Hálózati alapismeretek, alapfogalmak

Programtervező informatikus BSc

Számítógép hálózatok és architektúrák

előadás

A hálózatok kialakulása

- Független számítógépek problémái
  - információ megosztásának nehézsége
  - módosítások követése
  - többszörös erőforrások
- Kezdeti számítógép hálózatok
  - minden gyártó saját "szabvány" szerint fejleszt
  - egymással nem kompatibilis eszközök, megoldások
  - gyakran a teljes hálózat cseréje volt indokolt
- LAN hálózati szabványok megalkotás
- Hálózatok előnyei és hátrányai

Történelmi áttekintés

1876	Bell, elektronikus úton történő hangtovábbítás szabadalma (174465)
1901	Marconi szikratávírója
1947	Félvezető tranzisztorok feltalálása
1950	Az integrált áramkörök feltalálása
1957	DoD - ARPA hálózat
1962	Paul Baran terve az első csomagkapcsolt hálózatról
1973	TCP/IP protokoll kifejlesztése
1981	Az internet szó használata összekapcsolt hálózatok értelemben
1983	A TCP/IP lesz az internet hivatalos protokollhja
1991	A World Wide Web megalkotása
1993	Az első grafikus böngésző megjelenése (MOSAIC)
1999	Az IPv6 használatának kezdete

Hálózati topológiák

- Topológiák
  - Busz topológia
  - Gyűrű topológia
  - Csillag topológia
  - Kiterjesztett csillag topológia
  - Hierarchikus (fa) topológia
  - Háló topológia
  - Vegyes topológia
- A hálózati kommunikáció megvalósítása
  - szórásos (broadcast) rendszerek
  - vezérjeles rendszerek

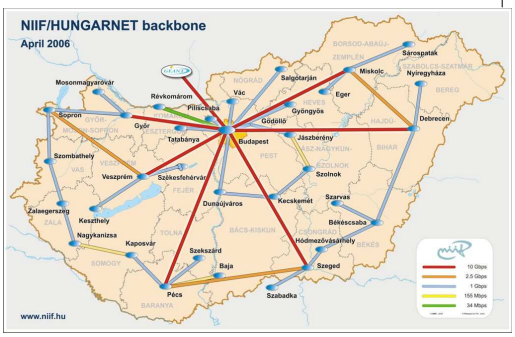
Hálózatok kiterjedése

- Hálózatok osztályozása kiterjedés szerint
  - LAN (Local Area Network)
  - MAN (Metropolitan Area Network)
  - WAN (Wide Area Network)
- LAN
  - fizikálisan egymáshoz közeli eszközök összekapcsolása
  - földrajzilag korlátozott működési terület
  - folyamatos hozzáférést biztosít az erőforrásokhoz
  - általában a használó szervezet felügyeli és menedzseli

Hálózatok kiterjedése

- MAN
  - Általában LAN-ok összekapcsolásával jön létre
  - Földrajzilag korlátozott, nagyváros méretű területeken
  - Különböző szolgáltatásokat integrálhat
- WAN
  - LAN-ok összekapcsolása
  - Nagy földrajzi távolságok
  - Általában lassabb működés az egyes LAN-ok között
  - Állandó vagy időszakos kapcsolat
  - Az internet …

A magyarországi gerinchálózat HBONE



Az internet története, ARPANET

- 1950-es évek vége, a hidegháború csúcsa
- Az USA-ban a katonai kommunikáció a nyilvános távbeszélő hálózatot használta
  - kulcsfontosságú távhívó központok
  - sebezhető rendszer
- Paul Baran megoldási javaslata
  - elosztott, hibatűrő rendszer
  - digitális csomagkapcsolás
  - A kormány az AT&T-t kérte fel a megvalósításra

ARPA (Advanced Research Agency)

- Szerény költségvetés
- Egyetlen iroda (nincsenek tudósok, laborok)
- Feladata szerződések kötése és támogatások odaítélése az ígéretesnek tartott egyetemi, vállalati kutatásokhoz.
- 1967-ben az ARPA vezetője (Larry Roberts) egy Gatlinburg-i konferencián igazolást és egy működő példát (NPL - National Physical Laboratory, anglia) talált arra, hogy Baran ötlete, a csomagkapcsolás megvalósítható.

Az ARPANET terve

- IMP (Interface Message Processor)
- Minden csomóponti gép (IMP) legalább két másik IMP-vel tart kapcsolatot
- Datagrammos hálózat → alternatív útvonalak
- Minden csomópontban
  - hoszt (max. 8063 bites üzeneteket küld)
  - csomóponti gép (max. 1008 bites csomagok)
  - csomagok egymástól független továbbítása
  - tárol és továbbít típusú csomagkapcsolt hálózat

Az ARPANET megvalósítása

- Csomóponti gép
  - speciális Honeywell DDP-316 miniszámítógép
    - 12K 16 bites szó tárolására alkalmas memória
    - diszket nem tartalmazott
  - 56 kbit/s bérelt vonal
- Szoftver probléma
  - a fejlesztés befejeződött azzal, hogy a hosztok felől érkező csomagokat egyszerűen továbbították a cél csomóponti gép és a cél hoszt közötti vonalra
  - a hosztoknak szoftverre volt szükségük

Az ARPANET megvalósítása

- 1969 hálózati kutatók találkozója (Snowbird)
- Várakozások a kutatók részéről
  - szakemberek magyarázzák el a hálózat struktúráját
  - szakemberek mutatják be a szoftverrel kapcsolatos átfogó terveket
  - kiosztják a részfeladatokat
- A valóság …
  - nincsenek szakemberek
  - nincsenek átfogó tervek
  - azt várják tőlük, hogy kitalálják mit kell csinálni

Az ARPANET fejlődése

- 1969 decembere és 1972 szeptembere között a csomópontok száma 4-ről 34-re nőtt
- További terjeszkedési területek
  - műholdas hálózatok
  - mobil csomagkapcsolású rádiós hálózatok
- Világossá vált, hogy a protokollokat egységesíteni kell az összekapcsolt hálózatokban
- TCP/IP modell és protokoll kifejlesztése (1974)
- Berkley UNIX fejlesztésének ösztönzése
- 4.2 BSD TCP/IP-vel és hálózati segédprogramokkal
- Hirtelen megnőtt az ARPANET-hez kapcsolt LAN-ok száma
- Az 1980-as években bevezették a DNS rendszert

NSFNET

- Az NSF felismerte az ARPANET hatását az egyetemi kutatásokra
- Az ARPANET-hez azonban csak az csatlakozhatott akinek volt kutatási szerződése a DoD-vel.
- Az NSF egy minden egyetemi kutatócsoport számára elérhető hálózatot tervezett az ARPANET mintájára
- Az ARPANET-tel azonos műszaki megoldások
- Kezdettől fogva TCP/IP!
- Kapcsolódási pont az ARPANETHEZ

Az Internet

- 1983. január 1-én a TCP/IP lett az ARPANET és a hozzá kapcsolódó hálózatok hivatalos protokollja
- A csatlakozó hálózatok, gépek száma exponenciálisan növekedett
- az 1980-as évek közepétől kezdték ezt internetnek (világhálózatnak) tekinteni, így lett később Internet
- Az összetartó erő a TCP/IP hivatkozási modell és a TCP/IP protokoll

Tárolóhálózatok (SAN)

- A szerverek és a háttértárak közötti hálózat
- Dedikált, nagy teljesítményű hálózat
  - Külön hálózati infrastruktúra
- Jellemzők
  - Teljesítmény
  - Rendelkezésre állás
    - megbízhatóság
    - duplikált adatok, biztonsági mentések, stb.
    - hibatűrés
  - Skálázhatóság

Virtuális magánhálózatok

- VPN (Virtual Private Network)
  - Biztonságos összeköttetés
  - Nyilvános hálózatok használatával
  - Azonos felügyeleti és biztonsági szabályok
- VPN típusok
  - Hozzáférési VPN
    - ad-hoc kapcsolat, mobil, otthoni felhasználóknak
  - Intranetes VPN
    - dedikált kapcsolat, csak a hálózat tagjainak
  - Extranetes VPN
    - dedikált kapcsolat, külső tagokkal, ügyfelekkel

A sávszélesség

- Értéke csak véges lehet
  - Analóg modem vs ADSL
  - Optikai szál …
- A sávszélesség igény változása
  - E-mailek letöltése vs IP TV
  - Előrelátó felmérés és tervezés szükséges
- Költségek
  - Tervezés fontossága
- Alapegység: bps (bit/sec)
  - nagyságrendek: 1 kbps = 1000 bps, stb.
  - Letöltési sebességek Bps-ben megadva

Elméleti korlátok

- Nyquist-tétel (1924)
  - véges sávszélességű, zajmentes csatornára
  - H sávszélességű jel másodpercenként legalább 2H mintavételezéssel állítható helyre
  - max adatsebesség = $2H \log_2 v$ [bps]
  - bináris átvitel távbeszélő csatornán?
- Shannon-tétel (1948)
  - véletlenszerű zajjal terhelt csatornákra
  - max adatsebesség = $H \log_2 (1+S/N)$ [bps]

Az aktuális adatsebesség

- Kisebb mint az átviteli közeg sávszélessége
- Értékét meghatározza:
  - Sávszélesség
  - A hálózat terheltsége (más felhasználók)
  - Az átvitel zavaró tényezői (zajok)
  - Végpontok
    - Kiszolgáló
    - Kliens
  - A hálózatban alkalmazott eszközök
  - A hálózat átviteli közegei
  - Topológia, protokollok, útválasztás …

Hálózati összeköttetések típusai

- Összeköttetés alapú (virtuális áramkör)
  - csomagok állandó útvonalon a forrás és cél között
  - virtuális áramkör az összeköttetés felépítésétől a bontásig
  - a forgalomszabályozás az összeköttetés része
  - pl.: telefon
- Összeköttetés mentes
  - a datagrammok útválasztása egymástól független
  - a csomagok a forrás és a cél teljes címét tartalmazzák
  - egy meghibásodott csomópont nem okoz komoly gondot
  - pl.: e-mail

Kapcsolási módok

- Vonalkapcsolás
  - Az átvitel megkezdése előtt virtuális áramkör épül fel
  - a dedikált csatorna a kommunikáció végéig fennmarad
- Üzenetkapcsolás
  - tárol és továbbít (store and froward) elv
  - az üzenet csak az összes darab megérkezése után kerül továbbításra
- Csomagkapcsolás
  - a meghatározott méretű csomagok önálló egységként kerülnek továbbításra

Hálózati kapcsolat feltételei

- Fizikai kapcsolat
  - hálózati kártya, modem, stb.
- Logikai kapcsolat
  - protokollok ismerete
- Felhasználói programok

A hálózati kártya kiválasztása

- Átviteli közeg
  - Csavart érpár
  - Optikai szál
  - Vezeték nélküli átvitel
  - (Coax)
- Átviteli sebesség
- Szabvány
  - Ethernet
  - (Token Ring, FDDI)

A hálózati kártya csatlakoztatása

- Asztali számítógépek
  - PCI
  - PCI-Express
  - USB
  - (ISA, VLB)
- Hordozható számítógépek
  - Mini-PCI
  - PCMCIA
  - USB

Az információátvitel iránya

- Simplex átvitel
  - egyirányú adatátvitel
  - pl.: rádióadás
- Half duplex átvitel
  - kétirányú átvitel
  - egyszerre csak az egyik irány aktív
  - pl.: CB rádiók
- (Full) duplex átvitel
  - kétirány átvitel minden időpillanatban
  - pl.: telefon

Modemek, modulációk

- **Mo**dulátor - **dem**odulator
- Analóg modemek
  - Analóg jelet modulál a digitális jel függvényében
  - Vételi oldalon pedig demodulálja
- Alapvető modulációk
  - Amplitúdó moduláció (AM)
  - Frekvencia moduláció (FM)
  - Fázis moduláció (PM)
- ISDN modemek

Multiplexelés

- Egy közegen több csatorna párhuzamos átvitele
- Multiplexer - demultiplexer (szinkronizálás!)
- Időosztásos (TDM)
  - a csatornák időben egymás után periódikusan kerülnek átvitelre
  - pl.: E1 távközlési trunk 2 Mbit/s, 30+2 csatorna
- Frekvenciaosztásos (FDM)
  - jellemzően analóg jelek átviteléhez
  - több kisebb sávszélességű jel egymás mellé helyezése
- Hullámhosszosztásos (WDM)
  - optikai szálak kihasználtságának növelésére

Hálózati átviteli közegek

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

Lehetséges átviteli közegek

- Vezetékes átvitel
  - Rézvezeték
    - Coax, UTP, STP
  - Optikai szál
    - Mono- és multi módus
- Vezeték nélküli átvitel
  - Látható vagy nem látható fény
    - IrDA, lézer
  - Rádióhullámok
    - WiFi
  - Optikai vagy mágneses hordozó …

Koaxiális kábelek

- Felépítés
  - Réz (ónozott alumínium) vezető
  - Szigetelés
  - Árnyékolás
  - Külső szigetelés
- Szerelési megoldások
  - "T" csatlakozó
  - Vámpír csatlakozó (a kábel vágása nélkül)
  - Lezárások
- Jellemzők
  - Hullámimpedancia
  - Egységnyi hosszra jutó csillapítás
  - Egységnyi hosszra jutó futási idő

Koaxiális kábelek

- Alapsávi koaxiális kábelek
  - Jellemzően digitális átvitelhez
  - Z=50Ω
  - 10Base2 - vékony koax (thinn coax)
    - Arcnet, Ethernet hálózatok
  - 10Base5 - vastag koax (thick coax)
    - Ethernet hálózatok
- Szélessávú koaxiális kábelek
  - Jellemzően analóg átvitelhez
    - Akár 100 km-es szakaszon 300MHz (450MHz) sávszélesség
    - A teljes szélesség csatornákra osztása
  - Analóg erősítők → szimplex átvitel
    - Egykábeles rendszerek (adás és vétel különböző frekvencián)
    - Kétkábeles rendszerek
  - Z=75Ω

Csavart érpár - UTP és STP

- Felépítés
  - Patch és fali kábelek
  - Érpárok csavarása
  - Külső szigetelés, védelem
- Maximálisan áthidalható távolság: 100 méter
- Maximális sebesség: függ a kategóriától
- Árnyékolás
  - UTP (Unshielded Twisted Pair)
  - ScTP, F(s)TP (Screened UTP, Foil screened Twisted Pair)
  - STP (Shielded Twisted Pair)
- Ár, méret, szerelhetőség, használhatóság …

CAT kábelek jellemzői

	CAT1	CAT2	CAT3	CAT4	CAT5	CAT5e	CAT6	CAT7
Sávszélesség	100 KHz	1,5 MHz	16 MHz	20 MHz	100 MHz	100 MHz	250 MHz	600 MHz
Csillapítás					24 dB	24 dB	21,7 dB (36 dB)	20,8 dB (54,1 dB)
NEXT					27,1 dB	30,1 dB	39,9 dB (33,1 dB)	62,1 dB (51 dB)
PS-NEXT					-	27,1 dB	37,1 dB (30,2 dB)	59,1 dB (48 dB)
ELFEXT					*17 dB*	17,4 dB	23,2 dB (15,3 dB)	
PS-ELFEXT					*14,4 dB*	14,4 dB	20,2 dB (12,3 dB)	
Futási idő					50 nsec	50 nsec	50 nsec	20 nsec
Maximális sebesség	-	4 Mbit/s	16 Mbit/s	20 Mbit/s	100 Mbit/s	1 Gbit/s	1 Gbit/s	10 Gbit/s
Felhasználási terület	Kaputel. csengő	telefon hálózatok	10Base-T	Token Ring	100 Base-T	1000 Base-T	1000 Base-T	Multi-média

Optikai szálak

- A fény terjedésének feltétel az optikai szálakban
  - A mag törésmutatója nagyobb mint a héj törésmutatója
  - A fény beesési szöge nagyobb a mag és a héj határszögénél
  - Ha a fenti feltételek teljesülnek → teljes visszaverődés
  - egyéb esetekben a fény egy része kilép a magból
- Felépítés
  - mag: szilícium-dioxid alapú üveg
  - héj: a maghoz hasonló, de kisebb törésmutatójú anyag
  - védőburkolat: általában műanyag mechanikai védelem
    - laza védőburkolat
    - szoros védőburkolat
  - Teherviselő réteg: kevlár szál (húzás ellen)
  - Köpeny: külső, mechanikai védelem

Többmódusú optikai szálak

- A fénysugarak különböző útvonalon haladnak
- Változó törésmutatójú mag
  - A törésmutató a középpont felől kifelé haladva csökken
  - A külső rész optikai sűrűsége kisebb
  - A fény gyorsabban halad a mag külső részein
  - A különböző fénysugarak egyszerre érnek a szál végére
- Jellemzők
  - Nagyobb magméret: 50 vagy 62,5 mikron (héj: 125 mikron)
  - Kisebb áthidalható távolság: maximum 2 km
  - Általában LED
  - A megengedett veszteség nagyobb

Egymódusú optikai szál

- A fénysugár a szál közepén egyenesen halad
- Jellemzők
  - Kisebb magméret: 9 mikron (héj: 125 mikron)
  - Nagyobb áthidalható távolság: maximum 3 km
  - Általában lézer
  - Kisebb megengedhető veszteség
- Biztonsági kérdések
  - A lézer hullámhossza eshet a látható tartományon kívül
  - Nem ajánlott belenézni:
    - Csatlakoztatott optikai szál végébe
    - Optikai jeleket előállító eszközök adóportjába
    - A használaton kívüli csatlakozókra védősapkát kell tenni

Elektromos jelek átalakítása

- Használható fényforrások
  - LED (infravörös tartományban)
    - Jellemzően többmódusú szálakhoz
    - 850 nm és 1310 nm hullámhossz
  - Lézer
    - Jellemzően egymódusú szálakhoz
    - 1310 nm és 1550 nm hullámhossz
    - nagyobb teljesítmény, nagyobb áthidalható távolság
- Közös jellemzők
  - Gyors ki- és bekapcsolás

Optikai átvitel

- Előnyök a rézvezetékekkel szemben
  - Érzéketlen a külső zavarásokra
  - Nem keletkezik interferencia
  - Nincs áthallás
- Az optikai átvitel problémái
  - Csillapítás
    - Szóródás
    - Abszorpció
    - Diszperzió
    - Kromatikus diszperzió
    - Mag és héj határfelületének tökéletlensége

Szerelési, telepítési problémák

- Apró törések a magban
  - Túlzott erejű húzás vagy hajlítás → szóródás
- Mikrohajlítások
  - A telepítés során fellépő mechanikai hatások
- Makrohajlítások
  - A minimális hajlítási sugár be nem tartása miatt
- Csatlakozók szerelése
  - felületek csiszolás
- Illesztési hibák
  - egyenes csiszolás + légrés
  - eltérő szögű csiszolás, kábelvégek szögben illesztése
  - Kerekre csiszolt kábelvégek
- Csatlakozók tisztán tartása, tisztítása
- Optikai szálak tesztelés

Vezeték nélküli adatátvitel

- Vezeték nélküli átvitelt használó eszközök
  - Kis hatótávolságú adóvevők
  - Kis energiafogyasztás
  - Kis helyigény
- Jól használható megoldás
  - Mobiltelefonokban
  - Kéziszámítógépekben
  - Notebookokban
  - Fejhallgatókban
  - Távirányítókban
  - Nyomtatókban

IrDA

- IrDA (Infrared Data Association)
  - átvitel fény segítségével
  - hatótávolság: kb. 5-10 méter
  - kis teljesítményű verziók hatótávolsága kb. 20 cm
  - adatátviteli sebesség: akár 4 Mbit/s (max.: 1 méter)
  - rádiófrekvenciás zavarásra érzéketlen
  - Kizárólag akadálymentes környezetben használható
  - Csak pont-pont összeköttetésre használható

Bluetooth

- 1998 - IBM, Intel, Nokia, Ericsson, Toshiba
- átvitel rádióhullámok segítségével
  - nem igényel "rálátást"
  - Maximális átviteli sebesség 1 Mbit/s
- frekvenciasáv: 2,4 GHz
  - 2.402GHz - 2.480GHz
  - 79 vivőfrekvencia (1 MHz-es csatornaosztás)
  - 1600 (ál)véletlenszerű frekvenciaugrás másodpercenként
- Mester - szolga (Master - Slave) viszony
  - Időosztásos duplexelés
    - Mester: minden páratlan időrésben adhat
    - Szolga: minden páros időrésben adhat
  - 1 mesterhez maximum 7 szolga tartozhat egyszerre

Bluetooth csomagok

- 1, 3 vagy 5 egymás utáni időrést foglalhatnak el
  - egy időrés 1/1600 = 625µs
- csomagok felépítése
  - Hozzáférési mód (Access Code): 68/72 bit
    - időszinkronizálás, keresés, tudakozódás, felderítés
  - Fejrész (Header): 54 bit
    - csomagazonosítás, csomagszámozás (csomagok újrarendezéséhez), szolga címe, hibaellenőrző bitek
  - Adatrész (Payload): 0 … 2745 bit
    - beszédbitek, adatbitek vagy mindkettő

Bluetooth frekvenciák és teljesítmények

- Frekvenciaugrások
  - 1600 frekvenciaugrás másodpercenként
- Adaptív frekvenciaugrások
  - Bluetooth 1.2 szabványtól kezdve
  - A 802.11b és 802.11g szabványokkal való interferencia elkerülése érdekében
  - Közös frekvenciák kizárása
  - Egy kérdés-válasz alatt a mester és a szolga azonos frekvenciát használ → 800 ugrás másodpercenként
- Eszközök teljesítménye
  - alacsony energiaigény
  - alacsony kimenő teljesítmény
    - Class1: 100 mW
    - Class2: 2,5 mW
    - Class3: 1 mW
  - Élettani hatása elhanyagolható

Bluetooth átviteli módok

- SCO (Szinkron, kapcsolat alapú összeköttetés)
  - szimmetrikus pont-pont összeköttetés (Master-Slave)
  - meghatározott időközönként foglal a mester egy időrést
  - 64 kbit/s mindkét irányban (ált. beszédátvitelhez)
  - nincs csomagismétlés
  - egy mester maximum 3 párhuzamos kapcsolatot tud fenntartani
- ACL (Aszinkron, kapcsolat nélküli összeköttetés)
  - aszimmetrikus pont- több pont közötti összeköttetés
  - azokban az időrésekben használható ahol nincs SCO kapcsolat
  - egyszerre egy aktív ACL kapcsolat lehetséges
  - általában alkalmazzák a csomagok újraküldését
  - maximális átviteli sebesség: 732 kbit/s

Bluetooth állapotok

- Nyugalmi állapot (Standby)
  - alacsony energiafogyasztás
  - csak az óra működik, nincs élő kapcsolat
- Lekérdezés és keresés (Inquiry and Page)
  - Lekérdezés (a környezetben található eszközök detektálása)
  - Keresés - a kapcsolat felépítése az adott eszközzel
- Kapcsolati állapot
  - Aktív mód - ha az eszköz ténylegesen kommunikál
  - Sniff mód
    - a slave csak meghatározott időrésekben figyel
    - a mester csak ezekben az időrésekben üzenhet a szolgának
  - Tartás (Hold) mód
    - a mesterrel egyeztetett ideig a szolga csak az SCO csomagokra figyel
    - az idő lejárta után a szolga feléled, újraszinkronizál és veszi a csomagokat
  - Park mód
    - egy pikohálózatban akár 255 eszköz is lehet virtuálisan
    - ha már van 7 aktív szolga vagy 1 aktív mester, akkor kerülhet park állapotba az eszköz

Vezeték nélküli hálózatok WLAN

- 2000 környékén terjedt el széles körben
- Manapság bizonyos esetekben alternatívája a vezetékes hálózatoknak
- Alacsony ár, egyszerű kiépíthetőség
- Mobil felhasználási lehetőségek
- Széles körű felhasználási lehetőségek
- Hatósugár
  - Épületeken belül akár 100 méter
  - Épületeken kívül akár 300 méter
  - Hatósugár tovább növelhető. Antennák, ismétlők

WLAN szabványok - Home RF

- Legkorábbi szabvány
- Működési frekvencia: 2,4 GHz
- Moduláció: FHSS (Frequency Hopping Spread Spectrum)
- 15 interferencia mentes csatorna
- Zavarásokra kevésbé érzékeny
- Maximális sebesség
  - 1,6 Mbit/s (v 1.2 - 2001-ig)
  - 10 Mbit/s (v 2.0 - 2001 végétől)
- A 802.11b szabvány a 2.0-ás verzió megjelenésekor már népszerűbb volt …

WLAN szabványok
IEEE 802.11b

- Működési frekvencia: 2,4 GHz
- Nem harmonizált, szabadon felhasználható sáv
- Moduláció: DSSS (Direct Sequence Spread Spectrum)
- Maximális sebesség: 11 Mbit/s
  - távolság miatti sebesség visszaesések
    - 5,5 Mbit/s
    - 2 Mbit/s
    - 1 Mbit/s
- 3(+1) interferencia mentes csatorna
- Hatótávolság: akár 100 méter épületen belül
- Bluetooth eszközök, vezeték nélküli telefonok, mikrohullámú sütők esetleg zavarhatják az átvitelt

IEEE 802.11b csatornakiosztás

Csatorna	Vivőfrekvencia	Frekvenciasáv	Amerika	Európa	Izrael	Kína	Japán
1	2412 MHz	2401-2423 MHz	X	X	-	X	X
2	2417 MHz	2406-2428 MHz	X	X	-	X	X
3	2422 MHz	2411-2433 MHz	X	X	X	X	X
4	2427 MHz	2416-2438 MHz	X	X	X	X	X
5	2432 MHz	2421-2443 MHz	X	X	X	X	X
6	2437 MHz	2426-2448 MHz	X	X	X	X	X
7	2442 MHz	2431-2453 MHz	X	X	X	X	X
8	2447 MHz	2436-2458 MHz	X	X	X	X	X
9	2452 MHz	2441-2463 MHz	X	X	X	X	X
10	2457 MHz	2446-2468 MHz	X	X	-	X	X
11	2462 MHz	2451-2473 MHz	X	X	-	X	X
12	2467 MHz	2456-2478 MHz	-	X	-	-	X
13	2472 MHz	2461-2483 MHz	-	X	-	-	X
14	2484 MHz	2473-2495 MHz	-	-	-	-	X

WLAN szabványok
IEEE 802.11a

- Bemutatkozás: 2001 végén
- Működési frekvencia: 5 GHz
- Moduláció: OFDM (Orthogonal Frequency Division Multiplexing)
- Maximális sebesség: 54 Mbit/s
- 12 interferencia mentes csatorna
- Nem kompatibilis visszafelé a 802.11b szabvánnyal
- A nagyobb frekvenciás jelek nehezebben hatolnak át falakon, épületen belüli felhasználást korlátozza
  - Épületen belül jellemzően a max. áthidalható távolság 30m

IEEE 802.11a csatornakiosztás

Csatorna	Vivőfrekvencia	Frekvenciasáv	Amerika	Japán	Szingapúr	Taiwan
34	5170 MHz	5160-5180 MHz	-	X	-	-
36	5180 MHz	5170-5190 MHz	X	-	X	-
38	5190 MHz	5180-5200 MHz	-	X	-	-
40	5200 MHz	5190-5210 MHz	X	-	X	-
42	5210 MHz	5200-5220 MHz	-	X	-	-
44	5220 MHz	5210-5230 MHz	X	-	X	-
46	5230 MHz	5220-5240 MHz	-	X	-	-
48	5240 MHz	5230-5250 MHz	X	-	X	-
52	5260 MHz	5250-5270 MHz	X	-	-	X
56	5280 MHz	5270-5290 MHz	X	-	-	X
60	5300 MHz	5290-5310 MHz	X	-	-	X
64	5320 MHz	5310-5330 MHz	X	-	-	X
149	5745 MHz	5735-5755 MHz	-	-	-	-
153	5765 MHz	5755-5775 MHz	-	-	-	-
157	5785 MHz	5775-5795 MHz	-	-	-	-
161	5805 MHz	5795-5815 MHz	-	-	-	-

WLAN szabványok
IEEE 802.11g

- 2003-ban elfogadott szabvány
- Működési frekvencia: 2,4 GHz
- Moduláció: OFDM (Orthogonal Frequency Division Multiplexing)
- Maximális sebesség: 54 Mbit/s
- 3 interferencia mentes csatorna
- Kompatibilis visszafelé a 802.11b szabvánnyal
- Bluetooth eszközök, vezeték nélküli telefonok, mikrohullámú sütők esetleg zavarhatják az átvitelt

IEEE 802.11g csatornakiosztás

Csatorna	Vivőfrekvencia	Frekvenciasáv	Amerika	Európa	Izrael	Kína	Japán
1	2412 MHz	2401-2423 MHz	X	X	-	X	X
2	2417 MHz	2406-2428 MHz	X	X	-	X	X
3	2422 MHz	2411-2433 MHz	X	X	X	X	X
4	2427 MHz	2416-2438 MHz	X	X	X	X	X
5	2432 MHz	2421-2443 MHz	X	X	X	X	X
6	2437 MHz	2426-2448 MHz	X	X	X	X	X
7	2442 MHz	2431-2453 MHz	X	X	X	X	X
8	2447 MHz	2436-2458 MHz	X	X	X	X	X
9	2452 MHz	2441-2463 MHz	X	X	X	X	X
10	2457 MHz	2446-2468 MHz	X	X	-	X	X
11	2462 MHz	2451-2473 MHz	X	X	-	X	X
12	2467 MHz	2456-2478 MHz	-	X	-	-	X
13	2472 MHz	2461-2483 MHz	-	X	-	-	X
14	2484 MHz	2473-2495 MHz	-	-	-	-	X

2,4 GHz vs. 5 GHz

- Felhasználás földrajzi helye
- Teljesítőképesség
  - 802.11a - 12 db. nem átlapolódó 20 MHz széles csatorna
  - 802.11b/g - 3 db. független csatorna, 80 MHz teljes sávszélesség
- Épületméret
- Rádiófrekvenciás interferencia
- Kompatibilitás
- Biztonság (elérhetőség épületen kívül)

WLAN eszközök - Rádió modem

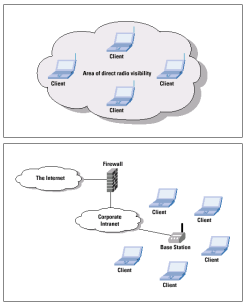
- Rádió modem
  - Feladatok
    - moduláció, jeltovábbítás
    - jelek vétele, demoduláció
  - Részei: antenna, erősítők, frekvencia szintézerek és szűrők
  - Főbb jellemzői: frekvenciasáv, jelzéssebesség, moduláció, kimenő teljesítmény
- MAC (Message Authentication Code) kontroller
  - Feladatok
    - csatorna hozzáférés
      - TDMA - időosztásos többszörös elérés
      - CSMA/CA - vivő érzékelő többszörös elérés / ütközés elkerülés
      - MAC lekérdezés
    - hálózatmenedzsment

WLAN hardver elemek

- Rádiófrekvenciás hálózati kártyák
  - Fizikai réteg: 802.11a, 802.11b/g, 802.11a/b/g
  - Csatlakoztatás: PCI, mini PCI, PCMCIA, CF, USB
- Hozzáférési pontok
  - Rádiófrekvenciás + vezetékes hálózati kártya
  - Általában HTTP protokollon keresztül konfigurálható
- WLAN Routerek
  - Többportos Ethernet router + hozzáférési pont
  - Jellemző szolgáltatások: NAT, DHCP, Firewall, Repeater
- Ismétlők (repeater)
  - Hatósugár kiterjesztése jelformázással és erősítéssel
  - Összes keret újraküldése azonos csatornán, duplázódó forgalom
- Antennák
  - Körsugárzó vagy irányított antennák
  - Csatlakoztatási lehetőségek az eszközökön
  - Előírt kimenő teljesítmény

WLAN topológiák

- Ad-hoc hálózatok
  - két vagy több kliens összekapcsolása egymással
  - nincs kiemelt elem
- Menedzselt vagy infrastrukturális hálózatok
  - a kliensek egy kiemelt elemen (AP) keresztül kapcsolódnak
  - A forgalom szűk keresztmetszete lehet az AP
  - Lehetőség van hitelesítésre, forgalom szűrésre, a hozzáférések kontrollálására



http://www.isoc.org

Rétegszemlélet
OSI és TCP/IP modell

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

Hálózati architektúrák céljai

- Összekapcsolhatóság
  - Eltérő hardver és szoftver elemek → egységes hálózat
- Egyszerű implementálhatóság
  - A felhasználók igényeit lefedő általános megoldás
- Használhatóság
  - A felhasználók hatékony kiszolgálása
  - A valós megoldások elrejtése a felhasználók elől
- Megbízhatóság
  - Hibák felismerése és javíthatósága
- Modularitás, bővíthetőség
  - Felhasználói vagy technológiai igény esetén

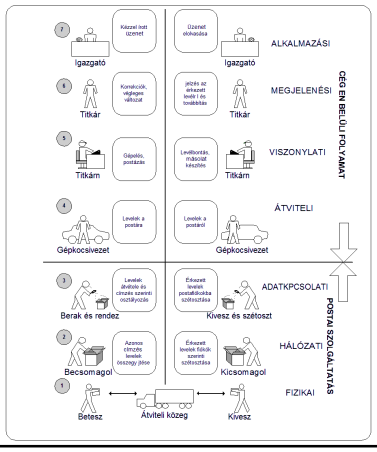
Rétegszemlélet

- A teljes architektúra komplex feladatokat lát el
- A feladatok csoportosítása → rétegek
  - Specifikus funkcióhalmaz (functions)
  - Specifikus szolgáltatási halmaz (services)
- Interfészek a rétegek között
  - Adott csomópontban a szomszédos rétegek között
  - Több csomópont azonos rétegei között
- Előnyök
  - Modularitás
  - Eltérő hardver és szoftver alkalmazhatósága

Rétegekkel szembeni követelmények

- Minden réteg jól elkülönülő önálló feladatot lát el
- A rétegek egymástól függetlenek
- A rétegek egymásra épülnek
  - Minden réteg az alsóbb rétegek információt használja
  - Minden réteg a felsőbb rétegek számára nyújt szolgáltatásokat
- A hosztok azonos rétegei egymással kommunikálnak
- A kommunikáció az interfészeken valósul meg
- A kommunikációhoz a protokollokat használják
  - protokoll verem (protocoll stack)

Egy postai levelezés rétegekre bontása



Szolgálatok

- Szolgáltatások csoportosítása
  - Összeköttetés alapú
    - Megbízhatatlan kapcsolat (telefon)
    - Megbízható adatfolyam (SSH)
  - Összeköttetés mentes
    - Nem megbízható datagrammok (UDP)
    - Megbízható (nyugtázott) datagrammok (TCP)
    - Kérés - válasz alapú szolgáltatások (adatbázisok)
- Leírja, hogy milyen műveletek hajthatók végre
  - Nem írja le az implementáció módját → protokoll

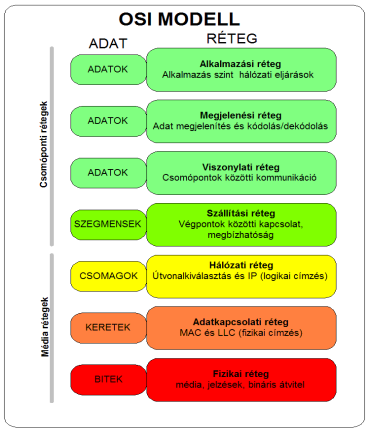
Szolgálatprimitívek

- Szolgálat típusok
  - Megerősített (confirmed)
  - Megerősítetlen (unconfirmed)
- Osztályok
  - Megerősített
    - Listen (blokkolt várakozás bejövő kapcsolatfelvételre)
    - Connect (összeköttetés létrehozása egy várakozó entitással)
    - Receive (blokkolt várakozás bejövő üzenetre)
    - Send (üzenet küldése)
    - Disconnect (összeköttetés bontása)
  - Megerősítetlen
    - Receive (blokkolt várakozás bejövő üzenetre)
    - Send (üzenet küldése)

Az OSI hivatkozási modell

- Nem hálózati architektúra → hivatkozási modell
- Általános, oktatásra alkalmas modell
- A rétegekhez kapcsolódó feladatok ma is fontosak
- A hozzá kapcsolódó protokollok már jellemzően nem használtak
- A rétegekre osztás szempontjai
  - A rétegek különböző absztrakciós szinteket képviseljenek
  - Minden réteg jól definiált feladatot hajtson végre
  - A rétegek feladatait a szabványos protokollokhoz kell igazítani
  - A rétegek közötti információcsere minimális legyen
  - A rétegek száma úgy legyen kialakítva, hogy:
    - eltérő feladatok ne kerüljenek azonos rétegbe
    - ne jelenjen meg kezelhetetlenül sok réteg

Az OSI modell rétegei



A fizikai réteg

- Bitek továbbítása a kommunikációs csatornán
- Feszültségszintek
  - Logikai magas szint
  - Logikai alacsony szint
- Időzítések
- Modulációk, bitek kódolása
- Csatlakozók
  - Típus, kialakítás
  - Csatlakozó pontok
- Tervezés feladatai: mechanikai, elektromos tervezés

Az adatkapcsolati réteg

- A fizikai átviteli hibáinak elfedése a hálózati réteg elől
- Keretezés
  - Adatfolyam tördelése
  - Küldés sorrendben
  - Nyugtázás (megbízható szolgáltatás)
  - Kerethatárok felismerése
- Forgalomszabályozás
  - Elárasztás elleni védelem (felsőbb rétegekben is)
  - Adó tájékoztatása a vevő szabad puffereiről
- Összeköttetés iránya (szimplex, fél duplex, duplex)
- Osztott csatornához való hozzáférés szabályozása

A hálózati réteg

- A csomag útja a forrástól a célig
  - Statikus útvonalak
  - Dinamikus útvonalak
    - Az aktuális terhelést figyelembe véve
- Csomóponti torlódás szabályozás
- A szolgáltatás minősége
- Egymástól eltérő hálózatok összekapcsolása
  - Eltérő címzési módok
  - Eltérő csomagméretek …

A szállítási réteg

- Adatok fogadása a viszony rétegtől
- Szegmentálás
- Szegmensek továbbítása a hálózati rétegnek
- Biztosítja a hibamentes átvitelt
  - Elrejti a felsőbb rétegek elől az átvitel problémáit
- Tényleges kommunikáció a végpontok között

A viszonyréteg

- Két gép közti viszony (session) létrehozására
  - pl. bejelentkezés egy alkalmazásba
- Párbeszédirányítás
- Vezérjel kezelés
- Szinkronizáció

A megjelenítési réteg

- Az átvitt információhoz kapcsolódó szintaktikai kérdések
- Az átvitt információhoz kapcsolódó szemantikai kérdések
- Regionális szempontok
- Karakterkódolások (pl.: ASCII, UniCode)

Az alkalmazási réteg

- Célja a felhasználó kiszolgálása
- Protokollok gyűjteménye

A TCP/IP hivatkozási modell

- Az ARPANET problémái
- Tervezési szempontok
  - Különböző hálózatok összekapcsolása
  - Redundáns, hibatűrő hálózat
  - Széles körben alkalmazható, rugalmas hálózat

A hoszt és hálózat közötti réteg

- Nem definiálja az internet réteg alatti réteg pontos feladatait
- A hosztnak olyan hálózathoz kell csatlakoznia amely IP csomagok továbbítására alkalmas protokollal rendelkezik
- Ez a protokoll eltérő lehet hosztonként vagy hálózatonként

Az internetréteg

- Összeköttetés nélküli internetwork réteg
- Az OSI modell hálózati rétegének felel meg
  - IP csomagok kézbesítése
  - Csomagok útvonalának meghatározása
  - Torlódásvédelem
- Szabványos csomagformátum és protokoll
  - Internet Protocol (IP)
- Képes legyen bármilyen hálózatba csomagot küldeni
- Képes legyen csomagokat továbbítani egy másik hálózatba

A szállítási réteg

- Feladata az OSI szállítási rétegéhez hasonló
- Forrás és cél közti párbeszéd biztosítása
- Szállítási protokollok
  - Átvitelvezérlő protokoll (TCP)
    - megbízható, összeköttetés alapú protokoll
    - hibamentes bájtos átvitel két gép között
    - forgalomszabályozás (elárasztás ellen)
  - Felhasználói datagram protokoll (UDP)
    - nem megbízható, összeköttetés nélküli protokoll
    - kliens-szerver típusú kérés-válasz (egylövetű)
    - ahol a gyors válasz fontosabb a pontos válasznál

Az alkalmazási réteg

- Az OSI alkalmazási rétegéhez hasonló
- Nincs viszony és megjelenítési réteg
- Eredetileg a következő protokollokat tartalmazta
  - Virtuális terminál (Telnet)
  - Fájltranszfer (FTP)
  - Elektronikus levelezés (SMTP)
- Manapság számos további protokollt tartalmaz
  - Domain Name Service (DNS)
  - Hyper Text Transfer Protocol (HTTP)
  - Network News Transfer Protocol (NNTP)

Az OSI modell értékelése

- Rossz időzítés
  - Szabványok megalkotásának időzítése
    - A két elefánt apokalipszise (David Clark)
- Rossz technológia
  - A rétegek száma és elosztása hibás
    - a viszony és megjelenítési réteg szinte üres
    - az adatkapcsolati és hálózati túltelített
  - Igen bonyolult szabványú szolgálatok és protokollok
- Rossz implementálás
  - A kezdeti bonyolultság mindenkinek elvette a kedvét
- Rossz üzletpolitika
  - Az OSI-tkormányok, minisztériumok alkotásának tekintették
  - A TCP/IP-t a UNIX részének tekintették (kezdeti implementáció)

A TCP/IP modell értékelés

- Nem tesz egyértelmű különbséget a szolgálat, protokoll és interfész között
- Nem tekinthető általános érvényű modellnek
  - Nem alkalmas új technológiákon alapuló hálózatok tervezéséhez
- A hoszt és hálózat közötti alréteg nem tekinthető valódi rétegnek
- Nincs adatkapcsolati és fizikai réteg
  - közegek átviteli jellemzői
  - keretezés
- Jól implementált, átgondolt TCP és IP protokollok
  - ad-hoc jellegű kiegészítő protokollok
- Széles körben elterjed és implementált (ingyenes) protokollok
  - Mélyen a rendszerbe épülve, nehezen változtatható
  - TELNET …

Az OSI és a TCP/IP modell összehasonlítása

- OSI
  - Tapasztalatlan tervezők
  - Modellhez protokollok
    - kellően általános modell maradhatott
    - nem befolyásolják protokollkészletek
  - Elemzésre, oktatásra alkalmas modell
  - Protokolljai ma már nem életképesek
- TCP/IP
  - Protokollokhoz modell
  - Csak az adott protokollokkal életképes
  - Gyakorlatban nem létező modell
  - Elterjedt, használható protokollok

A fizikai réteg és eszközei

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

A fizikai réteg

- Bitek továbbítása a kommunikációs csatornán
- Feszültségszintek
  - Logikai magas szint
  - Logikai alacsony szint
- Időzítések
- Modulációk, bitek kódolása
- Csatlakozók
  - Típus, kialakítás
  - Csatlakozó pontok
- Tervezés feladatai: mechanikai, elektromos tervezés

Lehetséges átviteli közegek

- Vezetékes átvitel
  - Rézvezeték
    - Coax, UTP, STP
  - Optikai szál
    - Mono- és multi módus
- Vezeték nélküli átvitel
  - Látható vagy nem látható fény
    - IrDA, lézer
  - Rádióhullámok
    - WiFi
  - Optikai vagy mágneses hordozó …

Repeater

- A szabvány maximális hosszánál nagyobb szakaszok kialakítása
- Kizárólag a fizikai rétegben működik
  - Jelek vétele
  - Regenerálás
  - Továbbküldés
- A felsőbb rétegek és a szoftverek számára egy kábelszakasznak látszik a szegmens
- Azonos közegek összekapcsolására szolgál
- Késleltetés
- Wireless repeaters
  - Repeater + AP
  - Egységes WLAN hálózat

HUB (koncentrátor)

- Többportos ismétlő
- Jellemzően 8, 16, 24 port
- 10Base-T, esetleg 100Base-T hálózatokban
- Csillag topológia
- Típusok
  - Passzív
    - az átviteli közeg megosztása
    - nem regenerálja a jelet
  - Aktív
    - a regenerált jele küldik ki minden portjukra
  - Intelligens
    - aktív + hibakereső funkciók
- Ütközések …

Média konverter

- Különböző átviteli közegek illesztése
  - Csavart érpár ↔ optikai szál
  - Soros vonal ↔ optikai szál
  - RS232 ↔ RS422
  - …
- Optikai leválasztó eszközök

Általános felhasználó igények

- Otthon vagy kisebb irodákban
  - Gépek hálózatba kapcsolása (Switch)
    - Gépek hálózatba kapcsolása vezeték nélkül (WLAN)
  - Átjáró biztosítása a kimenő kapcsolatok számára (Router)
  - Hálózati kapcsolat megosztása (NAT)
  - A belső hálózat védelme (Firewall)
  - Hálózati nyomtató használata (Printserver)
- DSL routerek
  - Nem csak a fizikai réteghez köthetők!

Szinkron átvitel

- Adatátvitel előre meghatározott ütemben
- A bitek kezdete és hossza időben szigorúan kötött
- Szinkronizáció, szinkronjel
  - Közös szinkronjel használatával
  - Szinkronizáló bitek átvitelével az adatok előtt
    - Olyat kell választani ami az adatok között nem fordulhat elő
    - Jellemzően a logikai alacsony és magas szint váltakozása
    - A vevő a jelet használva képes saját ütemezését beállítani
- Ha nincs adatforgalom
  - A szinkront meg kell tartani, a kommunikáció nem áll le

Aszinkron átvitel

- Nincs folyamatos adatátvitel
- Nincs közös szinkron vagy folyamatos szinkronizálás
- Az adó és a vevő összhangban kell, hogy működjön
- Keretező információk szükségesek
  - A hasznos információ keretbe foglalása
    - START bit(ek)
    - STOP bit(ek)
- Átviteli hibák jelzése
  - Paritás bit(ek)

Az átvitel paraméterei

- Start bit
- Adatbitek: 5, 6, 7 vagy 8 bit
- Paritás (ha használunk)
  - Páros
  - Páratlan
- Stop bit(ek)
  - 1 stop bit - elégséges a következő start bit felismeréséhez
  - 2 stop bit - időt biztosít az adatbitek feldolgozásához
- Adatátviteli sebesség [bit/s]
  - bit/s ≠ Baud

Aszinkron soros átvitel

- Számítógép és modem közti átvitel
- Pont-pont közti duplex átvitelt igényel
- EIA RS-232-C (CCITT V.24)
- Számítógép vagy terminál
  - adatvég-berendezés
  - DTE (Data Terminal Equipment)
- Modem
  - adatberendezés (adatáramköri-végberendezés)
  - DCE (Data Circuit-terminating Equipment)
  - Illesztés a fizikai közeghez

RS-232-C

- Mechanikai megvalósítás
  - 25 tűs D-CANNON csatlakozó
  - DTE - "apa" csatlakozó
  - DCE - "anya" csatlakozó
- Villamos megvalósítás
  - -3V -nál alacsonyabb jelszint (-12V) → bináris 1
  - +3V -nál magasabb jelszint (+12V) → bináris 0
  - Kábelhossz: max 15 méter
  - Sebesség: 20 kbit/s

RS-232-C átviteli vonalak

- DTE ↔ DCE (1) védőföldelés
- DTE → DCE (2) adás (TxD)
- DTE ← DCE (3) vétel (RxD)
- DTE → DCE (4) adáskérés (RTS)
- DTE ← DCE (5) adásra kész (CTS)
- DTE ← DCE (6) adat kész (DSR)
- DTE ↔ DCE (7) jelföldelés
- DTE ← DCE (8) vivőérzékelés (CD)
- DTE → DCE (9) adatterminál kész (DTR)

Adat és vezérlőinformációk

- Sávon belüli jelzésátvitel
  - A hasznos adatok és jelzések közös sávban
  - Fenntartott sávok a jelzéseknek
  - Átviteli problémák …
- Sávon kívüli jelzésátvitel
  - 1976 AT&T CCIS nevű csomagkapcsolt hálózat
  - Az analóg átvitel kezelése is külön csatornán
  - A hálózat részei:
    - analóg nyilvános vonalkapcsolt hálózat (hangátvitel)
    - CCIS hálózat (hangátvitel vezérlése)
    - Csomagkapcsoló hálózat (adatátvitel)

ISDN

- Számos hagyományos és új szolgáltatás
- Átvitel egy digitális bitcső segítségével
  - Kétirányú kommunikáció, független csatornákon
  - Időosztásos multiplexelés
- Bitcső szabványok
  - ISDN-2 (2B+D)
  - ISDN-30 (30B+1D)
- Csatornatípusok
  - A - analóg csatorna (4 kHz)
  - B - digitális csatorna (PCM) hang és adatátvitelre (64 kbit/s)
  - C - digitális csatorna (8 kbit/s vagy 16 kbit/s)
  - D - digitális csatorna a sávon kívüli jelzésre (16 kbit/s v. 64 kbit/s)
- Hibajavítás nincs, az ISDN bites átvitelt valósít meg

ATM

- Célja a B-ISDN
- 53 bájtos cellák (keretek)
  - 48 hasznos bájt
  - Hatékony berendezésoriántált áramkörök
    - routereknél nagyobb hatékonyság
- Aszinkron, csomagkapcsolt átvitel
- Statisztikus multiplexelés
- Leggyakoribb sebességek
  - STS-1 51,84 Mbit/s
  - STS-3c/STM-1 155,52 Mbit/s
  - STS12c/STM-4 622,08 Mbit/s

Az adatkapcsolati réteg

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

Az adatkapcsolati réteg

- A fizikai átviteli hibáinak elfedése a hálózati réteg elől
- Keretezés
  - Adatfolyam tördelése
  - Küldés sorrendben
  - Nyugtázás (megbízható szolgáltatás)
  - Kerethatárok felismerése
- Forgalomszabályozás
  - Elárasztás elleni védelem (felsőbb rétegekben is)
  - Adó tájékoztatása a vevő szabad puffereiről
- Összeköttetés iránya (szimplex, fél duplex, duplex)
- Osztott csatornához való hozzáférés szabályozása

Az adatkapcsolati réteg

- Tervezési szempontok
  - Jól definiált interfész biztosítása a hálózati rétegnek
  - Az átviteli hibák kezelése
  - Az adatforgalom szabályozása
- Megvalósítás: Keretezés
  - A hálózati réteg csomagjainak keretbe foglalása
    - keret fejrész
    - adatmező
    - keret farokrész

Szolgáltatások típusai a hálózati réteg felé I.

- Nyugtázatlan összeköttetés mentes szolgálat
  - Egymástól független keretek küldése a forrástól a célig
  - Nincs előzetes kapcsolatépítés és bontás
  - Az elveszett kereteket nem állítja helyre a réteg
  - Alkalmazhatóság
    - Alacsony hibaarány esetén (javítás a felsőbb rétegekben)
    - Valós idejű adatforgalom esetén (hangátvitel)
- Nyugtázott összeköttetés mentes szolgálat
  - Szintén nincs előzetes kapcsolatépítés és bontás
  - Minden egyes keret megérkezését nyugtázza a cél állomás
  - Alkalmazhatóság
    - Pl.: vezeték nélküli kapcsolatoknál

Szolgáltatások típusai a hálózati réteg felé II.

- Nyugtázott összeköttetés alapú szolgálat
  - Összeköttetés felépítése az adatátvitel előtt
  - Sorszámozott keretek
    - minden keret garantáltan megérkezik
    - minden keret garantáltan egyszer érkezik meg
    - minden keret a megfelelő sorrendben érkezik meg
  - Az átvitel folyamata
    - összeköttetés felépítése (számlálók, változók inicializálása)
    - keret(ek) továbbítása
    - összeköttetés bontása (számlálók, változók felszabadítása)

Keretezés

- A fizikai réteg nem garantál hibamentes átvitelt
- A réteg feladata ezen hibák jelzése, javítása
- Keretezés
  - Az adatfolyam feldarabolása kisebb részekre (keret)
  - Ellenőrző összegek számítása minden kerethez
- Az átvitel ellenőrzése
  - A fogadott adatok alapján az ellenőrző összeg kiszámítása
  - A fogadott és az újraszámolt összeg összehasonlítása
- A kerethatárok jelölésének problémái
  - Szünetek beszúrása az egyes keretek közé?

A kerethatárok jelölése - Karakterszámlálás

- Minden keret fejrészében megadásra kerül a keret karaktereinek száma
  - A vevő a fejrészből tudja, hány karakter tartozik a kerethez
  - Illetve, hogy hol lesz a keret vége (a következő eleje)
- Problémák:
  - A karakterszám mezőt is érheti átviteli hiba
    - A vevő kiesik a szinkronból, nem találja a következő keretet
    - Hibás ellenőrző összeg → hibás keret
      - de hol kezdődik a következő keret?
    - Az újraküldés sem megoldás

Kezdő- és végkarakterek karakterbeszúrással

- A kerethatárok jelzése egy különleges karakterrel
  - Régebben eltérő protokollok eltérő bájtot használtak
  - Manapság egységes "jelző bájt" (flag byte) jellemző
- Ha a vevő kiesik a szinkronból csak megvárja a következő flag byte-ot
  - Az első flag byte az adott keret vége
  - A második flag byte a következő keret eleje
- Mi történik ha a flag byte-nak megfelelő karaktert akarunk átvinni? (bináris átvitel)
  - Kivétel bájt (escape byte) beszúrása
- És ha escape byte-ot kell átvinni?

Kezdő- és végjelek bitbeszúrással

- A karakterkódok hossza ne legyen része a keretezésnek
- Tetszőleges számú bit legyen átvihető egy keretben
- Flag byte: 01111110
- Az adó minden ötödik 1-es után beszúr egy 0-t
- A vevő minden ötödik 1-es után törli a követő 0-t
- A jelző bájt is probléma nélkül átvihető
  - Adási oldal: 01111110 → 011111010
  - Vételi oldal: 011111010 → 01111110
- Transzparens átvitel mindkét irányban
- Adatfolyam az adó oldalán: 0110111111011111111111010101
- Átviteli vonal: 0110111110101111101111101 1010101
- Adatfolyam a vevő oldalán: 0110111111011111111111010101

Fizikai rétegbeli kódolássértés

- Alkalmazható ha a fizikai réteg kódolása redundáns
- Például ahol egy bit kódolása is jelváltással történik
  - Előnyös:
    - a vevő könnyen felismeri a bithatárokat
    - Nincsenek szinkronizációs problémák
  - Logikai magas szint: magas → alacsony jelváltás
  - Logikai alacsony szint: alacsony → magas jelváltás
  - Nincs magas → magas vagy alacsony → alacsony átmenet
    - Ezek használhatók a kerethatárok jelzésére
- A gyakorlatban több megoldás kombinációja használt

Forgalomszabályozás

- A lassabb (terhelt) gép védelme elárasztás ellen
  - A túlterhelés keretek elvesztéséhez vezet
- Visszacsatolás alapú forgalomszabályozás
  - A vevő tájékoztatja az adót a pillanatnyi állapotáról
  - A vevő engedélyezi az adónak a további küldést
  - Az adatkapcsolati réteg jellemző megoldása
- Sebesség alapú forgalomszabályozás
  - A protokoll tartalmazza a sebességkorlátozást
  - Ez minden adóra nézve kötelező érvényű

Hibakezelés

- Lehetséges problémák
  - Megérkezett-e minden keret?
  - Minden keret csak egyszer érkezett-e meg?
  - A keretek megfelelő sorrendben érkeztek-e meg?
- Visszacsatolás szükséges a vevő felől
  - Pozitív és negatív nyugták
  - Ha nem érkezik meg a keret?
    - Időzítők alkalmazása
- Keretek újraküldése
  - Többször megérkezhet ugyanaz a keret
  - Kimenő keretek sorszámozása

Egybites és csoportos hibák

- Egybites hibák
- Csoportos hibák
  - Bizonyos közegek esetén sokkal gyakoribb
  - Azonos hibaarány mellett kevesebb hibás keret
  - Jelzése és javítása lényegesen nehezebb
- Példa:
  - 1 adatblokk legyen 1000 bit, a hibaarány = 0,1%
  - Független hibák esetén átlagban minden keret hibás lesz
  - 100 bites csoportos hibáknál 100-ból 1-2 keret lesz hibás

Hibajelző és hibajavító kódok

- Hibajelző kódok
  - Csak a hibás átvitel tényét jelzi → újraküldés
  - Alacsony hibaarány mellett lehet praktikus
- Hibajavító kódok
  - A hibás adatokból helyreállítható a helyes üzenet
  - Alkalmas lehet bizonytalan átviteli közegek esetén
- Redundancia
  - *m* - adatbitek
  - *r* - redundáns bitek
  - *n* = *m* + *r* (teljes keret - *n* bites kódszó)

Hamming-távolság

- Azonos helyen előforduló különböző bitek (XOR)
- Teljes kód Hamming-távolsága
- *d* számú hiba jelzéséhez *d*+1 Hamming-távolságú kód szükséges
- *d* számú hiba javításához 2*d*+1 Hamming-távolságú kód szükséges
- Paritásbit alkalmazása
  - Hamming-távolság: 2
  - Alkalmas 1 bites hibák jelzésére

Hibajavító Hamming-kód

- Az üzenet bitjeit balról jobbra 1-től számozzuk
- 2 egész számú hatványai lesznek az ellenőrző bitek
- Az egyéb bitek az adatbitek

1	2	3	4	5	6	7	8	9	10	11
1	2	1,2	4	1,4	2,4	1,2,4	8	1,8	2,8	1,2,8

- Minden paritás számításában azok a bitek vesznek részt amelyekben kettő adott hatványa szerepel
- Például
  - 1-es paritásbit: 3, 5, 7, 9, 11 bitek
  - 4-es paritásbit: 5, 6, 7 bitek

Hamming-kód példa

1	2	3	4	5	6	7	8	9	10	11
1	2	1,2	4	1,4	2,4	1,2,4	8	1,8	2,8	1,2,8

- Kódolandó bitek: 1100101

1	2	3	4	5	6	7	8	9	10	11
0	0	1	1	1	0	0	0	1	0	1

- Hiba az átvitel során a 6-os számú biten

1	2	3	4	5	6	7	8	9	10	11
0	0	1	1	1	**1**	0	0	1	0	1

- Történt-e átviteli hiba? Hányadik bit a hibás?

Csoportos hibák javítása Hamming-kóddal

- Alapesetben egy bit javítható, csoportos hiba nem
- Rendezzünk *k* darab kódszót egymás alá
- Az átvitel ne kódszavanként és azon belül bitenként
- Hanem oszloponként, azon belül bitenként végezzük
- *k* bitnyi csoportos hiba esetén
  - Minden kódszóban csak egy bitnyi hiba lesz
  - Minden kódszó javítható
- Ellenőrző bitek száma = *kr*
- Adatblokk mérete = *km*
- *k* hosszúságú csoportos hiba javítható!

CRC hibaellenőrzés

- CRC - Cyclic Redundancy Code
  - Polinom kód
- A leggyakrabban alkalmazott megoldás hibajelzésre
- A bitsorozatokat polinomoknak tekintjük
  - pl.: 10011001 → $x^7+x^4+x^3+1$ → hetedfokú polinom
- Műveletek
  - Összeadásnál, kivonásnál nincs átvitel → XOR
  - Osztás: mint a bináris osztás
    - A kivonásnál nincs átvitel
    - Az osztó megvan az osztandóban ha az osztandó ugyanannyi bitet tartalmaz mint az osztó

CRC hibaellenőrzés

- Továbbítandó keret: M(x)
- Generátor polinom G(x)
  - Az adónak és a vevőnek is ismerni kell
  - A legfelső és legalsó bitnek 1-nek kell lennie
  - Rövidebbnek kell lennie mint a továbbítandó keretnek
- Feladat: fűzzünk ellenőrző összeget a kerethez, hogy az így kapott keret (polinom) osztható legyen G(x)-el
- Átvitel ellenőrzése: a vevő elosztja a vett keretet a generátorral, ha van maradék akkor hibás az átvitel

CRC ellenőrző összeg számítása

- Legyen r $G(x)$ foka. Fűzzünk r darab 0 értékű bitet a keret alacsony helyi értékű végéhez → $x^rM(x)$ amely $m + r$ bitből áll.
- Osszuk el a az így kapott keretünket [$x^rM(x)$] a generátor $G(x)$ bitsorozatával.
- Vonjuk ki a maradékot a bővített keretből így megkapjuk az ellenőrző összeggel ellátott továbbítandó keretet → $T(x)$

A CRC erőssége

- Minden egybites hibát képes jelezni
- Két izolált egybites hiba is jelezhető
  - G(x) nem oszthatja $x^k + 1$ -et, ahol k<kerethossz
  - Alacsony fokszámú polinomok, hosszú keretek védelmére
    - Pl.: $x^{15} + x^{14} + 1$ nem osztja $x^k + 1$-et ha k<32768
- Minden páratlan számú hibás bitet tartalmazó hiba felismerhető
  - ha $G(x)$ osztható $x + 1$ -gyel
- Minden r ellenőrző bittel ellátott polinomkód minden maximum r hosszúságú csoportos hibát tud jelezni

Néhány klasszikus CRC polinom

- CRC12 = $x^{12} + x^{11} + x^2 + x^1 + 1$
  - 6 bites karakterek kódolására
- CRC16 = $x^{16} + x^{15} + x^2 + 1$
  - 8 bites karakterek kódolására
  - Képes felismerni:
    - 1 bites hibák, 2 bites hibák
    - Páratlan hibás bitet tartalmazó hibák
    - 16 vagy kevesebb bitet tartalmazó csoportos hibát
    - 17 bites csoportos hibák 99,997%-át
    - 18 vagy nagyobb bitszámú csoportos hibák 99,998%-át
- CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
  - 8 bites karakterek kódolására (CCITT ajánlás)

CRC problémák?

- Bonyolult algoritmus az ellenőrző összeg számításához?
  - Áramkörileg egyszerűen megvalósítható
    - léptető regiszteres áramkör - Peterson és Brown
  - Gyakorlatilag szinte minden LAN használja
- Véletlenszerű-e a keretek tartalma?
  - Eredeti feltételezés: igen
  - Partridge és társai (1995)
    - Valós adatok elemzése
    - Alaptalan az eredeti feltevés, nem teljesen véletlenszerű
    - Gyakoribbak lehetnek a felderítetlen hibák

Ethernet alapismeretek

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

A közegelérési alréteg

- Az adatkapcsolati réteg alsó alrétege
- MAC (Media Access Control)
- Egyetlen közös csatorna
  - Többszörös elérési csatorna (multiaccess channel)
- Statikus csatornakiosztás
  - Például FDM
    - Hatékony lehet alacsony számú felhasználónál
    - Nem működik változó felhasználószám, lökésszerű terhelés esetén

Dinamikus csatornakiosztás

- Állomás modell
  - *N* darab független állomás feltételezése (terminál)
  - Egy keret generálása után az állomás blokkolt marad a keret továbbításáig
- Egyetlen csatorna feltételezése
  - Az összes kommunikációhoz egyetlen közös csatorna áll rendelkezésre
  - Az állomások képesek ezen adatot küldeni és fogadni
- Ütközések feltételezése
  - Két keret egy időben nem továbbítható (ütközés)
  - Az ütközést minden állomás képes érzékelni
  - Az ütközésen kívül más hiba nem történhet

Dinamikus csatornakiosztás

- Küldés időzítése
  - Folytonos idő: egy keret bármelyik időpillanatban elküldhető
  - Diszkrét idő: egy keret továbbítása mindig csak egy időrés elején kezdődhet
- Vivőjel érzékelés
  - Vivőjel érzékeléses hálózat esetén az állomás küldés előtt képes megvizsgálni a csatorna foglaltságát
    - Elképzelhető-e ilyenkor ütközés?
  - Ha nincs vivőjel érzékelés az állomás bármikor adhat
    - Adás után dől el, hogy sikeres volt-e a küldés

ALOHA

- Földi telepítésű rádiós üzenetszórás
- Felhasználók versengése a közös csatornáért
- Egyszerű ALOHA
  - Bármikor kezdeményezhet adást minden felhasználó
  - Az ütközések miatt keretek fognak elveszni
  - Visszacsatolás - a küldő figyeli a csatornát
  - Akár egy bitnyi ütközés is tönkre tehet egy teljes keretet
- Réselt ALOHA
  - Keretidőhöz igazodó időrések
  - Szinkronizáció (egy speciális állomás órajelet sugároz)
  - Adás csak az időrések elején kezdeményezhető

CSMA - Carrier Sense Multiple Access

- Adás előtt az állomás belehallgat a csatornába
- Perzisztens CSMA
  - Ha foglalt a csatorna, akkor addig várakozik még szabad nem lesz
  - Ha szabad a csatorna elküldi a keretet
  - Ütközés esetén véletlen idejű várakozás majd újrakezdés
    - Terjedési késleltetés
    - Ütközés nulla terjedési idő esetén?
- Nemperzisztens CSMA
  - Foglalt csatorna esetén
    - Nem figyeli, hogy mikor szabadul fel a vonal
    - Véletlenszerű várakozás után újrakezdi a protokollt

CSMA/CD

- Ethernet hálózatokra jellemző
- Ütközés érzékelése esetén nem fejezik be (feleslegesen) a keret küldését
  - Idő és sávszélesség takarítható meg
  - A keretek továbbítása véletlenszerű várakozás után történik
- Ütközés felismerése
  - A csatorna feszültségszintjének növekedéséből
  - A kibocsátott és a csatornán lévő jelek összehasonlításából
  - A felismeréshez szükséges idő a késleltetéstől függ
    - Mikor lehetünk biztosak abban, hogy nem történt ütközés?

Ethernet kábelezés

- 10Base5
  - Vastag koax (thick coax)
  - Az eredeti ethernet kábelezés
  - Vámpírcsatlakozók (2,5 méterenként)
  - Maximum 100 állomás szegmensenként
- 10Base2
  - Vékony koax (thin coax)
  - Maximális szegmenshossz: 185 méter
  - BNC csatlakozók, "T" elosztók, lezárók
  - Maximum 30 állomás szegmensenként

Ethernet kábelezés

- 10Base-T
  - Minden állomás saját kábellel csatlakozik
  - Központi elosztó (HUB, Switch)
  - Maximális szegmenshossz: 100 méter
  - Maximum 1024 állomás szegmensenként
- 10Base-F
  - Optikai kábelezés, épületek között is jól használható
  - Maximális szegmenshossz: 2000 méter
  - Maximum 1024 állomás szegmensenként

A Manchester kódolás

- Az egyszerű bináris jelszintek nem használhatók
  - 0V-os jel átviteli szünet, vagy logikai alacsony szint?
  - Szinkronizációs problémák
  - Cél, hogy külső óra nélkül felismerhetők legyenek a bithatárok
- Manchester kódolás
  - Logikai "1": a bitidő első fele "1", a második "0" (1→0 átmenet)
  - Logikai "0": a bitidő első fele "0", a második "1" (0→1 átmenet)
  - Hátrány: kétszeres sávszélességet igényel a bináris kódoláshoz
- Differenciális Manchester kódolás
  - Logikai "1": a bitidő elején hiányzó átmenet
  - Logikai "0": a bitidő elején meglévő átmenet
  - Plusz mindkét esetben átmenet a bitidő felénél

A DIX keretformátum

- 8 - Előtag
  - 10101010 mintával kitöltve
  - Manchester kódolással: 10MHz-es, 6,4µs-os négyszögjel
- 6 - Célcím
- 6 - Forráscím
- 2 - Típus
  - A több működő protokoll közül melyiknek kell átadni a keretet
- 0-1500 - Adat
- 0-46 - Kitöltés
  - Ha az adatmező rövidebb mint 46 bájt
  - Meg kell különböztetni az érvényes (de rövid) kereteket az ütközések során keletkező kerettöredékektől
  - Túl rövid keret küldése esetén az első állomás nem észlelné az ütközést
  - A hálózati sebesség növekedésével a minimális kerethossznak is nőni kell
- 4 - Ellenőrző összeg (CRC)

Az IEEE 802.3 keretformátum

- 7 - Előtag
- 1 - SOF (Start Of Frame)
  - A 802.4 és 802.5-tel való kompatibilitás miatt
- 6 - Célcím
- 6 - Forráscím
- 2 - Hossz
  - A típus mező változott hosszra → nincs típus
    - Ezt az információt az adat mező fejrészébe helyezték
  - Manapság a Típus és a Hossz is támogatott (IEEE)
    - >1500 → Típus (a típus értékei kezdetektől fogva nagyobbak 1500-nál)
    - ≤1500 → Hossz
- 0-1500 - Adat
- 0-46 - Kitöltés
- 4 - Ellenőrző összeg (CRC)

Ütközések kezelése

- Ütközések után véletlen idejű várakozás
- Kettes exponenciális visszalépés
  - 1. ütközés: 0 vagy 1 időrésnyi várakozás
  - 2. ütközés: 0, 1, 2 vagy 3 időrésnyi várakozás
  - 3. ütközés: 0 … 7 időrésnyi várakozás
  - n. ütközés: 0 - 2^n-1 időrésnyi várakozás
  - Maximális intervallum a 10. ütközés után 0 … 1023
  - Hibaüzenet a 16. ütközés után
- Miért nem választunk azonos számú lehetőségből?
  - Sok állomás együttes ütközése
  - Néhány állomás ütközése

Sebesség, hatékonyság

- Az állomások számának növelésével
  - Növekszik az átviteli közeg kihasználtsága
  - Növekszik az ütközések gyakorisága
  - Növekszik a terhelés
- Megoldás a szegmensek felosztása
  - Kisebb ütközési tartományok létrehozása
  - Híd (bridge) alkalmazása
    - A második rétegben működő eszköz
  - Kapcsoló (switch) alkalmazása
    - Többportos híd
    - Minden port külön ütközési tartományt jelent

Ütközési tartományok

- Hálózati szegmens kiterjesztése
  - 1. rétegbe tartozó eszközökkel (ismétlő, HUB)
    - Egyetlen ütközési tartomány
    - Jelentős teljesítménycsökkenés várható
  - 2. és 3. rétegbe tartozó eszközökkel
    - Különálló szegmensek, több kisebb ütközési tartomány
- A négyismétlős (5-4-3-2-1) szabály
  - 5 szegmensnyi átviteli közeg
  - 4 ismétlő (vagy HUB)
  - 3 állomásokat csatlakoztató szegmens
  - 2 összekapcsoló szegmens (állomások nélkül)
  - 1 ütközési tartomány

Kapcsolási módok

- Közvetlen kapcsolás
  - A MAC célcím megérkezése után kezdődik a továbbítás
  - Minimális kapcsolási késleltetés
  - Hibaellenőrzésre nincs lehetőség
  - Csak szimmetrikus kapcsolás valósítható meg
- Töredékmentes továbbítás
  - Az első 64 bájt után kezdődik a továbbítás
  - Ellenőrizhető a címek és a protokollinformációk helyessége
- Tárol és továbbít módszer
  - A keret továbbítása csak a teljes keret vétele után történik
  - Újraszámolható a keret ellenőrző összege
    - Egy hibás keret nem kerül továbbításra, azonnal eldobható
  - Aszimmetrikus kapcsolás is megvalósítható

Szórási és csoportos címek

- Csoportos címzés
  - Többesküldés (Multicast)
  - Több állomás elérése egyetlen csoportcímmel
  - A címben az MSB "1" értékű (egyébként "0")
- Adatszórás
  - A cím minden bitje "1", azaz FF:FF:FF:FF:FF:FF
  - A szórási tartomány minden állomása megkapja
- Szórási vihar
  - A szórási és csoportcímzéses forgalom telíti a hálózatot
  - Újabb kapcsolatok nem hozhatók létre
  - A meglévő kapcsolatok megszakadhatnak
  - Szélsőséges esetben leállhat a hálózati forgalom

Szórási tartományok

- Második rétegbeli eszközökkel összekapcsolt ütközési tartományok
- A második réteg eszközei továbbítják a szórást
- Szórási tartományok létrehozása
  - Harmadik rétegbeli eszközökkel (router)
    - Első és második rétegben is működnek
    - A harmadik rétegbeli működés teszi lehetővé a szórási tartományok szegmentálását
- MAC címek helyett IP címek használata (3. réteg)
- Csak más LAN-okba tartó csomagok kerülnek ki
- Fenntartott (belső) IP címek

Fast Ethernet (802.3u)

- A 10 Mbit/s kezdett kevésnek bizonyulni
- Új, gyűrű alapú optikai szabványok
  - FDDI (Fiber Distributed Data Interface)
  - Fibre Channel
  - Jellemzően ipari szinten, gerinchálózatokban használták
  - A végfelhasználók gépeihez drága és bonyolult volt
- 1992 - törekvés a 802.3 felgyorsítására
  - A jelenlegi szabványt felgyorsítása (bitidő 100 ns-ról, 10 ns-ra)
    - Maradjon visszafelé kompatibilis
    - Kiforrott protokollok
    - Gyors megvalósíthatóság
      - 1995 júniusában fogadják el a 802.3u szabványt
  - Teljes átalakítás új szolgáltatásokkal, régi névvel
    - 802.12 - bukás …

A Fast Ethernet közegei

- CAT3
  - A legtöbb helyen már ilyen kábeleket használtak
  - Nincs szükség újrakábelezésre
  - Nem alkalmas 100 Mbit/s-os jel 100 méterre történő továbbításra
    - Sávszélessége csak 25 MHz
  - 100Base-T4
    - 4 érpár használata 2 érpár helyett
      - 1 érpár az elosztó irányába továbbítja az adatokat
      - 1 érpár az elosztó irányából fogadja az adatokat
      - 2 érpár pedig az aktuális átvitel irányába átkapcsolható

A Fast Ethernet közegei

- CAT5
  - 125 MHz-es sávszélesség
  - 1-1 érpár elegendő mindkét irányba
  - 100Base-T
- Multimódusú optikai szál
  - 100Base-FX
  - 100 Mbit/s-os duplex átvitel
  - Maximális kábelhossz 2000 méter
- Kapcsolók használata
  - A kompatibilitás miatt minden kapcsoló képes a 10 és 100 Mbit/s-os működésre is

Gigabites Ethernet (802.3z)

- Tervezés kezdete: 1995, jóváhagyás 1998
- Cél: a 802.3u szabvány felgyorsítása, a visszafelé kompatibilitás megőrzése mellett
- Kizárólag pont-pont összeköttetés
- Működési módok
  - Duplex
    - kapcsoló-számítógép vagy kapcsoló-kapcsoló esetén
    - minden vonal pufferelt
    - A keretek küldése bármikor lehetséges
    - Ütközés nem keletkezik
      - Nem használja a CSMA/CD protokollt sem
      - A maximális kábelhosszt a jelerősség határozza meg

Gigabites Ethernet (802.3z)

- Működési módok
  - Fél-duplex
    - Elosztó (HUB) és számítógép között
    - Nincs pufferelés, minden a klasszikus Ethernet-re hasonlít
    - Maximális kábelhossz: 25 méter lenne (64 bájtos keret)
- A 802.3z további szolgáltatásai
  - Vivőkiterjesztés (carrier extension)
    - A keret kiegészítése 512 bájtra (hardver szinten)
      - Minimális (46 bájtos) adat esetén 9%-os hatásfok
  - Keretfűzés (frame bursting)
    - Egyetlen adás során több keret továbbítása
  - Maximum 200 méteres távolság

A gigabites Ethernet közegei

- 1000Base-SX
  - Multimódusú optika szál (50 vagy 62,5 mikron)
  - Maximális hossz: 550 méter
- 1000Base-LX
  - Monomódusú optika szál (10 mikron)
  - Multimódusú optika szál (50 vagy 62,5 mikron)
  - Maximális hossz: 5000 méter
- 1000Base-CX
  - Árnyékolt sodrott érpár (2 érpár)
  - Maximális hossz: 25 méter
- 1000Base-T
  - CAT5 UTP - árnyékolatlan sodrott érpár (4 érpár)
  - CAT6 UTP - árnyékolatlan sodrott érpár (2 érpár)
  - Maximális hossz: 100 méter

A hálózati réteg útválasztás, torlódások

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

A hálózati réteg

- A csomag útja a forrástól a célig
  - Statikus útvonalak
  - Dinamikus útvonalak
    - Az aktuális terhelést figyelembe véve
- Csomóponti torlódás szabályozás
- A szolgáltatás minősége
- Egymástól eltérő hálózatok összekapcsolása
  - Eltérő címzési módok
  - Eltérő csomagméretek …

A hálózat réteg szolgálatai

- Összeköttetés nélküli szolgálat
  - Az alhálózatot megbízhatatlannak tekinti (tapasztalat)
  - Egyenként, egymástól függetlenül továbbított csomagok
  - Lényegében két primitív elegendő (Send-, Receive Packet)
  - Az egyes datagramok útjáról a forgalomirányító algoritmusok döntenek
- Összeköttetés alapú szolgálat
  - Az alhálózat nyújtson megbízható szolgáltatást
  - Az útvonal meghatározása a kapcsolat felépítésekor
  - Minden csomag ezen a virtuális áramkörön továbbítódik

A két szolgálat összevetése

	Datagram	Virtuális áramkör
Kapcsolat felépítés/bontás	Nincs	Szükséges
Címzés	Teljes cél- és forráscím minden csomaghoz	Csak virtuális áramkör azonosító
Forgalomirányítás	Dinamikus, minden csomagot függetlenül	Azonos, a kapcsolat felépítésekor meghatározva
Meghibásodott szakasz vagy router	Maximum néhány a hiba során elveszett csomag	Minden érintett virtuális áramkör megszakad
Szolgáltatásminőség	Bonyolult biztosítani	Kellő erőforrás foglalása esetén könnyen megvalósítható
Torlódásvédelem	Bonyolult biztosítani	Kellő erőforrás foglalása esetén könnyen megvalósítható

Forgalomirányítás

- Az adott csomag melyik kimenő irányba legyen továbbítva?
  - Datagram: minden csomagnál újra meghozott döntés
    - A legjobb út változhat a kapcsolat folyamán
  - Virtuális áramkör: csak új virtuális áramkör felépítésekor
- Forgalomirányító algoritmusok
  - Helyesség
  - Robosztusság
  - Igazságosság
  - Hatékonyság
  - Egyszerűség
  - Stabilitás
  - Optimalitás

Forgalomirányító algoritmusok

- Nem adaptív (statikus) algoritmusok
  - Döntéseikben nem játszik szerepet
    - az aktuális forgalom mérése vagy becslése
    - az aktuális topológia állapota
  - A rendszergazda által kézzel felvitt állandó útvonalak
  - Az eszköz indulásakor töltődnek be
- Adaptív algoritmusok
  - Döntéseik a következők függvényében változnak
    - a forgalom
    - és a topológia változásának követésével
  - Honnan kapják az új információkat?
  - Mikor változtassanak egy útvonalon?

A legrövidebb útvonal

- Többféle legrövidebb út is létezhet
  - Legkevesebb ugrás
  - Legrövidebb földrajzi távolság
  - Leggyorsabb átvitel
  - Általában a földrajzi távolság, költség, sávszélesség, késleltetés, aktuális forgalom együttesen határozzák meg
- Legrövidebb útvonal meghatározása
  - Felrajzoljuk az alhálózat gráfját
    - Csomópontok: routerek
    - Élek: kommunikációs csatornák (kapcsolatok)
  - A gráf két csomópontja közti legrövidebb út kiszámításával

Elárasztás

- A bejövő csomagokat minden más irányba továbbítja
- Probléma: a csomagok többször érkeznek meg
  - Ugrásszámláló a csomag fejrészében
    - Kezdeti érték: a forrástól célig tartó ugrások száma
    - Ha nem ismert, az alhálózat legnagyobb távolságára
  - Elárasztással továbbküldött csomagok nyilvántartása
    - Minden csomagot sorszámmal lát el a forrásrouter
    - Kétszer ugyanaz a csomag ne kerüljön szétküldésre
    - Ha a csomag a listában van (már elküldte) akkor eldobja
- Szelektív elárasztás (selective flooding)
- Felhasználható pl.: hibatűrő rendszerek (katonaság)

Távolságvektor alapú forgalomirányítás

- Bellmann (1957), Ford és Fulkerson (1962)
- Az Arpanet eredeti irányító algoritmusa
- Az interneten is használható, például: RIP
- Minden router egy táblázatban kezel az alhálózat többi routeréről, ami tartalmazza
  - Az adott router távolságát
    - Ugrásszám
    - Késleltetés (speciális ECHO csomagokkal mérhető)
  - preferált kimenő vonalat az adott routerhez
- Meghatározott időközönként a szomszédos routerek kicserélik egymással a táblázataikat

A végtelenig számolás problémája

- A távolságvektor alapú forgalomirányítás
  - gyorsan reagál a pozitív változásokra
    - vonal vagy eszköz helyreállása
    - Ha a leghosszabb út N ugrás, akkor N csere múlva minden eszköz értesül a változásról
  - lassan reagál az eszközök, útvonalak meghibásodásra
    - vonal vagy eszköz meghibásodása
    - probléma, hogy ha az 1. router elmondja a 2. routernek, hogy van egy útvonala a 3. router felé, akkor a 2. router nem tudhatja, hogy ő része-e ennek az útvonalnak?
- Milyen felső korlát után tekinthető egy útvonal hibásnak?
  - Ugrásszámok használata esetén a ∞ = leghosszabb út + 1
  - Késleltetés esetén nincs pontosan meghatározható felső korlát
    - magas érték kell, hogy a nagy késleltetést ne tekintsük hibás útnak

Néhány megoldás az előzőekre

- Látóhatár megosztás
  - Egy hálózatra vonatkozó információt csak a hálózat felől fogad a router
- Útvonalak mérgezése
  - A kiesett útvonalhoz tartozó érték végtelenre állításával
  - A szomszédos eszközök azonnal rögzítik az új értéket
  - Általában látóhatár megosztással együtt használt
- Eseményvezérelt frissítések
  - A topológia változásakor azonnali üzenetküldés a szomszédos eszközöknek
  - A frissítési hullám a teljes hálózaton végighalad
  - Az útvonalak mérgezésével együtt használható hatékonyan
- Visszatartási időzítők alkalmazása
  - Ha egy hálózat elérhetetlenné válásáról érkezik frissítés, elindul egy időzítő
  - Ha az időzítés lejárta előtt
    - ugyanonnan helyreállásról érkezik frissítés → minden rendben, helyreállt rsz.
    - máshonnan, de alacsonyabb értékkel érkezik frissítés → az lesz az új irány
    - máshonnan, de magasabb értékkel érkezik frissítés → nem veszi figyelembe
  - Időt biztosít az információ elterjedésére a teljes hálózatban

Kapcsolatállapot alapú forgalomirányítás

- A távolságvektor alapú rendszerek még az előbbi megoldásokat használva is lassan konvergálnak
- A kapcsolatállapot alapú forgalomirányítás lépései
  1. A szomszédok felkutatása és felderítése
  2. A szomszédok felé vezető út (késleltetés, költség) felmérése
  3. Az új információkból egy csomag generálása
  4. A csomag továbbítása a hálózat összes routere felé
  5. A kapott csomagokból kiszámítani az utat a többi router felé
- Minden router a teljes hálózatról rendelkezik információval
  - Topológia
  - Késleltetések, költségek
- Dijkstra algoritmusa alapján meghatározzák a legrövidebb utat az összes routerhez

Torlódásvédelem

- Torlódásvédelem vagy forgalomszabályozás?
- A torlódás hatásai
  - Túl sok csomag jelenléte esetén csökken a szállítási kapacitás
  - Az elveszett csomagok további forgalmat generálnak
  - Egy határ után összeomlik a rendszer
- A torlódás okai
  - Több bemenő vonal egy kimenő irányba
  - Memóriahiány (csomagok elvesztése)
    - Végtelen nagyságú memória?
  - Lassú processzorok
  - Kis sávszélességű vonalak
- A rendszer részeinek egyensúlyban kell lenni
- Hajlamos önmaga gerjesztésére

A torlódásvédelem alapjai

- Nyílthurkú szabályozás (vezérlés)
  - A probléma megelőzése gondos tervezéssel
  - Nem alakulhat ki torlódás, nincs szükség futás közbeni beavatkozásra
  - Típusai
    - Forrásnál beavatkozó algoritmusok
    - Célnál beavatkozó algoritmusok
- Zárthurkú szabályozás (visszacsatolás)
  - A rendszer folyamatos figyelése, a torlódás észlelése
  - Az információ továbbítása a beavatkozás helyére, beavatkozás
  - Típusai
    - Explicit visszajelzéssel működő algoritmusok
    - Implicit visszajelzéssel működő algoritmusok

Torlódásvédelem Virtuális Áramkörök esetén

- Belépés ellenőrzés
  - Ha ismert a torlódás ténye nem épülhet fel több VÁ
    - Sikertelen kapcsolat felépítést eredményez a szállítási rétegben
    - Drasztikus de egyszerű és hatékony megoldás
  - Ha a torlódás megszűnt felépíthetők az új VÁ-ök
  - Pl.: telefonközpont nem ad tárcsahangot
- A torlódott csomópontok elkerülése
  - A VÁ felépítése csak a torlódást elkerülve, alternatív útvonalon történhet meg
  - Ha nincs más útvonal a célig akkor nem épülhet fel új VÁ
- Erőforrások foglalása a VÁ felépítésekor
  - A szükséges erőforrások garantáltak → nem lehet torlódás
  - Rendszerint pazarló megoldás

Torlódásvédelem Datagram alapú hálózatokban

- Kimenő vonalak kihasználtságának figyelése
  - Küszöbérték felett beavatkozás
- Figyelmeztető bit használata
  - A kimenő csomag fejrészében egy bit beállítása torlódáskor
  - A nyugtába a cél bemásolja a figyelmeztető bit értékét
    - A forrás folyamatosan csökkenti a sebességet amíg a bit igaz értékű marad
    - A sebesség újra növelhető ha a bit hamisra változik
  - Probléma: az átvitel során bármely router elhelyezhette a bitet, a forgalom csak akkor nőhet ha sehol nincs torlódás

Torlódásvédelem Datagram alapú hálózatokban

- Lefojtó csomagok
  - A torlódást érzékelő router azonnal jelez az adónak
    - lefojtó csomagot küld a célcsomópont megjelölésével
    - a továbbított csomagot is megjelölik a fejrészében
  - A forrás csökkenti a sebességét a lefojtó csomag hatására
    - Újabb lefojtó csomagok érkeznek …
  - Több küszöbérték is lehetséges, melyek átlépése más-más hatású lefojtó csomagot eredményez
- Lefojtás lépésről lépésre
  - Nagy távolság esetén hosszú a reakcióidő
  - A lefojtás az előző routerre hat, lépésenként ér a forráshoz

A terhelés eltávolítása

- Fő kérdés: melyik csomagot dobjuk el?
- Csomagok eldobása véletlenszerűen
- Csomagok eldobása sorszám alapján
  - Újabb csomagok eldobása
    - Pl.: fájlátvitel → kevesebb csomagot kell újraküldeni
    - A régebbi csomag értékesebb az újnál ("bor politika")
  - Régebbi csomagok eldobása
    - Pl.: valós idejű hangátvitel (pl.: VoIP)
    - Az új csomag jobb mint a régi ("tej politika")
- Intelligens csomageldobás
  - Az alkalmazásnak prioritással kell ellátnia a csomagot
  - Először az alacsonyabb prioritásúak kerülnek eldobásra
  - A feladót ösztönözni kell(ene) az osztályba sorolásra …

Véletlen korai detektálás

- A torlódás kialakulását megelőzni célszerű egy küszöbérték átlépésekor, amíg kezelhető a helyzet
- Bizonyos szállítási protokollok az adás lassításával reagálnak az elveszett csomagokra (pl.: TCP)
- Melyik forrás okozza a feltorlódott kimenő sort?
  - Általában nem egyszerű kideríteni …
  - A sorból véletlenszerűen dobunk el csomagokat
- Az érintett források csökkentik az adási sebességet
- Nem alkalmazható pl. vezeték nélküli hálózatokban
  - A csomagvesztést jellemzően rádiós probléma okozza

Dzsitterkezelés

- Bizonyos esetekben a késleltetés nagyságánál lényegesen fontosabb a késleltetés ingadozása
  - Például: IP TV, webes rádiók
    - lényegtelen hogy 25 ms vagy 55 ms késleltetéssel érkezik-e az adás
    - azonban fontos, hogy azonos időközönként érkezzenek a képkockák
- Megadható a maximális és minimális késleltetések értéke (dzsitter)
- A késleltetés befolyásolása
  - Pufferelés a vevő oldalán
    - Valós idejű interaktivitást igénylő alkalmazások nem engedik meg
    - Például: IP telefónia, videokonferencia
  - Minden ugrásra kiszámoljuk az átviteli időt a teljes út mentén
    - Ha a csomag siet, az adott router hosszabb ideig pufferei
    - Ha a csomag késik, igyekszik a lehető leghamarabb továbbítani

A hálózati réteg QoS, hálózatok összekapcsolása

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

A hálózati réteg

- A csomag útja a forrástól a célig
  - Statikus útvonalak
  - Dinamikus útvonalak
    - Az aktuális terhelést figyelembe véve
- Csomóponti torlódás szabályozás
- A szolgáltatás minősége
- Egymástól eltérő hálózatok összekapcsolása
  - Eltérő címzési módok
  - Eltérő csomagméretek …

A szolgáltatás minősége

- Legfontosabb jellemzők
  - Megbízhatóság
  - Késleltetés
  - Dzsitter
  - Sávszélesség
- Eltérő igények
  - Különböző alkalmazások
  - Különböző átviteli utak és eszközök

Alkalmazások összehasonlítása

Alkalmazás	Megbízhatóság	Késleltetés	Dzsitter	Sávszélesség
E-mail	Fontos	Nem fontos	Nem fontos	Nem fontos
Fájlátvitel	Fontos	Nem fontos	Nem fontos	Kevéssé fontos
Web elérés	Fontos	Kevéssé fontos	Nem fontos	Kevéssé fontos
Távoli bejelentkezés	Fontos	Kevéssé fontos	Kevéssé fontos	Nem fontos
Webes rádiók	Nem fontos	Nem fontos	Fontos	Kevéssé fontos
Webes videók	Nem fontos	Nem fontos	Fontos	Fontos
IP telefónia	Nem fontos	Fontos	Fontos	Kevéssé fontos
Videókonferencia	Nem fontos	Fontos	Fontos	Fontos

A QoS biztosításának eszközei

- Túlméretezés
  - Pontosan kell ismerni az igényeket
    - Az igények idővel változhatnak
    - Megjelenhetnek átlagostól eltérő csúcsértékek is
  - Általában drága
- Pufferelés
  - Növeli a késleltetést, de csökkenti a dzsittert
- Forgalomformálás
  - Az adás átlagos sebességének szabályozása
  - Kapcsolat felépítésekor: szolgáltatásszintű megállapodás
  - Forgalmi rendfenntartás

A QoS biztosításának eszközei

- Lyukas vödör algoritmus
  - Minden hoszt egy véges sort tartalmazó interfésszel kapcsolódik
  - Csomag érkezésekor
    - Ha a sorban van hely, a csomag a sor végére kerül
    - Ha a sorban nincs hely, a csomag eldobásra kerül
  - A hoszt minden órajelkor azonos számú csomagot küld tovább
    - Azonos csomagméretnél: órajelenként egy csomagot
    - Változó csomagméretnél: bájtszámlálás
- Vezérjeles vödör algoritmus
  - Szükség esetén változtatható sebesség a kimeneten
    - Rövid ideig megengedi a kimenet gyorsítást
    - Cél az adatvesztés elkerülése lökésszerű terhelés esetén
  - Nem dob el csomagot
    - A vödör telítődése után a hosztot utasítja a küldés felfüggesztésére

A QoS biztosításának eszközei

- Erőforrás lefoglalás
  - Szükséges egy kijelölt út minden csomag számára
  - A kijelölt út mentén lefoglalhatók erőforrások
    - Sávszélesség
    - Processzoridő
    - Puffer
- Belépés engedélyezés
  - Biztosíthatók-e egy adott folyam igényei?
    - A forrás és a cél között minden eszköznek vizsgálni kell
    - A folyamnak pontosan kell leírni az igényeit
  - Folyammeghatározás

A QoS biztosításának eszközei

- Belépés engedélyezés
  - A folyammeghatározás fontosabb paraméterei
    - Vezérjeles vödör sebessége
    - Vezérjeles vödör mérete
    - Adatsebesség csúcsértéke
    - Minimális csomagméret
    - Maximális csomagméret
- Arányos útvonalválasztás
  - Azonos célba tartó csomagok szétosztása alternatív utakon
    - Egyenlő részekre osztás
    - Felosztás a kimenő vonalak kapacitásának függvényében

A QoS biztosításának eszközei

- Csomagütemezés
  - Egy kimenő sort használva
    - Egyetlen folyam nagy sávszélességre tehet szert
    - Más folyamok szolgáltatásminősége nehezen biztosítható
  - Egyenlő esélyű sorbaállítás
    - Minden folyam saját várakozó sort használ
    - Round robin körforgás a várakozó sorok között
    - Hátránya: nagyobb csomagméret → nagyobb sávszélesség
    - Megoldás: bájtonkénti körforgás szimulálása
  - Súlyozott egyenlő esélyű sorbaállítás
    - Szükség esetén prioritás biztosítható bizonyos folyamoknak

Eltérő hálózatok használata

- Különböző hálózatok használatának okai
  - Eltérő igények, eltérő technológiák
  - Különböző hardverek ↔ különböző szoftverek
  - Alacsonyabb telepítési költségek, lokális döntések
- Legfontosabb különbségek
  - Szolgálat típusa
  - Szolgálat minősége
  - Hibakezelés
  - Címzés
  - Protokollok
  - Csomagméret
  - Forgalomszabályozás
  - Torlódásvédelem

Hálózatok összekapcsolásának eszközei

- A fizikai rétegben
  - Repeater vagy HUB
    - Azonos típusú hálózatok között továbbítják a biteket
- Az adatkapcsolati rétegben
  - Bridge vagy Switch
    - Keretek továbbítása különböző hálózatokba (MAC)
    - Egyszerű protokoll konverziók pl.: Ethernet → 802.11
- A hálózati rétegben
  - Router
    - Több protokoll kezelése
    - Esetenként a csomagformátumokat is átalakíthatja
- A szállítási rétegben
  - Szállítási átjárók
    - Két eltérő szállítási protokollal rendelkező hálózat összekapcsolása
- Az alkalmazási rétegben
  - Alkalmazási átjárók

Virtuális áramkörök összekapcsolása

- Az összekapcsolt hálózat virtuális áramkörök sorozata
  - Távoli cím esetén az alhálózat VÁ-t épít ki az első routerig
  - Majd az adott router a következő routerig
    - A routerek között lehetnek többprotokollos routerek is (átjárók)
  - Egészen az utolsó router és a célhálózat közötti VÁ-ig
- A routerek feladata
  - Táblázatokban jegyzik a rajtuk áthaladó virtuális áramköröket
  - Az egyes VÁ-ök továbbításának irányát, az új VÁ számát
- Hatékony ha közel azonos hálózatokat kapcsol össze
  - Pl.: elég ha egy hálózat nem garantál megbízható kézbesítést

Datagram alapú hálózatok összekapcsolása

- Az egyes alhálózatokat routerek kapcsolják össze
- Az egyes csomagok különböző útvonalakon haladhatnak
  - Meghibásodások kivédése
  - Forgalom és terhelés figyelése
- Eltérő protokollok a hálózati rétegben
  - Konverzió a többprotokolos routerek segítségével
    - Komolyabb eltérések esetén jellemzően nem megoldható
  - Útvonalak keresése azonos típusú alhálózatokat használva
- Címzés
  - Nagy méretű, mindenre kiterjedő leképzési táblák? Problémás …
  - Univerzális csomagok használata (IP)
    - Cégek egyedi formátumai, üzleti érdekei miatt szintén kivitelzhetetlen

Alagutak használata

- Azonos típusú hálózat hosztjainak összekötése
  - Más típusú hálózat(ok) felhasználásával
- Például:
  - A forrás és a cél TCP/IP-t használó Ethernet hálózat hosztja
  - A forrás a cél IP címével Ethernet keretet küld
  - Az első router kiveszi az IP csomagot a keretből és a megfelelő módon és formában a cél hálózat routerének címzi
  - A másik router kiveszi a kapott csomagból az IP csomagot és egy Ethernet keretbe ágyazva továbbítja a célhosztnak
- A routertől-routerig tartó szakasz egy soros vonalként fogható fel
  - Ezen a vonalon az IP csomag beágyazva halad a WAN csomaghoz tartozó adatmezőben
  - A WAN-on történő átvitelben az eredeti csomagnak nincs szerepe

Csomagok tördelése

- Különböző hálózatok → különböző csomagméreteket
  - ATM (48 bájt)
  - IP (maximum 65515 bájt)
- Nem engedjük a nagyobb csomagokat a kisebb csomagméretet használó hálózatok irányába
  - Elvben működő, de a gyakorlatban nem megoldás
- A nagyobb csomagot darabokra kell tördelni
  - Az egyes darabok önálló csomagként kerülnek továbbításra
  - A darabokat később újra össze kell állítani

Csomagok tördelése

- Transzparens darabolás
  - A kimenő átjárónak tudnia kell, mikor kapott meg minden darabot
  - Minden csomagnak ugyanazon az átjárón kell végződnie
  - A darabolás és összeállítás többszöri elvégzése késleltetést okoz
- Nem transzparens darabolás
  - Amit egyszer feldaraboltunk azt a továbbiakban önálló csomagként kezeljük
    - A darabokhoz kapcsolódó kiegészítő információk miatt megnő az adatmennyiség
  - A darabok összerakása a célnál történik
    - Minden hosztnak képesnek kell lennie a darabok összeállítására
  - Több átjáró, különböző útvonalak használhatók

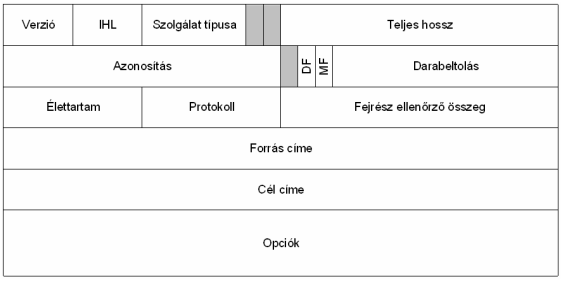
Darabok számozása

- Fa struktúra
  - Első darabolásnál 0.0, 0.1, 0.2 stb.
  - Ha további darabolás szükséges: 0.1.0, 0.1.1, 0.1.2 stb.
- Elemi darabméret meghatározásával
  - Elégségesen kis méret minden hálózaton való áthaladáshoz
  - Minden darab mérete megegyezik (kivéve az utolsót)
  - Az összeállításhoz minden darab tartalmzza
    - A csomag számát
    - A csomagban lévő első elemi darab számát
    - A csomag végét jelző bitet

Az Internet hálózati rétege

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

Az IP csomag fejrésze



Az IP fejrész

- IP csomag
  - Fejrész
  - Adatrész
- Verzió (4 bit)
  - Az adott csomag a protokoll melyik verziójához tartozik
    - Folyamatos áttérés IPv4-ről IPv6-ra
    - Értéke jellemzően 4 (IPv4) vagy 6 (IPv6)
- IHL (4 bit)
  - A fejrész hossza 32 bites szavakban
  - Megadja az opció maximumát (40 bájt)

Az IP fejrész

- Szolgálat típusa (6 bit)
  - Régen
    - 3 bit - precedencia mező
      - Értéke: 0 (normál csomag), 1 (prioritásos) … 7 (vezérlőcsomag)
    - 3 jelzőbit: D (delay), T (Throughput), R (Reliability)
    - *1 jelzőbit: C (cost)*
    - *1 bit: MBZ*
  - Napjainkban
    - DSCP (Differentiated Services Code Point) mező (6 bit)
    - IP-prioritást és a szolgáltatástípust jelölő mezők kombinációja
    - A QoS biztosításban játszik szerepet a mező

Az IP fejrész

- Teljes hossz (16 bit)
  - A fejrész és az adatrész együttes hossza
  - Egy datagram maximális mérete: 65.535 bájt
- Azonosítás (16 bit)
  - A datagram darabjainak azonosítására
  - A datagram minden darabja ugyan azt az azonosítót kapja
- DF: Don't Fragment (1 bit)
  - Jelzi a routerek számára, hogy ne darabolják a datagramot
  - Szükséges lehet néhány (kiscsomagos) hálózat elkerülése
- MF: More Fragment (1 bit)
  - Minden darabnál az értéke 1 kivéve az utolsó darabot (0)

Az IP fejrész

- Darabeltolás (13 bit)
  - A darab helyének meghatározása a datagramban
  - Elemi darabméret: 8 bájt
  - Meghatározza az IP csomag maximális méretét (65.536 bájt)
- Élettartam (8 bit)
  - Az ugrások számlálására
    - Értéke minden ugrásnál 1-el csökken
    - 0-nál eldobja a router a csomagot
  - Az egyes csomagok nem keringhetnek a végtelenségig
- Protokoll (8 bit)
  - A feldolgozó szállítási folyamat azonosítására

Az IP fejrész

- Fejrész ellenőrző összeg (16 bit)
  - A fejrész mezőiben történt hibák jelzésére
  - Minden ugrásnál újra kell számolni!
- Forrás címe (32 bit)
- Cél címe (32 bit)
- Opciók
  - Olyan információk melyekre csak ritkán van szükség
    - Nem foglalnak (feleslegesen) állandó helyet a fejrészben
    - Fejlesztési, kísérleti folyamatokban jól használható
    - Az eredeti fejrészből "kifelejtett" paraméterek pótlása

Az IP fejrész opciói

- Biztonság
  - Az információ titkosságáról szolgál információval
  - A routerek jellemzően nem foglalkoznak az értékével
  - "Hasznos" lehet a figyelem felkeltésére
- Szigorú forrás általi forgalomirányítás
  - A teljes utat adja meg IP címek sorozatával a forrástól a célig
  - A csomag útja pontosan meghatározható
  - Az irányítótáblák összeomlása esetén is küldhetők csomagok
  - Lemérhető egy útvonal késleltetése

Az IP fejrész opciói

- Laza forrás általi forgalomirányítás
  - A felsorolt routereken a felsorolás sorrendjében kell áthaladni
    - Más routerek is érinthetők
  - Egyes helyek, útvonalak érinthetők vagy kikerülhetők
- Útvonal feljegyzése
  - Minden router az opció végére fűzi az IP címét
  - A csomag útja pontosan követhető, elemezhető
    - Megtalálhatók a hibás forgalomirányítási döntések
  - Problémát jelenthet a fejrész opció mezőjének korlátozott mérete
- Időbélyeg
  - Az útvonal feljegyzése opcióval azonosan működik
  - A router IP címe mellett az időbélyeget is feljegyzi

Az IP-címek

- Egyedi kombináció, nincs két azonos IP cím
- A hálózat és a hoszt számát kódolja
- 32 bit hosszú címek
- Megtalálhatók az IP csomagok forrás és cél mezőiben
- Egy hálózati interfészre utal (egy hosztnak több IP címe is lehet)

IP címosztályok

- Általános forma: **w.x.y.z** ahol 1-1 betű 8 bitet jelöl. A cím egyes bájtjait "." karakterrel választjuk el

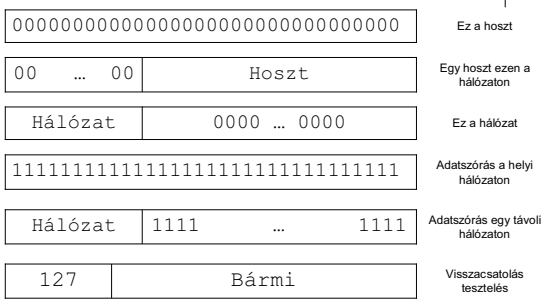
osztály	kezdőbitek	w értéke	hálózat azonosítója	hoszt	hálózatok száma	hosztok száma hálózatonként
A	0	1-127	w	x.y.z	127	16.777.214
B	10	128-191	w.x	y.z	16.384	65.534
C	110	192-223	w.x.y	z	2.097.152	254
D	1110	224-239	csoportos címek számára	-	-	-
E	1111	240-254	kísérleti célokra fenntartva	-	-	-

Fenntartott címtartományok

- Routerek nem engedik az Internet felé
- Otthoni hálózathoz is használhatók

- Loopback 127.x.x.x
- A osztály esetén: 10.x.x.x
- B osztály esetén: 172.16.x.x - 172.31.x.x
  169.254.x.x
- C osztály esetén: 192.168.x.x

Különleges IP-címek



Az alhálózatok (subnets)

- Miért hozunk létre alhálózatokat?
  - Nem tudunk hatékonyan kihasználni egy teljes címosztályt
    - az intézmény logikai működése, térbeli elhelyezkedése
    - több üzenetszórási tartomány létrehozása indokolt
- Hogyan hozhatunk létre alhálózatokat?
  - Az IP-cím hoszt részének legmagasabb helyiértékű bitjeiből néhányat az alhálózat azonosítására használunk
  - Az új hálózat-hoszt határt az IP-címben egy hálózati maszk (netmask) segítségével jelöljük
  - A hálózati maszkkal az osztályba sorolás által statikusan meghatározott hálózat-hoszt határ dinamikusan eltolható

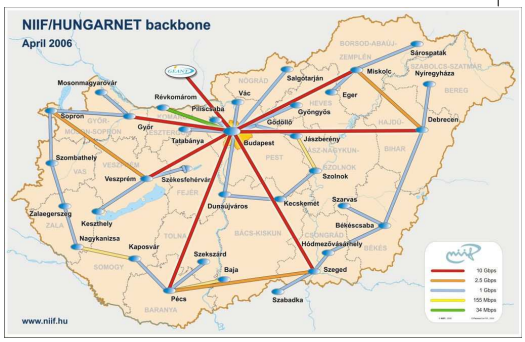
Hálózati maszk a gyakorlatban

- Vegyünk egy B osztályú hálózatot: 130.50.0.0
- Ez alkalmas 65.534 hoszt címzésére
- Alakítsunk ki 64 alhálózatot, alhálózatonként 1022 lehetséges hoszttal
- Netmask: 255.255.252.0 vagy /22
- Az egyes alhálózatok címei:
  - 130.50.4.0 (130.50.4.1 - 130.50.7.254)
  - 130.50.8.0 (130.50.8.1 - 130.50.11.254)
  - 130.50.12.0 (130.50.12.1 - 130.50.15.254)
  - …

CIDR

- Megmaradt IP címek kiosztása
  - változó méretű blokkokban
  - az eddigi osztályoktól függetlenül
  - 2 hatványainak megfelelő blokkok választhatók
- Átmeneti megoldás az IP címek gyors fogyására
- Minden IP címhez szükséges egy 32 bites maszk
- Útválasztás az IP + a maszk alapján
  - Több illeszkedés is lehetséges különböző maszkokkal
  - A leghosszabb maszk alapján történik az irányítás

CIDR példa



CIDR példa

- Kezdő cím: 200.200.0.0
- Igények
  - Egy váci szervezet: 1000 IP
  - Egy tatabányai szervezet: 500 IP
  - Egy gyöngyösi szervezet: 100 IP
  - Egy miskolci szervezet: 250 IP

Szervezet	Hálózat	Broadcast	Hosztok száma	Maszk
Vác	200.200.0.0	200.200.3.255	1024	200.200.0.0/22
Tatabánya	200.200.4.0	200.200.5.255	512	200.200.4.0/23
Gyöngyös	200.200.6.0	200.200.6.127	128	200.200.6.0/25
Miskolc	200.200.7.0	200.200.7.255	256	200.200.7.0/24

CIDR útválasztás

- Route tábla
  - Vác
    - IP: `11001000.11001000.00000000.00000000`
    - Mask: `11111111.11111111.11111100.00000000`
  - Tatabánya
    - IP: `11001000.11001000.00000100.00000000`
    - Mask: `11111111.11111111.11111110.00000000`
  - Gyöngyös
    - IP: `11001000.11001000.00000110.00000000`
    - Mask: `11111111.11111111.11111111.10000000`
  - Miskolc
    - IP: `11001000.11001000.00000111.00000000`
    - Mask: `11111111.11111111.11111111.00000000`

CIDR útválasztás

- Üzenet küldése 200.200.6.100-ra
  - IP: `11001000.11001000.00000110.01100100`
  - Továbbítás Gyöngyös irányába
- Csoportos route bejegyzés 200.200.0.0/21
  - Azonos irányokba tartó tartományok
  - Csökken a route tábla mérete
    - IP: `11001000.11001000.00000000.00000000`
    - Mask: `11111111.11111111.11111000.00000000`
  - Ki nem osztott címek:
    - 200.200.6.128/25 (128 cím)
      - Kiosztjuk egy salgótarjáni szervezetnek
      - Kiosztjuk egy szekszárdi szervezetnek

Hálózati címfordítás (NAT)

- A véges számú IP címek problémájának egy lehetséges megoldása
- A kisebb (nagyobb) hálózatok csak egy (néhány) IP címet kapnak (átjáró)
- A hálózaton belüli hosztok a fenntartott címtartományokból egyedi IP-t kapnak
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255
- Címfordítás szükséges ha egy csomag elhagyja a hálózatot
  - A kifelé tartó csomagok az átjáró IP címét kapják fordításkor
  - Fontos az átjáró címére érkező válaszcsomagok azonosítása

Hálózati címfordítás (NAT)

- Szükséges a válaszok azonosítása
- Az IP fejrészben jelezhető lenne az eredeti cím
  - Csak egyetlen szabad bit áll rendelkezésre
  - Opcióként?
- A TCP és UDP protokollok forrás- és cél port mezői
  - 16 bites mezők a távoli folyamatok összekapcsolására
  - 0-1023-ig számos ismert szolgáltatás (pl.: 22 SSH, 23 Telnet)
- TCP vagy UDP esetén a forrás port mező használható a címfordítás azonosításra

Hálózati címfordítás (NAT)

- Címfordítás a hálózatból kifelé tartó csomag esetén
  - A "belső" IP cseréje az átjáró IP címére
  - A forrás port mező cseréje a NAT doboz mutatójára
    - A NAT rekord tartalmazza
      - Eredeti IP cím
      - Eredeti forrás port
  - IP és TCP (UDP) fejrész ellenőrző összegek újraszámolása
- Címfordítás a hálózatba érkező válasz esetén
  - A forrás port mező alapján a megfelelő NAT rekord keresése
  - Az eredeti IP és forrás port kiolvasása és visszaírása
  - Az ellenőrző összegek újraszámolása

A NAT előnyei és hátrányai

- Megoldja (átmenetileg) az IP címek hiányát
- Megsérti az IP modell alapjait
  - Minden IP egyértelműen egyetlen hosztot azonosít
- Összeköttetés alapúvá teszi a kapcsolatokat
  - A kapcsolatok állapotait a VÁ-ökhöz hasonlóan tárolni kell
  - A NAT doboz összeomlása
- Sérti a rétegek függetlenségének alapelvét
  - A felsőbb réteg változása hatással lenne a NAT-ra is
- Jellemzően TCP és UDP protokollokkal használható
  - Új vagy speciális szállítási protokollal nem használható
- Egy IP címhez csak véges számú hoszt rendelhető
  - 16 bit → 65.536 (speciális portok miatt 65.536 - 4.096 = 61.440)

Vezérlő protokollok - ICMP

- Internet Control Message Protocol
- Váratlan események jelzése, tesztelés
- Fontosabb ICMP üzenetek
  - Cél elérhetetlen
  - Időtúllépés
  - Paraméter probléma
  - Forráselfolytás
  - Visszhang kérés
  - Visszhang válasz
  - Időbélyeg kérés
  - Időbélyeg válasz

Vezérlő protokollok - ARP

- Address Resolution Protocol
- A keretek küldéséhez Ethernet címekre van szükség
  - Minden hálózati kártyának egyedi MAC címe van (48 bit)
  - A hálózati kártyák az IP címeket nem kezelik
- Ethernet cím rendelése IP címhez
  - A küldő hoszt broadcast üzenetben keresi az IP-hez tartozó gépet
  - Az adatszórásra csak az IP tulajdonosa válaszol
    - Saját Ethernet címét küldi válaszként
  - Az Interneten szinte minden gép futtatja a szükséges ARP-ot
- Az ARP teljesítményének fokozása
  - ARP gyorstár - a feloldott címek átmeneti tárolására
  - Üzenetszórás a saját leképzési adatokkal - a válasz üzenetekhez
  - Leképzési adatok szórása induláskor

Vezérlő protokollok - RARP

- Reverse Address Resolution Protocol
- Ethernet címhez keresünk IP címet
- Pl.: winchester nélküli, hálózatról induló gépek
- A RARP működése
  - Bekapcsoláskor üzenetszórással keresi a hoszt az IP címét saját Ethernet címe alapján
  - A RARP szerver a konfigurációs állománya alapján válaszol
- Egységes memóriaképek az operációs rendszerről
- A RARP szervernek az adott hálózaton kell lennie

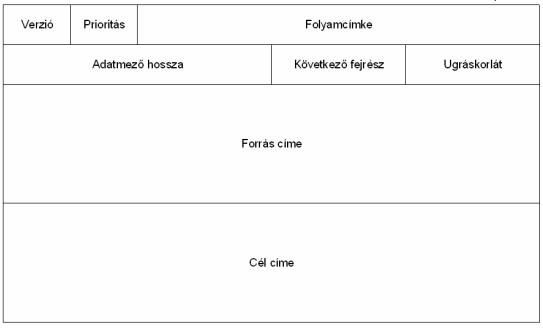
Vezérlő protokollok - DHCP

- Dynamic Host Configuration Protocol
- Kérésre külön szerver osztja ki az IP címeket
- A DHCP szerver más hálózatban is lehet
  - Üzenetszórással nem biztos, hogy elérhető
  - DHCP-közvetítő ügynökök alkalmazása
- A DHCP működése
  - Az IP-t kérő hoszt DHCP DISCOVER csomagot szór
  - A hálózaton lévő DHCP ügynök minden ilyen csomagot elfog
  - Az ügynök továbbküldi a csomagot a DHCP szervernek
  - A szerver visszaküldi a szükséges paramétereket
- DHCP leasing
  - A kiosztott IP címek csak korlátozott ideig élnek
  - A lízingelés lejárta előtt a hosztnak meg kell újítani az IP címét
  - Megakadályozható a kiosztható IP címek elfogyása

Az IPv6 előnyei

- Az IPv4 előnyeinek megtartása
  - Kompatibilis a legtöbb IPv4-es protokollal
  - Az IPv4-gyel nem kompatibilis, de párhuzamosan használhatók
- Az IPv6 legfontosabb fejlesztései
  - Hosszabb (128 bites) címek - "kifogyhatatlan"
  - Egyszerűbb fejrész
    - Gyorsabb feldolgozhatóság a routerekben
  - Az opciók továbbfejlesztett támogatása
    - Néhány eddig állandó érték opcióként jelenik meg
    - Az opció felesleges részei könnyen átléphetők (gyors feldolgozás)
  - A biztonság fokozása
    - Hitelesítés és titkosság biztosítása
  - A szolgálat típusának és a szolgálatminőségnek kiemelt kezelése

Az IPv6 csomag fejrésze



Az IPv6 fejrész

- Verzió (4 bit)
  - Az adott csomag a protokoll melyik verziójához tartozik
    - Folyamatos áttérés IPv4-ről IPv6-ra
    - Értéke jellemzően 4 (IPv4) vagy 6 (IPv6)
- Forgalmi osztály (8 bit)
  - Az adott forgalom prioritási osztályba sorolásához
  - A valós idejű szállítási követelmények besorolása
- Folyamcímke (20 bit)
  - Egy folyamathoz tartozó csomagok útjának azonosítása a forrástól a célig
  - Az egyes címkékhez különböző igények tartozhatnak a routerkben
    - Erőforrások foglalása
    - Késleltetéssel kapcsolatos igények kezelése

Az IPv6 fejrész

- Adatmező hossza (16 bit)
  - Az adatmező mérete bájtokban (fejrész nélkül)
- Következő fejrész (8 bit)
  - A fejrész egyszerűsítését biztosító mező
  - További, kiegészítő fejrészeket azonosíthat
  - Ha nincs további fejrész, a szállítási protokollt azonosítja
- Ugráskorlát (8 bit)
  - Az IPv4 élettartam mezőjével azonos funkció
  - Értéke minden ugrásnál csökken (0-nál a csomag eldobása)

Az IPv6 fejrész

- Forrás és cél címe (128 bit)
  - Új formátum
    - Nyolc csoportban négy-négy hexadecimális számjegy
    - Elválasztó karakter: ":"
  - Teljes formátum
    - Pl.: 1080:0000:0000:0000:0008:0800:200C:417A
  - Egyszerűsítések
    - Vezető nullák minden csoport elején elhagyhatók
    - A csak nullát tartalmazó csoportok ":"-al helyettesíthetők
    - A "::" kombináció minden címben csak egyszer szerepelhet
    - Pl.: 1080::8:800:200C:417A
    - IPv4-es címek írásmódja: ::193.6.50.195

Az IPv6 "hiányzó" mezői

- IHL: a rögzített méretű fejrész miatt felesleges
- Protokoll: a következő fejrész mező adja meg
- DF, MF, Darabeltolás
  - A datagramok méretének dinamikus meghatározása
  - Minimális méret 1280 bájt (576 bájt helyett)
  - A csomagok darabolása helyett a router hibaüzenetet küld
    - A forrás hosztot utasítja a címzettnek szóló további üzenetek darabolására
- Fejrész ellenőrző összeg
  - Gyakorlatilag már nincs rá szükség

Az IPv6 kiegészítő fejrészei

- Átugrás opciók
  - Minden routerre érvényes opciók
  - Jelenleg 64 kB-nál nagyobb datagramok támogatására
    - Óriás datagramok (jumbogram)
    - Gigabájtos nagyságrendű adatok hatékony átvitelére
- Címzetti opciók
  - jelenleg nem használt, csak a címzettnek szóló opciók átvitelére
- Forgalomirányítás opció
  - Hasonló a laza forrás általi forgalomirányításhoz
- Darabolási opció
  - Az IPv4-hez hasonlóan a darabok jelzésére és számozására
  - Csak a forrás darabolhat, a routerek nem (hatékonyság!)
- Hitelesítés opció
- Titkosított biztonsági adatmező

A szállítási réteg

Programtervező informatikus BSc
Számítógép hálózatok és architektúrák
előadás

A szállítási réteg

- Adatok fogadása a viszony rétegtől
- Szegmentálás
- Szegmensek továbbítása a hálózati rétegnek
- Biztosítja a hibamentes átvitelt
  - Elrejti a felsőbb rétegek elől az átvitel problémáit
- Tényleges kommunikáció a végpontok között
- Működése hasonló a hálózati réteghez, de
- Teljes egészében a felhasználó gépén fut

UDP

- User Datagram Protocol
- Az Internet összeköttetés nélküli szállítási protokollja
- UDP szegmens
  - 8 bájt fejrész
    - Forrásport (16 bit)
    - Célport (16 bit)
    - UDP szegmens hossz (16 bit)
    - UDP ellenőrző összeg (16 bit)
  - adatrész
- A fejrészben már a portok is megtalálhatók

UDP

- Amire az UDP képes
  - Interfészt biztosít az IP protokoll használatához
  - Párhuzamos kapcsolatok a portok használatával
- És amire nem
  - Hibakezelés
  - Nyugtázás, újraküldés
  - Forgalomszabályozás
- Jellemző felhasználási terület: kliens-szerver alkalmazások
  - Rövid kérések, rövid válaszok
  - Ha nincs válasz → újabb kérés
  - Egyszerű megvalósíthatóság
  - Kisebb forgalom
  - Pl.: DNS

A TCP feladatai

- Transmission Control Protocol
- Az IP megbízhatatlanságának kiküszöbölése
- Végpontok közötti megbízható átvitel biztosítása
  - Megbízhatatlan hálózatokon
  - Összekapcsolt hálózatokon
- Az elveszett datagramok észlelése
  - Időzítők kezelése
  - Újraküldés
- Datagramok helytelen sorrendjének felismerése
  - Üzenetek felépítése a datagramok megfelelő sorrendjével

TCP portok

- A kommunikáció a forrás és cél socket között zajlik
- Socket cím: hoszt IP címe + hoszt portszáma
- A jól ismert (well-known) portok
  - Az 1024 alatti portok
  - gyakran használt szolgáltatások részére
  - /etc/services

Port	Protokoll	Port	Protokoll	Port	Protokoll
21	FTP	25	SMTP	110	POP3
22	SSH	69	TFTP	143	IMAP
23	Telnet	80	HTTP	161	SNMP

A TCP protokoll

- Sorszámozás
  - Minden bájt 32 bites egyedi sorszámot kap
  - Számlálók átfordulása
- TCP szegmens
  - Fejrész (20 bájt) + [Fejrész opció] + [Adatok]
  - A szegmens méretét a TCP szoftvere határozza meg
    - Több írási művelet is gyűjthető egy szegmensbe, de egy adatsor is küldhető több szegmensben
    - Maximum (fejrésszel együtt): 65.515 bájt (IP adatmező)
    - MTU (Maximum Transfer Unit): gyakorlatban 1.500 bájt (Ethernet adatmező)

TCP nyugtázás

- Csúszóablakos protokoll
  - Szegmensek küldésekor időzítő indítása
  - Szegmens érkezésekor válasz szegmens (nyugta)
    - Tartalmazza a következő várt szegmens sorszámát
    - Felhasználói adatokat (ha van továbbításra váró adat)
  - Ha a nyugta nem érkezik meg időben → újraküldés
- A nyugtázás lehetséges problémái
  - Helytelen sorrendben érkező szegmensek
  - Torlódás, nagy késleltetés → kétszer érkezik a szegmens
  - Újraküldésnél eltérő bájt tartományok a szegmensben
  - Mi történjen a nem nyugtázható szegmensekkel?

A TCP fejrész

<table>
<tr><td colspan="2">Forrásport</td><td colspan="8">Célport</td></tr>
<tr><td colspan="10">Sorszám</td></tr>
<tr><td colspan="10">Nyugta</td></tr>
<tr><td>Fejrész hossz</td><td></td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">Ablakméret</td></tr>
<tr><td colspan="6">Ellenőrző összeg</td><td colspan="4">Sürgősségi mutató</td></tr>
<tr><td colspan="10">Opciók</td></tr>
<tr><td colspan="10">Adatok</td></tr>
</table>

A TCP fejrész

- Forrásport (16 bit)
- Célport (16 bit)
- Sorszám (32 bit)
- Nyugta (32 bit)
  - A következő küldendő bájt sorszáma
- Fejrész hossz (4 bit)
  - A TCP fejrész hossza 32 bites szavakban
  - Az opciók mező változó hossza miatt szükséges
- Fenntartott mező (6 bit)

A TCP fejrész

- URG
  - Ha értéke "1" ha a sürgősségi mutató mező használt
- ACK
  - Ha értéke "1" ha a fejrész nyugtát (is) tartalmaz
  - Ha értéke "0" a nyugta mező átugorható
- PSH
  - Késedelem nélküli adattovábbítás kérésére
- RST
  - Összeomlott vagy összezavart összeköttetés helyreállítása
- SYN
  - Az összeköttetés felépítéséhez használt jelzőbit
    - SYN=1 ACK=0 → Összeköttetés kérés (Connection Request)
    - SYN=1 ACK=1 → Összeköttetés fogadása (Connection Accepted)
- FIN
  - Az összeköttetés bontásának jelzésére

A TCP fejrész

- Ablakméret
  - A csúszóablak méretének szabályozása (forgalomszabályzás)
  - Lehetséges értékek
    - 0: az adatok rendben megérkeztek, ne küldj további adatokat
    - >0: a nyugtázott bájttól kezdődően ennyi bájtot küldj
- Ellenőrző összeg
  - A teljes szegmens ellenőrző összege
- Sürgősségi mutató
  - A sürgős adat helyének jelzése az adatok között az aktuális sorszámhoz képest

Összeköttetések felépítése

- Háromutas kézfogás
- A Server várakozik a bejövő kérésekre
- A Kliens csatlakozási kérést küld
  - IP cím + portszám
  - Maximális TCP szegmens mérete
  - SYN=1 ACK=0
- Ha a célgép célportján nincs várakozó folyamat a TCP RST=1 értékkel válaszol
- Ha a Server folyamat elfogadja a kérést nyugtázó szegmenst küld vissza (SYN=1 ACK=1)
- A nyugtát a kliens gép nyugtázza
- Fontos a kezdő sorszám megválasztása

Összeköttetések bontása

- Duplex átvitel
- Bontás irányonként (szimplex átvitel)
- Bontási kérelem FIN=1 (hoszt1)
  - hoszt1 már nem küldhet adatot
  - hoszt1 továbbra is fogadhat adatot hoszt2 felől
- Bontási kérelem FIN=1 (hoszt2)
  - Az összeköttetés vége
- A két hadsereg problémája (támadás = bontás)
  - Elméletben (sem) létezik tökéletes megoldás
  - Gyakorlatban: ha a FIN kérésre nem érkezik időben ACK → a bontást kezdeményező hoszt befejezi a kapcsolatot

TCP pufferelés

- Mikor továbbítsa a TCP az alkalmazás által küldött adatokat?
- Mikor nyugtázzunk egy átvitelt?
- Egyetlen karakter leütése telnet használatával (azonnali továbbítás mellett)
  - 21 bájtos szegmenst hoz létre a TCP
  - Az IP hozzáteszi a saját fejrészét (41 bájt)
  - A megérkezett csomag nyugtázása (40 bájt)
  - A feldolgozott karakter visszaküldése (41 bájt)
  - A megérkezett csomag nyugtázása (40 bájt)
  - 1 (2) bájt átviteléhez összesen 162 bájtot használtunk

TCP pufferelés

- Nyugták késleltetése 500 ms hosszan
  - Ha az alkalmazás feldolgozta a karaktert a nyugta a választ tartalmazó adattal együtt küldhető
  - Folyamatos adatfolyam esetén a nyugták megspórolhatók
- Bájtonként érkező adatoknál
  - A küldő TCP entitás elküldi az első bájtot
  - Az érkező további bájtokat puffereli az első bájt nyugtájáig
  - Majd a pufferelt bájtokat egyetlen szegmensben továbbítja
  - Lehetőség a pufferelt adatok küldésére a nyugtázás előtt
  - Nem praktikus pl.: távoli asztalon az egér mozgatására

TCP pufferelés

- A buta ablak (silly window) jelenség
  - A fogadó entitás puferre tele van, nagy szegmensekben kapta az adatokat (ablakméret = 0)
  - A fogadó bájtonként olvassa ki a kapott adatokat
  - 1 bájt kiolvasása után 1 bájt hely keletkezik a pufferben (ablakméret = 1)
  - Egyetlen bájt érkezése után újra megtelik a puffer …
- A fogadó akkor küldhessen ablakméret információt
  - Ha képes a maximális méretű szegmens fogadására
  - Ha a puffere félig kiürült

TCP torlódásvédelem

- A torlódás detektálás
  - Az időzítők nyugtázás előtti lejárását okozhatja
    - Zajos, rossz minőségű átviteli közeg
    - Torlódás (az Internet TCP folyamatai ezt feltételezik)
- A torlódás okai
  - A vevő kapacitása
  - A hálózat kapacitása
- A TCP eszköze az ablakméret változtatása
  - Vevő által szabályozott ablak
  - Torlódási ablak
  - A kettő minimuma határozza meg a tényleges ablakméretet

TCP torlódásvédelem

- Lassú kezdés (slow start) algoritmus
  - A torlódási ablak kezdőértékét a maximális szegmens méretre állítják
  - Az adó elküld egy maximális szegmenst
  - Ha a nyugta időben megérkezik az ablakméret duplázódik
  - Az adó az új maximumot kihasználva küld löketet
  - Az exponenciális növekedés az első nyugta elvesztéséig tart
  - A megelőző érték lesz a megfelelő ablakméret

Torlódásvédelem az Interneten

- A torlódási küszöb bevezetése (kezdőérték 64 kB)
- Időtúllépés esetén
  - A torlódási küszöb új értéke a torlódási ablak fele lesz
  - A torlódási ablak új értéke a maximális szegmensméret lesz
  - A teljesítőképesség meghatározása a lassú kezdet módosított algoritmusával
    - Az exponenciális növekedés csak a torlódási küszöbig tart
    - A torlódási küszöb felett a növekedés csak a maximális szegmensméret értéke (lineáris növekedés)
  - A torlódási ablak mérete a vevő ablakméretéig növekszik

Vezeték nélküli hálózatok

- A TCP-t megbízható hálózatokra optimalizálták
- Kell-e külön törődni a hálózat megbízhatóságával?
  - A rétegszemlélet szerint nem (független rétegek)
  - A gyakorlatban muszáj …
- Alapvető probléma a torlódásvédelem
  - A csomagok jellemzően elveszni és nem torlódni fognak
  - Az adó sebességének csökkentése csak olaj lenne a tűzre
  - A sebességet ilyenkor lehetőség szerint inkább növelni kell
- Inhomogén átviteli utak
  - Vezetékes (megbízható) szakaszok
  - Vezeték nélküli (megbízhatatlan) szakaszok

Vezeték nélküli hálózatok

- Közvetett TCP
  - A TCP összeköttetés felosztása vezetékes és vezeték nélküli részre
  - Az új összeköttetések határa a bázisállomás lesz
  - A bázisállomás mindkét irányba átmásolja a csomagokat
  - Két homogén (teljes TCP) összeköttetés
    - A vezetékes rész időtúllépései lassítják a forrást
    - A vezeték nélküli rész időtúllépései gyorsítják a forrást
  - Hátrány, hogy ha a forrás nyugtát kap a vételről akkor még nem biztos, hogy célba ért a csomag (a bázis nyugtázott)