Kaj je omrežje? Kaj je komunikacija?

- Fizično (infrastruktura, ki povezuje,...)
- Logično (omogoča storitve,...)

Naprave v omrežju: končni sistemi:

- So izvor ali ponor podatkov
- Poganjajo aplikacije (strežniki, računalniki, prenosniki, tablice, telefoni, senzorji,...)
- Vloga: odjemalec, strežnik ali oboje (P2P)

Rob omrežja. Dostopovno omrežje:

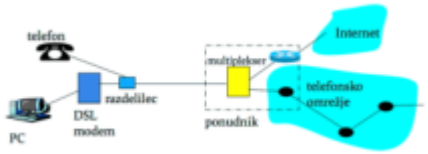
- Končni sistemi morajo dostopati do omrežja: klicni dostop (modem), DSL, kabelski dostop, optika (FTTH), Ethernet (Baker), brezžični dostop

Naprave v omrežju: jedro ali hrbtenica

- Posredujejo promet: usmerjevalniki
- Komunikacijske povezave: bakrene žice, optične povezave, brezžične tehnologije

Dostop do omrežja:

1. Preko telefonske infrastrukture:
    a. Modemski (klicni) dostop: analogne telefonske linije, nizke hitrosti, tipično 56 kb/s, telefon je med uporabo zaseden. Zgodovina.
    b. DSL (Digital subscriber line): lahko uporablja obstoječo telefonsko infrastrukturo, tipično do nekaj 100 Mb/s v vsako smer.



2. Kabelski dostop:
    a. Ne uporablja telefonske infrastrukture, ampak omrežje za kabelsko TV. Več odjemalcev si deli isto povezavo. Tipična hitrost 10/100 Mb/s
3. Računalniško omrežje
    a. FTTH (Fiber to the home): optika in visoke hitrosti, npr. 100/100 Mb/s
    b. Bakrene žice in Ethernet
        i. Tipično za javne ustanove, univerze, institute
        ii. Standardne hitrosti (1, 10, 100 Mb/s), 1, 10, 100 Gb/s
        iii. Priklop preko stikala in robnega usmerjevalnika (prehod)
4. Brezžično
    a. WiFi (IEEE 802.11, več različic: b/g/an/ax,...): različne hitrosti
        i. Skupinski prenosni medij (deljen)
        ii. Neusmerjen prenos (fizična varnost)
    b. Mobilno telefonsko omrežje 3G/4G/5G,...:
        i. Uporaba central mobilnih operaterjev
        ii. Hitrosti so različne, mnogo različic

Protokol

- Omrežje je več kot le povezave
- Protokol:
  - Zbirka pravil za komunikacijo
  - katera sporočila so veljavna, kdaj jih lahko oddam, kaj naredim ko sprejmem določeno sporočilo?

Kdo s kom komunicira?

- Horizontalna (logična komunikacija) – vsaka plast ima svoje protokole:
  - Uporabnik (človek s človekom)
  - Aplikacija z aplikacijo (brskalnik s spletnim strežnikom)
  - Proces s procesom
  - Naprava z napravo
  - ...
- Vertikalna (fizična) komunikacija – nižja plast nudi storitve višji plasti: uporabnik z aplikacijo, aplikacija s procesom, proces z napravo, naprava z adapterjem,...

Kaj sploh je plast?

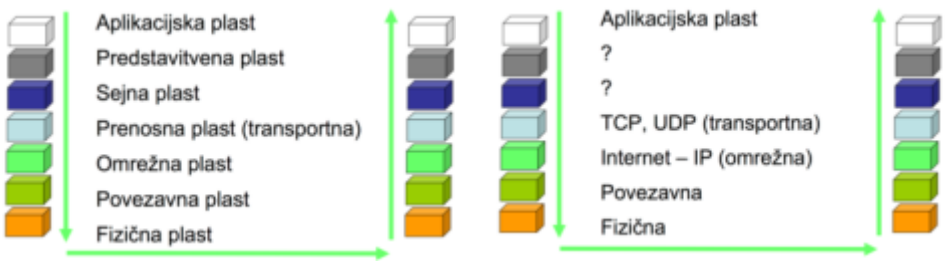
- Strukturiranje sorodnih problemov!
- Zajema skupino storitev, ki potrebujejo specifično obravnavo
- Natančno opredeljena funkcionalnost
- Minimalen pretok podatkov med plastmi
- Ustrezno število plasti
- Kompatibilno s standardizacijo

Delovanje plasti

- Plast N nudi storitve plasti N+1
- Plast N zahteva storitve od plasti N-1
- Vmesnik: storitvena pristopna točka. Pomembna dobra opredelitev!
- Komunikacijski protokol: pravila komunikacije med istoležnima procesoma
- N-protokol: izvedba storitev plasti N (logična komunikacija!) – je transparenten (neviden) za višje plast

Arhitektura in struktura omrežja

- Arhitektura opredeljuje: plasti (njihovo funkcijo in hierarhijo) ter logične povezave
- Struktura opredeljuje: topologija sistema, izvedba vertikalnih povezav, fizične zmogljivosti sistema



Povezavna in fizična plast

- Fizična plast: Fizikalne lastnosti prenosnih medijev
- Povezavna plast: Zaznavanje in popravljanje napak, Multiple access: dostop do skupnega medija, naslavljanje, zanesljiv prenos in kontrola pretoka

Fizična plast:

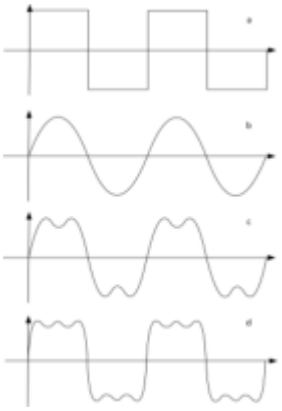
- Prenosni mediji: naprava, ki omogoča razširjanje valovanja (el-mag, radijsko, svetloba – laser, IR)
- Fizični vmesniki: konektorji
- NALOGE:
    - Kodiranje bitov z neko fizikalno veličino (U, I…)
    - Pretvorba el. signalov v obliko za prenos po mediju (radijski, IR, optika…)
    - Prenos signala – toka bitov, kodiranih v analogni ali digitalni obliki po prenosnem mediju

Analogno-digitalno

- Podatki: digitalni ali analogni?
- Prenosni kanal: kodiranje:
    - Digitalni: z diskretnimi vrednostmi (npr. dva napetostna nivoja)
    - Analogni: z analognimi signali (zvezno spreminjanje vrednosti)
- Naprave: digitalne ali analogne
- Omrežja: digitalna ali analogna

Prenosni medij:

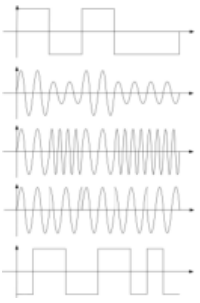
- Frekvenčna karakteristika: kakšne frekvence lahko medij prenese (govor: 300 do 7000 Hz, telefonski kanal: 500 do 3600 Hz, HiFi oprema: 100 do 20.000 Hz)
- Prenos signala: Fourierova analiza (splošen signal = vsota osnovnega signala in višjih harmonskih komponent)
- Čimveč višjih komponent se lahko prenese, tem bolj lepo pravokoten bo signal (vsota)
- Slabljenje, popačenje, šum



Prenos digitalnih podatkov po analognem kanalu:

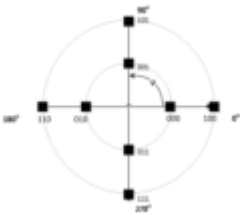
- Uporabniški vmesnik: tel. Vtičnica
- Modem: pretvorba D ↔ A oblika
- Modulacija: način prikaza razlike med ničlo in enico

Modulacija



- Amplitudna modulacija: glasen pisk je 0, tih pisk je 1
- Frekvenčna modulacija: visok pisk je 0, nizek pisk je 1
- Fazna: sprememba faze za določen fazni kot pomeni spremembo signala

Kvadratna modulacija



- Kombinacija amplitudne in fazne modulacije
- Več nivojev amplitude
- 4 fazni koti (0, 90, 180, 270 stopinj)
- Posamezna sprememba signala (amplitude in faze označuje skupino 3 do 6 bitov

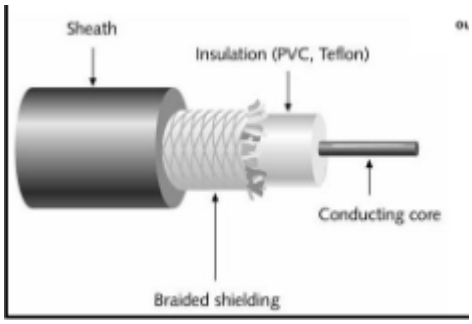
Prenos analognih podatkov po digitalnem kanalu

- Analogni signal vzorčimo z 2x max. frekvenco (Nyquist),beležimo amplitudo vzorcev
- 8000 vzorcev/s
- PCM – pulzno kodna modulacija: 8 bitov za opis amplitude (to pomeni 64 kbps)
- Delta modulacija: za opis vzorca pošiljamo le razliko od prejšnje amplitude.

Prenosni mediji

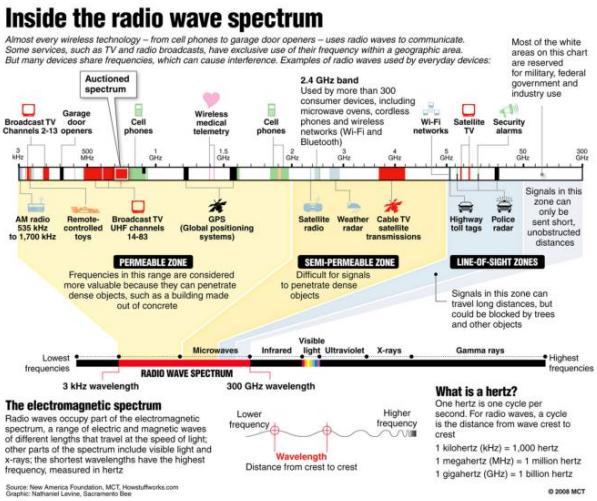
Industry acronyms	ISO/IEC 11801 name	Cable screening	Pair shielding
UTP	U/UTP	none	none
STP, ScTP, PiMF	U/FTP	none	foil
FTP, STP, ScTP	F/UTP	foil	none
STP, ScTP	S/UTP	braiding	none
S-FTP, SFTP, STP	SF/UTP	braiding, foil	none
FFTP	F/FTP	foil	foil
SSTP, SFTP, STP PiMF	S/FTP	braiding	foil

- Fizični prenos pomnilnih medijev
  - Kanal 512 kb/s, 10min hoje, 2GB baza
  - Omrežje: 8ur, peš: 10min
- Parica in zvita parica (UTP)
  - Dve vzporedni izolirani bakreni žici
  - Zvita: manj interferenc, presluha ipd
  - 10 Gb/s na krajše razdalje (lokalna omrežja)
  - Komutirane (običajne telefonske) in najete linije (rezrevirane za IK opremo)
- Koaksialni kabel – do 2 Gbps



  - Bakrena žica, izolacija, oklop – drug vodnik, še ena izolacija
  - Odpornost proti motnjam, ni sevanja
- Optično vlakno – Tera bps
  - Do 100 km brez ponavljalnikov
  - Mehanska občutljivost, zahtevno spajanje
  - WDM (Wavelength Division Multiplexing): za prenos več signalov po enem vlaknu uporabimo več valovnih dolžin (barv) svetlobe – to je v bistvu isto kot FDM!
  - Veliko dobrih lastnosti
  - V začetku le omrežne hrbtenice, danes tudi “last mile” povezave (FTTH)

- Brezžične povezave
    - Radijske (WLAN, Bluetooth, GSM,...)
    - Mikrovalovne (usmerjene)
    - IR (majhne razdalje)
    - Satelitske (velike razdalje): Iridium, GPS, Galileo



Varnost na fizični plasti:

- Poskrbeti je potrebno za fizično zaščito naprav in povezav
    - Pred priskuškovanjem (odliv podatkov)
    - Pred poškodovanjem (onemogočanje dostopa)
- Različne lastnosti različnih prenosnih medijev
    - Glede območja širjenja signala
    - Glede možnosti prisluškovanja

Prenosni sistem

- Povezavna plast + fizična plast na OSI modelu
- Prenosni kanal: naprava, ki lahko prenese paket (okvir) po mediju
- Analogija iz resničnega življenja »pod od Vrhnike do Ormoža«

Tipi prenosnih sistemov

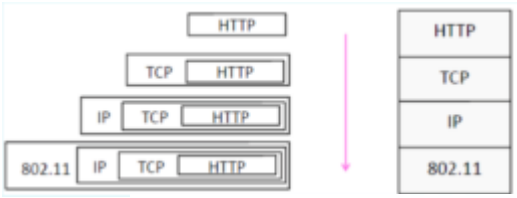
- Prenosni kanal: smer
    - Dvosmeren (sočasno ali izmenično)
    - Enosmeren
- Prenosni kanal: zaporednost
    - Serijski (bit za bitom)
    - Paralelni (več bitov hkrati) – težava s sinhronizacijo
- Prenosni kanal: število točk
    - Dvotočkovni
    - Skupinski

Povezavna plast

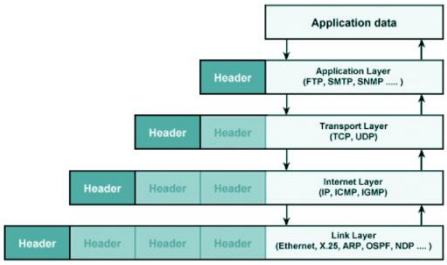
- Vozlišče: računalnik, usmerjevalnik
- Povezava (ang. link) povezuje dve sosednji vozlišči
- Enota povezavne plasti je OKVIR; ta enkapsulira datagram
- Naloge: povezavna plast LAHKO nudi naslednje storitve:
    - Enkapsulacija in dekapsulacija datagrama
    - Prenos okvirja po povezavi med sosednjima vozliščema
    - Ureja dostop do deljenega (“skupinskega”) medija

- Ureja pretok (hitrost pošiljanja), zaznava in popravlja napake, ureja smernost

Kaj je enkapsulacija



- Dodajanje dodatnih podatkov, potrebnih za prenos preko omrežja
- Za vsako plast in protokol so dodani podatki specifični



Komunikacija med adapterji

- Povezavna plast se nahaja v adapterju (NIC)
- Oddajnik: enkapsulacija datagrama v okvir, detekcija, kontrola pretoka
- Sprejemnik: preveri napake, pretok, dekapsulacija

Zaznavanje in odpravljanje napak:

- Dodamo kontrolne bite, ki pomagajo zaznavati in/ali odpravljati napake
- Kontrola parnosti: doda se 1 bit
  - Liha paritetna shema – dodatni bit ima vrednost (0 če je v podatkih liho št. Enic, 1 sicer če je sodo)
  - Samo zaznavanje enojnih oziroma lihih napak!
- Parnost v 2 dimenzijah (vrstica + stolpec): zaznavanje in odpravljanje enojnih napak.
- Kontrolne vsote, npr. Internet checksum (uporaba na omrežni, transportni plast: telo datagrama je zaporedje 16-bitnih števil. Njihova vsota (eniški komplement) gre v glavo datagrama)
- Hammingov kod: med podatkovne bite vrinemo ustrezno število kontrolnih in jim določimo vrednosti 0 ali 1 tako, da je v določenih zaporedjih bitov vedno predvidljivo št. enic.
- CRC: n-bitov za rezultat – detekcija napak do n bitov (in nekaterih večjih). Zahtevnejše operacije (polinomske)

Protokoli za dostop do deljenega (skupinskega medija)

- Multiple Access. Kateri medij je deljen? Kolizija.
- Isti kanal se uporablja tudi za koordinacijo!
- Idealni protokol: eno vozlišče oddaja: hitrost H, M vozlišč oddaja: vsaka s hitrostjo H/M
- Možne rešitve za uporabo skupinskega medija: razdeliti kanal (ni kolizij), naključni dostop (dovoljene kolizije), določeno zaporedje dostopov (ni kolizij)

Načini za delitev kanala

- TDMA: Time Division Multiple Access

    - V vsakem “krogu” vsaka postaja dobi enak časovni interval (1 paket), neizkoriščeni intervali
- FDMA: Frequency Division Multiple Access
    - Vsaka postaja ima svoj fiksen frekvenčni pas
    - Neizkoriščen pas, kadar ni zahtev za prenos
- Pošteno in učinkovito pri visoki obremenitvi, pri nizki neizkoriščenost kanala.
- CDMA (Code Division), WDM (Wavelength Division - optika)

Kolizijski protokoli – naključni dostop: PRAVILA

- Določajo kako zaznati kolizijo in kako ukrepati ob koliziji
- Uporaba bontona: Vsak lahko dobi priložnost za govorjenje, Ne odgovori če nisi vprašan, Ni monopolov (ne izvajaj monologov), Dvigni roko če imaš vprašanje, Ne prekinjaj tistega ki govori, Poslušaj če nekdo govori s tabo

Kolizijski protokoli (naključni dostop) Primeri protokolov:

- ALOHA: paket je ranljiv ves čas oddajanja, preprost, nizka prepustnost (18%), kolizija (počaka naključen čas, nato spet odda)
- Razsekana ALOHA: čas je razsekan na delčke, sinhronizacija, boljša prepustnost (37%), paket je ranljiv le v začetku oddajanja, kolizija: z verjetnostjo p odda v naslednjem intervalu.

Kolizijski protokoli (ostali) Primeri protokolov:

- CSMA: Carrier Sense Multiple Access (ni takta)
    - Pred oddajo posluša, če kdo drug oddaja
    - Vztrajni: če je kanal zaseden, posluša dokler se ne sprosti
    - Nevztrajni: šele po č.k. ponovno prisluhne
    - P-vztrajni: vztrajno posluša, ko se kanal sprosti, z verjetnostjo p odda paket, z (1-p) počaka še določen čas.
- CSMA/CD: vztrajni CSMA z zaznavanjem trkov
    - Takoj ko zazna trk, ustavi oddajanje
    - IEEE 802.3 Ethernet
- Učinkoviti pri nizki obremenitvi; pri visoki je preveč režije (kolizij)

Nekolizijski protokoli - protokoli za izmenični dostop

- Namesto faze boja za medij je faza rezervacije (v tej fazi se vzpostavi vrstni red dostopa)
- Poizvedovanje (polling) – centralno vozlišče (master) sprašuje, kdo želi oddajati
- Podajanje žetona (token passing)
    - Rezervacijski paket obišče vse postaje, te vanj zapišejo svoj ID (prijava za oddajo)
    - Nato postaje oddajajo po vrstnem redu.
    - Protokoli: vodilo in obroč z žetonom
    - FDDI, Token Ring 802.5, RPR 802.17

MAC naslov:

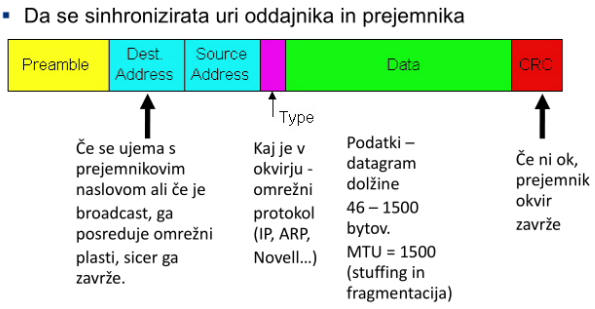
- 48 bitov oz. 12 hex znakov, npr: 00-21-85-80-1A-B7
- Leva polovica: proizvajalec, desna: ID adapterja
- Veliko standardov
- Posebni naslovi
    - Broadcast FF:FF:FF:FF:FF:FF
    - Multicast – poseben naslov, ki ga sprejemajo le določene naprave (prijavljene v multicast skupino) – predpona 01:00:5e

Ethernet:

- Topologija: vodilo (včasih), zvezda (danes).
- Hub – razdelilnik signala (na fizični plasti)
- Stikalo: preklaplja okvirje na podlagi MAC naslova (na pov. plasti)
- [Usmerjevalnik: na podlagi IP naslova – na omrežni plasti]
- 10BaseT (10 Mb/s), 100 BaseT – fast Ethernet (baker, optika), 1000 base-T 1 Gb/s, 10 Gb/s
- Fizična plast: Manchester encoding za 10 Mb/s (vsak bit vsebuje prehod), 4b/5b za 100 Mb/s, PAM-5 in TCM za Gb/s …

Ethernet okvir:

- Ethernet IEEE 802.3 (lila – polje length) in Ethernet II (lila – polje Ethertype): če je vrednost > 1536, gre za Ethernet II, če manjša od 1500, gre za 802.3
- Preambula: 7 x 10101010 in 1 x 10101011
    - Da se sinhronizirata uri oddajnika in prejemnika



Storitev, ki jo nudi Ethernet

- Nepovezavna – ni rokovanja
- Nezanesljiva – ni potrjevanja:
    - Ali omrežna plast dobi vse datagrame?
    - Ali jih dobi v pravem zaporedju?
    - Ali je kaj razlike, če se uporablja TCP ali UDP?
    - Ali aplikacija “vidi” manjkajoče podatke?
- CSMA/CD: zvezen čas, posluša pred oddajo, v primeru kolizije preneha, pred ponovno oddajo čaka naključen čas: Exponential backoff: če je več zaporednih kolizij, vsakič dlje čaka

Hub – razdelilnik

- Deluje na prvi plasti
- Možna večja razdalja med vozlišči, če je vmes hub (deluje kot ojačevalec signala)

- Ne ločuje kolizijskih domen – vsi segmenti so ena, razdelilnik le ponavlja signal
- Ne more povezovati segmentov različnih hitrosti

	Hub	Stikalo	Usmerjevalnik
Izolacija prometa	Ne	Da	Da
Potrebna konfiguracija?	Ne	Ne	Da
Optimalno usmerjanje	Ne	Ne	Da
Možno oddajanje, ko se PPE še sprejema	Da	Da	Ne

Stikalo

- Deluje na povezavni plasti - posreduje okvirje
- Transparentno delovanje (računalniki ga ne vidijo)
- Plug and play - sam se uči:
    - CAM tabela (MAC naslov, vmesnik, čas) , ttl ~ 60 min
    - Ko pride okvir, si stikalo zapomni naslov izvora in ga zapiše v tabelo
    - Če ima ciljni naslov v tabeli – okvir na ta vmesnik
    - Sicer poplavi na vse razen izvorni vmesnik
- Ločuje kolizijske domene (vsak segment je svoja)
- Omrežje brez kolizij – vsak računalnik ima svojo full duplex povezavo do stikala.

VLAN – navidezno krajevno omrežje

- Vmesnike na stikalu grupiramo. Vsaka skupina je videti, kot da bi bila v svojem omrežju (npr. broadcast promet ne gre v druge skupine). Za to skrbi stikalo.
- Med VLANi je treba promet usmerjati (stikalo 3. plasti zna)
- Članstvo v skupini je dinamično, lahko na osnovi MAC naslova
- VLAN prek več fizičnih stikal:
    - vmesnik za povezavo stikal (trunk port)
    - Okvir dobi VLAN ID (802.1q) – vrine se za MAC naslove

PPP

- En pošiljatelj, en prejemnik, MAC naslovi nepotrebni
- WAN - klicna povezava, SONET/SDH, ISDN
- Naloge: Okvirjanje in detekcija napak, Preverjanje povezave in pogajanje o omrežnih naslovih, Potrebno je vzpostavljanje povezave!
- Ni korekcije napak, ponovnega pošiljanja, sortiranja, kontrole pretoka
- Byte stuffing: 01111110 označuje začetek in konec okvirja. Če je isti niz v podatkih, vrinemo še enega 01111101. Če prejemnik zazna ta dva zapored, drugega zavrže.

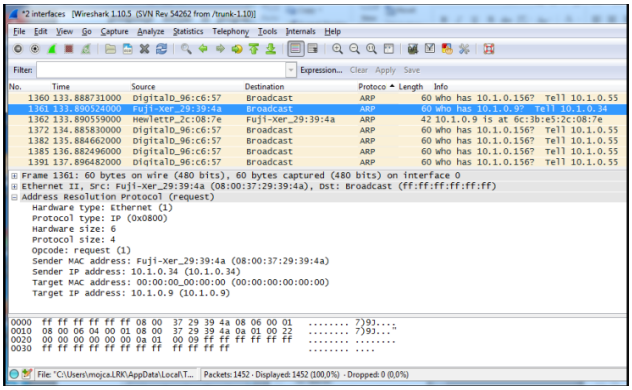
Naslavljanje na 2. in 3. plasti

- MAC naslovi (LAN naslov, fizični naslov)
    - Prenosljivi, nehierarhični, nespremenljivi
    - MAC naslov izvora in ponora sta v glavi okvirja
    - MAC naslov (v glavi okvirja) lahko ponaredimo!
- ARP – Address Resolution Protocol
    - Preslikava IP – MAC naslov (omrežne v povezavne)

    - Vsako vozlišče ima ARP tabelo (IP – MAC – TTL)
- RARP – v obratni smeri (zastarel, nadomestil ga je BOOTP, DHCP)

ARP protokol (Ni potreben administrator)

- Vozlišče A: Kako poslati datagram na IP naslov B?
- A: ARP query na FF-FF-FF-FF-FF-FF: “Kdo ima B”?
- Vsi sprejmejo ARP query
- B: Pošlje svoj MAC naslov A-ju
- A: doda zapis v ARP tabelo



Če je iskani naslov zunaj omrežja:

- Omrežna plast ugotovi, da je ciljni naslov zunaj omrežja.
- Naredi ARP poizvedbo po IP naslovu privzetega prehoda (tega ima v nastavitvah) -> odgovori usmerjevalnik R – prehod v B-jevo omrežje, s svojim MAC naslovom.
- Ko R prejme okvir od A, pogleda ciljni IP naslov.
- R naredi ARP poizvedbo v omrežje B.
- R pošlje okvir na novi ciljni MAC naslov.

ARP spoofing (ARP poisoning)

- Okvir z lažnim izvornim MAC naslovom – “naj mislijo, da sem jaz npr. prehod”
- Posledica v zastrupljeni ARP tabeli: -> Napadalčev MAC naslov – legalen IP naslov
- Napadalec -> Pasiven: posluša in posreduje promet naprej ALI Aktiven: spreminja in posreduje promet naprej (napad man-in-the-middle) ALI DOS napad: napadalec poveže IP naslov prehoda žrtve z neveljavnim MAC naslovom.
- Preprečevanje
    - Fiksni zapisi v ARP tabelah (ročni vnosi)
    - DHCP snooping: pozna MAC naslove na linkih in preverja vsak ARP paket, če ustreza (Cisco)
    - ArpWatch: program, ki opozarja na spremembe ARP tabel (npr. Mail administratorju)
- Legalna uporaba: npr. redundančna infrastruktura (rezervni strežnik, če glavni odpove)

DHCP stradanje

- Napadalec: broadcast veliko zahtev za DHCP naslov iz lažnih MAC naslovov.
- DHCP strežnik: zmanjka naslovov
    - DOS napad (uporabnik ne dobi naslova)
    - Napadalec lahko zdaj postavi lažni DHCP strežnik
- Preprečevanje:
    - DHCP avtentikacija (RFC 3118)
    - Omejevanje števila različnih MAC naslovov na posam. vmesniku stikala ali usmerjevalnika

Še več napadov

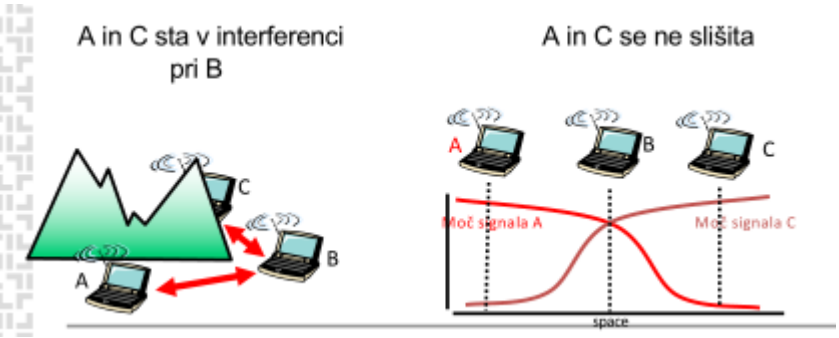
- ARP request replay: napad na WEP z namenom povzročiti več prometa (napadalec lovi inicializacijske vektorje
- ARP storm (DoS): Ponarejeni ARP broadcasti, tako da prejemniki odgovorijo napadenemu.

Brezžično omrežje

- Sestavljajo ga:
  - Bazne postaje, povezane v ožičeno omrežje
  - Brezžični odjemalci (prenosnik, telefon, tablica…)
  - Brezžične povezave
- Ad hoc omrežje:
  - Ni baznih postaj: pošiljanje le odjemalcem, ki so v dometu
  - Vozlišča se lahko tudi organizirajo v omrežje z lastnim usmerjanjem (MANET – mobile ad hoc network; VANET –vehicular ad hoc network)
- MESH (mreža): več skokov v brezžičnem omrežju, preden pride do ožičene infrastrukture.

Brezžična povezava: lastnosti in težave

- Slabljenje signala, interferenca
- “Multipath propagation” (zaradi odbojev signal potuje po več poteh, daljše imajo večjo zakasnitev)
- Skriti terminal, slabljenje signala



CDMA

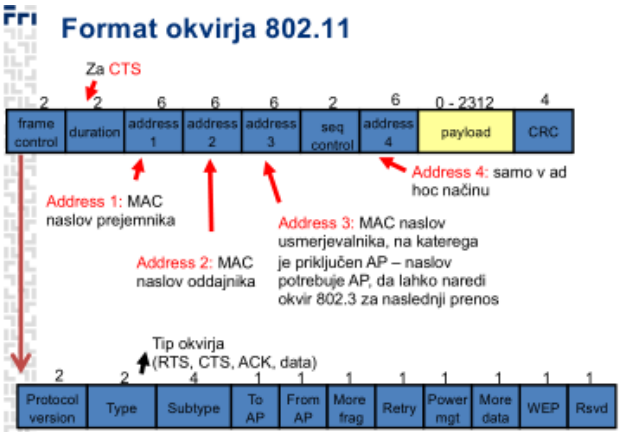
- Code-division multiple access – še en način multipleksiranja
- Tehnologija spread spectrum: ozkopasovni signal se razprši na širše frekvenčno območje, signal izgleda podoben šumu. V IEEE 802.11 sta dve tehnologiji SS:
  - Frequency hopping SS: hitro spreminjanje frekvenc (11b)
  - Direct sequence SS: fazna modulacija kratkih pulzov, mnogo krajših od 1 bita (11a in 11g)
- Vsak odjemalec ima svojo razprševalno kodo, s katero kodira oziroma dekodira signal.
- Kode so tako izbrane, da je interferenca minimalna (ortogonalni signal) in se sočasni različno kodirani signali ne motijo med seboj.
- Težko prisluškovanje, “anti-jamming”, skrivanje obstoja komunikacije

Principi delovanja WLAN

- Uporaba na omejenih področjih (stavba)
- Prihodnost: fiksna brezžična omrežja - npr. za last-mile širokopasovne povezave nekaj km, Mobilni telefon z WLAN + VOIP (poceni pogovor mimo operaterja)

- Primer: 2.4 GHz področje: 11-14 delno prekrivajočih kanalov različnih frekvenc (niso povsod vsi dovoljeni – regulativa). Administrator izbere kanal za AP. Uporabnik skenira kanale, ko išče AP.
- CSMA/CA
    - carrier sense: posluša pred oddajo, ni detekcije kolizij (med oddajanjem je sprejemnik izključen)
    - collision avoidance
        - Več algoritmov, npr. MACAW (Multiple Access Collision Avoidance for Wireless),
        - Postaja si "rezervira" kanal: Odda RTS (request to send), Prejme CTS (clear to send: katera postaja, koliko časa)
        - Šele po prejemu CTS odda podatke.
        - CTS slišijo vsi, zato počakajo: v podatkih ni kolizij

Protokol vključevanja v WLAN



- Postopek aktivne izbire pristopne točke – scanning :
    - Probe (Je v bližini kak AP?)
    - Probe response (Jaz sem AP)
    - Association Request (Rad bi se pridružil)
    - Association Response (Kar izvoli)
- Pasivna izbira (passive scanning)
    - AP periodično oddaja beacon frame ("Jaz sem AP in podpiram naslednje hitrosti prenosa...")
    - Naprava lahko odgovori z Association Request
- Možna je mobilnost znotraj IP podomrežja.

IEEE 802.15 – osebno omrežje

- PAN – personal area network
- Razvoj iz Bluetooth specifikacije
- Manj kot 10 m, namesto kablov (miš, slušalke...)
- Ad hoc omrežje. (Bluetooth ima lahko tudi AP).
- Gospodar (npr. PC) mora sužnjem (npr. miški) dovoliti oddajanje.
- BLE – del BT4 specifikacije (Low energy

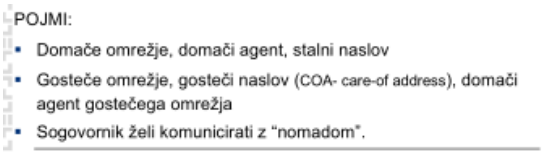
Celularna omrežja

- Bazne postaje, mobilni uporabniki, ožičeno omrežje
- Kombinacija FDMA/TDMA (GSM) ali CDMA
- Generacije: 1G, 2G,..., 5G
- Kaj sploh je 5G? več povezav na celico (4G:nekaj 1000, 5g: nekaj MIO na km2)
    - mmWave – kratek domet, večja gostota uporabnikov
    - O tehnologijah se še ne ve dosti. 5G NR - "new radio"
    - Latenca (4G: 50 ms, 5G: 5ms): "self driving car"

Delovanje celularnega omrežja

- Omrežje: bazna postaja pokriva svojo “celico” (uporablja okrog 200 kanalov)
- Mobilni terminal poišče celico z najmočnejšim signalom in se prijavi.
- Bazna postaja obvesti o prijavi lokalno centralo, ta pa matično.
- Ko pride klic, se ta usmeri v ustrezno celico.
- Če jakost signala pade, se terminal preklopi na drugo celico.
- Podatkovni prenos: ločena arhitektura od tiste za prenos zvoka.

Zagotavljanje mobilnosti



- Pri omrežjih mobilne telefonije so podobni problemi kot pri zagotavljanju mobilnosti v IP (vgrajeno v IPv6).
- Mobilnost znotraj omrežja : mobilnost med omrežji
- Ohranjanje seje, ohranjanje naslova

Usmerjanje – 3 možnosti

- Usmerjevalni algoritem oglašuje stalne (fiksne) naslove gostov – ni skalabilno!
- Posredno usmerjanje: prek domačega agenta
    - Nomad se prijavi pri domačem agentu gostečega omrežja, ta obvesti nomadovega domačega agenta.
    - Sogovornik kliče prek nomadovega domačega agenta.
    - Nomad odgovarja direktno sogovorniku.
    - Neučinkovito, če sta oba v istem omrežju!
    - Pri premiku v drugo omrežje povezava ostane.
- Neposredno usmerjanje: sogovornik pridobi od domačega agenta gosteči naslov nomada in se direktno poveže z njim (Težji premik v drugo omrežje (forwarding prometa - chaining)).

Omrežna plast

- Omrežni protokoli so v vsakem računalniku in usmerjevalniku!
- NALOGE: Prenos segmenta transportne plasti od izvornega do ciljnega računalnika (Iskanje poti, naslavljanje, delo z datagrami, obvestila), Pošiljatelj: enkapsulacija segmentov v IP datagrame, Prejemnik: izluščenje in predaja segmentov transportni plasti

Omrežna plast nudi storitve transportni plasti

- Transportna: od procesa do procesa
- Omrežna: od računalnika do računalnika

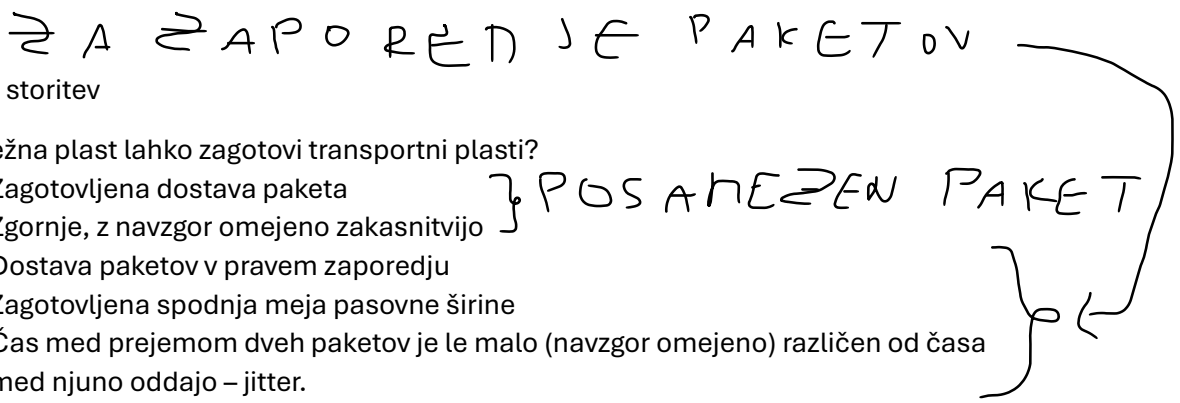
Usmerjevalnik

- Naprava, ki deluje na omrežni plasti

- Posreduje datagrame iz enega v drugo omrežje
- Prenaša datagrame po hrbtenici omrežja
- Izvaja posredovanje in usmerjanje

Ključni funkciji omrežne plasti

- Posredovanje paketov (forwarding) -> “Prenos” paketa iz vhoda v usmerjevalnik na ustrezno izhodno povezavo. Znotraj enega usmerjevalnika!
- Usmerjanje (routing) -> Določitev in izvedba poti paketov od izvora do cilja. “Kolektivno delo” vseh naprav po pravilih usmerjevalnega protokola.
- Pogosto zamenjavanje teh dveh pojmov (npr. usmerjevalna tabela - posredovalna…)
- V nekaterih omrežjih je funkcija omrežne plasti tudi vzpostavljanje povezave (ATM, Frame Relay, X.25)



Model omrežnih storitev

- Kaj omrežna plast lahko zagotovi transportni plasti?
    - Zagotovljena dostava paketa
    - Zgornje, z navzgor omejeno zakasnitvijo
    - Dostava paketov v pravem zaporedju
    - Zagotovljena spodnja meja pasovne širine
    - Čas med prejemom dveh paketov je le malo (navzgor omejeno) različen od časa med njuno oddajo – jitter.
- Kaj od tega zagotavlja Internet? -> best effort -> ni nobenih zagotovil

IPv4 naslavljanje

- Vmesnik: povezuje računalnik ali usmerjevalnik s fizično linijo (network interface, omrežna kartica…).
- IPv4 naslov je 32-bitni ID vmesnika

Podomrežje

- IP naslov vsebinsko pomeni dvoje: naslov omrežja (predpona) | naslov naprave znotraj tega omrežja (analogija: hišne številke na ulici)
- (Pod)omrežje je množica vmesnikov, ki imajo enak naslov (pod)omrežja ter/ali med seboj so dosegljivi brez posredovanja usmerjevalnika.
- Maska podomrežja določa dolžino naslova (pod)omrežja (je 32-bitni niz, ki ima enice na mestih, ki označujejo naslov omrežja, na ostalih so ničle). Je poljubno dolga.
- Usmerjevalnik ima na vsakem vmesniku drugo (pod)omrežje.
- Znotraj (pod)omrežja ni usmerjevalnikov, so pa lahko stikala (switch) in razdelilniki (hub).
- Prefiksna ali CIDR notacija (classless inter-domain routing): 223.1.1.0/24
- Broadcast naslov: same enice. Velja za omrežje in napravo. Pošilja se vsem v omrežju, usmerjevalnik ga ne posreduje naprej. 233.1.1.255 -> 255.255.255.255

Kako določati podomrežja?

- Nekoč so bili definirani razredi omrežij z masko 8, 16 ali 24 bitov. Težava: prevelika ali premajhna podomrežja, neizkoriščenost naslovnega prostora. Classful usmerjanje: maske ne potrebujemo.
    - Razred A – prvi bit =0
    - Razred B – prva dva bita 10
    - Razred C – prvi 3 biti 110
- Kasneje: brezrazredno usmerjanje (classless) – CIDR ali prefiksna notacija, potrebujemo masko
- Broadcast naslov: razpošiljanje vsem adapterjem znotraj podomrežja (same enice v naslovu naprave).

ISP-jev blok:	11001000 00010111 00010000 00000000	200.23.16.0/20
Podjetje1:	11001000 00010111 00010000 00000000	200.23.16.0/23
Podjetje2:	11001000 00010111 00010100 00000000	200.23.18.0/23

Kako poteka dodeljevanje IP naslovov

- Naprava: Administrator vpiše naslov (fiksen) ali DHCP strežnik dodeli naslov (dinamičen) – admin prej strežniku dodeli ustrezen rang naslovov
- Omrežje podjetja: Ponudnik dostopa do interneta (ISP) dodeli del svojega naslovnega prostora.
- ISP: ICANN dodeli naslovni prostor (Internet Corporation for Assigned Names and Numbers)

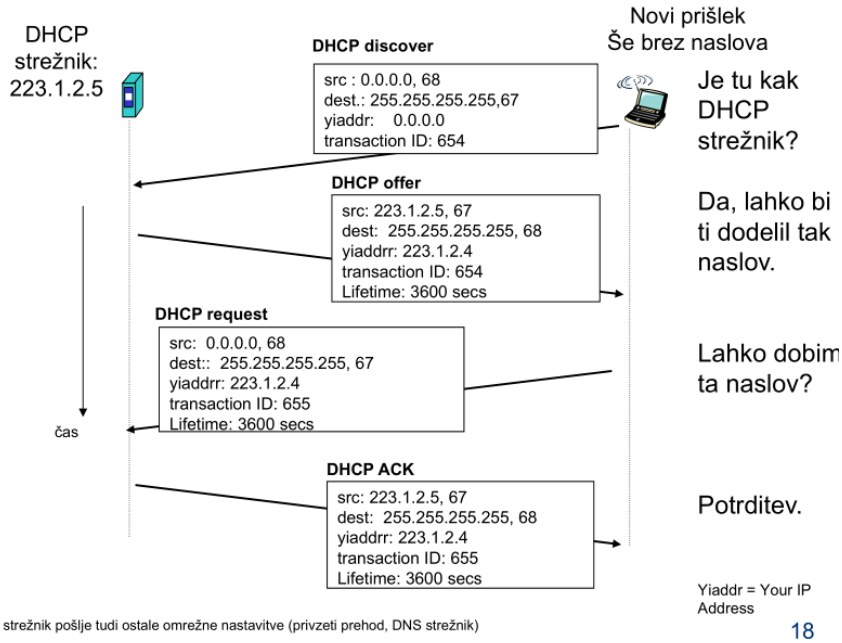
Hierarhično naslavljanje

- Pravilno dodeljevanje CIDR naslovov olajša usmerjanje!
- Agregiranje ali sumarizacija naslovov – en prefiks za usmerjanje v več omrežij.

Manj učinkovito naslavljanje

- ISP2 ima bolj specifičen naslov (daljši prefiks se ujema) za usmerjanje v Podjetje2. Usmerjevalne tabele so daljše.

Dodelitev naslova s pomočjo DHCP

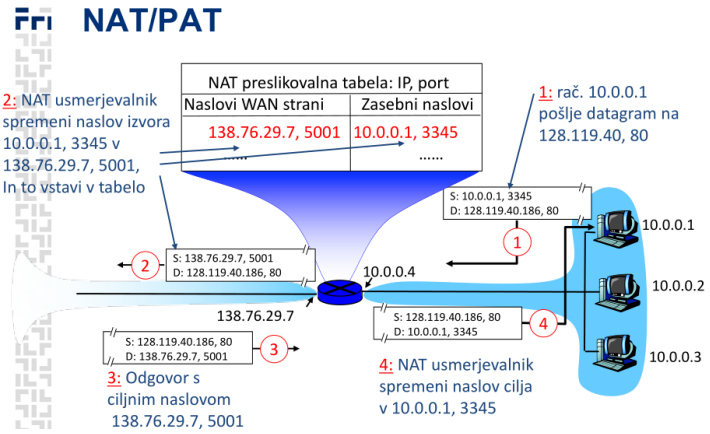


DHCP strežnik pošlje tudi ostale omrežne nastavitve (privzeti prehod, DNS strežnik)

NAT – Network Address Translation (RFC 2663,3022)

Naslovi	Omrežje/maska	Št. naslovov
10.0.0.0 - 10.255.255.255	10.0.0.0/8	2^{24}
172.16.0.0 - 172.31.255.255	172.16.0.0/12	2^{20}
192.168.0.0 - 192.168.255.255	192.168.0.0/16	2^{16}

- Motivacija: pomanjkanje IPv4 naslovnega prostora
- Zasebni naslovni prostor, RFC 1918
- Zasebni (notranji, interni) naslovi se uporabljajo le znotraj omrežja.
- Na NAT usmerjevalniku se naslov preslika v zunanji naslov
- NAT usmerjevalnik in celo omrežje za njim navzven izgleda kot ena naprava.
- NAT usmerjevalnik: Zamenja naslov izvora izhodnim datagramom -> Zapomni si preslikavo (par notranji + zunanji naslov) -> Zamenja naslov cilja vhodnim datagramom



Prednosti uporabe NAT

- Za celotno omrežje zadošča le en javni IP naslov
- V omrežju je lahko preko 65000 naprav (port – št. vrat je 16 bitna številka)
- Notranje naprave niso neposredno dostopne od zunaj, zato so manj varnostno izpostavljene
- Naslove notranjih naprav lahko spreminjamo neodvisno od zunanjega naslova
- Lahko zamenjamo ponudnika dostopa do interneta brez spreminjanja notranjih naslovov

Kritika NAT-a

- Usmerjevalniki – 3.plast: naj ne bi imeli opravka s 4. plastjo (vrata - porti)!!! Št.vrat je namenjena za naslavljanje procesov, ne računalnikov.
- Težava s strežniki na notranji strani (poslušajo na dogovorjenih vratih – well known port, NAT to številko zamenja).
- Pomanjkanje naslovov: raje uporabimo IPv6!
- Krši „end-to-end argument“ (za aplikacije naj bi bilo omrežje transparentno): npr. P2P načrtovalci morajo programirati tudi za primer NATa.
- Računalnik za NAT-om ne more sprejemati povezav, ker nima fiksnega naslova in ga ne more objaviti. Lahko le sam zahteva povezave (NAT traversal)

Rešitve za prehod čez NAT (NAT traversal)

1. Statično konfiguriramo NAT – dodamo zapis v NAT tabelo (npr. 123.76.29.7, 2500 gre vedno v 10.0.0.1, 25000).

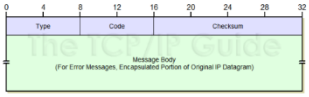
2. Universal Plug and Play (UPnP) Internet Gateway Device (IGD) protokol omogoča napravi za NATom ugotoviti zunanji IP naslov, in statične vnose v tabelo.
3. Prek posrednika: rač. za NAT-om ima stalno povezavo do posrednika, ki niza NAT-om. Sogovornik vzpostavi povezavo s posrednikom. Posrednik posreduje promet med njima, ali pa signalizira prvemu, da vzpostavi povezavo do drugega. (Connection reversal: Peer A se poveže z B prek C-ja, s katerim ima B trenutno aktivno povezavo, in ga prosi, naj B vzpostavi povezavo z A.).

ICMP (RFC 792)

- Internet Control Message Protocol
- Sporočila v zvezi z omrežjem – napake, …
- Pod-plast v omrežni plasti, leži rahlo nad IP (uporablja IP datagram za prenos ICMP sporočila, kot protokol višje plasti v glavi je naveden ICMP)
- Polja ICMP sporočila: tip, koda, glava in del IP datagrama, ki je povzročil napako (če je bila…)

ICMP sporočila

Tip	Koda	Pomen
0	0	echo reply (ping)
3	0	dest network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control – ni v uporabi)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header



Traceroute

- Po kateri pot igre promet do določenega IP-ja?
- Izvor pošilja serijo UDP paketov na (redek) port – Prvi: TTL=1, drugi: TTL=2, itd.
- Usmerjevalnik prejme datagram s TTL=0 -> Ga zavrže -> Izvoru pošlje obvestilo – ICMP tip 11, koda 0 -> Obvestilo vključuje ime in IP usmerjevalnika
- Izvor izračuna čas vrnitve
- STOP: ko naslednji UDP paket doseže cilj, ali pa izvor dobi sporočilo “host unreachable” – tip3, koda 3.

Napadi na ICMP

- Ponarejen ICMP "Time exceeded" ali "Destination unreachable" povzroči, da takoj pade TCP povezava.
- Ping of Death – napad s fragmentacijo – pošljemo fragmentiran ping paket, daljši kot 65635 bytov
    - Obramba: kontrola odmikov in dolžin fragmentov (polje odmik: 13 bitov -> zadnji fragment z max. odmikom je lahko dolg max 7 bytov, sicer je datagram predolg).
- Smurf – napadalec pošlje ping s ponarejenim naslovom izvora na broadcast naslov v omrežju. Vsi odgovorijo napadenemu – DoS. Tako omrežje je smurf amplifier. Obramba:
    - Blokirati ping promet / broadcast promet ALI Usmerjevalniki (prehodi) ne spustijo v omrežje paketov na broadcast naslov.

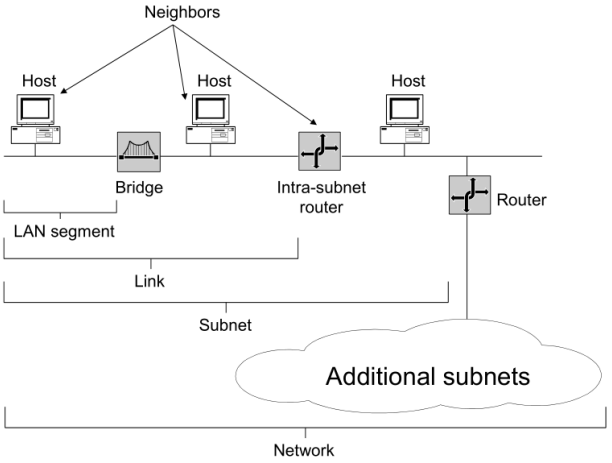
IPv6

- Motivacija: večji naslovni prostor je potreben – 128 bitov, format glave – hitrejše usmerjanje, glava – omogoča QoS
- IPv6 datagram: fiksna glava 40 bytov, fragmentacija ni dovoljena

Prednosti IPv6

- Dovolj velik naslovni prostor
- Mednarodno uravnoteženje
- End-to-end komunikacija (P2P)
- Strukturirano izbiranje naslovov
- Razširljivost
- Hitro usmerjanje in posredovanje
- Vgrajeno: varnost in mobilnost, QoS

IP v6 terminologija



Naslovni prostor IPv6

- 128-bitni naslovni prostor
- Zato imamo lahko fleksibilno večnivojsko hierarhijo (naslavljanje, usmerjanje)
- Tipičen unicast naslov: 64 bitov za ID podomrežja in 64 bitov za ID vmesnika

Sintaksa IPv6 naslova

- 8 16-bitnih skupin, lahko hex/binarno
- Vodilne ničle v vsaki skupini lahko izpustiš
- Kompresija ničel:
  - Dolga zaporedja samih ničel
  - Zaporedje 16-bitnih blokov iz samih ničel lahko zapišemo kot dve dvopičji ::(le 1x)
  - Kompatibilnost z v4 naslovi: spredaj dodamo ničle
    - 193.2.72.1 → ::193.2.72.1
    - Lahko pustimo tudi pike iz v4 naslova!

Datagramsko omrežje

- Na omrežni plasti ni vzpostavljanja klica.
- Usmerjevalniki ne vedo nič o končnih povezavah.
- Paket se posreduje glede na naslov cilja.
- Med istim izvorom in ciljem lahko po več poteh.

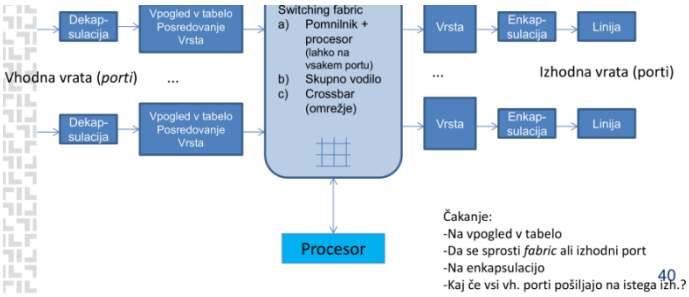
Posredovalna tabela v datagramskem omrežju

- Če je 32-bitni naslov: 4 mrd. različnih naslovov!
- V tabeli uporabimo rang naslovov, npr:
- Ujemanje najdaljše predpone (longest prefix match)

Ciljni naslov	Vmesnik povezave
Od 11001000 00010111 00010000 00000000 Do 11001000 00010111 00010111 11111111	0
Od 11001000 00010111 00011000 00000000 Do 11001000 00010111 00011000 11111111	1
Od 11001000 00010111 00011001 00000000 Do 11001000 00010111 00011111 11111111	2
sicer	3

- Na kateri vmesnik posredovati
  - 11001000 00010111 00010110 10100001 ?
  - 11001000 00010111 00011000 10101010 ?

Kaj dela usmerjevalnik?



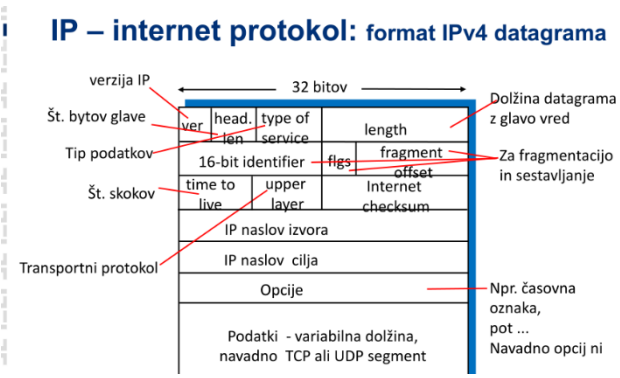
- Izvaja usmerjevalni protokol (npr. OSPF, BGP, RIP, EIGRP...)
- Posreduje datagrame iz vhodnih na izhodne povezave.
- Vhod:
  - Sprejem na nivoju bitov
  - Povezavna plast – dekapsulacija
  - Omrežna plast, ciljni IP naslov, vpogled v posredovalno tabelo, po potrebi čakanje v vrsti za prenos na izhod
  - Težave, če je jedro počasnejše kot kombinacija vseh vhodov! Vrste, zakasnitve, izgube paketov.
  - HOL (Head of the Line) blokiranje – prvi datagram v vrsti blokira tiste za njim, ki bi sicer lahko napredovali prek jedra.
- Težava: posredovanje je potrebno izvajati s hitrostjo vhodne povezave.

Preklapljanje med vhodnimi in izhodnimi vmesniki (porti)

- Preko pomnilnika:
  - Preklapljanje je pod nadzorom CPU
  - Datagram se prebere v sistemski pomnilnik, nato CPU naredi vpogled v posredovalno tabelo
  - Datagram se skopira na ustrezni izhod
  - Za vsak datagram sta potrebna 2 prehoda po vodilu
- Preko vodila:
  - Datagram se prebere iz pomnilnika na vhodu direktno v pomnilnik na izhodu
  - Za vsak datagram le en prehod po vodilu

Kaj se dogaja na izhodu?

- Jedro je hitrejše kot izhod: potrebna je vrsta.
- Čakanje – zakasnitve
- Datagrami se lahko izgubijo (zamašitev)
- Kaj če je intenzivnost prihajanja višja kot intenzivnost odhajanja?
- Razvrščanje datagramov v vrsti za izhod (prioritete – kdo dobi najboljše performanse)
- „Output Port Buffer Overflow“ – zakasnitve in izgube
- Koliko prostora v izhodnem bufferju?
  - (RFC 3439) : RTT (npr. 150 ms) * hitrost povezave
  - Če je N tokov: RTT*C / sqrt(N)

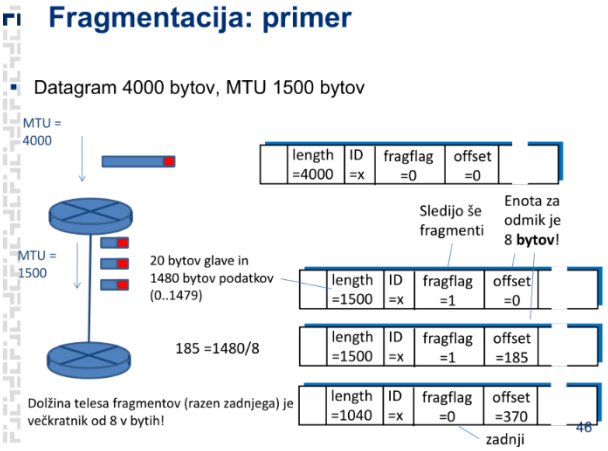


Režija

- 20 bytov: TCP glava
- Plus 20 bytov IP glava
- Plus režija aplikacijske plasti
- Delež režije v paketu je odvisen od dolžine podatkovnega dela!

Fragmentacija

- Povezavna plast: omejena dolžina okvirja (MTU), odvisna od tehnologije.
- V omrežju je lahko več tehnologij, zato se "med potjo" spreminja MTU!
- Fragmentacija: velik IP datagram z vhoda se razbije na več manjših IP datagramov-fragmentov.
- Fragmentira lahko usmerjevalnik sredi poti.
- Nazaj sestavlja vedno šele omrežna plast na cilju, pred predajo transportni plasti.

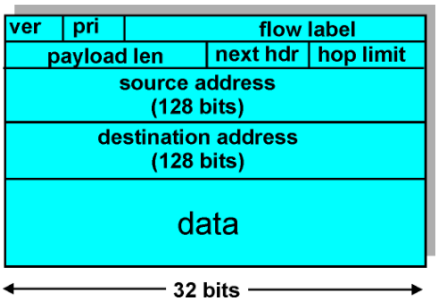


Napadi na fragmentacijo

- Klasika: TEARDROP napad - spada med DoS napade
  - Napadalec: fragmentirani paketi z namerno napačnimi odmiki/dolžinami (prekrivanje) – „fragment overlapped"
  - Pri sestavljanju se ciljni sistem zmede in (lahko) sesuje – napaka v kodi TCP/IP sklada!
- Ping of Death – pošljemo fragmentiran ping paket, daljši kot 65635 bytov
  - Obramba: kontrola odmikov in dolžin fragmentov (polje odmik: 13 bitov -> zadnji fragment z max. odmikom je lahko dolg max 7 bytov, sicer je datagram predolg).
- Fragment overlapped – prekrivanje
  - Sistem se zmede, lahko crash (DoS)
  - Fragment se (delno) prepiše – želimo zaobiti IDS, da ne prepozna napada (če IDS ne defragmentira) (Fragment overwrite)
- Fragmentation Buffer Full - posledica (želimo zaobiti IDS)
  - Veliko datagramov z manjkajočimi fragmenti (Incomplete Datagram)
  - Posamezni datagrami z veliko/velikimi fragmenti
- Fragment Overrun – sestavljen datagram je večji kot dovoljuje dolžina polja length v glavi. (crash – DoS napad)
- Fragment Too Small – ne-zadnji fragment krajši od 400 bytov (zaobiti IDS ali druge filtre)

IPv6 format datagrama

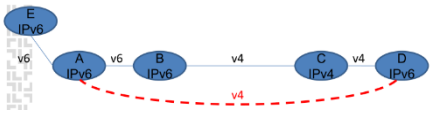
Pri – prioriteta med datagrami (razred prometa)
Flow label – omogoča identificirati datagrame, ki pripadajo istemu toku (npr. video)
Next header – protokol višje plasti ali lokacija razširitve glave
Hop limit = TTL



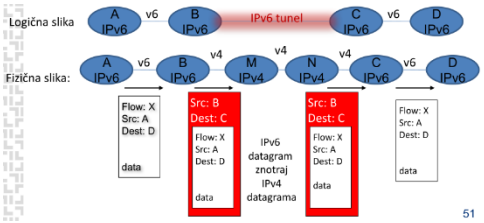
Ni polj fragmentacije, kontrolne vsote, opcij (le kot razširitev glave).

ICMP v6 – dodatne funkcije, npr. sporočilo Packet Too Big.

Prehod IPv4 – IPv6



- Dual-stack: usmerjevalnik pozna v4 in v6. Z v6-enabled "govori" v6, z ostalimi pa v4.
    - Kako to ugotovi? DNS vrne v6 ali v4 naslov. DNS mora biti že na v6!
    - Če je na poti med dvema v6 vozliščema kakšno v4, se bo promet vmes pretvarjal v v4; v6-specifična polja se bodo izgubila!
- Tuneliranje: IPv6 datagram zapakiramo v enega ali več IPv4 datagramov kot podatke.
- Translacija naslovov (prevajanje).



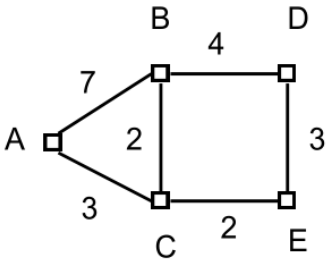
51

Usmerjanje

- Abstraktni model: teorija grafov, vozlišča, povezave.
- Algoritmi za iskanje najkrajše (najcenejše) poti: to je naloga usmerjevalnih algoritmov – prilagoditi posredovalne tabele tako, da bodo šli paketi po najkrajši poti.

Principi

- Statično (neadaptivno) ali dinamično (adaptivno): ali upošteva trenutne razmere v omrežju in jim prilagaja usmerjanje prometa?
- Po eni poti ali po več poteh: ali gredo v nekem trenutku vsi paketi z istim ciljem po isti poti?
- Globalno (centralizirano) ali porazdeljeno: Ali so pri izračunu poti znani podatki za celo omrežje?
- Prilagodljivi in neprilagodljivi na obremenitev povezav: prilagodljivi avtomatsko prilagajajo cene povezav glede na zasičenost povezave, s čimer dobijo manjšo ceno bolj proste poti
- Možne so vse kombinacije.
- OPTIMALNO usmerjanje: Vsebovanost krajših optimalnih poti v daljši, drevo ponora (sink tree)



Usmerjanje po najkrajši poti glede na čas, ceno, št. skokov,...

Usmerjevalna tabela za vozlišče A
-zakasnitev
-št. skokov

- statično
- po eni poti

AB	AB (1)
AC	AC (1)
AD	ABD (2)
AE	ACE (2)

AB	ACB (5)
AC	AC (3)
AD	ACED (8)
AE	ACE (5)

55

Dijkstrin algoritem za iskanje najkrajše poti: Iščemo pot A-E

- Začnemo v A -> vsako vozlišče dobi oznako: ceno + zadnjo postajo do sedaj najboljše poti -> v vsaki iteraciji smo korak bližje cilju -> nehamo, ko so vsa vozlišča označena.

Usmerjanje po več poteh

- Določen je delež paketov za vsako izmed možnih poti.
- Uporaba npr. za uravnoteženo obremenitev (load balancing).
- Ponekod je lahko možna le ena pot.
- Paketi lahko blodijo – preprečiti!

Usmerjevalna tabela za vozlišče A:

A➔B: B 33%, C 67%
A➔D: B 50%, C 50%
A➔C: B 12%, C 88%
A➔E: C 100%

- statično
- po več poteh

Centralizirano usmerjanje

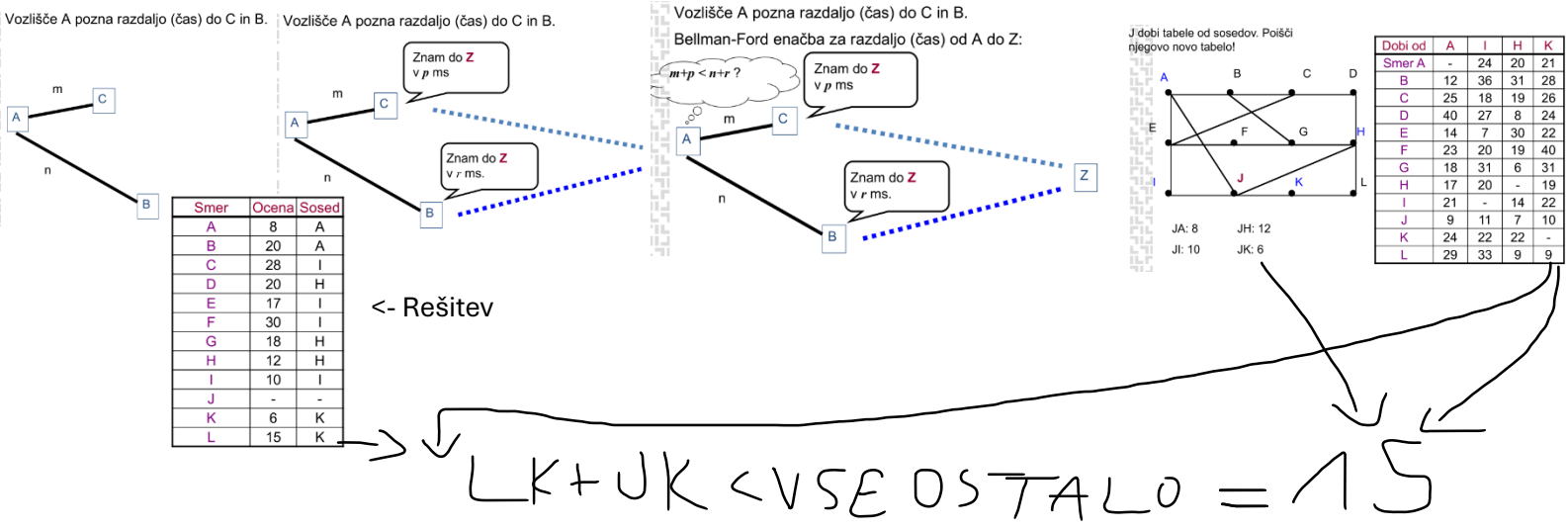
- Glavno vozlišče (master, koordinator)
- Zbira podatke o razmerah v omrežju
- Izračuna tabele in jih razpošlje
- Alternativa: vsi razpošiljajo podatke, vsak zase izračunava globalno usmerjanje (link state routing)
- TEŽAVA: velika omrežja s hitrimi spremembami
- Dinamično / lahko po eni ali po več poteh

Izolirano usmerjanje

- NE UPOŠTEVA razmer v omrežju
- Hot potato: vozlišče (usmerjevalnik) se hoče čimprej znebiti paketa, zato ga vrže
  - V najkrajšo izhodno vrsto
  - Dolžina vrste ´ utež
- Poplavljanje – v vse izhodne vrste
- Selektivno poplavljanje – tiste, ki so približno v pravi smeri

Porazdeljeno usmerjanje

- Vsako vozlišče pozna razdaljo do svojih sosedov.
- Med seboj si izmenjujejo usmerjevalne tabele (asinhrono, ob spremembah lokalnih povezav ali ob prejemu drugih sprememb)
- Potem pregledajo in prilagodijo svoje tabele.
- Lastnosti:
  - Dobre novice se širijo hitro, slabe počasi (počasi konvergira).
  - Problem štetja do neskončnosti (pomagamo si s poisoned reverse)



Smer	Ocena	Sosed
A	8	A
B	20	A
C	28	I
D	20	H
E	17	I
F	30	I
G	18	H
H	12	H
I	10	I
J	-	-
K	6	K
L	15	K

Dobi od / Smer A	A	I	H	K
B	12	36	31	28
C	25	18	19	26
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	-	19
I	21	-	14	22
J	9	11	7	10
K	24	22	22	-
L	29	33	9	9

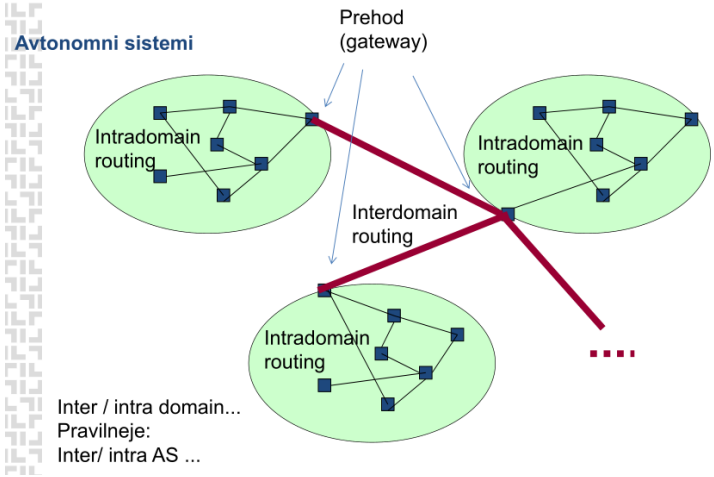
Porazdeljeno usmerjanje ali usmerjanje z vektorjem razdalj (angl. Distance vector routing)

- Internet:
  - RIP: se opušča
  - Cisco: IGRP (ne podpira VLSM - variabilne maske) – se opušča (Interior Gateway Routing Protocol)
  - Cisco: EIGRP – Enhanced IGRP (podpira VLSM)
  - BGP – Border Gateway Protocol
- DSDV - Destination-Sequenced Distance-Vector Routing (za ad hoc mobilna omrežja)

Usmerjanje glede na stanje povezav

- Usmerjevalnik: odkrivanje sosedov, naslovi -> HELLO paketi
- Meritev zakasnitve (cene) do sosedov -> ECHO paketi -> upoštevati tudi čas v vrsti ali ne?
- Izdelava paketa z vsemi temi podatki (+zap.št. in TTL) -> Pošiljati periodično ali ob večjih spremembah?
- Pošiljanje tega paketa ostalim + sprejem ostalih (broadcast) -> Poplavljanje, detekcija duplikatov
- Vsak: izračun najkrajših poti (npr. Dijkstra, Prim) – celotnih.
- V praksi: OSPF, IS-IS (interdomain)

Usmerjanje v internetu



- Usmerjanje z vektorjem razdalj (distance vector routing): porazdeljeno. RIP (se opušča): algoritem Bellman-Ford oz. Ford-Fulkerson
- Usmerjanje glede na stanje povezav (link state routing) – temelji na najkrajših poteh (alg.: Dijkstra)
- Usmerjanje broadcastov in multicastov
  - Vpeto drevo ali “sink tree”; Reverse path forwarding
  - Multicast: usm. mora vedeti, kateri naslovi so v grupi.
- Hierarhično usmerjanje (podomrežja, agregacija)
- Znotraj domene (AS) / med domenami (AS) - (intradomain, interdomain routing)

Usmerjanje med avtonomnimi sistemi

- Interdomain routing, v internetu BGP4 (RFC 1771)
- ZAKAJ dve vrsti usmerjanja?
  - politika, velikost interneta, zmogljivost znotraj AS
- Medsebojno informiranje
  - AS oglašuje naslove, ki jih premore.
  - AS oglašuje (nekatere) naslove, do katerih zna usmerjati (politika).

Usmerjanje iz AS

- Če je v AS le en prehod
  - promet, namenjen iz AS, se usmerja na ta prehod
- Če je več kot en prehod
  - Na katerega naj se usmerja promet, namenjen iz AS?
    - Usmerjevalnik ugotovi, da je več prehodov do X.
    - Iz intra-AS ugotovi, do katerega prehoda pride najceneje
    - Hot potato: promet usmeri na najcenejšega
    - Doda ta podatek v svojo posredovalno tabelo

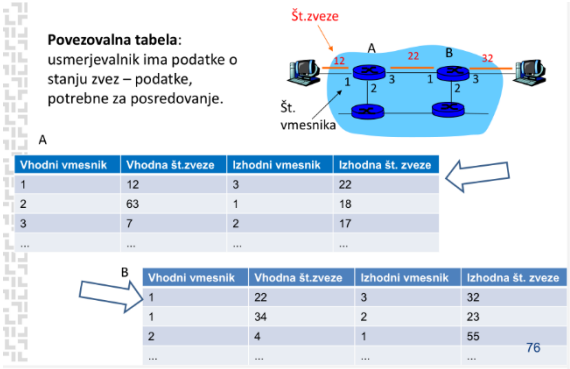
BGP

- BGP seje: med usmerjevalniki znotraj AS in med AS-ji
- Različna omrežja (stub – ne posreduje prometa v druge AS, multihome – več kot 1 prehod, ...)
- Ogromne tabele (več 10.000 zapisov). Naslovi v tabelah predstavljajo omrežja – CIDR prefiksi.
- BGP: prehodi usmerjajo po ideji vektorja razdalj, merilo je št. skokov.
- Oglaševanje poti gre tudi v ne-sosedne AS.
- BGP mora upoštevati še politiko, ki ni odvisna od tehnologije. Npr: Promet z izvorom ali ponorom v IBM ne sme prek Microsofta.

Povezavne in nepovezavne storitve

- Podobno kot pri transportnih storitvah (vendar) :
  - Storitev od izvornega do ciljnega računalnika
  - Ni izbire (le eno ali drugo - kar ponuja omrežje)
  - Izvedba je v jedru omrežne hrbtenice – usmerjevalnikih
- Datagramsko omrežje: nepovezavna storitev
- Virtualne zveze (virtual circuit): povezavna storitev, npr. ATM, Frame Relay, X.25

Virtualne zveze



- Podobno kot telefonske zveze
  - Vzpostavljanje in rušenje povezave: sodelujejo vsi
  - usmerjevalniki na poti. Signalizacija: protokoli vzp. in rušenja (klic prihaja, sprejem klica)...
  - Vsak paket ima identifikator zveze (ne naslov cilja)
  - Ob vsakem hopu se št. zveze zamenja
  - Vsak usmerjevalnik na poti: vodi stanje vsake aktivne zveze
  - Za zvezo se lahko se rezervirajo viri (vmesniki, pasovna širina)
- Elementi virtualne zveze: celotna pot, številke zveze (po ena za vsak hop), zapisi v tabelah na poti.

MPLS

- Multiprotocol label switching
- Namen: pospešiti IP usmerjanje (posredovanje):
  - Na podlagi oznake (fiksne dolžine) namesto IP naslova
  - – Ideja je sposojena iz virtualnih zvez, vendar datagram obdrži IP naslov

Primerjava datagramskega in omrežja z virtualnimi zvezami

Internet	ATM
Komunikacija med računalniki. Elastične storitve, čas ni tako pomemben	Izvira iz telefonije. Zakasnitev in zanesljivost sta pomembna
"Pametni" končni sistemi (računalnik)	"Neumni" končni sistemi (telefon)
Preprostejše omrežje (usmerjevalnik)	Kompleksnejše omrežje (usmerjevalnik)
Lažje dodajati nove storitve (aplikacija). Lažje povezovati heterogena omrežja.	Težje dodajati nove storitve (infrastruktura)

MPLS usmerjanje

- "Label-switched" usmerjevalnik
- Posredovanje paketov glede na oznako
- MPLS tabela je drugačna od usmerjevalne
- (v IP usmerjanju npr. določanje poti glede na izvor prometa ne bi bilo možno)
- Potreben je signalizacijski protokol za vzpostavljanje poti (RSVP– Resource ReSerVation Protocol, RFC 2205)
- Dobra združljivost z IP-usmerjevalniki

Varnost in IP: IPsec

- Uporaba za VPN: kriptiranje prometa od izvora do ponora, IPsec funkcionalnost potrebna le na izvoru in ponoru, IPsec plast vzame transportni segment, ga kriptira, doda svojo glavo in vse to zapakira kot telo v navaden IP datagram.
- Storitve: Dogovor o kriptografiji in ključih, Enkripcija in dekripcija, Integriteta podatkov

Transportna plast

Naloge transportne plasti:

- povezovanje dveh oddaljenih procesov
- multipleksiranje/demultipleksiranje komunikacije med procesi
- zanesljiv prenos podatkov
- kontrola pretoka in zamašitev

Storitve transportne plasti

- Logična komunikacija med aplikacijskimi procesi
  - pošiljatelj: sporočilo razbije v SEGMENTE in jih posreduje v enkapsulacijo omrežni plasti
  - prejemnik: dekapsulira segmente iz paketov, sestavljene segmente združi v sporočila in jih posreduje aplikacijski plasti
- protokola TCP in UDP
- razlika med omrežno in transportno plastjo
  - omrežna plast: logična povezava med končnimi sistemi
  - transportna plast: logična povezava med procesi
- storitve transportne plasti:

- so omejene s storitvami nižje (t. j. omrežne) plasti
- vsak transportni protokol lahko zagotavlja svojo množico storitev
  - TCP: zanesljiva, povezavna storitev, ima nadzor zamašitev
  - UDP: best-effort (nezanesljiva), nepovezavna storitev
- v Internetu nimamo naslednjih storitev: zagotovljen čas dostave, zagotovljena pasovna širina

Kako komunicirati s procesom (aplikacijo)?

- vsak proces (~ aplikacija) ima vstopno točko, ki jo imenujemo vtič (socket)
- vtič je vmesnik med aplikacijsko in transportno plastjo
- če na končnem sistemu teče več procesov, ima vsak od njih svoj vtič
- preko vtiča proces sprejema in oddaja sporočila v omrežje

Kako poteka demultipleksiranje?

- vsak transportni segment potuje znotraj svojega paketa IP
- transportni segment v glavi 16-bitni polji: številki vrat izvora (oznaka procesa, ki pošilja) in ponora (oznaka procesa na ciljni strani)

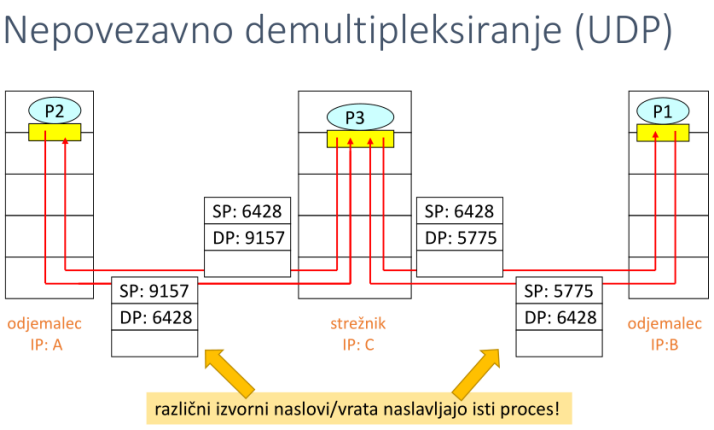
Multipleksiranje in demultipleksiranje

- pošiljatelj: pobira podatke z več vtičev (socket), opremi jih z glavo, pošlje
- prejemnik: segmente razdeli ustreznim vtičem

Kako nasloviti proces na drugi strani?

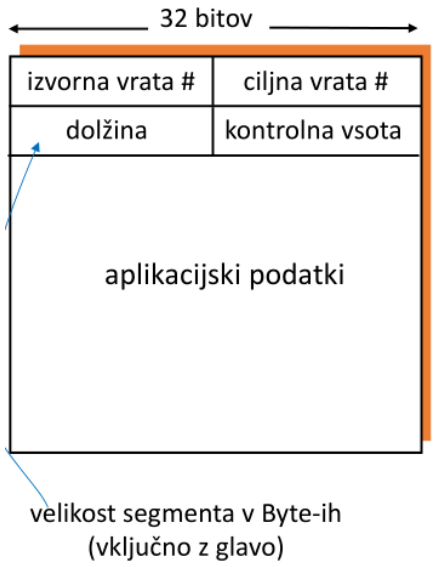
- za enolično naslovitev vtiča potrebujemo:
  - naslov vmesnika naprave (host address): IP številka
  - naslov procesa (znotraj naprave): številka vrat
- znane aplikacije uporabljajo znane številke vrat 0-1023 (t.i. well-known ports), npr. http-80, smtp – 25, dns – 53, telnet – 23, irc – 194, https – 443

Varnost: napad portscan: je namenjen ugotavljanju, na katerih vratih se strežnik odziva. Nudi vpogled v procese, ki tečejo na strežniku. S poznavanjem šibkih točk strežniške programske opreme (npr. OS, SQL server...) lahko napadalec ogrozi delovanje sistema.



SP = source port, izvorna vrata (predstavlja naslov za odgovor)
DP = destination port, ciljna vrata (za naslavljanje vtiča ciljnega procesa)

UDP (User Datagram Protocol) – nepovezavni transport

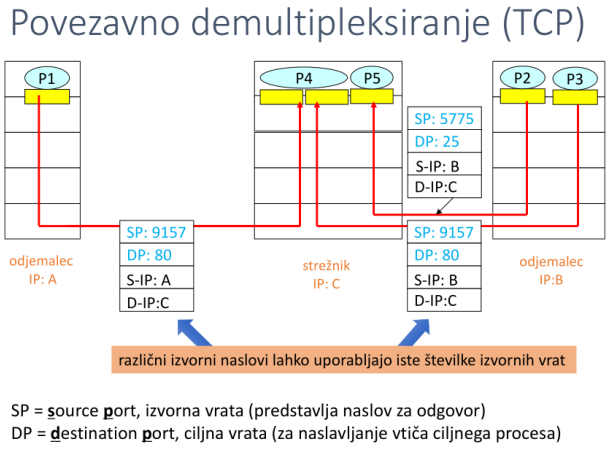


- lastnosti
  - nudi le "best-effort" storitev: izgubljeni datagrami, ne zagotavlja vrstnega reda
  - nepovezaven (nima rokovanja)
  - nima nadzora zamašitev
- prednosti
  - okleščen, najbolj osnoven prenosni protokol brez dodatkov
  - hiter, učinkovit, lahek, minimalističen (ne hrani stanja o povezavi, medpomnilnikov, ni rokovanja)
  - majhna glava datagrama (samo 8B), torej manj režije
- datagram
  - namenjen uporabi v okoljih, kjer lahko toleriramo izgube in je pomembna hitrost pošiljanja: multimedija, DNS/SNMP (upravljanje), usmerjevalni protokoli
  - če pri UDP potrebujemo zanesljivost, ki je protokol ne omogoča, jo moramo zagotoviti na aplikacijski plasti
- internetna kontrolna vsota

  - algoritem za izračun imenujemo internetna kontrolna vsota (Internet Checksum)
  - pošiljatelj sešteje 16 bitne besede in shrani eniški komplement = kontrolna vsota
  - prejemnik sešteje 16 bitne besede skupaj s kontrolno vsoto -> dobiti mora same enice
  - zakaj datagram vsebuje kontrolno vsoto?
    - ni zagotovila, da nižji protokol na posameznih povezavah zagotavlja zaznavanje in odpravljanje napak
    - do napak lahko pride tudi pri hranjenju segmenta v spominu usmerjevalnika in ne nujno pri prenosu (prenosni protokol zagotavlja samo zaznavanje napak pri prenosu)
    - UDP kontrolna vsota je namenjena preverjanju pravilnosti med izvornim in ciljnim procesom, ne pa pri potovanju po posameznih povezavah (t. i. princip končnih sistemov, end-to-end argument/principle)

TCP (Transfer Control Protocol) – povezavni transport

- Potrebujemo protokol, ki zagotavlja zanesljivo dostavo z uporabo nezanesljivega kanala (!). Kaj mora tak protokol nuditi?
  - podatki se ne okvarijo (zaznavamo zamenjave bitov 0 <-> 1)
  - podatki se ne izgubljajo (zaznavamo izgube, ponovno pošiljamo)
  - podatki so dostavljeni v pravilnem zaporedju (urejanje)



SP = source port, izvorna vrata (predstavlja naslov za odgovor)
DP = destination port, ciljna vrata (za naslavljanje vtiča ciljnega procesa)

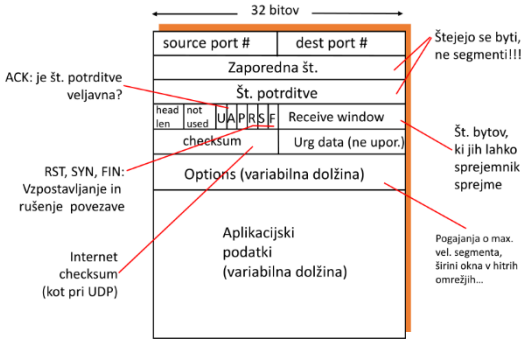
Zagotavljanje zanesljivosti: potrjevanje

- Paket se okvari, paket se izgubi – ni potrditve, Izguba potrditve (pride podvojen paket), Prekratek interval časovne kontrole (duplikat pride), Posredno potrjevanje – samo ACK (optimizacija), Neučinkovitost sprotnega potrjevanja: tekoče pošiljanje, Kontrolna vsota in potrditve ACK-NACK, Časovna kontrola (ponovitev), Številčenje paketov omogoča zaznavanje duplikatov, Številčenje paketov, številčenje potrditev, Tekoče pošiljanje brez čakanja na sprotne potrditve (drseče okno)

Lastnosti protokola TCP

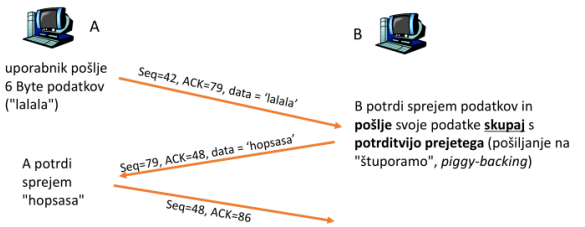
- izvaja se med dvema točkama (point-to-point): en pošiljatelj, en sprejemnik
- znotraj TCP povezave izvaja dvosmerni promet: (full duplex, omejitev MSS)
- nudi zanesljiv, urejen prenos podatkov
- je povezavni protokol: vzpostavitev/rušenje zveze
- ima kontrolo pretoka (angl. flow control): pošiljatelj ne preobremeni prejemnika
- ima kontrolo zamašitev (angl. congestion control): pošiljatelj ne preobremeni omrežja
- uporablja tekoče pošiljanje: velikost okna se avtomatsko določa glede na kontrolo pretoka in kontrolo zamašitve

TCP segment:



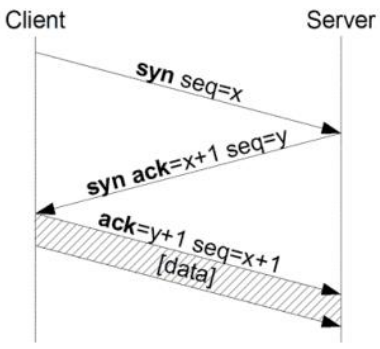
Številčenje segmentov in potrditev

- pošiljatelj in prejemnik najprej VZPOSTAVITA ZVEZO. Povezava je nato dvosmerna (vsak lahko pošilja drugemu podatke in potrditve)
- pošiljatelj lahko v enem segmentu istočasno pošlje nove podatke in potrditev (ACK) prejšnjega segmenta
- številke pomenijo:
  - SEQ (zaporedna številka): zap. številka prvega byte-a v segmentu
  - ACK (potrditev): zap. številka naslednjega pričakovanega byte-a

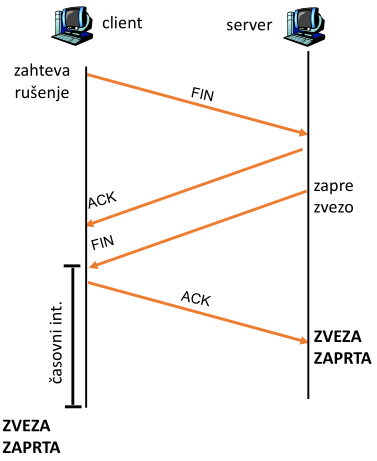


TCP: vzpostavljanje povezave

- pošiljatelj in prejemnik pred pošiljanjem izvedeta rokovanje (handshake), v katerem izmenjata parametre:
  - začetne pričakovane zaporedne številke (naključno določene)
  - velikosti medpomnilnikov (za kontrolo pretoka)
- trojno rokovanje (three-way handshake)
  - Odjemalec pošlje segment z zastavico SYN (sporoči začetno številko segmenta, ni podatkov)
  - Strežnik vrne segment SYN ACK (rezervira medpomnilnik, odgovori z začetno številko svojega segmenta)
  - Odjemalec vrne ACK, lahko že s podatki (potrjevanje "štuporamo")

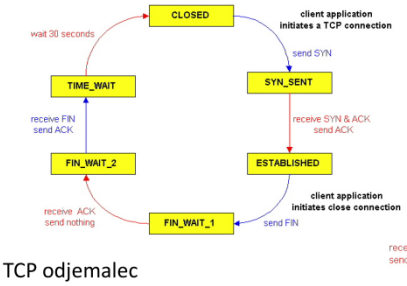


TCP: rušenje povezave



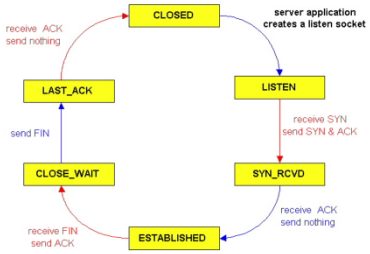
- odjemalec pošlje segment TCP FIN strežniku (zastavica!)
- strežnik potrdi z ACK, zapre povezavo, pošlje FIN
- odjemalec prejme strežnikov FIN, potrdi ga z ACK (počaka časovni interval, da po potrebi ponovno pošlje ACK, če se ta izgubi)
- strežnik sprejme ACK, končano

Življenjska cikla odjemalca in strežnika



TCP odjemalec

TCP strežnik



Varnost: napad SYN FLOOD

- Napadalec pošlje strežniku veliko število paketov (TCP SYN). Strežnik vsakič rezervira del svojega medpomnilnika
- Napadalec ne zaključi rokovanja z ACK., prostor na strežniku ostane zaseden do timeouta.

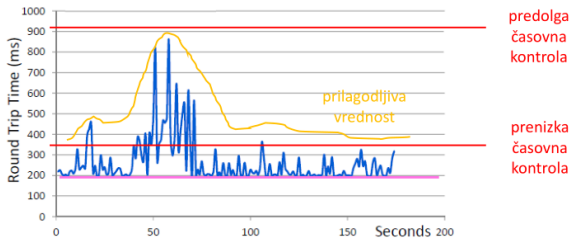
- Zaradi velikega števila odprtih povezav strežniku zmanjka prostora in ne more več sprejemati novih povezav - DoS (angl. denial of service)
- porazdeljeni DoS napad (DDoS): pošiljanje TCP SYN iz več virov

Nastavitev časovne kontrole v TCP

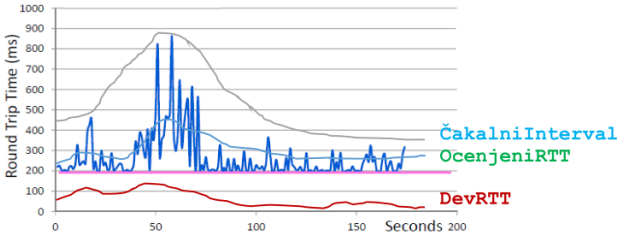
- štoparica (časovna kontrola): potrebna za zanesljivo dostavo - če se izgubi paket ali potrditev, sproži ponovno pošiljanje
- Kakšna je primerna dolžina čakalnega intervala?
  - daljši od časa vrnitve (RTT, Round Trip Time) = čas za pot paketa od pošiljatelja do prejemnika in potrditve nazaj
    - če je prekratek, imamo preveč ponovnih pošiljanj
    - če je predolg, prepočasi reagiramo na izgubljene segmente

Primer ocenjevanja RTT

- avtomatsko opravimo meritve RTT (round-trip time) od pošiljanja segmenta do prejema potrditve, da ocenimo smiselno velikost časovne kontrole
- izmerjen RTT je lahko nestabilen zaradi različnih poti in obremenjenosti usmerjevalnikov!
- potrebujemo "prilagodljivo vrednost" časovne kontrole



Primer ocenjevanja RTT in čakalnega int.



- izračunamo gibajoče povprečje
  `OcenjeniRTT[i] = (1-α)*OcenjeniRTT[i-1] + α*IzmerjeniRTT[i]`
  običajno uporabimo: α=0.125
- izračunamo gibajoči odmik (deviacijo)
  `DevRTT[i] = (1-β)*DevRTT[i-1] + β*|IzmerjeniRTT[i] - OcenjeniRTT[i]|`
  običajno uporabimo β=0.25
- vrednost čakalnega intervala TCP nastavi kot OcenjeniRTT + "rezerva":
  `ČakalniInterval[i] = OcenjeniRTT[i] + 4*DevRTT[i]`

Način potrjevanja

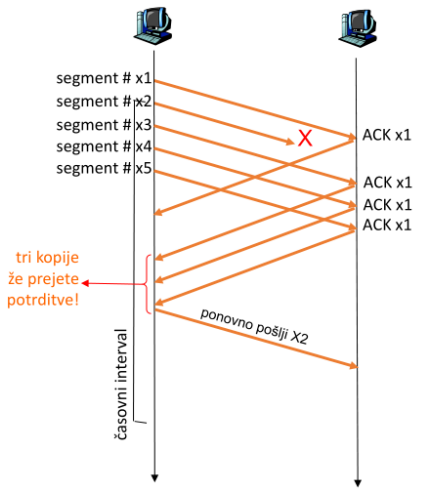
- Kakšne vrste ponavljanje uporablja TCP? Ali
  - •ponavljanje zaporedja (N nepotrjenih - go-back-N) ali
  - •potrjevanje posameznih (selective repeat)?
- ODGOVOR: kombinirano rešitev obeh
  - podoben ponavljanju N nepotrjenih (kjer je štoparica le za najstarejši nepotrjeni segment), vendar ob poteku časovne kontrole ne pošlje vseh segmentov v oknu, temveč le najstarejši nepotrjeni segment

Posebnosti pri potrjevanju

Dogodek pri prejemniku	Odziv prejemnika
Sprejem segmenta s pričakovano številko, vsi prejšnji že potrjeni.	Počakaj na nasl. segment še max 500ms. • Če pride, oddaj **zakasnjeno potrditev obeh** (delayed ACK). • Če ne pride, potrdi samo prejetega.
Isto kot zgoraj, a prejšnji segment še ni nepotrjen.	Takoj pošlji **kumulativno potrditev obeh**.
Sprejem segmenta s previsoko številko (**zaznamo vrzel**)	Takoj potrdi zadnji v zaporedju sprejeti segment (pošlji duplikat ACK).
Sprejem segmenta z najnižjo številko iz vrzeli (**polnjenje vrzeli**)	Takoj potrdi segment.

Hitro ponovno pošiljanje (fast retransmit)

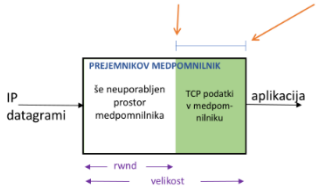
- običajno se izvede po preteku časovne kontrole
- včasih je časovni interval predolg in ga lahko v določenih situacijah skrajšamo
- hitro ponovno pošiljanje (fast retransmit) pošiljatelj izvede pred potekom časovnega intervala, če prejme za nek paket 3 podvojene potrditve



Kontrola pretoka TCP

- usklajevanje med pošiljateljem in prejemnikom:
  - pošiljatelj ne sme pošiljati hitreje, kot lahko prejemnik bere,
  - da ne povzroči prekoračitve medpomnilnika (prejemnikov prostor, kjer se začasno shranjujejo prejeti segmenti pred predajo aplikaciji)

```
rwnd = velikost - [LastByteRcvd - LastByteRead]
```



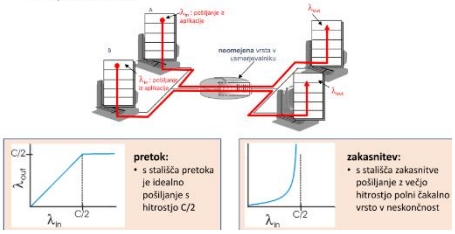
- razpoložljiv prostor medpomnilnika, sprejemno okno – receive window:
- prejemnik sporoča pošiljatelju velikost razpoložljivega prostora v glavi vsakega segmenta (rwnd)
- pošiljatelj ustrezno omeji število paketov, za katere še ni prejel potrditve

Nadzor zamašitev

- zamašitev: stanje preobremenjenosti omrežja, ko več virov naenkrat prehitro pošilja preveč podatkov za dano omrežje
- posledica zamašitve:
  - izguba segmentov (prekoračitve medpomnilnika v usmerjevalnikih)
  - velike zakasnitve (čakalne vrste v usmerjevalnikih)
- ni isto kot nadzor pretoka!

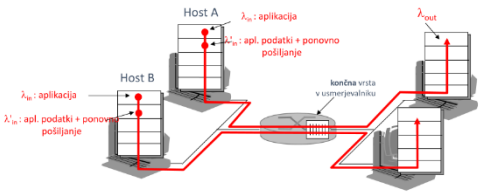
Zamašitev – primer 1

- dva pošiljatelja, neomejen pomnilnik v usmerjevalniku (za čakalno vrsto)
- C - kapaciteta kanala



Zamašitev – primer 2

- končna vrsta
- ponovna pošiljanja segmentov zaradi izgub (vrste) in zakasnitev

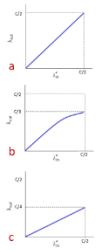


Zamašitev – primer 2

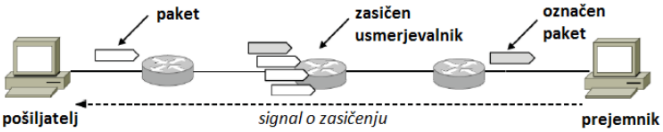
Preučimo tri scenarije:

a. segment oddamo le, ko je prostor v vrsti, tako da ni izgub (v praksi to ni možno, ker tega ne vemo)
b. dogajajo se izgube paketov in ponovna pošiljanja
c. ponovna pošiljanja tudi zaradi velikih zakasnitev

Torej: Več dela omrežja za manjši učinek. Nepotrebne ponovitve.

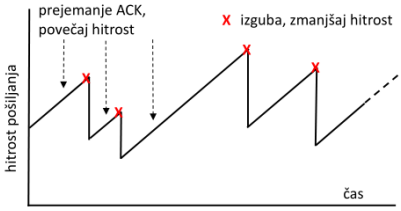


Kako nadzorovati zamašitve?



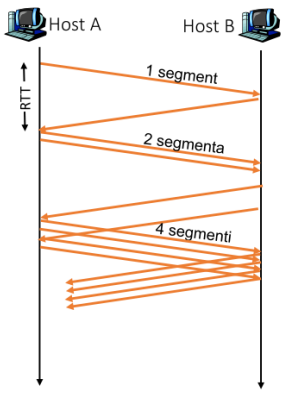
1. na podlagi končnih sistemov (end-to-end)- to tehniko uporablja TCP.
    a. bodisi prejemnik sporoči pošiljatelju, da so usmerjevalniki na poti sporočili zamašitev
    b. bodisi pošiljatelj opazuje čas do prejema potrditve
2. z uporabo omrežnih storitev: usmerjevalniki v omrežju obvestijo pošiljatelja, da je prišlo do zamašitve
    a. uporaba obvestila o zamašitvi (ECN – explicit congestion notification) v IP/TCP
    b. usmerjevalnik nastavi ustrezen bit in sporoči sprejemljivo hitrost oddajanja (npr. pri ATM)

TCP nadzor zamašitev



- rešitev: vsak pošiljatelj si sproti nastavlja hitrost na podlagi opazovanja reakcij v omrežju na pošiljanje:
    - če prejme potrditev (ACK), ni zamašitve, poveča hitrost
    - če se segment izgubi, je to posledica zamašitve, zmanjšaj hitrost
- okno rwnd (receive window) smo že spoznali (omejitev količine nepotrjenih podatkov za kontrolo pretoka)
- za nadzor zamašitev uporabljamo okno cwnd (congestion window). TCP torej pošilja s hitrostjo, ki ustreza min(rwnd, cwnd)
- možni dogodki:
    - POZITIVEN: prejem ACK: povečuj cwnd (eksponentno (slow start)/linearno)
    - NEGATIVEN: potek časovnega intervala (segment se izgubi): zmanjšaj cwnd na 1

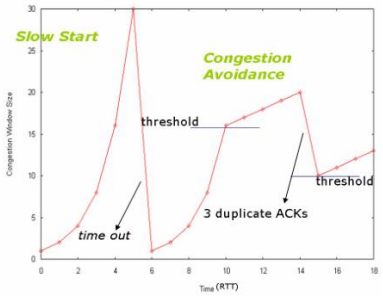
Počasen začetek (Slow Start)



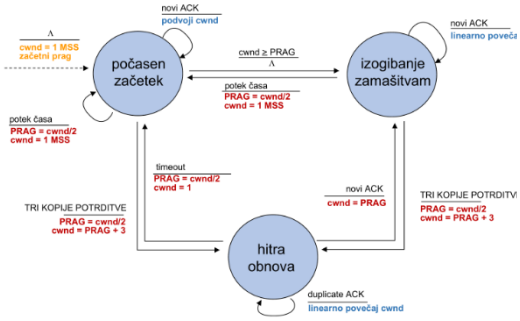
1. ob vzpostavitvi povezave: velja cwnd = 1 segment
2. hitrost povečuj eksponentno, tako da za vsak prejeti ACK: cwnd <- cwnd*2
3. ko pride do prve izgube, se ustavi in si zapomni PRAG (polovica trenutnega cwnd, ko pride do zamašitve) ter nastavi cwnd=1
4. izvajaj počasen začetek od koraka 1. Ko prideš do vrednosti PRAG, preidi v način izogibanja zamašitvam.

Izogibanje zamašitvam (Congestion Avoidance)

- kadar cwnd > PRAG, povečuj cwnd linearno za 1 MSS
- na ta način se bolj počasi približaj pragu zamašitve
- poznamo tudi način hitre obnove (fast recovery), v katero preideta počasen začetek in izogibanje zamašitvam ob prejemu 3 ponovljenih ACK (prepolovi cwnd + 3).

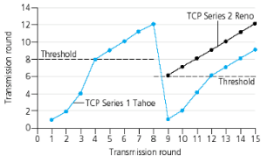


Končni avtomat za TCP nadzor zamašitev

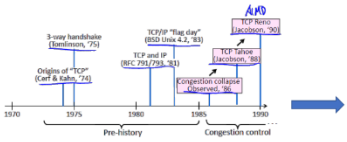


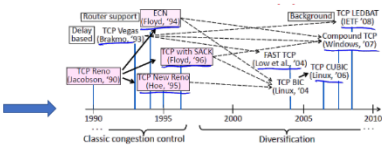
Razvoj nadzora zamašitev skozi različice TCP

1. **TCP Tahoe**: osnovna verzija (uporablja samo *počasen začetek* in *izogibanje zamašitvam*), po izgubi paketa vedno nastavi cwnd=1
2. **TCP Reno**: dodana faza *hitre obnove* - po prejemu treh kopij iste potrditve, preskoči počasen začetek in nastavi cwnd <- cwnd/2 + 3
3. **TCP Vegas**: dodano zaznavanje situacij, ki vodijo v zamašitve in linearno zmanjševanje hitrosti pošiljanja ob zamašitvah



Zgodovina razvoja TCP





Je TCP pravičen?

- cilj pravičnosti: Vsaka od N TCP sej po isti povezavi s kapaciteto C naj bi dobila delež prenosa C/N.
- izkaže se, da si več TCP pošiljateljev v praksi pravično deli pasovno širino (mehanizem nadzora zamašitev skonvergira v sredinsko točko grafa)

Pravičnost TCP in UDP

- UDP in TCP po istem omrežju: ni pravično do TCP
  - UDP pošilja brez omejitev pretoka in se pri tem ne ozira na TCP

Aplikacijska plast

Temeljna načela omrežnih aplikacij

- Teče na več končnih napravah (ni isto kot aplikacija, ki le uporablja omrežje)
- Več (različnih?) programov / procesov

Komunikacija med procesi

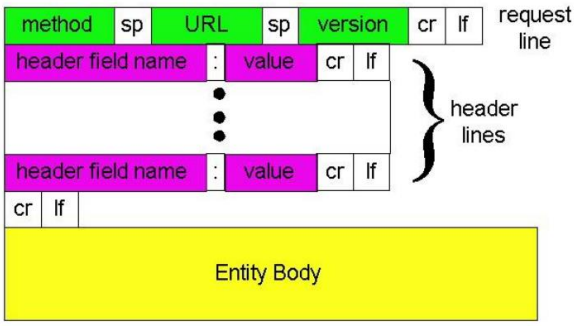
- Komunicirajo procesi, ne programi!
- Proces: program, ki teče na končnem sistemu (“živ“ primerek programa; skupek vseh virov, potrebnih za izvedbo programa).
- Izmenjava sporočil.
- Omrežna aplikacija: pari procesov, ki si izmenjujejo sporočila. Par = odjemalec + strežnik
- Odjemalec: proces, ki sproži komunikacijo.
- Strežnik: proces, ki čaka, da ga bo kdo kontaktiral.

Protokoli aplikacijske plasti

- Protokol določa pravila za izmenjavo sporočil.
  - Vrste sporočil (npr. zahteva, odgovor, potrditev...)
  - Zgradbo sporočila (polja, meje med polji...)
  - Pomen sporočila (kaj je v nekem polju)
  - Kdaj in kako proces oddaja sporočila in kako reagira na prejeta sporočila
- Javni (odprti) protokoli, npr. HTTP (RFC 2616)
- Lastniški (zaprti) protokoli, npr. Skype
- Protokol je le DEL aplikacije!
- Aplikacijski protokoli so navadno lepo berljivi uporabniku

Uporaba TCP in UDP za aplikacijske protokole

Aplikacija	Protokol	Transportni p.
E pošta	SMTP	TCP
Oddaljen dostop	telnet	TCP
Prenos datotek	ftp	TCP
Splet	http	TCP
Multimedija	http, rtp	TCP ali UDP
IP telefonija	SIP, RTP, lastniški	Pogosto UDP



Splet in http

- Je aplikacija (roj. 1990), ki omogoča Vsebine „kar hočeš, kadar hočeš“ – na zahtevo. Vsak lahko objavlja karkoli
- Delovanje:
  - Spletno stran sestavljajo objekti (html, jpg, applet, audio, flash...)
  - Vsak objekt ima svoj URL naslov (gostitelj+pot)
  - Odjemalec naslovi http zahtevo (request) na vrata 80 strežnika
  - Strežnik vrne http odgovor (response) z zahtevanim objektom.
- TCP poskrbi za potrditve, ponovitve, vrstni red.
- Protokol brez stanj (stateless)

http zahteva: metode:

- GET (zahteva objekta), POST (zahteva objekta + deli objekta imajo poslane vrednosti (html forms), HEAD, PUT, DELETE (brisanje s strežnika), TRACE, CONNECT, OPTIONS

http status kode:

- 1xx: informativne kode (100: Continue)
- 2xx: uspešno (200: OK)
- 3xx: preusmeritev (301: Moved Permanently- prestavljen dokument + vrne novi naslov Location : ...)
- 4xx: napake pri odjemalcu (400: Bad Request – sintaksa; 404: Not Found – ni dokumenta)
- 5xx: napake na strežniku (500: Internal Server Error; 505: HTTP Version Not Supported)

Piškotki

- Strežnik brez piškotkov ne loči zahtev različnih odjemalcev, nima zgodovine, nima spomina.

- Sestavni deli: Piškotkova vrstica v glavi zahteve, Piškotkova vrstica v glavi odgovora, Odjemalčeva datoteka piškotkov, Strežnikova zaledna podatkovna zbirka izdanih piškotov in povezanih odjemalcev

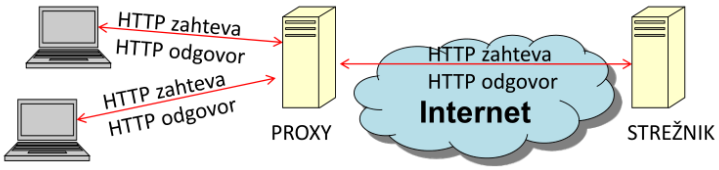
Scenarij uporabe piškotkov:

- Bogatejša uporabniška izkušnja (avtorizacija, košarica, stanje – spletna pošta, personalizacija)..., sporno glede zasebnosti.
- Nad plastjo HTTP (brez stanj) se tako ustvari sejna plast (s stanji).

Vrste piškotkov

- Session cookie – samo za čas trajanja seje (nima roka trajanja)
- Persistent cookie (tracking) – daljši rok trajanja , npr.1 leto
- http- only (ni dostopen skriptom) – manj nevarnosti za krajo
- 3rd party – od strani, katere naslov ni v naslovni vrstici (npr. oglaševalci)
- Zombie cookie – se spet pojavi, ko ga pobrišemo (obstaja rezervna kopija in nek skript poskrbi, da se po brisanju restavrira)
- Napadi: kraja piškotka in ugrabitev seje, zastrupljen piškotek in DoS

Posredniški strežnik



- Imenuje se tudi Web cache, proxy server (navadno pri ISP-ju)
- Pošilja sporočila namesto strežnikov in odjemalcev
- Ima svoje kopije spletnih strani (samo sveže).
- Ustrezno konfiguriran odjemalec!
- Če posrednik zahtevane strani nima pri sebi, jo zahteva od pravega strežnika.
- Zakaj posredniki? Manj prometa, hitrejši odgovor odjemalcu, ozka grla, manj izpostavljeni odjemalci (anonimnost). Pogojna zahteva -> metoda Conditional GET

FTP: sporočila

- RFC 959. Nadzorna povezava: 7-bitni ASCII
- Ukazi
  `USER ime; PASS geslo; LIST`
  `RETR ime_dat` (retrieve = get)
  `STOR ime_dat` (store = put)
- (Nekateri) odgovori strežnika
  331 Username OK, password required
  125 Data connection open, transfer starting
  452 Error writing file
  425 Can't open data connection

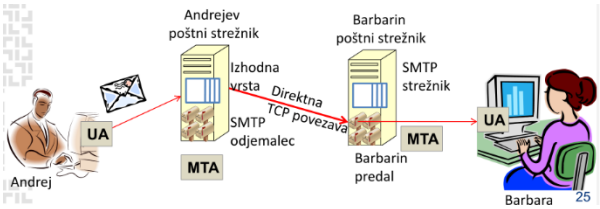
Prenos datotek – protokol FTP

- Prijava na oddaljeni računalnik + prenos datotek z oddaljenega računalnika k uporabniku in obratno.
- 2 ločeni TCP povezavi na FTP strežnik:
  - Nadzor (vrata 21) na zahtevo odjemalca (trajna): uporabniško ime, geslo, CD ukazi, ukazi za prenos datotek
  - Prenos podatkov – datotek (vrata 20) na zahtevo strežnika (minljiva – za vsako datoteko nova!) – to je aktivni način
- Protokol s stanji: strežnik ve, kdo je odjemalec, kateri imenik pregleduje...
- Potreben je odjemalski program (UA)!

- Pasivni način: odjemalec ne more sprejeti povezave od strežnika, zato tudi podatkovno vzpostavi sam

Protokoli elektronske pošte: SMTP, POP3, IMAP

- Osnovni elementi sistema: poštni strežniki (poštni predali, izhodna vrsta sporočil), Odjemalski programi (UA): tekstovni, grafični, Protokol za prenos sporočil (SMTP).
- Pošiljatelj – pošiljateljev UA – pošiljateljev strežnik –prejemnikov strežnik – prejemnikov UA – prejemnik.



SMTP

- Strežnik posluša na TCP vratih 25
- 7-bitni ASCII (tudi za telo sporočila)
- Binarne priponke je potrebno prekodirati v ASCII. In na prejemni strani nazaj v binarno.
- Odjemalec: SMTP strežnik, ki pošilja sporočilo
- Strežnik: SMTP strežnik, ki sprejema sporočilo
- Povezava na vrata 25
- Aplikacijsko rokovanje (Medsebojna predstavitev, Odjemalec: e-mail naslov pošiljatelja in prejemnika)
- Prenos sporočila (lahko več po isti povezavi)
- Rušenje TCP povezave
- Prejemni strežnik: V glavo doda vrstico Received, lahko je več teh vrstic

MIME razširitve sporočila

- Multipurpose Internet Mail Extensions
- ČŠŽÁÃÇÊËΩξ, večpredstavna sporočila
- Nova polja glave -> MIME-Version:, Content-Transfer-Encoding:

Primerjava SMTP in HTTP

Podobnosti
- Prenos datotek
- Trajne (persistent) povezave (HTTP: možne)

Razlike
- HTTP: pull (potegnem vsebino s strežnika)
  SMTP: push (oddajni strežnik pošto porine prejemnemu)
- SMTP: 7-bitno ASCII kodiranje, HTTP ne
- HTTP: vsak objekt enkapsulira v svoj HTTP odgovor, SMTP: vse objekte maila zavije v eno sporočilo

Kodiranje (Encoding)

- Quoted-printable
- Base 64 (abeceda iz 64 znakov)
- Binary
- Primer: jpg priponka (decode, jpeg dekompresija)

Dostop do poštnega predala

- Včasih: oddaljen dostop do strežnika (telnet), nato neposredno branje iz poštnega predala…
- Danes: dohodna pošta (POP3, IMAP, http dostop) -> PULL (prenos pošte k sebi) ter Pošiljanje odhodne pošte na strežnik: SMTP -> PUSH

POP3

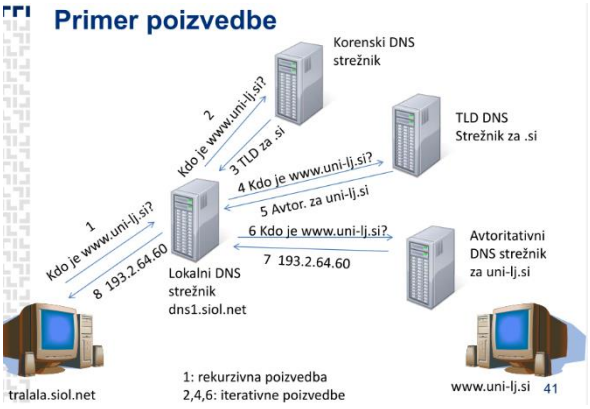
- Preprost, omejena funkcionalnost
- UA odpre TCP povezavo na vrata 110
- 3 faze: Avtorizacija -> Transakcija (prenos sporočil, oznake za brisanje, statistika) -> posodabljanje (odjemalec : QUIT, strežnik izvede brisanje)
- Slabosti: lokalno urejanje pošte, dostop z več računalnikov.

IMAP in http

- IMAP
  - Kompleksen, zahtevnejši, več funkcionalnosti
  - Uporabnik lahko določi mape na strežniku
  - Vsako sporočilo je v mapi
  - UA lahko prenese tudi le dele sporočil
  - Večja obremenitev strežnika
- HTTP dostop do pošte
  - Brskalnik, dostop od koderkoli, brezplačni ponudniki
  - Mape kot pri IMAP
  - Dostop do map in sporočil omogočajo skripte na http strežniku, te npr. prek IMAP komunicirajo s poštnim strežnikom.

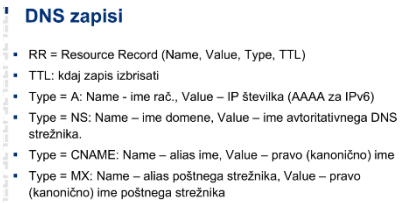
DNS

- IP številka ali znano ime (www.google.com)?
- Bistvena omrežna funkcionanost, ne direktno za uporabnika.
- DNS vključuje: Porazdeljeno podatkovno zbirko in Protokol za poizvedovanje po njej
- Storitve: Preslikava med imeni in IP številkami, Aliasi (več imen za isto IP številko) hostov in poštnih strežnikov ter Porazdeljevanje bremena (več IP številk za isto ime)



Organizacija

- 13 korenskih strežnikov (A-M), vsak je replicirana gruča
- Posamezni TLD (Top-Level Domain) strežniki -> com, org, net, edu, biz, info, si ,fr, it, de
- Avtoritativni strežniki: Organizacija z javno dostopnimi računalniki (UL: uni-lj)
- Lokalni strežniki: posredniki do DNS hierarhije



DNS caching

- DNS strežnik si zapomni prejete odgovore (za določen čas, npr. 2 dni)
- Njegov odgovor ne bo avtoritativen
- Manj poizvedb, hitrejši odziv
- Zapomni si lahko tudi naslove TLD strežnikov (razbremeni korenskega)

DNS sporočila

- Poizvedba in odgovor. Format je enak.
- Glava 12 bytov, več polj
  - ID sporočila 16 bitov
  - Zastavice (zahteva ali odgovor, želim rekurzijo, možna rekurzija, avtoritativni odgovor…)
  - Število vprašanj, število odgovorov (RR-jev), št. avtoritativnih in št. dodatnih RR
- Poizvedba (ali več) (ime, tip, npr. A/MX)
- Odgovor(i) (RR zapisi za ime)
- Avtoritete (RR zapisi drugih avt. strežnikov)
- Dodatni podatki (RR)

- Nslookup – za vpogled v bazo sistema

Kako raste DNS zbirka podatkov?

- Registracija domene lrk.si in dodelitev ranga IP številk
- Določitev primarnega in sekundarnega (backup) avtoritativnega DNS strežnika
- Registrar: vnos NS in A zapisov zanju v TLD DNS strežnik:
  - `lrk.si, dns1.lrk.si, NS`
  - `dns1.lrk.si, 123.123.122.5, A`
- Vnos A zapisa za spletni strežnik, MX zapisa za poštni strežnik domene v avt. DNS strežnik
  - Statično (ročni vnos)
  - Dinamično (z DNS sporočili – RFC 2136)

Storitev aplikacijske plasti je še več...

- Standardne: oddaljen dostop, novice, imenik
- Nestandardne: iskanje, P2P izmenjava datotek
- Podporne (sejna + predstavitvena plast po OSI): stiskanje (jpeg), predstavitev podatkov (ASCII), kriptiranje

Nestandardne storitve: P2P

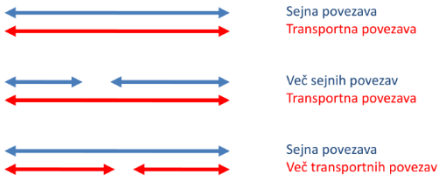
- Dinamično omrežje, nestalni člani
- Ponovni priklop z drugim IP
- Izmenjava podatkov med poljubnima končnima sistemoma
- Osrednji strežnik (Napster)
- Popolna enakost (osnovna Gnutella, Kazaa) – Poplavljanje poizvedb ali omejeno poplavljanje
- Popolna enakost + super vozlišča (eMule, eDonkey) – Prioritete uporabnikov, paralelno pretakanje, vrste zahtev
- Podobno: BitTorrent: iskanje je tu ločeno od prenašanja

Podporne storitve sejne plasti

- Vsebina: logično povezovanje apl. procesov
- TCP model: logično povezovanje opredeli programer
- OSI model: predlog standardnih funkcij
- Sejne storitve: So na voljo aplikacijski plasti: SSPT nudi dostop do funkcij logičnega povezovanja, nadzora,...

Sejna in transportna povezava

- Možni odnosi:



- Multipleksiranje se izvaja na nižjih plasteh.

OSI: struktura seje

- Sejna povezava
  - Seja: ena ali več aktivnosti (ena naenkrat)
    - Aktivnost: en ali več dialogov (en naenkrat)
  - Aktivnost lahko zajema več kot eno sejo
    - Prekinitev, zamrznitev, bujenje, ponovitev
- Žetoni pomagajo strukturirati sejno povezavo
  - Podatkovni (pošiljanje)
  - Rušilni (sproščanje povezave)
  - Sinhronizacijski
    - Glavne sinhronizacijske točke (potrditev, čakanje)
    - Pomožne (ni potrditve – nepovezana storitev)

OSI: funkcije sejne plasti

Različni nivoji kakovosti sejne storitve! Funkcionalni sklopi:

1. Jedro: osnovna povezana storitev, dvosmerni kanal
2. Usklajeno sproščanje logičnega kanala
3. Izmenično dvosmerni kanal
4. Sinhronizacija med sejo
5. Nadzor in upravljanje aktivnosti
6. Sporočanje o neregularnostih

OSI nivoji kakovosti sejnih protokolov:
1, 1+3, 1+4, 1+5+6, 1-6 (full)