

KOMUNIKACIJSKE MREŽE

SEVTIĆ DRAGAN

SLIVAR IVAN

JAKOVAC JAKOV

Informacije o kolegiju

- Email: km@fer.hr
- IMUNES - modeliranje, simuliranje ;
ispitivanje mreža
- Bodovanje:
 - Sudjelovanje u nastavi 10b
→ na predavanjima, labosima, domaćim zadacima...
 - Domaće zadatce $2 \times 5b = 10b$
 - Labosi $3 \times 5b = 15b$
 - MI 30b (1. ciklus)
 - ZI 35b (svejali većinom 2. ciklus)
 - Ispitni rok 65b
- Uvjeti:
 - ukupno $\geq 50b$
 - položeni Labosi

Uvod u komunikacijske mreže

Komunikacijska mreža

- medusobno povezani komunikacijski sustavi na koje se spaja korisnička oprema
- najčešće se prikazuje grafom

Vrste mreža

Klasifikacijski kriteriji:

- Raspšrostranjenost (kašnjenja)
- Namjena (javnna/privatna)
- Vrste informacija (govor, podatak, slika)
- Nacin komuniciranja (kanal, paket)
- Topologija (povezanost čvorova)
- Pokretljivost korisnika (da/ne)

Raspšrostranjenost

- mreža širokog područja (WAN)
- metropolitanska ili gradskna mreža (MAN)
- lokalna mreža (LAN)
- itd.

Nacin komuniciranja:

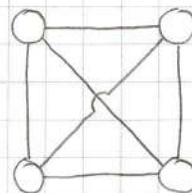
- komunikacijski kanal
 - prednost: kontinuiran signal
 - nedostatak: stalno zauzeće kanala
- informacijski paket
 - sadrži zaglavljicu s informacijom o primatelju
 - prednost: privremeno zauzeće
 - nedostatak: kašnjenje i promjena redoslijeda
 - Datagram (internet)
 - svaki paket usmjerava se neovisno kroz mrežu

Virtualni kanal

- svaki paket ide istim putem (nema promjene redoslijeda, samo promjena kašnjenja)

Topologija

- potpuna povezanost (fully connected)
 - izravna povezanost svaka dva čvora u mreži
 - otpornost na kvarove (mogućnost alternativnog puta)
 - primjenjujući eni broj čvorova
 - veliki troškovi povezivanja

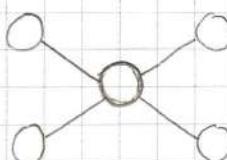


zvijezda (star)

- ispredom središnjeg čvora omogućuje se komunikacija

- primjena: lokalna mreža, priključak korisniku

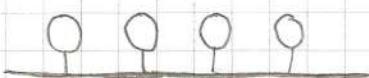
mreža



sabirница

- svi čvorovi priključeni na zajednički prijenosni medij

- prekid onemogućuje komunikaciju



prsten

- sabirница zatvorena u krug

→ primjena: mreže velikog kapaciteta (optičke)



• Osnovni referentni modeli:

- OSI

- TCP/IP (internet)

• Komunikacijski protokol

- skup pravila za postupak razmjene informacija mreži

- omogućuje usklađenost prednjeg i prijamnog entiteta

- zaštita od pogrešaka

→ npr. definirano što se događa ako podatak ne stigne u nekom vremenskom intervalu

- stablo

→ hijerarhijska struktura

→ primjena: međunarodna → nacionalna →

regionalna → lokalna povezanost



- neregularne topologije

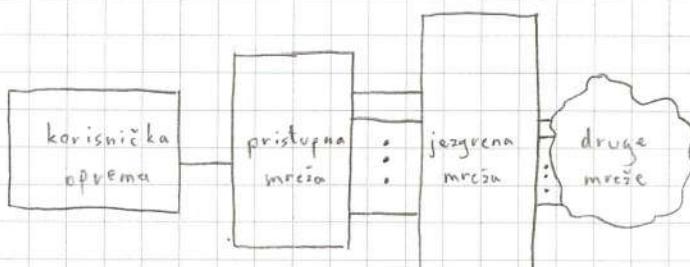
→ nepotpuna povezanost

→ međusobno povezane regularne topologije

• Dijelovi mreže:

- pristupna mreža (access network)

- jezgrna mreža (core network)



Slojirana mrežna arhitektura

- svakom sloju dodjeljuju se funkcije i specificiraju svećelja sa susjednim slajevima kako bi viši sloj moguo koristiti usluge nižeg sloja

• Najviši sloj je uvijek aplikacijski (interakcija sa korisnicima)

• Najniži sloj je fizički

• Osnovni referentni modeli:

- OSI

- TCP/IP (internet)

• Komunikacijski protokol

- skup pravila za postupak razmjene informacija mreži

- omogućuje usklađenost prednjeg i prijamnog entiteta

- zaštita od pogrešaka

→ npr. definirano što se događa ako podatak ne stigne u nekom vremenskom intervalu

• Spojna usluga

- podaci se preko veze isporučuju u redoslijedu

- npr. virtuelni kanal

• Nespojna usluga

- svaki podatak se razmjenjuje neovisno o ostalim

- npr. datagram

- zaključak: brz, ali nepouzdana usluga

• Funkcije sloja:

1.) Identifikacija posiljatelja i primatelja

2.) Određivanje smjera podataka

- Dodatno:

3.) Otkrivanje i ispravljanje pogrešaka

4.) Upravljanje tokom podataka

• Referenti model OSI

1.) Fizički sloj

→ Zadatak:

- prijenos sljedn bita

- sučelje s prijenosnim medijem

-> žični (wired)

-> optički (fibre optics)

-> bežični (wireless)

-> prikaz (sintaksa) i značenje informacija koja se prikazuje

7.) Aplikacijski sloj

-> aplikacije i usluge za korisnike

-> sadrži skup protokola za korisničke usluge i aplikacije

* Referenti model TCP/IP

1.) Nedefinirana kombinacija fizičkog sloja i sloja podatkovne poveznice

2.) Mrežni/internetski sloj

-> Internet protocol (IP)

-> međusobno povezivanje mreža i podmreža

-> mreža s komunikacijom paketa (datagram)

-> IP over X (IP_X)

-> Y over IP (y₀IP)

3.) Transportni sloj

-> Protokoli:

- Transmission Control Protocol (TCP)

-> prijenos bez grešaka i bez promjene redoslijeda

- User Datagram Protocol (UDP)

-> prijenos uz najmanje kašnjenje

4.) Aplikacijski sloj

-> Protokoli:

- korisnički (SMTP, HTTP...)

- Sustavski (DNS...)

Aplikacijski sloj

Prezentacijski sloj

Sjednički sloj

Transportni sloj

Mrežni sloj

Sloj podatkovne poveznice

Fizički sloj

Aplikacijski sloj

Prezentacijski sloj

Sjednički sloj

Transportni sloj

Mrežni sloj

Nedeterminans

OSI

TCP/IP

2.) Sloj podatkovne poveznice

-> komunikacija između dva izravno povezana čvora

čvora

-> zadaci:

- upravljanje pogreškama

- upravljanje tokom

3.) Mrežni sloj

-> komunikacija između dva krajnjih čvora

-> zadaci:

- usmjeravanje podataka

- međusobno povezivanje mreža i podmreža

- upravljanje pogreškama

- upravljanje tokom

4.) Transportni sloj

-> prijenos podataka (end-to-end)

-> zadaci:

- prijenos bez pogrešaka (semantička transparentnost)

- minimizacija kašnjenja (vremenska transparentnost)

5.) Sjednički sloj

-> usklajivanje sustava koji komuniciraju

-> zadaci:

- uspostavljanje, održavanje i prekid

dijaloga

6.) Prezentacijski sloj

Kvaliteta usluge i performanse

- Kvaliteta usluge (Quality of Service) jest zajednički
vršnik performansi usluge koji određuje zadovoljstvo
korisnika

Mrežne performanse:

- Sirina pojasa (bandwidth)

→ najviša frekvencija koja se može prenijeti

→ max. broj bitova u jedinici vremena (bitrate)

- Propusnost (throughput)

→ broj korisnih bitova u jedinici vremena

→ manja od max. kapaciteta kanala

- Kašnjenje (delay, latency)

→ vrijeme potrebno da bit stigne s izvora na
odredišće

→ uključuje vrijeme potrebno za:

- odašiljanje na izvoru

- propagaciju kroz medij

- prijam na odredištu

- dodatno:

→ obradu na svakom čvoru

→ čekanje za obradu

Normalizacija

- ISO, ITU, IETF, IEEE

Fizički sloj i sloj podatkovne poveznice

Fizički sloj - Prijenosni medij

Parica (pair) 

- dva bakrena vodiča (d. 1 mm) upredeni kako bi se smanjio međusobni EM utjecaj

- Tipovi:

→ upredena parica (twisted pair)

→ neoklopljena upredena parica (unshielded twisted pair - UTP)

→ oklopljena upredena parica (shielded twisted pair - STP)

- vrlo rasprostranjena (npr. CAT 5)

- digitalni i analogni prijenos

- Brzina ovisi o:

→ debjini

→ duljini

→ načinu upredanja

→ načinu slaganja parica u kabel

Koaksijalni kabel (coax)

- dobra zaštita od smetnji

Optičko vlakno

- indeks loma ovajnici manji od indeksa loma

vlakno kako bi se svjetlost reflektirala

u vlaknu

- Nobelova nagrada iz fizike 2009. Charles Kuen

- Tipovi:

→ jednomodno vlakno (single-mode)

- tanja vlakna ($8\text{-}10.5\ \mu\text{m}$)

- složenija i skuplja oprema

- brzina (npr. 50Gb/s) ; udaljenost (npr. 100km)

→ višemodno vlakno

- deblica vlakna ($60\text{-}100\ \mu\text{m}$)

- jednostavnija ; jeftinija oprema

- manja brzina (npr. 1Gb/s) ; manja udaljenost (npr. 500m)

Prednosti:

- brzina (u mediju jednaka bakru)

- neosjetljivost na EM utjecaj i koroziju

- prisluškivanje teško izvedivo

Nepovoljnosti:

- jednosmjerni prijenos

- složenija i skuplja oprema

• radijski prijenos

Primjene:

→ pristup korisnika javnoj pokretnoj mreži

→ pristup korisniku lokalnoj mreži

→ povezivanje dvaju točaka

- Spektar ograničen

→ dio uz naplatu (npr. GSM, LTE) cca 750-1750 MHz

→ dio slobodan (npr. bežični telefon) cca 1750-2600 MHz

- Višestruka uporaba - multipleksiranje

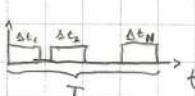
- Podjela prema vremenu (Time Division Multiplexing - TDM)

→ svakom paru izvor - adresište dodjeljuje se

filejni vremenski odsječak unutar okvira trajnim T

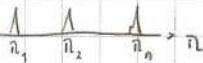
→ odsječci se ciklički izmjenjuju unutar ponavljajućeg

okvira T



- Podjela prema valnoj duljini (Wavelength -Division -WD) (Wavelength Division Multiplexing - WDM)

-> svakom paru izvor-odredište dodjeljuje se

druga valna duljina π 

-> upravljačka informacija

- Podjela prema frekvenciji

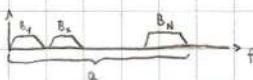
- zaglavljic (header)

-> svakom paru izvor-odredište dodjeljuje se

- završetak (trailer)

drugi dio odabranne komponente informacijskog

-> podaci (payload)

volumena 

- u slučaju podatku manjem od okvira, dodaje se filler ili padding do ispunе

- Pulsna kodna modulacija (PCM)

- početak i kraj okvira se označava zastavicom (flag)

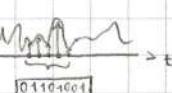
-> digitalizacija analognog signala

-> npr. 01111

bit stuffing

-> uzorkovanje svakih $125 \mu s$ ($2B = 8 kHz$)

• Fragmentiranje

- 64 kbit/s 

• Usluga mrežnom sloju

-> 32 kanala $32 \times 64 = 2.048 \text{ Mbit/s}$

- Nespojna usluga bez potvrde

- 30 govornih

-> za real-time veze (govor) i veze s malom mogućnostij pогрешака

- 1 sinkronizacijski

- Nespojna usluga s potvrdom

- 1 signalizacijski

-> za veze sa smetnjama

-> Sinkrona digitalna hijerarhija (SDH)

-> ponovno slanje okvira u slučaju ne-primitka

- mogućnost multiplexiranja - reč brzina

- Spojna usluga s potvrdom

Sloj podatkovne poveznice

-> za veze gdje je važna visoka pouzdanost i redoslijed (rijetko)

- Oblikovanje:

• Upravljanje pogreškama

- Definiranje jedinice podataka (okvir)

- Zaštitno kodiranje

- Fragmentiranje ("rezanje" prevelikih okvira na manje)

- predajnik kodira

- Definiranje usluge mrežnom sloju (spojna/nespojna, sa/bez potvrde)

- prijamnik dekodira i otkriva pogreške

- Upravljanje pogreškama (otkrivanje, ispravljanje)

-> Backward Error Correction (BEC)

- Upravljanje tokom (izvor ne smije slati više podataka nego što odredište može primiti)

- u slučaju otkrivene pogreške prijamnik traži od predajnika ponovo slanje (ispravljanje)

- Okvir

-> Forward Error Correction (FEC)

- Sadržaj:

- prijamnik otkriva i ispravlja pogrešku

- primjena: velika udaljenost (npr. Zemlja-Mars)

- Tipovi pogrešaka:

-> oštećeni okvir (damaged frame)

-> sa smetnjama

-> izgubljen okvir (lost frame)

- šalje se povratna potvrda (ponovno slanje)

- ograničenje vremena (Retransmission TimeOut)

v slučaju nedobivanja potvrde

- vremenska kontrola za ponovno slanje

- numeracija okvira

-> numeracija okvira (sequencing)

- tzw. Automatic Repeat reQuest (ARQ) ili
Positive Acknowledgment with Retransmission

Upravljanje tokom (flow control)

(PAR)

- osnovni mehanizam - povratna veza (prijamnik daje

-> Dvosmjerni protokol

predajniku dopuštenje za odašiljanje podataka)

-> podaci se prenose od sustava A do B, ali i od

B do A

Komunikacijski protokoli

-> sa smetnjama

- Prijenos:

-> oba sustava uz podatke šalju i potvrde

-> znakova (oktet)/byte)

-> umjesta zasebnih okvira, šalje se jedan

-> bilo kakve kombinacije bitova

koji sadrži i podatak i potvrdu

-> Jednosmjerni protokol

-> rade po načelu "stani i čekaj"

-> podatkovni okviri prenose se od sustava A do
sustava B

-> u potvrdama se koristi alternirajući bit

-> Bez ograničenja (laka utopijski protokol)

Zadaci

- predajnik i prijemnik uvijek spremni

21.) Treba prenesti 9910 okteta od mesta A do B

- prijenos bez pogrešaka

udaljenih 600 km. Max kapacitet kanala jest

- obrada beskonačno brza

2118 okteta od kojih je 2100 okteta veličina

- spremnici beskonačni

polfra podataka. Propusnost iznos: $C = 8 \cdot 10^6$ bit/s, a

-> "stani i čekaj"

brzina propagacije $d = 2 \cdot 10^8$ m/s.

- dvosmjerna komunikacija, ali jednosmjerni tok

Koliko traje prijenos od A do B?

podataka od A do B

+ okvira duljine $2100 + 4 \text{ PCI} = 8472$ okteta

- nakon slanja predajnik čeka potvrdu

1 okvir duljine $1510 + 1 \text{ PCI} = 1528$ okteta

(upravljački okvir) od prijemnika

ukupno 10 000 okteta = 80 000 bitova

PCI	podaci
-----	--------

 podatkovni okvir A → B

$C = 8 \cdot 10^6$ bit/s

PCI	upravljački okvir B → A
-----	-------------------------

$\frac{N}{C} = 3 \cdot 10^{-3}$ s.

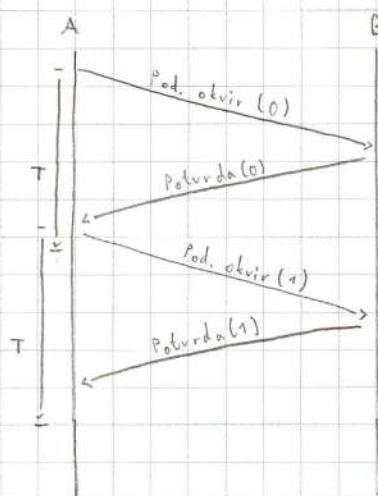
vrijeme = kašmijenje + $3 \cdot 10^{-3}$ = 0.013s

21) Načrtajte vremenski dijagram za protokol "Stanje čekaj" s označenim vremenima obrade u predajniku i prijamniku, prijenosa okvira i propagacijskim kašnjenjem.

;

predajniku i prijamniku, prijenosa okvira:

propagacijskim kašnjenjem

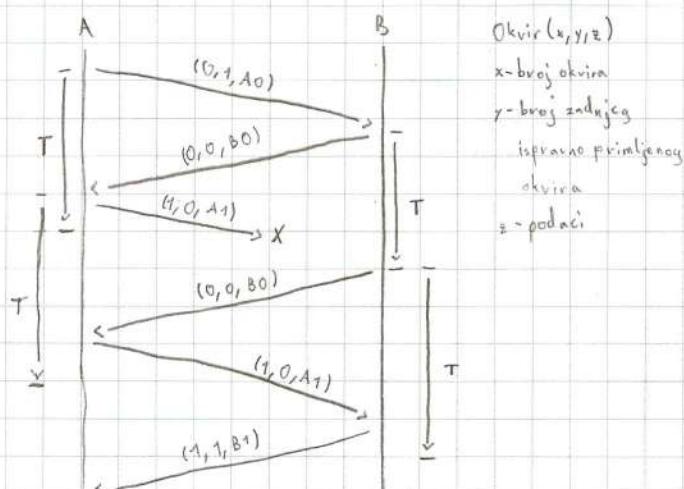


22) Primjenjuje se dvostruki protokol s alterniranjem

bitom, kao u ranijem primjeru. Okvir $(1, 0, A^1)$

primljen je oštećen. Načrtajte i objasnite

slijedni dijagram.

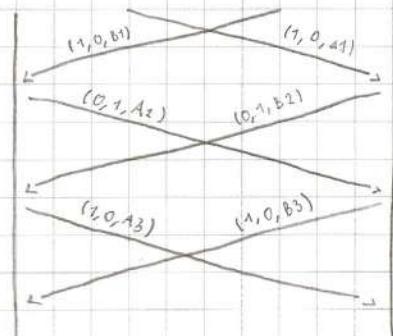
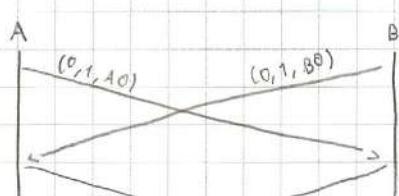


23) Primjenjuje se dvostruki protokol s alterniranjem

bitom, kao u prethodnom primjeru. A i B

započinju slanje okvira $(0, 1, A0)$ i $(0, 1, B0)$

istodobno. Načrtajte i objasnite slijedni dijagram.



Lokalna mreža

- Cilj: ostvariti povezivanje ograničenog broja stanica (krajnjih sustava/kredita) unutar zgrada/susjednih zgrada uz dobre uvjete komuniciranja (mala kašnjenja, mala vjerojatnost greške).

• Podjela sloja podatkovne poveznice:

- podstoj upravljanja pristupnom mediju (MAC)

- specifično rješenje za svaku vrstu lokalnih mreža

- dodjela medija stanici (na zahtjev)

- pristupni protokoli (pravila)

- upravljanje pristupnom mediju:

- centralizirano/distribuirano

- pristup mediju:

- multiplexiranje (TDMA)/proizvoda/slučajni pristup (ALOHA, CSMA/CD)

-> ALOHA

- stanica šalje podatke kad ih ima (slučajno)

- u slučaju istodobnog slanja i sudara, okviri se uništiti (čest. sudari)

-> ponovno slanje dok se ne dobije potvrda

-> CSMA/CD

- osluškivanje zauzeća kanala

- otkrivavanje sudara (ponovno slanje)

- Podložjje upravljanja logičkom poraznicom (LLC)

→ vezujuća podatkovna ćelija u susjednih stanica

→ univerzalno rješenje za sve lokalne mreže

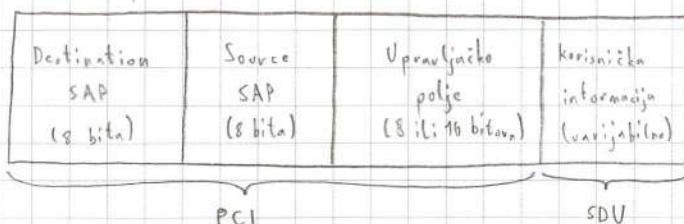
→ Usluge:

- nespojna bez potvrde (veličina LAN-ova)

- nespojna sa potvrdom (iznimke)

- spojna (rijetko)

→ struktura podatka PDU LLC



→ Ethernet

Preamble	MAC adresa odredišta	MAC adresa izvorišta	Tip	Podaci (LLC)	FCS
(8 bytes)	(6 bytes)	(6 bytes)	(2 bytes)	(46-1500 bytes)	(4 bytes)

→ IEEE 802.3

Preamble	SFD	MAC adresa odredišta	MAC adresa izvorišta	Duljina podataka	Podaci (LLC)	FCS
(7B)	(1B)	(6B)	(6B)	(2B)	(46-1500B)	(4B)

→ MAC adresa odredišta

- 47. bit 0 (adresa pojedine stanice) ili 1

[adresa skupine stanica]

- 46. bit 0 (sklopovski unos) ili 1 (mrežni administrator)

→ Otkrivanje sudara

→ minimalna vrijeme potrebno za sigurno otkrivanje

sudara iznosi 2x trajanje prijenosa (d) + kašnjenje

→ nakon sudara ponovno slanje (vrijeme između slanja nasumično ili eksponentijalno raste)

• Bežični LAN: IEEE 802.11

- koristi CSMA/CA sa sprječavanjem sudara

- stanica prije slanja čeka nasumično "backoff"

vrijeme (koje se udvostručuje nakon svakog sudara)

- problem: teško detektirati sudar

Normiranje lokalnih mreža

→ 1XXBYYYZ

→ 1XX označava brzinu prijenosa podataka

- npr. 1 Mbit/s, 100 Mbit/s...

→ BYYY označava način prijenosa

- npr. BASE (osnovni pojas), BROAD (širokopojasni prijenos)

→ Z označava max duljinu segmenta na 100 m ili

korišteni medij

- npr. 5, 2, 36

- npr. T (twisted pair), F (fiber), L (long R fiber)

S (short R fiber)

Ethernet i IEEE 802.3

- Ethernet definira DIX (Digital, Intel, Xerox)

→ Norme: Ethernet I, (1980.) ; Ethernet II, (1982.)

- IEEE nastavio red DIX-a

→ naziv Ethernet se zadružio

- struktura okvira:

Mrežni sloj

- omogućava komunikaciju između dva kraja

čvorova

Usluge mrežnog sloja

- spojna i nespojna (internet)

Izvedba usmjerenosti	DATAGRAM	VIRTUALNI KANAL
Značajka		
Vspomnena veza	Ne treba	Treba
Adresiranje	Svaki paket sadrži potpunu adresnu informaciju oznaku virt. (izvora i odredišta)	Svaki paket sadrži kratku oznaku virt. kanala
Informacija o uspostavljenim vezama	Ne pohranjuje se	Svaki virt. kanal je jedan unos u tablici usmjeravanja
Usmjeravanje	Neovisno (random)	Svi paketi idu istim putem
Utjecaj kvara	Gubitak samo paketa	Pretid svih virt. trenutno u obradi
Upravljanje zagrijenjem	Složeno	Jednostavno, ako se unaprijed dodijele resursi

Komutacija paketa i usmjeravanje

- Usmjeravanje (routing) - određivanje puta od izvora do odredišta

- algoritmi usmjeravanja

- prikazuju se grafoom

- Prosljedjivanje (forwarding) - odlučivanje kome paket ide dalje (unutar čvora)

Algoritmi usmjeravanja

1) Neadaptivni (statički)

- 1.1) unaprijed izračunati: putevi za svaki čvor

2.2) Dijkstra

- 1.3) Preplavljivanje (svaki paket se šalje svima, duplikati se odbacuju)

2) Adaptivni (dinamički)

-> donose odluke na temelju trenutnog stanja u mreži

(npr. opterećenje)

-> Pitanja:

- što pratiti (kriterij)?

- koga pratiti (koje čvorove)?

- kada reagirati (na koji podrazaj)?

-> Usmjeravanje prema vektoru udaljenosti

- svaki vremjelj sadrži tablicu (vektor) koji daje najbližu "poznatu udaljenost" za svaku adresu i prijelaz

u njemu

- algoritam konvergira prema pravom stanju, ali sp

- brzo reagira na "dobre vijesti" (iskrcanje puta)

- sporo reagira na "loše vijesti" (produljenje puta)

-> Usmjeravanje stanjem poveznice

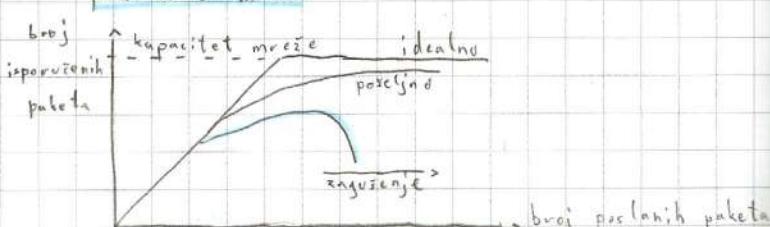
- algoritam periodično mjeri kašnjenje i onda

koristeći Dijkstre izračunava optimalan put

-> povećana složenost (komunikacija čvorova i pretopologije)

Nacela upravljanja zagrijenjem

- degradacija performansi mreže zbog prevelikog broja paketa u mreži



broj poslanih paketa

Upravljanje zagrušenja

- Teorija upravljanja (Control Theory):

1) Rješenja s otvorenom petljom

- cilj: izbjegći zagrušenje
- ograničeni prihvrat novih zahtjeva, odbacivanje paketa (i odluka kojih), oblikovanje i raspoređivanje prometa

2) Rješenja sa zatvorenom petljom

- cilj: nadzirati sustav i djelovati po potrebi;

Mutusobno povezivanje mreža i podmreža

Adresiranje

- Dinamicka adresa

- privremeno dodijeljena tijekom pristupa usluzi
(npr. IP)

- Statička adresa

- trajno dodijeljena (npr. url)

- Adresiranje u internetu (IPv4 - 32 bita)

- identifikator koji globalno i jednoznačno određuje mrežno sučelje

- Način zapisai

- numerički (binari i dekadski)
- simbolički (npr. www.fev.unizg.hr)
- DNS je veza između numeričkog i simboličkog zapisa

Fragmentsacija

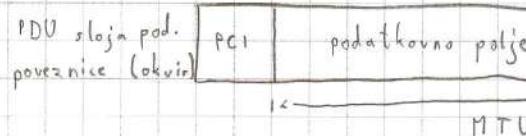
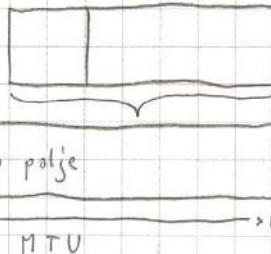
- PDU mrežnog sloja se smješta u podatkovno polje

PDU sloja pod. poveznice

- maximum transmission unit (MTU)

- za IEEE 802.3 MTU iznosi 1500 bytes

PDU mrežnog sloja (paket)



- Transparentnost:

-> Transparentna fragmentacija

- fragmentacija i sastavljanje na ulazu/izlazu svake podmrežje

-> Netransparentna fragmentacija

- sastavljanje tek na odredištu

Mrežni sloj u Internetu

Struktura i organizacija Interneta

Normiranje u internetu

- Internet - mreža međusobno povezanih mreža osnovanih na TCP/IP arhitekturi: protokolima

- IESG

1) Logički pogled (jedna mreža: jedinstveni adresni prostor)

- IETF

2) Fizički pogled (mreža sastavljena od podmreža)

- IRSG

- IRTF

- RFC Editor

- rfc-editor.org/rfc-index.html

- samo 70-tak standarda, ostatak preporuke

- Internet society (ISOC)

- ICANN

-> IANA

Autonomni sustav (AS)

- skupina IP mreža i usmjeritelja pod zajedničkom upravom i sa zajedničkom politikom usmjeravanja prema Internetu

- jedinstveni broj dodjeljuje org. IANA

(npr. CARNet - AS 2108)

Usmjeravanje

1) Unutar AS-a (Interior Gateway Protocol - IGP)

- najčešći OSPF, RIP, EIGRP, IS-IS

Internet Protocol (IP)

- neovisan o njizim protokolima

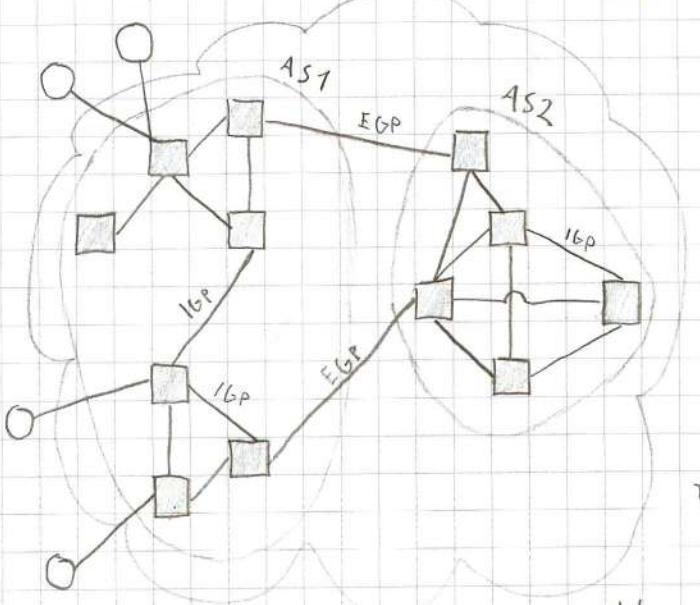
- datagramski način rada

- nespojna usluga bez potvrde

- nema kontrole toka

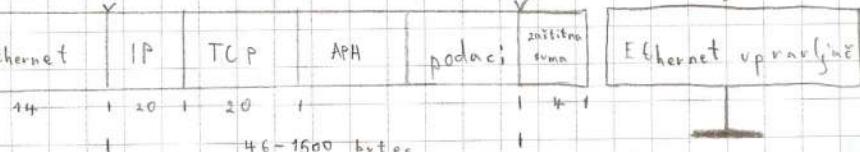
- nema čvrstanje redoslijeda datograma

- enkapsulacija podataka



□ router

○ host



Funkcionalnost:

1) Definira shemu adresiranja

→ jedna IP-adresa po krajnjem mrežnom svučju

→ Opće razširjavanje (broadcast)

- adresom svima (255.255.255.255)

- samo u lokalnoj mreži

2) Definira fragmentaciju

→ primatelj sastavlja pakete

→ Vlastita mreža

- od 0.0.0.0 do 0.0.0.8

• Struktura IP adresi

1) Identifikator mreže (Net ID)

→ dodjeljuje ICANN

• Postavljanje IP adresa

→ identificira mrežu u kojoj se nalazi mrežno svučje

1) Statičko

- male mreže (poslužitelji i usmjeritelji)

2) Identifikator krajnjeg računala (Host ID)

→ dodjeljuje lokalni administrator

2) Dinamičko

→ identificira mrežno svučje u mreži

- velike mreže (za osobna računala)

→ mogućnost podijeljenja (podmreže)

- protokol DHCP

• Fragmentacija

- Nettransparentna

- MTU = 1500 bytes

Besklasno usmjeravanje (CIDR)

- duljina mrežnog dijela označava se mrežnim prefiksom

Usmjeravanje u internetu

~ npr. 195.24.0.0/13

11000011.00011000.00000000.00000000
mrežni prefiks (13)

• Usmjeritelj (router) je mrežni uređaj koji usmjerava

i prestavlja pakete

• Načela usmjeravanja:

1) Upravljačka informacija

→ izvorišna adresa (source address)

→ odredišna adresa (destination address)

→ ograničenje broja skokova na putu (TTL)

- sprječavanje beskonačnih petlji

2) Tablica usmjeravanja

3) Područje usmjeravanja

→ unutar ili između AS-ova

• Internet Control Message Protocol (ICMP)

- za javljanje stanja (npr. ping)

Vrste IP adresa

1) Javni adresni prostor

2) Privatni adresni prostor

3) Rezervirani adresni prostor

- preslikavanje iz privatnih adresa u javne

→ obrnuto održuje NAT

- rezervirane adrese

→ Povratna adresa (Loopback)

- od 127.0.0.0 do 127.255.255.255

Međusobno povezivanje mreža

Povezivanje adresu mrežnog sloja i sloja

podatkovne poveznice

- Adresa mrežnog sloja
- Format neovisno o tehnologiji mreže
 - identifikacija mrežnog učesnika : usmjeravanje
 - npr. IP adresa
- Adresa sloja podatkovne poveznice
 - Format ovisan o tehnologiji mreže
 - npr. Ethernet
- Adrese različitih slojeva su neovisne

Address Resolution Protocol (ARP)

- povezivanje IP-adrese s MAC-adresom

Nacin rada:

1.) upit za IP-adresu se šalje svim učesnicima

na poveznici (broadcast)

2.) na upit odgovara samo tražen učesnik svojom

MAC adresom

3.) pošiljatelj i primatelj privremeno pohranjuju

uparenu IP-MAC adresu (nekoliko minuta)

Nacela povezivanja mreža

1.) Ustanoviti zahtjeve

2.) Odrediti moguća rješenja

3.) Odabrati najpotpunije rješenje

Mrežni uredaji:

4. Transportni sloj

Prilaz (gateway)



3. Mrežni sloj

Usmjeritelj (router)



2. Sloj pod. poveznice

Most (bridge)

Komutator (switch)



1. Fizički sloj

Repeater

Hub

- Hub

→ presljeđuje svim povezanim uređajima (ne koristi se više)

- Repeater

→ prolužuje medije fizičkog sloja

- Most

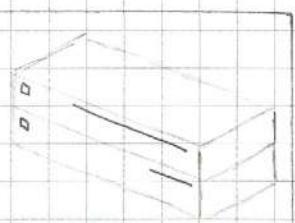
→ povezuje različite medije fizičkog sloja

(npr. bakar-most-optika)

7. Aplikacijski sloj

6. Prezentacijski sloj

5. Sjednički sloj



Pristup Internetu i Transportni sloj

Pristupu Internetu

Nacini pristupa:

1) Kroz fiksnu mrežu

-> od krajnjeg uređaja do Interneta se stvara fiksni kanal

-> Point of Presence (PoP)

-> Point to Point Protocol (PPP)

- bajt-orientiran

- na sloju podatkovne poveznice

- adresa u zaglavljiv nevažna

- komponente:

1) Protokol za kontrolu poveznice (LCP)

- konfiguriranje, uspostavljanje, ispitivanje i raskidavanje podatkovne poveznice

2) Mrežni kontrolni protokol (NCP)

- neovisno konfiguriranje: uspostavljanje protokola mrežnog sloja (zasebni NCP za svaki mrežni protokol)
- npr. IPCP

- primjer komunikacije s PPP:

1.) Uspostava poveznice (LCP)

1.5.) Ovijenje i upravljanje kvalitetom

2.) Pregovaranje o konfiguraciji mrežnog sloja (NCP => IPCP)

3.) Komunikacija na mrežnom sloju (IP)

4.) Raskidavanje poveznice (LCP)

-> ADSL (Asymmetric Digital Subscriber Line)

- stalna povezanost

- frekvenčni pojas podignut iznad 4 kHz (ne smeta telefonu 0-4 kHz)

2) Kroz pokretnu mrežu

Transportni sloj

- transparentan prijenos transportnih jedinica podataka od izvora do odredišta

Usluge:

- može biti spojna i nespojna

- Adresiranje

-> Network-Service Access Point (N-SAP)

- adresa mrežnog svjetla

- svjetlo transporta i mreže

-> Transport-Service Access Point (T-SAP)

- adresa transportnog entiteta

- svjetlo transporta i aplikacije

- Multiplexiranje

-> Odozgo 

- npr. TCP ; UDP

-> Odozdo 

- npr. uTCP ; SCTP

- Uspostava veze

-> numeracija poruka

-> pozitivne i negativne potvrde

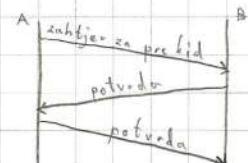
-> vremenska kontrola

-> klijenti pravir

- Raskid veze

-> vredno zatvaranje

-> nužna vremenska kontrola



- Kontrola toka

- > prilagodba mrežnom sloju
- dinamički klizeći prostor
- privremena pohrana T-PDU-a

- Izbor transportnog protokola

-> Kriteriji:

- Pouzdanost

- Kašnjenje

- Kolебање каšњења (varijacija)
- Širina pojasa

• Protokoli transportnog sloja u Internetu

1) Transmission Control Protocol (TCP)

-> prijenos bez pogrešaka u nepromijenjivom redoslijedu

-> TCP PDU se naziva (TCP) segment

-> Funkcionalnosti:

1) Transport podataka

-> avosmjerni transport kontinuiranog niza podataka

-> pakiranje bajtova u segmente

-> predaja T-PDU-a mrežnom sloju

-> Maximum Segment Size (MSS)

- APH + podaci

2) Adresiranje i multiplexiranje

-> vrata na izvoru i vrata na odredistvu

-> parovi vrata-IP adresa

-> pouzdana TCP veza, rali nepouzdan

prijenos IP datagramma

3) Pouzdanost

-> detekcija pogrešaka

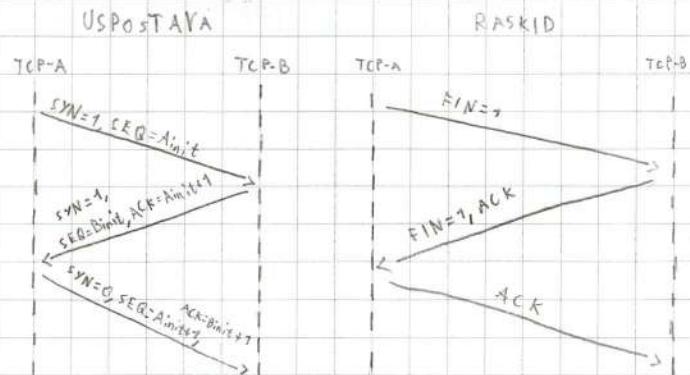
-> retransmisija

-> potvrde (numeracija segmenata)

-> vremenska kontrola (RTO)

4) Upravljanje rezom

-> SYN, FIN, ACK...



5) Upravljanje tokom podataka

-> klizeći prozor

6) Upravljanje zagruženjem

-> Polaganji početak (slow start)

-> Izbjegavanje zagruženja (congestion avoidance)

-> Prag polaganog početka (sthresh)

-> Prozori:

- primateljni (rwnd)

- zagruženja (cwnd)

- posiljalci (swnd): $\min\{rwnd, cwnd\}$

- proces kod gubitka segmenta:

- Prepoznavanje gubitka

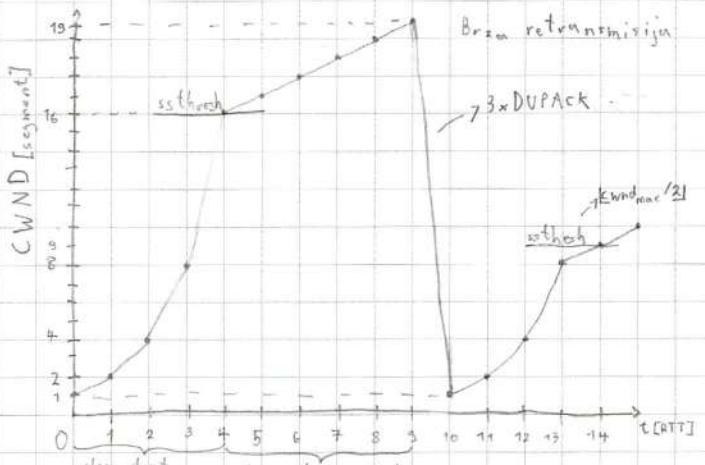
1) Istečne RTO = RTT + 4 * D

2) Primetak dvostrukke potvrde (DUPACK)

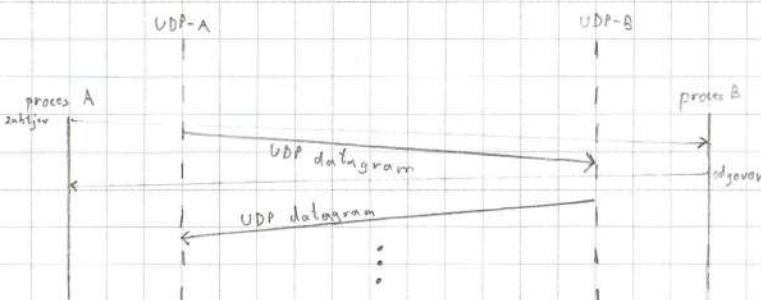
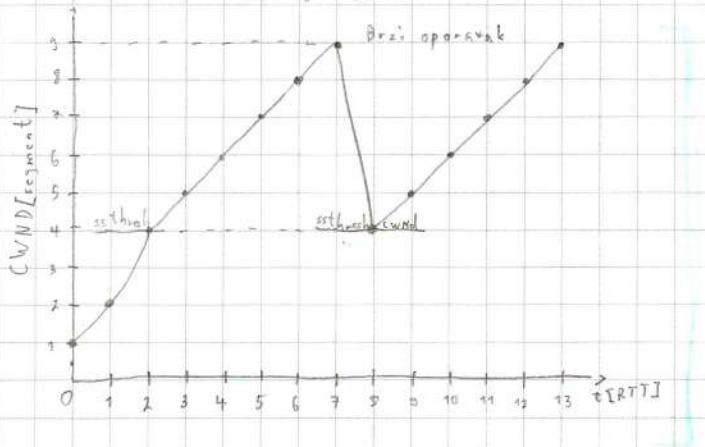
- npr. primetak niza segmenta 0, 1, 3, 2,

če na strani primatelja generirati

potvrde 1, 2, 2, 4, 5



- ne uspostavlja veze
 - nema potvrda i ne garantira isporuku
 - ne otkriva gubitak
 - ne garantira redoslijed segmentata
 - ne pruža kontrolu taka niti kontrolu zagruženja
- Primjena: time-sensitive (real-time) potrebe (npr. online igrice)



→ Razine izvedbe:

- 1.) TCP Tahoe
- 2.) TCP Reno
- 3.) TCP New-Reno
- 4.) TCP - Selective acknowledgements

→ Primjena: transfer datoteka, email, transakcije,

rad na udaljenom računalu, Web server

→ Ograničenja:

1) Nema mehanizme za sigurnost i privatnost podataka

2) Ne radi računa o granicama poruke (spojna vrlova)

3) Ne garantira isporuku višem sloju

2) User Datagram Protocol (UDP)

→ Funkcionalnosti:

- 1) Multiplexiranje
- 2) Zaštitna suma cijelog datograma (opcionalno)

→ Ograničenja:

Aplikacijski sloj i DNS

* Aplikacijski protokoli:

- FTP
- TELNET
- SMTP, POP, IMAP
- HTTP

* Model izvedbe usluge:

- client-server

-> posebni slučajevi:

- single-server/multiserver
- proxy server
- caching server

-> komunikacija se temelji na nizu zahtjeva

i odgovora

-> Program klijenta

- pruža korisničko sučelje
- odgovarajuće formativa zahtjev iz poslužitelja
- i odgovor za korisnika

-> Program poslužitelja

- ostvaruje i prihvata zahtjev
- obrađuje zahtjev i šalje odgovor
- Podjela prema memoriji:

1) Memorijski (statefull)

2) Bezmemorijski (stateless)

- Podjela prema načinu obrade:

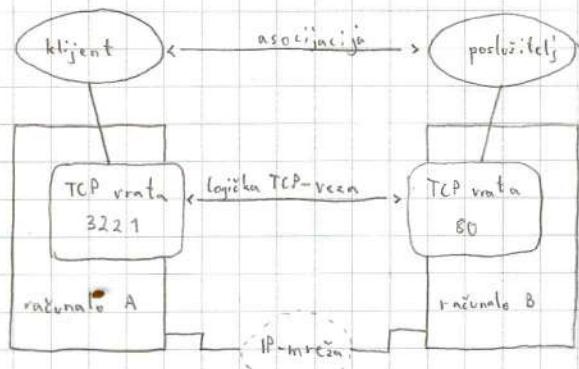
1) Iterativni (jedan po jedan)

→ pogodan za zahtjeve kratkotrajne obrade

2) Konkurenčni

→ poslužitelj raspoređuje zahtjeve procesima

-> Asocijacije klijenta i poslužitelja



- Promalaženje usluga

→ klijent mora unaprijed znati adresu poslužitelja da bi mogao pristupio

- na razini interneta postoji dobro-poznata vrata (well-known ports) za standardne internetске usluge

→ npr. 21 (ftp), 22 (ssh), ..., 80 (http), ..., 102

- za ostale usluge mora povezati drugi način promakšanja vrata

- Programska sučelje (socket API)

→ socket = (IP-adresa, transportni protokol, broj vrata)

- peer-to-peer

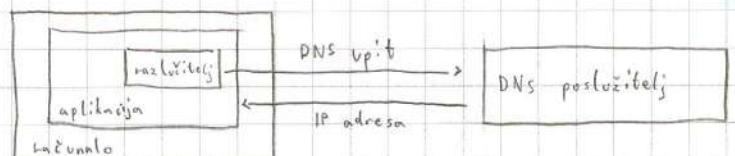
- ...

Domain Name System

• Najčešća uporaba: povezivanje numeričke IP adrese s imenom

- sustavna usluga

• Prvo rješenje: popis hoststata, kasnije uređen DNS



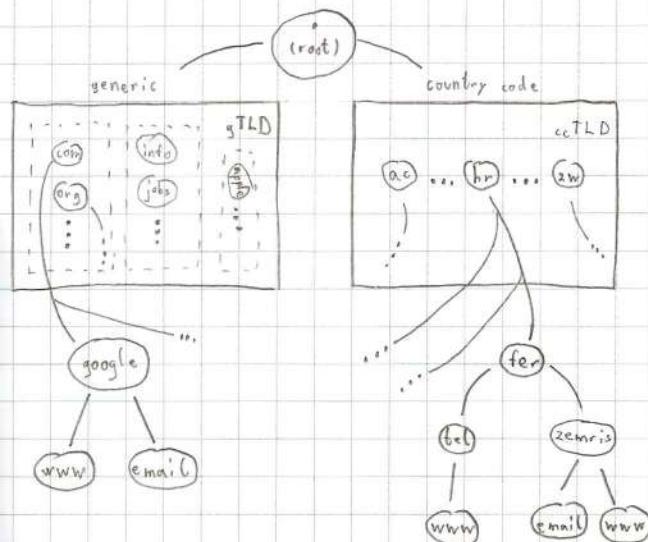
→ sustav domenskih imena (hierarhijski)

- Domena

→ skupina mrežnih sučelja koje karakterizira prigodnost

- FQDN (host, poddomena, domena)

→ jedinstvena identifikacija mrežnog svijetla



International Domain Name (IDN)

- npr. župan.hr
- puny code kodiranje
- CARNet uveo 2016.

Razlučivanje IP adrese

- depth search
- Načini razlučivanja:
 - 1) Iterativni
 - 2) Rekursivni
- u praksi kombinirano (lokalni DNS poslužitelj sa caching)
- primjer na nslookup.io

DNS koristi UDP

WWW i Email

WWW

- Hipertekst ; hipermedij
- Informacijski izvor/resurs
- Bilo šta što daje informaciju
- Pitanja:
 - 1) Kako zapisati? HTML
 - jednostavan i prenosiv zapis
 - mogućnost hipervraca i drugih medija
 - 2) Kako adresirati? URL
 - 3) Kako povezati? HTTP
- Hypertext Transfer Protocol (HTTP)

Email

- Jedna od najstarijih internetskih usluga (1973.)
- Model izvedbe: klijent(MUA)-poslužitelj(MTA)
- Funkcionalnosti:
 - 1) Stvaranje poruke
 - 2) Predaj, transfer i isporuka poruke
 - 3) Pređelovanje (pregleđ) pristiglih poruka
 - 4) Izvršavanje (o uspešnosti) isporuke
 - 5) Raspolaganje (kontrola nad) porukama
- Format email adrese: korisnicko_ime@FQDN

- točke u korisničkom-imenu se ignoriraju u gmail-u

- tekstučan zapis
- načelo rada zahtjev-odgovor
- Format poruka:
 - 1) Početni redak
 - 2) Polja zaglavljia
 - 3) Prazni redak (\n)
 - 4) Tijelo poruke (npr. <html>...</html>)

- oblik zahtjeva:
 - metoda put-iz-URL verzija
 - npr. POST /shop/order HTTP/1.1

- statusni kod odgovora

1) 1XX - Informativna poruka

2) 2XX - Uspjeh (obradm i odgovor)

3) 3XX - Preusmjerenje

4) 4XX - Greška na klijentu (zahtjev neispravan)

5) 5XX - Greška na poslužitelju (zahtjev

Format poruke

1.) Zaglavljic

-> To:

-> Cc (carbon copy):

-> Bcc (blind cc):

-> Subject:

-> Date:

-> From: (izvorni posiljač)

-> Received: (popis MTA-a na putu)

2.) \n

3.) Tijelo

- Multi-purpose Internet Mail Extensions (MIME)

(ispraviti za poslužitelj ne može ispuniti)

- razmjenja teksta s različitim znakovnim skupovima te razmjenjuje ne-tekstualnih i višemedijskih poruka

- Internetski aplikacijski protokoli:

- 1) Simple Mail Transfer Protocol (SMTP)

- > ne ovira o mrežnom protokolu niti o vrsti mreže
- > strogo definira sintaksu i redoslijed odvijanja transakcije (kodovi)

- 2) Post Office Protocol v3 (POP3)

- > način rada "dohrati i obrnjeti"
- > nešifrirane poruke
 - proširenje protokola: Authenticated POP (APOP)
 - dodatna zaštita: SSL ili TLS

- 3) Internet Message Access Protocol (IMAP)

- > poruke ostaju na posložitelju, (pogoden za više vrednosti)

- Naučni pristup poštanskom sandučiću:

- 1) Stalni (on-line) model

- > veza s poslužiteljem uspostavljena je cijelo vrijeme dok se koristi: MUA

- 2) Povremeni (off-line) model

- > korisnik uspostavi vezu, prenese poštu na svoje računalo i prekine vezu (POP)
- > daljnji rad se izvodi lokalno

- 3) Odspojeni (disconnected) model

- > klijent uspostavlja vezu, kopira poruke i prekine vezu (IMAP)
- > daljnji rad se izvodi lokalno (uz povremenu sinkronizaciju)

Rad na udaljenom računalu i transfer datoteka

Remote work

• Osnovni zahtjevi:

- univerzalni rad (neovisno o OS-u) : transparentan pristup aplikacijama i podacima
- zaštitu od neovlaštenog pristupa
- zaštitu od interferencija

TELNET protokol

- lokalno računalo (local host)
- udaljeno računalo (remote host)
- potrebno imati korisnički račun
- jedna TCP veza za kontrolu i podatke
- Temeljne ideje:

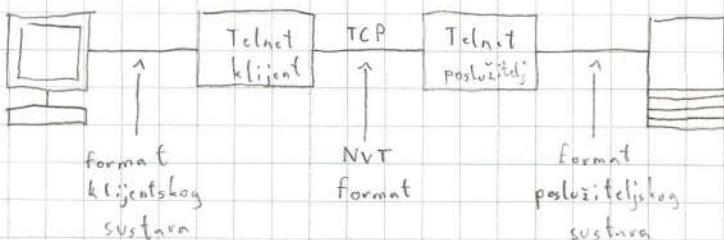
1.) Umreženi virtual terminal (NVT)

- Osnovna svojstva propisana

2.) Pregovaranje o izbornim svojstvima

3.) Oba kraja veze se tretiraju simetrično

klijent



Mekhanizam pregovaranja

1) Kada klijent postavlja željena svojstva za sebe

- "will" služi za postavljanje svojstava

→ odgovori: "do" : "don't"

- "want" služi za uklanjanje svojstava

→ odgovori: "don't" (za prihvatanje), ne odbija se

- "do" služi za postavljanje svojstva

→ odgovori: "will" : "won't"

- "don't" služi za uklanjanje svojstva

→ odgovori: "won't" (za prihvatanje), ne

odbija se

• > telnet towel.blinkenlights.nl 23

- Star Wars ep IV u ASCII kodu

File transfer

• Ideja: postavljanje/preuzimanje datoteke na/na

udaljenog računala

→ protokol TCP

File Transfer Protocol (FTP)

- Funkcije:

1) Kopiranje datoteka s jednog sustava na drugi

2) Interaktivni pristup (npr. ispis sadržaja)

3) Specifikacija formata (binarna, ASCII,..)

4) Autentifikacija klijenta

Ustavljanje veze:

1.) Kontrolna (TCP port 21)

2.) Podatkovna (TCP port 20)

- Odgovori kodirani u obliku troznamenkastog broja

2) Kada klijent pregovara o svojstvima koja traži od poslužitelja

Sigurnost u internetu

- ovisi o kontekstu (npr. lažinke, web stranice, poslužitelji itd.)

Sigurnosni zahtjevi (CIA+2)

- 1) Povjerenljivost (confidentiality)
- 2) Integritet (integrity)
- 3) Raspoloživost (availability)
- 4) Autentičnost (authenticity)
- 5) Nepovećivost (nonrepudiation)

Predviđati za incident:

- 1) Ranjivost (vulnerability)
 - pogreška ili slabost u dizajnu sustava
 - npr. bugs

Prijetnja (threat)

- dogadjaj koji može iskoristiti ranjivost te na taj način provoćišti štetu

Tipovi:

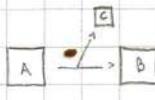
1) Ljudske prijetnje

- namjerno ili slučajno

2) Prirodne prijetnje

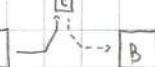
- npr. potres, nestanak struje itd.

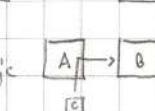
Primjeri:

- Presretanje/prisluškivanje 
- Prekidanja/uskracivanja usluge 



- Promjena (MITM) 

- Fabrikacija/ponavljanje 

- Lažno predstavljanje/maskiranje 

Kontrole:

1) Fizičke kontrole

- > npr. kamere, zaštitari, vrata itd.

2) Administrativne kontrole

- > različiti propisi kojima je definirana sigurnost, pravilnici, postavke

- > npr. politike, pravilnici itd.

3) Tehničke kontrole/sigurnosni mehanizmi

- > npr. kriptografija, javni ključ, vratocišta

Osnove kriptografije

* Kriptologija:

1) Kriptografija (šifriranje)

2) Kriptoanaliza (dekriptiranje)

* Osnovni algoritmi

- Šifriranje i dešifriranje

1) Simetrično šifriranje i dešifriranje

- isti ključ se koristi za šifriranje i dešifriranje

- znaga algoritma je obično proporcionalna veličina ključa

1) Blok orijentirani

- ključ je fiksne veličine (X bitova)

- npr. DES (1977. - 56 b), AES (2001. - 128 b)

2) Bit/broje orijentirani

- ključ je veličine poruke

2) Asimetrično šifriranje i dešifriranje

- temelje se na teškim matematičkim problemima

- različiti ključ za šifriranje i dešifriranje

- primjeri:

1) Kriptografija javnog ključa (PKI)

→ kriptiranje javnim ključem E(p)

→ npr. lice v lice, leap of faith

→ dekriptiranje privatnim ključem D[E(p)] ⇒ P

- ako se javni ključ promijeni, znamo da je voza

2) RSA

→ temelj u faktorizaciji velikih brojeva

→ pristup koriste PGP i SSH

→ potrebeni dugi ključevi

- Certifikacijsko tijelo (CA)

- u praksi se za razinjenu ključevu koriste asimetrični

→ svi imaju njegov ključ

algoritmi, a za šifriranje simetrični (brži)

→ izdaje certifikate autentičnosti korisnicima

- Kriptografska funkcija sažetka (hashiranje)

(uključujući i samom sebi - self signed

→ npr. SHA1, SHA2 i SHA3

certificate)

- Digitalni potpis

1.) Postupak generiranja (šalje sažetak i poruku)

- svi mogu izdati sebi, ali preglednici

- posljednji izračunava sažetak MD(P)

upozoravaju i teško dobiti priznanje

- sažetak poruke kriptirati svojim tajnim

- placena usluga

ključem $D_A[MD(P)]$ (digitalni potpis)

→ delegira provjeru korisnika registracijskim

2.) Postupak provjere

tijelima (RA)

- primatelj dekriptira kriptirani sažetak

→ distribucija certifikata se obavlja putem

$E_A(D_A[MD(P)]) \Rightarrow MD(P)$

posebnih aplikacija (public key infrastructure - PKI)

- izračunava sažetak primljene poruke

DN: cn=Anja Kovac, o=FER,

← informacije o korisniku

MD(P') te provjerava identičnost

c=HR

← jednečnačni serijski broj

→ u slučaju velikog broja poruka, koristi se

Serial #: 3913133

→ informacije o važećem certifikatu

slučajni dogovoren broj s koji konkatenirani

Start: 1-9-2011 3:33

← informacije o važećem certifikatu

sažetak te se njegovom provjerom osigurava

End: 31-8-2012 3:33

← informacije o važećem certifikatu

komunikacija

CRL: cn=CRL2, c=FER,

← info o povratak certifikata

- tzv. message authentication/integrity code

c=HR

← javni ključ korisnika

(MAC/MIC)

Key: abc385...

← informacije o izdavaču certifikata

CA DN: o=UNI-ZG, c=HR

← digitalni potpis izdavača certifikata

- u pravilu se prvo šifriraju, a potom dodaje kod za



← digitalni potpis izdavača certifikata

značitu integritetu: autentičnosti

Sigurnost komunikacije - Protokol SSL/TLS

* Problem distribucije javnog ključa

SSL (Secure Sockets Layer)

- Ideja: alternativni način provjere ispravnosti

- osmislio Netscape, danas se ne koristi (nesiguran)

TLS (Transport Layer Security)

- razvio IETF, trenutna verzija 1.2
- omogućuje utvrđivanje identiteta poslužitelja
 - (! autentifikaciju klijenta, ali to niste certifikati)
- zaštita od prislушкиvanja, loženja / ponavljanja, izmijene i fabrikacije

Komunikacija:

- 1.) Klijent šalje poruku "Client Hello"
- 2.) Poslužitelj šalje poruku "Server Hello"
- 3.) Poslužitelj šalje svoj certifikat
 - 3.1) Klijent javnim ključem poslužitelja (iz certifikata) šifrira ključ sjednice u digitalnoj omotnici
- 4.) Klijent šalje poruku "Client Key Exchange"
 - sa omotnicom
- 4.1) Poslužitelj privatnim ključem dešifrira poruku i vodi ključ sjednice
- 5.) Oba šalju poruku "Change Cipher Spec"
- 6.) Oba šalju poruku "Finished"
- 7.) Slanje (šifriranih) podataka aplikacije

- HTTP umjesto TCP-a koristi TLS na portu 443

- Email koristi S/MIME; PGP potpisivanje i/ili

kriptiranje poruka

→ jer ne možemo osigurati da će svaka

komunikacija ići preko TLS (između poslužitelja)

→ temelji se na sustavu PKI

Vnetosid (firewall)

- sigurnost krajnjih sustava i mreža

→ ne komunikacije

- sadrži bazu pravila te provjerava svaki paket

Vrste:

1) Bez stanja (stateless)

- brzi, ali teži za podešavanje i sigurniji

2) Sa stanjem (stateful)

- sprema informacije o vidjenim paketima

- sporiji, ali jednostavniji za podešavanje i sigurniji

Demilitarizirana zona (DMZ)

→ ako u mreži postoji poslužitelji kojima treba pristupiti izvana

- u praksi arhitekture s jednim ili dva vnetosida

Povezivanje mreža u internetu

Network Address Translation (NAT)

- privatnu adresu prevodi u javnu i obratno
- više računala iz lokalne mreže komunicira u internetu preko jedne ili nekoliko javnih IP-adresa

Kombinacija s Port Address Translation (PAT)

- Prednosti:

- 1) Štednja adresnog prostora
- 2) Povećana razina sigurnosti (skrivene IP-adrese)

- Nedostaci:

- 1) Povećane kačnjenje
- 2) Nemogućnost praćenja paketa s kraja na kraj
- 3) Povećana kompleksnost adresiranja