

Alapok, TCP/IP, IPv6, Routing

Hálózati szolgáltatások

1. Alapok, TCP/IP, IPv6, Routing

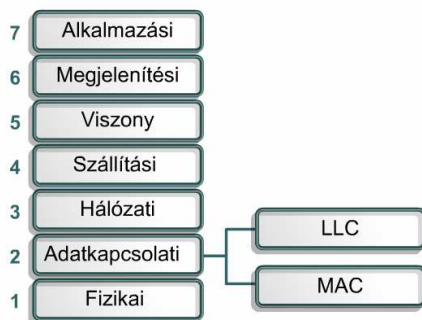
Informatikus
(rendszerinformatikus)

Ismétlés: fogalmak

- Rétegek
- Forrás, cél
- Adatcsomag
- Átviteli közeg
- Protokoll

2

Ismétlés: OSI rétegmódel



3

A TCP/IP modell



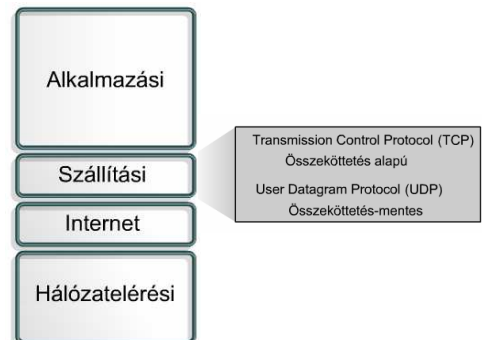
4

A TCP/IP modell



5

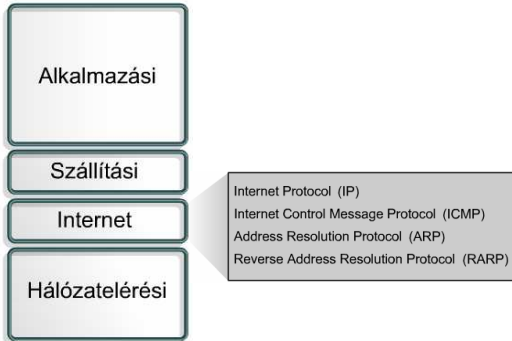
A TCP/IP modell



6

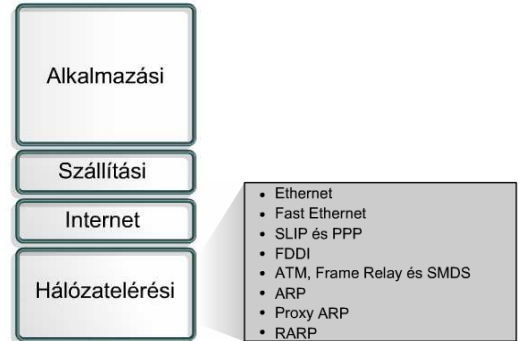
Alapok, TCP/IP, IPv6, Routing

A TCP/IP modell



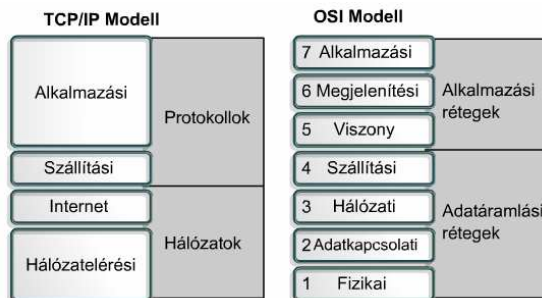
7

A TCP/IP modell



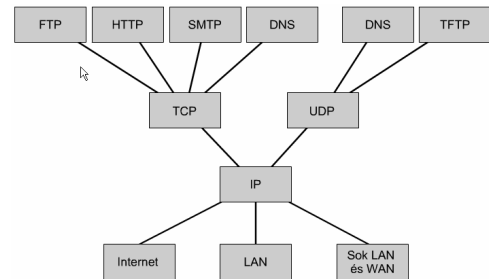
8

OSI és TCP/IP



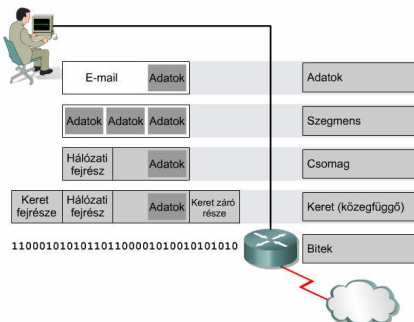
9

A TCP/IP protokollgráfja



10

Adatbeágyazás



11

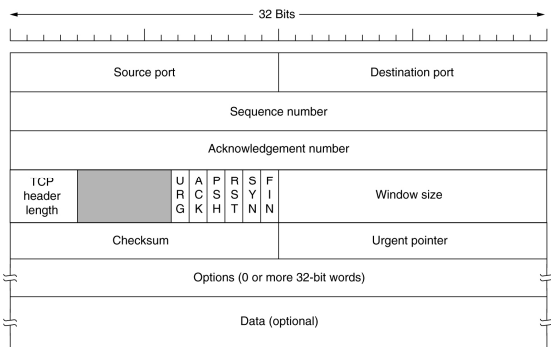
TCP

- Az Internet szállítási rétege
- *Transmission Control Protocol* - átvitel vezérlési protokoll
- megbízhatatlan (C típusú) alhálózatokkal is együttműködik

12

Alapok, TCP/IP, IPv6, Routing

TCP fejrész



TCP fejrész

- Forrásport, célport A minimális TCP fejrész 20 bájtos.
- A **FORRÁS**PORT és a **CÉL**PORT mezők az összeköttetések végpontjait (TSAP-címek az OSI terminológia szerint) azonosítják. Minden egyes hozsnak magának kell eldöntenie, hogy miképpen allokálja (osztja ki) a portjait.
- A **SORSZÁM** és a **RÁÜLTETETT NYUGTA** mezők a szokásos funkcióikat hajtják végre. A TCP minden bájtot megsorszámoz, ezért 32 bit hosszúak.
- A **FEJRÉSZ HOSSZ** kijelöli, hogy a TCP fejrész hány 32 bites szót tartalmaz. Erre az információra az Opció mező változó hossza miatt van szükség.

14

TCP fejrész

- Ezután hat jelzőbit következik.
 - Az **URG** jelző akkor 1, ha a protokoll használja a **SÜRGŐSSÉGI MUTATÓ**-t (Urgent pointer). Ez valójában egy eltolási értéket ad meg, amely az aktuális sorszámtól számolva kijelöli a sürgős adatok helyét.
 - A **SYN** és **ACK** biteknek összeköttetés létesítések van funkciója. Összeköttetés kérésekor SYN=1, valamint ACK=0 annak jelzésére, hogy a ráültetett nyugta mező nincs használatban. Az összeköttetés válaszában van nyugta, így SYN=1 és ACK=1.
 - A **FIN** az összeköttetés lebontására használható, azt jelzi, hogy a küldőnek nincs több adata.
 - A hoszt hibák miatti nem jó állapotba került összeköttetéseit az **RST** bit használatával lehet megszüntetni.
 - A **PSH** bit a késedelem nélküli adattovábbítást jelzi a vevőnek, hogy ne puffereljen, hanem azonnal továbbítsa a vett adatot az alkalmazás felé

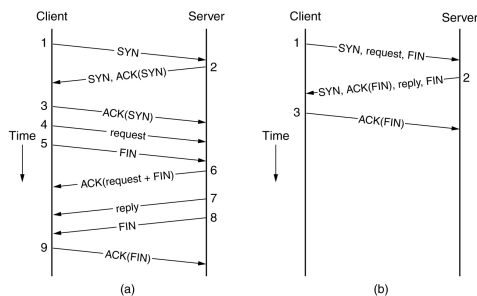
15

TCP fejrész

- A TCP-beli forgalomszabályozás változó méretű forgóablakot használ. 16-bites mezőre van szükség, mivel az **ABLAK** azt adja meg hogy hány bájtot lehet még elküldeni.
- Az **ELLENŐRZŐÖSSZEG** képzési algoritmus egyszerű: 16-bites szavakként az adatokat összegzik, majd az összeg 1-es komplementjét veszik. Vételkor a képződött összeghez ezt hozzáadva, hibátlan átvitel esetén nullát kapunk.
- Az **OPCIÓK** mező különféleképpen használható fel, pl. összeköttetés létesítése során a puffer-méret egyeztetésére.

16

Transitional TCP



- (a) RPC using normal TPC.
(b) RPC using T/TCP.

17

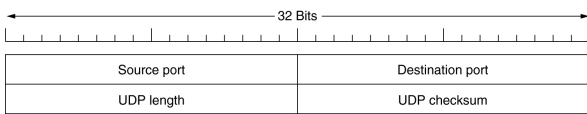
UDP, TCP

- Az IP használata csak a TCP-vel kiegészítve praktikus az alkalmazások számára;
- A TCP visszaigazolást feltételez
- A kérdés-felelet kapcsolat során a válasz maga a visszaigazolás, ezért a TCP-nél egyszerűbb protokoll is elegendő:
- Ez az UDP (pl. DNS használja)

18

Alapok, TCP/IP, IPv6, Routing

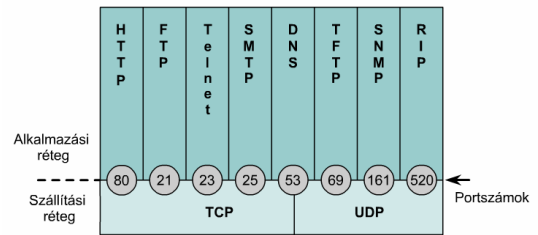
UDP



- A legtöbbet használt ilyen protokoll az UDP (user datagram protocol — felhasználói datagram protokoll). Hasonlóképpen illeszkedik a rendszerbe, mint a TCP. A hálózati szoftver az adatok elejére ráilleszti az UDP fejléct ugyanúgy, ahogy a TCP fejléc esetében teszi. Az UDP ezek után az IP-nek adja át a datagramot. Az IP hozzáteszi a saját fejlécét, amibe a TCP helyett az UDP protokollszámát helyezi el a Protokoll mezőben (lásd IP fejléc). Az UDP csak portszámokat biztosít, hogy egyszerre több program is használhassa a protokollt. Az UDP portszámok ugyanúgy használhatók, mint a TCP portszámok. Az UDP-t használó kiszolgálókhöz is léteznek jól ismert portszámok. Látható, hogy az UDP fejléc sokkal rövidebb, mint a TCP fejléce.

19

A TCP- és UDP-portszámok



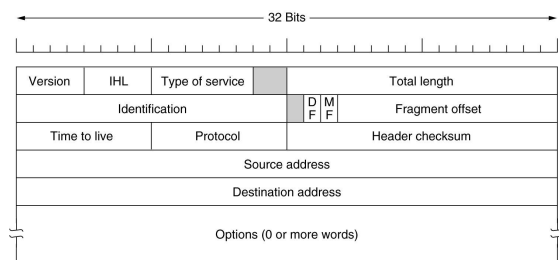
20

IP

- A TCP/IP modell hálózati rétege;
- Összeköttetésmentes
- Datagram, részei
 - fejrész
 - szövegrész

21

IP fejrész



22

IP fejrész

- A **VERZIÓ** mező a protokoll verzióját azonosítja, így a protokoll módosítását is ezzel figyelembe lehet venni.
- Az **IHL** adja a fejrész teljes hosszát 32 bites egységekben (20bájt+opció rész). Minimális értéke:5. (Nincs opció.)
- A **SZOLGÁLAT TÍPUS** mező teszi lehetővé a hoszt számára, hogy jelölje az alhálózattól kívánt szolgálat típusát. Különböző sebességek és megbízhatósági fokok különböző kombinációi között lehet választani.

23

IP fejrész

- A **TELJES HOSSZÚSÁG** mező a teljes datagram hosszát tartalmazza (fejrész+adat). A maximális hosszúság 65 536 bájt.
- Az **AZONOSÍTÁS** mező alapján állapítja meg a célhoszt, hogy egy újonnan érkezett csomag melyik datagramhoz tartozik. Egy datagram minden egyes darabja ugyanazzal az Azonosítás mező értékkel rendelkezik.
- Ezután egy nem használt bit, majd két 1-bites mező következik.

24

Alapok, TCP/IP, IPv6, Routing

IP fejrész

- Az azonosítás után egy nem használt bit, majd két 1-bites mező következik.
- A **DF** mező a Don't Fragment (ne tördelj!) kifejezés rövidítése. Ha ez a bit 1 értékű, akkor az átjárók nem tördelhetik a datagramot, mert a célállomás képtelen azt ismét összerakni. Ha a datagram nem vihető keresztül a hálózaton, akkor vagy kerülő utat kell választani, vagy el kell dobni.
- Az **MF** mező neve a More Fragments (több darab) rövidítése. A széttördelt datagramdarabokat jelzi, kivéve az utolsót. A Teljes hosszúság mező mintegy második ellenőrzésként használható, vajon nem hiányzik-e datagramdarab, és hogy az egész datagram összeállt-e.

25

IP fejrész

- a **DATAGRAMDARAB-ELTOLÁS** mező, ami azt jelöli ki, hogy az adott darab hol található a datagramban. Minden datagramdarab hosszúságának, (kivéve az utolsót), 8 bájt egész számú többszörösének kell lennie, amely az elemi datagramdarab hosszúsága. Mivel e mező 13 bit hosszú, ezért maximálisan 8192 darabból állhat egy datagram, amelyből a maximális datagramhossz $8 \cdot 8192 = 65\,536$ bájt.
- Az **ÉLETTARTAM** mező lényegében egy 8 bites számláló, amely a csomagok élettartamát tartalmazza másodpercben. Amikor értéke nullává válik, akkor az adott csomag megsemmisül. Így a maximális élettartam 255 s lehet.
- Amikor a hálózati réteg összerak egy teljes datagramot, tudnia kell, hogy mit tegyen vele. A **PROTOKOLL** mező kijelöli, hogy a datagram a különféle szállítási folyamatok közül melyikhez tartozik. A TCP a leggyakoribb választás, de léteznek egyéb is.

26

IP fejrész

- A **FEJRÉSZ ELLENŐRZŐ ÖSSZEGE** csak a fejrész ellenőrzésére szolgál. Egy ilyen ellenőrzőösszeg azért hasznos, mert a fejrész a darabolások miatt változhat az átjárókban.
- A **FORRÁSCÍM** és a **CÉLCÍM** hálózati számot és a hoszszámot adják meg.
- Az **OPCIÓK** mező rugalmasan alkalmazható biztonsági, forrás általi forgalomirányítási, hibajelentési, hibakeresési, időpont-megjelölési és egyéb információs célokra. A mező biztosításával elkerülhető, hogy a fejrészben levő biteket és mezőket ritkán használt információk számára kelljen lefoglalni.

27

IPv4 - Problémák

- Az IP címzési rendszere 32 bites: ez az IPv4;
- Sokkal több IP címre lenne szükség, mint amennyi ennek alapján kiosztható lenne;
- Elvileg csaknem 4 milliárd gép címezhető, a valóságban (pl. a címtartományokra bontás miatt) ennél jóval kevesebb!

28

IPv4 - Problémák

- Az osztályozás azon a feltételezésen alapul, hogy az Internet:
 - nagyon sok kisméretű intézmény (kevesebb mint 250 gép, C osztályú cím),
 - kevés közepes méretű (kevesebb mint ~64000 számítógép, B osztályú cím),
 - és még kevesebb nagyon nagy méretű cég (~15 millió számítógép, A osztályú cím) összekapcsolásából épül fel.

29

IPv4 - Problémák

- Az IPv4 támogatja a fragmentálást, de ez roppant erőforrás-igényes!
- A csomag-darabok kezelése a streaming-adatátvitelt brutálisan lassítja.
- Nem támogatja a hierarchikus útválasztást.
- Semmilyen titkosítást nem támogat!

30

Alapok, TCP/IP, IPv6, Routing

IPv6 - Jellemzés

- 1995 december: RFC1883 az IPv6 születése.
- Az IPv6 az IPv4 (szerves?) folytatása.
- A szállítási és az alkalmazási rétegek protokolljai nem változnak!
- Strukturális változás, hogy nincs külön címfeloldásra protokoll (ARP), hanem ezt maga az IP tartalmazza *Neighbour Discovery* (ND, szomszédkeresés) néven.

31

IPv6 - Jellemzés

- Új fejlécformátum
- Nagy címtér:
 - forrás- és célcímei 128 bitesek
 - Jelenleg a kiosztható címeknek csak kis hányada foglalt
 - szükségtelenné az olyan címmegőrzési technika, mint a hálózati címfordítás (NAT).

32

IPv6 - Jellemzés

- Hierarchikusan felépülő címzési és útválasztási infrastruktúra
- Automatikus címkonfiguráció:
 - Állapotmentes
 - A címek konfigurálása a beérkező útválasztóhirdetmény-üzenetek alapján történik

33

IPv6 - Jellemzés

- Állapotnyilvántartó
- A konfigurálás a címek és egyéb konfigurációs beállítások felvételét lehetővé tevő állapotnyilvántartó konfigurációs protokoll
 - ilyen például a DHCPv6 – használatán alapul.
- Kettős

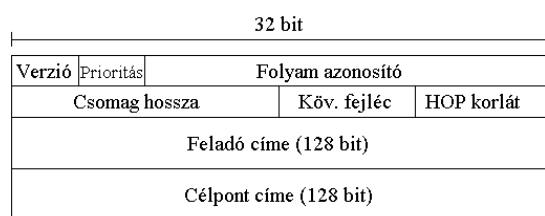
34

IPv6 - Jellemzés

- Beépített biztonsági szolgáltatások
 - Bizalmas adatok továbbítása
 - Hitelesítés
 - Az adatok sértetlensége
- A szolgáltatás minőségének (QoS) szélesebb körű támogatása
- Új protokoll a szomszédos csomópontokkal való kapcsolatokhoz
- Bővíthetőség

35

IPv6 - fejléc



36

Alapok, TCP/IP, IPv6, Routing

IPv6 - fejléc

- Verziószám: 4 bit
- Forgalom osztálya (*Traffic class*): 8 bit
 - 0-7 prioritások olyan forgalomfajtákat jelölnek, melyek késleltetést szenvedhetnek, ha torlódás van (pl.: FTP, E-Mail);
 - 8-15 pedig olyanokat, melyek nem (pl.: interaktív, real-time forgalom)

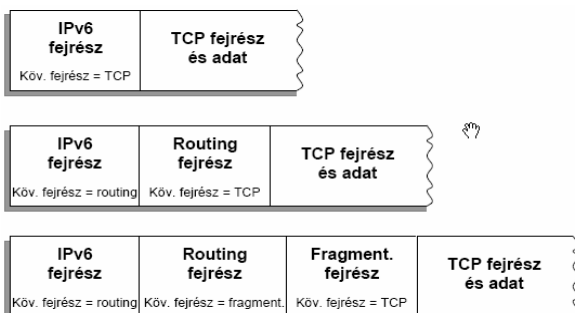
37

IPv6 - fejléc

- Folyam azonosító (*Flow label*): 24 bit
 - az ugyanattól a feladótól ugyanaddig a feladóig futó logikailag egybetartozó csomagok megjelölése.
 - Ha sehova sem tartozik, 0!
- Csomag hossza (*Payload length*): 16 bit
- Következő fejléc (*Next header*): 8 bit
 - IPv4-ben opció!

38

Következő fejléc (*Next header*):



39

IPv6 - fejléc

- HOP korlát (*Hop limit*): 8 bit
 - Korábban TTL mező
 - Most nem élettartam másodpercben hanem HOP száma: ha az itt megadott ugrásszámot meghaladja, akkor el kell dobni a csomagot!
- Forrás címe (*Source Address*): 128 bit
- Cél címe (*Destination Address*): 128 bit

40

IPv6 - Címzés

- IPv4: 32 bit, 4 bájtos ábrázolás; pl.: c3:c7:d7:c2
- IPv6: 128 bites cím:
 - 8 darab
 - 16 bites csoport
 - hexadecimális formában

41

Az IPv6-címek írásmódja

- Az alábbiakban egy IPv6-cím bináris formája látható:
0010000111011010000000001101001100000000000000000101111
00111011000000101010101000000001111111111111111000101000
1001110001011010
- A 128 bites cím 16 bites egységekre tagolódik, a következőképpen:
0010000111011010 0000000011010011
0000000000000000 0010111100111011
0000001010101010 0000000011111111
1111111000101000 1001110001011010

42

Alapok, TCP/IP, IPv6, Routing

Az IPv6-címek írásmódja

- Minden 16 bites egység átalakul hexadecimálissá, kettőspontokkal elválasztva. Az eredmény a következő:
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
- Az IPv6 címmegjelenítése tovább egyszerűsíthető a 16 bites egységek kezdő nulláinak eltávolításával. A kezdő nulla letiltása után a cím a következőképpen néz ki:
21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

43

IPv6 - Címzés

- IPv6 pl.: FF7B:0:0:0:0:2C98:FFE8:0021
- Egyszerűsítés, hogy a nullák ::-tal helyettesíthetők, azaz:
FF7B::2C98:FFE8:0021
- A nullatömörítés egy címben csak egyszer alkalmazható. Máskülönből nem lehetne meghatározni a dupla kettőspont (::) egy-egy példányát által jelölt 0 bitek számát.

44

IPv6 - Címzés

- Az IPv6 cím lehet
 - unicast: egy állomás egy interface-ét jelöli;
 - multicast: több interface, a csomag minden címre megérkezik;
 - anycast: több interface, a csomag csak egy állomásra érkezik meg

45

Routing

- Routing fogalma: az a folyamat, ami során egy hálózati protokoll (3. réteg) egy csomagja a kapcsológépek (router-ek) sorozatán keresztül a feladótól eljut a címzettig. Ehhez szükséges, hogy a router-ek kommunikáljanak egymással, hogy eldönthessék, hogy egy adott végcél felé melyik irányba kell továbbítani a csomagot.
- A hálózati protokollt hívjuk **route-olt** protokollnak (IP, IPX, AppleTalk, stb.), a router-ek egymás közötti kommunikációját bonyolító protokollt pedig **routing** protokollnak.
- A routing protokoll a kommunikáció módjainak lerögzítése mellett meghatározza az útvonal kiválasztás mikéntjét is. Maga az útvonal kiválasztás a routing problémakörének legérdekesebb kérdése.

46

Routing

- **statikus**: Nincs routing protokoll, előre definiált fix táblázat alapján történik a csomagkapcsolás. (Az ilyen eljárásokról nincs mit beszélni, kézzel beírjuk, mi merre menjen és vége a problémának.)
- **dinamikus**: A router-ek egymás között kommunikálva a hálózat topológiájának megfelelően állítják elő a táblázatot. Jelen fejezetben erről a kategóriáról beszélünk.

47

Routing

- **egyutas** (*single path*): Minden célpont felé csak egy út tárolódik a router-ekben.
- **többutas** (*multipath*): Minden célpont felé több (esetleg minden) utat tárol. Csak ezek a protokollok lehetnek képesek load balancing-ra.

48

Alapok, TCP/IP, IPv6, Routing

Routing

- **lapos (flat):** Minden router minden célpontról tud.
- **hierarchikus:** A router-ek nem minden célpont felé ismerik az utat. Egy ismeretlen címzettű csomagot egy fixen, előre meghatározott router felé (default router) küldenek, aki a routing információk egy szélesebb körével rendelkezik.

49

Routing

- **Hop-by-Hop:** Itt minden router afelől dönt, hogy ő merre adja tovább a csomagot és autonóm módon határozza meg a továbbítás irányát. Ezen az elven működik a legtöbb hálózati protokoll (IP, IPX) route-olása is. Az ilyen elven működő router-ek csak olyan utakat hirdethetnek, melyeket maguk is használnak, hiszen ha az A router az általa hirdetett úttól vagy költségtől elérő irányba vagy költséggel továbbítja a csomagot, akkor lehet, hogy egy másik router, ha ezt tudná, inkább nem A felé továbbítaná a csomagot, hanem más irányba. A router-ek tehát hirdetményeikben azt állítják, hogy „én erre, ekkora költséggel fogom továbbítani a csomagot. Ha ez neked jó, akkor nekem küldd, ha nem jó, ne nekem küldd.”
- **Source routing:** Ez esetben viszont a feladó határozza meg az útvonalat, a router-ek csupán az elérhetőségi információkat terjesztik és magukat a csomagokat kapcsolják a csomagba beleirt útvonal szerint. Ezen az elven működik az ATM eddig ismert egyetlen útkereső protokollja.
- A két megoldás között léteznek átmenetek, mikor a feladó hatással van ugyan a csomag útjára, de nem teljesen határozza meg azt.

50

Routing

- **Intradomain:** Az IGP általános megfogalmazása; valamely területen (domain) belüli route-olásért felelős.
- **Interdomain:** A fenti ellentéte, a területek közötti útvonalválasztásért felel.

51

Routing

- **link-state:** Az ilyen protokollok először feltérképezik a hálózat topológiáját és utána ebben a gráfban keresik a legrövidebb utat. A router-ek egymás között csak saját interface-eik állapotát beszélnek meg, de ezeket az információkat minden a hálózatban levő router-rel kicserélik, ebből építeti fel aztán ki-ki a saját (de egymással megegyező) topológiai gráfját. Így tehát sok, mindenhova elküldött, apró üzenetből áll a kommunikáció.
- **distance-vector:** Ezek a protokollok csak a szomszédos router-ek között kommunikálnak. Minden router elmondja összes szomszédjának, hogy ő mekkora költségű utat ismer egy adott célponthoz. Arról, hogy ez az út merre vezet, nem szól. A router-ek begyűjtik a szomszédjaiktól ezeket a hirdetéseket és kiválasztják, ki hirdette a legolcsóbb utat és a felé a router felé továbbítják a csomagot, valamint saját költségüket hozzáadva ők is hirdetni fogják az adott célponthoz vezető utat. Itt tehát kevés, csak a szomszédoknak elküldött, de nagyméretű üzenetből áll a kommunikáció.

52

Routing protokollok: RIP

- **RIP: Routing Information Protokoll:**
 - A RIP a XEROX PARC által kifejlesztett GWINFO nevű protokollból származik, melyet az XNS-be RIP néven integráltak. Az Internethez 1982-ben kapcsolódik, amikor a BSD UNIX egy „routed” elnevezésű RIP implementációval került forgalomba, mely segítségével a munkaállomások route-olhattak.
- TCP/IP routing protokoll
- 1988-ban RFC1058, v1 majd 1993-ban az RFC1387-88, v2
- Egyszerű, ezért népszerű protokoll

53

Routing protokollok: RIP

- Egy lapos, egyutas, distance-vector protokoll
- A RIP-et futtató router-ben konfigurálni kell

54

Alapok, TCP/IP, IPv6, Routing

Routing protokollok: RIP

- A RIP egy célponthoz táblázatában a következő információkat tárolja:
 - A célpont IP címét (0.0.0.0 a default route címe)
 - Az odavezető út költsége, a 16-os költség a „végtelent”, az elérhetetlen célpontot jelöli.
 - Az odavezető út első router-e
 - Időzítők

55

Routing protokollok: OSPF

- OSPF: *Open Shortest Path First*
- 1991 július: RFC1247
- TCP/IP routing protokoll

56

Routing protokollok: OSPF

- Előnyök:
 - topológiai változás esetén a konvergencia gyors;
 - a költségek kezelése egyszerűbb;
 - több út kiszámítható

57

Routing protokollok: OSPF

- Alprotokollok:
 - Hello protokoll, ami segítségével a router-ek a link-ek állapotát tesztelik, felderítik egymást és meghatározzák a kiválasztott router-t.
 - Az Exchange protokoll, ami segítségével topológiai adatbázisok szinkronizációja folyik.
 - A Flooding protokoll, ami a link-state rekordok terjesztéséért felelős.

58

Routing protokollok: IGMP

- IGMP: *Internet Group Management/Membership Protocol*
- TCP/IP routing protokoll
- Multicast routing
 - árasztás
 - feszítőfa

59

Routolható, nem routolható protokollok

- Routolható:
 - IP (Internet Protocol);
 - IPX (Internet Packet eXchange); és
 - XNS (Xerox Network Systems)
- Nem routolható:
 - NetBIOS

60

Alapok, TCP/IP, IPv6, Routing

NAT, PNAT

- Proxy
- MASQ
- NAT

61

DNS

- DNS: Domain Name System – Tartománynév kezelő rendszer
- A DNS létrehozásának oka
- A DNS Architektúrája
- A DNS tartomány-hierarchiája
- A DNS szolgáltatásai

62

ICMP

- Az Internet működését az IMP-k és az átjárók felügyelik;
- Az eseményt az ICMP alapján jelentik.
- Kb. egy tucat ICMP üzenettípus van.
- Minden üzenettípus IP-csomagban utazik.
- A protokoll az Internet tesztelésére is használható.

63

ICMP

- DESTINATION UNREACHABLE
- TIME EXCEEDED
- PARAMETER PROBLEM
- SOURCE QUENCH
- REDIRECT
- ECHO REQUEST, ECHO REPLY
- TIMESTAMP REQUEST, TIMESTAMP REQUEST

64

ARP, RARP

- ARP: *Address Resolution Protocol*
- Az ARP kéréseket: üzenetszórás ...
- RARP: *Reverse Address Resolution Protocol*

65

Források: IPv6

- IPv6 Information Page:
<http://www.ipv6.org/>
- IPv6 from Wikipedia:
<http://en.wikipedia.org/wiki/IPv6>
- Az IPv6:
<http://www.szabilinux.hu/trendek/trendek73.html>
- IPv6
<http://www.iif.hu/rendezvenyek/networkshop/97/tartalom/NWS/1/15/index.htm>

66