelistán lévő címekről származó leveleket. Később azonban ez is kevésnek bizonyult, mert spam küldők egyre gyakrabban váltogatták e-mail címüket, sőt különböző szervezetek hálózatán működő SMTP szervereket használtak leveleik továbbítására.

A korábbiakban már említettük, hogy az SMTP szerverek kezdetben semmiféle autentikációt nem kértek. Ha egy kliens átadott egy levelet az SMTP szervernek, akkor az gondolkodás nélkül továbbította az üzenetet a címzettnek. Bárki megtehette, hogy levelezőprogramjában egy tetszőleges hálózaton működő gépet SMTP szerveren keresztül spameket küldött. A szervereket üzemeltető rendszergazdáknak megvolt a válaszuk. Egyre általánosabbá vált, hogy az SMTP szervereket úgy konfigurálták, hogy csak saját hálózatukban lévő gépekről érkező leveleket legyenek hajlandók továbbítani. Ez ugyan megtörte spam küldés lendületét, de megnehezítette a becsületes felhasználók munkáját is.

Gondoljunk csak bele a következő helyzetbe:

Gábor a NOSPAM nevű cégnél dolgozik, amely néhány tucat gépből álló hálózat mail.nospam.hu nevű gépén SMTP, és POP3 protokollokkal működő levelező szerver biztosítja a munkatársak elektronikus levelezését. Gábor gabor@mail.nospam.hu című mailboxa ezen a gépen van. Amikor Gábor bent van a munkahelyén, és levelet akar küldeni, akkor levelezőprogramjával a mail.nospam.hu SMTP szerverén keresztül küldi el a leveleket. A beérkező leveleket ugyanerről a gépről a POP3 szerverhez csatlakozva tudja letölte-

ni. Eddig minden rendben van, de vajon mi történik, ha Gábor otthonról is szeretné elolvasni a leveleket, sőt szükség esetén válaszolni is akar rájuk?

Barátunk úgy állítja be otthoni gépének levelező kliensét, hogy az SMTP szerverként és POP3 szerverként is **mail.nospam.hu**-t használja. Ez logikus is, hiszen ide kerülnek Gábor beérkezett levelei. Amikor neves felhasználónk leveleket próbál letölteni, levelző programja csatlakozik a **mail.nospam.hu** POP3 szerveréhez, felhasználói nevének és jelszavának megadásával igazolja magát. Ezt követően levelei letöltődnek otthoni gépére.

Miután Gábor elolvasta a kapott leveleket, az egyikre válaszol. A Küldés gombra kattintva azonban szomorúan kell tapasztalnia, hogy levéltovábbítás meghiúsul.

Képes ugyan letölteni a cég levelező szerverére érkezett leveleit, de nem tud levelet küldeni.

Lássuk mi történt! Gábor otthoni gépe valamelyik internet szolgáltató hálózatához kapcsolódik, azaz nem a NOSPAM hálózatában van. A NOSPAM rendszergazdája azonban, a spamküldést megakadályozandó úgy állította be az SMTP szervert, hogy az más hálózatok gépeiről érkező leveleket ne továbbítson.

Ha értjük a problémát, lássuk a megoldásokat!

10.8.1 Levél küldése a szolgáltató SMTP szerverével

Gáborunk bárkitől is vásárolja az internet hozzáférést, a szolgáltató szinte teljesen biztosan rendelkezésére bocsátja a saját hálózatán működő SMTP szervert. A spamerek áldozata beállíthatja úgy otthoni gépe levelezőprogramját, hogy az POP3 szerverként változatlanul az **mail.nospam.hu**-t használja. Így Gábor otthon is meg fogja kapni a céges e-mail címére érkező leveleket. A levélküldést azonban úgy állítja be, hogy az SMTP szerver szolgáltató szervere például a smtp.myisp.hu legyen. Így most már el is tudja küldeni a leveleket.

10.8.2 Levél küldése tunnelinggel

Ha Gábor barátunk kellő ambícióval rendelkezik, a NOSPAM hálózatában van SSH szerver, és a cég tűzfala be is engedi az SSH kapcsolatot, akkor a probléma szolgáltató SMTP szervere nélkül is megoldható.

Gábornak úgy kell beállítania SSH kliensét, hogy az, tunnelinget használva „elvegye" a helyi számítógép egy meghatározott portjára küldött üzeneteket, és azokat a cég SSH szerverén keresztül a **mail.nospam.hu** SMTP szerverének továbbítsa. Ezt követően a levelező programot is át kell állítani. SMTP szerverként a helyi gépet kell megadni az SMTP szerver által figyelt portként pedig SSH kliens által figyelt portot kell megadni.

El kell indítani az SSH klienst, be kell jelentkezni cég SSH szerverére, majd a levelező programmal el lehet kezdeni a levélküldést. A levelező program, a saját gépen futó egyik portra küldi a levelet. Az SSH kliens figyeli a portot, és az oda érkező levelet a NOSPAM hálózatán belül lévő SSH szervernek küldi. Az SSH szerver továbbítja a levelet a hálózaton belüli SMTP szervernek. Az SMTP szerver úgy érzékeli, hogy a hálózaton belülről érkezett a levél, így elküldi az a címben megjelölt rendeltetési helyre.

Ez a megoldás némileg bonyolultnak tűnik, de csak egyszer kell beállítani, és azt követően bármelyik hálózatban működik, amelyik „kiengedi" az SSH kapcsolatokat. Azaz Gábor barátunk nyugodtan utazgathat (tételezzük fel, hogy notebookja van), bárhol is csatla-

koztatja az internethez a számítógépét, mindenhonnan hozzájut letöltött leveleihez, és válaszolni is tud rájuk.

10.8.3 Jelszóval védett SMTP szerver

Mivel a felvázolt probléma nem egyedi, a fejlesztők és rendszergazdák is kerestek jól használható, rugalmas válaszokat. A mai SMTP szerverek beállíthatók úgy, hogy kérjenek autentikációt, azaz csak magukat név, és jelszó megadásával igazoló, regisztrált felhasználóktól érkező levelet legyenek hajlandók továbbítani. Ha egy hálózat rendszergazdája így állítja be az SMTP szervert, akkor nem kell tiltania az idegen hálózatokból érkező levelek továbbítását. A három közül természetesen ez a legjobb megoldás.

10.9 AZ ELEKTRONIKUS LEVELEZŐ KLIENSEK SZOLGÁLTATÁSAI

Miután áttekintettük az elektronikus levelezés fontosabb kérdéseit, lássuk milyen szolgáltatásokat várhatunk el egy levelező klienstől. A levelező klienseknek biztosítaniuk kell mindazokat a funkciókat, amelyekre a felhasználónak az elektronikus levelezés közben szüksége lehet.

10.9.1 Konfigurálhatóság

A levelezőprogramnak képesnek kell lennie a levelezéshez szükséges beállítások, paraméterek, adatok tárolására. Nem lenne szerencsés, ha minden levél elküldése előtt meg kellene adni az SMTP szerver címét, vagy újra és újra meg kellene adnunk a POP3 szervernek a felhasználói nevünket. Minden levelező program lehetővé teszi, hogy a felhasználó tárolhassa és tárolhassa a levezéshez szükséges alábbi beállításokat:

- A használt POP3 szerver címe és portszáma (alapértelmezett érték 110),
- az SMTP szerver címe, és portszáma (alapértelmezett érték 25),
- a felhasználó azonosítója (POP3, esetleg SMTP autentikációhoz),
- a felhasználó jelszava (POP3, esetleg SMTP autentikációhoz),
- a felhasználó neve, ami a címzetteknél a feladó neveként jelenik meg,
- a felhasználó válasz e-mail címe, ahová egy elküldött levélre válaszolni kell.

> Ha csak lehet, sosem tárolunk jelszót, mert az mindig komoly biztonsági kockázatot rejt!

Egyes levelezőprogramok többféle konfigurációs csomagot, úgynevezett fiókokat képesek létrehozni. Az ilyen levelezőkben a felhasználó maga választhatja ki, hogy épen melyik fiók beállításait akarja használni.

10.9.2 Levelek írása, elküldése, letöltése

A levelező programok mindegyike biztosítja a levéliráshoz szükséges felületet, lehetőséget teremt a levelek fejlécének és szövegének kitöltésére, a levelekben bináris tartalom elhelyezésére.

A letöltött leveleket képesek áttekinthető mappaszerkezetben tárolni, és különböző szempontok szerint rendezve megjeleníteni.

Biztosítják a letöltött levelek tartalmának megtekintését, képesek bináris mellékleteket állományként menteni.

Egyszerűvé teszik a levelekre adott válaszok megírását és elküldését. Lehetőséget nyújtanak az elküldött levelek másolatának tárolására.

Képesek partnerek adatait, illetve azokból álló csoportokat címlistákban tárolni, címlistákban feljegyzett partnerek, vagy akár csoporttok számára küldött leveleket egyszerűen címezni.

10.9.3 Archiválás

A legtöbb levelezőprogrammal archív állományokba exportálhatók a mappaszerkezetben tárolt levelek.

10.9.4 Levelezési szabályok

A fejlettebb levelező programokban kritériumok és azokhoz rendelt műveletekből álló levelezési szabályokat állíthatunk fel. Az ilyen programok képesek átvizsgálni a beérkező leveleket és az illeszkedő feltételek alapján el tudják végezni a megfelelő műveleteket. A levelezési szabályokkal megfelelő mappákba rendezhetjük a különböző feladóktól érező leveleket, automatikusan törölhetünk, válaszolhatunk a levelekre.

10.10 LEVELEZÉS ÉS BIZTONSÁG

Napjainkban az informatikai rendszereket ért támadások döntő többsége e-mail közvetítéssel valósult meg. Rendkívül fontos kérdés tehát, hogy levelező programok felhasználói ismerjék az informatikai támadások típusait, a támadásokat lehetővé tévő védelmi hiányosságokat, illetve a védekezés, megelőzés lehetséges módjait.

A következőkben tekintsük át röviden a ránk leselkedő veszélyeket, és kivédésük legfontosabb lépéseit!

10.10.1 Informatikai támadások

Az informatikai támadások általában **kéretlen információ** terjesztésére, **adatok, ezeken keresztül anyagi javak megszerzésére**, számítógépes **rendszerek működésének megbénítására** vagy lassítására, személyek **szervezetek rossz színben történő feltűntetésére**, esetleg mások **provokálására** irányulnak.

Megvalósításukhoz általában valamilyen **kártékony kódot kell bejuttatni** a megtámadott számítógépre, majd el kell érni, hogy a program el is induljon. A támadás másik módja a hálózaton haladó adatcsomagok elfogása, és tartalmuk elemzése.

10.10.2 Hogyan védekezzünk?

Ne feledjük! Tökéletes biztonság nem létezik, de megfelelő szabályok betartása mellett minimálisra csökkenthetjük számítógépünk elleni támadások sikerességének valószínűségét.

Legfontosabb feladatunk a kártékony kódok bejutásának és futtatásának megakadályozása.

Ezért már a hálózathoz való első csatlakozás előtt telepítsünk gépünkre a szükséges védelmi szoftvereket. Telepítsünk **vírusellenőrző, vírusírtó, adware- és spyware-ellenes programokat és tűzfalat**. Állítsuk be őket megfelelően, és frissítsük folyamatosan adatbázisaikat! A legnagyobb odafigyeléssel megírt felhasználói programok is tartalmazhatnak hibákat, amelyeket kihasználva a támadók képesek bejuttatni rendszerünkbe kártékony programjainkat. A szoftvergyártók általában hozzáférhetővé teszik a legújabb javítócsomagokat, amelyekkel igyekeznek kijavítani programjaik hibáit. **Fontos, hogy rendszeresen végezzük el a gépünkre telepített szoftverek frissítését.**

Ezeken az alapvető biztonsági intézkedéseken túl feltétlenül tartsuk be a következő javaslatokat!

1. Telepítsünk és futtassunk folyamatosan jól konfigurált tűzfalat, vírus adware, és spyware írtót, hogy megakadályozzuk a kártékony kódok bejuttatását.
2. Lehetőleg olyan vírusellenőrző programot használjunk, amelyik képes a beérkező és kimenő levelek ellenőrzésére, vírusmentesítésére.
3. A gyártók honlapjáról rendszeresen töltsük le, és telepítsük szoftvereink frissítését! Így javíthatjuk ki programjaink biztonsági réseit.
4. Használjunk erős (minimum 8, kis- és nagybetűből, valamint számjegyből álló) jelszavakat, amelyeket minden belépés alkalmával gépeljünk be. Ezzel elérhetjük, hogy az erre alkalmas programok ne tudják kitalálni a helyes jelszót.
5. Soha semmilyen rendszerrel ne jegyeztessük fel felhasználói adatainkat! Jelszavainkat és fontos személyes adatainkat ne tároljuk számítógépen, különben az esetleg a gépünkre juttatott kártékony kódok révén azokat mások megszerezhetik.
6. Adatainkat ne továbbítsuk semmiféle elektronikus szövegben. Üzeneteinket lehetőség szerint titkosítsuk!
7. Személyes adatokat kérő üzenetekre még akkor se válaszoljunk, ha az ismert partnertől érkezett!
8. Ne fogadjunk, vagy nagyon nagy körültekintéssel kezeljünk olyan üzeneteket, amelyek ismeretlen partnertől érkeznek!
9. Az üzenetekben található programfájlokat sose futtassuk, mert azok kártékony kódokat tartalmazhatnak és elindításkor megfertőzhetik gépünket.
10. Az üzenetekben található egyéb állományokat csak alapos vírusellenőrzés után nyissuk meg!
11. Ha csak lehet, ne kattintsunk a levelekben látható hivatkozásra. Különösen akkor ha, ha azok ismeretlentől származó üzenetben találhatók, mert a linkek vírussal fertőzött weblapra irányíthatják böngészőnket.

10.11 ÖSSZEFOGLALÁS

Az elektronikus levelezés az internet egyik legismertebb és legnépszerűbb szolgáltatása. Eredeti cél szerint egyszerű szöveges üzenetek aszinkron továbbítását teszi lehetővé, de mára az elektronikus levelek mellékleteként tetszőleges bináris tartalom továbbítható.

A levelek fejrészből és testből (törzs) épülnek fel. A fejrészben a levél kezeléséhez szükséges információk, a törzsben pedig a tartalom helyezkedik el. A bináris tartalmak beágyazását a MIME formátum teszi lehetővé.

A levelek címzése *felhasználó@gépcím* formában történik. A cím első része a címzett felhasználó elektronikus postaládájának, általában egy alkönyvtárnak a neve, amely a *gépcím*-ben megadott gépen tárolódik. A levelek küldése és a címzett mailboxába juttatása SMTP szerverek segítségével, a mailboxban tárolt levelek letöltése pedig általában POP3 szerver közreműködésével történik. A levelezéshez kapcsolódó felhasználói feladatokat (levelező program konfigurálása, levelek megírása és elküldése, mailbox leveleinek letöltése, és rendezése, stb.) a levelező kliensekkel végezhetjük el.

A levelezés napjaink informatikai támadásainak leggyakoribb platformja, ezért levelezés közben fokozottan be kell tartani az alapvető védelmi szabályokat.

10.12 ÖNELLENŐRZŐ KÉRDÉSEK

1. Hogyan épül fel egy e-mail cím?
2. Mi a feladata az SMTP szervernek?
3. Melyik a POP3 szerverek leggyakrabban használt alternatívája?
4. Mit jelent SIMPLE szó az SMTP protokoll nevében?
5. Igaz-e, hogy a levelekben csak ASCII karakterek továbbíthatók?
6. Milyen részekre tagolódik az elektronikus levél?
7. Mi a levélfejben lévő Bcc adat jelentése?
8. Hogyan küldhet egy cég munkatársa az otthoni számítógépéről elektronikus levelet?
9. Letölthetjük-e otthoni gépünkre, a munkahelyük szerverének postafiókjába érkező leveleinket?
10. Mit tegyünk, ha bankunktól olyan levelet kapunk, amelyben „ellenőrzés céljából” bankkártyánk adatait kérik?

11. A WORLD WIDE WEB

11.1 CÉLKITŰZÉS

Túlzás nélkül kijelenthetjük, hogy a World Wide Web az internet legnépszerűbb szolgáltatása. Olyannyira igaz ez, hogy sok felhasználó magával az internettel azonosítja a WWW-t. Azon túl, hogy a weblapok letöltésekor elhangzó „Beléptem az internetbe!" jellegű mondatok nem csekély tájékozatlanságról árulkodnak, megérthetjük a tévhit okát. A felhasználók zöme elsősorban World Wide Webet használ, ezért a fejlesztők igyekeznek a legfontosabb szolgáltatások webes elérhetőségének biztosítására. Napjaink weblapjai alkalmasak fájlok le- és feltöltésére, elektronikus levezésre, vagy akár teljes értékű, hálózati alkalmazások használatára. Ezért a hálózati ismeretekkel nem rendelkező felhasználó joggal hiheti, hogy a weblapok alkotta Világháló azonos magával az Internettel. Bízunk benne, hogy e könyv olvasói számára már teljesen világos, hogy az internet számítógépek, kommunikációs csatornák és kapcsolóelemek alkotta fizikai hálózat, amelyen a TCP/IP protokollcsomag elemei biztosítják az adatátvitelt. A WWW egy kommunikációs szolgáltatás, amely az interneten mint hálózaton valósul meg.

Az információk webes közzététele kezdetben egy viszonylag szűk felhasználói kör privilégiuma volt. Napjainkra azonban olyan eszközök váltak elérhetővé a világhálón, amelyek bárki számára lehetővé teszik, hogy részese legyen világméretű közösségi kommunikációnak. A WWW napjainkra túllépett az egyirányú információtovábbítás lehetőségén. A „csak olvasható", úgynevezett web 1.0 korszakból, az „írható-olvasható", web 2.0 korszakba érkezett. Tankönyvünk utolsó leckéjében megismerheti a World Wide Web történetét, és működésének alapjait. Megtanulhatja, milyen szoftverkomponensek biztosítják a WWW működését, olvashat a biztonságos böngészésről, megtanulhatja mit jelent a statikus és a dinamikus oldalak fogalma, és hogy hogyan járul hozzá a web programozás a web fejlődéséhez.

11.2 A LECKE TÉMAKÖREI

- A World Wide Web kialakulása
- A web korszakai
- A webszolgáltatás alapjai
- A webszerverek feladatai
- Webhely, weblap, honlap
- Az URL címzés
- A HTML nyelv
- A webkliensek feladatai
- A http kapcsolat
- Statikus és dinamikus weblapok

11.3 A WWW TÖRTÉNETE

A World Wide Web kialakulása előtt, a kilencvenes évek első felében volt népszerű a Gopher nevű szolgáltatás, amelyet Minnesotai Egyetemen fejlesztettek ki. A Gopherben menük segítségével lehetett szöveges fájlokhoz, és újabb menükhöz eljutni. A fájlok és a további menük az internet különböző gépein helyezkedhettek el, így a Gopher valójában különböző gépeken elhelyezkedő fájlok és menük „hálózata" volt. A Gopherrel letölthető dokumentumok ugyan csak szövegesek lehettek, a szolgáltatás mégis nagy népszerűségnek örvendett a képzési intézményekben és az üzleti szférában egyaránt.

A Gopher fejlesztői azonban, 1993-ban bejelentették, hogy a jogdíjat kérnek a szerverek kódjának felhasználásáért. Ezzel a lépéssel gyakorlatilag megpecsételték a szolgáltatás jövőjét. A fejlesztők új megoldásokat kezdtek keresni a Gopher nyújtotta lehetőségek megvalósítására.

11.3.1 A World Wide Web születése

Gopher alternatíva kidolgozásába fogott Tim Berners-Lee, a CERN (Európai Atommagkutató Tanács) genfi laboratóriumának fizikus-informatikusa is, akinek feladata az volt, hogy fizikusok kutatásainak dokumentációját tegye hozzáférhetővé az Internet különböző helyein lévő szervereken. A publikációknak formázott szöveget, képeket, ábrákat, és más publikációkra mutató hivatkozásokat kellett tartalmaznia.

A Tim Berners-Lee által megalkotott eszköz felhasználta a kor informatikai fejlesztéseinek különböző elemeit, de saját ötleteinek, elképzeléseinek hozzáadásával egy új szolgáltatást teremtett meg az Interneten. Az új eszközt Word Wide Web-nek nevezte el a fejlesztő.

Az 1991-ben útjára indított World Wide Web-ről azóta világossá vált, hogy nem pusztán informatikai eszköz, hanem egy kulturális, és kommunikációs forradalmat gerjesztő találmány. A web olyan mértékben gyorsította fel és egyszerűsítette le az információszerzést és a közzétételt, hogy minden túlzás nélkül kijelenthetjük, a WWW jelentőségében felér a könyvnyomtatás megjelenésével. Könnyen lehet, hogy az eszköz jelentősen hozzájárul egy olyan bolygó méretű intellektus kialakulásának, amelyet Isaak Asimov vizionált híres regényciklusának Gaia bolygóról szóló részében.

Munkája jelentőségének elismeréseként II. Erzsébet brit királynő 2004-ben a brit korona lovagjává ütötte Leet. Bár hivatalos megszólítása, azóta Sir Timothy Berners-Lee, a web feltalálója továbbra sem tétlenkedik. Még 1994-ben alapította meg a World Wide Web Consortium-ot (W3C), amelynek azóta is vezetője. A W3C szakemberei folyamatosan munkálkodnak a Web technológiai tökéletesítésén, és újabb technikák kifejlesztésén.

11.3.2 A World Wide Web

A World Wide Web (www, vagy egyszerűen csak web) szolgáltatás egyik alapvető eleme a képernyőn megjeleníthető elektronikus dokumentum, a weblap. A weblap hipermédia dokumentum, amely szöveget, képeket és egyéb multimédia elemeket, valamint, linkeket tartalmazhat. A linkek más weblapokra mutató hivatkozások.

A weblap általában grafikus felületen jelenik meg a felhasználó előtt, elkészítése, leírása, azaz forrásának összeállítása azonban egyszerű szöveg (plain text) formájában történik. Egy weblap tartalma formázatlan karakterek, szavak, mondatok, illetve a weblap szövegé-

be ágyazott, szintén szöveges utasítások sorozata. Utóbbiak írják le a weblap megjelenítéskor használt elrendezését, formátumokat, a szövegben megjelenő multimédia fájlok (pl. képek) elhelyezkedését, és a kapcsolódó weblapokra mutató hivatkozásokat, linkeket. Röviden a weblap tiszta szöveg, ami a megjelenő szöveges tartalomból és a megjelenítést, kezelést leíró szöveges utasításokból épül fel.

A weblap szövegébe ágyazódó utasítások, más néven jelölők egy úgynevezett jelölő nyelvet képeznek. Ezt a nyelvet nevezzük **HTML**-nek (Hypertext Markup Language)

A www kliens szerver szolgáltatás, amellyel a szervereken (webszerver) tárolt weblapokat, a világ bármely pontján elhelyezkedő klienssel (böngésző) le lehet tölteni, és azonnal meg is lehet jelenítni a képernyőn. A böngészők nem csak letöltik weblapokat, hanem a forrásba ágyazott jelölőknek megfelelően formázva meg is jelenítik a dokumentumot a képernyőn.

A weblapokban lévő linkek nem csupán passzív hivatkozások, tartalmazzák a hivatkozott dokumentum pontos címét az interneten. Segítségükkel egyetlen kattintással letölthető, és megtekinthető a hivatkozott weblap is.

A szerver és kliens közötti kommunikációt egyedi protokoll a **HTTP** (Hypertext Transfer Protocol) biztosítja. A szolgáltatás fontos eleme még az úgynevezett **URL** (Universal Resource Locator) címzési rendszer, amivel letöltéskor, illetve hivatkozásokban pontosan megadható egy dokumentum tárolásának helye.

11.3.3 A WWW korszakai

A tananyagunk írásakor még „fiatalkorú” WWW máris komoly múlttal, sőt történelemmel rendelkezik. Mai ismereteink birtokában, a web fejlődésére visszatekintve korszakokat különíthetünk el a www történetében.

- **Web 0**-ként a www kialakulásának, kezdeti fejlődésének éveit szokás emlegetni.
- A hozzávetőleg az 1990-es évek közepén elkezdődött a **Web 1.0** korszakot „*csak olvasható*” web-ként emlegetjük. A jelző azért találó, mert rámutat az akkori web fontos jellemzőjére, miszerint a weblapok készítése, az információ közzététele egy viszonylag szűk kör privilégiuma volt, még a internet nagyközönsége számára csupán az oldalak megtekintésére, és elolvasására volt lehetőség.
- Bár a www alaptechnológiája változatlan maradt, néhány további, kiegészítő fejlesztésnek köszönhetően olyan weblapok jelenhettek meg, amelyeken a felhasználó saját ismereteit, tudását, élményeit is megoszthatta, illetve más felhasználókkal kommunikálhatott. Ebben, a napjainkban is zajló **Web 2.0** korszakban már nem csak olvashatjuk, hanem írhatjuk is a weben megjelenő tartalmakat. A Web 2.0-t ezét nevezik „*írható-olvasható*” webnek.
- Az „*írható-olvasható és futtatható*”, **Web 3.0** korszaka ugyan még csak részben következett be, kiteljesedése kétségtelenül küszöbön áll. Ebben a korszakban a manapság még a személyi számítógépeken futtatott operációs rendszerek várhatóan átkerülnek web platformra, és a különböző felhasználói programok is web felületen működnek majd. Utóbbira már ma is látunk példákat, hiszen számos webmail alkalmazást, szövegszerkesztőt, grafikus alkalmazást, sőt weblapkészítő programokat is futtathatunk már böngészőinkben.

- Egyelőre csak beszélünk róla, de a 2010 őszére bejelentett Google TV megjelenésével, várhatóan beköszönt a **Web 4.0** korszaka, amikor is az informatika és a web használata kilép a személyi számítógépek egyre szűkebbnek bizonyuló keretei közül. Új, internet hozzáféréssel rendelkező, és a weblapok megjelenítésére alkalmas eszközök, például televíziókészülékek jelennek majd meg. A Web 3.0 és 4.0 a World Wide Web, és egyben az emberi kultúra napjainkban jelenlévő jövője.

11.4 A WWW ELEMEI

A Tim Berners-Lee által kifejlesztett World Wide Web szolgáltatás tehát a következő pillérekre épül:

- Web szerver,
- URL cím,
- HTML nyelv,
- Web kliens (böngésző),
- HTTP protokoll.

A következőkben áttekintjük ezen elemek feladatait.

11.4.1 Webszerver

- A webszerver a host könyvtárszerkezetének egy részét (webroot) teszi elérhetővé interneten keresztül.
- Figyeli a beérkező weblapokra vonatkozó kéréseket.
- Ha weblapot kérnek tőle, megkeresi és elküldi az interneten.

A webszerverek a kliens-szerver alapú www szolgáltatás kiszolgáló oldali összetevői. Felügyelik az őket futtató host háttértárainak egy (vagy több) területét, könyvtárát, az abban elhelyezkedő fájlokat és alkönyvtárakat. A könyvtárszerkezetnek ezen az úgynevezett webterületén jellemzően weblapok és azokhoz kapcsolódó egyéb állományok helyezkednek el. A webszerverek (általában a 80-as TCP porton) folyamatosan figyelik, kliensektől érkező kéréseket, amelyek általában weblapokra vonatkoznak.

A kérés beérkezése után a webszerver, a host webterületen megkeresi az adott oldalt, majd az internet segítségével elküldi az igénylő web kliensnek. A kliens ezután gondoskodik a weblap kezeléséről, megjelenítéséről.

A webterület fölépítése

A webterület a webszervert futtató host könyvtárszerkezetének csak egy része, de számtalan weblapot és kapcsolódó fájlt tartalmazhat. Ugyanazon a szerveren több, különböző témakörökkel foglalkozó oldal helyezkedhet el. Az azonos témakörökhöz kötődő weblapokat és fájlokat a webterületen közös könyvtárában helyezik el. Ezeket a könyvtárakat nevezik webhelynek, vagy site-nak.

A webhely, vagy site több, azonos témakörrel foglakozó weblap, illetve kapcsolódó állomány gyűjtőhelye a webszerver webterületén. Egy webhely fizikailag a webterület egy alkönyvtára.

A webhelyeken általában nem egyetlen, hanem sok weblap található. A webhely egyik kiemelt szerepű oldalának tartalmát általában úgy alakítják ki, hogy az abban lévő hivatkozásokkal az összes többi weblap elérhető legyen. Ezt a központi oldalt nevezzük a webhely honlapjának, vagy homepage-nek. Az egyszerű kiválasztás érdekében a honlapnak konvencionális nevet adnak. Ez jellemzően **index.htm**, vagy **index.html**.

A honlap egy webhelyen található weblap, amelyről hivatkozásokkal elérhető a webhely összes további oldala. A honlap neve szokásosan index.htm, vagy index.html.

Az URL címzés

A World Wide Weben az internet különböző hostjain működő webszerverek, hozzávetőleg 80 000 000 webhelyén több milliárd weboldal helyezkednek el. Bárki, bárhol is indít el egy böngészőt, ezen oldalak bármelyikéhez hozzáférhet[14], és letöltheti azt. Ehhez arra van szükség, hogy bármelyik oldal pontosan azonosítható, címezhető legyen. Ezt biztosítja az URL címzési rendszer. Amikor böngészőnkkel le akarunk tölteni egy weblapot, pontosan be kell gépelnünk az oldal URL címét. A címet elsőként a böngésző használja, de kérésben elküldi a webszervernek is.

Az URL cím [*protokoll***://**]*gépcím*[*/útvonal*][*/fájlnév*][**?***paraméter1***&***paraméter2*…] formában[15] épül fel. Mint tudjuk a szögletes zárójelek között részeket csak szükség esetén kell használni.

Például: **http://www.ektf.hu/user/gyakorlo/udvozlet.html**

- *protokoll*: A protokoll azt határozza meg, hogy a böngésző milyen protokoll alapján fogalmazza a meg a szervernek szóló kérést. Az esetek többségében http protokollra van szükség. Ha nem adjuk meg, a böngésző általában ezt tekinti alapértelmezettnek.
- **://** Elválasztásra való. A protokoll megadása esetén kötelező, különben tilos használni.
- *gépcím*: a webszerver futtató host domain neve, vagy IP címe. (pl.: **www.ektf.hu**)
- *útvonal*: a weblapot tartalmazó könyvtárnak, a szerver webterültetén, vagy egy webhelyen elfoglalt helyét adja meg. A **/user/gyakorlo** útvonal azt jelzi, hogy a webhely **user** könyvtárának **gyakorlo** alkönyvtárából akarunk letölteni egy weblapot.
- *fájlnév*: a kért weblap, vagy más fájl (például kép) neve (pl.: **udvozlet.html**).
- *paraméterek*: dinamikus weblapok esetén jelentőségük.

Gyakran adunk meg úgy egy URL címet, hogy a végén nem gépeljük be a fájlnevet. Például: **http://www.ektf.hu/user/gyakorlo** Ilyenkor a szerver az útvonalban megadott könyvtárban található, honlapot (index.htm, index.html…) küldi vissza. Ez teszi lehetővé, hogy egyszerűen letöltsük egy site honlapját.

[14] Természetesen számos webhely hozzáférése korlátozott. Ezeket csak bejelentkezés után, sőt gyakran a hálózat meghatározott tartományán belülről csak tölthetjük le.

[15] A formátum megadása azonos az FTP utasítások leírásánál alkalmazottakkal. A [ ] közötti részt nem kötelező használni, a *dőlt betűs* szavakat értelemszerűen helyettesíteni kell.

Az is előfordul, hogy a címben az útvonalat is elhagyjuk. Pl.: **http://www.ektf.hu** Ilyenkor a webterület főkönyvtárában lévő honlapot kapjuk vissza.

A HTML nyelv

A HTML (Hypertext Markup Language) az úgynevezett jelölő nyelvek családjába tartozik. A jelölő nyelvekkel egy szövegfájl egyes elemeinek jellemzőit a szövegfájlon belül elhelyezett szöveges parancsokkal jelölhetők.

A HTML az SGML-ből (Standard Generalized Markup Language) származó jelölő nyelv, amit weblapok jelölésére fejlesztettek ki. Segítségével a weblap szövegébe ágyazott jelölőkkel, megadható szöveg szerkezete, elemeinek formátuma, és a weblaphoz kapcsolódó külső fájlokra mutató hivatkozások is. A HTML legfontosabb jellemzője, hogy egyetlen szöveges dokumentum tartalmazhatja a tényleges szövegtartalmat, a szerkezet, a formátum leírását, és a kapcsolódó oldalakra mutató hivatkozásokat.

Jelölőnyelvek esetében meg kell oldani a szöveg, és a jelölők egyértelmű elkülönítését. A HTML-ben a <> jelpárt használják erre a célra. A weblap forrásában minden <> jelek közé zárt rész jelölőnek, a többi szöveg pedig a megjelenítendő szövegtartalomnak számít.

A következő weblap részletben például két jelölő látszik: **<B>Hello</B> World!**

A <B> azt mutatja, hogy a következő szöveget félkövér betűkkel kell írni. A </B> azt jelöli, hogy be kell fejezni a félkövér írást. A jelölők utasításait betartva a szöveg így nézne ki: **Helló** Wordl!

A HTML nyelv valójában a weblap formázásra felhasználható jelölők rendszere. A nyelv több változatot, verziót élt már meg, jelenleg a 4.0 illetve az XHML verziók használata a legelterjedtebb.

A web kliens feladatai

A webkliensek, más néven böngészők alapvető feladata a weblapok letöltése, és megjelenítése, valamint a weblapokban elhelyezkedő hivatkozások kezelése.

Amikor a felhasználó böngészőjének címmezőjében megadja egy weblap URL címét, a böngésző kiemeli a szerver gépcímét leíró részt. Ha ez egy domain név, akkor a DNS szolgáltatás segítségével feloldja azt, és a gépcím helyére a kapott IP címet illeszti. Ha eleve IP címet adtunk meg, akkor a feloldásra nincs szükség. Ezt követően kapcsolatot épít fel a címzett szerverrel és egy kérésben elküldi neki URL címet. A szerver megkeresi a kért weblapot, és visszaküldi a böngészőnek.

A böngésző elemzi a weblap forrását. Előfordulhat, hogy elemzés közben olyan jelölőkre bukkan, amelyek külső állományokra, például képekre hivatkoznak. Ilyenkor a böngésző ismét kérést küld webszervernek, és letölti a képet is. Miután a hivatkozott fájlok is letöltődtek a kliens a weblapban található jelölőknek megfelelően megjeleníti az oldal tartalmát. A weblap látható képének előállítását nevezzük renderelésnek. A renderelés eredményeként a képernyőn megjelenik a formázott szerkesztett szöveg, és a weblapról hivatkozott képek.

Ha a weblapban a felhasználó más oldalakra mutató hivatkozásra, linkre kattint, a böngésző kiemeli HTML dokumentumból a hivatkozás URL címét és – mintha azt beírtunk volna – letölti a hivatkozott dokumentumot.

Ezeken az alapfeladatokon kívül a böngészők számos egyéb funkciót támogatnak. Lehetőséget teremtenek például:

- A letöltött weblap szövegének, vagy akár a kapcsolódó állományoknak mentését a lokális lemezre.
- Oldalalak tartalmának nyomtatását.
- A weblap tartalmának vágólapos kezelést.
- A kedvenc weblapok, illetve az elmúlt időszakban a meglátogatott oldalak címének tárolását.
- Dinamikus oldalakban elhelyezkedő programkódok futtatását.
- Lehetővé teszik beépülő programok hozzáférését a weblap tartalmához, és a rendereléshez.…

Kommunikáció a szerver és a kliens között

A web kliens és a szerver közötti kommunikációt más szolgáltatásokhoz hasonlóan protokollok írják le. A WWW alapértelmezett protokollja a http, de más protokollok használatára is van mód. A szerver-kliens kommunikáció egyébként kérések és válaszok formájában történik.

A HTTP kapcsolatot mindig a kliens kezdeményezi úgy, hogy kérést küld a szerver számára. A kérés a protokollban meghatározott szerkezetű fejlécet tartalmaz, amelyben a kliens pontosan megadja a kérés tartalmát. A szerver válasza szintén egy fejléccel kezdődik, amelyben a kérés végrehajthatóságáról küld tájékoztatást. Ha a kért fájlt a szerver megtalálta, akkor a fejlécet ennek adatai követik.

A http eredeti, 1.0 verziójában a kliens és szerver kapcsolata minden egyes válasz után elbomlott. Ez azt is jelentette, hogy egy weblap letöltésekor több kapcsolatot is föl kellett építeni egymás után. Egyet HTML dokumentum, majd egyet-egyet minden a weblapban lévő kép illetve egyéb állomány kérésekor. A http 1.1 verzió lehetővé teszi több állomány egyetlen kapcsolat alatt történő letöltését is.

A HTTPS

A HTTPS a http továbbfejlesztésével létrehozott protokoll. A HTTPS kapcsolat során a szerver és kliens között titkosított csatorna alakul ki, ami biztosítja, hogy harmadik fél ne tudja „ellopni”, vagy meghamisítani a küldött adatokat. A protokollnak különösen nagy jelentősége van például webfelületen történő banki műveletek során.

Az FTP

Bármilyen meglepő, a webböngészők FTP kliensként is képesek működni. Ha ftp szerverrel szeretnénk web felületen kommunikálni, szerver címét az **ftp://** előtag begépelésével kell beírni a böngésző címmezőjébe. A kapcsolat felépülését követően a böngésző beolvassa a felhasználói nevünket valamint jelszavunkat, majd elküldi azt a szervernek. Ha a bejelentkezés sikeres, a képernyőn az FTP szerver fájljai és könyvtárait hivatkozásként tartalmazó weblap jelenik meg. Fájlok linkjére kattintva letöltődik a kérdéses állomány, a könyvtárak hivatkozásával pedig beléphetünk a könyvtárba. Ha a böngészőt bezárjuk, a kapcsolat elbomlik.

11.5 STATIKUS ÉS DINAMIKUS WEBLAPOK

A World Wide Web kialakulásának kezdetén csak **statikus weblapok** készítésére nyílt lehetőség. A statikus oldalak tartalmát és formátumát a weblap készítője meghatározza meg. Előre elkészíti a HTML oldalt, és feltölti egy webszerver webterületére. Az oldal ezt követően elérhető a böngészők számára, de mindig ugyanolyan tartalommal és formában jelenik meg. A statikus oldalakat tehát **emberek, előre készítik** el.

Később a webszervereket felkészítették arra, hogy számítógépes **programok által, valós időben** készített, **dinamikus oldalakat** is tudjanak kezelni.

Az ilyen oldalak nincsenek előre megírva. A webszerver nem is a HTML nyelven írt dokumentumok, hanem számítógépes programkódok tárolódnak. Amikor a böngésző lekér egy oldalt, a szerver gondoskodik a megfelelő program elindításáról. A program lefut, és egy weblapot, valódi HTML oldalt állít elő. A szerver ezt küldi vissza a böngészőnek. Az ilyen oldalakat dinamikus weblapoknak nevezzük.

A dinamikus oldalak nincsenek előre megírva, hanem mindig a kérés pillanatában, valós időben lefutó számítógépes program állítja elő őket. Használatukat azt teszi igazán érdekessé, hogy a weblapok felületén megjelenő vezérlőelemekkel (gombok, szövegmezők, listák) bevitt adatokat a böngésző a szerverhez intézett kérésben el tudja küldeni. A dinamikus oldalt előállító program, feldolgozza, és kiértékeli ezeket az adatokat, majd a weblapot ezek figyelembevételével készíti el.

> Ez azért figyelemre méltó, mert ugyanaz a program, a bejövő adatoktól függően más-más tartalmú weblap előállítására képes.

A dinamikus oldalak tették lehetővé a különböző webes alkalmazások elkészítését. Manapság egyre ritkábban találkozunk olyan oldalakkal, amelyek kódját, vagy annak legalább egy részét ne programok készítenék. Dinamikus oldalakkal dolgozunk, amikor a tanulmányi rendszert, a távoktatási oldalt használjuk, banki ügyeinket intézzük, pizzát, vagy repülőjegyet rendelünk, esetleg leadjuk elektronikus adóbevallásunkat.

A web igazi diadalútja, a web 2.0, 3.0 illetve 4.0 megjelenése a dinamikus oldalaknak és a web programozásnak köszönhető.

11.6 ÖSSZEFOGLALÁS

A World Wide Web, azaz világméretű hálózat, tagadhatatlanul az Internet legnépszerűbb szolgáltatása. Használata során távoli gépeken tárolt szöveges, képi, hang, és egyéb médiumokat tartalmazó dokumentumokat tölthetünk le saját gépünkre, hogy elolvassuk, megnézzük, vagy meghallgassuk azokat. A WEB úgynevezett hypermédiás dokumentumai, hivatkozások segítségével összeköttetésben állnak, hivatkoznak egymásra. A hivatkozások használatával a felhasználó egyszerűen hozzájuthat olyan dokumentumokhoz, amelyek címét, pontos helyét nem is ismeri.

Könnyű használatának, sokoldalú lehetőségeinek köszönhetően a WWW nem csak napjaink elsőszámú Internetes információforrásává vált, de jelentős szerepet kapott a hálózaton folyó kommunikáció, és az on-line kereskedelem felületének biztosításában is. Fejlődése olyannyira dinamikus, hogy napjainkra sok felhasználó az Internet összes egyéb szolgáltatását a WEB segítségével használja.

A web szolgáltatás alapjait Tim Berners-Lee dolgozta az 1980-as évek végén. Az első webszerver 1991-ben kezdet működni.

A kliens szerver alapú szolgáltatás alap protokollja a http. A html nyelven írt oldalak tárolása letölthetőségük biztosítása a szerver feladata, a felhasználó web kliensek, azaz böngészők segítségével juthat hozzá a szervereken tárolt weblapokhoz. A http protokoll szerint kommunikáló kliens meghatározott szerkezetű kérés közli a szerverrel a két weblap URL címét, a szerver pedig fejlécet tartalmazó válaszban küldi vissza az oldalt.

Az előre megírt változatlan tartalmú weblapokat statikus oldalaknak, a számítógépes programok által, valós időben készített weblapokat dinamikus oldalaknak nevezzük. A dinamikus oldalak és a webprogramozás eredményeként indult meg a web igazi fejlődése.

11.7 ÖNELLENŐRZŐ KÉRDÉSEK

1. Miben hasonlít a Gopher és a WWW?
2. Miért nevezik világhálónak a web-et?
3. Miért mondják a Web 2.0-t „írható-olvasható” web korszakának?
4. Miért kapta a lovagi címet Sir Timothy Berners-Lee?
5. Mi az a **HTTP**?
6. Hogyan ftp-zhet egy web böngészővel?
7. Mi az a site?
8. Hogyan épül fel az URL cím?
9. Igaz-e hogy a HTML programozási nyelv?
10. Mit ért dinamikus weblap alatt?

12. ÖSSZEFOGLALÁS

12.1 A KURZUSBAN KITŰZÖTT CÉLOK ÖSSZEFOGLALÁSA

Tananyagunk 10 leckéjének áttanulmányozása után Ön megismerte a hálózati alapfogalmakat. Megtanulta, milyen ismérvek alapján jellemezhetjük, és csoportosíthatjuk a hálózatokat. Megismerte a hálózati kommunikáció feladatainak rétegstruktúráját, megértette a rétegek, protokollok, és entitások jelentőségét.

Betekintést kapott az OSI referencia modellbe, és pontos ismereteket szerzett a TCP/IP architektúra elemeiről, azok működéséről.

Megismerte az irodai hálózatok legfontosabb elemeit, és a LAN internethez kapcsolásának lehetőségeit. Részletes ismertetést olvashatott a TCP/IP hálózatok legfontosabb szolgáltatásainak működéséről, megismerkedhetett a hálózati biztonság alapvető problémáival, az azok megoldására alkalmas módszerekkel.

12.2 A TANANYAGBAN TANULTAK RÉSZLETES ÖSSZEFOGLALÁSA

12.2.1 Hálózati alapismeretek

A leckéből megismerhette a számítógépes hálózat felépítését, fogalmát. Megtudhatta miért előnyös és hátrányos használata, és milyen szempontok alapján csoportosíthatja. Megismerkedhetett legfontosabb jellemzőivel.

12.2.2 Hálózati architektúrák

A lecke ismerteti a hálózati feladatok rétegeit, és az ezek közötti kommunikációt. A lecke segít megérteni a szabványok jelentőségét az informatikában, és bemutat néhányat a létrehozó szervezetek közül.

Bemutatásra kerül a két legjelentősebb referenciamodell az OSI és a TCP/IP modell.
A lecke végén megismerhette az Ethernetet, a mai LAN hálózatok legelterjedtebb technológiáját.

12.2.3 Hálózati eszközök

A hálózati eszközöket ismertető leckéből megismerhette az aktív és passzív eszközök fogalmát. Megtudta a hálózati kártya, a repeater, a hub, a bridge, a switch, a router és a gateway szerepét a hálózatok felépítésében.

Megtudhatta mi az az Access Point. És megismerte napjaink leggyakrabban használt hálózati kábeltípusait.

12.2.4 Az Internet működése

A leckéből megismerhette az Internet kialakulásának történetét és ismereteket szerezhetett működéséről. Megtanulta az IP címek jelentőségét, ezek jelenlegi és jövőbeni formáját, szállítási: TCP, UDP és vezérlő protokolljait: ICMP, ARP, RARP.

12.2.5 Irodai és otthoni hálózatok

A lecke bemutatja az internetre kapcsolódáshoz szükséges eszközökkel, és ismerteti a már meglévő internetkapcsolatunk megosztásának lehetőségét akár vezeték nélküli környezetben is. A lecke második felében foglalkozunk egy kiemelt jelentőségű témakörrel, a biztonsággal.

12.2.6 A Domain Name System

Ebben a leckében, az internet hierarchikus tartományrendszerén alapuló címzéssel, a DNS-sel ismerkedhetett meg. Megtanulhatta, hogyan teszi lehetővé a DNS, hogy az IP címzés változatlan használata mellett a felhasználók könnyebben megjegyezhető, alfabetikus host címeket alkalmazhassanak.

12.2.7 Telnet, SSH, Távoli asztal

A 8. lecke a távoli hozzáférés szolgáltatásairól nyújtott átfogó képet. A hallgató megismerhette a már az internet korai időszakában is használt, Telnet szolgáltatást. Rávilágítottunk a Telnet előnyeire, és a végül háttérbe szorulásához vezető hiányosságaira. Bemutattuk és bizonyos mértékékig a Telnettel szembe állítottuk az SSH szolgáltatást, utaltunk az SSH más protokollok beágyazására alkalmas tunneling lehetőségére.

A lecke megismertette Önnel a Microsoft, Távoli Asztal szolgáltatása által nyújtott lehetőségeket.

12.2.8 Az FTP szolgáltatás

Az File Transfer Protocolt bemutató lecke megismertette a TCP/IP hálózatok mai napig legjellemzőbb fájl átviteli protokollját. Az FTP szerverek és kliensek alapvető feladatainak megértése mellett, Ön elsajátíthatta, egy karakteres, és egy grafikus felületű FTP kliens használatának módját, de megismerkedhetett az SSH, fájlok titkosított csatornán való továbbítását lehetővé tévő funkciójával is.

12.2.9 Az elektronikus levelezés

Ebben a leckében áttekintettük az e-mail szolgáltatáshoz kapcsolódó legfontosabb fogalmakat. Elmagyaráztuk a SMTP, és POP3 illetve IMAP szerverek funkcióját. Megismerte az e-mail címzést, az elektronikus levelek felépítését. Megérthette, hogyan vált alkalmassá az e-mail tetszőleges fájlok csatolt továbbítására. A levelezés működésén kívül Ön megtanulhatta, hogyan küldhet és tölthet le leveleket távoli hálózatból.

12.2.10 A World Wide Web

Tankönyvünk utolsó leckéje napjaink legnépszerűbb szolgáltatása, a WWW kialakulását és fejlődését mutatta be. Ön megismerhette a WWW legfontosabb elemeit, a web szerverek és kliensek szerepét, a közöttük megvalósuló kommunikáció módját, a http protokollt, a weblapok címzésére alkalmas URL címzési rendszert, és a hipermédiás dokumentumok jelölőnyelvét a HTML-t.

13. KIEGÉSZÍTÉSEK

13.1 IRODALOMJEGYZÉK

13.1.1 Könyv

KÓNYA LÁSZLÓ:Számítógép hálózatok. Budapest, LSI Oktatóközpont Alapítvány 1999
LENGYEL VERONIKA: Az Internet világa, Budapest, ComputerBooks Kiadói Szolgáltató és Kereskedő Kft. 1999
JAMES MARTIN: Lokális hálózatok, Budapest, Novotrade Kiadó Kft., 1993
ANDREW S TANENBAUM: Számítógép-hálózatok, Budapest, Novotrade Kiadó Kft., 1997

13.1.2 Elektronikus dokumentumok / források

INTERNET ENGINEERING TASK FORCE: *Request for Comments*., IETF [elektronikus dokumentum] [2010.június 1.] <URL: http://www.ietf.org/rfc.html>