

# Számítógépes Hálózatok

Készítette: Katona Bence  
Dr. Laki Sándor kérdései, előadás diái  
és  
Dr. Nikovits Tibor kidolgozása alapján

2016-2017-1



## Tartalomjegyzék

1	Előadás	2
2	Előadás	5
3	Előadás	8
4	Előadás	12
5	Előadás	13
6	Előadás	16
7	Előadás	18
8	Előadás	18
9	Előadás	21
10	Előadás	24
11	Előadás	26

# 1 Előadás

## 1. Hány réteget különböztet meg az ISO/OSI referencia modell? Sorolja fel őket.

7 darab: alkalmazási-, megjelenítési-, ülés-, szállítói-, hálózati-, adatkapcsolati- és fizikai réteg.

## 2. Hány réteget különböztet meg a Tannenbaum-féle hibrid rétegmodell? Sorolja fel őket.

5 darab: alkalmazási-, szállítói-, hálózati-, adatkapcsolati- és fizikai réteg.

## 3. Mi az "Open System Interconnection Reference Model" (ISO OSI), hogyan specifikáljuk az egyes rétegeket?

Egy 7-rétegű standard, koncepcionális modell kommunikációs hálózatok belső funkcionalitásaihoz.

## 4. Mi a feladata és mik a főbb funkcionalitásai az ISO OSI modell fizikai rétegének?

Fizikai réteg:

- Szolgáltatás: Információt visz át két fizikailag összekötött eszköz között, definiálja az eszköz és a fizikai átviteli közeg kapcsolatát
- Interfész: Specifikálja egy bit átvitelét
- Protokoll: Egy bit kódolásának sémája, feszültség szintek, jelek időzítése
- Példák: koaxiális kábel, optikai kábel, rádió frekvenciás adó

## 5. Mi a feladata és mik a főbb funkcionalitásai az ISO/OSI modell adatkapcsolati rétegének?

Adatkapcsolati réteg:

- Szolgáltatás: Adatok keretekre tördelése (határok a csomagok között), közeghozzáférés vezérlés (MAC), per-hop megbízhatóság és folyamvezérlés
- Interfész: Keret küldése két közös médiumra kötött eszköz között
- Protokoll: Fizikai címezés (pl. MAC address, IB address)
- Példák: Ethernet, Wifi, InfiniBand

## 6. Mi a feladata és mik a főbb funkcionalitásai az ISO/OSI modell hálózati rétegének?

Hálózati réteg:

- Szolgáltatás: Csomagtovábbítás, útvonalválasztás, csomag fragmentálás kezelése, csomag ütemezés, puffer kezelés
- Interfész: Csomag küldése egy adott végpontnak
- Protokoll: Globálisan egyedi címeket definiálása, routing táblák karbantartása
- Példák: Internet Protocol (IPv4), IPv6

## **7. Mi a feladata az ISO/OSI modell ülés (session) rétegének?**

Session réteg:

- Szolgáltatás: Kapcsolat menedzsment (felépítés, fenntartás és bontás), munkamenet típusának meghatározása, szinkronizációs pont menedzsment (checkpoint)
- Interfész: Attól függ...
- Protokoll: Token menedzsment, szinkronizációs checkpoints beszúrás
- Példák: nincs

## **8. Mik a főbb funkcionálisai az ISO/OSI modell megjelenítési rétegének?**

Megjelenítési réteg:

- Szolgáltatás: Adatkonverzió különböző reprezentációk között, pl. big endian to little endian, Ascii to Unicode
- Interfész: Attól függ...
- Protokoll: Adatformátumokat definiál, transzformációs szabályokat alkalmaz
- Példák: nincs

## **9. Mit jelent a hálózatok esetén az adatok burkolása?**

Az egyes rétegek fejéc/lábléc információkat illesztnek a kapott csomaghoz és úgy küldik azt tovább.

## **10. Mit jelent a legjobb szándék (best effort) elv a hálózati kommunikációban?**

Ha egy csomag nem éri el a célt, akkor törlődik. Az alkalmazás újraküldi ilyen esetekben

## **11. Mit jelent a "Black-box" megközelítés a kapcsolatokra?**

A Black Box-okat később Gateway-eknek és Router-eknek keresztelték át. Csomaginformációk nem kerülnek megőrzésre és nincs folyam-felügyelet.

## **12. Mi az a PAN?**

Magánhálózat (angolul Personal Area Network), 1 m.

## **13. Mi az a WAN?**

Nagy kiterjedésű hálózat (angolul Wide Area Network), 100 km - 1000 km.

**14. Sorolja fel az internet 5 (előadáson elhangzott) jellemzőjét.**

Jellemzői: rendszerfüggetlenség, nincs központi felügyelet, építőelemei a LAN-ok, globális és olyan szolgáltatásokat nyújt, mint a World Wide Web, e-mail vagy fájlátvitel.

**15. Definiálja a hálózati sávszélességet?**

Az adat átviteléhez elérhető vagy felhasznált kommunikációs erőforrás mérésére szolgáló mennyiség, amelyet bit per másodpercben szoktak kifejezni.

**16. Definiálja az átviteli késleltetést.**

Az az időtartam, amely egy csomag összes bitjének az átviteli csatornára tételéhez szükséges. Jelölése:  $d_T$ .

**17. Definiálja a propagációs késést.**

Az az időtartam, amely a jelnek szükséges ahhoz, hogy a küldőtől megérkezzen a címzetthez. Jelölése:  $d_{prop}$  vagy  $d$ .

**18. Mi a hálózati hoszt?**

Olyan eszköz, amely egy számítógépes hálózattal áll összeköttetésben. Egy hoszt információkat oszthat meg, szolgáltatást és alkalmazásokat biztosíthat a hálózat további csomópontjainak. (Továbbiakban csak hosztként hivatkozunk rá.)

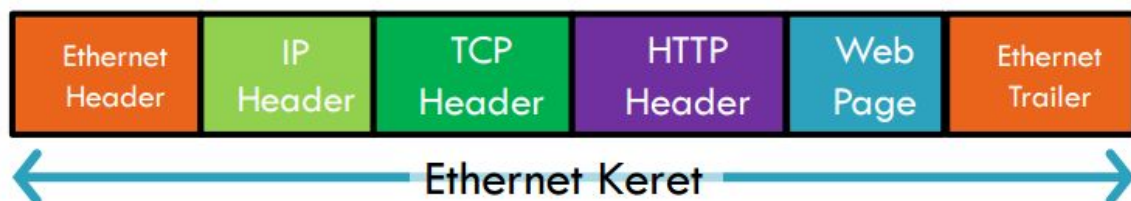
**19. Mi az átviteli csatorna?**

Az a közeg, amelyen a kommunikáció folyik a résztvevő hosztok között. Ez a közeg lehet egy koaxális kábel, a levegő, optikai kábel, stb.

**20. Mi a fő különbség a csomagkapcsolt és az áramkörkapcsolt hálózatok között?**

Csomagkapcsolt hálózat (pl. Internet), áramkör kapcsolt hálózat (vezetékes telefon).

**21. Adjon egy valós példát adatok beburkolására (pl. az előadáson látott Internet példa)!**



**22. Mit értünk Internet homokóra alatt? Miért nehéz az IPv6-ra való átállás?**

Az Internet rétegnek hála, minden hálózat képes együttműködni. Minden alkalmazás működik minden hálózaton. Ezen réteg felett és alatt lehetnek újabb fejlesztések. Azonban az IP-t lecserélni nagyon nehéz pontosan az összekötő szerepe miatt.

### 23. Jellemezze egy mondatban a tűzfalakat, proxykat és NAT dobozokat!

Jellemzők:

- Tűzfal: Alkalmazási réteg fejléceit is vizsgálhatja
- Proxy: Alkalmazási végpontot szimulál a hálózatban
- NAT doboz: Megtöri a végpont-végpont elérhetőséget a hálózatban

### 24. A Hálózati réteg funkcióit milyen síkok (planes) mentén csoportosíthatjuk még?

Merőleges síkok:

- Control plane/Vezérlési sík: Hogyan határozzuk meg az Internetes útvonalakat?
- Data plane/Adat sík: Hogyan továbbítjuk az adatot egy útvonal mentén?

## 2 Előadás

### 1. Ismertesse a fizikai rétegben a lehetséges átviteli közegek fajtáit!

Vezetékes, vezeték nélküli (földi rádiós), műholdas.

### 2. Mit mond ki a Nyquist tétel?

Zajmentes csatorna esetén a Maximális Adatsebesség  $= 2H * \log_2(V)$

Mértékegysége:  $\frac{b}{s}$

H: sávszélesség

V: szimbólumok száma

### 3. Mit mond ki a Shannon tétel?

Zajos csatorna esetén a Maximális Adatsebesség  $= H * \log_2(1 + \frac{S}{N})$

Mértékegysége:  $\frac{b}{s}$

H: sávszélesség

$\frac{S}{N}$ : jel-zaj arány

### 4. Soroljon fel 4 különböző vezetékes átviteli közeget!

Mágneses adathordozók (kimentjük, majd elszállítjuk), sodort érpár, koax kábel, fénykábelek.

### 5. Mit nevezünk frekvenciának? Hogyan jelölik? Mi a mértékegysége?

Frekvencia:

- Definíció: elektromágneses hullám másodpercenkénti rezgésszáma
- Jelölés:  $f$
- Mértékegység: Hertz (Hz)

## 6. Mi a hullámhossz?

Két egymást követő hullámcsúcs (vagy hullámvölgy) közötti távolság. Jelölés:  $\lambda$

## 7. Soroljon fel 3 elektromágneses tartományt a frekvenciáik növekvő sorrendjében!

Rádió ( $< 3 * 10^9$ ) < Mikrohullám ( $3 * 10^9 - 3 * 10^{12}$ ) < Infravörös ( $3 * 10^{12} - 4.3 * 10^{14}$ )

## 8. Milyen frekvencia tartomány átvitelére alkalmas a sodort érpár, a koax kábel, az optikai szál?

Sodort:  $10^4 - 10^6$  Hz, koax kábel:  $10^5 - 10^8$  Hz és optikai szál:  $10^{14} - 10^{15}$  Hz.

## 9. Soroljon fel 4 vezeték nélküli átviteli közeget!

Rádiófrekvenciás átvitel, mikrohullámú átvitel, infravörös átvitel és látható fényhullámú átvitel(pl. lézer).

## 10. Mi a szimbólumráta és az adatrata? Mi a mértékegységük?

Szimbólumráta (BAUD): elküldött szimbólumok száma másodpercenként

Adatrata (bps): elküldött bitek száma másodpercenként.

## 11. Soroljon fel 3 óraszinkronizációs módszert!

Óraszinkronizációs módszerek:

1. Explicit órajel
2. Kritikus időpontok
3. Szimbólum kódok (önütemező jel)

## 12. Mi az önütemező jel? Mire használható?

Önütemező jel: külön órajel szinkronizáció nélkül dekódolható jel.

## 13. Ismertesse az NRZ-L (Non-Return to zero) kódolás szabályait!

A digitális kódok 3 lényeges momentumban térnek el:

- Mi történik egy szignál intervallum elején? 1-es bit magas jelszint / 0-s bit alacsony jelszint
- Mi történik egy szignál intervallum közepén? Semmi
- Mi történik egy szignál intervallum végén? Semmi

#### 14. Ismertesse a Manchester kódolás szabályait!

A digitális kódok 3 lényeges momentumban térnek el:

- Mi történik egy szignál intervallum elején? Semmi
- Mi történik egy szignál intervallum közepén? 1-es bit magasról alacsonyra / 0-s alacsonyról magasra
- Mi történik egy szignál intervallum végén? Semmi

#### 15. Ismertesse az NRZI (Non-return to zero inverted)? Mi a fő probléma ezzel a kódolással?

A digitális kódok 3 lényeges momentumban térnek el:

- Mi történik egy szignál intervallum elején? Semmi
- Mi történik egy szignál intervallum közepén? 1-es bit átmenet / 0-s ugyanaz marad
- Mi történik egy szignál intervallum végén? Semmi

#### 16. Ismertesse a 4-bit/5-bit módszert? Miért van erre szükség? Hol használjuk?

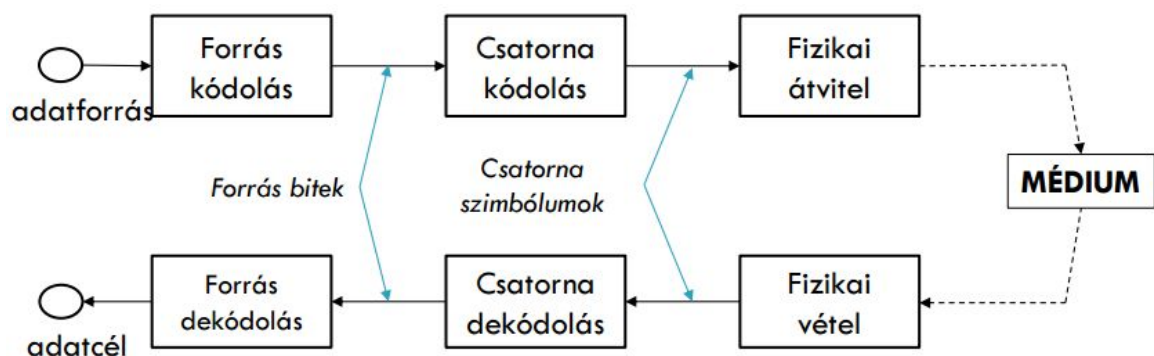
NRZI jól működik, amíg nincs csupa 0-ákból álló sorozat.

Ötlet: Kódoljunk minden 4 hosszú bitsorozatot 5-bitbe: nem lehet egynél több nulla a sorozat elején, és nem lehet kettőnél több a végén. Hátrányok: 80%-ot veszítünk a hatékonyságból.

#### 17. Mik a főbb tulajdonságai az alapsávú átvitelnek?

Fő tulajdonságai: a digitális jel direkt árammá vagy feszültséggé alakul, a jel minden frekvencián átvitelre kerül és átviteli korlátok.

#### 18. Ismertesse a digitális alapsávú átvitel struktúráját!



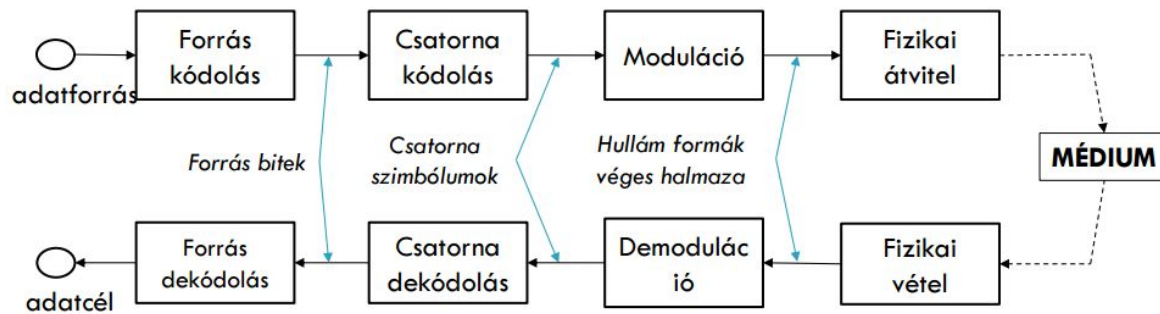
#### 19. Mik a főbb tulajdonságai a szélessávú átvitelnek?

Fő tulajdonságai: egy széles frekvencia tartományban történik az átvitel, a jel modulálására az alábbi lehetőségeket használhatjuk:

- adatok vivőhullámra "ültetése" (amplitúdó moduláció)
- vivőhullám megváltoztatása (frekvencia vagy fázis moduláció)
- különböző vivőhullámok felhasználása egyidejűleg



## 20. Ismertesse a digitális szélessávú átvitel struktúráját!



## 21. Mi az amplitúdó moduláció?

Egy szinusz rezgés amplitúdó ábrázolása  $T$  periódus idejű függvényre  $s(t) = \sin(2\pi ft + \varphi)$ , ahol  $A$  az amplitúdó,  $f$  a frekvencia és  $\varphi$  a fáziseltolás.

Az  $s(t)$  szignált a szinusz görbe amplitúdójaként kódoljuk, azaz:  $f_A(t) = s(t) * \sin(2\pi ft + \varphi)$

## 22. Mi a frekvencia moduláció?

Egy szinusz rezgés amplitúdó ábrázolása  $T$  periódus idejű függvényre  $s(t) = \sin(2\pi ft + \varphi)$ , ahol  $A$  az amplitúdó,  $f$  a frekvencia és  $\varphi$  a fáziseltolás.

Az  $s(t)$  szignált a szinusz görbe frekvenciájában kódoljuk, azaz:  $f_F(t) = a * \sin(2\pi s(t)t + \varphi)$

## 23. Mi a fázis moduláció?

Egy szinusz rezgés amplitúdó ábrázolása  $T$  periódus idejű függvényre  $s(t) = \sin(2\pi ft + \varphi)$ , ahol  $A$  az amplitúdó,  $f$  a frekvencia és  $\varphi$  a fáziseltolás.

Az  $s(t)$  szignált a szinusz görbe fázisában kódoljuk, azaz:  $f_P(t) = a * \sin(2\pi ft + s(t))$

## 3 Előadás

### 1. Ismertesse a médium többszörös használatának 5 módszerét!

Tér-, frekvencia-, idő-, hullámhossz- és kód multiplexálás.

### 2. Mi a CDMA? Ismertesse a működési algoritmusát.

A kódosztásos többszörös hozzáférés (angolul Code Division Multiple Access, röviden CDMA) a multiplexálás egy formája és a többszörös hozzáférés egy lehetséges megvalósítása, amely az adatokhoz csatornánként speciális kódokat rendel, és kihasználja a konstruktív interferencia tulajdonságát a multiplexáláshoz.

Algoritmus:

1. Minden bitidőt  $m$  darab rövid intervallumra osztunk, ezek a töredékek (angolul chip)
2. Minden állomáshoz egy  $m$  bites kód tartozik, úgynevezett töredéksorozat (angolul chip sequence)
3. Ha 1-es bitet akar továbbítani egy állomás, akkor elküldi a saját töredéksorozatát

4. Ha 0-es bitet akar továbbítani egy állomás, akkor elküldi a saját töredéksorozatának egyes komplementjét
5. m-szeres sávszélesség válik szükségessé, azaz szórt spektrumú kommunikációt valósít meg
6. Szemléltetésre bipoláris kódolást használunk: bináris 0 esetén -1, bináris 1 esetén +1, az állomásokhoz rendelt töredék sorozatok páronként ortogonálisak

### 3. Mi az a Walsh mátrix? Mire használható?

Egy olyan négyzetes mátrix, aminek a mérete csak 2 hatványa lehet és az elemei  $\pm 1$  értéket vehetnek csak fel. A CDMA használja.

### 4. Hogyan áll elő a $H(2^k)$ -nal jelölt Walsh mátrix?

$$H(2^1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad H(2^2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad \forall k \in \mathbb{N} \wedge k \geq 2 : H(2^k) = \begin{bmatrix} H(2^{k-1}) & H(2^{k-1}) \\ H(2^{k-1}) & -H(2^{k-1}) \end{bmatrix}$$

### 5. Melyek az adatkapcsolati réteg legfontosabb feladatai?

Feladatok:

- Jól definiált szolgálati interfész biztosítása a hálózati rétegnek:
  - Nyugtázatlan összeköttetés alapú szolgálat
  - Nyugtázott összeköttetés nélküli szolgálat
  - Nyugtázott összeköttetés alapú szolgálat (3 fázis)
- Átviteli hibák kezelése
- Adatforgalom szabályozása (elárasztás elkerülése)

### 6. Milyen módszereket ismer a keretezésre az adatkapcsolati rétegben?

Karakterszámlálás, bájt beszúrás, bit beszúrás, óra alapú keretezés (SONET).

### 7. Hogyan működik a karakterszámlálás?

A keretben lévő karakterek számának megadása a keret fejlécében lévő mezőben. Emiatt a vevő adatkapcsolati rétege tudni fogja a keret végét, viszont a módszer rendkívül érzékeny a hibára.

### 8. Hogyan működik a karakterbeszúrás (bájt beszúrás)?

Egy speciális FLAG bájt (jelölő bájt) jelzi az adat keret elejét és végét. Ha a FLAG szerepel az adat bájtok között, akkor egy speciális ESC bájtot szúrunk be a FLAG elé. Ha az ESC szerepel az adat bájtok között, akkor egy másik ESC bájtot szúrunk be a FLAG elé.

### 9. Hogyan működik a bit beszúrás?

Minden keret speciális bitmintával kezdődik és végződik. A kezdő és záró bitsorozat ugyanaz (pl.: 01111110 a High-level Data Link Protocol (HDLC) esetén). A Küldő az adatban előforduló minden 11111 részsorozat elé 0 bitet szúr be. A Fogadó miután az 11111 részsorozattal találkozik a fogadott adatban olvas még egy bitet. Ha ez a bit 0, akkor eltávolítja a 0-át, mivel az a bit beszúrás eredménye volt, ha 1, akkor olvas még egy bitet. Ha ezután 0-át olvas, akkor a keret végetért, ha 1-et, akkor hiba történt és eldobja a keretet, mivel ilyen nem fordulhat elő a küldő oldalon.

### 10. Hogyan működik az óra alapú keretezés (pl. SONET)?

Synchronous Optical Network, nagyon gyors optikai kábelben való átvitel. Az STS-1 keretei rögzített mérettel rendelkeznek:  $9 * 90 = 810$  bájt  $\rightarrow$  810 bájt fogadása után újabb keret-kezdő mintázat keresése.

### 11. Mit tud mondani a bájt beszúrás és a bit beszúrás hatékonyságáról legrosszabb esetben?

Bájt beszúrás: rendkívül érzékeny a hibára  
Bit beszúrás: legrosszabb esetben 20% teljesítmény csökkenés.

### 12. Definiálja a csoportos bithibát adott védelmi övezet (m) mellett!

Csoportos hiba (angolul burst error): Az átviteli csatornán fogadott bitek egy olyan folytonos sorozata, amelynek az első és utolsó szimbóluma hibás, és nem létezik ezen két szimbólummal határolt részsorozatban olyan  $m$  hosszú részsorozat, amelyet helyesen fogadtunk volna a hiba burst-ön belül. A definícióban használt  $m$  paramétert védelmi övezetnek (guard band) nevezzük.

### 13. Mi az egyszerű bithiba definíciója?

Egyszerű bithiba: az adataegység 1 bitje nulláról egyre avagy egyről nullára változik.

### 14. Definiálja egy tetszőleges S kódkönyv Hamming távolságát?

Az olyan bitpozíciók számát, amelyeken a két kódszóban különböző bitek állnak, a két kódszó Hamming távolságának nevezzük. Jelölése:  $d(x, y)$   
Legyen  $S$  egyenlő hosszú bitszavak halmaza, ekkor  $S$  Hamming távolsága az alábbi:

$$d(S) = \min_{x, y \in S \wedge x \neq y} d(x, y)$$

### 15. Mi az a Hamming korlát?

Minden  $C \subseteq \{0, 1\}^n$ , ahol  $d(C) = k (k \in \mathbb{N}_+)$ . Akkor teljesül az alábbi összefüggés:

$$|C| \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{n}{i} \leq 2^n$$

**16. Mi a kódráta és a kód távolság? Milyen a rátája és távolsága egy jó kódkönyvnek?**

Egy  $S \subseteq \{0,1\}^n$  kód rátája  $R_S = \frac{\log_2(|S|)}{n}$ . (A hatékonyságot karakterizálja)

Egy  $S \subseteq \{0,1\}^n$  kód távolsága  $\delta_S = \frac{d(S)}{n}$ . (A hibakezelési lehetőségeket karakterizálja)

A jó kódoknak a rátája és a távolsága is nagy.

**17. Milyen összefüggés ismeretes egy tetszőleges kódkönyv, a Hamming távolsága és hibajavítási képessége között?**

$d$  bithiba javításához legalább  $2d + 1$  Hamming-távolságú kód szükséges.

**18. Milyen összefüggés ismeretes egy tetszőleges kódkönyv, a Hamming távolsága és hibafelismerő képessége között?**

$d$  bithiba felismeréséhez legalább  $d + 1$  Hamming távolságú kód szükséges.

**19. Mikor érdemes hibajelző kódot és mikor hibajavító kódot használni?**

Megbízható csatornán elég a hibajelző kódot használni.

**20. Hogyan működik a Hamming kód (több paritásos módszer)?**

Egy paritást használó módszer:

1. A kódszó bitjeit számozzuk meg 1-gyel kezdődően
2. 2 egészhatvány sorszámú pozíciói lesznek az ellenőrző bitek, azaz 1,2,4,8,16...
3. A maradék helyeket az üzenet bitjeivel töltjük fel
4. Mindegyik ellenőrző bit a bitek valamilyen csoportjának a paritását állítja be párosra (vagy páratlanra)
5. Egy bit számos paritásszámítási csoportba tartozhat:
  - $k$  pozíciót írjuk fel kettő hatványok összegeként, a felbontásban szereplő ellenőrző pozíciók ellenőrzik a  $k$ -adik pozíciót
  - Példa:  $k = 13$ -ra  $k = 1 + 4 + 8$ , azaz az első, a negyedik illetve a nyolcadik ellenőrző bit fogja ellenőrizni

**21. Mi a redundancia szerepe a hibafelügyeletben?**

Egy keret felépítése:  $m$  adat bit (ez az üzenet),  $r$  redundáns / ellenőrző bit (az üzenetből lett kiszámolva, új információt nem tartalmaz). A keret teljes hossza:  $n = m + r$ . Az így előálló  $n$  bites bitsorozatot  $n$  hosszú kódszónak nevezzük!

## 4 Előadás

### 1. Mi a CRC? Mire használható?

Polinom-kód, avagy ciklikus redundancia (Cyclic Redundancy Check). Hibajelző kód.

### 2. Ismertesse a CRC-t használó algoritmus 4 lépését!

$G(x)$  egy generátor polinom, aminek a foka  $r$ , ezt a polinomot a küldő és a vevő egyaránt ismeri.

1. Fűzzünk  $r$  darab 0 bitet a keret alacsony helyiértékű végéhez, tehát az  $m + r$  bitet fog tartalmazni és reprezentálja a  $x^r M(x)$  polinomot
2.  $x^r M(x)$  elosztása  $G(x)$ -szel modulo 2 (bitsorozatok)
3. Az előző osztás maradékának kivonása  $x^r M(x)$ -ből modulo 2 (bitsorozatok), az eredmény az ellenőrző összeggel ellátott, továbbítandó keret. Jelölése:  $T(x)$
4. A vevő a  $T(x) + E(x)$  polinomnak megfelelő sorozatot kapja, ahol  $E(x)$  a hibapolinom. Ezt elosztja a  $G(x)$  generátor polinommal, ha van maradéka ennek az osztásnak, akkor hiba történt.

### 3. Mikor nem ismeri fel a hibát a vevő oldal?

A  $G(x)$  generátor polinom többszöröseinek megfelelő bithibákat nem ismerjük fel.

### 4. CRC esetén mit lehet mondani hibajelző képességéről, ha a generátor polinom $x+1$ többszöröse?

Ha  $G(x)$  generátor polinom az  $x + 1$  többszöröse, akkor minden páratlan számú hiba felismerhető.

### 5. Mutassa be röviden a korlátozás nélküli szimplex protokollt!

Az adó és a vevő mindig készen állnak. Nincs adathiba vagy adatvesztés. Nincs sem sorszámozás sem nyugta. A küldő végtelen ciklusban küldi felfele a kereteket. Nincs feldolgozási idő és végtelen puffer-területet feltételezünk. ("Utópia")

### 6. Mutassa be röviden a szimplex megáll-és-vár protokollt!

Az adó és a vevő mindig készen állnak. Nincs adathiba vagy adatvesztés. A feldolgozás ideje  $\Delta t$  (vevő), de nincs puffereles és sorban állás. A küldő egyesével küldi a kereteket és addig nem küld újat, amíg nem kap nyugtát a vevőtől.

### 7. Mutassa be röviden a szimplex protokollt zajos csatorna esetén!

Az adó és a vevő mindig készen állnak. Lehet adathiba vagy adatvesztés. A feldolgozás ideje  $\Delta t$  (vevő), de nincs puffereles és sorban állás. A küldő egyesével küldi a kereteket és addig nem küld újat, amíg nem kap nyugtát a vevőtől egy megadott határidőn belül, ha ez lejár, akkor újra küldi az aktuális keretet.

## 8. Mutassa be röviden a csúszóablak protokollt!

Egy adott időpontban egyszerre több keret is átviteli állapotban lehet, a fogadó n keretnek elég méretű puffert foglal le. Tehát a küldő legfeljebb n (ablak méretnyi) nyugtázatlan keret küldése megengedett. A keret sorozatszáma adja meg a keret méretét.

## 9. Mit neveznek adási ablaknak?

A küldő nyilvántartja a küldhető sorozatszámok halmazát.

## 10. Mit neveznek vételi ablaknak?

A fogadó nyilvántartja a fogadható sorozatszámok halmazát.

## 11. Mi a visszalépés N-nel stratégia lényege?

Az összes hibás keret utáni keretet eldobja és nyugtát sem küld róluk. Mikor az adónak lejár az időzítője, akkor az összes nyugtázatlan keretet újra küldi, kezdve a sérült vagy elveszett kerettel.

## 12. Mi a szelektív ismétléses stratégia lényege?

A hibás kereteket eldobja, de a jó kereteket a hibás után pufferelem. Amikor az adónak lejár az időzítője, akkor a legrégebbi nyugtázatlan keretet küldi el újra.

## 13. Mely 3 dolgot biztosítja a PPP protokoll?

Biztosítja a PPP protokollt:

1. Keretezési módszert (egyértelmű kerethatárok)
2. Kapcsolatvezérlő protokollt a vonalak felélesztésére, tesztelésére, az opció egyeztetésére és a vonalak elengedésére. LCP protokoll. (szinkron/aszinkron áramkörök, bájtalapú/bitalapú kódolás)
3. Olyan módot a hálózati réteg-opciók megbeszélésére, amely független az alkalmazott hálózati réteg-protokolltól. Külön-külön NCP protokollok mindegyik támogatott hálózati réteghez.

# 5 Előadás

## 1. A csatorna kiosztásra mik a legelterjedtebb módszerek?

Statikus módon (FDM, TDM)

Dinamikus módon

1. Verseny vagy ütközés alapú protokollok (ALOHA, CSMA, CSMA/CD)
2. Verseny-mentes protokollok (bittérkép-alapú protokollok, bináris visszaszámlálás)
3. Korlátozott verseny protokollok (adaptív fa protokollok).

## **2. Röviden mutassa be a frekvenciaosztásos nyálábolás módszerét!**

N darab felhasználót feltételezünk, a sávszélességet N egyenlő méretű sávra osztják, és minden egyes sávhoz hozzárendelnek egy felhasználót. Következésképpen az állomások nem fogják egymást zavarni. Előnyös a használata, ha fix számú felhasználó van és a felhasználók nagy forgalmi igényt támasztanak. Löketszerű forgalom esetén használata problémás.

## **3. Röviden mutassa be az időosztásos nyálábolás módszerét!**

N darab felhasználót feltételezünk, az időegységet N egyenlő méretű időrésre (slotra) osztják, és minden egyes réshez hozzárendelnek egy felhasználót. Löketszerű forgalom esetén a használata nem hatékony.

## **4. A csatorna modellben mit nevezünk ütközésnek?**

Ha két keret egy időben kerül átvitelre, akkor átlapolódnak, és az eredményül kapott jel értelmezhetetlenné válik.

## **5. Írja le a folytonos és a diszkrét időmodell lényegét!**

Folytonos – Mindegyik állomás tetszőleges időpontban megkezdheti a küldésre kész keretének sugárzását.

Diszkrét – Az időt diszkrét részekre osztjuk. Kerettovábbítás csak időrés elején lehetséges. Az időrés lehet üres, sikeres vagy ütközéses.

## **6. Mit jelent a vivőjel érzékelési (Carrier Sensing) képesség?**

Az egyes állomások vagy rendelkeznek ezzel a tulajdonsággal vagy nem.

1. Ha nincs, akkor az állomások nem tudják megvizsgálni a közös csatorna állapotát, ezért egyszerűen elkezdenek küldeni, ha van rá lehetőségük.
2. Ha van, akkor állomások meg tudják vizsgálni a közös csatorna állapotát a küldés előtt. A csatorna lehet: foglalt vagy szabad. Ha a foglalt a csatorna, akkor nem próbálják használni az állomások, amíg fel nem szabadul.

## **7. Hogyan működik az egyszerű ALOHA protokoll?**

Bármikor megkezdhető a küldés, ütközés esetén véletlen ideig várakozás, majd újra küldés, a fogadó nyugtázza a kereteket.

## **8. Mit jelent a keretidő az ALOHA protokoll esetén?**

Egy fix hosszúságú keret átviteléhez szükséges időt.

**9. Mennyi az Aloha protokoll esetén az áteresztőképesség (átvitel) a terhelés függvényében?**

$$S = G * e^{-2G}$$

S: azt jelöli, hogy egy keretidő alatt átlagosan hány keret jut át sikeresen

G: azt jelöli, hogy egy keretidő alatt átlagosan hány keretet küldenek az állomások összesen.

**10. Mit nevezünk sebezhetőségi időnek?**

Az az időtartam, amely alatt, ha másik keret is elküldésre kerül, akkor az aktuális keret sérül.

**11. Hogyan működik a réselt ALOHA protokoll?**

Diszkrét időmodellt használ, csak időrés elején lehet küldeni, ütközés esetén véletlen ideig vár, majd újra küldés.

**12. Mennyi a réselt Aloha protokoll esetén az áteresztőképesség a terhelés függvényében?**

$$S = G * e^{-G}$$

S: azt jelöli, hogy egy keretidő alatt átlagosan hány keret jut át sikeresen

G: azt jelöli, hogy egy keretidő alatt átlagosan hány keretet küldenek az állomások összesen.

**13. Hogyan működik az 1-perzisztens CSMA protokoll?**

Vivőjel érzékelés van, azaz minden állomás belehallgathat a csatornába. Folytonos időmodellt használ a protokoll. Keret leadása előtt belehallgat a csatornába:

1. Ha foglalt, akkor addig vár, amíg fel nem szabadul. Szabad csatorna esetén azonnal küld. (perzisztens)
2. Ha szabad, akkor küld.

Ha ütközés történik, akkor az állomás véletlen hosszú ideig vár, majd újrakezdi a keret leadását. A terjedési késleltetés nagymértékben befolyásolhatja a teljesítményét. Jobb teljesítményt mutat, mint az ALOHA protokollok.

**14. Hogyan működik a nem-perzisztens CSMA protokoll?**

Vivőjel érzékelés van, azaz minden állomás belehallgathat a csatornába. Folytonos időmodellt használ a protokoll. Mohóság kerülése. Keret leadása előtt belehallgat a csatornába:

1. Ha foglalt, akkor véletlen ideig vár (nem figyeli a forgalmat), majd kezdi előről a küldési algoritmust. (nem-perzisztens)
2. Ha szabad, akkor küld.

Ha ütközés történik, akkor az állomás véletlen hosszú ideig vár, majd újrakezdi a keret leadását. Jobb teljesítményt mutat, mint az 1-perzisztens CSMA protokoll. (intuitív)



## 15. Hogyan működik a p-perzisztens CSMA protokoll?

Vivőjel érzékelés van, azaz minden állomás belehallgathat a csatornába. Diszkrét időmodellt használ a protokoll. Adás kész állapotban az állomás belehallgat a csatornába:

1. Ha foglalt, akkor vár a következő időrésig, majd megismétli az algoritmust.
2. Ha szabad, akkor  $p$  valószínűséggel küld, illetve  $1-p$  valószínűséggel visszalép a szándékától a következő időrésig. Várakozás esetén a következő időrásben megismétli az algoritmust. Ez addig folytatódik, amíg el nem küldi a keretet, vagy amíg egy másik állomás el nem kezd küldeni, mert ilyenkor úgy viselkedik, mintha ütközés történt volna.

Ha ütközés történik, akkor az állomás véletlen hosszú ideig vár, majd újakezdi a keret leadását.

## 16. Hogyan működik a CSMA/CD protokoll? (CD $\rightarrow$ Collision Detection: ütközés érzékelés)

Minden állomás küldés közben is figyeli a csatornát, ha ütközést tapasztal, azonnal megszakítja az adást (nem adja le a teljes keretet), véletlen ideig vár, majd újra küld. Nincs szükség nyugtára, mert az állomások észlelik az ütközést.

## 17. Hogyan működik az alapvető bittérkép eljárás?

Az ütköztetési periódus  $N$  időrés. Ha az  $i$ -edik állomás küldeni szeretne, akkor az  $i$ -edik versengési időrásben egy 1-es bit küldésével jelezheti (adatszórás). A versengési időszak végére minden állomás ismeri a küldőket. A küldés a sorszámok szerinti sorrendben történik meg.

# 6 Előadás

## 1. Hogyan működik a bináris visszaszámlálás protokoll?

Alapvető bittérkép eljárások hátránya, hogy az állomások számának növekedésével a versengési periódus hossza is nő.

1. Minden állomás azonos hosszú bináris azonosítóval rendelkezik
2. A forgalmazni kívánó állomás elkezd a bináris címét bitenként elküldeni a legnagyobb helyi értékű bittel kezdve. Az azonos pozíciójú bitek logikai VAGY kapcsolatba lépnek ütközés esetén. Ha az állomás nullát küld, de egyet hall vissza, akkor feladja a küldési szándékát, mert van nála nagyobb azonosítóval rendelkező küldő
3. Következmény: a magasabb címmel rendelkező állomásoknak a prioritásuk is magasabb az alacsonyabb című állomásokénál.

## 2. Mi a korlátozott versenyekes protokollok célja?

Ötvözni a versenyhelyzetes és ütközésmentes protokollok jó tulajdonságait.

### 3. Hogyan működik az adaptív fabejárési protokoll?

Adaptív fabejárési protokoll:

- 0-adik időrésben mindenki küldhet (Ha ütközés történik, akkor megkezdődik a fa mélységi bejárása)
- A rések a fa egyes csomópontjaihoz vannak rendelve
- Ütközéskor rekurzívan az adott csomópont bal illetve jobb gyerekcsomópontjánál folytatódik a keresés
- Ha egy bitrés kihasználatlan marad, vagy pontosan egy állomás küld, akkor a szóban forgó csomópont keresése befejeződik

### 4. Mi a repeater, és mire használják?

Analóg eszköz, mely két kábelszegmenshez csatlakozik. Felerősíti a jelet és továbbítja. (fizikai réteg)

### 5. Mi az elosztó (Hub) és mire használják?

Több bemenettel rendelkezik, a beérkező keretet minden vonalon továbbítja, ha két keret egyszerre érkezik, ütközni fognak! Általában nem erősíti a jelet. (fizikai réteg)

### 6. Mi a bridge (híd), és mire használják?

Az adatkapcsolati rétegben működő eszköz, amely LAN-ok összekapcsolását végzi. A bejövő keretet csak a megfelelő LAN-hoz továbbítja (forgalomirányítás az adatkapcsolati rétegben). A portok külön ütközési tartományt képeznek és különböző sebességű hálózatokhoz csatlakozhatnak. Pufferelést, csomagfeldolgozást végez, továbbító táblázatot (forwarding table) tart karban.

### 7. Mi a "backward learning" (Címek tanulása) lényege?

A hidak használják ezt a módszert a keretek továbbításához használt táblázatuk feltöltésére. Ha egy keret érkezik hozzájuk, megnézik a forráscímet (feladót) és "megtanulják", hogy az melyik porton érhető el (ahonnan a keret jött), és ezt bejegyzik a táblázatukba.

### 8. Ismertesse a feszítőfa protokoll (STP) lépéseit?

Feszítőfa: egy gráf éleinek részhalmaza, melyre teljesül, hogy lefed minden csomópontot és körmentes.

1. Az egyik bridge-et megválasztjuk a fa gyökerének
2. Minden bridge megkeresi a legrövidebb utat a gyökérhez
3. Ezen utak unióját véve megkapjuk a feszítőfát

## 9. Mi a forgalomirányító algoritmusok definíciója?

A hálózati réteg szoftverének azon része, amely azért a döntésért felelős, hogy a bejövő csomag melyik kimeneti vonalon kerüljön továbbításra. A folyamat két jól-elkülöníthető lépésre bontható fel: forgalomirányító táblázatok feltöltése, karbantartása és továbbítás.

## 10. Mi a statikus (nem adaptív) forgalomirányító algoritmusok fő jellemzője?

Offline meghatározás, betöltés a router-ekbe induláskor.

## 11. Mi az adaptív forgalomirányító algoritmusok fő jellemzője?

A topológia és rendszerint a forgalom is befolyásolhatja a döntést.

## 12. Mit mond ki az optimalitási elv (forgalomirányítás esetén)?

Ha  $J$  router az  $I$  router-től  $K$  router felé vezető optimális útvonalon helyezkedik el, akkor a  $J$ -től a  $K$ -ig vezető útvonal ugyanerre esik.

## 13. Mi a távolságvektor (distance vector) alapú forgalomirányítás lényege?

Minden router-nek egy táblázatot kell karbantartania, amelyben minden célhoz szerepel a legrövidebb ismert távolság, és annak a vonalnak az azonosítója, amelyiken a célhoz lehet eljutni. A táblázatokat a szomszédoktól származó információk alapján frissítik.

# 7 Előadás

## 1. Socket programozás - Ehhez az előadáshoz nem tartoznak kérdések!

# 8 Előadás

## 1. Magyarazza el a végtelenig számolás problémáját!

Ha egy állomás ( $A$ ) meghibásodik a közvetlen szomszédja ( $B$ ) észleli, hogy a költség végtelen lett, mert nem érkezik  $A$ -tól csomag.  $B$ -nek egy szomszédja ( $C$ ), amelyik korábban  $B$ -n keresztül érte el  $A$ -t, elküldi  $A$  elérési költségét.  $B$  azt fogja hinni, hogy  $C$ -n keresztül  $A$  elérhető, és a  $C$ -től kapott költséget megnöveli  $B-C$  költséggel, majd ezt küldi vissza  $C$ -nek. Ezután mindketten folyamatosan azt fogják hinni, hogy a másikon keresztül  $A$  elérhető, és minden lépésben  $B - C$  költséggel növelik  $A$  elérési költségét a táblázatukban.

## 2. Mik a link-state (kapcsolatállapot) alapú forgalomirányítás megvalósításának lépései?

Link-state routing:

1. Szomszédok felkutatása, és hálózati címeik meghatározása
2. Megmérni a késleltetést vagy költséget minden szomszédhoz
3. Egy csomag összeállítása a megismert információkból
4. Csomag elküldése az összes többi router-nek
5. Kiszámítani a legrövidebb utat az összes többi router-hez (Dijkstra algoritmusát használják).

**3. Hasonlítsa össze a távolságvektor alapú és a link-state (kapcsolatállapot) alapú forgalomirányítást.**

Az első esetében a routerek minden más routerre vonatkozó általuk ismert költséget elküldenek, de csak a közvetlen szomszédoknak. A második esetében csak a szomszédokra vonatkozó ismert költségeket küldik el mindenkinek.

**4. Mi a hierarchikus forgalomirányítás lényege?**

A router-eket tartományokra osztjuk. A saját tartományát az összes router ismeri, de a többi belső szerkezetéről nincs tudomása. Nagy hálózatok esetén többszintű hierarchia lehet szükséges.  $N$  darab router-ből álló alhálózathoz az optimális szintek száma  $\ln N$ , amely router-enként  $e * \ln N$  bejegyzést igényel.

**5. Mit nevezünk adatszórásnak vagy broadcasting-nak?**

Adatszórás (vagy angolul broadcasting): egy csomag mindenhová történő egyidejű küldése.

**6. Sorolja fel az adatszórás megvalósítási lehetőségeit.**

Külön csomag küldése, elárasztás, többcélú forgalomirányítás (vagy angolul multidestination routing), a forrás router-hez tartozó nyelőfa használata, visszairányú továbbítás.

**7. Mi a többcélú forgalomirányítás lényege?**

Csomagban van egy lista a rendeltetési helyekről, amely alapján a router-ek eldöntik a vonalak használatát, mindegyik vonalhoz készít egy másolatot és belerakja a megfelelő célcím listát.

**8. Mi a visszairányú továbbítás (reverse path forwarding) lényege?**

Amikor egy adatszórásos csomag megérkezik egy routerhez, a router ellenőrzi, hogy azon a vonalon kapta-e meg, amelyen rendszerint ő szokott az adatszórás forrásához küldeni. Ha igen, akkor nagy esély van rá, hogy az adatszórásos csomag a legjobb utat követte a router-től, és ezért ez az első másolat, amely megérkezett a router-hez. Ha ez az eset, a router kimásolja minden vonalra, kivéve arra, amelyiken érkezett. Viszont, ha az adatszórásos csomag más vonalon érkezett, mint amit a forrás eléréséhez előnyben részesítünk, a csomagot eldobják, mint valószínű másodpéldányt.

**9. Mit nevezünk többesküldésnek vagy multicasting-nak?**

Többes-küldés (vagy angolul multicasting): egy csomag meghatározott csoporthoz történő egyidejű küldése.

**10. Mire szolgál a DF bit az IPv4 fejlécében?**

DF: "ne darabold" flag a router-eknek.

**11. Mire szolgál a MF bit az IPv4 fejlécében?**

MF: "több darab" flag, minden darabban be kell legyen állítva, kivéve az utolsót.

**12. Mire szolgál az azonosító (azonosítás) az IPv4 fejlécében?**

Azonosítás: egy datagram minden darabja ugyanazt az azonosítás értéket hordozza.

**13. Mire szolgál a darabeltolás (fragment offset) az IPv4 fejlécében?**

Darabeltolás: a darab helyét mutatja a datagramon belül. (elemi darab méret 8 bájt)

**14. Mire szolgál az élettartam (TTL) mező az IPv4 fejlécében?**

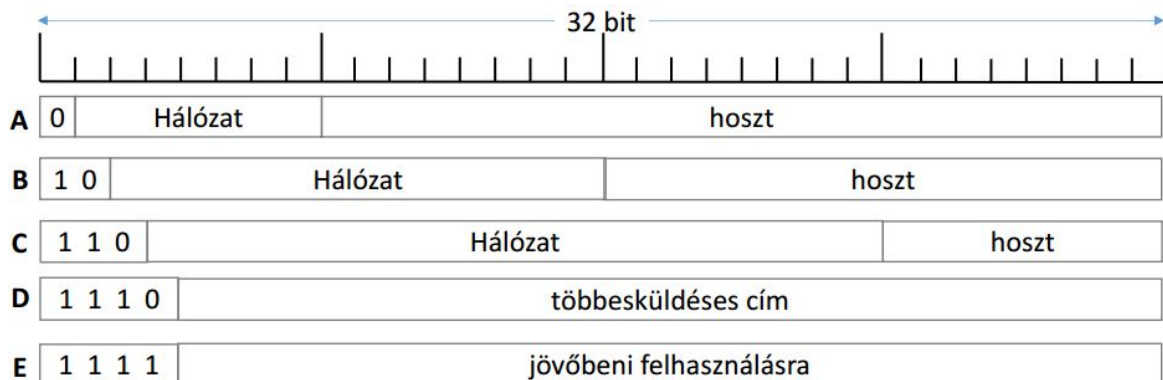
Élettartam: másodpercenként kellene csökkenteni a mező értékét, minden ugrásnál csökken-tik eggyel az értékét.

**15. Mi az IPv4 cím és hogyan ábrázoljuk?**

Minden hoszt és minden router az Interneten rendelkezik egy IP-címmel, amely a hálózat számát és a hoszt számát kódolja (egyedi kombináció). 4 bájton ábrázolják, pontokkal elválasztott decimális rendszerben írják a számokat (0-255).

**16. Milyen IP cím osztályokat ismer? Jelemezze ezeket!**

Több évtizeden keresztül 5 osztályos címzést használtak: *A, B, C, D* és *E*.



**17. Milyen speciális IPv4 címek léteznek?**

Van pár speciális cím. Lásd az alábbiakban:

0 0	Ez egy hoszt.	
0..0	hoszt	Ez egy hoszt ezen hálózaton.
1 1	Adatszórás a helyi hálózaton.	
Hálózat	1..1	Adatszórás egy távoli hálózaton.
0 1 1 1 1 1 1 1	(bármilyen)	Visszacsatolás.

## 18. Mi az alhálózati maszk és mire szolgál?

Segítségével elkülöníthető a hálózati azonosító és az állomás azonosító. Az IP cím hálózati részével megegyező hosszúsággal 1-est, utána 0-kat tartalmaz.

## 19. Mi az a NAT doboz és mire szolgál?

(Network Address Translation - hálózati címfordítás) Hálózati címfordítást végez. A vállalaton belüli globálisan nem egyedi IP címeket globálisan egyedi IP címre fordítja.

# 9 Előadás

## 1. Mi az az MTU és mire szolgál?

MTU: Maximum Transmission Unit – lényegében a maximális használható csomag méret egy hálózatban.

## 2. Hogyan működik az MTU felderítés?

MTU felderítő protokoll:

1. Csomagküldés a "don't fragment" flag bittel
2. Folyamatosan csökkentjük a csomag méretét, amíg egy meg nem érkezik

## 3. Hogyan ÉS hol történik az fragmentált/darabolt IP csomagok helyreállítása?

A végponton történik a hossz és eltolás (offset) ismeretében.

## 4. Mi az IPv6 cím és hogyan ábrázoljuk?

Az IPv4 kibővítése. 128 bites címek,  $4.8 * 10^{28}$  cím / ember. Formátum: 16 bites értékek 8 csoportba sorolva (':'-tal elválasztva), minden csoport elején szereplő nulla sorozatok elhagyhatók és csupa nulla csoportok elhagyhatók, ekkor '::'.

## 5. Mi a localhost IPv6 esetén?

A localhost IPv6 esetén: ::1.

## 6. Soroljon fel két olyan lehetőséget (az EA-on látott 4-ből), melyet az IPv6 támogat, de az IPv4 esetén nem találkoztunk vele?

Forrás routing, mobil IP, privacy kiterjesztések és jumbograms.

## 7. Mi gátolja az IPv6-ra való átállást?

IPv6 bevezetése a teljes Internet frissítését jelentené, minden router, minden hoszt.

## 8. Hogyan oldható meg az IPv6 csomagok átvitele IPv4 hálózaton felett?

Tunneleket használunk az IPv6 csomagok becsomagolására és IPv4 hálózaton való továbbítására.

## 9. Mire szolgál az ICMP protokoll?

Internet Control Message Protocol, váratlan események jelentésére használjuk. Többféle ICMP-üzenetet definiáltak:

- Elérhetetlen cél
- Időtúllépés
- Paraméter probléma
- Forráslefojtás
- Visszhang kérés
- Visszhang válasz
- ...

## 10. Mire szolgál az ARP és hogyan működik?

Feladata az IP cím megfeleltetése egy fizikai címnek. (Address Resolution Protocol)  
Adatszóró csomag kiküldése az Ethernetre "Ki-e a 192.60.34.12-es IP-cím?" kérdéssel az alhálózaton, és mindenegyes hoszt ellenőrzi, hogy övé-e a kérdéses IP-cím. Ha egyezik az IP a hoszt saját IP-jével, akkor a saját Ethernet címével válaszol. Erre szolgál az ARP.

## 11. Mire szolgál a RARP és hogyan működik?

Feladata a fizikai cím megfeleltetése egy IP címnek. (Reverse Address Resolution Protocol)  
Az újonnan indított állomás adatszórással csomagot küld ki az Ethernetre "A 48-bites Ethernet-címem 14.04.05.18.01.25. Tudja valaki az IP címemet?" kérdéssel az alhálózaton. Az RARP-szerver pedig válaszol a megfelelő IP címmel, mikor meglátja a kérést.

## 12. Mi az a DHCP és hogyan működik?

Lehetővé teszi a dinamikus IP címkiosztást. A kliensek a DHCP esetén egy (megújítható) időszakra kapják az IP címet. A kiszolgáló másik LAN-on is lehet; DHCP közvetítő van LAN-onként

## 13. Milyen lehetőségeket támogat a DHCP?

IP címek kiosztása MAC cím alapján vagy dinamikusan. További hálózati paraméterek kiosztása (hálózati maszk, névkiszolgáló, domain név stb.)

#### 14. Mi DHCP esetén a cím bérlet?

A DHCP szerver a klienseknek az IP-címeket bizonyos bérleti időtartamra adja "bérbe".

#### 15. Mi az AS (Autonóm rendszer)?

Az Internet egy két szintű hierarchiába van szervezve. Első szint: autonóm rendszerek (AS-ek), egy adminisztratív tartomány alatti hálózat. Pl.: ELTE, Comcast, AT&T, Verizon, Sprint, ...

#### 16. Miért van szükségünk AS-ekre?

Okok:

- A routing algoritmusok nem elég hatékonyak ahhoz, hogy a teljes Internet topológián működjenek
- Különböző szervezetek más-más politika mentén akarnak forgalom irányítást (policy)
- Lehetőség, hogy a szervezetek elrejtsek a belső hálózatuk szerkezetét
- Lehetőség, hogy a szervezetek eldöntsék, hogy mely más szervezeteken keresztül forgalmazzanak
- Röviden: egyszerűbb az útvonalak számítása, nagyobb rugalmasság és nagyobb autonómia/függetlenség.

#### 17. Mi azonosít egy AS-t?

Minden AS-t egy AS szám (ASN) azonosít, ami egy 16 bites érték (a legújabb protokollok már 32 bites azonosítókat is támogatnak).

#### 18. Milyen routing megoldást/protokollt alkalmaz a BGP?

Path vector (útvonalvektor) protokollt.

#### 19. Hogyan működik az útvonalvektor protokoll?

A távolságvektor protokoll kiterjesztése. A teljes útvonalat meghirdeti (nem csak a következő ugrást).

#### 20. Mit értünk az alatt, hogy minden AS saját útválasztási politikát alkalmazhat?

Az AS-en belüli protokoll független a többi AS-tól.

#### 21. Sorolja fel az IGP, iBGP és eBGP szerepét?

Szerepeik:

- IGP: útválasztás egy AS-en belül belső célállomáshoz
- iBGP: útválasztás egy AS-en belül egy külső célállomáshoz
- eBGP: routing információk cseréje autonóm rendszerek között



## 22. Mikor mondjuk két AS-ről, hogy azok össze vannak kötve?

Ha van közöttük a BGP routereiket összekötő vonal.

## 23. Adjon meg 3 példát forgalomirányítási korlátozásra AS-ek közötti routing esetén.

Kereskedelmi forgalom ne menjen keresztül oktatási hálózaton. IBM forgalma ne menjen át a Microsoft-on. Albánián csak végszükség esetén haladjunk át.

## 24. Mit nevez a BGP csonka hálózatnak?

Azon hálózatok, amelyeknek csak egyetlen összeköttetésük van a BGP gráffal ezek csak egy útválasztón keresztül küldhetik a forgalmat.

## 25. Mit nevez a BGP többszörösen bekötött hálózatnak? Mit nevez a BGP tranzit hálózatnak?

Többszörösen bekötött hálózat: amelyeket használhatna az átmenő forgalom, de ezek ezt megtagadják. Nem hajlandók átengedni a forgalmat tetszőleges AS felé (nics velük szerződés).

Tranzit hálózat: amelyek némi megkötéssel, általában fizetség ellenében, készek kezelni harmadik fél csomagjait.

# 10 Előadás

## 1. Mire szolgál a TCP protokoll? Mik a főbb jellemzői?

Megbízható, sorrend helyes, kétirányú bájt folyamat létrehozására (Transmission Control Protocol). Port számok teszik lehetővé a demultiplexálást, kapcsolat alapú, folyam vezérlés, torlódás vezérlés, fair viselkedés. 20 bájtos fejléc + options fejlécek.

## 2. Mire szolgál az UDP protokoll? Mik a főbb jellemzői?

8 bájtos UDP fejléc (User Datagram Protocol). Egyszerű, kapcsolat nélküli átvitel. Port számok teszik lehetővé a demultiplexálást, 16 bit  $\rightarrow$  65535 lehetséges port, 0 port nem engedélyezett. Kontrollösszeg hiba detektáláshoz, felismeri a hibás csomagokat viszont nem ismeri fel az elveszett, duplikátum és helytelen sorrendben beérkező csomagokat.

## 3. Hogyan történik egy TCP kapcsolat felépítése? Mik a lépései?

A TCP kapcsolat felépítése fontos TCP flagek (SYN, ACK, FIN) segítségével történik.

1. SYN szegmens elküldése, SYN bit: 1-es. (connect hívás)
2. A fogadó nyugtázza és ő is küld egy SYN szegmenst, SYN bit és ACK bit 1-es. (accept)
3. A küldő nyugtázza a megkapott SYN szegmenst. (első send hívás)

#### 4. Hogyan történik egy TCP kapcsolat lezárása?

Két félig-lezárással, amit mindkét oldal kezdeményezhet. Félig-lezárás: a küldő küld egy FIN szegmenst (FIN bit 1-es), jelezve, hogy nem fog több adatot küldeni.

#### 5. Mit mondhatunk a TCP átviteléről az ablak és az RTT függvényében?

Az átvitel arányos a  $\frac{ablak}{RTT}$ -vel. Nagy ablakméret, vagy kis RTT esetén gyorsul az átvitel.

#### 6. Mit jelent az RTO, és hol használják?

Ez szabályozza az időközt a küldés és egy duplikátum újraküldése között, ha egy nyugta kimarad. (Retransmission Timeout)

#### 7. Hogyan történik az RTT becslés az eredeti TCP esetén?

RTT becslése mozgóátlaggal:  $new\_rtt = \alpha * (old\_rtt) + (1 - \alpha) * (new\_sample)$   
Javasolt  $\alpha : 0.8 - 0.9$  (0.875 a legtöbb TCP esetén).

#### 8. Mit mondhatunk TCP esetén a hibadetektálásról?

Hibamentes átvitelt biztosít. Mivel a csomaghibát, sorrendhibát, elveszett és a duplikált csomagot is detektálja.

#### 9. Mi a fogadó által felajánlott ablakméret (*wnd*)?

A fogadó ezzel a mérettel jelzi, hogy mennyi adatot tud pufferelni, vagyis ez a csúszóablak protokollnál megismert fogadási ablak mérete. A tényleges ablakméretet (*wnd*) több paraméter határozza meg.

#### 10. Mit jelent, ha a fogadó *wnd* = 0-át küld?

A fogadó puffere tele van, átmenetileg nem tud több adatot fogadni (gyors adó).

#### 11. Mit nevezünk folyamvezérlésnek?

A folyamvezérlés azt szabályozza, hogy a küldő milyen ütemezéssel küldheti az adatokat. Túl sok csomag túlterhelné a fogadót. A megoldás: csúszóablak.

#### 12. Mit nevezünk torlódásnak TCP esetén?

Amikor a hálózat terhelése nagyobb, mint a kapacitása.

#### 13. Mi a TCP Nagle algoritmus működési alapelve?

Nagle algoritmus:

1. Ha az ablak  $\geq$  MSS (Maximum Segment Size) és az elérhető adat  $\geq$  MSS, akkor küldjük el az adatot (egy teljes csomag küldése)
2. Különben, ha van nem nyugtázott adat, akkor várakoztassuk az adatot egy pufferben, amíg nyugtát nem kapunk
3. Különben, küldjük az adatot (küldjük egy nem teljes csomagot, ha nincs más)

#### 14. Mi a TCP Karn algoritmusa? A kapcsolódó problémát is ismertesse!

Hogyan becsüljük meg az RTT-t? Megmérjük a küldés és a válasz között eltelt időt. A probléma: a válasz félreértelmezhető újraküldés esetén. Karn algoritmusa: dobjuk el azokat a mintákat, melyek egy csomag újraküldéséből származnak.

#### 15. Vázzon a TCP Incast problémát!

Sok szimultán küldő egy fogadóhoz, ami miatt a switchek pufferei megtelítődnek és csomagok vesznek el és a nyugta nem megy vissza.

### 11 Előadás

#### 1. Mi az a torlódási ablak? Mire szolgál?

Az az ablakméret ( $cwnd$ ), ami a nyugták illetve csomagvesztések hatására nő, illetve csökken. Ha nyugta jött  $\rightarrow$  nincs torlódás (nő). Ha elveszett egy csomag  $\rightarrow$  torlódás lehet (csökken). A ténylegesen elküldhető adatok mennyiségét, vagyis a csúszóablak protokollnál megismert küldési ablak méretét e két ablak minimuma adja:  $wnd = \min\{adv\_wnd, Cwnd\}$ .  $adv\_wnd \rightarrow$  a fogadóra tekintettel és  $Cwnd \rightarrow$  a torlódás miatt.

#### 2. Mi az a "slow start" TCP esetén?

A küldőnek nem szabad a fogadó által felajánlott ablakméretet ( $adv\_wnd$ ) azonnal elfogadnia (a hálózatot nem szabad azonnal maximálisan terhelnie), inkább fokozatosan növeli a terhelést. Kezdetben  $cwnd = 1$  szegmens, majd nyugtázott csomagonként növeli egy szegmessel ( $MSS$ ) a torlódási ablak méretét, egész addig, amíg el nem ér egy határt ( $ssthresh$ ) vagy csomagvesztés nem történik.

#### 3. Mi az AIMD TCP Tahoe esetén?

Additive Increase Multiplicative Decrease (additív növelés, multiplikatív csökkentés). Az elküldhető csomagok számát (valójában  $cwnd$ -t) additív módon növeljük ha még nem értük el a hálózat kapacitását, és multiplikatív módon csökkentjük, ha már elértük. Ezt a stratégiát a slow start után, a torlódás elkerülési fázisban alkalmazza a TCP.

#### 4. Mi a gyors újraküldés TCP RENO esetén?

Ha csak egy csomag veszik el, akkor NEM várjuk meg a timeoutot ( $RTO$ ), hanem újraküldjük a csomagot és folytatjuk a küldést. Az egy csomag elveszését a háromszoros nyugtaduplikátum jelzi. Ezt még a TCP Tahoe is ugyanígy csinálja.

#### 5. Mit jelenthet az ha három nyugta-duplikátum érkezik egymás után?

Hogy valószínűleg elveszett egy csomag (lehet, hogy csak késik), de az utána következők megérkeztek, hiszen emiatt jönnek ugyanolyan sorszámú nyugták duplikátumai. Ha az utána következők is elvesztek volna, akkor semmilyen nyugta nem érkezne, hanem timeout lenne.

## 6. Mi a gyors visszaállítás TCP Reno esetén?

A gyors újraküldés után felezzük  $cwnd$ -t (ez a Multiplikatív Decrease), azaz nem állítjuk vissza 1-re (elkerüljük a lassú indulást). A TCP Tahoe ilyen esetben a lassú indulás fázisba lépne. Ha az RTO lejár akkor  $cwnd = 1$  lesz (lassú indulás) Tahoe és Reno esetén is.

## 7. Mivel több a TCP NewReno? Mi a problémája az alkalmazott megoldásnak?

Minden duplikált ACK egy újabb csomag elküldését (nem újraküldést) váltja ki. Probléma: ha egy csomag  $> 3$ -mal eltér a sorrendjétől, az felesleges gyors helyreállítást és ezzel felesleges újraküldést okoz.

## 8. Mi a probléma nagy késleltetés-sávszélesség szorzatú hálózatok esetén?

Sok a szállítás alatt lévő adatmennyiség. A slow start és additív increase lassan konvergál.

## 9. Mely TCP variánsok használatosak napjainkban?

TCP NewReno, TCP Vegas, Compound TCP, TCP BIC, TCP CUBIC stb.

## 10. Hogyan működik a Compound TCP?

Reno alapú, két torlódási ablak, egy késleltetés alapú ( $dwnd$ ) és egy vesztes alapú ( $cwnd$ ). Ha nő az  $RTT$ ,  $dwnd$  csökken, ha csökken az  $RTT$ ,  $dwnd$  nő.  
 $wnd = \min\{cwnd + dwnd, adv\_wnd\}$   
Hátrány: folyamatos  $RTT$  becslést igényel.

## 11. Hogyan működik a CUBIC TCP?

Alap TCP implementáció Linux rendszereken. Az AIMD helyettesítése egy "köbös" (CUBIC) függvényvel:

$$W_{cubic} = C(T - K)^3 + W_{max}$$
$$C \text{ egy konstans, } K = \sqrt[3]{\frac{W_{max}\beta}{C}}$$

## 12. Mik a TCP problémái kis folyamatok esetén?

Nincs lehetőség felgyorsulni a kevés adat miatt. Szinte végig a slow start fázisban marad.

## 13. Mik a TCP problémái vezeték nélküli hálózatok esetén?

Itt a csomagvesztés gyakoribb, és nem jelent torlódást, ahogy a TCP hiszi.

## 14. Mi a DoS támadás? Miért probléma ez TCP esetén?

Denial of Service. A TCP kapcsolatok állapottal rendelkeznek, a SYN csomagok erőforrást foglalnak le a szerveren. A DoS támadás abból áll, hogy meglehetősen sok SYN csomagot küldenek a szervernek, aminek a hatására elfogy a memóriája és összeomlik.