

Komunikacijske mreže

Uvodno o predmetu ...

Ak.g. 2007./2008.

27.9.2007

Nastavnici

Prof.dr.sc. Ignac Lovrek¹

Prof.dr.sc. Vlado Glavinić²

Prof.dr.sc. Dragan Jevtić¹

Prof.dr.sc. Maja Matijašević¹

Doc.dr.sc. Gordan Ježić¹

Suradnici

Vedran Podobnik¹ (AHyCo)

Stjepan Groš²

Mr.sc. Josip Gracin¹

Ognjen Dobrijević¹

Tomislav Grgić¹

¹Zavod za telekomunikacije, C zgrada 7. i 8. kat

²Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave,
D zgrada, 3. kat

Komunikacijske mreže

27.9.2007

2 od 9

Cilj predmeta



znanje o komunikacijskim mrežama,
mrežnim arhitekturama i komunikacijskim protokolima,
s naglaskom na Internetu

temeljni koncepti i

praktično iskustvo na odabranim primjerima

zašto
što
kako

problem koji se rješava
funkcionalnost
izvedba

Komunikacijske mreže

27.9.2007

3 od 9

Sadržaj predmeta



Uvod u komunikacijske mreže. Mrežne arhitekture, klasifikacija i topologija. Komunikacijski kanal i informacijski paket. Komunikacijski protokol. Slojeviti modeli: referentni model povezivanja otvorenih sustava (OSI), internetski model (TCP/IP). Mrežni protokoli, protokol IP i drugi protokoli mrežnog sloja u Internetu. Organizacija IP-zasnovanih mreža. Transportni protokoli, TCP i UDP. Sustav imena, internetske domene. Sigurnost. Usluge i aplikacije, društveni i ekonomski aspekti. Lokalne mreže, mreže širokog područja, povezivanje mreža. Primjeri: javne te akademске i istraživačke mreže.

Komunikacijske mreže

27.9.2007

4 od 9

Organizacija nastave



Predavanja 3 bloka (4+4+5 predavanja)
 3 sata tjedno

Laboratorijske vježbe 3 bloka

Samostalni rad kontinuirano
 učenje i provjera znanja
 domaće zadaće
 programski modeli mreža

Komunikacijske mreže

27.9.2007

5 od 9

Nastavna literatura (1)



Bilješke s predavanja

- nastavni sadržaj s primjerima: slide + tekst (Power Point), dva radna dana prije predavanja (web)
- vlastite zabilješke, tijekom predavanja i učenja

Laboratorijske vježbe

- programski sustav Imunes (www.imunes.net) Integrated MULTIProtocol Network Emulator/Simulator
- modeli mreža (web)

Provjera znanja

- zadaci (web)
- rješenja zadataka prije (među)ispita (web)

Komunikacijske mreže

27.9.2007

6 od 9

Nastavna literatura (2)



Osnovne knjige:

- A. Bažant, G. Gledec, Ž. Ilić, G. Ježić, M. Kos, M. Kunštić, I. Lovrek, M. Matijašević, B. Miklac, V. Sinković: Osnovne arhitekture mreža, Element, 2007.
- A.S. Tanenbaum: Computer Networks, Fourth Edition, Pearson Education Inc., 2003. (preporučena knjiga na engleskom jeziku)

Dodatne knjige:

- F. Halsall: Computer Networking and the Internet (5th Edition), Addison Wesley, 2005.
- J.F. Kurose, K.W. Ross: Computer Networking: A Top-Down Approach Featuring the Internet (4th Edition), Addison Wesley, 2007.
- J.L. Peterson, B.S. Davie: Computer Networks: A Systems Approach, 4th Edition, Morgan Kaufmann, 2007.

Komunikacijske mreže

27.9.2007

7 od 9



Ocenjivanje

Komponente ocjene:

Sudjelovanje u nastavi	10 % (nazočnost + aktivnost)
Domaće zadaće	10 % (5 zadaća u semestru)
1. Međuispit (90 min.)	20 % (prva trećina gradiva)
2. Međuispit (90 min.)	20 % (druga trećina gradiva)
Laboratorijske vježbe	15 % (sve obvezne)
Završni ispit (90 min.)	25 % (sve, s naglaskom na treću trećinu)

Prolazna ocjena:

Ukupno	>50 %, uz obavljeni labos
--------	---------------------------

Komunikacijske mreže

27.9.2007

8 od 9

Informacije o predmetu:

<http://www.fer.hr/predmet/kommre>

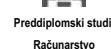
Konzultacije:

tjedni termin za svaku grupu (nastavnik i suradnik)

Komunikacijske mreže

27.9.2007

9 od 9



Prediplomski studij
Računarstvo

Komunikacijske mreže

1.

Uvod u komunikacijske mreže i osnove arhitekture mreža

Ak.g. 2007./2008.

4.9.2007

Sadržaj predavanja



- ♦ Klasifikacijski kriteriji i vrste mreža
- ♦ Komunikacijski kanal i informacijski paket
- ♦ Arhitektura mreže
- ♦ Slojeviti modeli
- ♦ Referentni model povezivanja otvorenih sustava (OSI)
- ♦ Internetski model (TCP/IP)
- ♦ Normizacija

Komunikacijske mreže

4.9.2007

2 od 45

Komunikacijska mreža



- ♦ Komunikacijsku mrežu čine međusobno povezani komunikacijski sustavi na koje se spaja korisnička oprema (komunikacijska, računalna) i druga oprema potrebna za pružanje informacijskih i komunikacijskih usluga te potporu aplikacija korisnicima (poslužiteljska računala i drugi sustavi).
- ♦ Mreža se može predočiti grafom čiji čvorovi odgovaraju sustavima (računalnim, komunikacijskim), a grane prijenosnim medijima koji ih međusobno povezuju.

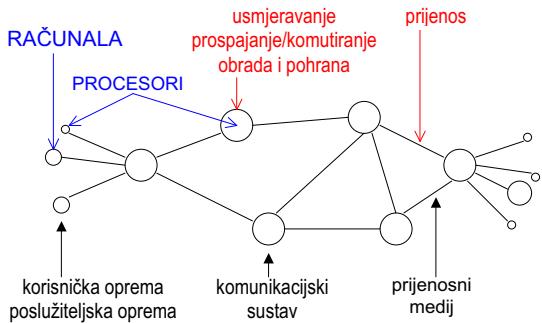
Komunikacijske mreže

4.9.2007

3 od 45

Prikaz mreže

MREŽA RAČUNALA



U mreži se razlikuju krajnji čvorovi koji predočuju korisničku i poslužiteljsku opremu te međusobno povezani mrežni čvorovi koji predočuju komunikacijske sustave. Mrežni čvorovi na koje su priključeni ili s kojima su povezani krajnji čvorovi nazivaju se pristupnim čvorovima.

Komunikacijski sustavi provode operacije s informacijskim tokovima u mreži. Oni ih usmjeravaju kroz mrežu (engl. *routing*), prospajaju, odnosno komutiraju (engl. *switching*) sa svojih ulaza na svoje izlaze, po potrebi obrađuju i pohranjuju. Kako poslužuju više ili mnogo korisnika, ovisno o namjeni i veličini mreže, u pravilu su većeg ili velikog kapaciteta, a moraju omogućiti unapređenje postojećih usluga i aplikacija, kao i uvođenje novih. Stoga su komunikacijski sustavi procesorski upravljeni, a njihovi upravljački sustavi sadrže mnoštvo procesora s različitim zadatacama.

Pojam korisnika (engl. *user*) obuhvaća osobe te različite uređaje i sustave priključene na mrežu. „Korisnik“ upotrebljava mrežu za informacijske i komunikacijske usluge i aplikacije. Korisnička oprema koja omogućuje različite informacijske i komunikacijske usluge (npr. pokretni telefon), isto tako sadrži jedan ili nekoliko procesora, a mnoge usluge i aplikacije korisnici izvode izravno sa svog računala.

Sve današnje komunikacijske mreže u svojim krajnjim i mrežnim čvorovima sadrže računala ili procesore, tako da velikih konceptualnih razlika između komunikacijske mreže, ili, u užem smislu mreže računala (engl *computer network*) nema.

Vrste mreža

Klasifikacijski kriteriji:

- ◆ Rasprostranjenost (područje na kojem se prostire)
- ◆ Namjena (javna/privatna)
- ◆ Vrsta informacije – medij (govor, podatak, slika,)
- ◆ Način komuniciranja (kanal, paket)
- ◆ Topologija (povezanost čvorova)
- ◆ Pokretljivost korisnika (da/ne)

Klasifikacijski kriteriji se međusobno ne isključuju, već nadopunjaju.

Tako je npr. Hrvatska akademski i istraživački mreža CARNet, po rasprostranjenosti nacionalna mreža, namijenjena je akademskoj i istraživačkoj zajednici, a kao dio Interneta omogućuje prvenstveno paketsku komunikaciju podacima, a uz to govorom i multimedijom. Korisnici pristupaju mreži iz akademskih i istraživačkih institucija putem lokalnih mreža, iz svojih stanova putem javne mreže, npr. modemom kroz telefonsku mrežu, ili brzom asimetričnom digitalnom pretplatničkom linijom (engl. *Asymmetric Digital Subscriber Line*, ADSL). Isto o takom mogućenju im je pristup iz pokretne mreže.

Rasprostranjenost

- ◆ mreža širokog područja
(engl. Wide Area Network, WAN)
- ◆ metropolitanska ili gradska mreža
(engl. Metropolitan Area Network, MAN)
- ◆ lokalna mreža
(engl. Local Area Network, LAN)
- ◆ ostale:
 - kućna mreža (engl. Home Network)
 - osobna mreža (engl. Personal Area Network, PAN)
 - tjelesna mreža (engl. Body Area Network, BAN)
 - ...

Namjena

- ◆ javna mreža (engl. public network)
 - dostupna korisnicima s ugovornim odnosom s mrežnim operatorom
(engl. network operator)
- ◆ privatna mreža (engl. private network)
 - namijenjena ograničenoj skupini korisnika unutar iste zajednice
 - akademska i istraživačka mreža (engl. Academic Research Network, ARN)
 - korporacijska mreža (engl. corporate network)

U javnim mrežama pravo na usluge stječe se temeljem ugovornog odnosa s mrežnim operatorom. Preplatniku je omogućeno komuniciranje s preplatnicima i korisnicima vlastite ili drugih mreža te davaljima usluga (engl. *service provider*) u zemlji i inozemstvu, bez vremenskih i prostornih ograničenja. Privatne mreže povezuju se s javnim mrežama, uz ograničenja određena namjenom privatne mreže.

S motrišta vlasništva, javne su mreže u manjinskom, većinskom ili potpunom privatnom vlasništvu, a privatne mreže u državnom (npr. akademski i istraživačka mreža), ili privatnom vlasništvu (npr. bankovna mreža).

Izvedba javnih mreža uključuje, uz Internet, fiksne (nepokretnе) mreže:

- javna komutirana telefonska mreža (engl. *Public Switched Telephony Network*, PSTN)
 - digitalna mreža integriranih usluga (engl. *Integrated Services Digital Network*, ISDN)
- te pokretne mreže:

- globalni sustav pokretnih komunikacija (engl. *Global System for Mobile communications*, GSM), s proširenjima za komunikaciju podacima: opća paketska radijska usluga (engl. *General Packet Radio Service*, GPRS) i poboljšane brzine prijenosa podataka (engl. *Enhanced Data rates for Global Evolution*, EDGE),
- opći pokretni telekomunikacijski sustav (engl. *Universal Mobile Telecommunication System*, UMTS)

Povijesno, mreže su se razvijale odvojeno, za osnovnu i prvobitnu namjenu, tj. govor, podatak ili sliku. Telefonska mreža primjer je mreže za govornu komunikaciju, koja omogućuje i komunikaciju podacima, posebno važnu za pristup Internetu. Internet je primjer mreže izvorno izvedene za podatke i povezivanje računala, a koja se upotrebljava i za višemedijske komunikacije. Mreže postupno konvergiraju tako da integriraju više vrsta informacija - medija (npr. govor, podatak, slika) i objedinjeno tretiraju više medija, odnosno multimediju.

Postupno ujednačavanje, kako koncepata tako i postupaka, započelo je u sedamdesetim godinama razvojem digitalne tehnologije, a danas je u tijeku tzv. konvergencija mreža prema višeuslužnim i višemedijskim, s paketskim načinom komunikacije i zajedničkim mrežnim protokolom.

Treba uočiti da je za prijenos korisničke informacije na raspolažanju puni kapacitet kanala koji je osiguran tijekom uspostavljanja komunikacije.

Vrsta informacije

Od:

- ◆ govor (npr. telefonska mreža)
- ◆ podatak (npr. Internet)
- ◆ slika (npr. mreža kabelske televizije)

Prema:

- ◆ više vrsta informacije – više medija objedinjeno istom mrežom (engl. multimedia),
- ◆ više usluga u istoj mreži (engl. multiservice), uz
- ◆ međusobno povezivanje raznovrsnih mreža

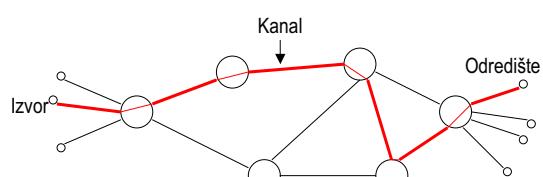
Način komuniciranja: komunikacijski kanal

Komunikacijski kanal

- ◆ put kroz mrežu između izvora i odredišta određenog kapaciteta (bit/s) koji se dodjeljuje na zahtjev (npr. pozivanjem), ili trajno (npr. najmom), zauzet cijelo vrijeme trajanja komunikacije
- ◆ **prednost:** prikladno za kontinuirani protok informacija u stvarnom vremenu, npr. kod razgovora, kad je važno održati vremenske uvjete komuniciranja kako se ne bi ugrozila razumljivost zbog prevelikih kašnjenja ili promjene kašnjenja
- ◆ **nedostatak:** neučinkovito, jer se dodijeljeni kapacitet zauzima (i naplaćuje) neovisno o tome da li se i koliko informacije prenosi

Mreža s komutacijom kanala

engl. circuit switched network



Komunikacija se odvija u tri faze:

1. Uspostavljanje komunikacije: komunikacijski između izvora i odredišta dodjeljuje se put kroz mrežu, od čvora do čvora, s propajanjem kroz čvorove na putu. Dodijeljeni kanal zauzima mrežne resurse sve do prekidanja komunikacije.

2. Izmjena informacije: informacija „teče“ od izvora do odredišta dodijeljenim kanalom koji je raspoloživ sve do prekidanja komunikacije. Dodijeljeni mrežni resursi su zauzeti neovisno o tome da li informacija izmjenjuje ili ne (“prazan kanal”).

3. Prekidanje komunikacije: po završetku izmjene informacije komunikacija se prekida i oslobađaju mrežni resursi.

Način komuniciranja: paket

(Informacijski) paket

- informacija se dijeli na blokove kojima se dodaje zaglavje s adresom na temelju koje ih se usmjerava od izvora do odredišta, i drugom upravljačkom informacijom
- prednost:** mreža se zauzima samo tijekom prijenosa paketa, a broj i veličina paketa može se prilagoditi količini informacije; u razdobljima kad jedan izvor ne odašilje pakete, mogu se prenositi paketi iz drugih izvora.
- nedostatak:** teže održati vremenske uvjete komuniciranja (kašnjenje i promjena kašnjenja); dio kapaciteta se troši na prijenos upravljačke informacije - zaglavja paketa

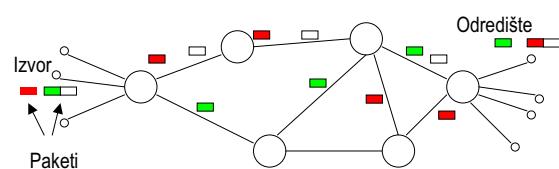
Mreža s komutacijom paketa

engl. packet switched network

Usmjeravanje paketa (engl. routing):

- datagramski
- virtualni kanal

Datagram



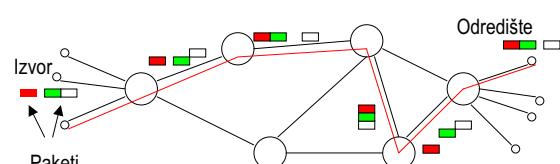
Svaki paket usmjerava se zasebno kroz mrežu, od izvora prema odredištu, tako da prolaze različitim putovima; takav paket naziva se **datagram**

Informacija se na izvoru dijeli na pakete – datagrame koji se proslijedu u mrežu. Svaki datagram sadrži adresu izvora i odredišta te drugu upravljačku informaciju potrebnu za usmjeravanje u mrežu.

Na temelju odredišne adrese, datagrami se usmjeravaju se svaki za sebe u čvorovima mreže, prolaze mrežom različitim putovima i na odredište pristižu u redoslijedu koji ne mora biti istovjetan onome u kojem su odaslati. Na to utječu kapacitet i trenutno opterećenje putova kojima prolaze, tako da kasnije odaslanu paketu može proći kraćim putom i brže, te biti isporučen ranije.

Na slici je predložen slučaj u kojem svi paketi s izvora stignu do odredišta. Međutim, pogreške uzrokovane smetnjama, kvarom sustava ili prekidom prijenosnog medija mogu onemogućiti isporuku nekih ili svih paketa odredištu.

Virtualni kanal



Najprije se određuje put kojim će se paketi usmjeravati kroz mrežu od izvora do odredišta, a zatim se svi paketi usmjeravaju tim istim putom, a što se naziva **virtualnim kanalom** (engl. virtual circuit)

Virtualnim kanalom oponaša se koncept stvarnog kanala kojim se ostvaruje put kroz mrežu između izvora i odredišta, a koji se dodjeljuje na zahtjev ili trajno. Najprije se uspostavlja put kojim će prolaziti svi paketi za traženu komunikaciju izvor-odredište. Taj put se označuje u čvorovima mreže na putu, te se nakon toga svi paketi prosljeđuju tim putom i u nepromijenjenom redoslijedu isporučuju na odredištu. Po završetku komunikacije virtualni kanal se prekida.

Na slici je predložen slučaj u kojem svi paketi s izvora stignu do odredišta. Međutim, pogreške uzrokovane smetnjama, kvarom sustava ili prekidom prijenosnog medija mogu onemogućiti isporuku nekih ili svih paketa odredištu.

Topologija

Regularne topologije:

- ◆ potpuna povezanost (engl. fully connected)
- ◆ zvijezda (engl. star)
- ◆ sabirnica (engl. bus)
- ◆ prsten (engl. ring)
- ◆ stablo (engl. tree)

Ostale topologije:

- ◆ nepotpuna povezanost
- ◆ međusobno povezane različite regularne topologije

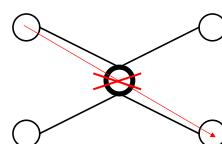
Potpuna povezanost

Izravna povezanost svaka dva čvora u mreži

- ◆ jednostavno povezivanje i usmjeravanje informacijskih tokova
- ◆ otpornost na kvarove - pri prekidu grane između dva čvora može ostvariti alternativni put preko ostalih čvorova
- ◆ primjena: umjereni broj čvorova i/ili ograničeno područje zbog troškova povezivanja (manje mreže)

Zvijezda

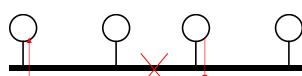
Središnji čvor na koji su spojeni svi ostali čvorovi posreduje pri komunikaciji između njih



- ◆ smanjen broj grana u mreži
- ◆ osjetljivost na kvarove - ispad središnjeg čvora onemogućuje bilo kakvu komunikaciju
- ◆ primjena: ograničeno područje (lokalna mreža, priključak korisnika na mrežu)

Sabirnica

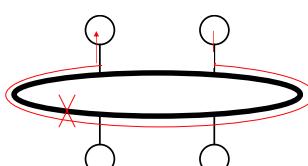
Svi čvorovi priključeni na zajednički prijenosni medij



- ◆ potrebni posebni mehanizmi dodjele prava komuniciranja pojedinom čvoru
- ◆ osjetljivost na kvarove - prekid onemogućuje komunikaciju
- ◆ primjena: lokalna mreža

Prsten

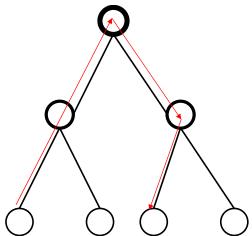
Svi čvorovi priključeni na zajednički prijenosni medij koji stvara zatvoreni put



- ◆ potrebni posebni mehanizmi dodjele prava komuniciranja pojedinom čvoru
- ◆ osjetljivost na kvarove - prekid prstena onemogućuje komunikaciju
- ◆ primjena: mreže velikog kapaciteta (optičke mreže)

Stablo

Hijerarhijska struktura



- komunikacija nadređenog i njemu podređenog čvora je izravna, a svaka druga zahtijeva posredovanje jednog ili više čvorova
- primjena: međunarodna - nacionalna - regionalna - lokalna povezanost

Arhitektura mreže

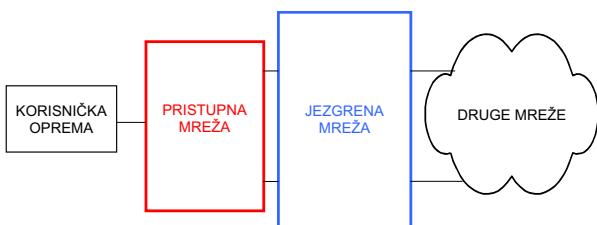
Dijelovi mreže:

- pristupna mreža (engl. access network) preko koje se priključuju korisnici
- jezgrena mreža (engl. core network) koja povezuje sustave u pristupnoj mreži te omogućuje komunikaciju s drugim mrežama

Slojevi mreže:

- vertikalna podjela funkcija po slojevima (engl. layer), od prijenosa informacije fizikalnim medijem (najniži sloj), do usluga i primjena na raspolažanju korisnicima (najviši sloj)

Dijelovi mreže



Slojevita mrežna arhitektura (1)

Aplikacijski sloj, sloj primjene
.....
(N+1)-sloj
(N)-sloj
(N-1)-sloj
....
Fizikalni/fizički sloj

- Vertikalna dekompozicija na slojeve**
- svakom sloju dodjeljuju se funkcije i specificiraju sučelja sa susjednim slojevima kako bi viši sloj mogao koristiti **uslugu** nižeg sloja
 - najviši je uvijek **aplikacijski** sloj koji predstavlja aplikacije i usluge za korisnike
 - najniži je uvijek **fizikalni sloj** koji ostvaruje stvarni prijenos informacija fizikalnim medijem

Slojevita mrežna arhitektura (2)

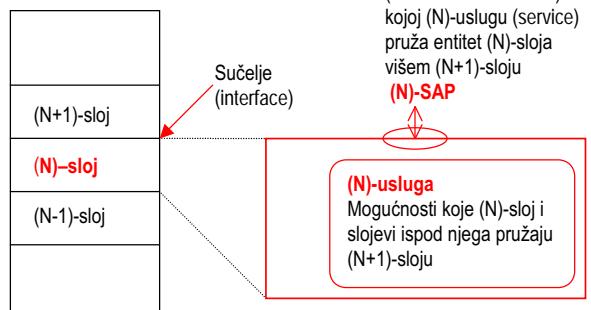
Namjena:

- definiranje koncepcata i normiranje,
- utvrđivanje pravila povezivanja sustava u mrežu te mreža međusobno,
- stvaranje otvorenih rješenja, neovisnih o proizvođaču opreme ili mrežnom operatoru.

Osnovni modeli:

- referentni model povezivanja otvorenih sustava (engl. Reference Model of Open System Interconnection, OSI)
- referentni model TCP/IP (internetski model) (engl. TCP/IP Reference Model)

Koncept sloja



Primjenit će se terminologija i notacija prema referentnom modelu povezivanja otvorenih sustava koji je normirao ISO (*International Organisation for Standardisation*).

Svaki sloj građen je od elemenata koji se nazivaju entiteti (engl. *entity*). Entitet je aktivni element koji sadrži skup mogućnosti sloja, a funkcija je dio aktivnosti entiteta. Za (N)-sloj to su (N)-entitet i (N)-funkcija.

Koncept sloja uključuje usluge sloja, sučelja sa susjednim slojevima i komunikacijske protokole. Za (N)-sloj to su:

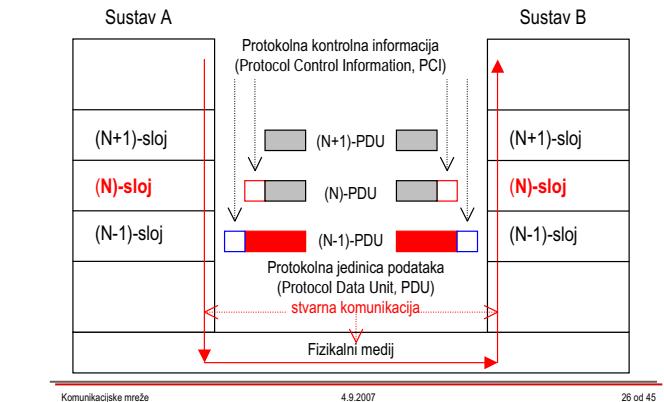
- (N)-usluga
- (N)-SAP
- (N)-protokol

(N)-usluga koju pruža (N)-sloj, definirana je mogućnostima koje (N)-sloj i slojevi ispod njega pružaju (N+1)-sloju.

Sučelje (N+1)-sloja i (N)-sloja definirano je uslužnom pristupnom točkom (N)-SAP u kojoj (N)-uslugu pruža (N)-sloj i slojevi ispod njega, višem (N+1)-sloju.

(N)-protokol određuje pravila i formate komunikacije u (N)-sloju.

Komunikacija između slojeva



26 od 45

Stvarna komunikacija obavlja se vertikalno od najvišeg sloja prema najnižem na prednjoj strani, pa zatim fizičkim medijem do prijamne strane, pa opet vertikalno, od najnižeg prema najvišem sloju.

Svaki sloj stvara protokolnu jedinicu podataka PDU koju predaje nižem sloju. Npr. (N+1)-sloj predaje (N+1)-PDU nižem (N)-sloju. Za (N)-sloj (N+1)-PDU predstavlja njegovu uslužnu jedinicu podataka (engl. *Service Data Unit, SDU*) koju treba poslužiti, (N)-SDU. (N)-sloj dodaje protokolnu kontrolnu informaciju (N)-PCI uslužnoj jedinici podataka (N)-SDU i tako stvara vlastitu protokolnu jedinicu podataka (N)-PDU:

$$(N\text{-SDU}) = (N+1\text{-PDU})$$

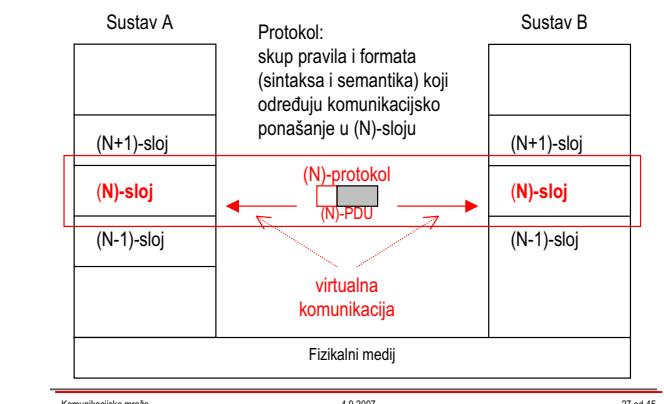
$$(N\text{-PDU}) = ((N\text{-PDU}), (N\text{-SDU}))$$

Treba uočiti da (N)-ti sloj ne zadire u podatke koje je primio od višeg sloja, odnosno (N+1)-PDU, tako da se jedinice podataka između slojeva prenose transparentno.

Na prednjoj strani svaki sloj preuzima protokolnu jedinicu podataka od višeg sloja, dodaje joj vlastitu protokolnu kontrolnu informaciju i prosljeđuje nižem sloju, i tako sve do fizičkog medija kojim se prenose bitovi podataka. Na prijamnoj strani provodi se obrnuti postupak. Svaki sloj prima protokolnu jedinicu podataka od nižeg sloja, obrađuje i oduzima vlastitu protokolnu kontrolnu informaciju i tako sve do najvišeg sloja na kojem je izvodi aplikacija.

Adresa je primjer protokolne kontrole informacije.

Komunikacija unutar sloja



27 od 45

Istovrsni entiteti (engl. *peer*), tj. entiteti unutar svakog sloja međusobno komuniciraju komunikacijskim protokolom. To je virtualna komunikacija koja se ostvaruje skupom pravila i formata koji određuju komunikacijsko ponašanje sloja, a što se naziva protokolom. Npr. u (N)-sloju se komunicira protokolnim jedinicama podataka (N)-PDU prema (N)-protokolu.

Komunikacijski protokol

Skup pravila

- ◆ za postupak izmjene informacije između entiteta u mreži (npr. dva računala, korisničke opreme i pristupnog čvora, dva čvora u mreži, dva korisnika, korisnika i davatelja usluge)
- ◆ kojim se ostvaruje usklađenost predajnog i prijamnog entiteta te
- ◆ zaštita od mogućih pogrešaka u prijenosu i kvarova na sustavima i prijenosnim medijima.

Skup formata

- ◆ jedinice podataka koje služe za izmjenu informacije.

Komunikacijski protokoli razvrstavaju se prvenstveno prema sloju kojem pripadaju. Nadalje, komunikacijski protokoli razlikuju se po dijelu mreže u kojem se primjenjuju (npr. pristupna mreža, lokalna mreža), vrsti informacije kojom se komunicira (npr. korisnička informacija, upravljačka informacija) itd.

Komunikacijskih protokola ima izuzetno mnogo, a konvergencijski procesi u mrežama dovode do smanjenja broja komunikacijskih protokola i razlika među njima.

Spojna usluga

(engl. connection-oriented service)

- ◆ izmjeni jedinica podataka prethodi uspostavljanje veze kojim se određuje put kroz mrežu, a po završetku izmjene podataka veza se prekida
- ◆ sve jedinice podataka izmjenjuju se na isti način koji određuje "veza" (npr. usmjeravaju se istim putem, isporučuju se ispravne u redoslijedu u kojem su poslane i dr.)
- ◆ veza može biti:
 - stvarna,
 - virtualna,
 - logička,
 - ...

Nespojna usluga

(engl. connectionless service)

- ◆ svaka jedinica podataka izmjenjuje se neovisno o ostalima, odnosno usmjerava i isporučuje na odredištu neovisno o ostalima
- ◆ primjer: datagram
 - prenosi se od izvorišta do odredišta (prosljeđuje i usmjerava između čvorova) svaki za sebe
 - ne jamči se isporuka na odredištu
 - ne potvrđuje se primitak na odredištu
 - zaključak: nepouzdana usluga

Kvaliteta usluge
(engl. Quality of Service, QoS)

Funkcije sloja

Svaki sloj treba moći:

- ◆ identificirati pošiljaljca i primatelja s kojima komunicira
- ◆ odrediti smjer prijenosa podataka:
 - jednosmjerno (engl. simplex)
 - dvosmjerno (engl. duplex)
 - naizmjenično, u oba smjera (engl. half-duplex)

Dodatno, sloj može:

- ◆ otkrivati i ispravljati pogreške (kontrola pogrešaka)
- ◆ upravljati tokom podataka (kontrola toka)
- ◆ usmjeravati jedinice podataka i
- ◆ višestruko iskoristiti raspoloživu vezu (engl. multiplex)

Referentni model OSI

7 Aplikacijski sloj, sloj primjene (Application Layer)
6 Prezentacijski/predodžbeni sloj (Presentation L.)
5 Sjednički sloj, sloj sesije (Session Layer)
4 Transportni sloj (Transport Layer)
3 Mrežni sloj (Network Layer)
2 Sloj podatkovne poveznice (Data Link Layer)
1 Fizikalni sloj (Physical Layer)

Ključna riječ u nazivu referentnog modela je „otvoreno“. Naime, pri razradi tog modela cilj je bio predložiti koncepte i rješenja za sustava otvorene za povezivanje s drugim sustavima.

OSI: 1. fizički sloj

Komunikacijski put ostvaren fizičkim medijem između dva ili više fizičkih entiteta

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizički sloj

- jedinica podataka: bit

Osnovne funkcije

- prijenos slijeda bita
- mehaničko, električno/fotoničko i vremensko sučelje s prijenosnim medijem:
 - žični (engl. wired, wireline)
 - optički (engl. fibre optics)
 - bežični (engl. wireless)

OSI: 2. sloj podatkovne poveznice

Komunikacija između dva izravno povezana (susjedna) čvora

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizički sloj

- jedinica podataka: ograničeni niz bita - okvir (engl. frame)

Osnovne funkcije

- prijenos okvira od točke do točke (engl. point-to-point) ili od točke do više točaka (engl. point-to-multipoint)
- kontrola pogrešaka
- kontrola toka

OSI: 3. mrežni sloj

Komunikacija između dva (krajnja) čvora u mreži, izravno ili preko međučvora

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizički sloj

- jedinica podataka: ovisna o vrsti mreže, npr. paket

Osnovne funkcije

- usmjeravanje jedinica podataka
- kontrola pogrešaka
- kontrola toka
- međusobno povezivanje mreža i podmreža

OSI: 4. transportni sloj

Transparentan prijenos s kraja na kraj mreže (engl. end-to-end)

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizički sloj

- jedinica podataka: ovisna o vrsti mreže, npr. paket

Osnovne funkcije

- transportne usluge:
 - prijenos bez pogrešaka (semantička transparentnost)
 - prijenos uz najmanje kašnjenje (vremenska transparentnost)
- kontrola pogrešaka
- kontrola toka

OSI: 5. sjednički sloj

Usklađivanje sustava koji međusobno komuniciraju

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizički sloj

- uspostavljanje, održavanje i prekidanje dijaloga
- dodjela prava za komuniciranje
- nastavljanje komunikacije u slučaju prekida

OSI: 6. prezentacijski sloj

Prikaz (sintaksa) i značenje informacije (semantika) koja se izmjenjuje

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizički sloj

- kodovi
- formati
- struktura podataka

OSI: 7. aplikacijski sloj

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovne poveznice
1 Fizikalni sloj

Aplikacije i usluge za korisnike

- ◆ aplikacijski (računalni) procesi
- ◆ skup protokola za korisničke usluge i aplikacije

TCP
IP

Internetski model, TCP/IP

4 Aplikacijski sloj (Application Layer)

3 Transportni sloj (Transport Layer)

2 Mrežni sloj, internetski sloj (Network Layer, Internet Layer)

1 nije definiran → sloj podatkovnog linka i fizikalni sloj upotrijebljene mreže (pristupa mreži)

Referentni model TCP/IP koji se tako naziva prema dva najvažnija protokola, ima četiri sloja, od kojih najniži nije definiran modelom. Pod tim se slojem podrazumijeva mreža upotrijebljena za izvedbu Interneta (npr. lokalna mreža) ili pristup Internetu (npr. modemski pristup telefonskom mrežom), tako da taj nedefinirani sloj odgovara fizikalnom sloju i sloju podatkovne poveznice.

Internetski model: 2. mrežni/internetski sloj

4 Aplikacijski sloj

3 Transportni sloj

2 Mrežni/internetski sloj

1

- ◆ internetski protokol (Internet Protocol, IP) i dodatni protokoli za usmjeravanje, kontrolu komunikacije i komunikaciju u skupini
- ◆ međusobno povezivanje mreža/podmréža (engl. internetworking)
- ◆ mreža s komutacijom paketa, svaki se paket usmjerava zasebno - datagram
- ◆ IP preko X (IP over X, IPoX)
- ◆ Y preko IP (Y over IP, YoIP)

Protokol IP najvažniji je mrežni protokol. Osim Interneta, cijela klasa mreža zasniva se na njemu (tzv. IP zasnovane mreže), a posebno je važan za konvergenciju mreža. Za IP kao mrežni protokol izvedena su i istražuju se različita rješenja nižeg sloja ("IP preko X"). Isto tako razvijene su i istražuju se različita rješenja za usluge podržane protokolom IP ("Y preko IP").

Internetski model: 3. transportni sloj

4 Aplikacijski sloj

3 Transportni sloj

2 Mrežni/internetski sloj

1

- ◆ transmisijski kontrolni protokol (Transmission Control Protocol, TCP)
 - pouzdana transportna usluga: prijenos bez pogrešaka, uz isporuku potpune informacije u nepromijenjenom redoslijedu
- ◆ Korisnički datagramske protokol (User Datagram Protocol, UDP)
 - jednostavna transportna usluga: prijenos uz najmanje moguće kašnjenje informacije

Internetski model: 4. aplikacijski sloj

4 Aplikacijski sloj

3 Transportni sloj

2 Mrežni/internetski sloj

1

- ◆ aplikacijski protokoli za različite usluge i primjene
- ◆ korisnički, npr.:
 - SMTP (Simple Mail Transfer Protocol): elektronička pošta
 - HTTP (Hyper Text Transfer Protocol): WWW
- ◆ sustavski, npr.:
 - DNS (Domain Name System): sustav imenovanja domena

Usporedba OSI - TCP/IP

7 Aplikacijski sloj

6 Prezentacijski sloj

5 Sjednički sloj

4 Transportni sloj

3 Mrežni sloj

2 Sloj podatkovnog linka/veze

1 Fizikalni sloj

Prezentacijski i sjednički sloj u modelu TCP/IP ne postoje, a njihova funkcionalnost pokrivena je u najvećoj mjeri aplikacijskim slojem.

Središnji slojevi, transportni i mrežni, oba modela podudaraju se, iako ne u potpunosti. Sloj podatkovnog linka i fizikalni sloj nisu obuhvaćeni modelom TCP/IP, ali se mogu pretpostaviti u nedefiniranom sloju ispod mrežnog.

Može se reći da je vrijednost modela OSI veća na teorijskoj i konceptualnoj razini, a modela TCP/IP u primjeni, tako da će se u nastavku detaljnije razradivati TCP/IP.

Odabранe ostale normizacijske organizacije

Svjetske:

International Electrotechnical Commission (IEC)
<http://www.iec.ch>

Europske:

Comité Européen de Normalisation (CEN)
<http://www.cen.eu>

Comité Européen de Normalisation ELECtrotechnique (CENELEC)
<http://www.cenelec.org>

Conférence Européenne des administrations des postes et Télécommunications (CEPT)
<http://www.cept.org>

European Telecommunications Standardisation Institute (ETSI)
<http://www.etsi.org>

Internet i Web:

Internet Society (ISOC)
<http://www.isoc.org>

Internet Architecture Bord (IAB)
<http://www.iab.org>

World Wide Web Consortium (W3C)
<http://www.w3c.org>

Normizacija

International Organisation for Standardisation (ISO)

<http://www.iso.org>

International Telecommunication Union (ITU)

<http://www.itu.int>

ITU-T (International Telecommunication Union - Telecommunications)

CCITT (Comité Consultatif International Télégraphique et Téléphonique) – stari naziv!

Institute of Electrical and Electronics Engineers (IEEE)

<http://www.ieee.org>, <http://standards.ieee.org>

Internet Engineering Task Force (IETF)

<http://www.ietf.org>

Komunikacijske mreže

2.

Fizikalni sloj i
sloj podatkovne poveznice

Sadržaj predavanja



- ◆ Fizikalni sloj
- ◆ Prijenosni medij
- ◆ Sloj podatkovne poveznice



Kako korisnik "vidi" mrežu?

...kroz mogućnost upotrebe informacijskih i komunikacijskih usluga, odnosno aplikacija.

Kvaliteta usluge (engl. Quality of Service, QoS) definirana je kao zajednički učinak **performansa** usluge koji određuje stupanj zadovoljstva korisnika.

Korisnik izražava subjektivni dojam o kvaliteti usluge, npr.:

"slabo te razumijem", "dugo čekam stranicu weba", "datoteka je prenesena jako brzo", "u tekstu ima puno pogrešaka", "glas nije uskladen s otvaranjem usta", "slika je jako dobra", ...

Što su performanse?



Mrežne performanse

- ◆ definirane su kao sposobnost mreže ili dijela mreže da ostvari funkcije potrebne za komunikaciju između korisnika te korisnika i poslužiteljskih sustava.
- ◆ karakterizirane su skupom izračunljivih i mjerljivih parametara, kao što su:
 - širina pojasa
 - propusnost
 - kašnjenje i
 - drugi
- ◆ svaki sloj i njegove performanse utječu na ukupne mrežne performanse

Širina pojasa

engl. bandwidth

B (Hz)

- ◆ širina frekvencijskog pojasa koje se može upotrijebiti za prijenos,
- ◆ fizikalno svojstvo prijenosnog medija, opisano najvišom frekvencijom koja se može prenijeti.

B (bit/s)

- ◆ maksimalni broj bita koji se može prenijeti u jedinici vremena
 - "digitalni" propusni opseg
 - brzina prijenosa bita (engl. bit rate)

Pojam "bandwidth" je vjerojatno jedan od najraznovrsnije upotrebljavanih u informacijskoj i komunikacijskoj tehnologiji (engl. *Information and Communication Technology*, ICT), a i riječ koja se s engleskog prevodi na različite načine.

Izvorno značenje pojma koje potječe iz teorije informacije. Pojam i njegov izravan prijevod "širina pojasa" opisuju frekvencijski pojas (područje frekvencija), označeno s B i mjereno u Hz. Nastao je u doba analognih sustava.

U digitalnom svijetu, a posebice u računalnom, često se isti termin koristi za najveću količinu podataka koju se može prenijeti mrežom ili dijelom mreže i mjeri s bit/s, a naziva se i propusnim opsegom.

Kada se N Hz i N bit/s mogu smatrati istovrsnim mjerama koje opisuju prijenos informacije? Tada kad se po 1 Hz širine pojasa prenosi točno 1 bit podataka!

Propusnost

engl. throughput

(bit/s)

- ◆ broj korisnih bita prenesen u jedinici vremena,
- ◆ manja je od kapaciteta kanala/propusnog opsega/brzine prijenosa bita, jer se uz korisne prenose i dodatni bitovi (ovisno o protokolu i načinu prijenosa)

Teorija informacije

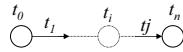
- ◆ kapacitet kanala (bit/s) - najveća brzina prijenosa bita koja ovisi o širini frekvencijskog pojasa te odnosu signal/šum

Kašnjenje

engl. delay, latency

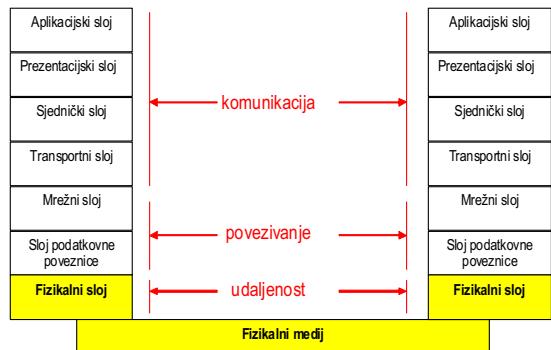
(s)

- vrijeme potrebno da bit s izvora stigne na odredište
- ako se radi o izravnoj vezi, uključuje:
 - vrijeme potrebno za odašiljanje na izvor,
 - vrijeme propagacije prijenosnim medijem (udaljenost/brzina svjetlosti u mediju),
 - vrijeme potrebno za prijam na odredištu.
- ako postoje međučvorovi, dodatno:
 - vrijeme retransmisije, vrijeme čekanja na obradu, i vrijeme obrade u svakom čvoru.



Potrebno je precizno definirati relaciju za koju se izračunava ili mjeri kašnjenje!

Fizikalni sloj (1)



Razrada fizikalnog sloja i sloja podatkovne poveznice zasnivat će se na modelu OSI, jer, kao što je poznato, model TCP/IP ne specificira slojeve ispod mrežnog niti protokole ispod IP.

Svi slojeviti modeli rješavaju, odozgo prema dolje, probleme komunikacije između različitih entiteta, njihovog povezivanja te udaljenosti između njih.

Zadaća fizikalnog sloja je "premostiti udaljenost".

Fizikalni sloj (2)

Zadaća fizikalnog sloja:

- prijenos slijeda bita fizikalnim medijem
- jedinica podataka: bit
- mehaničko, električko/optičko i vremensko sučelje s prijenosnim medijem
- omogućiti komunikaciju na daljinu

Prijenos informacije:

- električki
- optički (fotonički)

Prijenos bita

Signalna domena prijenosa informacije:

- **izvor:** pretvorba digitalnog signala – bita – u signalne elemente prilagođene uvjetima prijenosa (modulacija kodiranje),
- **prijenos** fizikalnim medijem, uz moguće djelovanje smetnji koje izazivaju pogreške,
- **odredište:** pretvorba primljenih signalnih elemenata (demodulacija, dekodiranje) u digitalni signal – bit

Teorija informacije!

Oblikovanje fizikalnog linka

Na brzinu prijenosa i domet utječu:

- širina prijenosnog pojasa B (Hz)
- izobličenja u prijenosu (gušenje signala),
- interferencija (smetnje od vlastitog ili drugih signala),
- broj prijamnika (prigušenje i izobličenje signala).

Kapacitet komunikacijskog kanala određuju:

- širina prijenosnog pojasa B
- odnos signal – šum S/N

Fizikalni medij

Prijenosni mediji (engl. transmission media)



Parica (1)

engl. pair



- ♦ dva bakrena vodiča promjera do 1 mm koji su upredeni kako bi se smanjio međusobni elektromagnetski utjecaj
- ♦ upredena parica (engl. twisted pair)
- ♦ neoklopljena upredena parica (engl. Unshielded Twisted Pair, UTP)
- ♦ jako rasprostranjena, prikladna i za analogni i za digitalni prijenos

Primjer primjene parice za analogni prijenos je priključak telefonskog aparata na lokalnu centralu (engl. *local exchange*) javne komutirane telefonske mreže (engl. *Public Switched Telephone Network*, PSTN). To je ujedno jedini dio telefonske mreže s analognim prijenosom, sve ostalo riješeno je digitalno.

Tom istom paricom može se ostvariti digitalni prijenos, što se u sve većoj mjeri i provodi. Primjeri digitalizacije pretplatničke linije su digitalna mreža integriranih usluga (engl. *Integrated Services Digital Network*, ISDN) i asimetrična digitalna pretplatnička linija (engl. *Asymmetric Digital Subscriber Line*, ADSL).

Uz javnu mrežu, parica se takođe primjenjuje u lokalnim mrežama.

Koju su razlozi velike primjene parice danas?

Parica (2)

Brzina prijenosa ovisi o:

- ♦ debljini žice,
- ♦ duljini žice,
- ♦ načinu upredanja,
- ♦ načinu slaganja parica u kabel.

Kategorija parice ("CAT") – klasifikacija prema postizivoj brzini prijenosa (npr. CAT 5 – primjena u LAN-ovim do 100 Mbit/s)

Primjer ADSL:

- ♦ maksimum: ili brzina (u dolaznom smjeru 8 Mbits, u odlaznom 640 kbits) ili udaljenost (5486 m) – obrnuto proporcionalno!
- ♦ RH: dobra izvedba - u gradovima duljina parice do 1km

Najveća postiziva brzina prijenosa ovisi o fizikalnim svojstvima upredene parice. Na brzinu prijenosa najviše utječe prigušenje i preslušavanje, koji rastu s porastom frekvencije. Stoga se na višim frekvencijama moraju koristiti kabeli boljih karakteristika.

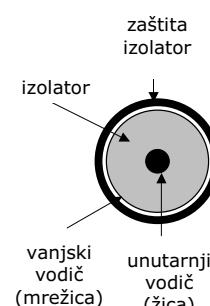
ANSI/EIA standardi specificiraju kategorije (engl. category, od čega skraćeno "CAT" kao oznaka kategorije) paričnih sustava kabliranja (ozičenje, konektori, spojevi) prema brzini prijenosa signala koju garantirano podržavaju.

Na primjer, CAT 5 se testira na frekvenciji do 16 MHz, CAT 5/5e na 100 Mhz, CAT 6 na 200 Mhz.

Danas najviše korištena kategorija je CAT 5 UTP, za uporabu u lokalnim mrežama brzine do 100 Mbit/s, te u novijim instalacijama poboljšana inačica CAT 5e za Gigabit Ethernet LAN (brzine do 1000 Mbit/s).

Koaksijalni kabel

engl. coaxial cable coax



- ♦ velika širina pojasa i dobra zaštita od smetnji, ali
- ♦ lošije performanse od svjetlovodnih niti koje su ih istisnula iz uporabe
- ♦ primjena: kabelska TV

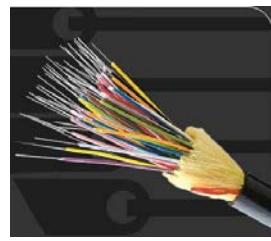
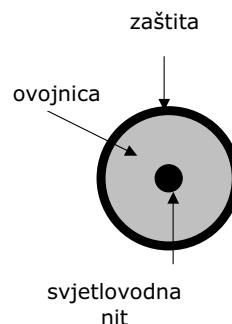
Koaksijalni kabeli su se ranije primjenjivali u lokalnim mrežama sabirničke topologije. Npr. prva lokalna mreža koja je u ranim 80-tima prošlog stoljeća pokrivala zgrade FER-a imala je koaksijalni kabel za prijenosni medij.

U Hrvatskoj se u gradskim mrežama, kao i između gradova, ne primjenjuju koaksijalni kabeli. Od početka 90-tih prošlog stoljeća zamjenili su ih optički kabeli.

(fotografija koaxa preuzeta s www.radioinc.com)

Svetlovodna nit (1)

engl. fibre fiber optics

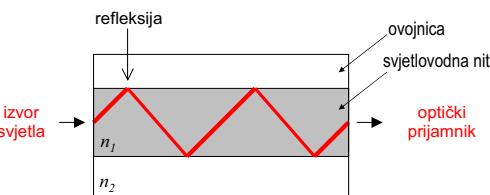


- svjetlovodna nit i ovojnica: staklo
- kabel sa svjetlovodnim nitima (engl. fibre optic cable), optički kabel sadrži više niti

Uz staklene niti, u primjeni su i optički kabeli s plastičnim nitima, slabijih performansa od staklenih.

(fotografija optičkog kabela preuzeta s: www.occfiber.com)

Svetlovodna nit (2)



- indeks loma ovojnice manji od indeksa loma niti kako bi se svjetlost zadržala u niti ($n_1 > n_2$)
- višemodna nit (engl. multimode fibre): više zraka svjetla, odbijanje
- jednomodna nit (engl. single-mode fibre): kad promjer niti nije veći od nekoliko valnih duljina svjetlosnog signala, može se postići propagacija svjetla na jedan način (mode), jednom zrakom

Skica prikazuje lom zrake svjetla kod propagacije u višemodnoj niti.

Predajnik: dioda LED (*Light Emitting Diode*), poluvodički laser

Prijamnik: fotodioda

Uz jednomodne, postoje i višemodne niti (engl. *multi-mode fibre*) slabijih karakteristika (veće prigušenje signala, manja brzina prijenosa).

Usporedba svjetlovodna nit - bakar (1)

Prednosti svjetlovodne niti:

- veća brzina prijenosa (Gbit/s, Tbit/s)
- malo prigušenje signala, tako da se obnavljanje signala provodi na većim udaljenostima, od nekoliko desetaka do iznad sto kilometara (npr. za jednomodnu nit s 50 Gbit/s na 100 km)
- neosjetljivost na elektromagnetske utjecaje i koroziju,
- tanka i lagana,
- prisluškivanje teško izvedivo.

Usporedba svjetlovodna nit - bakar (2)

Nepovoljne strane svjetlovodne niti:

- inherentno jednosmjerni prijenos, tako da su potrebne dvije niti za dvosmjerni prijenos,
- optička sučelja složenija i skuplja od električnih,
- instrumentarij za izvedbu i održavanje mreža složeniji i skuplji.

Usporedba svjetlovodna nit - bakar (3)

Propagacijsko kašnjenje – mala razlika

$$D = d/c$$

d udaljenost (m)

c brzina svjetlosti u mediju (m/s)

bakreni vodič: $c = 2,3 \times 10^8$ m/s

optička nit: $c = 2 \times 10^8$ m/s

Primjeri:

■ optičkom niti 1 km: 5 μs

■ optičkom niti Zagreb – Split: 2 ms

■ optičkom niti oko zemlje: 0,2 s

■ Koliko će trajati prijenos 1Gbita podataka iz Zagreba u Split optičkim sustavom koji osigurava propusnost od 1Gbit/s?

Optički kabeli – nacionalna razina RH



Uz prstene nacionalne razine predočene slikom, izvedeni su i prteni regionalne (županijske razine) te gradski prsteni. Na relacijama s velikim informacijskim prometom za koje postoji veliki komercijalni interes (npr. Zagreb – Rijeka) izgrađeni su paralelni sustavi.

Radijski prijenos

- prijenos informacije elektromagnetskim valom u prostoru u definiranom dijelu **radiofrekvencijskog spektra**
- prednost pred infracrvenim (domet, usmjerenost, od točke do točke) i laserskim prijenosom (osjetljivost na atmosferske utjecaje)
- primjena u mreži:
 - pristup korisnika javnoj pokretnoj mreži,
 - pristup korisnika lokalnoj mreži,
 - povezivanje dvaju točaka (npr. usmjereni mikrovalna veza).

Radijski prijenos je jedna vrsta bežičnog prijenosa, koja se temelji na prijenosu informacije elektromagnetskim valom u prostoru u definiranom dijelu **radiofrekvencijskog spektra**.

Radiofrekvencijskim spektrom naziva se raspon frekvencija od 9 kHz do 300 GHz.

Osim radijskog prijenosa, postoje i druge bežične tehnologije, kao što su, na primjer, infracrvene veze i optičke veze. (I kod tih tehnologija se informacija prenosi elektromagnetskim valom, ali na frekvencijama iznad onih u radiofrekvencijskom spektru!).

Radiofrekvencijski spektar, od samih početaka primjene, služi kao osnova za usluge utemeljene na razaziljanju (radio i televizija), radar, te pokretne i satelitske komunikacije. S izuzetnim porastom broja korisnika pokretne telefonije te pojmom sasvim novih usluga koje koriste spektar (na primjer, lokacijske usluge), potražnja za spektrom je u velikom porastu.

Na primjer, za pokretne mreže koriste se radio signali u rasponu frekvencija od 450 MHz do 2.2 GHz (v. slide 24).

Naziv „mikrovalne veze“ odnosi se na komunikaciju radio valovima frekvencije iznad 1 GHz.

Primjer: Dodjela frekvencija unutar radiofrekvencijskog spektra u SAD

<http://www.ntia.doc.gov/osmhome/allocchart.pdf>

Radiofrekvenčijski spektar (1)

- ♦ upravljanje radiofrekvenčijskim spektrom:
 - međunarodni dogovor i nacionalna provedba kojom rukovodi regulatorno tijelo (Hrvatska agencija za telekomunikacije),
 - ograničeni resurs koji ograničava i broj bežičnih mreža,
- ♦ uporaba dijela radiofrekvenčijskog spektra uz naplatu, npr.:
 - javne pokretne mreže (GSM, UMTS), bežične pristupne mreže
- ♦ slobodna uporaba dijela radiofrekvenčijskog spektra, npr.:
 - bežični telefon (DECT)
 - bežična lokalna mreža u pojasu ISM (Industrial Scientific Medical)

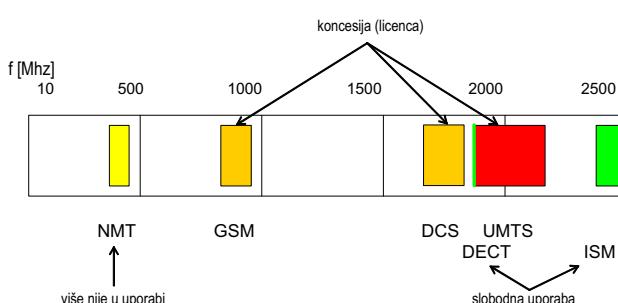
Radiofrekvenčijski spektar je ograničeni resurs, što proizlazi iz fizičkih karakteristika radijskog prijenosa.

Kako se radijski val širi bez umjetnog vodenja, kod pojave više istovremenih radijskih signala na istoj frekvenciji dolazi do *interferencije*, odnosno štetnog međudjelovanja s posljedicom slabljenja i poništavanja korisnog signala. Radi izbjegavanja interferencije javlja se potreba uvođenja *upravljanja spektrom*, odnosno planske i namjenske dodjele frekvencija.

Upravljanje spektrom provodi se na dvije razine: 1) međunarodna dodjela spektra po rasponima za definirane usluge; i 2) nacionalna dodjela licenci koju provodi nacionalno regulacijsko tijelo, pri čemu je takva licenca korisniku daje pravo isključivog rada putem određenih frekvencija unutar dodjeljenog raspona.

Upravljanje spektrom na međunarodnoj razini provode organizacija ITU, odnosno njen sektor radiokomunikacija, ITU-R. Unutar dijela radiofrekvenčijskog spektra pogodnog za komunikaciju, ITU-R definira 40-tak "blokova", koji se nazivaju frekvencijskim pojasevima, i njihovu namjenu uslugama koje se koriste širom svijeta (npr. radiodifuzija, radionavigacija, amaterski radio, pokretna mreža, radioastronomija, itd.).

Radiofrekvenčijski spektar (2)



Operatori pokretne mreže upotrebljavaju za to namijenjeni dio radiofrekvenčijskog spektra uz naplatu, temeljem koncesije (licence).

Javne pokretne mreže, po generacijama (G) sustava su sljedeće:

1G: NMT (*Nordic Mobile Telephony*),

2G: GSM (*Global System for Mobile communications*) i

DCS (*Digital Communication System*),

3G: UMTS (*Universal Mobile Telecommunication System*)

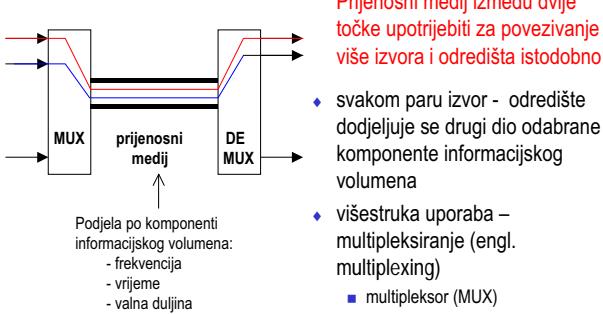
Slobodna uporaba radiofrekvenčijskog spektra:

- 1880-1900 MHz: bežični telefon (DECT – *Digital Enhanced Cordless Telecommunications*, 1880-1900 MHz) i

- 1880-1900 MHz (ISM): industrijske, znanstvene i medicinske primjene, te bežične lokalne mreže, Bluetooth i sl.

Slobodna uporaba frekvencijskog spektra pretpostavlja poštivanje tehničkih parametara kao što su snaga signala i domet.

Višestruka uporaba prijenosnog medija



Osnovni načini višestruke uporabe prijenosnog medija su:

• frekvenčijska podjela

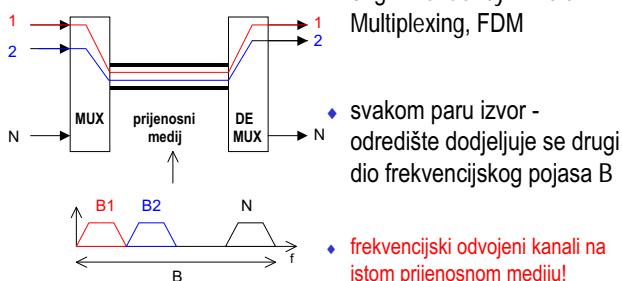
• vremenska podjela

• valna podjela

Uz frekvenčijsku, vremensku i valnu podjelu, istražuju se primjenjuju se i drugi načini višestrukog iskorištenja prijenosnog medija, posebice u radijskim komunikacijama.

Multiplexiranje u frekvenčkoj podjeli

engl. Frequency Division Multiplexing, FDM

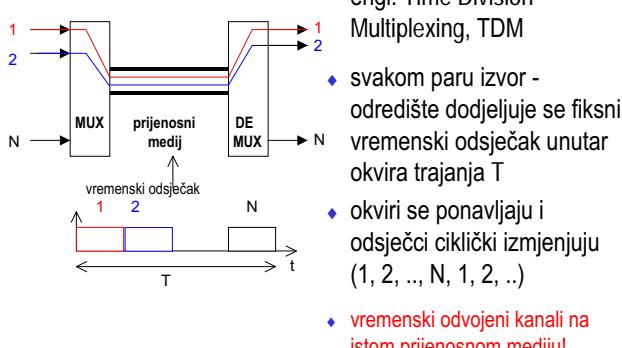


- svakom paru izvor - odredište dodjeljuje se drugi dio frekvenčkog pojasa B
- frekvenčki odvojeni kanali na istom prijenosnom mediju!

Frekvenčka podjela imala je puno veću primjenu u analognim sustavima, nego što je ima danas.

Multiplexiranje u vremenskoj podjeli

engl. Time Division Multiplexing, TDM



- svakom paru izvor - odredište dodjeljuje se fiksni vremenski odsječak unutar okvira trajanja T
- okviri se ponavljaju i odsječci ciklički izmjenjuju (1, 2, .., N, 1, 2, ..)
- vremenski odvojeni kanali na istom prijenosnom mediju!

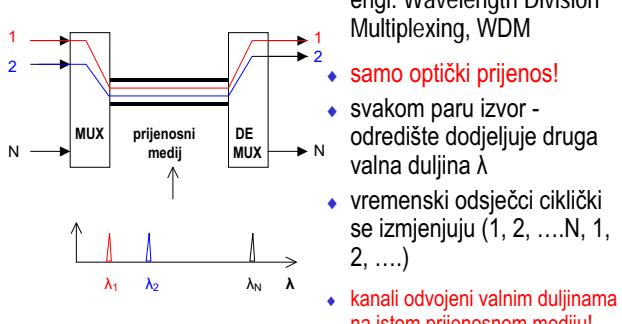
Uz multipleksiranje u vremenskoj podjeli s fiksnom dodjelom vremenskih odječaka, primjenjuje se i dinamičko ili statističko multipleksiranje (engl. statistic multiplexing).

Kod fiksne vremenske podjele, vremenski odsječak ostaje dodijeljen tijekom komunikacije neovisno o tome ima li podataka na izvoru ili ne, što karakteristično za mreže s komutacijom kanala kao što je telefonska.

Statističko multipleksiranje vodi računa o količini podataka, te više odsječaka dodjeljuje prometno jačem izvoru, što je primjerenoje komunikaciji podacima između računala.

Multiplexiranje u valnoj podjeli

engl. Wavelength Division Multiplexing, WDM



- samo optički prijenos!
- svakom paru izvor - odredište dodjeljuje druga valna duljina λ
- vremenski odsječci ciklički se izmjenjuju (1, 2, ..., N, 1, 2, ...)
- kanali odvojeni valnim duljinama na istom prijenosnom mediju!

gusta podjela valnih duljina (engl. Dense Wavelength Division Multiplexing, DWDM): razmak valnih duljina do 0,1 nm

Primjer transmisijskog sustava: PCM

Pulsno kodna modulacija

(engl. Pulse Code Modulation, PCM)

- ♦ osnovna primjena: digitalizacija govora u telefonskoj mreži
 - govor: analogni signal 300 – 3400 Hz ($B = 4$ kHz)
 - uzimanje uzorka frekvencijom $2B = 8$ kHz, tj. svakih 125 μ s, kodiranje svakog uzorka s 8 bita, što daje $8 \times 8 = 64$ kbit/s
- ♦ okvir:
 - trajanje 125 μ s
 - 32 kanala: 30 govornih
 - 1 sinkronizacijski (usklađivanje predajnika i prijamnika)
 - 1 signalizacijski (pozivni broj, stanje poziva, ...)
 - kapacitet: $32 \times 64 = 2048$ kbit/s = 2,048 Mbit/s ← “2 Mbit/s”

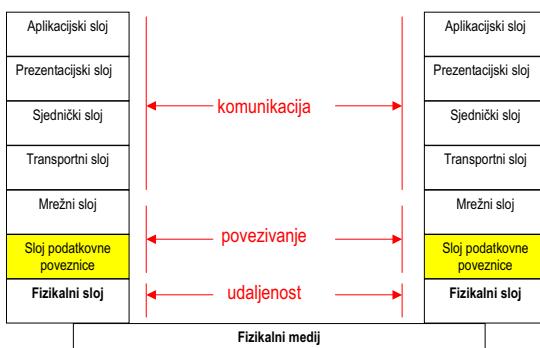
Primjer transmisijskog sustava: SDH

Sinkrona digitalna hijerarhija

(engl. Synchronous Digital Hierarchy, SDH)

- ♦ prijenos bita u ekstremno točnim trenucima (usklađenost predajnika i prijamnika) upravljan glavnim satom točnosti 10^9 (atomski sat)
- ♦ mogućnost multipleksiranja kanala različitih kapaciteta
- ♦ okvir:
 - sinkroni transportni modul (engl. Synchronous Transport Module, STM)
 - u RH su u primjeni STM-1 (155 Mbit/s), STM-4 (620 Mbit/s) i STM-16 (2500 Mbit/s)

Sloj podatkovne poveznice



Razrada fizičkog sloja i sloja podatkovne poveznice zasnovat će se na modelu OSI, jer, kao što je poznato, model TCP/IP ne specificira slojeve ispod mrežnog niti protokole ispod IP:

Kao što je već rečeno, slojeviti modeli rješavaju, odozgo prema dolje, probleme komunikacije između različitih entiteta, njihovog povezivanja te udaljenosti između njih. Zadaća sloja podatkovne poveznice je “povezivanje”, a time se u širem kontekstu bavi još mrežni sloj.

Oblikovanje podatkovnog linka (1)

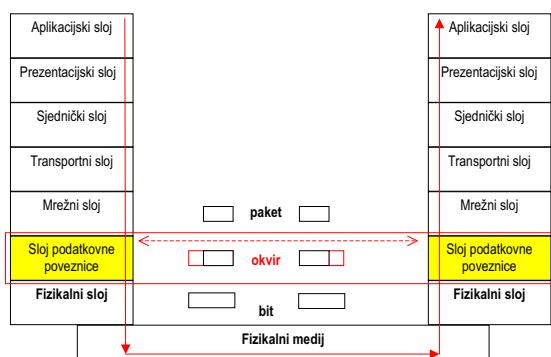
Zadaća:

- ♦ omogućiti povezivanje te učinkovitu i pouzdanu komunikacija između dva susjedna (izravno povezana) čvora:
 - pružanje usluge mrežnom sloju,
 - obrada pogrešaka u prijenosu,
 - upravljanje tokom podataka.
- ♦ jedinica podataka: okvir (engl. frame)

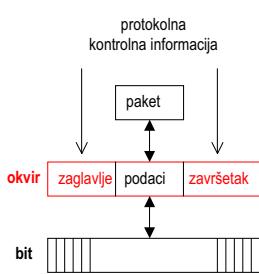
Problemi:

- ♦ konačni kapacitet, kašnjenje, djelovanje smetnji koje izazivaju pogreške bita, kvarovi,

Oblikovanje podatkovnog linka (2)



Okvir



Sadržaj okvira:

- ◆ polje za podatke (engl. payload)
- ◆ polja s kontrolnom informacijom:
 - ispred polja s podacima: zaglavje (engl. header)
 - iza polja s podacima: završetak (engl. trailer)
- ◆ u polje za podatke smješta se protokolna jedinica sloja mreže – paket

Formiranje okvira

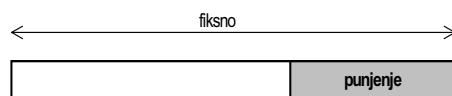
Duljina okvira:

- ◆ fiksna, utvrđena unaprijed
- ◆ varijabilna, zbog varijabilnog polja za podatke pri čemu je utvrđena najveća moguća duljina

Veličina polja podataka:

- ◆ veća ili jednaka mrežnoj jedinici podataka: mrežna jedinica podataka se smješta u okvir
- ◆ manja od mrežne jedinice podataka: mrežna jedinica podataka se dijeli na više manjih dijelova (fragmenata, segmenata) koji se smještaju svaki u poseban okvir

Fiksna duljina okvira

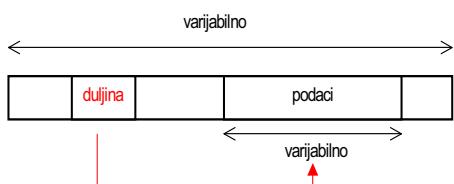


Ukoliko su podaci koji se prenose (tj. mrežna jedinica podataka) kraći od duljine okvira, dodaje se tzv. punjenje (engl. filler) do pune duljine okvira

Primjer:

- sloj podatkovne poveznice na radijskom sučelju mreže GSM

Varijabilna duljina okvira – brojanje znakova

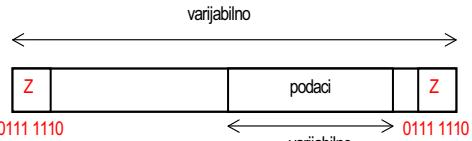


Varijabilno je najčešće samo polje podataka, tako da se u zaglavju specificira broj znakova, pa prijamnik može odrediti kraj okvira.

Primjer:

- lokalna mreža IEEE 802.3

Varijabilna duljina okvira – označavanje granice



Označavanje početka i kraja posebnim znakom – zastavicom (engl. flag)

- ◆ opasnost: kombinaciju bita u polju podataka koja odgovara zastavici prijamnik će prepoznati kao kraj okvira
- ◆ rješenje: ubacivanje dodatnog bita (engl. bit stuffing) nakon 11111 u predajniku i njegovo izbacivanje u prijamniku

Primjer:

- protokoli vrste HDLC (High-level Data Link Control)

Primjer 1 (11111):

Predajnik: 0001001**1111**0101 (ubacuje 1 iza 11111)

Fizikalni medij: 0001001**1111**0101

Prijamnik: 0001001**1111**0101 (izbacuje 1 iza 11111)

Primjer 2 (111111):

Predajnik: 0001001**11111**0101 (ubacuje 1 iza 111111)

Fizikalni medij: 0001001**111110**0101

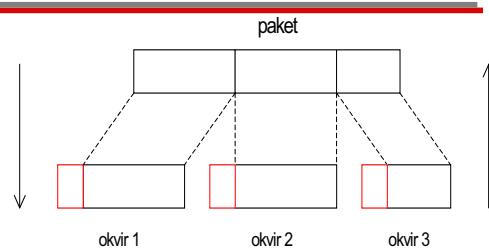
Prijamnik: 0001001**11111**0101 (izbacuje 1 iza 111111)

Primjer 3: polje podataka sadrži same "1". Kako će izgledati slijed bita na fizikalnom mediju?

Primjer 4: zbog djelovanja smetnji u prijenosu nastane 111111. Što će se dogoditi na prijamnoj strani?

Primjer 5: zbog djelovanja smetnji dolazi do pogreške na zastavici, npr. 01110110. Što će se dogoditi na prijamnoj strani?

Fragmentiranje



Na prednjoj strani se paket dijeli na fragmente, a svaki fragment prenosi posebnim okvirom.

Na prijamnoj se strani iz primljenih okvira sastavlja paket.

Sljedeći put

komunikacijski protokoli i usluge

sloja podatkovne poveznice

Komunikacijske mreže

3.

Komunikacijski protokoli
podatkovne poveznice

Sadržaj predavanja

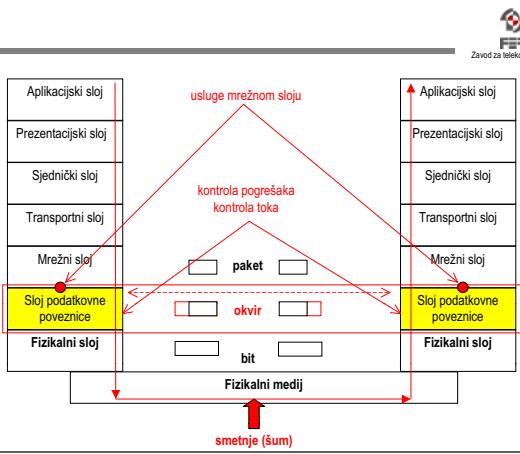
- ◆ Usluge sloja podatkovne poveznice (mrežnom sloju)
- ◆ Kontrola pogrešaka
- ◆ Kontrola toka
- ◆ Komunikacijski protokoli podatkovne poveznice

Podsjetimo se

- Zadaća sloja podatkovne poveznice:
- ◆ omogućiti povezivanje te učinkovitu i pouzdanu komunikaciju između dva susjedna (izravno povezana) čvora:
 - pružanje usluge mrežnom sloju,
 - obrada pogrešaka u prijenosu,
 - upravljanje tokom podataka.

Problemi:

- ◆ konačni kapacitet, kašnjenje, djelovanje smetnji koje izazivaju pogreške bita, kvarovi,



Komunikacijski protokol

Skup pravila i formata za postupak izmjene informacije između entiteta u mreži kojim se ostvaruje usklađenost prednjog i prijamnog entiteta te zaštita od mogućih pogrešaka u prijenosu i kvarova na sustavima i prijenosnim medijima.

Usluge sloja podatkovne poveznice

Vrste usluga s obzirom na način izmjene jedinice podataka:

- ◆ nespojna
- ◆ spojna

Vrste usluga s obzirom na potvrdu prijama:

- ◆ bez potvrde
- ◆ s potvrdom

Nespojna usluga bez potvrde

engl. unacknowledged connectionless service

Opis usluge:

- ◆ izvor šalje neovisne okvire (nema logičke veze)
- ◆ odredište ne potvrđuje prijam – **gubitak okvira moguć!**

Primjena:

- ◆ prijenos podataka uz malu vjerojatnost pogreške bita (npr. u lokalnoj mreži),
- ◆ komunikacija u stvarnom vremenu (npr. prijenos digitaliziranog govora)

Nespojna usluga s potvrdom

engl. acknowledged connectionless service

Opis usluge:

- ◆ izvor šalje neovisne okvire (nema logičke veze)
- ◆ odredište potvrđuje prijam svakog okvira zasebno
- ◆ ukoliko ne primi potvrdu, izvor ponovno šalje okvir – retransmisijska (engl. retransmission)

Primjena:

- ◆ prijenos s jako izraženim smetnjama (npr. bežični)

Spojna usluga s potvrdom

engl. acknowledged connection-oriented service

Opis usluge:

- ◆ uspostavljanje logičke veze između izvora i odredišta prethodi izmjeni okvira, nakon čega se veza prekida
- ◆ svaki okvir označava se brojem kako bi se moglo jamčiti da će:
 - svaki okvir biti primljen samo jednom
 - svi okviri biti primljeni u ispravnom redoslijedu

Primjena:

- ◆ zahtijeva se visoka pouzdanost

Kontrola pogrešaka

engl. error control

Problem:

- djelovanje smetnji izaziva pogreške bita ($0 > 1, 1 > 0$)
- pogreške su slučajne, a događaju se pojedinačno ili u snopu (engl. burst), tj. skupini bita u nizu
- mjera kvalitete digitalnog prijenosa
učestalost pogreške bita (engl. Bit Error Rate, BER), 10^{-n}
- npr. kod optičkog prijenosa zahtjeva se $BER = 10^{-9}$, što znači da broj neispravnih bita ne smije biti veći od jednog na svakih 10^9

Zaštitno kodiranje (1)

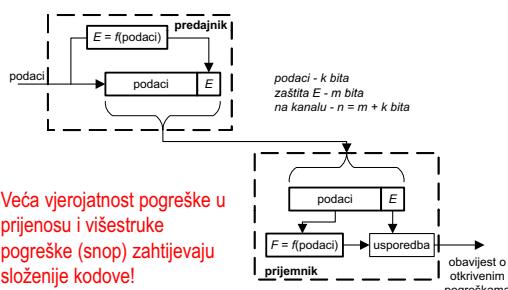
Komunikacija se nikad ne odvija u idealnim uvjetima tako da se pogreške u prijenosu ne mogu isključiti. Zaštitno kodiranje pretpostavlja je za **kontrolu pogrešaka**, tj. smanjenje broja pogrešno isporučenih bita na odredištu.

Zaštitno kodiranje omogućuje:

- otkrivanje pogrešaka
- ili
- ispravljanje pogrešaka

Kodiranjem se bavi Teorija informacije!

Zaštitno kodiranje (2)



Kad se primjenjuje zaštitno kodiranje, zaštita (E) se smješta u protokolnu kontrolnu informaciju (PCI).

Otkrivanje pogrešaka

engl. error detection

Postupak:

- predajnik kodira podatke
- prijamnik dekodira podatke i **otkrije** pogreške
- ispravljanje pogreške unatrag (engl. Backward Error Correction, BEC): prijamnik dojavljuje pogrešku **predajniku** koji ponavlja prijenos i tako **ispravlja** pogrešku

Primjena:

- u većini mreža (jednostavnija izvedba)
- primjer: paritetni bit (otkrivanje pojedinačne pogreške), ciklički kod

U većini mreža primjenjuje se otkivanje pogrešaka na odredištu i ispravljanje pogrešaka unatrag, ponavljanjem okvira, a provodi se relativno jednostavnim kodovima (npr. cikličkim), s umjerenim brojem zaštitnih bita, npr. 16. Naime, dobro izvedeni žični i optički prijenos, neće biti izložen takvim smetnjama koje bi onemogućile postizanje prihvatljive učestalosti pogreške bita.

Ispravljanje pogrešaka

engl. error correction

Postupak:

- ◆ predajnik kodira podatke
- ◆ prijamnik dekodira podatke, otkriva pogrešku i mjesto pogreške te je **ispravlja** - ispravljanje pogreške unaprijed (engl. forward Error Correction, FEC)

Primjena:

- ◆ teški/teži uvjeti prijenosa, smanjenje retransmisije (npr. Bluetooth, vozilo na Marsu)
- ◆ primjer: Hammingov kod (ispravljanje pojedinačne pogreške), konvolucijski kodovi

Kodovi za ispravljanje pogrešaka znatno su složeniji od onih koji ih samo ispravljaju. Usporedite paritetni bit i Hammingov kod!

Ispravljanje pogrešaka ponovnim prijenosom okvira nije učinkovito u slučaju kad je veća vjerojatnost pogreške bita, jer će retransmisija biti učestala. Isto tako, povećat će se kašnjenje isporuke okvira na odredištu.

Takve su situacije karakteristične za bežični prijenos.

Takov je primjer i prijenos na malim udaljenostima (do 100 m) kakav omogućuje Bluetooth na pokretnim telefonima i ručnim računalima koji se provodi u frekvencijskom području u kojem slobodno komuniciraju različiti uređaji ISM Industrial, Scientific, Medical) i međusobno se ometaju. Stoga se primjenjuje FEC.

Kod komunikacija s vozilom na Marsu, BER bi povećao ionako veliko kašnjenje!

Kontrola pogrešaka na podatkovnoj poveznici

Pogreška:

- ◆ oštećeni okvir (engl. damaged frame): okvir dolazi na odredište, ali su neki od njegovih bita pogrešni
- ◆ izgubljeni okvir (engl. lost frame): okvir koji ne stiže na odredište

Najčešće - ispravljanje pogrešaka unatrag:

- ◆ izvor mora saznati što se događa u prijenosu i na odredištu:
 - pozitivna potvrda: primljeni okvir ispravan
 - negativna potvrda: primljeni okvir s pogreškom
 - bez potvrde: ?

Ograničiti čekanje na potvrdu!

Postupak ispravljanja pogreške unatrag (1)

Osnovni mehanizmi:

- ◆ predajnik:
 - šalje okvir, postavlja vremensku kontrolu i čeka potvrdu odaslanog okvira,
 - zaustavlja vremensku kontrolu po prijemu potvrde,
 - ponavlja okvir ako je potvrda negativna (primljeni okvir s pogreškom) ili ako je istekla vremenska kontrola (izgubljeni okvir ili potvrda).
- ◆ prijamnik:
 - potvrđuje ispravan/neispravan prijem okvira predajniku.

Primjer 1

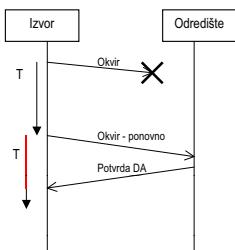
- ◆ prijenos okvira bez pogreške (DA - pozitivna potvrda ispravnog okvira)
- ◆ prijenos okvira s pogreškom (NE - negativna potvrda oštećenog okvira)
- ◆ retransmisija okvira

Prikaz:

slijedni dijagram
(engl. sequence diagram)

Slijedni dijagram jedan je od dijagrama definiranih jezikom UML (Unified Modelling Language).

Primjer 2



- ◆ izgubljeni okvir
- ◆ retransmisijska okvira nakon isteka vremenske kontrole T za prijem potvrde

Dodatni primjer:

Prijenos okvira proveden je uspješno, bez pogreške, a prijamnik je vratio pozitivnu potvrdu ispravno primljenog okvira (DA).

Ta potvrda je izgubljena tijekom prijenosa.

Kako će se dalje odvijati komunikacija? Rješenje prikažite odgovarajućim slijednjim dijagramom.

Postupak ispravljanja pogreške unatrag (2)

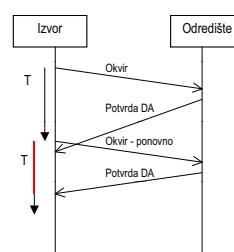
Vremenska kontrola:

- ◆ određuje se kao očekivano vrijeme potrebno da okvir dođe do odredišta i vrati se potvrda:
 - prekratka vremenska kontrola dovodi do prerane retransmisijske okvira koji je primljen ispravno, a time i do dvostrukog (višestrukog) prijema istog okvira
 - preduga vremenska kontrola dovodi do slabe iskoristivosti komunikacijskih resursa

Višestruki prijam okvira:

- ◆ može se spriječiti numeracijom okvira slijednim brojem (engl. sequence number) koji omogućuje prijemniku izbacivanje okvira koji su primljeni više puta

Primjer 3



- ◆ prijenos okvira bez pogreške (pozitivna potvrda ispravnog okvira)
- ◆ istek vremenske kontrole prije primanja potvrde
- ◆ retransmisijska okvira nakon isteka vremenske kontrole T za prijem potvrde
- ◆ **dvostruki prijem istog ispravnog okvira!**

Kontrola toka

engl. flow control

Izvor ne smije slati podatke brže nego ih odredište može primati:

- ◆ preopterećeni prijemnik prestaje primati podatke, što se očituje kao gubitak okvira
- ◆ treba ograničiti broj odaslanih, a nepotvrđenih okvira

Osnovni mehanizam:

- ◆ kontrola toka zasnovana na povratnoj vezi
 - prijemnik daje predajniku dopuštenje za odašiljanje podataka

Komunikacijski protokoli (1)

Skup pravila i formata za postupak izmjene informacije između entiteta u mreži kojim se ostvaruje usklađenost predajnog i prijamnog entiteta te zaštita od mogućih pogrešaka u prijenosu i kvarova na sustavima i prijenosnim medijima.

U sloju podatkovne poveznice:

- izmjena okvira
- kontrola pogrešaka
- kontrola toka

Komunikacijski protokoli podatkovne poveznice uvode načela koja se primjenjuju i na višim slojevima!

Kontrola pogrešaka i kontrola toka mogu se provoditi i provode se i na višim slojevima, od mrežnog pa na više, za jedinice podataka koje se izmjenjuju na odgovarajućem sloju.

Komunikacijski protokoli (2)

- ◆ Komunikacijski protokoli podatkovne poveznice mogu omogućiti transparentan prijenos:
 - znakova (okteta), npr. ASCII znakova
oktet-orientirani protokol (engl. byte-oriented protocol)
ili
 - bilo kakve kombinacije bita
bit-orientirani protokol (engl. bit-oriented protocol)
što je važnije za mreže!

Osnovni modeli protokola

- ◆ Jednosmjerni protokol bez ograničenja
- ◆ Jednosmjerni protokol "Stani i čekaj"
- ◆ Jednosmjerni protokol za kanal sa smetnjama (ARQ, PAR)
- ◆ Dvosmjerni protokol za kanal sa smetnjama

Pojam jednosmjernog protokola odnosi se na prijenos okvira koji sadrže podatke u jednom smjeru, od izvora (Sustav A) do odredišta (Sustav B). Pritom se u suprotnom smjeru (od Sustava B prema Sustavu A) mogu prenositi kontrolni okviri, odnosno okviri koji sadrže samo protokolnu kontrolnu informaciju (PCI), npr. potvrdu primitka okvira.

Dvosmjerni protokol omogućuje izmjenu okvira s podacima u oba smjera (od Sustava A prema Sustavu B i od Sustava B prema Sustavu A), tj. i u Sustavu A i u Sustavu B nalaze se predajnici i prijamnici okvira.

Jednosmjerni protokol bez ograničenja

engl. Unrestricted Simplex Protocol

Idealizacija:

- ◆ jednosmjerni tok podataka (jednosmjerni kom. kanal)
- ◆ predajnik i prijemnik uvijek spremni
- ◆ obrada beskonačno brza
- ◆ spremnici beskonačni
- ◆ prijenos bez pogrešaka

Način rada: predajnik stalno šalje okvire, a prijemnik ih prima bez ograničenja.

Tannenbaum: utopijski protokol!

Jednosmjerni protokol "Stani i čekaj" (1)

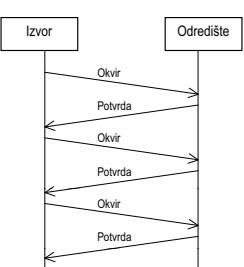
engl. Simplex Stop-and-Wait Protocol

Korak prema stvarnosti:

- ◆ jednosmjerni tok podataka, ali dvosmjerni tok okvira – podatkovni i kontrolni okviri (dvosmjerni kom. kanal)
- ◆ obrada realnog trajanja
- ◆ spremnici konačnog kapaciteta

Način rada: predajnik pošalje podatkovni okvir, pa stane s odašiljanjem i čeka kontrolni okvir s potvrdom od prijemnika da bi poslao sljedeći podatkovni okvir.

Jednosmjerni protokol "Stani i čekaj" (2)



Dvije vrste okvira

- ◆ okvir (podaci)
- ◆ kontrolni okvir (potvrda)

Zaustavljanje predajnika nakon odašiljanja okvira i čekanje na potvrdu sprječava preopterećenje prijamnika.

Jednosmjerni protokol za kanal sa smetnjama (1)

Stvarnost:

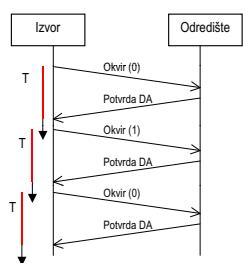
- ◆ pogreške u prijenosu
- ◆ vremenski kontrolirano čekanje potvrde
- ◆ može se dogoditi višestruki prijam istog okvira

Način rada: predajnik pamti koji okvir mora sljedeći poslati, a prijemnik pamti koji okvir očekuje

Numeracija okvira:

- ◆ slijedni broj
- ◆ najmanji slijedni broj: 1 bit (alternirajući bit, 0/1)

Jednosmjerni protokol za kanal sa smetnjama (2)

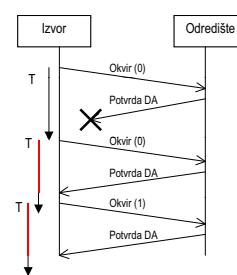


Protokol

Automatski zahtjev za ponavljanjem (engl. Automatic Repeat reQuest, ARQ)
ili
Positivna potvrda s ponavljanjem (engl. Positive Acknowledgment with Retransmission, PAR)

Potvrda ispravnih okvira naizmjenično označenih slijednim brojevima 0,1

Jednosmjerni protokol za kanal sa smetnjama (2)



Gubitak kontrolnog okvira s potvrdom

- ◆ prvi poslani okvir označen slijednim brojem 0 nije potvrđen na vrijeme
- ◆ predajnik ponavlja isti okvir
- ◆ prijemnik zna da je taj okvir već primio pa će ga potvrditi predajniku, ali ga neće isporučiti mrežnom sloju

Dvosmjerni protokol za kanal sa smetnjama

engl. Full-Duplex Protocol, Bidirectional Protocol

Dvosmjerni tok podataka i dvosmjerni tok okvira:

- ◆ podatkovni okviri i posebni kontrolni okviri s potvrdom ili
- ◆ jedinstveni okviri koji prenose podatke i potvrdu, što se zbog bolje iskoristivosti kom. kanala više primjenjuje

Jedinstveno rješenje za kontrolu pogrešaka i kontrolu toka:

- ◆ označavanje okvira slijednim brojem
- ◆ ograničavanje broja okvira u mreži

Učinkovitije je rješenje s dvosmjernim tokom okvira u kojima su sadržani i podaci i potvrda.

Klizajući prozor (1)

engl. sliding window

Predajnik:

- ♦ održava **predajni prozor** sa skupom slijednih brojeva okvira koje može poslati – više okvira odaslano

Prijamnik:

- ♦ održava **prijemni prozor** sa skupom slijednih brojeva okvira koje treba primiti – više okvira primljeno

Veličina prozora:

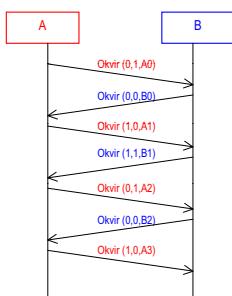
- ♦ ovisna o uvjetima u mreži, najmanji prozor: 1 bit (0, 1)

Veličina prozora od 1 bita dopušta numeraciju paketa naizmjenično s 0, 1. Takvi protokoli nazivaju se i protokolima s alternirajućim bitom.

Veći prozor od n bita omogućuje označavanje okvira s 0 do $2^n - 1$.

Klizajući prozor (2)

1-bitni klizajući prozor



- Okvir (x, y, z):
- ♦ x – broj okvira koji se šalje
 - ♦ y – broj zadnjeg ispravnog primljenog okvira
 - ♦ z – podaci

A šalje 0, potvrđuje 1, podaci A0
B šalje 0, potvrđuje 0, podaci B0
A šalje 1, potvrđuje 0, podaci A1
...

Klizajući prozor (3)

Protokol s 1-bitni klizajućim prozorom

Zadatak 1: Okvir (1,0,A1) primljen je oštećen. Nacrtati i objasniti slijedni dijagram!

Zadatak 2: A i B započinju slanje okvira (0,1,A0) i (0,1,B0) istodobno. Nacrtati i objasniti slijedni dijagram!

Složeni modeli protokola

Osnovna zamisao: prozor veličine $n > 1$

Protokol "vrati se za N" (engl. o Back N)

- ♦ prijamnik odbacuje i ne potvrđuje pogrešni okvir i sve iza njega
- ♦ ako je poslao j-ti okvir, a nije primio potvrdu za $i = j - N$ okvir, predajnik se vraća za N okvira unatrag te ponavlja i-ti okvir i sve iza njega

Protokol sa selektivnim ponavljanjem (engl. Selective Repeat)

- ♦ prijamnik odbacuje pogrešni okvir, a pohranjuje ispravne
- ♦ predajnik ponavlja nepotvrđene okvire

Složeni modeli protokola koji se praktički primjenjuju nastoje optimizirati broj okvira koje odašilje predajnik dok očekuje potvrdu prethodno poslanih. Naime, komunikacija "okvir po okvir" izrazito je neučinkovita kod duljih relacija s većim kašnjenjem.

Rasprava o učinkovitosti

Kako utječe na učinkovitost podatkovne poveznice:

- ♦ veličina okvira
- ♦ količina protokolne kontrolne informacije
- ♦ udaljenost komunicirajućih sustava
- ♦ vrsta prijenosnog medija
- ♦ brzina prijenosa podataka
- ♦ odabrani komunikacijski protokol
- ♦ ...

Komunikacijske mreže

4.
Lokalna mreža

Sadržaj predavanja

- ♦ Komunikacija u lokalnoj mreži
- ♦ Normiranje lokalnih mreža
- ♦ Podsloj upravljanja pristupom mediju
- ♦ Podsloj upravljanja logičkom poveznicom
- ♦ Lokalna mreža Ethernet, IEEE 802.3
- ♦ Povezivanje lokalnih mreža
- ♦ Druge izvedbe lokalnih mreža

Lokalna mreža

engl. Local Area Network, LAN

- ♦ povezivanje ograničenog broja **stanica** (krajnjih sustava/uređaja, najčešće **računala**) na ograničenom prostoru unutar zgrade ili skupine susjednih zgrada, u pravilu uz dobre uvjete komuniciranja (malo kašnjenje, mala vjerojatnost pogreške),
- ♦ veće i velike brzine prijenosa,
- ♦ u vlasništvu jedne organizacije,
- ♦ normiranje:
 - IEEE (The Institute of Electrical and Electronics Engineers)

Komunikacija u lokalnoj mreži (1)

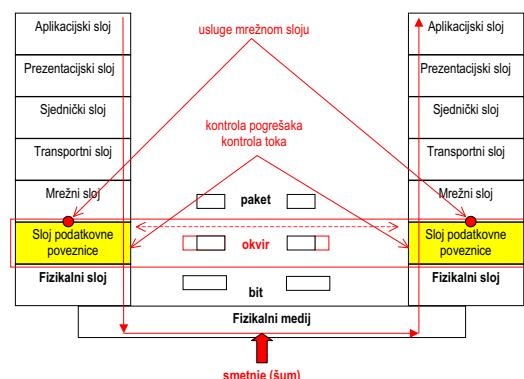
Fizikalni sloj:

- ♦ zajednički medij na koji su spojene sve stanice povezane u lokalnu mrežu
 - prijenosni medij (npr. kabel) ili
 - komunikacijski uređaj (npr. parični obnavljač, hub)

Sloj podatkovne poveznice:

- ♦ upravljanje pristupom prijenosnom mediju:
 - dodjela medija stanici radi odašiljanja podataka
- ♦ upravljanje logičkom poveznicom
 - izmjena jedinica podataka između dvije stanice

Komunikacija u lokalnoj mreži (2)



Komunikacija u lokalnoj mreži (3)



Komunikacijske mreže

27.9.2007

6 od 33

Komunikacija u lokalnoj mreži (4)

Dijeljeni medij:

- razašiljanje svima, difuzija (engl. broadcast)
- jedna stanica šalje protokolnu jedinicu podataka (PDU)
- sve stanice primaju PDU

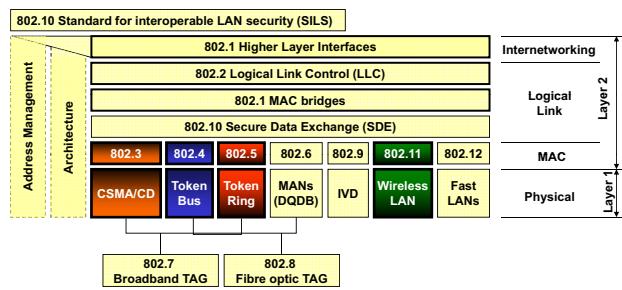
Pristup mediju:

- dvije stanice istodobno žele slati okvire?
 - kako dodijeliti medij jednoj stanici?
 - koja smije slati prva?

Normiranje lokalnih mreža

Odbor IEEE 802

Lokalna mreža Ethernet, IEEE 802.3



Komunikacijske mreže

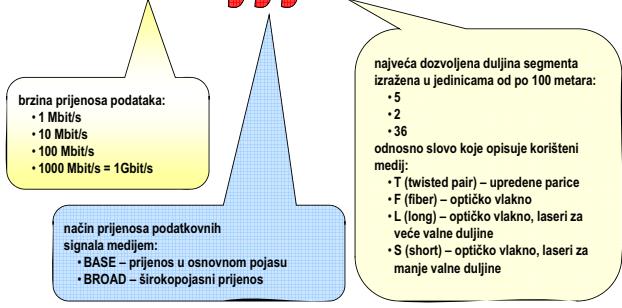
27.9.2007

8 od 33

Obradit će se lokalna mreža prema IEEE 802.3, odnosno Ethernet.

Označavanje norme IEEE 802.3

1xx Byy Z



Komunikacijske mreže

27.9.2007

9 od 33

Z = X

X označava različite vrste prijenosnog medija, npr. LX – jednomodno optičko vlakno.

Izvedbe norme IEEE 802.3



- ◆ brzina 10 Mbit/s
 - 10BASE5 - debeli koaksijalni kabel, topologija: sabirnica **FER 1985**
 - 10BASE2 - tanki koaksijalni kabel, topologija: sabirnica **FER 1985**
 - 10BASE-T - upredena parica (UTP, STP), topologija: sabirnica
 - 10BASE-F - optičko vlakno, topologija: zvijezda
 - 10BROAD36 - širokopojasni koaksijalni kabel
- ◆ brzina 100 Mbit/s
 - 100BASE-T - Fast Ethernet, topologija: zvijezda **FER 2007**
- ◆ brzina 1 Gbit/s
 - 1000 BASE-X - Gigabit Ethernet, topologija: zvijezda **FER 2007**

Komunikacijske mreže

27.9.2007

10 od 33



Upravljanje pristupom prijenosnom mediju

Podsloj MAC

- ◆ **dinamička** dodjela prijenosnog medija stanicu u lokalnoj mreži
- ◆ **specifično rješenje** za svaku vrstu lokalnih mreža
 - izvedeno na mrežnoj kartici stanice ili u priključku mrežnog uređaja (port)
- ◆ **pristupni protokoli:**
 - skupina pravila koja određuju redoslijed pristupanja mediju
- ◆ **upravljanje pristupom mediju:**
 - centralizirano, **distribuirano**
- ◆ **pristup mediju:**
 - prozivka (polling), **slučajni pristup (random access): ALOHA, CSMA/CD**

Komunikacijske mreže

27.9.2007

11 od 33

Slučajni pristup mediju - ALOHA



- ALOHA** – paketska radijska mreža (Abramson, 1970)
- ◆ stanica šalje podatke kad god ih ima, potpuno decentralizirano i slučajno
 - ◆ kad više stanica pošalje podatke istodobno, sukobljeni okviri će se uništiti
 - ◆ nakon što ustanovi da je okvir uništen, stanica će ponoviti slanje podataka
 - ◆ problem: slaba iskoristivost kanala zbog čestih sudara okvira
 - ◆ **Rješenja:**
 - uvođenje vremenskih odsječaka (Slotted ALOHA)
 - smanjivanje mogućnosti sudara i otkrivanje sudara (CSMA/CD)

Komunikacijske mreže

27.9.2007

12 od 33



Slučajni pristup mediju - CSMA/CD

CSMA/CD

(Carrier Sense Multiple Access Collision Detection)

- ◆ prije slanja okvira stanica ustanavljava je li medij zauzet osluškivanjem signala-nosioca na kanalu (Carrier Sense)
- ◆ više stanica pristupa mediju (Multiple Access)
- ◆ više stanica može istodobno ustanoviti da je medij slobodan i poslati okvir
- ◆ na mediju se događa i otkriva sudar (Collision Detection)

Komunikacijske mreže

27.9.2007

13 od 33

Upravljanje logičkom poveznicom



Podsloj LLC

- ◆ omogućuje protokolima mrežnog sloja da dijele podatkovnu poveznicu:
 - izведен programski kao upravljački program ili programski modul mrežnog uređaja
- ◆ **jednako rješenje** za sve vrste lokalnih mreža, neovisno o načinu upravljanja pristupom mediju
- ◆ usluge:
 - **nespojna usluga bez potvrde primitka okvira**
 - nespojna usluga s potvrdom primitka okvira
 - spojna usluga

Komunikacijske mreže

27.9.2007

14 od 33

U lokalnim mrežama (mala udaljenost, mala vjerojatnost pogreške bita, velika brzina prijenosa) može se primjeniti i primjenjuje se nespojna usluga bez potvrde primitka okvira.

IEEE 802.3 i Ethernet



- ♦ Industrijski konzorcij DIX (Digital, Intel, Xerox) razradio je i definirao Ethernet:
 - upravljanje pristupom CSMA/CD
 - dvije norme: Ethernet I (1980) i Ethernet II (1982)
- ♦ IEEE 802.3 nastavio rad koji je započeo DIX:
 - ista načela
 - okviri različiti, zbog uskladivanja s drugim normama za lokalne mreže
- ♦ za obje vrste lokalnih mreža koristi se naziv Ethernet

Komunikacijske mreže

27.9.2007

15 od 33

Struktura okvira



Ethernet	Preamble (8 okteta)	Odredište (6 okteta)	Izvođište (6 okteta)	Tip (2 okteta)	Podaci (46 - 1500 okteta)	FCS (4 okteta)
----------	------------------------	-------------------------	-------------------------	-------------------	------------------------------	-------------------

IEEE 802.3	Preamble (7 okteta)	SoF (1)	Odredište (6 okteta)	Izvođište (6 okteta)	Duljina (2 okteta)	LLC podaci (46 - 1500 okteta)	FCS (4 okteta)
------------	------------------------	------------	-------------------------	-------------------------	-----------------------	----------------------------------	-------------------

Određena adresa (48 bita, bitovi 0-47):

- Najviši (47.) bit "0": adresa pojedine stanice
- Najviši (47.) bit "1": skupina stanica (engl. multicast address)
 - Najviša dva bita (47. i 46) "10" – globalne adrese
 - Najviša dva bita (47. i 46) "11" – lokalne adrese
- Svi bitovi "1": sve stanice (engl. broadcast address)

Komunikacijske mreže

27.9.2007

16 od 33

Ethernet okvir sadrži sljedeća polja:

- preamble (engl. preamble): označava početak okvira (1010...), a služi za sinkronizaciju predajnika i prijamnika
- adresa odredišta (engl. destination address): 2 ili 6 okteta; za 10 M/bits primjenjuje se 6 oktet
- adresa izvođišta (engl. source address): 2 ili 6 okteta; za 10 M/bits primjenjuje se 6 oktet
- tip (engl. type): označava prijamniku kome je namijenjen okvir, tj. kojem protokolu u mrežnom sloju
- podaci, polje duljine 46-1500 okteta. Ako je količina podataka manja od 46 oktet, provodi se punjenje do 46 oktet. Minimalna duljina okvira a) olakšava njihovo prepoznavanje, b) sprječava odašiljanje novog okvira prije nego li je prethodni stigao do odredišta, čime se smanjuje broj potencijalnih sudara.
- Zaštitna suma (engl. Frame Checksum, FCS): primjenjuje se ciklički kod za otkrivanje pogrešaka

IEEE 802.3 okvir

Dvije promjene:

- preamble reducirana na 7 okteta, a uvedeno je polje sa značenjem početka okvira (engl. Start of Frame, SoF) da bi se postigla kompatibilnost s drugim normama za lokalne mreže (802.4, 802.5)
- polje tip je promjenilo naziv u duljinu (engl. length) koje označava duljinu okvira. Da bi se postiglo razlikovanje na prijamnoj strani na početak polja podataka uvedena su dodatna polja s informacijom za podsloj LLC.
- Nastala je zbrka s "tipom" i "duljinom" koja je praktički riješena tako da se sve vrijednosti tog polja do 1500 interpretiraju kao "duljina", a sve veće od 1500 kao "tip". Naime, do 1997. svi proizvodi za lokalne mreže i sve mreže u uporabi imale su "tip" veći od 1500!

Algoritamski opis: 1-ustrajni CSMA/CD

ponavljanje

```

ako kanal(medij) zauzet
  tada čeka oslobadanje kanala (medija)
  inače šalje okvir (s vjerojatnošću p = 1)
    ako sudar
      tada ponavljanje nakon slučajnog vremena
  obavi slanje okvira

```

Izvedba CSMA/CD u mreži Ethernet



1-ustrajni CSMA/CD (engl. 1-persistent)

- vjerojatnost prijenosa ako nađe na slobodan kanal $p = 1$
- stanica osluškuje kanal i ako je slobodan, šalje okvir
- ako dođe do sudara, to ponavlja nakon isteka slučajnog vremena



Komunikacijske mreže

27.9.2007

17 od 33

Sudari u mreži Ethernet (1)



Rani sudar:

- ♦ stanica ustanovljava da je kanal slobodan i šalje okvir
- ♦ tijekom slanja okvira stanica otkriva sudar

Kasni sudar:

- ♦ stanica ustanovljava da je kanal slobodan i šalje okvir
- ♦ do sudara dolazi nakon što je stanica završila slanje okvira

Domena sudara (engl. collision domain):

- ♦ dio mreže unutar kojeg vrijedi pravilo da se sudar javlja kad dvije stanice istodobno šalju okvire

Komunikacijske mreže

27.9.2007

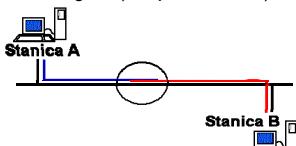
18 od 33

Sudari u mreži Ethernet (2)



Rani sudar:

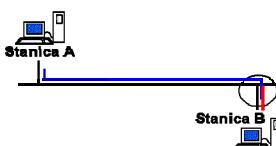
stanica A još uvijek odašilje i osluškuje medij, pa otkriva sudar, te će odaslati **amming signal** (snop od 48 bita)



Kasni sudar:

stanica A prestala je sa slanjem okvira i nije svjesna da je došlo do sudara

minimalna duljina okvira!



Minimalna duljina okvira

Zahtjev:

- stanica ne smije završiti slanje (zadnjeg bita) okvira prije nego prvi bit okvira stigne do odredišta

Rješenje:

- procijeniti minimalnu duljinu okvira za maksimalnu udaljenost stanica
vrijeme propagacije između A i B: t
minimalno vrijeme potrebno za otkrivanje sudara: 2t

Primjer:

brzina prijenosa $c = 10 \text{ Mbit/s}$ - vrijeme prijenosa bita $= 10^{-7} \text{ s}$
maksimalna udaljenost stanica $l = 2500 \text{ m}$, $2t = 50 \times 10^{-6} \text{ s}$ (prijenosni medij + obnavljači signala (engl. *repeater*))
minimalna duljina okvira: 500 bit ~ 512 bit ili 64 oktetra

Adresiranje stanica u lokalnoj mreži (1)

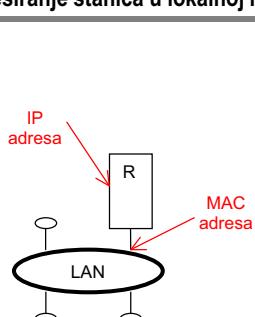


- svaka mrežna kartica ima svoju sklopovsku MAC adresu
 - 48 bita (MAC-48 identifikator)
 - prva tri okteta: jednoznačni identifikator organizacije (proizvođača)
 - druga tri okteta: identifikator NIC
- MAC adrese se zapisuju u heksadecimalnoj notaciji
 - primjer: 08 00 20 4C D3 E5

00001000	00000000	00100000	01001011	11000011	11100100
08:00:20			4C:D3:E5		
08:00:20			4C:D3:E6		

Identifikator organizacije (proizvođača): Sun Microsystems

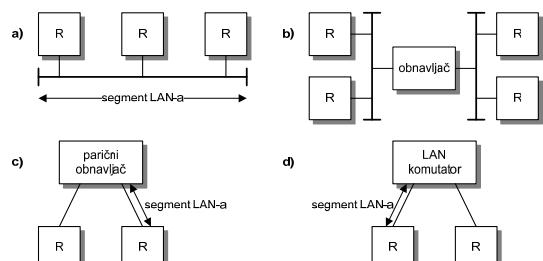
Adresiranje stanica u lokalnoj mreži (2)



Kakve adrese ima računalo spojeno na lokalnu mrežu putem koje pristupa Internetu?

- MAC adresa
(Sloj podatkovne poveznice)
- IP adresa
(Mrežni sloj)

Topologije mreže Ethernet



Fizička topologija: sabirnica (a, b), zvijezda (c, d)

Logička topologija: sabirnica (a, b, c), zvjezdasto povezane sabirnice (d)

Obnavljač i parični obnavljač

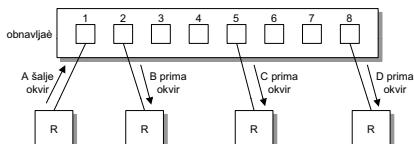


Obnavljač (engl. repeater)

uredaj koji povezuje dva segmenta lokalne mreže i obnavlja signal izobličen zbog prigušenja i disperzije (sabirnička topologija)

Parični obnavljač (engl. hub)

uredaj koji povezuje stанице u lokalnu mrežu i obnavlja signal (zvjezdasta topologija)



Komunikacijske mreže

27.9.2007

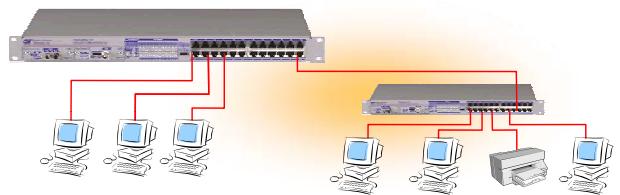
23 od 33

Parični obnavljač



- ne razdvaja domene sudara (svake dvije stанице mogu izazvati sudar)

- ne razdvaja domene razašiljanja - difuzije (engl. broadcast domain)



Komunikacijske mreže

27.9.2007

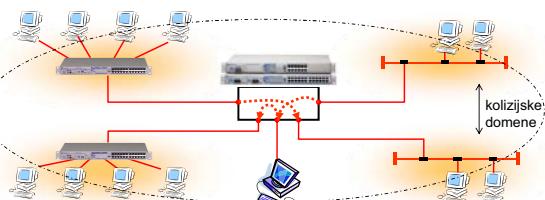
24 od 33

Komutator drugog sloja, LAN komutator (1)



engl. L2 switch, LAN switch

- radi na sloju podatkovne poveznice
- razdvaja domene sudara
- ne razdvaja domene razašiljanja - difuzije



Komunikacijske mreže

27.9.2007

25 od 33

Komutator drugog sloja, LAN komutator (2)



Komunikacijske mreže

27.9.2007

26 od 33

Povezivanje lokalnih mreža



Fizikalni sloj:

- obnavljač
- parični obnavljač

Sloj podatkovne poveznice

- most (engl. bridge)
 - izaziva kašnjenje ("spremi i proslijedi" okvir)
 - razdvaja domene sudara
 - ne razdvaja domene razašiljanja (manje mreže)

Opaska: komutator drugog sloja je most s većim brojem priključaka!

Komunikacijske mreže

27.9.2007

27 od 33

Obnavljač

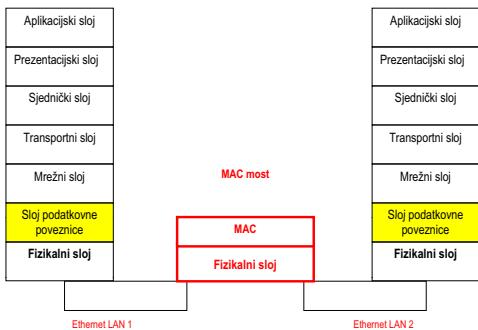


Komunikacijske mreže

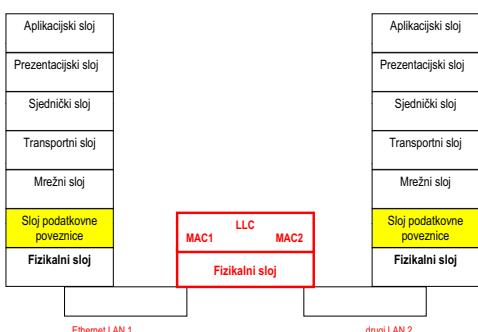
27.9.2007

28 od 33

Most (1)



Most (2)



MAC most, čije su funkcije u sloju podatkovne poveznice reducirane na podsloj pristupa mediju, može se primijeniti za povezivanje istovrsnih lokalnih mreža, npr. dva ili više Ethernet LAN-a.

Ostale izvedbe lokalnih mreža

IEEE 802.4 Token Bus

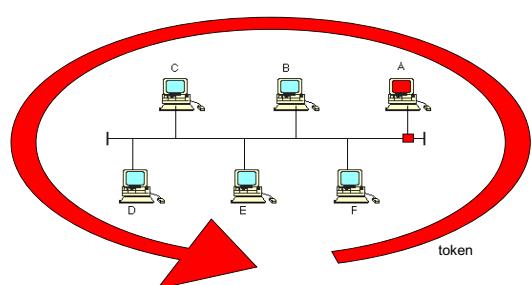
IEEE 802.5 Token Ring

- ♦ prozivka (engl. polling)
- ♦ pravo slanja okvira s podacima se označava znakom (engl. token) koji kruži između stanica
- ♦ pravo se ciklički prenosi narednoj stanici u slijedu
- ♦ znak: kratki pristupni okvir

IEEE 802.4 Token Bus

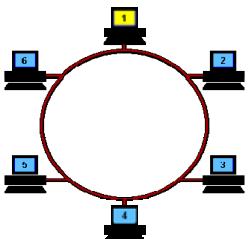
fizička topologija: sabirnica

logička topologija: prsten

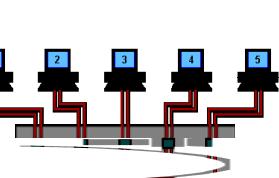


IEEE 802.5 Token Ring

fizička topologija: prsten
logička topologija: prsten



fizička topologija - zvijezda
logička topologija - prsten



Komunikacijske mreže

Priprema za laboratorijske vježbe
Programski sustav IMUNES

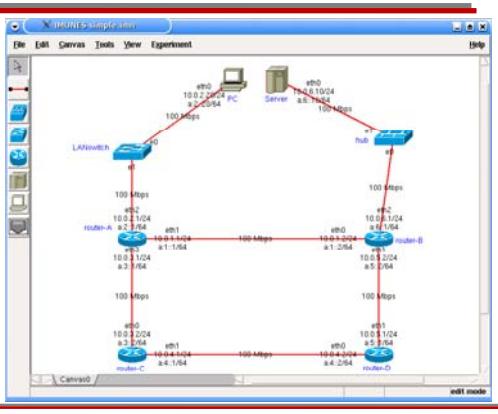
Sadržaj predavanja

- ◆ Uvod
- ◆ Način rada sustava IMUNES
- ◆ Pregled funkcionalnosti
- ◆ Primjena
- ◆ Dodatne informacije

Uvod

- ◆ IMUNES → Integrated Multiprotocol Network Emulator/Simulator
- ◆ Simulator mreža računala u stvarnom vremenu
- ◆ Prednosti
 - ◆ mogućnost obrade velikog broja računala (čvorova)
 - ◆ kratko vrijeme pokretanja simulacije
 - ◆ realistični rezultati simulacije
 - ◆ mogućnost emulacije (komunikacija simulirane i stvarne mreže)

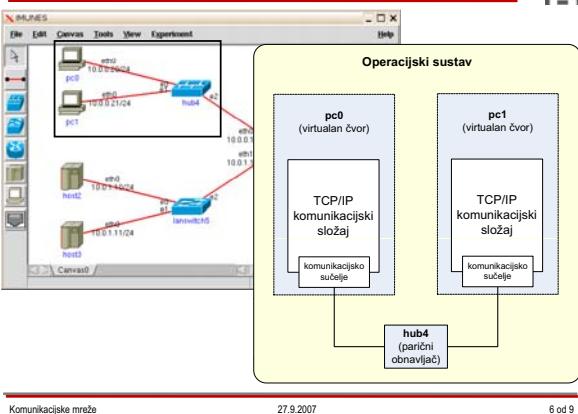
Primjer simulirane mreže



Način rada sustava IMUNES

- ◆ Operacijski sustav → izvedba funkcionalnosti modela TCP/IP (tzv. komunikacijski složaj)
- ◆ IMUNES → uvišestručenje komunikacijskog složaja na istom računalu
 - ◆ niz nezavisnih instanci složaja
 - ◆ svaka instance predstavlja čvor ("virtualni čvorovi")
 - ◆ virtualni čvorovi povezani međusobno i/ili s uređajima stvarne mreže

Način rada sustava IMUNES (nastavak)



Pregled funkcionalnosti

- ◆ Virtualni čvorovi rade na mrežnom sloju
 - ◆ podrška za internetski protokol
 - ◆ podrška za protokole usmjeravanja
 - ◆ podrška za aplikacijske protokole različitih usluga (npr., elektronička pošta)
- ◆ Međusobno povezivanje čvorova
 - ◆ podatkovna poveznica - širina pojasa, kašnjenje, učestalost pogreške bita (BER), itd.
 - ◆ parični obnavljač i ethernetski komutator

Primjena sustava IMUNES

- ◆ Istraživanje i razvoj → zamjena za eksperimentalne/testne mreže
- ◆ Razvoj i testiranje protokola usmjeravanja
- ◆ Provjera valjanosti mrežnih usluga
- ◆ Obrazovanje / podučavanje
- ◆ itd.



Komunikacijske mreže

27.9.2007

8 od 9

Dodatne informacije

- ◆ **FERWeb** i <http://www.imunes.net>
- ◆ Dostupan izvorni kod sustava
- ◆ Mogućnost korištenja sustava IMUNES putem CD-a za podizanje operacijskog sustava (*bootable CD*)
 - ◆ http://sef.tel.fer.hr/imunes/IMUNES_24_09_2007.iso



Komunikacijske mreže

27.9.2007

9 od 9

Komunikacijske mreže

5.
Mrežni sloj

Ak.g. 2007./2008.

22.10.2007

Zadaća mrežnog sloja je prebacivanje podatkovnih jedinica (paketa) od izvora do odredišta. Taj proces može uključivati niz od više poveznica od točke do točke.

Mrežni sloj je prvi, odnosno najniži sloj, koji rješava komunikaciju s jednog kraja mreže na drugi. Jedna od ključnih funkcija je stoga adresiranje. Mrežne adrese su logičke – dodjeljuje ih administrator mreže.

Kako bi mogao učinkovito prebaciti paket s jednog kraja mreže na drugi, mrežni sloj mora poznavati topologiju komunikacijske infrastrukture, odnosno povezanost između mrežnih čvorova – usmjeritelja, i na temelju toga odrediti put, odnosno niz "skokova" (od usmjeritelja do usmjeritelja) kojime će paket proći kroz mrežu od izvora do odredišta.

Uočimo da se neke funkcije, npr. kontrola pogrešaka (otkrivanje i ispravljanje pogrešaka) i kontrola toka, mogu izvesti i u sloju podatkovne poveznice i u mrežnom i u transportnom sloju. U internetskom modelu, na primjer, te funkcije nisu izvedene u protokolu IP, već je to prepusteno transportnom sloju – ako se želi pouzdana usluga koristi se protokol TCP.

Pri tome je važno odrediti put učinkovito, na primjer, da se paketi usmjeravaju najkraćim putem, ali i tako da se vodi računa o opterećenju poveznica i usmjeritelja. Konačno, treba omogućiti međusobno povezivanje mreža izvedenih različitim tehnologijama.

Podsjetnik na smještaj mrežnog sloja u mrežnoj arhitekturi.

Podsjetimo se



Zadaća mrežnog sloja

- ◆ omogućiti komunikaciju između dva (krajnja, korisnička) čvora u mreži, izravno ili preko niza međučvorova
 - adresiranje
 - usmjeravanje jedinica podataka
 - kontrola zagruženja
 - kontrola pogrešaka
 - kontrola toka
 - međusobno povezivanje mreža i podmreža

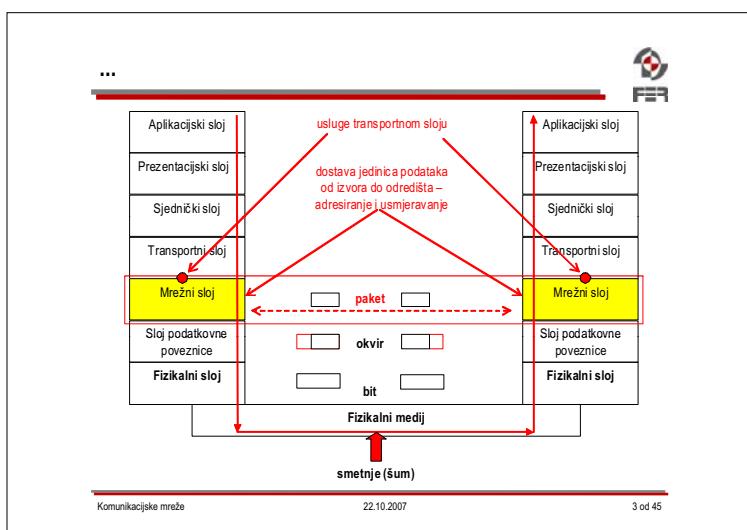
Problemi:

- ◆ znanje o topologiji, učinkovitost usmjeravanja, opterećenje poveznica, kontrola zagruženja, kvaliteta usluge

Komunikacijske mreže

22.10.2007

2 od 45



Komunikacijske mreže

22.10.2007

3 od 45

Sadržaj predavanja



- ◆ Usluge mrežnog sloja (transportnom sloju)
- ◆ Virtualni kanal i datagram, spojna usluga i nespojna usluga
- ◆ Komutacija paketa i usmjeravanje
- ◆ Načela upravljanja zagruženjem
- ◆ Međusobno povezivanje mreža i podmreža
- ◆ Protokoli mrežnog sloja u Internetu

Komunikacijske mreže

22.10.2007

4 od 45

Usluge mrežnog sloja



- ◆ osnovna zadaća mrežnog sloja: dostaviti pakete od izvođenog krajnjeg čvora (npr. korisničkog računala) do odredišnog krajnjeg čvora, izravno ili preko niza međučvorova
- ◆ dvije vrste usluga:
 - spojna usluga
 - nespojna usluga ← mrežni sloj u Internetu
- ◆ izvedba usmjeravanja u (pod)mrežama s komutacijom paketa:
 - virtualni kanal
 - datagramski ← mrežni sloj u Internetu

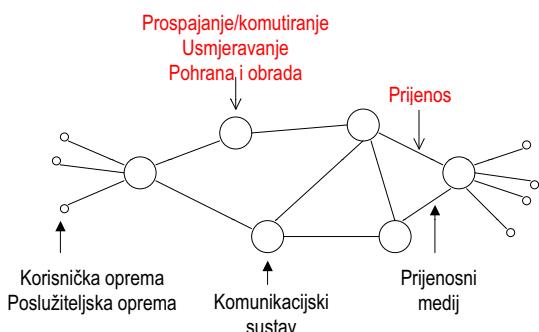
Predsjetnik:

Na prvom predavanju definirane su dvije vrste usluga koje sloj može pružiti sloju iznad: spojna i nespojna.

Ovisno o vrsti mreže, usluga mrežnog sloja može biti izvedena komutacijom kanala ili komutacijom paketa. Za uslugu izvedenu komutacijom paketa, da su računa usmjeravanja: virtualni kanal i datagramska.

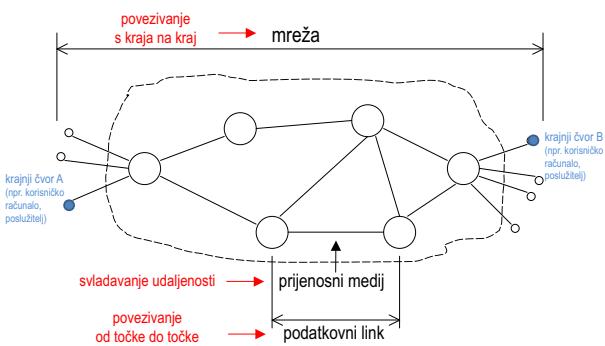
U nastavku predavanja naglasak je na nespojnoj usluzi koja je izvedena datagramska, budući da upravo takvu uslugu pruža mrežni sloj u Internetu.

Komunikacijska mreža (1)



(Ovdje su uvedene oznake koje se odnose na nekoliko sljedećih slika.)

Komunikacijska mreža (2)



Slika ilustrira razliku između usluga koje pružaju mrežni sloj, sloj podatkovnog linka i fizikalni sloj (prijenosni medij).

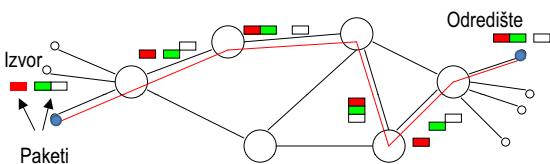
Mrežna usluga prenosi podatkovne jedinice (pakete) s kraja na kraj, za razliku od sloja podatkovne poveznice koji prenosi svoje podatkovne jedinice (okvire) na izravnoj vezi od točke do točke. Put kroz mrežu sastoji se od niza poveznica. Očito je da su i problemi ovdje složeniji – treba riješiti adresiranje na razini mreže i odabir puta kroz mrežu s jednog kraja na drugi.

Nespojna usluga izvedena virtualnim kanalom



Svi paketi usmjeravaju se istim putem - **virtualnim kanalom**.

Odluke o usmjeravanju donose se samo jednom, prilikom uspostavljanja novog virtualnog kanala.



Slika ilustrira nespojnu uslugu izvedenu komutacijom paketa uz način usmjeravanja virtualnim kanalom.

Primjer ovakvog načina rada je Multi Protocol Label Switching (MPLS). MPLS je tehnologija koja se ne uklapa u OSI model, već po funkcionalnosti dolazi negdje između 2. i 3. sloja te se zato naziva i "tehnologijom sloja 2,5.". MPLS se koristi u kombinaciji s IP-om pa se ne može direktno uspoređivati s njim. Koristi se uglavnom za privatne virtualne mreže i za mehanizam za uvođenje kvalitete usluge.

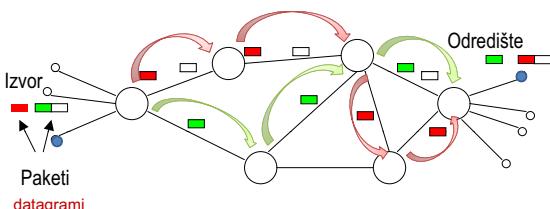
Nespojna usluga izvedena datagramski (1/2)



Svaki datagram **usmjerava se zasebno** kroz mrežu

Svaki usmjeritelj odluku o usmjeravanju datagrama donosi neovisno.

Moguće je da uzastopni datagrami prolaze različitim putovima



potrebni algoritmi usmjeravanja!

Slika ilustrira nespojnu uslugu izvedenu komutacijom paketa uz datagramski način usmjeravanja. Primjer – Internet!

Internet je mreža koja radi na načelu komutacije paketa u datagramskom načinu rada i u kojoj mrežni sloj transportnom služi pruža nespojnu uslugu.

Budući da se svaki datagram usmjerava neovisno o ostalima, očito je da mora sadržavati potpunu adresnu informaciju, tj. adrese izvora i odredišta.

Nespojna usluga izvedena datagramski (2/2)



◆ minimalni skup funkcija za dostavu datagrama s kraja na kraj mreže

◆ mogući problemi:

- povremeni gubitak paketa zbog pogreške, smetnji ili kvarova na nekoj od poveznica na putu
- povremeni gubitak paketa zbog zagušenja u nekom od mrežnih čvorova na putu
- povremena dostava paketa s narušenim redoslijedom u slučaju kad se izbor puta kroz mrežu promijeni tijekom komunikacije
- veće kašnjenje u slučaju retransmisije s kraja na kraj mreže
- pošiljatelj nema povratnu informaciju o ishodu

◆ rješavanje ovih problema prepušta se transportnom sloju!

Nespojni način rada relativno brzo rješava osnovni zadatak dostave datograma s kraja na kraj mreže, ali ništa više od toga. Mogući problemi navedeni su na slajdu.

Pojašnjenja:

-povremeni gubitak paketa na nekoj od poveznica na putu može se dogoditi zbog nedetektirane pogreške na sloju podatkovne poveznice, smetnji ili kvarova na poveznici.

-povremeni gubitak paketa zbog zagušenja u nekom od mrežnih čvorova na putu može se dogoditi zbog povećanog prometa na tom čvoru, za različite izvore i odredišta. Ako nema kontrole pristupa i kontrole toka, jedini način rukovanja s suvišnim paketima je odbacivanje.

-posljedica promjene puta može rezultirati narušen redoslijed paketa na odredištu

-kašnjenje u slučaju retransmisije s kraja na kraj je bitno veće od onog na sloju linka, gdje je retransmisija samo od točke do točke na izravnoj vezi, a preko cijele mreže to traje puno dulje.

Usporedba datagram – virtualni kanal

Značajka	Datagram	Virtualni kanal
Uspostava veze	Ne treba	Treba
Adresiranje	Svaki paket mora sadržavati polpunu adresnu informaciju (potpune mrežne adrese izvora i odredišta)	Svaki paket sadrži samo kratku oznaku virtualnog kanala
Informacija o stanju uspostavljenih veza	Usmjeritelji ne pohranjuju podatke o uspostavljenim vezama	Svakom virtualnom kanalu odgovara jedan unos u tablici usmjeravanja u usmjeritelju
Usmjeravanje	Svaki paket usmjerava se neovisno o drugima	Put se odabire prilikom uspostave veze, nakon toga svi paketi idu tim putem
Utjecaj kvara na usmjeritelju	Gubitak samo onih paketa koji su taj čas u obradi	Prekid svih uspostavljenih virtualnih kanala
Upravljanje zagušenjem Kvaliteta usluge	Složeno i teško izvedivo	Jednostavno, ako se potrebni resursi mogu unaprijed pridjeliti virtualnom kanalu

Komunikacijske mreže

22.10.2007

11 od 45

Sadržaj predavanja

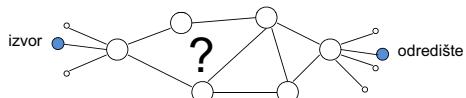
- ◆ Usluge mrežnog sloja (transportnom sloju)
- ◆ Virtualni kanal i datagram, spojna usluga i nespojna usluga
- ◆ Komutacija paketa i usmjeravanje
- ◆ Načela upravljanja zagušenjem
- ◆ Međusobno povezivanje mreža i podmreža
- ◆ Protokoli mrežnog sloja u Internetu



Osnovni pojmovi



- **usmjeravanje** (engl. routing) – određivanje puta kroz mrežu kojim će proći paket na putu od izvora do odredišta
- algoritmi kojima se računa taj put nazivaju se **algoritmima usmjeravanja** (engl. routing algorithm)
- problem usmjeravanja se formulira pomoću grafa u kojem čvorovi predstavljaju usmjeritelje, a grane grafa veze među njima



- **prosljedivanje** (engl. forwarding) – odluka unutar usmjeritelja: određivanje na koje odlazno sučelje proslijediti paket

Komunikacijske mreže

22.10.2007

13 od 45

Načelo optimalnosti



- ◆ Ako je usmjeritelj J na optimalnom putu od usmjeritelja I prema usmjeritelju K, onda je optimalni put od I do K dionica tog puta.
 - ◆ jednostavni dokaz (kontradikcijom):
 - nazovimo dionicu puta od I do J r_1 , i ostatak puta r_2
- $(I) \dots r_1 \dots (J) \dots r_2 \dots (K)$
- ako bi postojao bolji put od r_2 za dionicu od J do K, onda bi se taj put mogao nadovezati na r_1 , da bi poboljšao put od I do K, što je u kontradikciji s pretpostavkom da je J na optimalnom putu od I do K

Komunikacijske mreže

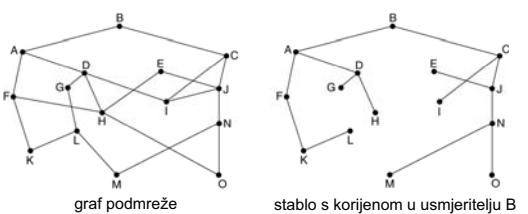
22.10.2007

14 od 45

Primjena načela optimalnosti na usmjeravanje



- ◆ za graf koji predstavlja mrežu i za zadano odredište, može se naći skup optimalnih puteva od svih izvora prema zadanim odredištu
- ◆ svi ti putevi čine stablo s korijenom u odredištu (engl. sink tree)
 - takvo stablo ne mora biti jedinstveno
 - cilj algoritama usmjeravanja: pronaći takvo stablo za sve usmjeritelje i iskoristiti ga za usmjeravanje (u praksi nije lako!)



Komunikacijske mreže

22.10.2007

15 od 45

Klasifikacija algoritama usmjeravanja



neadaptivni (statički) algoritmi

- unaprijed izračunati putevi na temelju nekog(ih) kriterija (npr. udaljenost, cijena, ...)
- putevi se postavljaju prilikom prvog pokretanja čvora i više se ne mijenjaju; ne uzimaju u obzir trenutno stanje

adaptivni (dinamički) algoritmi

- donose odluke o usmjeravanju temelje na mjerjenjima ili procjeni važećeg stanja u mreži (npr. aktualna topologija, opterećenje, ...)
- pitanja "skupljanja znanja" o stanju u mreži i prilagodbe:
 - što pratiti? (udaljenost, broj skokova, opterećenje, cijenu, ...?)
 - koga pitati? (samo susjedne čvorove, sve čvorove, ...?)
 - kada reagirati? (periodički, na promjenu topologije-opterećenja, ...?)

Komunikacijske mreže

22.10.2007

16 od 45

Algoritmi usmjeravanja

- ◆ Usmjeravanje najkraćim putem
- ◆ Preplavljanje
- ◆ Usmjeravanje prema vektoru udaljenosti
- ◆ Usmjeravanje prema stanju poveznice
- ◆ Posebni slučajevi:
 - hijerarhijsko usmjeravanje
 - opće razšiljanje, difuzija (engl. broadcast)
 - višeodredišno razšiljanje (engl. multicast)
 - kada su krajnji čvorovi u pokretu (pristup Internetu u pokretu)
 - kada nema infrastrukture (ad-hoc mreže)

Komunikacijske mreže

22.10.2007



17 od 45

Mi ćemo ovdje ilustrirati prva četiri navedena algoritma na primjerima.

Na višim godinama studija se detaljno obrađuju algoritmi i protokoli koji ih primjenjuju.

Engleski nazivi su:

Usmjeravanje najkraćim putem (engl. *shortest path routing*)

Preplavljanje (engl. *flooding*)

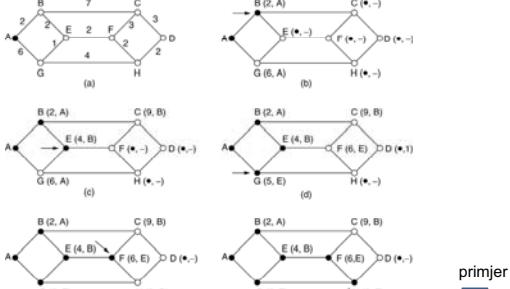
Usmjeravanje prema vektoru udaljenosti (engl. *distance vector routing*)

Usmjeravanje prema stanju poveznice (engl. *link state routing*)

Hijerarhijsko usmjeravanje (engl. *hierarchical routing*)

Usmjeravanje najkraćim putem

- ◆ statički; algoritam računa najkraći put od svih čvorova prema zadanom čvoru u grafu - poznati algoritam: Dijkstra (na slici prvih 5. koraka)



primjer

Komunikacijske mreže

22.10.2007

18 od 45

Duljina staze mjeri se brojem skokova. (Na slici, udaljenost A-B-C jednaka je udaljenosti A-B-E.)

U najopćenitijem slučaju, grane se mogu označiti kao funkcija stvarne udaljenosti, propusnosti,

prosječnog ili izmjereng kašnjenja, prosječnog opterećenja, cijene komunikacije, itd.)

Mijenjajući težinsku funkciju, najkraći put može se izračunati po bilo kojem zadanim kriteriju (ili kombinaciji kriterija).

(Primjer na slici je iz knjige A. Tannenbaum, Computer Networks).

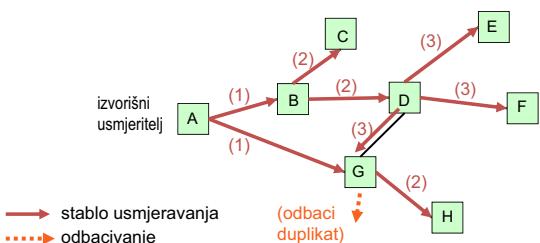
Udaljenost se inicijalizira kao <beskonačno>. Početni čvor je A. Oznaka čvora znači (prethodnik, udaljenost do A). Sve oznake su u početku privremene.

Postupak:

- Odabrati prvi čvor A i postaviti ga kao radni čvor. Promatramo susjedne čvorove od A i u privremenu oznaku upišemo udaljenost promatranočvora do A. U drugom koraku, odaberemo čvor s najmanjom privremenom oznakom udaljenosti kao sljedeći radni čvor (B).
- Promatramo susjede od B i osvježavamo njihove označke novom vrijednošću udaljenosti prema A (zbroj od A do B i udaljenosti do promatranočvora). Kada su svi susjadi osvježeni, oznaka s najmanjom udaljenosti do početnog čvora postaje

Preplavljanje

- ◆ statički; algoritam prosjećuje sve dolazne pakete na svako svoje odlazno sučelje, osim onog po kojem je primio paket
- ◆ paketi se označavaju i već viđeni paketi se odbacuju
- ◆ uvijek daje najkraći put!



Komunikacijske mreže

22.10.2007

19 od 45

Za smanjivanje rastućeg broja paketa, treba ugraditi brojač koji će sprječiti beskonačno uvišestručavanje i prosleđivanje paketa.

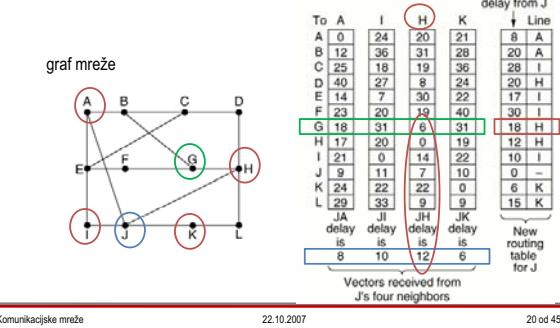
Drugi način je da izvojni usmjeritelj ubaci broj u nizu u "svoje" pakete (koji dolaze od krajnjih računala iz njegove mreže). Svaki usmjeritelj mora pratiti niz i čuvati listu "već viđenih" paketa, kako bi ga, ako se radi o duplikatu, mogao odbaciti.

Ovaj način uvijek daje najkraće stablo, ali nije baš učinkovit što se tiče opterećenja mreže. Preplavljanje nije praktično za većinu primjena, ali ima nekih za koje je vrlo dobar – na primjer konkurentno osvježavanje distribuiranih baza podataka, za vojne svrhe gdje se želi postići visoka otpornost na kvarove (robustnost), i za višeodredišno usmjeravanje.

Važnost ovog algoritma je u smislu usporedbe s drugima, budući da on uvijek daje najkraći put i najmanje kašnjenje.

Usmjeravanje vektorom udaljenosti (1/2)

- ◆ dinamički; svaki usmjeritelj ima tablicu (vektor) koji daje najbolju "poznatu udaljenost" za svako odredište i prvi korak ka njemu
- ◆ poznati algoritmi: Bellman-Ford i Ford-Fulkerson



Komunikacijske mreže

22.10.2007

20 od 45

(Primjer na slici je iz knjige A. Tannenbaum, Computer Networks).

Način rada:

Usmjeritelj zna "udaljenost" prema svakom od svojih susjednih čvorova, na temelju informacija koju razmjenjuje s njima.

(Udaljenost se može interpretirati kao broj skokova, kašnjenje, etc., ovisno koji je ključni kriterij. U praksi je to najčešće broj skokova ili kašnjenje.)

Tablica usmjeravanja sadrži po jedan unos za svaki usmjeritelj u mreži.

Unos se sastoji od oznake odlažnog sučelja prema tom odredištu i poznatoj udaljenosti. Tablica se osvježava na temelju periodičke razmjene podataka sa susjedima. Usporedbom podataka od svih susjeda, svaki usmjeritelj može izračunati svoju novu tablicu.

U ovom primjeru, zadane su tablice koje J primi od čvorova-susjeda A, I, H, K.

Pretpostavljamo da J ima vlastito znanje ili procjenu o kašnjenju prema svim susjedima, odn. zna vrijednosti JA, JI, JH, JK.

Kako J računa put prema G? A "zna" udaljenost od sebe do A, I, H, K, te njihovu procjenu vlastite udaljenosti prema G. Zbrajanjem tih dviju vrijednosti za svaki čvor (JA+AG, JI+IG...), najmanja udaljenost ispada JH+HG=12+6=18 (preko čvora H).

Isti postupak se ponavlja za sva odredišta i rezultat je prikazan slikom.

Protokol usmjeravanja koji koristi ovaj algoritam je Routing Information Protocol (RIP).

Usmjeravanje vektorom udaljenosti (2/2)

- ◆ algoritam konvergira prema pravom stanju, ali to čini sporo
- ◆ brzo reagira na dobre vijesti
 - npr. ako susjed A javi da ima kraći put do odredišta X, tablica se osvježava i promet za X se odmah počinje usmjeravati preko A
 - svaka sljedeća razmjena vektora propagira dobru vijest dalje
- ◆ sporo reagira na loše vijesti
 - npr. ako neki čvor ispadne, prvi susjed to zna, ali ne i drugi; nakon prve razmjene vektora, zna drugi susjed, ali ne i treći, itd. - u svakom slučaju razlika je uvek jedan više
 - postoje neka rješenja, ali nijedno nije univerzalno učinkovito

Komunikacijske mreže

22.10.2007

21 od 45

problem "brojanja u beskonačnost"

- jedno rješenje: ograničavanjem vrijednosti za "beskonačno"

- druga rješenja: postoji više ideja (npr. razdvajanje horizonta, uvedeno u većini izvedbi) koji pokušavaju popraviti algoritam, ali - kaže Tannenbaum - svako je složenije i manje praktično od prethodnog!

Usmjeravanje stanjem poveznice (1/2)

- ◆ dinamički; temelji se na razmjeni podataka o topologiji i stvarno izmjerenih podataka o stanju poveznice (kašnjenje) među čvorovima i zatim primjeni Dijkstrinog algoritma za izračun najkraćeg puta prema svim ostalim čvorovima
- ◆ algoritam uzima u obzir stvarno stanje – bolja prilagodljivost, ali uz povećanu složenost
 - kada, odn. kako često slati podatke susjedima i osvježavati stanje?
 - periodički
 - u slučaju značajnih događaja kao npr. ispad ili dodavanje čvora
 - kako pouzdano distribuirati poruke sa stanjem poveznice?
 - numerirati pakete, uvesti potvrde, uvesti oznaku starosti poruke, poslužiti se preplavljanjem (uz neka proširenja)

Komunikacijske mreže

22.10.2007

22 od 45

Usmjeravanje stanjem poveznice uvodi bolje metrike "udaljenosti" jer uzima u obzir eksperimentalno ustanovljene vrijednosti za parametre usmjeravanja, i nema problem spore konvergencije za veće mreže.

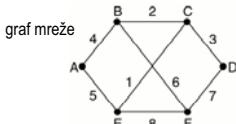
Protokol usmjeravanja koji koristi ovaj algoritam u Internetu je Open Shortest Path First (OSPF).

Usmjeravanje stanjem poveznice (1/2)



◆ Svaki čvor mora:

- otkriti svoje susjede i sazнати njihove mrežne adrese
- izmjeriti kašnjenje (ili drugi dogovoren parametar) prema svakom od njih
- stvoriti paket kojim javlja što je sve upravo saznao



poruke o stanju poveznice

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
F 6	E 1		F 8	E 8	

- razaslati paket svim ostalim čvorovima (ne samo susjedima!)
- izračunati najkraci put do svih ostalih čvorova (cijela topologija!)

Komunikacijske mreže

22.10.2007

23 od 45

Sadržaj predavanja



- ◆ Usluge mrežnog sloja (transportnom sloju)
- ◆ Virtualni kanal i datagram, spojna usluga i nespojna usluga
- ◆ Komutacija paketa i usmjeravanje
- ◆ **Načela upravljanja zagušenjem**
- ◆ Međusobno povezivanje mreža i podmreža
- ◆ Protokoli mrežnog sloja u Internetu

Komunikacijske mreže

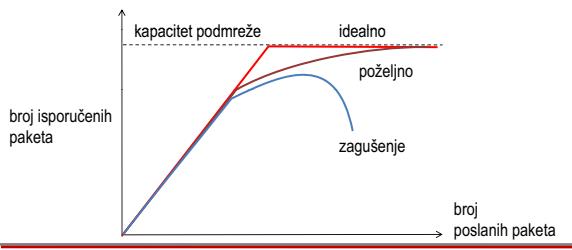
22.10.2007

24 od 45

Zagušenje



- ◆ **zagušenje** (engl. congestion) je degradacija performansi mreže uzrokovana prevelikim brojem paketa u mreži
- opterećenje je trenutno veće od onog koje je mrežna infrastruktura (čvorovi, poveznice) ili njen dio trenutno u stanju obraditi
- ◆ za razliku od kontrole toka, ovo je globalni problem!



Komunikacijske mreže

22.10.2007

25 od 45

Uzroci zagušenja



- ◆ razni uzroci i razna rješenja
- ◆ primjer:
Prometni tokovi iz raznih, neovisnih izvora u mreži mogu biti takvi da unutar nekog usmjeritelja konvergiraju na isto izlazno sučelje – stvara se rep čekanja:
 - nedovoljna količina memorije: odbacivanje paketa
 - više memorije sprečava odbacivanje, ali povećava kašnjenje zbog čekanja na obradu
 - povećano kašnjenje može uzrokovati istek vremenske kontrole i retransmisiju
- ◆ općenito, teži se ka smanjenju opterećenja (odbijanje/ograničavanje zahtjeva, smanjenje kvalitete, uvođenje prioriteta) i/ili povećanju resursa (brzina...), ali to ne rješava sve probleme (npr. povećanje brzine neće nužno smanjiti kašnjenje!) → **upravljanje zagušenjem**

Komunikacijske mreže

22.10.2007

26 od 45

Upravljanje zagušenjem (1/2)



- ◆ upravljanje zagušenjem obuhvaća dva osnovna pristupa iz teorije regulacije (engl. control theory):

1. rješenja s otvorenom petljom
2. rješenja sa zatvorenom petljom

- ◆ rješenja s otvorenom petljom temelje se na dobrom oblikovanju sustava s ciljem **izbjegavanja zagušenja**:

- ograničeni prihvat novih zahtjeva/prometnih tokova
- odbacivanje paketa po potrebi (i odluka kojih)
- oblikovanje prometa
- raspoređivanje unutar mreže

Komunikacijske mreže

22.10.2007

27 od 45

Upravljanje zagušenjem (2/2)



- ◆ rješenja sa zatvorenom petljom temelje na **stalnom praćenju ponašanja mreže i povratnoj vezi**:

- ponašanje
 1. nadziraj sustav i detektiraj pojavu i mjesto zagušenja
 2. proslijedi tu informaciju na mjesto ili mesta gdje se može djelovati
 3. prilagodi način rada sustava radi ispravljanja problema
- izravne indikacije zagušenja pomoći upravljačkim paketa, npr. zahtjev pošiljatelju da smanji brzinu slanja
- neizravne indikacije zagušenja na temelju praćenja ponašanja, npr. povećano prosječno kašnjenje, gomiljanje u usmjeriteljima, učestali gubici i retransmisije, povećan % izgubljenih paketa i sl.

→ Teorija informacije, Informacijske mreže, Teorija prometa

Komunikacijske mreže

22.10.2007

28 od 45

Sadržaj predavanja

- ◆ Usluge mrežnog sloja (transportnom sloju)
- ◆ Virtualni kanal i datagram, spojna usluga i nespojna usluga
- ◆ Komutacija paketa i usmjeravanje
- ◆ Načela upravljanja zagušenjem
- ◆ **Međusobno povezivanje mreža i podmreža**
- ◆ Protokoli mrežnog sloja u Internetu



Arhitektura mreže

Svaku mrežu obilježava:

- ◆ Organizacija - struktura (spajanje korisničke opreme na mrežu, međusobna povezanost komunikacijskih sustava, povezivanje s drugim mrežama)
- ◆ Adresiranje:
 - mrežnih sustava i umreženih resursa
 - korisnika
- ◆ Mrežni protokol (komunikacijski protokol mrežnog sloja)

Pozor:

Načela slična (ista) – terminologija različita za različite mreže!



Mrežni sloj – OSI model



7 Aplikacijski sloj, sloj primjene
6 Prezentacijski sloj
5 Sloj sesije/sjednice
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovnog linka/veze
1 Fizikalni/fizički sloj

- Prijenos informacije između dva čvora u mreži, izravno ili preko međučvorova
- Jedinica podataka: ovisna o vrsti mreže, npr. paket
- Usmjeravanje jedinica podataka
- Kontrola pogrešaka
- Kontrola toka
- Međusobno povezivanje mreža i podmreža

Mrežni sloj - internetski (TCP/IP) model



4 Aplikacijski sloj, sloj primjene
3 Transportni sloj
2 Mrežni/Internetski sloj
1 Prijenosna mreža

- ◆ Internetski protokol (Internet Protocol, IP) i dodatni protokoli za usmjeravanje, kontrolu komunikacije i komunikaciju u skupini
- ◆ Međusobno povezivanje mreža/podmreža (engl. internetworking)
- ◆ Mreža s komutacijom paketa, svaki se paket usmjerava zasebno - datagram

Uloga mrežnog sloja u mrežnoj arhitekturi



- ◆ mrežni sloj pruža uslugu transportnom sloju na sučelju između ta dva sloja
 - mrežni sloj daje transportnom **sloju jedinstveni adresni plan** (neovisno o broju podmreža, fizikalnom mediju, topologiji povezivanja i sl.) → **adresiranje**
 - mrežni sloj čini slojeve iznad, počevši od transportnog sloja, potpuno **odvojenima i neovisnima o izvedbenoj tehnologiji** mreže (protokol sloja podatkovne poveznice i prijenosni medij)
→ **pitanje fragmentacije**
 - sučelje mreža/transport je ujedno i **granica podmreže** prema krajnjim računalima (engl. host) → **povezivanje podmreža**
 - usmjeritelji imaju izvedene slojeve do (uključivo) mrežnog sloja
 - krajnja računala imaju izvedene sve slojeve

Adresiranje (1)



Jednoznačno označavanje komunicirajućih entiteta:

- ◆ Fizička adresa (mjesto priključka, pristupna točka)
- ◆ **Mrežna adresa (točka u mreži)**
- ◆ Adresa mrežnog/umreženog resursa:
 - Uslužna pristupna točka
 - Web stranica
 - ...
- ◆ Korisnička adresa:
 - Pozivni broj
 - Adresa elektroničke pošte
 - ...

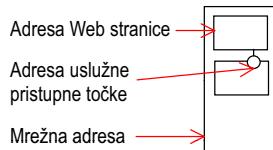
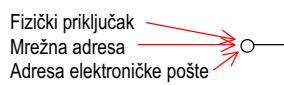
Adresiranje (2)

Dinamička adresa:

- dodijeljena privremeno, tijekom pružanja usluge
- pr: mrežna adresa (IP) kod pristupa Internetu preko telefonske mreže

Statička adresa:

- dodijeljena trajno
- pr: mrežna adresa Web poslužitelja i jedinstveni identifikator stranice



Komunikacijske mreže

22.10.2007

35 od 45

Primjer: adresiranje u Internetu

IP adresa - 32 bita (IPv4):

- identifikator koji globalno i jednoznačno određuje mrežno sučelje
 - krajnji sustav (npr. računalo priključeno na mrežu) obično ima jedno sučelje i jednu IP-adresu
 - mrežni čvor (npr. usmjeritelj) priključen na više (pod)mreža ima više sučelja i isto toliko IP-adresa

način zapisa:

- numerički zapis: binarni i dekadski

10100001 00110101 00010011 11001001
161 . 53 . 19 . 201

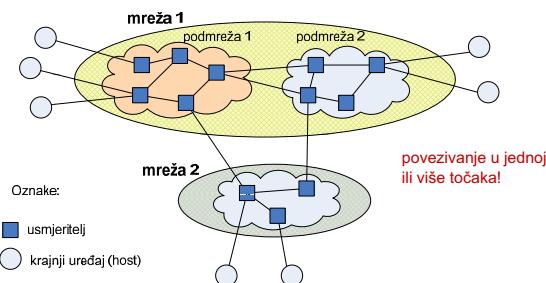
simbolički zapis: lakše pamtišljiv (npr. www.fer.hr) – veza: DNS

Komunikacijske mreže

22.10.2007

36 od 45

Povezivanje mreža i podmreža

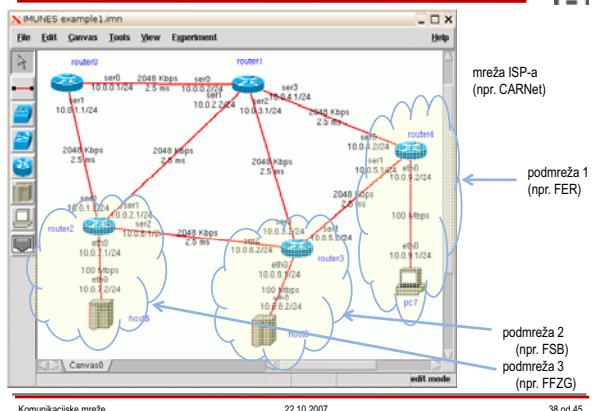


Komunikacijske mreže

22.10.2007

37 od 45

Povezivanje podmreža, primjer

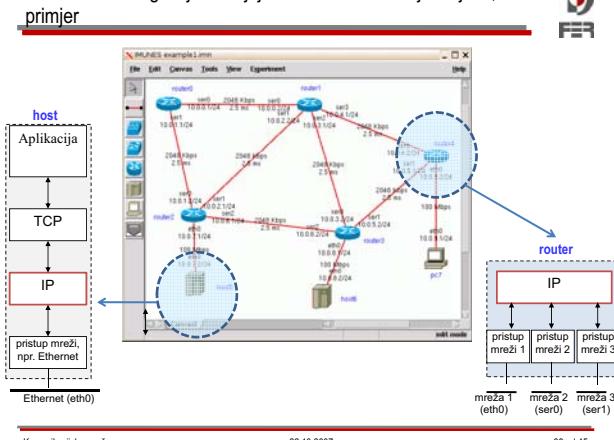


Komunikacijske mreže

22.10.2007

38 od 45

Izvedba mrežnog sloja u krajnjim računalima i usmjeriteljima, primjer



Komunikacijske mreže

22.10.2007

39 od 45

Primjer: usmjeravanje u Internetu

Određivanje puta i proslijedivanje paketa od izvorišnog do odredišnog čvora na temelju određene IP-adrese:

- ukoliko su izvorišni i odredišni čvor u istoj podmreži s dodeljenim medijem, tada komuniciraju izravno, ili
- ukoliko su izvorišni i odredišni čvor u različitim (pod)mrežama, tada komuniciraju preko jednog ili više usmjeritelja.

Pitanje:

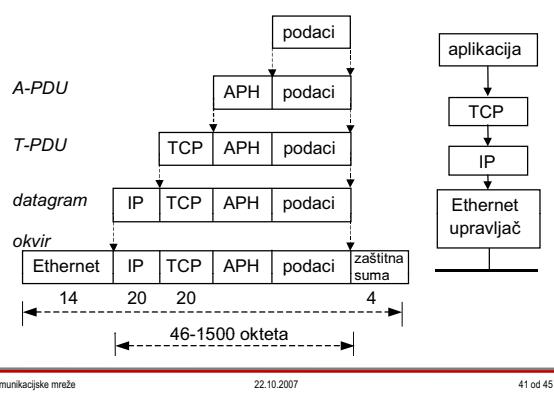
Kako se usmjeravaju paketi u usmjeritelju?

Komunikacijske mreže

22.10.2007

40 od 45

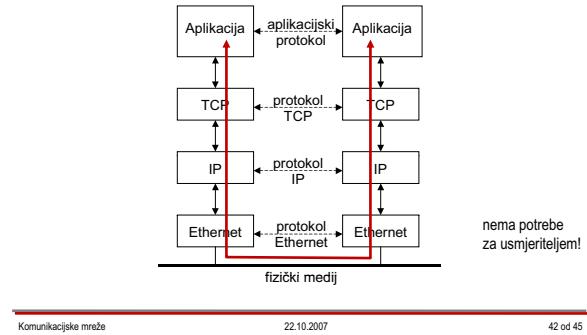
Obrada u krajnjem čvoru, protokolni složaj



Izravno usmjeravanje paketa



Primjer: Izvorišni i odredišni čvor u istoj lokalnoj mreži (Ethernet)

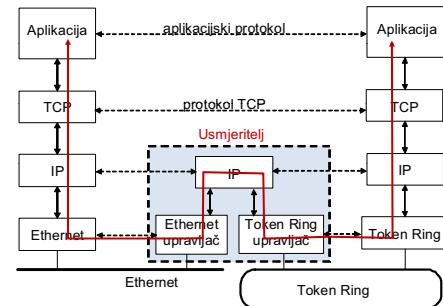


U ovom primjeru radi se o Ethernet lokalnoj mreži s dijeljenim medijem, odn. difuzijom.

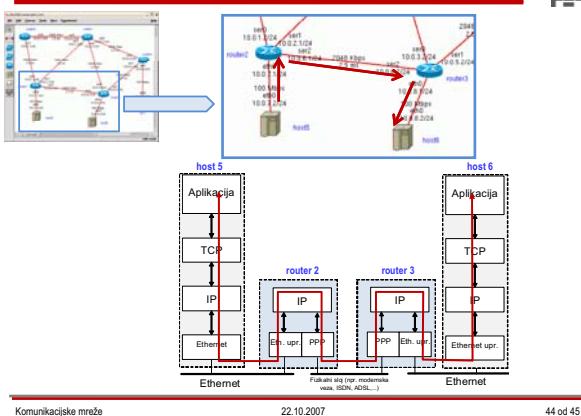
Usmjeravanje paketa preko usmjeritelja



Primjer: Izvorišni i odredišni čvor u lokalnim mrežama različite izvedbe (Ethernet, Token Ring)



Usmjeravanje paketa s kraja na kraj mreže



Protokoli mrežnog sloja u Internetu



4 Aplikacijski sloj, sloj primjene (Application Layer)

3 Transportni sloj (Transport Layer)

2 Mrežni sloj, Internetski sloj (Network Layer, Internet Layer)

Mrežni protokol: IPv4, IPv6

Kontrolni protokoli: ICMP, ARP, RARP,

Protokoli za komunikaciju u skupini: IGMP

Protokoli za pokretljivost: Mobile IP

Sigurnosni protokoli: IPsec

Protokoli usmjeravanja

1 nije definiran stvarna upotrijebljena mreža, pristup mreži (sloj podatkovnog linka i fizički sloj)

Komunikacijske mreže

6.

Mrežni sloj u Internetu. Internetski protokoli mrežnog sloja.

Ak.g. 2007./2008.

29.10.2007.

Sadržaj predavanja

- ◆ Protokolni složaj TCP/IP
- ◆ Organizacija i struktura Interneta
- ◆ Protokol Internet Protocol (IP)
 - ◆ adresiranje i fragmentiranje
- ◆ Usmjeravanje u Internetu
 - ◆ načela usmjeravanja
 - ◆ protokoli usmjeravanja
 - ◆ dijagnostika problema
- ◆ Ostali protokoli važni za mrežni sloj
 - ◆ dinamičko dodjeljivanje adresa, razlučivanje adrese

Komunikacijske mreže

29.10.2007.

2 od 48

Literatura: knjiga "Osnovne arhitekture mreža", poglavlje Internet

Mrežni sloj - internetski (TCP/IP) model



4 Aplikacijski sloj, sloj primjene
3 Transportni sloj
2 Mrežni/Internetski sloj
1 Prijenosna mreža

- ◆ Internetski protokol (Internet Protocol, IP) i dodatni protokoli za usmjeravanje, kontrolu komunikacije i komunikaciju u skupini
- ◆ Međusobno povezivanje mreža/podmrreža (engl. internetworking)
- ◆ Mreža s komutacijom paketa, svaki se paket usmjerava zasebno - datagram

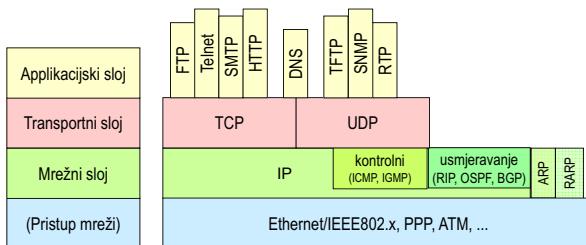
Zadaća mrežnog sloja: ostvariti transfer datagrama s jednog kraja mreže na drugi, gdje su krajnje točke mrežna sučelja.

Komunikacijske mreže

29.10.2007.

3 od 48

Protokolni složaj TCP/IP



Komunikacijske mreže

29.10.2007.

4 od 48

Najvažniji internetski protokol je *Internet Protocol* (IP), koji služi kao osnovni mehanizam dostave podatkovnih jedinica za sve ostale protokole.

Povrh osnovne mrežne povezivosti temeljene na IP-u gradi se cjelokupna internetska arhitektura, na koju se sam naziv *Internet* odnosi u širem, općenitijem smislu. Internetska arhitektura naziva se još i *TCP/IP arhitektura*, prema dvama najvažnijim protokolima, transportnom protokolu *Transmission Control Protocol* (TCP) i već spomenutom IP-u.

Protokolni složaj (stog) pokazuje skup protokola organiziranih po slojevima arhitekture (ovdje, internetskog) referentnog modela.

Sadržaj predavanja

- ◆ Protokolni složaj TCP/IP
- ◆ Organizacija i struktura Interneta
- ◆ Protokol Internet Protocol (IP)
 - ◆ adresiranje i fragmentiranje
- ◆ Usmjeravanje u Internetu
 - ◆ načela usmjeravanja
 - ◆ protokoli usmjeravanja
 - ◆ dijagnostika problema
- ◆ Ostali protokoli važni za mrežni sloj
 - ◆ dinamičko dodjeljivanje adresa, razlučivanje adrese

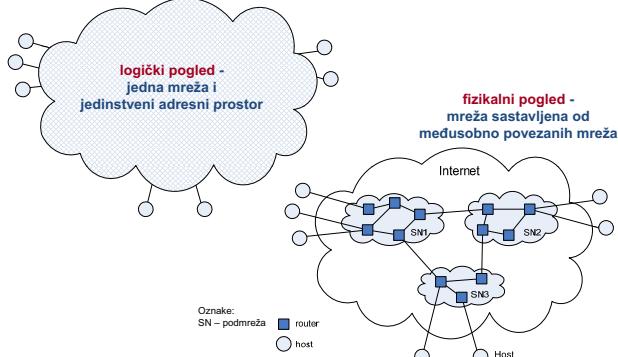
Komunikacijske mreže

29.10.2007.



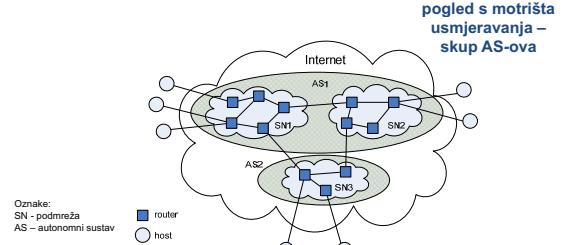
Literatura: knjiga "Osnovne arhitekture mreža", poglavje Internet

Internet = mreža međusobno povezanih mreža



Pojam autonomnog sustava

- ◆ Autonomni sustav (engl. Autonomous System, AS)
 - skupina IP mreža i usmjeritelja pod zajedničkom upravom i sa zajedničkom politikom usmjeravanja prema Internetu
- ◆ jedinstveni broj AS-a dodjeljuje IANA (npr., CARNet – AS 2108)



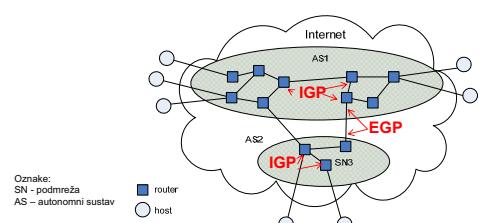
Promatrajući fizičku strukturu, Internet čine međusobno povezane *podmreže*, administrativno podijeljene u *autonomne sustave* (Autonomous System – AS).

Autonomni sustav definira se kao povezani dio mrežne topologije, tj. više podmreža s jedinstvenom i jasno definiranom politikom usmjeravanja "prema van", odnosno prema ostalim autonomnim sustavima.

Stoga se autonomni sustav najčešće nalazi pod administracijom i u vlasništvu jednog mrežnog operatora. Primjer AS-a je Hrvatska akademска i istraživačka mreža CARNet.

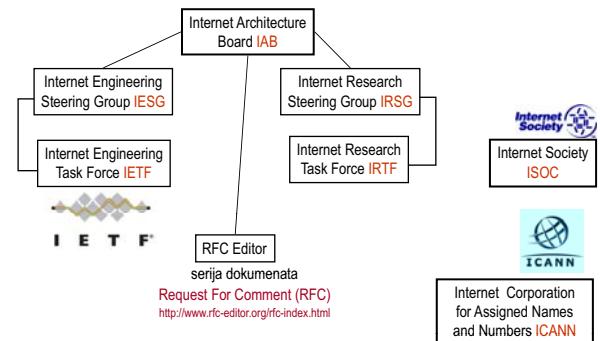
Povezanost unutar AS-a i između AS-ova

- ◆ Usmjeravanje unutar AS:
protokoli unutrašnjeg usmjeravanja (engl. Interior Gateway Protocol, IGP)
 - najčešće: Routing Information Protocol (RIP) i Open Shortest Path First (OSPF)
- ◆ Usmjeravanje između AS-:
protokoli vanjskog usmjeravanja (engl. Exterior Gateway Protocol, EGP)
 - u praksi samo jedan: Border Gateway Protocol (BGP)



U internetskoj terminologiji, protokoli za usmjeravanje unutar AS-ova nazivaju se *protokoli unutrašnjeg usmjeravanja* (Interior Gateway Protocol – IGP), a protokoli za usmjeravanje između različitih AS-ova nazivaju se *protokoli vanjskog usmjeravanja* (Exterior Gateway Protocol – EGP).

Globalna koordinacija i normiranje u Internetu



Komunikacijske mreže

29.10.2007.

9 od 48

Sadržaj predavanja



- ◆ Protokolni složaj TCP/IP
- ◆ Organizacija i struktura Interneta
- ◆ **Protokol Internet Protocol (IP)**
 - ◆ adresiranje i fragmentiranje
- ◆ Usmjeravanje u Internetu
 - ◆ načela usmjeravanja
 - ◆ protokoli usmjeravanja
 - ◆ dijagnostika problema
- ◆ Ostali protokoli važni za mrežni sloj
 - ◆ dinamičko dodjeljivanje adresa, razlučivanje adrese

Komunikacijske mreže

29.10.2007.

10 od 48

Literatura: knjiga "Osnovne arhitekture mreža", poglavje Internet

Protokol Internet Protocol (IP)



- ◆ Odlike i funkcionalnost protokola IP
- ◆ IP adresiranje i imenovanje
- ◆ Format datagrama
- ◆ Fragmentacija i spajanje

Komunikacijske mreže

29.10.2007.

11 od 48

Odlike protokola IP



- ◆ Internet Protocol (IP), verzija IPv4 (RFC 791, STD-5)

- ◆ Glavne odlike:

- neovisan o nižim protokolima
 - Ethernet, IEEE 802.3, PPP, ...
- datagramski način rada
- nespojna usluga
- nepotvrđena usluga
- nema mehanizma kontrole toka
- nema garancije očuvanja redoslijeda datagrama

usluga IP-a transportnom sloju:

nepouzdana dostava datagrama

- ◆ Uloga u protokolnom složaju TCP/IP: omatjanje (engl. encapsulation)

- prihvata podatke od višeg sloja (npr. transportnog protokola TCP, UDP), smješta ih u podatkovno polje IP datagrama i predaje datagram protokolu sloja podatkovne poveznice (npr., Ethernet)

Komunikacijske mreže

29.10.2007.

12 od 48

Protokol IP pruža *datagramsku*, odnosno nespojnu (*connectionless*) mrežnu uslugu. Mrežna povezanost temelji se na načelu komutacije paketa, pri čemu se paketski komutatori u Internetu nazivaju *usmjeriteljima* (*router*). Glavni zadatak usmjeritelja je "prebacivanje" IP datagrama sljedećem usmjeritelju na putu prema odredištu, što uključuje odabir sljedećeg usmjeritelja i odlaznog sučelja po kojem će se datagram proslijediti.

Specifikacije:

IP Internet Protocol RFC [791](#)

ICMP Internet Control Message Protocol RFC [792](#)

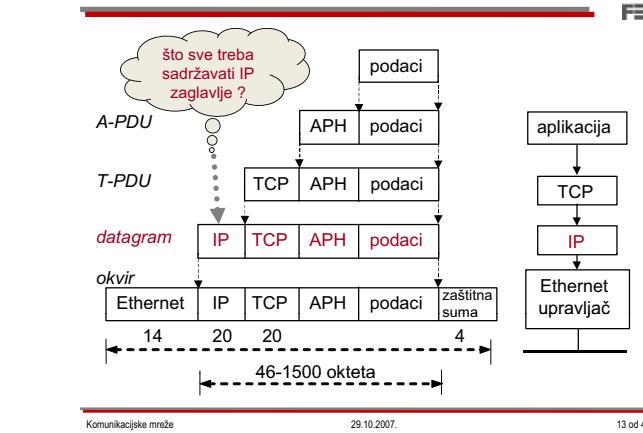
Broadcasting Internet Datagrams RFC [919](#)

Broadcasting Internet datagrams in the presence of subnets RFC [922](#)

Internet Standard Subnetting Procedure RFC [950](#)

IGMP Host extensions for IP multicasting RFC [1112](#)

Uloga protokola IP u TCP/IP protokolnom složaju



Funkcionalnost protokola IP

- ◆ definira **shemu adresiranja** u Internetu
 - jedinstveni adresni prostor
 - svako krajnje računalo ima po jednu IP-adresu za svako mrežno sučelje
 - svako krajnje računalo može koristiti i više posebnih adresa (npr., adresa localhost, multicast, broadcast ...)
 - ako su izvođač i odredišna adresa u različitim mrežama, IP datagrami se usmjeravaju preko jednog ili više IP-usmjeritelja
- ◆ definira kako provesti **fragmentaciju**
 - datagram mora "stati" u podatkovno polje okvira sloja podatkovne poveznice
 - datagram veći od toga mora se fragmentirati
 - na strani primatelja fragmenti se sastavljanju

Komunikacijske mreže

29.10.2007.

14 od 48



IP - adresiranje

IP adresa - 32 bita (IPv4):

- ◆ identifikator koji globalno i jednoznačno određuje mrežno sučelje
 - krajnji sustav (npr. računalo priključeno na mrežu) obično ima jedno sučelje i jednu IP-adresu
 - mrežni čvor (npr. usmjeritelj) priključen na više (pod)mreža ima više sučelja i isto toliko IP-adresa
- ◆ način zapisa:
 - numerički zapis: binarni i dekadski

10100001	00110101	00010011	11001001			
161	.	53	.	19	.	201

■ simbolički zapis: lakše pamtljiv (npr. www.fer.hr) – veza: [DNS](#)

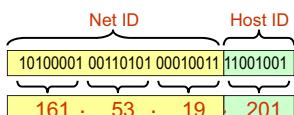
Komunikacijske mreže

29.10.2007.

15 od 48

Struktura IP adrese

- ◆ IP adresa ima dva dijela:
 - identifikator mreže (engl. Network Identifier, Net ID)
 - određeni broj bitova koji identificira mrežu u kojoj se nalazi mrežno sučelje
 - dodjela adrese preko ICANN-a
 - identifikator krajnjeg računala (engl. Host Identifier, Host ID)
 - ostatak bitova u adresi, koji služi za identifikaciju mrežnog sučelja u mreži zadanoj s NetID
 - dodjeljuje lokalni administrator
 - može se dodatno podijeliti za uvođenje podmreža (engl. subnetting)



Komunikacijske mreže

29.10.2007.

16 od 48

Dodjelu mrežnog dijela adrese nadzire **ICANN** (Internet Corporation for Assigned Names and Numbers), ranije **IANA** (Internet Assigned Numbers Authority), koji raspoređuje dijelove adresnog prostora regionalnim tijelima, u Europi **RIPE NCC** (Reseaux IP Europeens Network Coordination Centre), koji nacionalnim tijelima povjerava dodjelu adresa na državnoj razini, u Hrvatskoj **CARNet**.

Klase i rasponi IP-adresa

Klasa:	01	7 8	16	31	
A	0	NetID	HostID	0.0.0.0 – 127.255.255.255	
B	10	NetID	HostID	128.0.0.0 – 191.255.255.255	
C	110	NetID	HostID	192.0.0.0 – 223.255.255.255	
D	1110	višeodredišna adresa		224.0.0.0 – 239.255.255.255	
E	1111	rezervirano		240.0.0.0 – 247.255.255.255	

Odabране IP-adrese i blokovi IP-adresa rezervirani i zauzeti za posebne namjene!

Komunikacijske mreže

29.10.2007.

17 od 48



Besklasno adresiranje i prefiksni prikaz adrese

- ◆ **prefiksni prikaz** IP adrese ne uzima u obzir izvorne klase A, B i C
- ◆ dioba između mrežnog i računalnog dijela adrese može biti na bilo kojem mjestu unutar adrese (ne samo na granici okteta kao kod klasa!)
- ◆ duljina mrežnog dijela se označava **mrežnim prefiksom** iza adrese

195.24.0.0/13

11000011.00011000.00000000.00000000
mrežni prefiks
13 bita

- ◆ besklasno usmjeravanje – Classless Inter-Domain Routing (CIDR): putevi usmjeravanja više ne agregiraju prema klasama adresa, već prema mrežnom prefiksu

Komunikacijske mreže

29.10.2007.

18 od 48



RFC 4632

Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan

Aug 2006

Dodjela i upravljanje IP-adresama

- ◆ na razini globalnog Interneta:
ICANN – Internet Corporation for Assigned Names and Numbers
 - ◆ upravljanje dodjelom blokova adresa i DNS sustavom
 - ◆ danas se koristi CIDR – Classless Inter-Domain Routing
 - ◆ dodjela adresa se delegira RIR-ovima – Regional Internet Registry APNIC, ARIN, LACNIC, RIPE NCC (za Europu), AFRINIC



- ◆ RIR-ovi delegiraju odgovornost nacionalnim (NIR) i lokalnim (LIR) registrima u Hrvatskoj – CARNet!



- ◆ u konačnici se blokovi adresa daju ISP-ovima, koji ih dodjeljuju korisnicima ili nižim ISP-ovima

Komunikacijske mreže

29.10.2007.

19 od 48

Namjena IP-adresa



- ◆ javne mreže:
 - ◆ svaka adresa mora biti globalno jedinstvena
 - ◆ mora se omogućiti usmjeravanje
 - ◆ dodjela adresa - ICANN, RIR, LIR, NIR,...
 - ◆ u konačnici se blokovi adresa daju pružateljima internetskih usluga (ISP)
- ◆ privatne mreže:
 - ◆ ICANN definira samo raspone privatnih IP adresa
 - ◆ organizacija – vlasnik mreže nadzire i upravlja adresnim prostorom
 - ◆ svaka adresa mora biti jedinstvena unutar privatne mreže
- ◆ preslikavanje privatnih adresa u javne i obrnuto – uređaj **Network Address Translator (NAT)**

Komunikacijske mreže

29.10.2007.

20 od 48



Postavljanje IP adrese

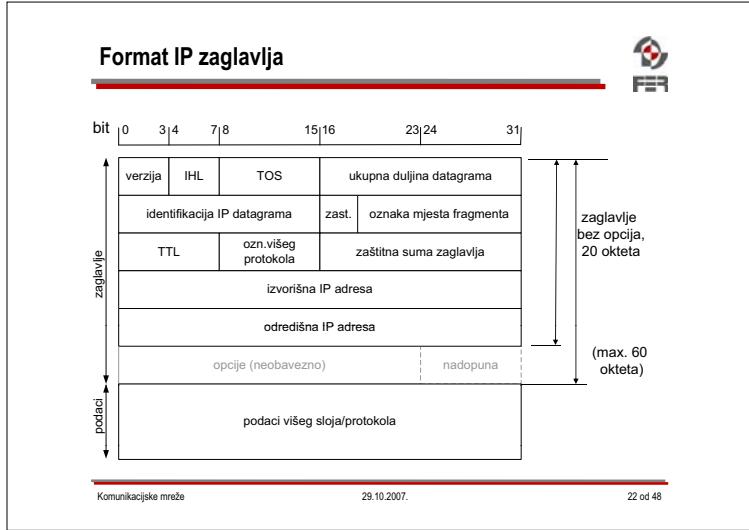
- ◆ **statičko**
 - ◆ IP adresa se upiše u postavkama računala
 - ◆ obično se koristi za poslužitelje, usmjeritelje i uređaje koji nikad ne mijenjaju svoju adresu
 - ◆ dobro za male mreže, (pre)složeno i nepraktično za velike mreže
- ◆ **dinamičko**
 - IP adresa i druge mrežne postavke dobivaju se od poslužitelja
 - pojednostavljuje dodjelu adresa u velikim mrežama (npr. tvrtke ili ISP-a)
 - tipična primjena: za osobna računala
 - **protokol DHCP** – Dynamic Host Configuration Protocol

Komunikacijske mreže

29.10.2007.

21 od 48

2131 Dynamic Host Configuration Protocol. R. Droms. March 1997. (Format: TXT=113738 bytes) (Obsoletes RFC1541) (Updated by RFC3396, RFC4361) (Status: DRAFT STANDARD)



Polja u zaglavlju IP datagrama:

verzija: inačica IP-a (u današnjim mrežama IPv4),

IHL, duljina zaglavja: broj 32-bitnih riječi (od 5 do 15),

TOS, vrsta usluge: oznaka kvalitete usluge tražene za datagram,

duljina: broj okteta u datagramu, uključujući zaglavje (najviše 64)

identifikacija: jedinstveni broj datagrama, isti za sve fragmente.

zastavice: 3 bita rezervirana za oznake vezane uz fragmentiranje,
mjesto fragmenta: ako se radi o fragmentu, oznaka za izračunavanje njegovog smještaja

u fragmentiranom datagramu,
TTL: najveći dopušteni broj usmjeritelja kroz koje datagram može proći prije nego što

bude odbačen (na svakom usmjeritelju TTL se umanjuje za jedan),

protokol: oznaka protokola višeg sloja čije podatke IP nosi (npr. TCP, UDP)

zaštitna suma zaglavlja: zaštitni kôd za otkrivanje pogrešaka u

izvoršna IP adresa: IP adresa s koje se odašilje datagram,

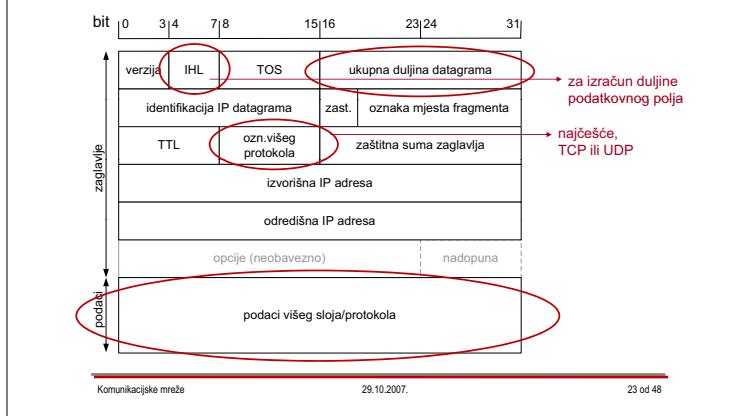
odredišna adresa: IP adresa na koju se šalje datagram,

opcije: posebne izborne mogućnosti, npr. za izvorno određivanje put

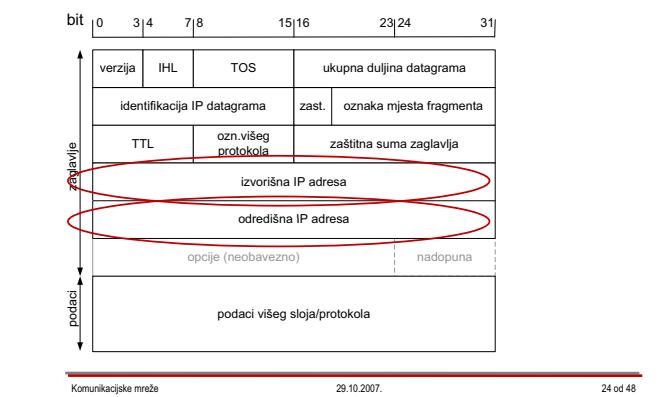
punjene: popunjavanje zaglavlja nulama do višekratnika od 32 bita.

[View all posts](#) | [View all categories](#)

IP začeljek – polja vezana uz ulogu omatanja

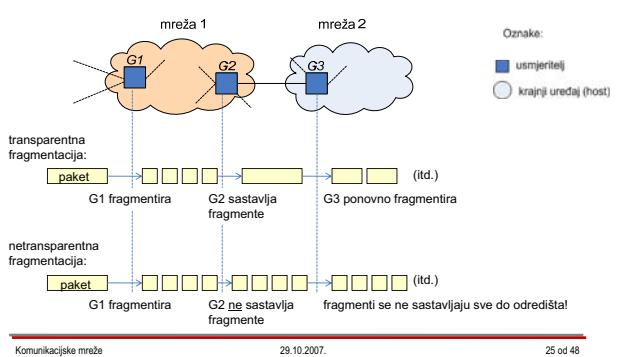


IP zaglavje – polja za adresiranje



Pojam fragmentacije

- ◆ transparentna fragmentacija –na ulazu/izlazu iz podmreže
 - ◆ netransparentna fragmentacija –fragmenti se sastavljaju na određenom računalu



Fragmentacija i sastavljanje IP datagrama

- datagram mora stati u podatkovno polje okvira protokola sloja podatkovne poveznice
 - pojam MTU - Maximum Transmission Unit
 - ovisi o tehnologiji izvedene mreže
 - na primjer, za Ethernet/IEEE 802.3: MTU=1500 byte
- ako je datagram veći od MTU, mora se podijeliti na dijelove odgovarajuće veličine – fragmente
 - fragmenti se šalju u novim, neovisnim datagramima i sastavljaju u originalni datagram na odredištu

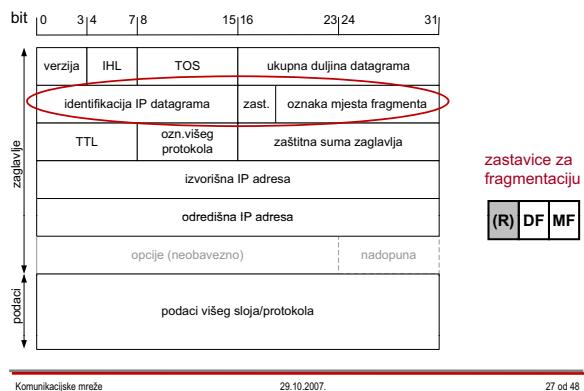


Komunikacijske mreže

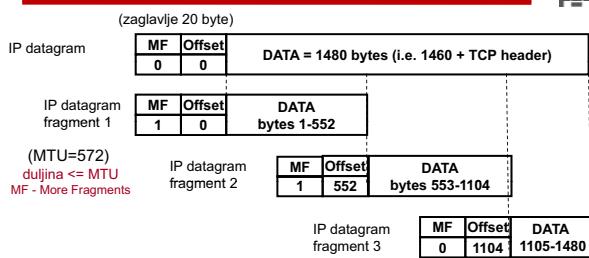
29.10.2007.

26 od 48

IP zaglavje – polja za fragmentaciju



Primjer fragmentacije



Zašto je fragmentacija nepoželjna?

- u slučaju gubitka fragmenta, cijeli datagram je uništen
- prenos se više kontrolnih podataka, a za istu korisnu informaciju (problem overheada!)

Komunikacijske mreže

29.10.2007.

28 od 48

Sadržaj predavanja

- Protokolni složaj TCP/IP
- Organizacija i struktura Interneta
- Protokol Internet Protocol (IP)
 - adresiranje i fragmentiranje
- Usmjeravanje u Internetu
 - načela usmjeravanja
 - protokoli usmjeravanja
 - dijagnostika problema
- Ostali protokoli važni za mrežni sloj
 - dinamičko dodjeljivanje adresa, razlučivanje adrese



Komunikacijske mreže

29.10.2007.

29 od 48

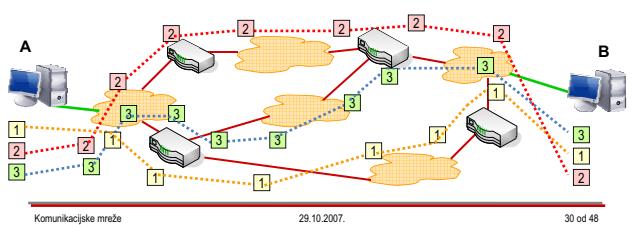
Literatura: knjiga "Osnovne arhitekture mreža", poglavlje Internet

Funkcionalnost mrežnog sloja

- nespojna, nepotvrđena usluga dostave datagrama između mrežnih sučelja
- svaki datagram usmjerava se neovisno o drugima, prema odredišnoj IP-adresi
- "best effort" usluga

Primjer:

- slijed slanja datagrama A → B: 1, 2, 3
- datagrami mogu putovati raznim putevima (ne često, ali se događa) i stići ovakvo: 3, 1, 2



Načela usmjeravanja paketa

- ◆ Osnovna upravljačka informacija (u zaglavju paketa):
 - ◆ izvorišna adresa (source address)
 - ◆ odredišna adresa (destination address)
 - ◆ ograničenje broja skokova na putu (TTL, hop limit)
- ◆ Područje usmjeravanja
 - ◆ usmjeravanje unutar autonomnog sustava
 - ◆ usmjeravanje između autonomnih sustava

Komunikacijske mreže

29.10.2007.



31 od 48

Format IP zaglavlja – polja važna za usmjeravanje

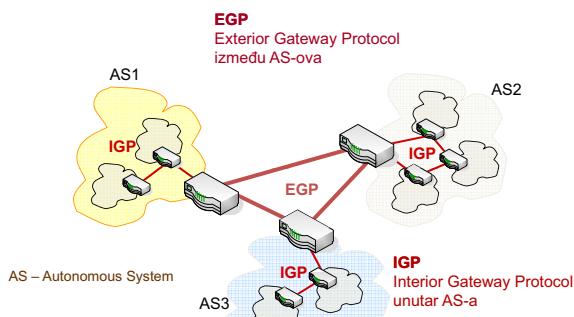


Komunikacijske mreže

29.10.2007.

32 od 48

Klasifikacija protokola usmjeravanja



Komunikacijske mreže

29.10.2007.

33 od 48

Stvarni protokoli

IGP protokoli:

- ◆ Routing Information Protocol (RIPv2)
 - ◆ temelji se na (dinamičkom) algoritmu vektora udaljenosti
- Open Shortest Path First Protocol (OSPFv2)
 - ◆ temelji se na (dinamičkom) algoritmu stanja poveznice

EGP protokol (u praksi, samo jedan!):

- ◆ Border Gateway Protocol (BGPv4)
 - ◆ algoritam vektora staza (engl. vector path)
 - ◆ sličan algoritmu vektora udaljenosti, ali uzima u obzir "staze" kao niz AS-ova na putu do odredišta

Komunikacijske mreže

29.10.2007.

34 od 48

Usmjeravanje u Internetu

- ◆ Internet je mreža s komutacijom paketa
- ◆ **usmjeravanje** – postupak pronađenja puta od izvorišnog do odredišnog čvora, izravno ili preko niza usmjeritelja i podmreža
 - zasnovano na **odredišnoj IP-adresi**
 - datagramske način rada – svaki paket (IP-datagram) usmjerava se neovisno o ostalima
- ◆ **usmjeritelj (usmjernik)** – sustav koji ima najmanje dva mrežna sučelja u dvije različite mreže
 - sadrži **tablicu usmjeravanja**

Komunikacijske mreže

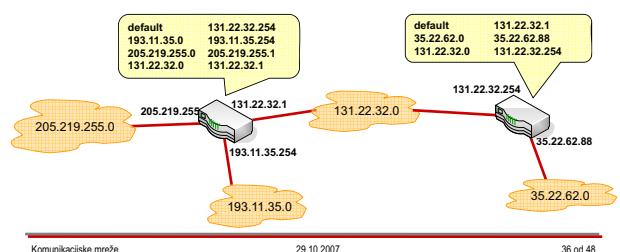
29.10.2007.

35 od 48



Tablica usmjeravanja

- ◆ tablica usmjeravanja = informacije koje usmjeritelji imaju o topologiji mreže
 - ◆ služi za odluku o odlaznom mrežnom sučelju za zadatu odredišnu IP adresu
 - ◆ unosi u tablici sadrže:
 - ◆ odredišnu adresu i adresu prvog sljedećeg usmjeritelja na putu ka odredištu
 - prepostavljeni put (default) – poseban unos koji se primjenjuje ako nema određenog puta



Komunikacijske mreže

29.10.2007.

36 od 48

Upravljanje tablicom usmjeravanja

- ◆ protokoli usmjeravanja izvedeni su u usmjeriteljima, a uključuju strategiju usmjeravanja i algoritme usmjeravanja
- ◆ svaki usmjeritelj održava svoju tablicu usmjeravanja
 - čuva popis mreža na koje je izravno spojen preko svojih sučelja
 - razmjenjuje informacije o usmjeravanju s drugim usmjeriteljima (odredišta za koja oni znaju put)
 - ažurira tablicu usmjeravanja na temelju:
 - informacija prikupljenih s vlastitih sučelja
 - znanja skupljenoj razmjenom informacija s drugim usmjeriteljima putem poruka
 - protokol usmjeravanja definira oblik i sadržaj poruka koje se razmjenjuju
- na osnovu podataka u tablici usmjeravanja, usmjeritelj za svaki datagram bira put i prosledjuje datagram po odabranom putu prema sljedećem usmjeritelju

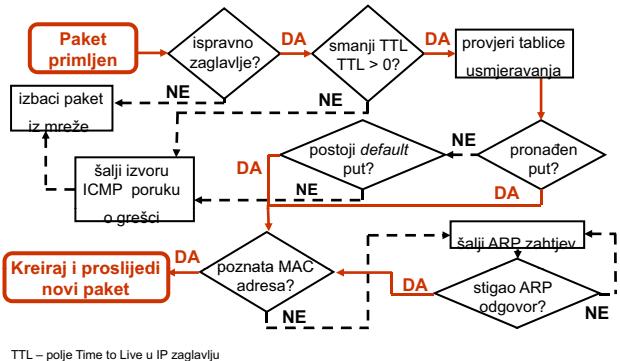
Komunikacijske mreže

29.10.2007.

37 od 48



Proces usmjeravanja paketa



Komunikacijske mreže

29.10.2007.

38 od 48



Protokol Internet Control Message Protocol

- ◆ ICMP služi za "dijagnostiku"!
- ◆ podsjetimo se: IP je jednostavan protokol
 - ♦ nepouzdan; nepotvrđena, bespojna usluga
 - ♦ sam nema mogućnost dojavе pogreške – to za njega radi ICMP
- ◆ ICMP definira mehanizam kojim se prenose dvije vrste kontrolnih poruka
 1. dojave o grešci – povratna informacija pošiljatelju o nekom problemu u mreži
 2. zahtjevi za informacijom – traži se informacija vezana za stanje u mreži
- ◆ ICMP ne ispravlja problem niti djeluje na temelju tih poruka, samo javlja stanje
- ◆ ICMP je proširiv - i drugi internetski protokoli osim IP-a mogu definirati svoje kontrolne poruke

Komunikacijske mreže

29.10.2007.

39 od 48



Slika prikazuje **proces usmjeravanja paketa**, odnosno što se događa s paketom kada ga primi usmjeritelj.

Dakle, kada usmjeritelj primi paket, prvo ispituje da li je ispravno zaglavje, odnosno provjerava zaštitnu sumu zaglavja. U slučaju da je zaglavje neispravno, izbacuje paket iz mreže.

U protivnom smanjuje TTL polje za jedan i provjerava da li je TTL = 0. Ako jest, izbacuje paket iz mreže i šalje ICMP poruku izvoruštu kojom ga obavještava da je došlo do greške. Inače provjerava tablicu usmjeravanja da vidi kojim putem treba usmjeriti paket (primjenjuje masku podmreže na odredišnu IP adresu).

Ako je put nepoznat, usmjerava ga na tzv. *default put*, a ako je poznat usmjerava ga navedenim putom. Da bi paket došao do odredišnog računala, potrebno je, na temelju IP adrese sazнати njegovu fizičku, MAC adresu. Ako MAC adresa nije poznata, šalje ARP zahtjev za MAC adresom tako dugo dok ne dobije odgovor.

Kada dobije odgovarajuću MAC adresu računala, proslijedi paket odredišnom računalu i u tom trenutku je proces usmjeravanja paketa završio.

Usmjeritelj je sada spremjan prihvati novi paket i ponoviti proces usmjeravanja.

0792 Internet Control Message Protocol. J. Postel. September 1981. (Format: TXT=30404 bytes) (Obsoletes RFC0777) (Updated by RFC0950) (Also STD0005) (Status: STANDARD)

ICMP - primjer: dijagnostika problema usmjeravanja

- Echo Request/Echo Reply – **ping** (1)
 - provjera je li odredište dohvatalno putem IP-a
- Time-to-Live (TTL) mehanizam – **traceroute** (1)
 - utvrđuje niz usmjeritelja kojim paket prolazi od izvora do odredišta

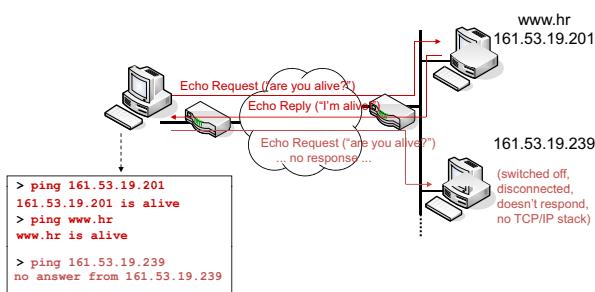
Komunikacijske mreže

29.10.2007.

40 od 48



ICMP - primjer: ping

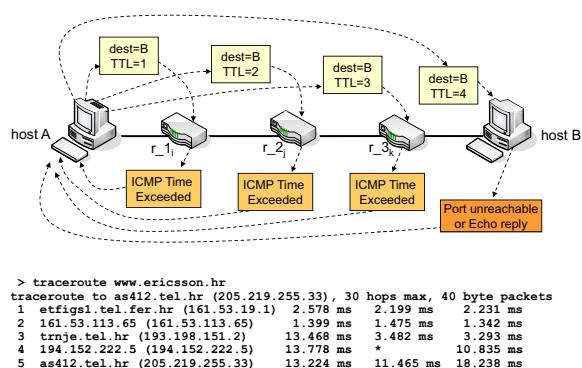


Komunikacijske mreže

29.10.2007.

41 od 48

ICMP - primjer: traceroute



Komunikacijske mreže

29.10.2007.

42 od 48

Sadržaj predavanja

- ◆ Protokolni složaj TCP/IP
- ◆ Organizacija i struktura Interneta
- ◆ Protokol Internet Protocol (IP)
 - ◆ adresiranje i fragmentiranje
- ◆ Usmjeravanje u Internetu
 - ◆ načela usmjeravanja
 - ◆ protokoli usmjeravanja
 - ◆ dijagnostika problema
- ◆ Ostali protokoli važni za mrežni sloj
 - ◆ dinamičko dodjeljivanje adresa, razlučivanje adrese

Komunikacijske mreže

29.10.2007.

43 od 48

Literatura: knjiga "Osnovne arhitekture mreža", poglavlje Internet

Ostali protokoli

- ◆ Dynamic Host Configuration Protocol (DHCP)
- ◆ Address Resolution Protocol (ARP)

Komunikacijske mreže

29.10.2007.

44 od 48

Protokol Dynamic Host Configuration Protocol (DHCP)

dvije uloge:

1. mehanizam dodjele IP adresa
 - ◆ administrator određuje raspon adresa koje DHCP poslužitelj može dodjeljivati klijentima
 - ◆ adresa se dodjeljuje na zahtjev, i to na određeno vrijeme ili dok je klijent ne vratiti
 - ◆ ista adresa višestruko se koristi (samo ne istovremeno!)
2. omogućuje klijentima da traže i poslužiteljima da daju i druge konfiguracijske parametre
 - ◆ npr. IP adresa, maska podmrežje, default usmjeritelj, adresa DNS-a, itd.

Komunikacijske mreže

29.10.2007.

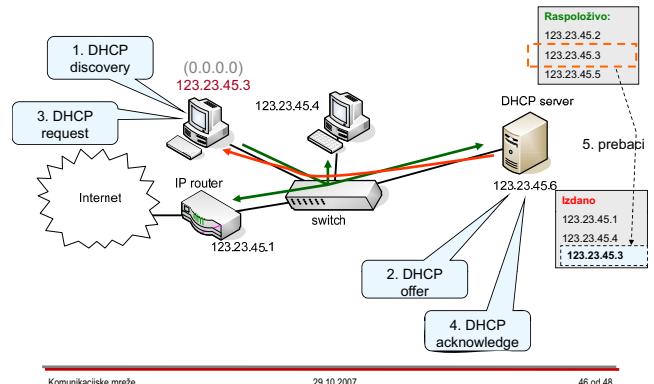
45 od 48

Protokol DHCP ima dvije glavne uloge:

1. Dodjela IP adresa
2. Konfiguracija TCP/IP parametara

Primjenjuje se vrlo često, i u privatnim mrežama (tada se dodjeljuju privatne adrese) i u javnim mrežama (na primjer, modemski ili ADSL pristup). Zavodi i laboratorijski na FER-u također (uglavnom) koriste DHCP za korisnička računala.

DHCP - primjer

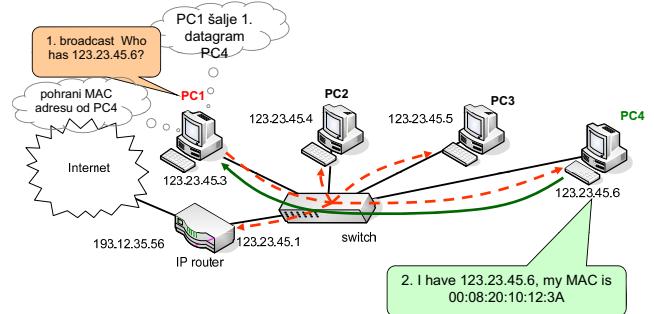


Protokol Address Resolution Protocol (ARP)



- ◆ protokol razlučivanja adrese
- ◆ dizajniran za mreže s dijeljenim medijem (npr. Ethernet)
- ◆ čemu služi ARP?
 - ◆ IP adrese su adrese mrežnog sloja - protokoli viših slojeva (transport, aplikacije, ali i usmjeravanje...) koriste mrežnu (IP) adresu
 - ◆ upravljač mrežne kartice prepoznaće samo MAC adrese
 - ◆ problem: kako dinamički povezati IP adresu s MAC adresom?
- ◆ način rada protokola ARP:
 - upit za IP adresu razasiliće se svim sučeljima na poveznici
 - upit primaju svi uređaji
 - odgovara samo onaj uređaj čija je IP adresa prozvana

ARP - primjer



- ◆ uparene adrese (IP adresa, MAC adresa) se pohranjuju u ARP-spremnik
- ◆ u spremniku se nalaze i statički i dinamički unosi
- ◆ dinamički unosi se automatski brišu ako se ne koriste (nekoliko minuta)

Komunikacijske mreže

7. (a)

Međusobno povezivanje mreža

Ak.g. 2007./2008.

31.10.2007

Sadržaj predavanja

♦ Pregled aktivnih mrežnih uređaja

- ♦ Obnavljač
- ♦ Parični obnavljač
- ♦ Most
- ♦ Komutator
- ♦ Usmjerivač

♦ Pravila spajanja

♦ Razdvajanje domena

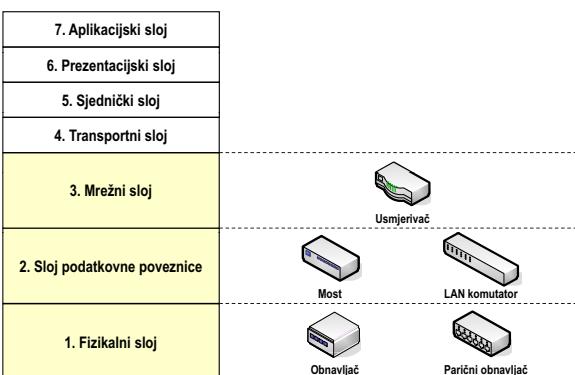
- ♦ Domene sudara
- ♦ Ethernet broadcast domene
- ♦ IP broadcast domene

Komunikacijske mreže

31.10.2007

2 od 21

Usporedba mrežnih uređaja



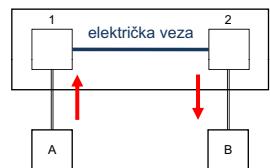
Komunikacijske mreže

31.10.2007

3 od 21

Obnavljač (repeater)

- ♦ Uredaj fizikalnog sloja
- ♦ Ne zna što su to okviri, paketi ili zaglavlja
- ♦ Pojačavanje primljenog signala
- ♦ Obnavljanje izvornog oblika i vremenskih odnosa u signalu



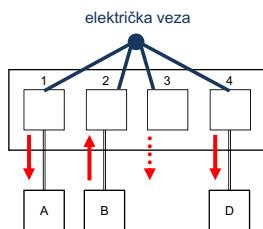
Komunikacijske mreže

31.10.2007

4 od 21

Parični obnavljač (hub)

- ♦ Uredaj fizikalnog sloja
- ♦ Ne zna što su to okviri, paketi ili zaglavlja
- ♦ Pojačavanje primljenog signala
- ♦ Ne razdvaja domene sudara i Ethernet broadcast domene
- ♦ Svi priključci rade na istoj brzini



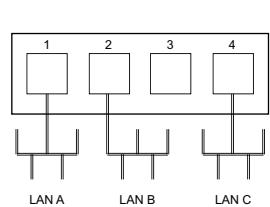
Komunikacijske mreže

31.10.2007

5 od 21

Most (bridge)

- ♦ Uredaj sloja podatkovne poveznice
- ♦ Povezivanje više LAN-ova
 - ♦ Različite vrste mreža (Ethernet, Token Ring, ...)
 - ♦ Različite brzine
- ♦ Prosljedjivanje okvira na temelju MAC adresa
- ♦ Razdvaja domene sudara, ali ne razdvaja Ethernet broadcast domene



Komunikacijske mreže

31.10.2007

6 od 21

LAN komutator (Layer 2 switch) (1)



- Uredaj sloja podatkovne poveznice
- Povezivanje više stanica
 - Iste vrste mreža (npr. Ethernet)
 - Različite brzine
- Prosljeđivanje okvira na temelju MAC adresa
 - Uparivanje oznaka priključaka i MAC adresa spojenih stanica
- Razdvaja domene sudara, ali ne razdvaja Ethernet broadcast domene



Komunikacijske mreže

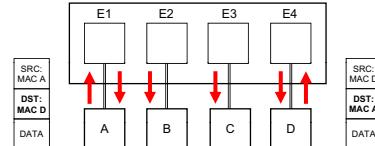
31.10.2007

7 od 21

LAN komutator (Layer 2 switch) (2)



Tablica komutiranja	
E1	A
E2	-
E3	-
E4	D



Komunikacijske mreže

31.10.2007

8 od 21

Usmjerivač (router)



- Uredaj mrežnog sloja
- Razdvaja domene sudara i Ethernet broadcast domene
- Ne razdvaja IP broadcast domene
- Svakom sučelju dodijeljene su MAC i IP adresa
- Sadrži tablicu usmjeravanja



Komunikacijske mreže

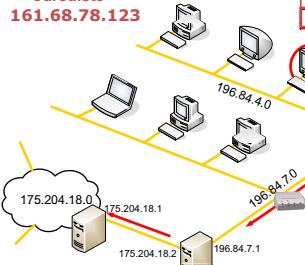
31.10.2007

9 od 21

Primjer usmjeravanja (1)



odredište
161.68.78.123



Odredišna mreža	Maska podmrežje	Gateway	Sučelje
196.84.4.0	255.255.255.0	196.84.4.12	196.84.4.12
default/0.0.0	0.0.0.0	196.84.4.1	196.84.4.12

161.68.78.0

Odredišna mreža	Maska podmrežje	Gateway	Sučelje
196.84.7.0	255.255.255.0	196.84.7.1	196.84.7.3
196.84.4.0	255.255.255.0	196.84.4.1	196.84.4.1
175.204.18.0	255.255.255.0	196.84.7.1	196.84.7.3
175.204.18.1	255.255.255.0	196.84.7.1	196.84.7.3
175.204.18.2	255.255.255.0	196.84.7.1	196.84.7.3
default/0.0.0	0.0.0.0	196.84.7.1	196.84.7.3

161.68.78.0

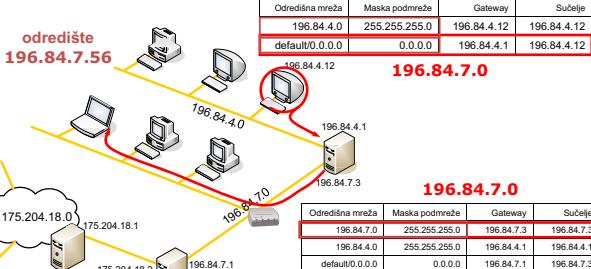
Odredišna mreža	Maska podmrežje	Gateway	Sučelje
196.84.7.0	255.255.255.0	196.84.7.1	196.84.7.1
196.84.4.0	255.255.255.0	196.84.4.1	196.84.4.1
175.204.18.0	255.255.255.0	175.204.18.2	175.204.18.2
175.204.18.1	255.255.255.0	175.204.18.2	175.204.18.2
175.204.18.2	255.255.255.0	175.204.18.2	175.204.18.2
default/0.0.0	0.0.0.0	175.204.18.1	175.204.18.2

Komunikacijske mreže

31.10.2007

10 od 21

Primjer usmjeravanja (2)



Odredišna mreža	Maska podmrežje	Gateway	Sučelje
196.84.4.0	255.255.255.0	196.84.4.12	196.84.4.12
default/0.0.0	0.0.0.0	196.84.4.1	196.84.4.12

196.84.7.0

Odredišna mreža	Maska podmrežje	Gateway	Sučelje
196.84.7.0	255.255.255.0	196.84.7.3	196.84.7.3
196.84.4.0	255.255.255.0	196.84.4.1	196.84.4.1
175.204.18.0	255.255.255.0	196.84.7.3	196.84.7.3
175.204.18.1	255.255.255.0	196.84.7.3	196.84.7.3
175.204.18.2	255.255.255.0	196.84.7.3	196.84.7.3
default/0.0.0	0.0.0.0	196.84.7.1	196.84.7.3

196.84.7.0

Komunikacijske mreže

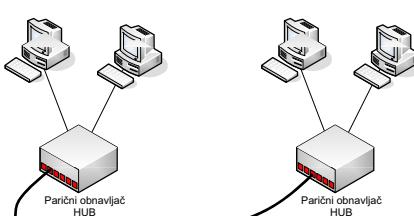
31.10.2007

11 od 21

Povezivanje mrežnih uređaja (1)



Da li je moguće ovakvo povezivanje mrežnih uređaja?



Komunikacijske mreže

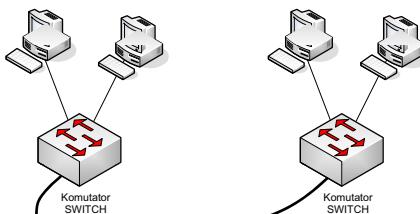
31.10.2007

12 od 21

Povezivanje mrežnih uređaja (2)



Da li je moguće ovakvo povezivanje mrežnih uređaja?



Komunikacijske mreže

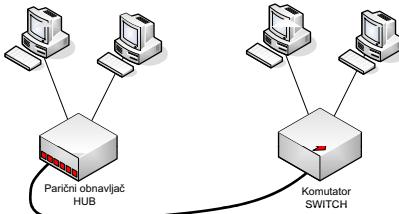
31.10.2007

13 od 21

Povezivanje mrežnih uređaja (3)



Da li je moguće ovakvo povezivanje mrežnih uređaja?



Komunikacijske mreže

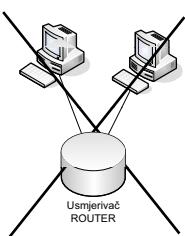
31.10.2007

14 od 21

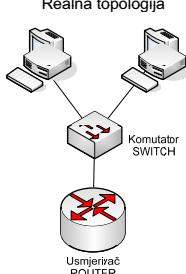
Povezivanje mrežnih uređaja (4)



"Mitska" topologija



Realna topologija



Komunikacijske mreže

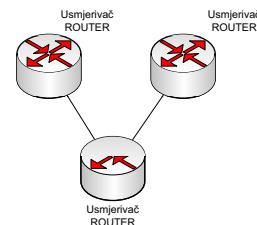
31.10.2007

15 od 21

Povezivanje mrežnih uređaja (5)



Je li ovo realna topologija?



Da! Često se usmjerivači povezuju direktno jer koriste i WAN tehnologije za povezivanje.

Komunikacijske mreže

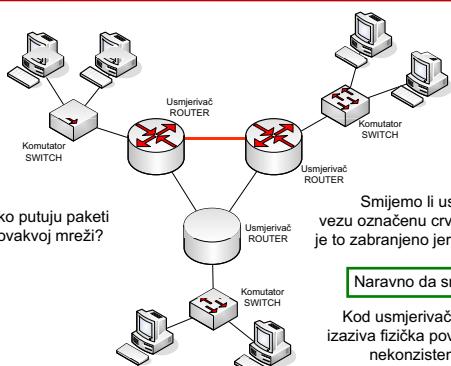
31.10.2007

16 od 21

Povezivanje mrežnih uređaja (6)



Kako putuju paketi u ovakvoj mreži?



Smijemo li uspostaviti vezu označenu crvenom bojom ili je to zabranjeno jer zatvara petlju?

Naravno da smijemo!

Kod usmjerivača, petlje ne izaziva fizička povezanost, već nekonzistentnost u usmjeravanju.

Komunikacijske mreže

31.10.2007

17 od 21

Povezivanje mrežnih uređaja (7)



Smijemo li uspostaviti vezu označenu crvenom bojom ili je to zabranjeno jer zatvara petlju?

Ne smijemo!

A što da su umjesto obnavljača iskorišteni komutatori?

Ne smijemo! (Ali, STP...)

Komunikacijske mreže

31.10.2007

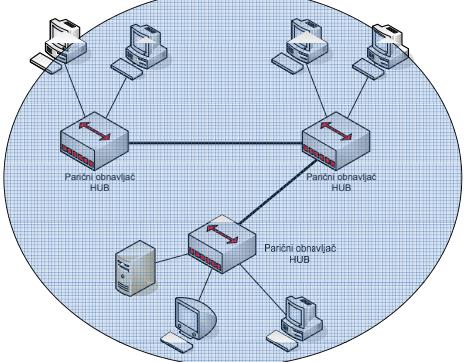
18 od 21

Razdvajanje domena (1)



Koliko ima kolizijskih domena?

Koliko ima Ethernet broadcast domena?



Komunikacijske mreže

31.10.2007

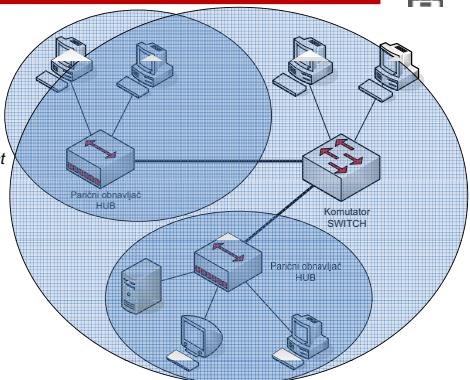
19 od 21

Razdvajanje domena (2)



Koliko ima kolizijskih domena?

Koliko ima Ethernet broadcast domena?



Komunikacijske mreže

31.10.2007

20 od 21

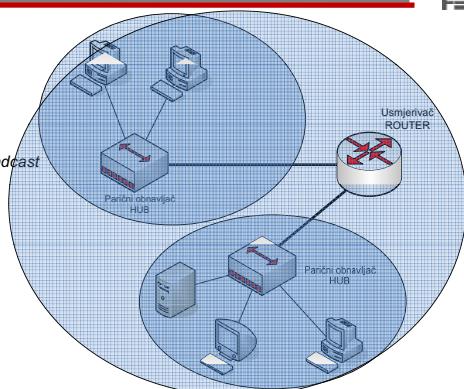
Razdvajanje domena (3)



Koliko ima kolizijskih domena?

Koliko ima Ethernet broadcast domena?

Koliko ima IP broadcast domena?



Komunikacijske mreže

31.10.2007

21 od 21

Komunikacijske mreže

7. (b)

Transportni sloj. Transportni protokoli u Internetu.

Ak.g. 2007./2008.

5.11.2007.

Zadaća transportnog sloja je prebacivanje podatkovnih jedinica transportnog sloja od izvora do odredišta, pri čemu su krajnje točke komunikacije aplikacijski *procesi*.

“Transparentnost” prijenosa znači da se ostvaruje logička veza među procesima, tj. da se oni međusobno “vide” kao da su izravno spojeni.

Transportni sloj oslanja se na mrežni sloj (i slojeve ispod mrežnog) za povezivanje preko niza mreža i podmreža. Transportni sloj “ne vidi” mrežnu infrastrukturu! Transportni sloj “vidi” mrežu isključivo preko pristupne točke mreži, tamo gdje predaje svoje podatkovne jedinice mrežnom sloju. Usluga transportnog sloja prema višim slojevima temelji se na skrivanju problema koji mogu nastati na nižim razinama od aplikacije.

U internetskom okruženju, glavne dvije vrste usluga transportnih protokola su:

- 1) pouzdana spojna transportna usluga preko nepouzdane, nespojne (datagramske) mrežne usluge koju nudi IP, i
- 2) nespojna nepouzdana transportna usluga (uz istu takvu mrežnu uslugu IP-a).

(U OSI okruženju definirano je 5 klasa transportnih protokola, s raznim svojstvima, kojima se nećemo baviti u ovom predmetu.)

Pouzdanost i kašnjenje su međusobno zavisni jer mehanizmi koji služe za pouzdan prijenos (detekcija pogrešaka, retransmisija, kontrola toka, ispravljanje redoslijeda, i sl.) ujedno povećavaju kašnjenje u slučaju da ih se mora primijeniti (greške, prekidi, gubici). Različiti transportni protokoli mogu ponuditi različite kombinacije parametara kvalitete usluge.

Podsetimo se

Zadaća transportnog sloja

- ◆ Transparentan prijenos transportnih jedinica podataka od izvora do odredišta
 - s kraja na kraj mreže (engl. *end-to-end*)
 - oslanja se na mrežni sloj, pruža (spojnu ili nespojnu) uslugu višem sloju (sjednički, prezentacijski, aplikacijski)
- ◆ prijenos uz zahtijevanu kvalitetu usluge:
 - pouzdana usluga - prijenos bez pogrešaka (dodatni mehanizmi za pouzdanost)
 - prijenos uz najmanje kašnjenje (minimalno procesiranje)

Komunikacijske mreže

5.11.2007.

2 od 44

Usluga transportnog sloja

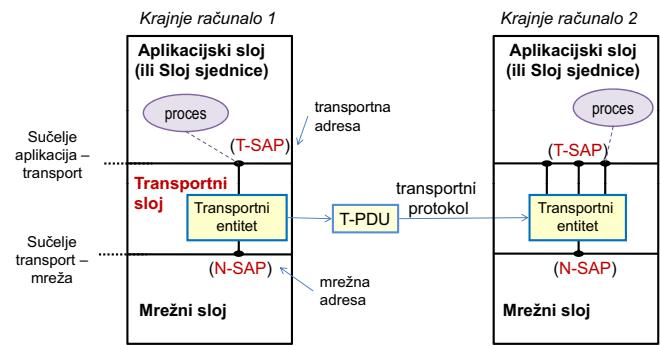


- ◆ svrha: omogućiti **logičko** povezivanje procesa na krajnjim računalima
- ◆ usluga može biti spojna i nespojna
- ◆ funkcije:
 - adresiranje (na razini transportnog sloja)
 - multipleksiranje
 - uspostava i raskid veze
 - kontrola toka i privremena pohrana
 - oporavak od prekida
- ◆ “kompenzacija nedostataka” mrežnog sloja
- ◆ izbor transportnog protokola ovisit će o parametrima kvalitete usluge koje zahtijeva aplikacija!

Logičko povezivanje procesa



logička veza – procesi koji komuniciraju ponašaju se kao da su izravno spojeni



Transportni entitet je proces koji sadrži izvedbu transportnog protokola na krajnjem računalu (najčešće izведен u jezgri operacijskog sustava, ili u korisničkom prostoru).
TPDU = Transport Protocol Data Unit – podatkovna jedinica sloja transporta
(Aplikacijski) proces je najčešće klijentski ili poslužiteljski program u korisničkom prostoru.

Adresiranje

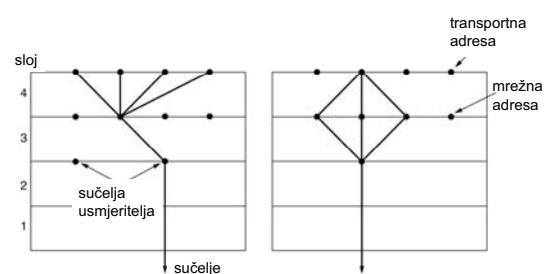
- ◆ na sučelju transporta i mreže: mrežna pristupna točka usluzi – N-SAP (Network-Service Access Point)
 - adresa mrežnog sučelja
 - u internetskom modelu: IP adresa
- ◆ na sučelju transporta i aplikacije: transportna pristupna točka usluzi – T-SAP (Transport-Service Access Point)
 - adresa transportnog entiteta
 - u internetskom modelu: vrata (engl. port)
- krajnje točke logičke veze:
(IP adresa izvora, vrata na izvoru) --- (IP adresa odredišta, vrata na odredištu)
 - u internetskom modelu: priključnica (engl. socket)
- ◆ multipleksiranje: način preslikavanja T-SAP:N-SAP
 - odozgo, n:1
 - odozdo, 1:n

Komunikacijske mreže

5.11.2007.

6 od 44

Multipleksiranje



- ◆ multipleksiranje odozgo: više procesa komunicira preko iste mrežne adrese
- npr: TCP, UDP
- ◆ multipleksiranje odozdo: proces otvara više mrežnih veza i šalje podatke naizmjence po njima

Komunikacijske mreže

5.11.2007.

7 od 44

Ustpostava veze

- ◆ kontrolne poruke: zahtjevi i odgovori u zadanom (dogovorenom) obliku
- ◆ mehanizmi:
 - ◆ numeracija poruka
 - ◆ (pozitivne) potvrde
 - ◆ negativne potvrde
 - ◆ vremenska kontrola
 - ◆ klizeći prozor
- ◆ vremenska kontrola (v.k.) nužna za slučajeve ispada ili gubitka zahtjeva/ potvrde

Komunikacijske mreže

5.11.2007.

8 od 44

Prilikom ustpostave logičke veze na razini transporta koriste se kontrolne poruke, tzv. "primitivi" transportne usluge.

Primitivi se koriste u formalnoj specifikaciji usluge i predstavljaju operacije koje su na raspolaganju korisniku

usluge. Za transportni sloj, radi se o uslugama tog sloja aplikacijskom sloju, odn. korisnik je aplikacijski proces.

Primitivi usluge općenito se dijele u četiri klase:

- zahtjev (engl. request) – entitet traži da se nešto napravi
- indikacija (engl. indication) – informacija entitetu o nekom događaju
- odgovor (engl. response) – odgovor entiteta na neki događaj
- potvrda (engl. confirm) – odgovor na prethodni zahtjev

Primitivi u sebi mogu nositi parametre one akcije ili događaja na koji se odnose.

Na primjer, primitivi za ustpostavu veze su CONNECT.request, CONNECT.response, itd.

Format poruka ovisi o izvedbi transportnog protokola.

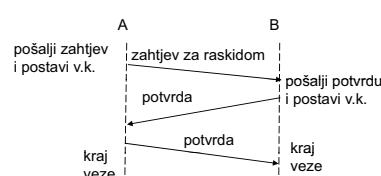
Primjena primitiva može se ilustrirati primjerom ustpostave veze.

Na slici je pokazan samo uspješan ishod trostrane razmjene poruka (engl. three-way handshake) prilikom ustpostave logičke veze.

Uočimo da gubitak bilo kontrolne poruke, bilo potvrde, treba rješavati posebno - na krajnjim točkama!

Raskid veze

- ◆ različiti scenariji urednog zatvaranja veze
- ◆ primjer:



- ◆ nužna vremenska kontrola (v.k.) za slučajeve ispada ili gubitka zahtjeva/ potvrde

Komunikacijske mreže

5.11.2007.

9 od 44

Na slici je pokazan samo uspješan ishod raskida logičke veze. Mogući problematični slučajevi su oni u kojima se izgubi bilo inicijalni zahtjev, bilo potvrda (ona prva od B, ili pak konačna povrda od A). Uočimo da je neophodno uvesti vremensku kontrolu za slučaj nedovršenog raskida veze, koja će prekinuti vezu nakon nekog vremena.



Kontrola toka i privremena pohrana

- ◆ kontrola toka – sličan problem kao u sloju podatkovne poveznice:
 - uskladijanje pošiljaljive brzine slanja i brzine primanja/obrade na strani primatelja
 - najčešći model kontrole toka – klizeći prozor!

- ◆ privremena pohrana – zbog nepouzdane dostave i moguće promjene redoslijeda datagrama
 - treba privremeno pohranjivati T-PDU
 - pohrana i prilikom slanja, i prilikom primanja!
 - rješenje: uskladijanje veličine klizećeg prozora i dinamičko rukovanje memoriskim spremnikom

Komunikacijske mreže

5.11.2007.

10 od 44

Oporavak (transportne veze) od prekida



- ◆ prekidi se događaju - moguća mjesta kvara:
 - krajnji uređaji
 - usmjeritelji

- ◆ kvar na usmjeritelju i krajnje točke sa očuvanim stanjem transportne veze – jednostavan oporavak
- ◆ ako je kvar na krajnjem uređaju - što se događa s transportnom vezom nakon ponovnog pokretanja?
 - teži problem, stanje nije sačuvano
 - općeniti zaključak: nemoguće je sasvim prikriti kvar od viših slojeva, ali vrijedi - prekid na sloju N može ispraviti sloj N+1 pod pretpostavkom da krajnje točke "znaju gdje su stale"

Komunikacijske mreže

5.11.2007.

11 od 44

Primjer Tannenbaum, section 6.2.6.

Slučaj kvara-ispada nekog od krajnjih uređaja:

Poстоje različite strategije oporavka izvedene na strani klijenta i poslužitelja, no za svaku od njih postoji neki (ne nužno isti) slučaj za koji je neuspješna.

Izbor transportnog protokola



Izbor transportnog protokola ovisi o parametrima kvalitete usluge (pouzdanost, kašnjenje, itd.) koje zahtijeva aplikacija!

Primjeri aplikacija – zahtjevnost /oština kriterija

Aplikacija	Pouzdanost	Kašnjenje	Kolebanje kašnjenja	Širina pojasa
Elektronička pošta	Visoki	Niski	Niski	Niski
Transfer datoteka	Visoki	Niski	Niski	Srednji
Pristup Webu	Visoki	Srednji	Niski	Srednji
Rad na daljinu	Visoki	Srednji	Srednji	Niski
Audio na zahtjev	Niski	Niski	Visoki	Srednji
Video na zahtjev	Niski	Niski	Visoki	Visoki
Telefonija	Niski	Visoki	Visoki	Niski/Srednji
Videokonferencija	Niski	Visoki	Visoki	Visoki

Komunikacijske mreže

5.11.2007.

12 od 44

Izbor transportnog protokola ovisi o parametrima kvalitete usluge (pouzdanost, kašnjenje, itd.) koje zahtijeva aplikacija!

U tablici su navedene neke poznate aplikacije i koliko su zahtjevi na pojedini kriterij oštiri, odn. ključni s motrišta korisnika.

Na ovo ćemo se osvrnuti prilikom analize potencijalnih primjena za internetske protokole TCP i UDP.

Oznake:

visoki – visoki kriteriji: jako važno za aplikaciju, ili važnije u odnosu na ostale kriterije

niski – niski kriteriji: manje važno ili nevažno za aplikaciju

(uz pretpostavku da su u svim slučajevima vrijednosti parametara u apsolutnim iznosima unutar prihvatljivih za normalno korištenje aplikacije)

Primjer: elektronička pošta

-pouzdanost je jako važna – želimo da poruka stigne na odredište u cijelosti i da bude identična originalu, dakle bez gubitaka

-kašnjenje nije važno – svejedno je putuje li poruka minutu ili dvije (nije pitanje sekunde ili manje!)

-kolebanje kašnjenja je prilično nevažno – ako kašnjenje pojedinih datagrama varira svejedno je, ionako se svi moraju skupiti na odredištu da bi se poruka rekonstruirala

-širina pojasa nije ključna – naravno, ako je veći, poruka će se prenijeti brže, ali ako malo i potraje, nije bitno

Ključne značajke protokola transportnog sloja



- ◆ dvosmjerna komunikacija
 - sposobnost istovremenog slanja i primanja
- ◆ pouzdanost transporta
 - detekcija gubitka paketa i eventualna reakcija
- ◆ transfer poruka ili niza okteta
 - dvije mogućnosti tretirajja podataka: kao blokovi/poruke, ili kao niz okteta
- ◆ očuvanje redoslijeda podataka
 - rekonstrukcija izvornog redoslijeda poruka ili okteta na odredištu za slučaj narušavanja redoslijeda pri prolasku kroz mrežu
- ◆ kontrola toka
 - uskladivanje brzina slanja i primanja podataka između krajnjih točaka (procesa)

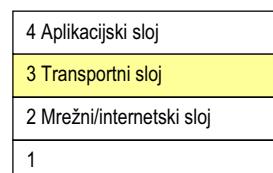
Protokoli transportnog sloja razlikuju se prema navedenim značajkama, koje ćemo ilustrirati na primjeru internetskih transportnih protokola, TCP i UDP.

Sadržaj predavanja



- ◆ Usluga transportnog sloja
- ◆ Funkcionalnost
 - adresiranje
 - multipleksiranje
 - uspostava i raskid veze
 - kontrola toka i privremena pohrana
 - oporavak od prekida
- ◆ Protokoli transportnog sloja u Internetu
 - Transmission Control Protocol
 - User Datagram Protocol

TCP/IP model: transportni sloj i protokoli



- ◆ transmisijski kontrolni protokol (*Transmission Control Protocol, TCP*)
 - pouzdana transportna usluga: prijenos niza okteta bez pogrešaka, uz isporuku potpune informacije u nepromijenjenom redoslijedu
- ◆ Korisnički datagramske protokol (*User Datagram Protocol, UDP*)
 - jednostavna transportna usluga: prijenos uz najmanje moguće kašnjenje informacije

Transmission Control Protocol - TCP



- ◆ TCP je spojno-orientirani, pouzdani internetski protokol transportnog sloja
 - TCP pruža spojnu uslugu transporta struje okteta povrh nespojnog IP-a
 - uspostavlja logičku vezu između procesa na krajnjim računalima
 - osigurava pouzdan transport s kraja na kraj pomoću mehanizama potvrde i retransmisije, uz očuvani redoslijed struje okteta i upravljanje transportnom vezom.
 - logička veza između procesa definirana je parom 16-bitnih transportnih adresa, koje se u internetskoj terminologiji nazivaju *vrrata* (engl. *port*).
 - TCP PDU naziva se **(TCP) segment**.

Protokoli koji djeluju na transportnom sloju TCP/IP protokolnog složaja su *Transmission Control Protocol (TCP)* i *User Datagram Protocol (UDP)*.

TCP je jedan od osnovnih protokola internetskog protokolnog složaja. Osnovna specifikacija protokola TCP je RFC 793 "Transmission Control Protocol", iz 9/1981.

U međuvremenu su nastala brojna proširenja i poboljšanja.

Pregledni dokument koji ukratko opisuje ostale RFC dokumente koji se odnose na TCP je relativno nedavni RFC 4614 iz 9/2006, pod nazivom "A Roadmap for Transmission Control Protocol (TCP) Specification Documents" ([ftp://ftp.rfc-editor.org/in-notes/rfc4614.txt](http://ftp.rfc-editor.org/in-notes/rfc4614.txt)).

TCP pruža spojnu uslugu (*connection-oriented*) transporta struje okteta povrh nespojnog (*connectionless*) IP-a, čime uspostavlja logičku vezu između procesa na krajnjim računalima. TCP osigurava pouzdan transport s kraja na kraj pomoću mehanizama potvrde i retransmisije, uz očuvani redoslijed struje okteta i upravljanje transportnom vezom.

Logička veza između procesa definirana je parom 16-bitnih transportnih adresa, koje se u internetskoj terminologiji nazivaju *vrrata* (engl. *port*).

U internetskoj terminologiji TCP PDU naziva se *TCP segment*. Najveća dopuštena veličina segmenta naziva se *Maximum Segment Size (MSS)* i ovisi o fizičkoj izvedbi mreže, odnosno *MTU (Maximum Transmission Unit)* mrežnog sloja umanjenoj za duljinu TCP i IP zaglavla.

Funkcionalnost TCP-a

◆ osnovne funkcije:

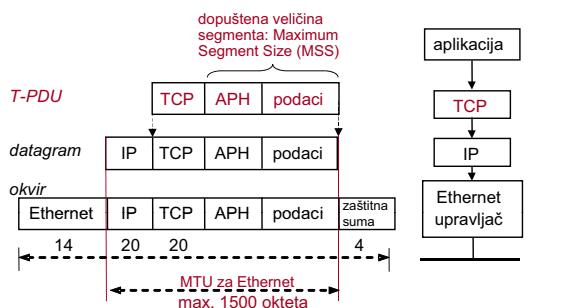
- osnovni transport podataka
- adresiranje i multipleksiranje
- pouzdanost
- upravljanje tokom
- upravljanje logičkom vezom
- prioritet i sigurnost (logičke veze, ne podataka!)

Funkcije TCP-a su:

- **osnovni transport podataka:** dvosmjerni transport kontinuiranog niza podataka pakiranjem okteta podataka u segmente koje potom predaje protokolu mrežnog sloja;
- **adresiranje i multipleksiranje:** više procesa na istom računalu može simultano koristiti TCP uporabom dodatne adresne informacije, odnosno broja vrata (port number);
- **pouzdanost:** TCP ima sposobnost oporavka od gubitaka, udvostrućenja, pogrešnog redoslijeda i pogreške u struji oktetova, jer dodjeljuje redni broj (sequence number) svakom oktetu koji predaje i traži da prijamna strana potvrdi ispravan prijam. Pogrešna informacija mora se ponovno poslati;
- **upravljanje tokom vezom:** mehanizam koji onemogućuje bržem pošiljatelju "preplavljivanje" sporijeg primatelja oktetima koje ovaj ne bi stigao obraditi; svaka potvrda popraćena je informacijom o veličini prozora (window) koji označuje koliko oktetova pošiljatelj smije odašlati prije prijema potvrde od primatelja;
- **upravljanje logičkom vezom:** logička veza između procesa uspostavlja se uporabom posebnih statusnih podataka prije početka komunikacije, i raskida se po obavljenoj komunikaciji;
- **prioritet i sigurnost:** posebni zahtjevi koje procesi mogu specificirati po potrebi i za pojedinačnu vezu (npr. urgent data, push, reset).

Transport podataka

- dvosmjerni transport kontinuiranog niza podataka, pakiranjem okteta podataka u **segmente**, koje potom predaje protokolu mrežnog sloja

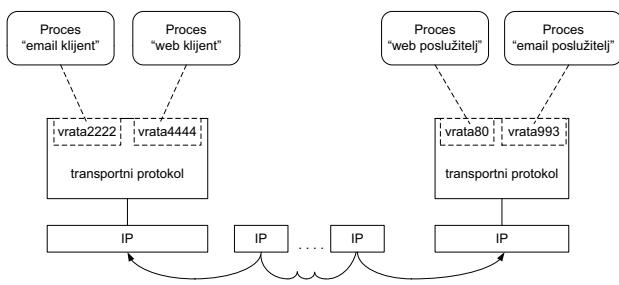


Pojam: najveća dopuštena veličina segmenta: Maximum Segment Size (MSS)

- zbrunjujući(!) naziv jer to nije duljina cijelog segmenta, već samo podatkovnog polja TPDUs!
- ovisi o fizičkoj izvedbi mreže, odnosno MTU (Maximum Transmission Unit) mrežnog sloja umanjenoj za duljinu TCP i IP zaglavija
- npr. MTU za Ethernet je 1500 oktetova, pa za MSS (uz pretpostavku da se ne koriste IP i TCP opcije) dobivamo: MSS=1500-20-20=1460 oktetova

Adresiranje i multipleksiranje

- ◆ raščlanjivanje tokova podataka koji pripadaju različitim procesima
- ◆ Krajnje točke komunikacije:
<IP adresa izvora, vrata na izvoru, IP adresa odredišta, vrata na odredištu>



Slika prikazuje primjer uspostave logičke TCP veze između procesa pokrenutih na krajnjim računalima. Treba napomenuti da logička veza između procesa nije istoznačna uspostavljenom putu usmjeravanja kroz mrežu. Pojedinačni paketi u istoj logičkoj vezi dostavljaju se preko nespojnog protokola IP.

Na istom računalu može se pokrenuti više procesa, budući da je svaki proces jednoznačno definiran dodatnom adresnom informacijom, odnosno brojem vrata.

Krajnje točke komunikacije između procesa nazivaju se *priklučnicama* (engl. socket). Priklučnica je definirana trima parametrima:

- transportni protokol (npr. TCP),
- IP adresa (npr. 161.53.19.10),
- broj vrata (npr. 80 za HTTP).

Logičko povezivanje procesa na višoj, aplikacijskoj razini nazivamo *asocijacijom*.

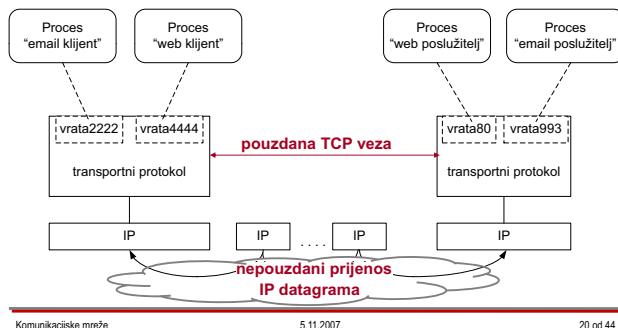
PRIMJER

Aplikacijski protokol HTTP (za Web) je jedan od onih koji koriste TCP kao transportni protokol. Asocijacija se uspostavlja između Web klijenta (preglednika) i Web poslužitelja.

Zamislimo da je računalo X (s IP adresom 152.22.41.55) osobno računalo spojeno na Internet, kojeg korisnik koristi za pregledavanje Web stranica, a računalo Y (s IP adresom 195.53.11.5) poslužiteljsko računalo s pokrenutim Web poslužiteljem. Na računalu X pokrenut je Web preglednik (proses A) koji preko vrata 4444 komunicira s Web poslužiteljem na dobro znanim vratima 80 na računalu Y. Asocijacija između Web preglednika i Web poslužitelja definirana je parom priključnica (tcp, 152.22.41.55, 4444) – (tcp, 195.53.11.5, 80).

TCP logička veza

- ♦ pouzdana TCP veza preko nepouzdanog datagramskog mrežnog sloja



Pouzdanost veze

- mehanizmi koji osiguravaju pouzdanost:
 - detekcija pogrešaka
 - retransmisija
 - kumulativna potvrda
 - vremenska kontrola
 - polja u zaglavljima koja služe za oznake segmenta u nizu i oznake potvrda

osnovna ideja:

- svaki segment je numeriran
- primatelj potvrđuje primjene segmente
- potvrda je kumulativna – potvrđuje sve oktete do onog na kojem se potvrda odnosi
- pošiljatelj postavlja vremensku kontrolu prilikom slanja segmenta
- ukoliko do isteka vremenske kontrole ne primi potvrdu, pošiljatelj smatra segment izgubljenim

važno! numeriraju se segmenti, ali taj broj NIJE redni broj segmenta, nego redni broj oktet-a koji je prvi u promatranoj segmentu!

Komunikacijske mreže

5.11.2007.

21 od 44

Mehanizmi kojima TCP osigurava pouzdan prijenos navedeni su na slici.

Struktura TCP segmenta



Komunikacijske mreže

5.11.2007.

22 od 44

TCP zaglavje sadrži sljedeća polja:

- izvorišna vrata: broj vrata procesa pošiljatelja na izvođačkoj strani,
- odredišna vrata: broj vrata procesa primatelja na odredišnoj strani,
- broj u nizu: redni broj onog oktet-a u nizu podataka koji je prvi u promatranoj segmentu,
- broj potvrde: redni broj sljedećeg oktet-a kojeg primatelj treba primiti, implicira potvrdu svih oktet-a prije toga,
- duljina zaglavja: broj 32-bitnih riječi sadržanih u zaglavju,
- rezerv.: bitovi rezervirani za buduće potrebe, ne koriste se,
- upravljački bitovi: bitovi za potvrdu i upravljanje transportnom vezom (URG, ACK, PSH, RST, SYN, FIN)
- veličina prozora: pošiljatelj segmenta oglašava najveći broj oktet-a koje je spreman primiti, odn. koje druga strana smije poslati prije prijema potvrde,
- zaštitna suma: zaštitni kod za otkrivanje pogrešaka u zaglavju i podacima (uzima se u obzir dio zaglavja, tzv. "pseudozaglavljek" i cijelo podatkovno polje),
- pokazivač hitnosti: pokazivač na početak hitnih podataka (urgent data) za koje se traži hitna, odnosno prioritetna obrada (npr. korisnički prekid kod interaktivnog rada (Ctrl+C)),
- opcije: posebne mogućnosti,
- punjenje: (ako su korištene opcije) popunjavanje zaglavja nulama do višekratnika od 32 bita.

(Uočimo da u zaglavju nema duljine segmenta. Ona je određena na temelju podataka u IP zaglavlj-u!)

Nakon TCP zaglavja slijede podaci aplikacijskog sloja.

Polja izvorišna vrata, odredišna vrata služe za adresiranje na razini transporta.

Polja broj u nizu, broj potvrde, veličina prozora služe za izvedbu mehanizma kliznih prozora u TCP-u.

Upravljački bitovi služe za razne kontrolne funkcije.

Opcije se mogu definirati razni parametri prilikom uspostavljanja veze.

Duljina zaglavja bez opcija je 20 oktet-a.

Nazivi i uloge upravljačkih bitova



upravljački bitovi

U	A	P	R	S	F
R	C	S	S	Y	I
G	K	H	T	N	N

uspostava i raskid veze:

- ♦ SYN (od engl. synchronize)

- ♦ FIN (od engl. finish)

potvrda:

- ♦ ACK (od engl. acknowledgement)

prioritetni podaci:

- ♦ URG (od engl. urgent)

- ♦ PSH (od engl. push)

poništavanje veze:

- ♦ RST (od engl. reset)

Komunikacijske mreže

5.11.2007.

23 od 44

Uspostava TCP veze

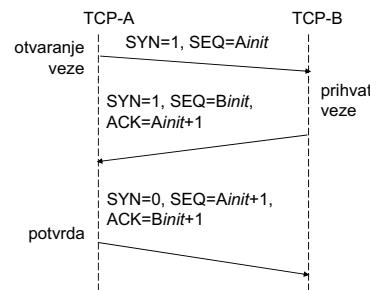


- Da bi ostvario svoje funkcije, TCP "pamti" niz parametara vezanih uz svaki par komunicirajućih procesa, odr. uz stanje logičke veze
 - ponašanje se može opisati automatom stanja
- Procedura uspostave veze:
 - svaka od strana mora poslati tzv. **SYN segment** u kojem objavljuje parametre bitne za vezu, npr.:
 - početni broj za numeraciju okteta
 - veličinu prozora
 - izvođačnu i odredišnu vrata
 - (može biti i drugih parametara, u opcijama)
 - strana koja primi SYN segment mora poslati potvrdu (ACK) da ga je primila

Uspostava TCP-veze



- prilikom uspostave veze, inicijaliziraju se parametri komunikacije



* nakon uspješne uspostave veze, slijedi razmjena podataka aplikacijskih procesa

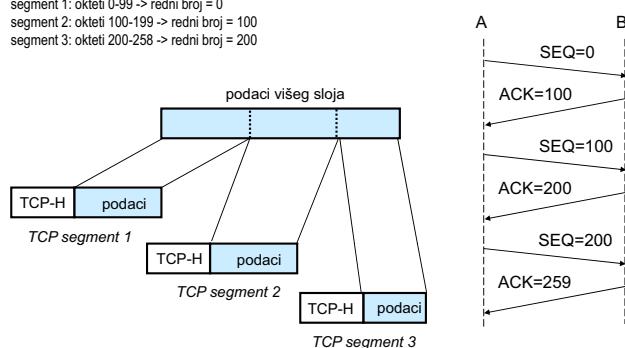
Primjer na ovoj i sljedećoj slici ilustrira mehanizme uspostavljanja i raskida TCP veze.

Otvaranje veze prolazi kroz trostranu proceduru uspostave veze (engl. *three-way handshake*), tijekom koje obje strane inicijaliziraju vezu i međusobno izmjenju svoje početne vrijednosti brojača segmenata. U prvoj poruci strana A inicira vezu (zastavica SYN je 1) i u zaglavljiju je postavljen početni redni broj za segmente od pošiljatelja (*Ainit*). Strana B potvrđuje uspostavu veze (ACK, zastavica SYN je 1) i u potvrdi ujedno šalje svoj početni redni broj (*Binit*), kojeg strana A potvrđuje trećom porukom (ACK, SYN=0). Nakon toga je veza uspostavljena te može uslijediti razmjena podatkovnih paketa.

Transport niza podatkovnih okteta - primjer



podaci 259 okteta
MSS = 100 oktet
segment 1: okteti 0-99 -> redni broj = 0
segment 2: okteti 100-199 -> redni broj = 100
segment 3: okteti 200-258 -> redni broj = 200



Primjer na slici ilustrira mehanizam označavanja broja segmenta i broja potvrda u TCP segmentu.

Uzmimo da je MSS=100 oktet i da pošiljatelj ima za poslati 259 oktet. Struja okteta dijeli se u odsječke duljine MSS, s tim da u ovom primjeru imamo dva cijela odsječka duljine MSS, odnosno 100 oktet, i jedan (zadnji) odsječak nešto kraći, od 59 oktet.

Podsjetimo se da **redni broj** označava redni broj **prvog okteta** u promatranoj segmentu, u odnosu na početak struje okteta; dok **broj potvrde** označava redni broj sljedećeg **očekivanog okteta** kojeg primatelj treba primiti.

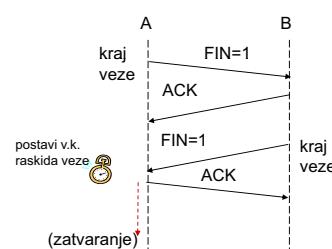
Ako pretpostavimo da je pošiljatelj inicijalizirao brojač segmenta na nulu na početku komunikacije (u stvarnosti se on postavlja po određenom algoritmu na slučajnu vrijednost), onda će redni broj u zaglavljiju prvog segmenta biti 0, redni broj u zaglavljiju drugog segmenta će biti 100, a redni broj u zaglavljiju trećeg segmenta će biti 200. Ukoliko su svi segmenti ispravno primljeni, potvrde će u zaglavljima redom imati brojove potvrda 100, 200, 259.

U ovom primjeru TCP-pošiljatelj šalje po jedan segment i čeka potvrdu za poslani segment prije slanja sljedećega. Naravno da takav način slanja nije učinkovit, niti se u stvarnosti koristi. Najveći dopušteni broj nepotvrđenih okteta koje TCP-pošiljatelj može poslati određen je veličinom prozora pošiljatelja.

Raskid TCP-veze



- kad aplikacije nemaju više podataka za poslati, započinju "dogovor" o raskidu veze



Raskid veze odvija se simetrično, budući da je veza dvosmjerna te svaka strana treba signalizirati zatvaranje svoga smjera komunikacije i primiti potvrdu te poruke. Poruka za raskid veze ima postavljenu zastavicu FIN. Za slučaj gubitka zadnje potvrde, postoji vremenska kontrola zatvaranja veze.



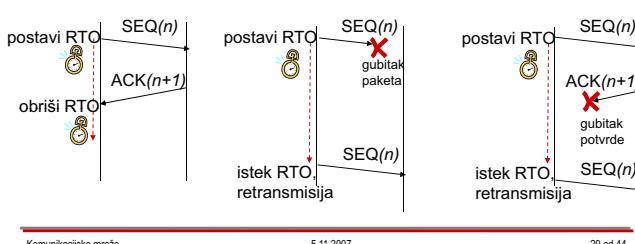
TCP – pouzdan prijenos

- ◆ Segmenti se u mreži mogu izgubiti iz više razloga
 - greške u prijenosu koje se ne daju ispraviti
 - usmjerivači ispuštaju pakete pri preopterećenosti linkova
 - petlje u usmjeravanju i TTL mehanizam
- ◆ TCP garantira da će poduzeti sve mjere da nadomjesti oktete izgubljene u mreži
 - ponavljanje slanja nakon određenog vremenskog perioda (*retransmission timeout, RTO*)
 - eksponencijalno produljivanje vremenskog intervala za ponavljanje slanja (*exponential backoff*)

Vremenska kontrola retransmisije



- ◆ TCP pošiljatelj postavlja RTO prilikom slanja segmenta
- ◆ ako potvrda za segment ne stigne do trenutka isteka RTO, pošiljatelj smatra segment izgubljenim i šalje ga ponovno



Primjer na slici ilustrira ponašanje RTO.

RTO se postavlja prilikom slanja segmenta i briše po primitu odgovarajuće potvrde.

S motrišta pošiljatelja, gubitak paketa i potvrde izgleda isto – učinak je taj da do isteka RTO ne dobiva potvrdu i nakon toga mora ponovno poslati isti paket.

Osim vremenske kontrole retransmisije, TCP ima još nekoliko vremenskih kontrola (npr. već spomenuto kontrolu zatvaranja veze), no njima se u ovom predavanju nećemo baviti.

TCP – kontrola toka

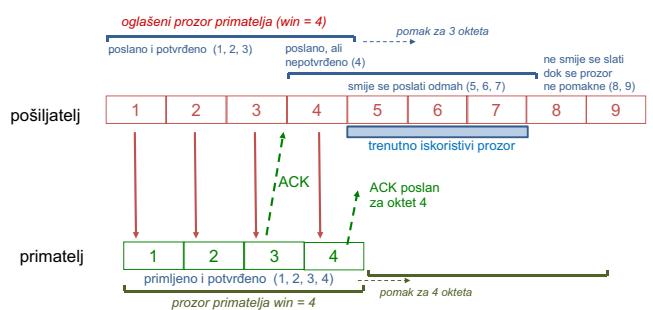


- ◆ Uslugačivanje brzine slanja i primanja
 - što ako pošiljatelj šalje brže nego što primatelj može obrađivati?
- ◆ TCP koristi mehanizam **klizećeg prozora**
 - prozor je broj okteta koje pošiljatelj u danom trenutku smije poslati a da ne čeka potvrdu bilo kojeg od tih oktetova
 - prozor objavljaju obje strane i to u sklopu potvrda koje šalju
- ◆ Primjer
 - pretpostavimo da je pošiljatelj primio potvrdu za oktet N-1 i u potvrdi je objavljen prozor W
 - pošiljatelj smije poslati sve oktete do N+W bez ikakve daljnje potvrde
 - međutim, ne smije poslati oktete od N+W nadalje sve dok mu se barem jedan dio oktetova prije N+W ne potvrdi

Mehanizmi upravljanja tokom



- ◆ prilagodba brzine slanja prema brzini primanja primatelja i stanju u mreži
- ◆ klizeći prozor - veličinom prozora je definiran max. broj nepotvrđenih okteta koje pošiljatelj može poslati odjednom



Mekanizam upravljanja tokom ima zadatak uskladiti brzinu slanja okteta s brzinom njihovog primanja, čime se sprječava da (pre)brzi pošiljatelj preplavi sporijeg primatelja. Na slici je ilustriran mehanizam klizćeg prozora.

Veličinom prozora određen je maksimalni broj nepotvrđenih oktetova koje pošiljatelj može poslati odjednom. Veličina prozora inicijalizira se prilikom uspostavljanja TCP-veze, kao manja od vrijednosti inicijalnih veličina prozora primatelja i prozora pošiljatelja (=polovi u zaglavju TCP segmenta).

Uzmimo niz oktetova na slici kao 1, 2, 3, ... Ako je prozor pošiljatelja $w=4$, to znači da pošiljatelj smije poslati 4 oktetova i nakon toga čekati dok ne počne dobivati potvrde. U ovom primjeru, pošiljatelj šalje okete 1, 2, 3, 4 i nakon toga čeka. Primatelj po primitu oketa 3 salje potvrdu, kojom potvrđuje okete 1-3. U trenutku kad pošiljatelj primi tu potvrdu prozor pošiljatelja "klizi" za tri oktetova i pošiljatelj (ne čekajući potvrdu za oktet 4) sada može poslati još i okete 5, 6 i 7 (trenutno iskoristivi prozor).

Ilustracija načina rada ovog mehanizma može se pogledati na:
http://www2.rad.com/networks/2004/sliding_window/

Ako je poznato vrijeme RTT (Round-trip-time) koje protekne od slanja segmenta do primitka potvrde o uspješnom primiku za taj segment, onda je maksimalna brzina koju može razviti TCP jednaka broju bitova koji se mogu poslati unutar prozora u vremenu RTT. Na primjer, ako je $w=4$ i $MSS = 1460$ oktetova, uz $RTT = 40$ ms dobivamo maksimalnu brzinu $(4 * 1460 * 8 \text{ bit}) / (40e-3) = 1,168 \text{ Mbit/s}$. Očito je da se, uz istu veličinu prozora, propusnost smanjuje kako RTT raste. Prosječna propusnost je (teorijski) oko $\frac{1}{4}$ maksimalne vrijednosti, zbog mehanizama upravljanja zagušenjem. U stvarnosti se, zbog gubitaka i mehanizama upravljanja zagušenjem, postignute vrijednosti kreću od oko 50% teoretskog maksimuma na više.

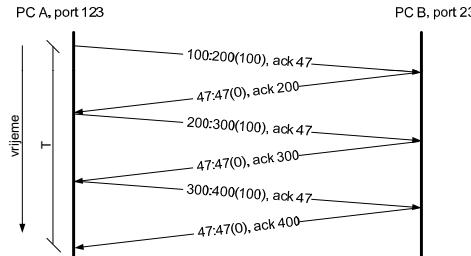
Utjecaj gubitaka: Ako se uzmu u obzir gubici, može se pokazati da je prosječna propusnost TCP veze jednaka $1.22 * MSS / (RTT * \text{sqrt}(L))$, gdje je L vjerojatnost gubitka segmenta. Pogledajmo kakva bi morala biti ta vjerojatnost da se postigne brzina od 10 Gbit/s. Dobivamo $2e-10$ (ekvivalent jednom izgubljenom segmentu na 5 miliardi)! Ta opažanja potaknula su razvoj novih inačica TCP-a za velike brzine.

Koja je uopće maksimalna moguća veličina prozora? Očito je da je ona u konkretnoj izvedbi TCP-a u operacijskom sustavu ograničena veličinom memoriskog spremnika za TCP vezu. U većini izvedbi ta vrijednost je obično inicijalno postavljena na 64 kB, s tim da se veće brzine može postići na veću vrijednost do najviše 1 MB. (Za to se koriste proširenja protokola TCP za velike brzine opisana u RFC1323, "TCP Extensions for High Performance" iz 1992.g. koja su danas implementirana u većini operacijskih sustava.)

TCP – kontrola toka

◆ Primjer:

Oznake: od:do(duljin), ack "oktet koji se potvrđuje"



Je li moguće prenijeti segmente sa slike u još kraćem vremenu?

Komunikacijske mreže

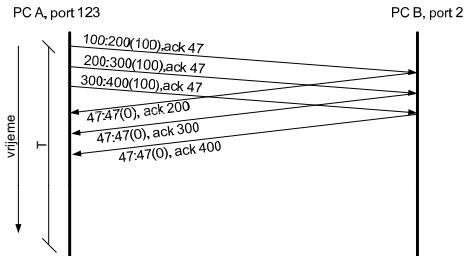
5.11.2007.

32 od 44

TCP – kontrola toka

◆ Pošiljatelj smije poslati više segmenata odjednom!

Oznake: od:do(duljin), ack "oktet koji se potvrđuje"



Komunikacijske mreže

5.11.2007.

33 od 44

TCP – kontrola zagušenja

◆ uvode se složeni mehanizmi kojima se TCP veza prilagođava (prepostavljenom) zagušenju u mreži

■ faze nastanka zagušenja:

- normalan rad: λ dovoljno manje od R
- početak zagušenja: λ se približava R
- nastupa zagušenje: $\lambda > R$
- drastičan pad performansi!

■ pitanja za TCP:

- kako detektirati zagušenje?
- ideja: učestali gubici, učestali istek RTO
- što napraviti?
- ideja: naglo smanjiti brzinu slanja, a zatim je postupno povećavati

Komunikacijske mreže

5.11.2007.

34 od 44

U 5. predavanju objašnjeni su razlozi nastanka zagušenja i načela upravljanja zagušenjem.

Jedan od razloga je kada su, na primjer, prometni tokovi iz raznih, neovisnih izvora u mreži takvi da unutar nekog usmjeritelja konvergiraju na isto izlazno sučelje, gdje se stvara se rep čekanja.

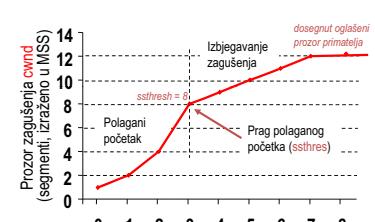
Zadržavanje u repu raste kako se rep puni (naranočasto područje) i povećava kašnjenje. Paketi i dalje prolaze, ali je propusnost na gornoj granici, jer se popunjenoš spremnika počinju približavati maksimumu. U trenutku kad se spremnici napune, dolazi do odbacivanja paketa, tj. gubitaka (crveno područje).

TCP – kontrola zagušenja

◆ TCP veza se nastoji dinamički prilagoditi raspoloživoj širini pojasa, uz "poštenu" podjelu s drugim vezama

- problem je što niješ pošiljatelj ne zna, niti može odrediti "svog dija"
- ideja – svatko za sebe postupno povećava brzinu slanja i prati stanje – cilj je da se opće stanje "stabilizira" i zagušenje popusti

- mehanizam: pošiljatelj uvodi još jedan "prozor": prozor zagušenja
- efektivni prozor pošiljatelja = $\min\{\text{oglašeni prozor primatelja}, \text{prozor zagušenja}\}$
- rukovanje prozorom zagušenja:
 - eksponencijalni rast u početku (faza "polaganji početak")
 - linearni rast kasnije (faza "izbjegavanje zagušenja")
- postoje i drugi mehanizmi upravljanja zagušenjem (i dalje se razvijaju!)



Komunikacijske mreže

5.11.2007.

35 od 44

Za one koje zanima ovo područje i žele znati više:

- TCP ima više mehanizama upravljanja zagušenjem:
 - polagan početak (engl. slow start)
 - izbjegavanje zagušenja (engl. congestion avoidance)
 - brza retransmisija (engl. fast retransmit)
 - brzi oporavak (engl. fast recovery)

Rezne izvedbe TCP-a imaju ugradene razne mehanizme, na primjer:

- TCP Tahoe: polagan početak, izbjegavanje zagušenja, brza retransmisija
- TCP Reno (temelj za većinu današnjih izvedbi TCP-a), sve što i TCP Tahoe + brzi oporavak
- TCP NewReno: TCP Reno + modificirani brzi oporavak (RFC 3782)

TCP-Selective Acknowledgements (TCP-SACK): TCP Reno + selektivne potvrdice

TCP-SACK omogućuje primatelju da javi pošiljatelju detaljniju informaciju o svim segmentima koji su uspješno primljeni, na temelju čega pošiljatelj može ponovno poslati samo one segmente koji su bili izgubljeni.



Oganičenja protokola TCP

◆ Što TCP ne radi?

- nema mehanizme za sigurnost i privatnost podataka
 - postoje razna rješenja na raznim slojevima
- ne vodi računa o granicama poruke
 - isporučuje niz okteta, neovisno o tome kako aplikacija pošiljatelja grupira podatke (ne vidi granice poruke)
- ne garantira isporuku višem sloju
 - ali se potrudi prije nego konačno odustane

Komunikacijske mreže

5.11.2007.

36 od 44

Primjena protokola TCP



- ◆ tamo gdje je aplikaciji najvažnija pouzdanost
 - transfer datoteka
 - elektronička pošta
 - Web
 - transakcijske primjene
 - rad na udaljenom računalu

Komunikacijske mreže

5.11.2007.

37 od 44

Sadržaj predavanja

- ◆ Usluga transportnog sloja
- ◆ Funkcionalnost
 - adresiranje
 - multipleksiranje
 - uspostava i raskid veze
 - kontrola toka i privremena pohrana
 - oporavak od prekida
- ◆ Protokoli transportnog sloja u Internetu
 - Transmission Control Protocol
 - User Datagram Protocol

Komunikacijske mreže

5.11.2007.

38 od 44

Protokol User Datagram Protocol



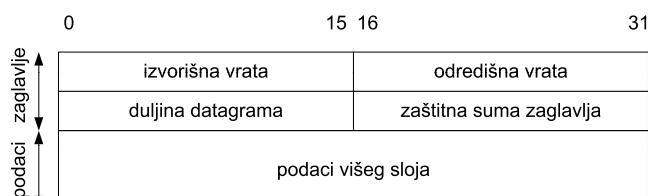
- ◆ Jednostavan transportni protokol
- ◆ Funkcije:
 - prima podatke od višeg sloja, omata ih u UDP datagram i proslijedi mrežnom sloju
 - minimalna funkcionalnost iznad IP-a: **multipleksiranje**
 - (opcionalno) radi zaštitnu sumu cijelog datagrama
- ◆ Ostale značajke:
 - nepouzdan prijenos
 - transfer blokova okteta (datagrami)
 - nema očuvanja redoslijeda
 - datagrami se isporučuju aplikaciji onim redoslijedom kojim su primljeni
 - ne pruža kontrolu toka - ako pošiljatelj prebrzo šalje, datagrami se gube

Komunikacijske mreže

5.11.2007.

39 od 44

Format UDP datagrama



Napomena: brojevi UDP-vrata neovisni od brojeva TCP-vrata!

Komunikacijske mreže

5.11.2007.

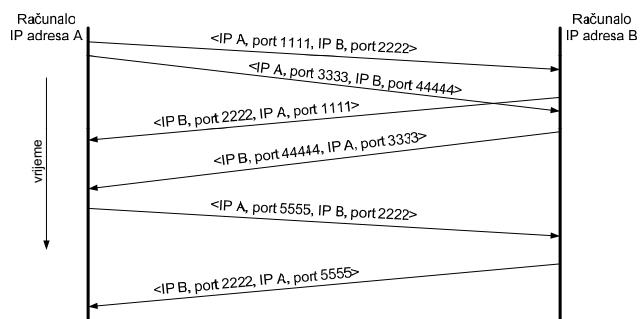
40 od 44

UDP zaglavje sadrži sljedeća polja:

- izvođačna vrata: broj vrata procesa pošiljatelja na izvođačnoj strani,
- odredišna vrata: broj vrata procesa primatelja na odredišnoj strani,
- duljina: broj okteta u UDP paketu, uključujući zaglavje i podatke,
- zaštitna suma zaglavja (opcionalna primjena, ali obavezna izvedba).

Nakon UDP zaglavja slijede podaci višeg (aplikacijskog) sloja.

UDP – primjer multipleksiranja tokova



Oznake: <IP adresa izvora, vrata na izvoru, IP adresa odredišta, vrata na odredištu>

Komunikacijske mreže

5.11.2007.

41 od 44

Koji parametri jednoznačno određuju par procesa koji komuniciraju?

<IP adresa izvora, port na izvoru, IP adresa odredišta, port na odredištu>

Ograničenja protokola UDP

◆ Što UDP ne radi?

- ne uspostavlja vezu prije slanja podataka
- ne potvrđuje primitak podataka
- ne garantira isporuku podataka
- ne otkriva gubitak paketa, niti radi retransmisiju izgubljenih paketa
- ne garantira očuvanje redoslijeda
- ne pruža kontrolu toka niti kontrolu zagušenja

OK, gdje se UDP koristi?

Komunikacijske mreže

5.11.2007.

42 od 44

Primjene protokola UDP



- ◆ tamo gdje je aplikaciji dostava podataka *na vrijeme* važnija od dostave *svih* poslanih podataka (prije ili kasnije)
 - višemedijske aplikacije u stvarnom vremenu
 - na primjer: internetska telefonija, višekorisničke igre
- ◆ pogodan za kratku komunikaciju (tamo gdje je *overhead* uspostave veze neprihvatljiv)
 - brzi zahtjev/odgovor
 - na primjer: upiti za razlučivanje adrese (DNS), dinamička dodjela adrese (DHCP)
- ◆ višeodredišne primjene i difuzija
 - način komunikacije 1:n ili n:m

Komunikacijske mreže

5.11.2007.

43 od 44

Osvrt na izbor transportnog sloja u aplikacijama

- ◆ Kako transportni sloj u Internet mreži utječe na maksimalnu brzinu kojom aplikacije mogu međusobno razmijenjivati podatke?
- ◆ Ako TCP pošiljatelj želi poslati veliku količinu podataka primatelju, o čemu sve ovisi brzina kojom će podaci biti preneseni?
 - ponavljanje slanja
 - kontrola toka
 - kontrola zagušenja
- ◆ A kod UDP-a?
 - aplikacije moraju same voditi računa o ispuštenim podacima i same moraju prilagođavati brzinu uvjetima u mreži

Komunikacijske mreže

5.11.2007.

44 od 44

Zaključimo – koji transportni protokol je pogodniji za aplikacije navedene na sl. 12?

Elektronička pošta - TCP

Transfer datoteka - TCP

Pristup Webu - TCP

Rad na daljinu - TCP

Audio na zahtjev - UDP

Video na zahtjev - UDP

Telefonijska - UDP

Videokonferencija - UDP

Komunikacijske mreže

8.
Sjednički sloj, prezentacijski sloj, aplikacijski sloj. Usluge i protokoli aplikacijskog sloja u Internetu.

Ak.g. 2007./2008.

12.11.2007

Podsetimo se...

Referentni model OSI

7 Aplikacijski sloj
6 Prezentacijski sloj
5 Sjednički sloj
4 Transportni sloj
3 Mrežni sloj
2 Sloj podatkovnog linka/veze
1 Fizikalni sloj

Referentni model TCP/IP

4 Aplikacijski sloj
3 Transportni sloj
2 Mrežni sloj
1

Komunikacijske mreže

12.11.2007



2 od 89

U sjedničkom sloju u OSI modelu obavlja se uskladivanje sustava koji međusobno komuniciraju: uspostavljanje, održavanje i prekidanje dijaloga, dodjela prava za komuniciranje i nastavljanje komunikacije u slučaju prekida. (U TCP-IP modelu neke od tih funkcija obavlja transportni sloj, a većinu aplikacijski sloj).

Prezentacijski model u OSI modelu bavi se prikazom (sintaksom) i značenjem informacije (semantika) koja se izmjenjuje. U tom sloju definiraju se: kodovi, formati i struktura podataka. Aplikacijski sloj sadrži skup protokola za korisničke usluge i primjene. U tom sloju djeluju aplikacijski (računalni procesi).

Prezentacijski i sjednički sloj u modelu TCP/IP ne postoje, a njihova funkcionalnost pokrivena je u najvećoj mjeri aplikacijskim slojem.

Središnji slojevi, transportni i mrežni, oba modela podudaraju se, iako ne u potpunosti.

Sloj podatkovnog linka i fizikalni sloj nisu obuhvaćeni modelom TCP/IP, ali se mogu pretpostaviti u sloju ispod mrežnog.

Internetski model: 4. aplikacijski sloj



- ◆ aplikacijski protokoli za različite usluge i primjene
- ◆ korisnički, npr.:
 - SMTP (Simple Mail Transfer Protocol): elektronička pošta
 - HTTP (Hyper Text Transfer Protocol): WWW
- ◆ sustavski, npr.:
 - DNS (Domain Name System): sustav imenovanja domena

4 Aplikacijski sloj
3 Transportni sloj
2 Mrežni/internetski sloj
1

Komunikacijske mreže

12.11.2007

3 od 89

Sadržaj predavanja



◆ Osnove internetskih usluga

- usluge i aplikacijski protokoli
- modeli izvedbe usluga
- pronaalaženje usluga
- programska podrška

◆ Odabранe internetske usluge i protokoli aplikacijskog sloja

- Sustav domenskih imena
- World Wide Web
- Elektronička pošta

Osnove internetskih usluga



◆ aplikacijski protokol

- vrste poruka
- sintaksa poruka – propisani formati poruka
- semantika poruka – značenje polja u poruci
- pravila kako se poruke razmjenjuju

◆ model izvedbe usluge

- najčešći model: klijent/poslužitelj
- postoje i drugi modeli (o tome kasnije)

◆ program klijenta

◆ program poslužitelja

Usluge i aplikacijski protokoli u Internetu



- ◆ usluge:
 - prijenos datoteka
 - rad na daljinu
 - elektronička pošta
 - mrežne novosti
 - interaktivne usluge
 - imenička usluga
 - globalni informacijski sustav
 - ...

- ◆ aplikacijski protokoli:
 - FTP, ...
 - TELNET, ...
 - SMTP, POP, IMAP, ...
 - NNTP, ...
 - IRC, H.323, ...
 - LDAP, X.500, ...
 - HTTP, ...
 - ...

Komunikacijske mreže

12.11.2007

6 od 89



Modeli izvedbe usluge

- ◆ model **klijent-poslužitelj** (engl. *client-server*)
 - više izvedbi: model s jednim poslužiteljem i model s više poslužitelja
 - posebni slučajevi:
 - posrednički (proxy) poslužitelji
 - međuspremnički (caching) poslužitelji
- ◆ model s ravnopravnim procesima (engl. *peer-to-peer*)
 - svaki proces je u "klijent" i "poslužitelj", uloge nisu odvojene
- ◆ postoje i druga rješenja:
 - pokretni kód, pokretni agenti, i dr.

Komunikacijske mreže

12.11.2007

7 od 89

Uz pojmove klijenta i poslužitelja ...



- ◆ ovisno o kontekstu, pojmovi **klijent**, odnosno **poslužitelj**, mogu se odnositi na:
 - klijentsko **računalo** ili klijentski **proces**
 - poslužiteljsko **računalo** ili poslužiteljski **proces**
- ◆ **proces** je instanca izvođenja (klijentskog ili poslužiteljskog) **programa**
- ◆ programi klijenta i poslužitelja mogu se izvoditi na istom računalu, ali glavna prednost je u mrežnom radu
- ◆ u dalnjim razmatranjima, uglavnom ćemo govoriti o klijentima i poslužiteljima u smislu **procesa**

Komunikacijske mreže

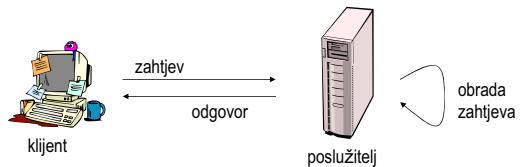
12.11.2007

8 od 89

Model klijent-poslužitelj



- ◆ izvedba usluge u modelu klijent/poslužitelj podijeljena je između programa *klijenta* i programa *poslužitelja*
- ◆ koristi se u većini internetskih usluga
- ◆ komunikacija se temelji na nizu zahtjeva i odgovora:
 - Klijent traži uslugu od poslužitelja (slanjem zahtjeva)
 - poslužitelj obrađuje zahtjev i odgovara klijentu šaljući rezultat obrade



Komunikacijske mreže

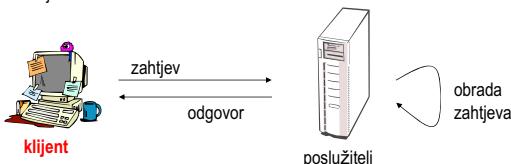
12.11.2007

9 od 89

Program klijenta



- ◆ "program klijenta" je programska podrška koja omogućuje računalu da djeluje kao *klijent* u opisanom modelu
- ◆ proces izvođenja klijentskog programa najčešće pokreće korisnik
- ◆ osnovni zadaci:
 - pruža **korisničko sučelje** koje korisniku omogućuje slanje zahtjeva poslužitelju
 - odgovarajuće formatira zahtjev kako bi ga poslužitelj mogao "razumjeti"
 - odgovarajuće formatira poslužiteljev odgovor kako bi ga korisnik mogao razumjeti



Komunikacijske mreže

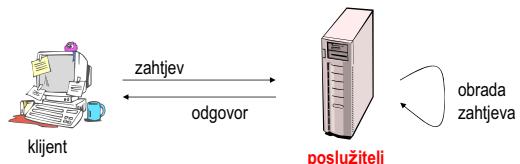
12.11.2007

10 od 89



Program poslužitelja

- ◆ program poslužitelja je programska podrška koja omogućuje računalu da djeluje kao *poslužitelj* u opisanom modelu
- ◆ proces izvođenja poslužiteljskog programa najčešće se pokreće automatski, prilikom pokretanja operacijskog sustava
- ◆ osnovni zadaci:
 - osluškuje i prihvata zahtjeve klijen(a)ta
 - obrađuje zahtjeve i odgovara šaljući rezultat obrade klijentu(im)



Komunikacijske mreže

12.11.2007

11 od 89

Način rada poslužitelja



- ♦ klasifikacija prema pamćenju stanja može biti:

- memoriski, čuva (pamti) stanje (engl. *statefull*)
 - obrada zahtjeva ovisi o rezultatu obrade prethodnih zahtjeva
 - pogodan za obradu niza međusobno povezanih zahtjeva
 - može se modelirati automatom stanja
- bezmemoriski, ne čuva (ne pamti) stanje (engl. *stateless*)
 - obrada svakog zahtjeva je neovisna o prethodnim
 - pogodan za obradu pojedinačnih, međusobno neovisnih zahtjeva
 - jednostavan model, samo jedno stanje - "obradi i zaboravi"

- ♦ klasifikacija prema načinu obrade zahtjeva:

- iterativan
- konkurentan

Komunikacijske mreže

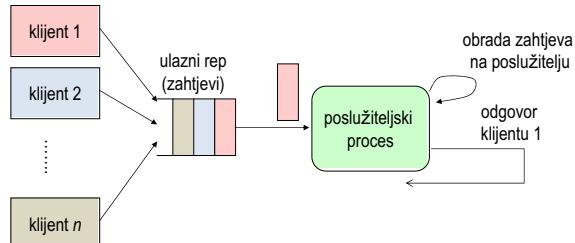
12.11.2007

12 od 89

Iterativni poslužitelj



- ♦ zahtjevi se obrađuju *iterativno*, tj. jedan-po-jedan
- ♦ poslužiteljski proces obrađuje zahtjeve i šalje odgovore
- ♦ jednostavniji; pogodan za zahtjeve s kratkim vremenom obrade



Komunikacijske mreže

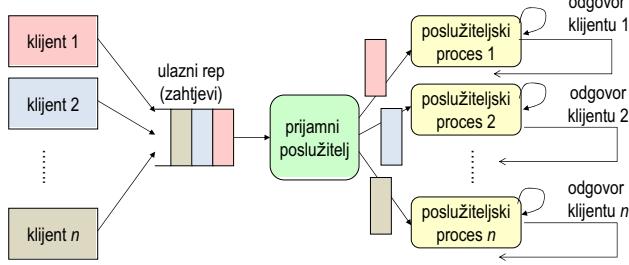
12.11.2007

13 od 89

Konkurentni poslužitelj



- ♦ zahtjevi se obrađuju *konkurentno*
- ♦ prijamni poslužitelj prima zahtjeve, ali ih ne obraduje sam, već raspoređuje posao obrade i odgovora na poslužiteljske procese
- ♦ složeniji; pogodan za više istovremenih ili dugotrajnijih obrada zahtjeva



Komunikacijske mreže

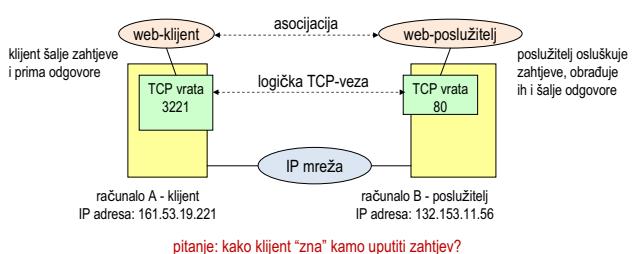
12.11.2007

14 od 89

Asocijacija klijenta i poslužitelja



- ♦ asocijacija: uspostavljen odnos između procesa klijenta i poslužitelja površ jedne transportne veze (npr. logička TCP veza) ili povezanosti (npr. UDP binding)
- ♦ za asocijaciju između klijenta i poslužitelja mora se znati:
 - aplikacijski protokol
 - IP adrese klijenta i poslužitelja
 - transportni protokol (TCP/ UDP) i brojne vrata za klijentski i poslužiteljski proces



Komunikacijske mreže

12.11.2007

15 od 89

Asocijacija predstavlja "komunikacijski kanal" između procesa klijenta i poslužitelja. Svaka asocijacija odgovara jednoj transportnoj vezi.

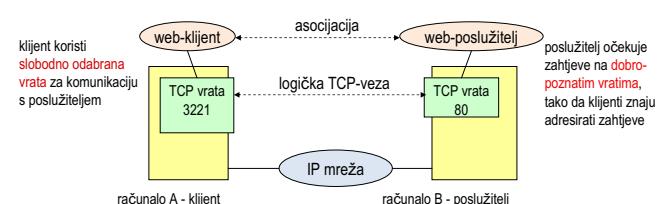
Uočimo: 1. klijent mora unaprijed znati adresu procesa poslužitelja
2. poslužitelj ne mora unaprijed znati adresu klijenta jer će je saznati iz zahtjeva

Primjer na slici ilustrira uslugu weba.

Pronalaženje usluga



- ♦ klijent mora unaprijed znati adresu poslužitelja da bi mu pristupio
- ♦ na razini cijelog Interneta, unaprijed su definirana *dobro-poznata vrata* (engl. well-known port) za standardne internetske usluge
- ♦ za usluge koje nemaju dobro-poznata vrata, mora postojati neki drugačiji način (npr. imenička usluga)



Komunikacijske mreže

12.11.2007

16 od 89

prije, RFC 1700 Assigned Numbers, sada on-line podaci na <http://www.iana.org/numbers.html>

Klijenti koji traže uslugu za koju ne postoji dobro-poznata vrata moraju nekako drugaćije saznati broj vrata kojeg trebaju slati zahtjeve (npr. putem imeničke usluge ili neke druge usluge koja sama koristi dobro-poznata vrata).

Neka dobro-poznata vrata

- ♦ dobro-poznata vrata: 0-1023 su "rezervirana" za standardne usluge
- ♦ primjeri nekih dobro-poznatih vrata:

Keyword	Decimal	Description
ftp-data	20/tcp	File Transfer [Default Data]
ftp-data	20/udp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
ssh	22/tcp	SSH Remote Login Protocol
ssh	22/udp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
...		
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer
...		
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
...		
http	80/tcp	World Wide Web HTTP

Komunikacijske mreže

12.11.2007

17 od 89

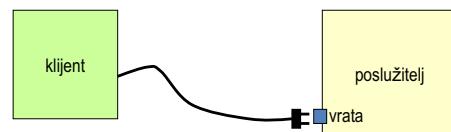
IANA definira dodjelu portova:

<http://www.iana.org/assignments/port-numbers>

- dobro-poznata vrata (well-known ports): 0-1023 su "rezervirana" za standardne usluge
- registrirana vrata (registered ports) za neke druge uobičajene usluge: 1024-49151
- dinamička i/ili privatna vrata (dynamic and/or private ports): 49152-65535

Programsko sučelje (socket API)

- ♦ socket (priključnica) je programska apstrakcija krajnje točke komunikacije između klijenta i poslužitelja



©

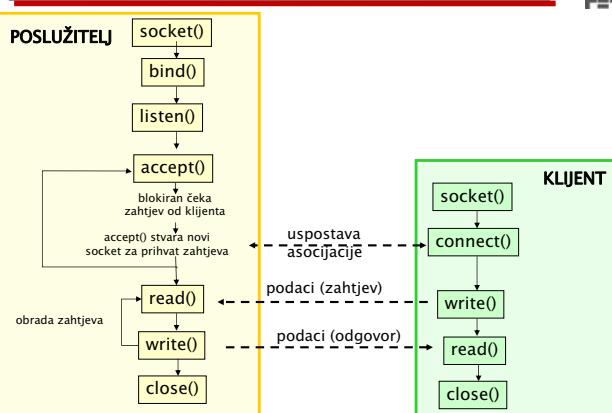
- ideja: klijent se "priključi" na vrata poslužitelja
- "priključenjem" se stvara asocijacija između procesa – to je prepostavka za daljnju komunikaciju
- socket = (IP adresa, transp. protokol, broj vrata)
- primjer: priključnica na strani Web poslužitelja (161.53.19.220, TCP, 80)

Komunikacijske mreže

12.11.2007

18 od 89

Socket API - tipične radnje klijenta i poslužitelja



Komunikacijske mreže

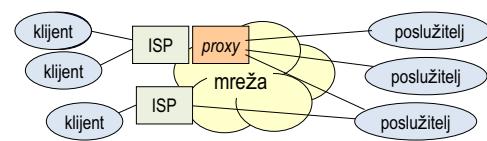
12.11.2007

19 od 89

Gdje usluge mogu biti smještene?



- ♦ na poslužitelju (uobičajen slučaj)
 - npr. pretraživači, e-trgovina, poslužitelji sadržaja i drugih usluga vezanih za odredište
- ♦ djelomično (i) na klijentu (npr. Java, JavaScript, ActiveX dodaci za Web)
 - npr. provjera unesenih podataka na web-obrascu prije slanja zahtjeva
- ♦ "negdje između"
 - posrednički poslužitelj (engl. proxy)



Komunikacijske mreže

12.11.2007

20 od 89

Uloge i primjeri posredničkih poslužitelja



◆ "klasična" posrednička uloga

- dobavljanje podataka za klijenta od nekog drugog poslužitelja
- posredovanje pri dohvatu sadržaja (kompresija, filtriranje, anonimizacija, jezično prevođenje, ...)
- prikupljanje sadržaja s više poslužitelja

◆ međuspremnička uloga

- privremeno pohranjivanje sadržaja (engl. *caching*)
- pohranjivanjem sadržaja dobiva se brži odziv jer se često traženi podaci uzimaju iz lokalnog spremnika umjesto s udaljenog poslužitelja (primjeri primjene: Web, DNS)

◆ nadzor i ograničenje pristupa

- filtriranje prometa (primjer: *firewall*)
- ograničenja u dolasku ili odlasku, najčešće na rubu interne poslovne mreže

Komunikacijske mreže

12.11.2007

21 od 89

Sadržaj predavanja



◆ Osnove internetskih usluga

- usluge i aplikacijski protokoli
- modeli izvedbe usluga
- pronalaženje usluga
- programska podrška

◆ Odabrane internetske usluge i protokoli aplikacijskog sloja

■ **Sustav domenskih imena**

- World Wide Web

- Elektronička pošta

Komunikacijske mreže

12.11.2007

22 od 89

Sustav domenskih imena



◆ engl. *Domain Name System (DNS)*

◆ "imenik Interneta"

◆ pridružuje razne vrste informacija *imenu domene*

- najčešća uporaba: pridruživanje numeričke IP adrese lako pamtljivom imenu računala
- postoje i druge uporabe

◆ DNS je jedna od sustavskih usluga u Internetu – njome se služe druge internetske usluge, a krajnji korisnici (uglavnom) ne

Komunikacijske mreže

12.11.2007

23 od 89

Glavni RFC-ovi:

•RFC 1035 (Standard: STD 13)

Domain Names—Implementation and Specification by P. Mockapetris
Nov-1987

updated by RFCs 1101, 1122, 1183, 1706, 1876, 1982, 1995, 1996, 2136, 2137, 2181, 2308, 2535, 2782, 2845, 3425 and RFC 3658; obsoletes RFCs 882, 883 and 973

•RFC 1034 (Standard: STD 13)

Domain Names—Concepts and Facilities by P. Mockapetris
Nov-1987

updated by RFCs 1101, 1122, 1183, 1706, 1876, 1982, 2181, 2308 and 2535; obsoletes RFCs 882, 883 and 973

Popis RFC-ova vezanih uz DNS:

<http://www.dns.net/dnsrd/rfc/>

Podsjetimo se...



IP adresa - 32 bita (IPv4):

- ◆ identifikator koji globalno i jednoznačno određuje mrežno sučelje
- ◆ način zapisa:

- numerički zapis: binarni i dekadski

10100001 00110101 01001000 00010111
161 . 53 . 72 . 23

- simbolički zapis: lako pamtljiv (npr. www.fer.hr) – veza: **DNS**
www.fer.hr → 161.53.72.23

analogija: Ivo Ivić → tel. broj +385 1 1234 567
DNS je nešto kao "imenik" Interneta!

Komunikacijske mreže

12.11.2007

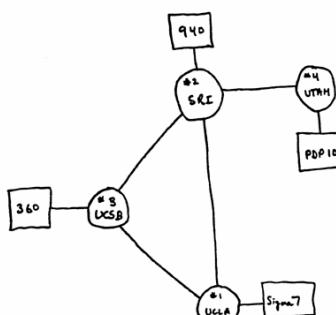
24 od 89

Veza simboličko ime – IP adresa, nekad davno



Skica ARPANET-a iz 1969.

– 4 čvora



dovoljan popis
IP adresa svih
računala s kojima
komuniciramo ☺

datoteka
hosts.txt

sredinom 1980.-tih
potreba za skalabilnim
rješenjem - **DNS**

http://www.computerhistory.org/internet_history/

Komunikacijske mreže

12.11.2007

25 od 89

Hijerarhija domena

- ◆ Vrh hijerarhije (.)
- ◆ Domene najviše razine, vršne domene

- generičke domene najviše razine

- engl. generic Top Level Domain (**gTLD**)
- ima ih samo 20: sedam početnih (.com, .edu, .gov, .int, .mil, .net, .org), te trinaest dodanih kasnije (.biz, .info., travel, ...)
- u 2007. postignut dogovor o pravilima za otvaranje novih gTLD

- domene najviše razine prema kodu države

- engl. country code Top Level Domain (**ccTLD**)
- ima ih više od 240
- standardne dvozlovne oznake država (popis ISO 3166-1)
- ccTLD za Hrvatsku - oznaka **hr**

- ◆ Poddomene, hijerarhijski organizirane (stablo)

Komunikacijske mreže

12.11.2007

30 od 89



Izvorni engleski nazivi:

- root DNS server
- generic Top Level Domain (gTLD)
- country code Top Level Domain (ccTLD)

Popis gTLD:

<http://www.iana.org/gtld/gtld.htm>

Pravila za nove gTLD:

<http://www.icann.org/meetings/lisbon/agenda-gnso-26mar07.htm>

Pravila dodjele ccTLD:

<http://www.iana.org/cctld/>

Registracija imena u DNS-u

- ◆ hijerarhijom domena upravlja ICANN, odn. IANA
- ◆ postoje tijela kojima se delegira odgovornost za domenu

- u Hrvatskoj: **CARNet**

- upravljanje vršnom domenom ".hr"
- registracija domena unutar domene ".hr"
- CARNet DNS služba <http://www.dns.hr/>



primjer:
registrirana
domena "fer.hr"

Komunikacijske mreže

12.11.2007

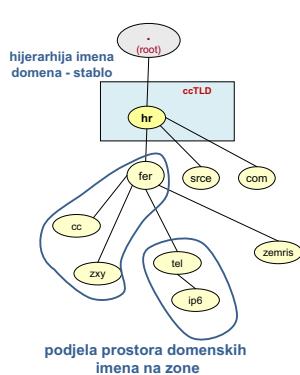
31 od 89



Organizacija sustava DNS (1/2)

- ◆ DNS je organiziran kao hijerarhijska distribuirana baza podataka

- postoji vrhovni ili "korijenski" DNS-poslužitelj na vrhu hijerarhije
- niti jedan DNS-poslužitelj nema popis svih domenskih imena!
- neki DNS-poslužitelji nadležni su za dio prostora domenskih imena – to može biti **domena ili zona** (= više domena, dio "stabla")



Komunikacijske mreže

12.11.2007



Poстојi vrhovni ili "korijenski" DNS-poslužitelj na vrhu hijerarhije (engl. *root DNS server*).

U praksi, za "root server" postoji 13 identičnih instalacija širom svijeta. Popis root servera može se naći na: <http://www.root-servers.org/>

Zona je podskup globalnog domenskog prostora imena, za kojeg se može delegirati odgovornost. Razlozi podjele na zone su tehnički, administrativni, ili oboje. Zona može obuhvaćati jednu domenu ili više njih (dio "stabla"), ali bez preklapanja! Jedna od najpoznatijih zona je *root zone*. Zapisi u root serveru obuhvaćaju popis domenskih imena i IP adresa DNS-poslužitelja nadležnih za sve gTLD i ccTLD.

Vrste zapisa u DNS-u

- ◆ podaci:

- zapisi o domeni i o pojedinim računalima (engl. *Resource Record*)
- definiran "rok trajanja" informacije (engl. *Time To Live*)

- ◆ vrste zapisa:

- za razlučivanje IP adrese krajnjeg računala:

zapis tipa **A**:

quark IN A 161.76.21.4

- za razlučivanje imena i IP adrese poslužitelja elektroničke pošte:

zapis tipa **MX** (mail exchange):

mail IN MX 161.76.21.10

- postoje i druge vrste zapisa, definira ih IANA

Komunikacijske mreže

12.11.2007



33 od 89

Zapis se izvorno naziva Resource Record.

Vrste DNS zapisa definira IANA.

<http://www.iana.org/assignments/dns-parameters>

Osim A i MX zapisa, pokazanih na slajdu, primjeri češće korištenih zapisa su:

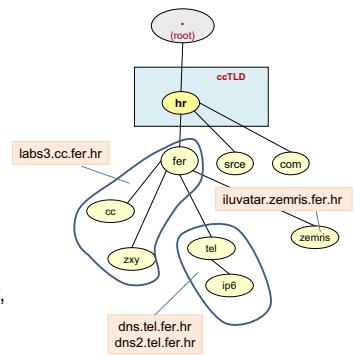
- SOA – parametri za zonu
- NS – ime poslužitelja za ovu domenu
- CNAME – kanonsko ime
- PTR – obrnuti upit – ime za zadani IP adresu

Organizacija sustava DNS (2/2)

- ◆ pitanje: podjela "odgovornosti" za točnost podataka?

- ◆ DNS-poslužitelj nadležan za domenu (zonu) ima potpun i ispravan popis podataka o toj domeni (zoni)

- ◆ ostali DNS-ovi, za upite koji se odnose na tu zonu, djeluju kao posrednici: "pitaju" nadležne i privremeno pohranjuju odgovor, kojeg (dok vrijedi) mogu vratiti na upite za istom adresom



Komunikacijske mreže

12.11.2007

34 od 89

DNS-administrator može konfigurirati DNS-poslužitelj tako da ima "nadležnost" (engl. authority) za zadani domenu/zonu. Nadležni poslužitelj ima potpuni popis podataka o domeni/zoni (engl. zone file), odnosno, o svim DNS poslužiteljima za tu domenu/zonu. Obično postoji barem dva nadležna poslužitelja za domenu/zonu, koji se nazivaju primarni i sekundarni.

Prilikom odgovaranja na DNS upit, odgovor može dati prvi DNS poslužitelj koji ima važeću informaciju. Odgovor kojeg šalje nadležni poslužitelj za zadani domenu (ili koji se temelji na lokalno pohranjenoj kopiji takvog odgovora, uz vremensko ograničenje informacije) naziva se "autorativnim", a onaj koji je doiven od bilo kojeg drugog poslužitelja naziva se "ne-autorativnim" (engl. non-authoritative).

Uočimo da je autorativni poslužitelj za jednu domenu u pravilu ne-autorativni za neku drugu.

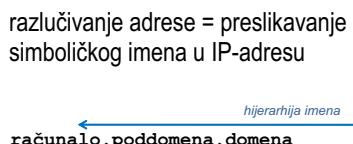
Ne-autorativni odgovor uvijek sadrži adresu izvora (npr. onog poslužitelja od kojeg je potekao pohranjeni odgovor) i trajnost zapisa (npr. 60 minuta).

Poštov i caching poslužitelji koji djeluju samo kao posrednici, tj. privremeno pohranjuju rezultate upita, a nisu autorativni za jednu domenu. Takvi poslužitelji su vrlo česti i uvođeni su radi poboljšanja performansi, odnosno mogućnosti raspoređivanja opterećenja te bržeg odgovaranja na upite.

Postupak razlučivanja IP adrese

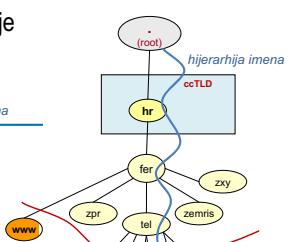
- ◆ logički gledano:

razlučivanje adrese = preslikavanje simboličkog imena u IP-adresu



- ◆ izvedbeno:

"prolaz" kroz hijerarhiju stabla domenskih imena odgovara nizu upita prema poslužiteljima nadležnim za zonu/domenu



Komunikacijske mreže

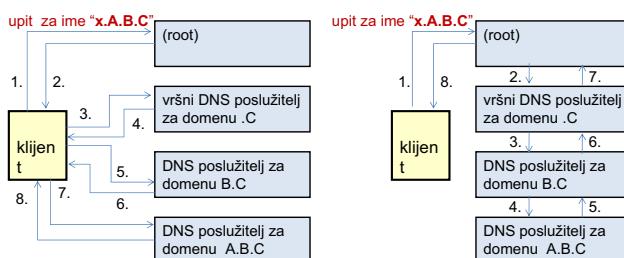
12.11.2007

35 od 89

Načini razlučivanja adrese

◆ iterativni način

- klijent iterativno formira i šalje zahteve dok ne dođe do poslužitelja koji ima traženu informaciju



Komunikacijske mreže

12.11.2007

36 od 89

◆ rekursivni način

- poslužitelj vraća traženu informaciju ako je imao; inače sam "pita dalje" (ponaša se kao klijent – rekursija)

Iterativni način rada:

Na iterativni upit klijenta, poslužitelj odgovara ili s konačnim odgovorom (traženom IP-adresom) ili imenom poslužitelja koji je "blizi" traženoj informaciji. Klijent mora iterativno formirati i slati nove zahtjeve, dok ne dođe do poslužitelja koji ima traženu informaciju.

Razmjena poruka na slici ima sljedeća značenja:

- 1.upit za adresu od x.A.B.C, upućen root DNS poslužitelju
- 2.odgovor sadrži ime vršnog poslužitelja za domenu C
- 3.upit za adresu x.A.B.C, upućen vršnom poslužitelju za domenu C
- 4.odgovor sadrži ime vršnog poslužitelja za domenu B.C
- 5.upit za adresu x.A.B.C, upućen vršnom poslužitelju za domenu B.C
- 6.odgovor sadrži ime vršnog poslužitelja za domenu A.B.C
- 7.upit za adresu x.A.B.C, upućen vršnom poslužitelju za domenu A.B.C
- 8.odgovor sadrži IP adresu računala x.A.B.C

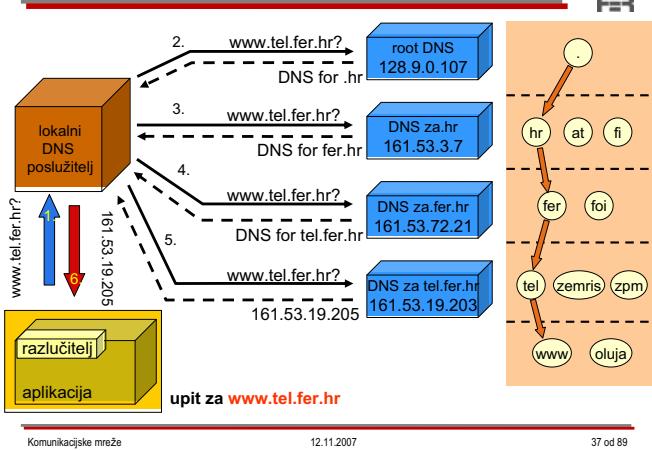
Rekursivni način rada:

Na rekursivni upit klijenta, poslužitelj odgovara s konačnim odgovorom, odnosno traženom IP-adresom ako je imao; u suprotnom on preuzima odgovornost slanjem zahtjeva sljedećem poslužitelju, ponašajući se prema njemu kao klijent (rekurzija).

Razmjena poruka na slici ima sljedeća značenja:

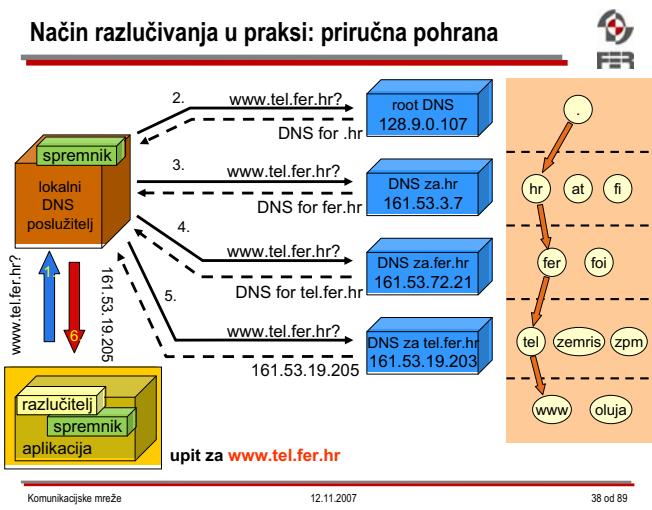
- 1.upit za adresu od x.A.B.C, upućen root DNS poslužitelju
- 2.upit za adresu x.A.B.C, upućen vršnom poslužitelju za domenu C
- 3.upit za adresu x.A.B.C, upućen vršnom poslužitelju za domenu B.C
- 4.upit za adresu x.A.B.C, upućen vršnom poslužitelju za domenu A.B.C
- 5.odgovor sadrži IP adresu računala x.A.B.C
- 6.odgovor sadrži IP adresu računala x.A.B.C
- 7.odgovor sadrži IP adresu računala x.A.B.C
- 8.odgovor sadrži IP adresu računala x.A.B.C

Način razlučivanja u praksi: rekurzivno + iterativno



U stvarnosti se često primjenjuje kombinacija rekurzivnog i iterativnog načina rada, kao na slici: razlučitelj ugraden unutar aplikacije (npr. Web-klijent) traži rekurzivno razlučivanje za traženu adresu (npr. Web-poslužitelja `www.tel.fer.hr`) od lokalnog DNS poslužitelja, koji se dalje ponaša kao iterativni klijent.

Način razlučivanja u praksi: priručna pohrana



Dobivena IP adresa privremeno se pohranjuje u priručni spremnik (engl. *cache*) u lokalnom DNS poslužitelju, tako da se u slučaju skorog ponovnog upita ne mora ponavljati cijeli proces razlučivanja. (Svaki unos u priručnom spremniku ima "rok trajnosti" (*time-to-live*), po isteku kojeg se briše!)

Razlučitelj unutar aplikacije obično isto ima lokalni priručni spremnik.

Primjer – nslookup

```
C:\>nslookup <
Default Server: mygateway1.ar7
Address: 192.168.1.1
> www.fer.hr <
Server: mygateway1.ar7
Address: 192.168.1.1
Non-authoritative answer:
Name: www.fer.hr
Address: 161.53.72.23 <
> www.zxyz.hr <
Server: mygateway1.ar7
Address: 192.168.1.1
DNS request timed out.
timeout was 2 seconds.
*** Request to mygateway1.ar7 timed-out <
>
```

nslookup – alat za postavljanje DNS upita

primjer 1:
upit za ime `www.fer.hr`

tražena IP adresa

primjer 2:
upit za nepostojeće ime
(ili greška u pisanju ☺)

neuspješni ishod

Drugi slični alati su "host" i "dig" (nisu baš naveliko izvedeni u svim OS-ovima).

On-line verzije:

<http://www.kloth.net/services/dig.php>

<http://www.webmaster-toolkit.com/dig.shtml>

Primjer – upit tipa A za računalo www.fer.hr

NsLookup Query the DNS for resource records

domain: <input type="text" value="www.fer.hr"/>	query type: <input type="button" value="A- Address"/>
server: <input type="text" value="70.84.161.11"/>	query class: <input type="button" value="IN- Internet"/>
port: <input type="text" value="53"/>	timeout (ms): <input type="text" value="5000"/>
<input type="checkbox"/> no recursion	<input type="checkbox"/> advanced output
<input type="button" value="Go"/>	
source code: view download	

[70.84.161.11] returned a non-authoritative response in 0 ms:

Answer records

name	class	type	data	time to live
www.fer.hr	IN	A	161.53.72.23	7109s (1h 58m 29s)

tražena IP adresa

Authority records

name	class	type	data	time to live
fer.hr	IN	NS	labs3.cc.fer.hr	50779s (14h 6m 19s)
fer.hr	IN	NS	branka.zesoi.fer.hr	50779s (14h 6m 19s)

Komunikacijske mreže 12.11.2007 40 od 89



Web tool za upite na DNS:
<http://centralops.net/asp/co/NsLookup.vbs.asp>

Primjer – upit tipa MX za domenu fer.hr

NsLookup Query the DNS for resource records

domain: <input type="text" value="fer.hr"/>	query type: <input type="button" value="MX- Mail exchange"/>
server: <input type="text" value="70.84.161.11"/>	query class: <input type="button" value="IN- Internet"/>
port: <input type="text" value="53"/>	timeout (ms): <input type="text" value="5000"/>
<input type="checkbox"/> no recursion	<input type="checkbox"/> advanced output
<input type="button" value="Go"/>	
source code: view download	

[70.84.161.11] returned a non-authoritative response in 156 ms:

Answer records

name	class	type	data	time to live
fer.hr	IN	MX	preference: 10 exchange: labs3.cc.fer.hr	600s (10m)

domensko ime
traženog poslužitelja

Additional records

name	class	type	data	time to live
labs3.cc.fer.hr	IN	A	161.53.72.21	1917s (31m 57s)
branka.zesoi.fer.hr	IN	A	161.53.64.4	9173s (2h 32m 53s)

razlučena IP adresa

Komunikacijske mreže 12.11.2007 41 od 89



Web tool za upite na DNS:
<http://centralops.net/asp/co/NsLookup.vbs.asp>

Primjer – upit tipa A za računalo www.google.hr

NsLookup Query the DNS for resource records

domain: <input type="text" value="www.google.com"/>	query type: <input type="button" value="A- Address"/>
server: <input type="text" value="70.84.161.11"/>	query class: <input type="button" value="IN- Internet"/>
port: <input type="text" value="53"/>	timeout (ms): <input type="text" value="5000"/>
<input type="checkbox"/> no recursion	<input type="checkbox"/> advanced output
<input type="button" value="Go"/>	
source code: view download	

[70.84.161.11] returned a non-authoritative response in 0 ms:

Answer records

name	class	type	data	time to live
www.google.com	IN	CNAME	www.l.google.com	542395s (0d 0h 39m 55s)

kanonsko ime
(jedinstveno)

više IP adresa

name	class	type	data	time to live
www.l.google.com	IN	A	209.85.165.102	176s (2m 56s)
www.l.google.com	IN	A	209.85.165.147	176s (2m 56s)
www.l.google.com	IN	A	209.85.165.99	176s (2m 56s)
www.l.google.com	IN	A	209.85.165.104	176s (2m 56s)

kraci "rok trajanja" zapisa – mogućnost raspoređivanja opterećenja

Komunikacijske mreže 12.11.2007 42 od 89



Web tool za upite na DNS:
<http://centralops.net/asp/co/NsLookup.vbs.asp>

Sadržaj predavanja



- ◆ Osnove internetskih usluga
 - usluge i aplikacijski protokoli
 - modeli izvedbe usluga
 - pronađenje usluga
 - programska podrška
- ◆ Odabrane internetske usluge i protokoli aplikacijskog sloja
 - Sustav domenskih imena
 - **World Wide Web**
 - Električna pošta

Komunikacijske mreže

12.11.2007

43 od 89



World-Wide Web

- ◆ usluga: globalni hipermehijski informacijski sustav
- ◆ aplikacijski protokol: HTTP
- ◆ model izvedbe usluge: klijent-poslužitelj
- ◆ program klijenta:
 - koristi se za pregledavanje sadržaja weba
 - često služi kao univerzalno sučelje prema drugim internetskim uslugama (npr., transfer datoteka, e-pošta, mrežne novosti, ...)
- ◆ program poslužitelja:
 - poslužuje informacijske resurse
 - može posredovati prema drugim poslužiteljima i uslugama (npr., usluge baze podataka,...)

Komunikacijske mreže

12.11.2007

44 od 89

World-Wide Web: pregled sadržaja



- ◆ zahtjevi usluge WWW
- ◆ osnovne komponente izvedbe
 - adresiranje - Uniform Resource Identifier (URI)
 - zapis sadržaja - Hypertext Markup Language (HTML)
 - aplikacijski protokol - Hypertext Transfer Protocol (HTTP)
- ◆ programska podrška

Komunikacijske mreže

12.11.2007

45 od 89



Zahtjevi usluge WWW

- ◆ osnovni zahtjev:
 - transparentni pristup informacijskom sustavu zasnovanom na međusobno povezanim hipermehijskim izvorima
 - sadašnji web temelji se na povezivanju električnih dokumenata i pristupu uslugama weba
 - budući web: "semantički Web", Web 2.0, ...
- ◆ (neki) dodatni zahtjevi
 - pristup drugim uslugama ("univerzalno sučelje")
 - standardne internetske usluge (e-mail, news, ftp, ...)
 - posebne usluge (kućno bankarstvo, digitalne knjižnice, ...)
 - jednostavnost korištenja
 - privatnost i sigurnost

Komunikacijske mreže

12.11.2007

46 od 89

Pojam hiperteksta i hipermehije



- ◆ **hipertekst** – aktivni dijelovi teksta omogućuju "skok" na drugo mjesto u (trenutnom ili nekom drugom) dokumentu
 - sustavi utemeljeni na hipertekstu su postojali i prije Weba
- ◆ **hipermehij** – stranice hiperteksta obogaćene drugim medijima, npr. slikama, audio i video dokumentima i sl.

dokument X



12.11.2007

47 od 89

Pojam informacijskog izvora ili resursa



- ◆ pojam hipermehijskog dokumenta proširuje se pojmom **informacijskog izvora** ili **resursa** (engl. *resource*)
 - u općenitom smislu, "bilo što" što daje informaciju i što se može identificirati
- ◆ obično promatramo konkretnе, automatizirane, mrežno dohvativljive informacijske izvore, npr.:
 - električni dokument,
 - slika,
 - izvor informacija jasne namjene (npr. tečaj HNB),
 - usluga (HTTP-SMS prilaz),
 - kolekcija resursa.
- ◆ primjer **izvora**: električni dokument ("datoteka")
 - **informacija** koju datoteka pruža je njen **sadržaj** (može biti statički ili promjenjiv)
 - prikaz, odnosno **reprezentacija** informacije se često naziva "Web stranicom"

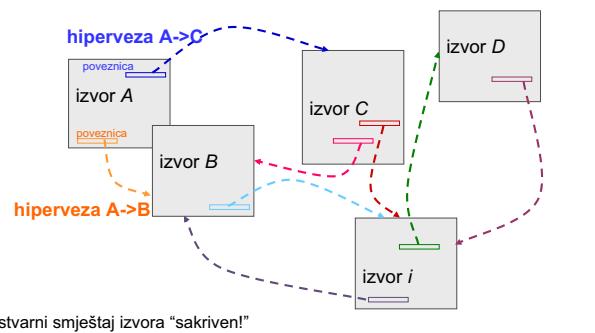
Komunikacijske mreže

12.11.2007

48 od 89

Informacijski prostor Weba

- informacijski prostor weba čine informacijski izvori međusobno povezani hiper-vezama (engl. *hyperlink*)



Komunikacijske mreže

12.11.2007

49 od 89



Pitanja koja treba riješiti

- zapis izvora
 - jednostavan, prenosiv zapis teksta
 - mogućnost umetanja hiperveza
 - korištenje datoteka s drugim medijima (slike, audio, video) u izvornom obliku
- adresiranje - identifikacija izvora
- način povezivanja i komunikacije
 - standardni aplikacijski protokol



**HTML
(XML)**

URI

HTTP

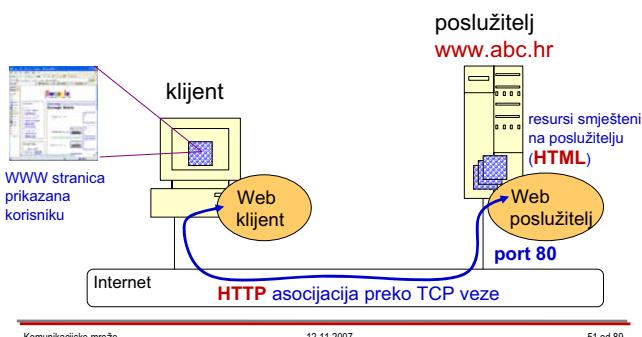
Komunikacijske mreže

12.11.2007

50 od 89

Izvedba usluge WWW u mreži (1/2)

- model klijent-poslužitelj
- resurs identificiran putem **URI**



Komunikacijske mreže

12.11.2007

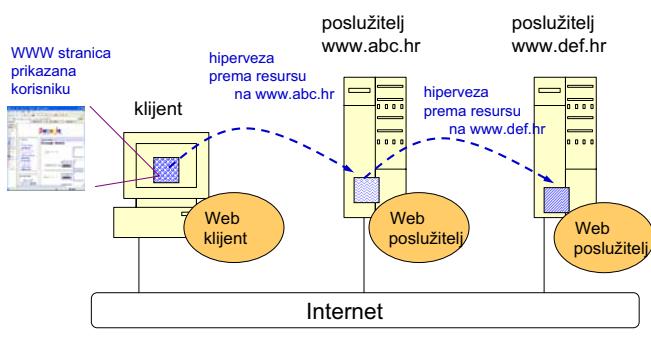
51 od 89



Kao što ćemo vidjeti kasnije, URI obuhvaća način pristupa (protokol HTTP), IP adresu (www.abc.hr) i stazu do resursa u datotečnom sustavu poslužitelja (npr. stazu do HTML datoteke na disku).

Izvedba usluge WWW u mreži (2/2)

- raspodijeljenost sustava je korisniku nevidljiva



Komunikacijske mreže

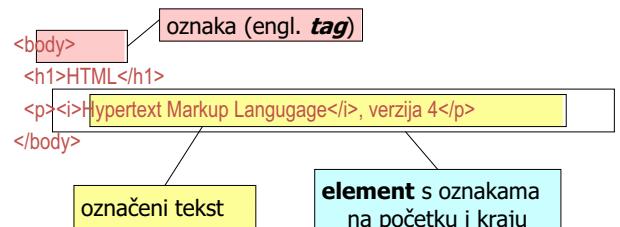
12.11.2007

52 od 89



Hypertext Markup Language - HTML

- prva verzija HTML-a 1992. godine; verzija 4.01 iz 1999. (preporuka W3C-a), osnovica za *Extensible Hypertext Markup Language XHTML*
- jezik za označavanje (*markup*) – običan tekst s umetnutim oznakama koje utječu na predločavanje teksta i služe za uvođenje hiperveza



Komunikacijske mreže

12.11.2007

53 od 89



Ustroj HTML dokumenta



```
<html>
  <head>
    <title>TU: HTML: ustroj dokumenta</title>
    <meta name="author" content="Ivo Ivic">
  </head>
  <body>
    <h1>Ustroj dokumenta u HTML-u</h1>
    <p>HTML dokument sa sastoji od <b>zaglavlja</b> i
       <b>tijela</b>.</p>
  </body>
</html>
```

DOKUMENT
ZAGLAVLJE
TIJELO

Komunikacijske mreže

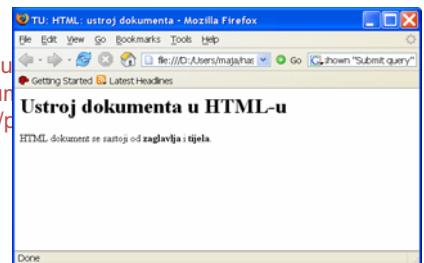
12.11.2007

54 od 89

Izgled u pregledniku



```
<html>
  <head>
    <title>TU: HTML: ustroj dokumenta</title>
    <meta name="author" content="Ivo Ivic">
  </head>
  <body>
    <h1>Ustroj dokumenta u HTML-u</h1>
    <p>HTML dokument sa sastoji od zaglavlja i tijela.</p>
  </body>
</html>
```



Komunikacijske mreže

12.11.2007

55 od 89

Drugi formati



- ◆ često primjenjivani formati dokumenata (neovisno o webu)
 - umetnute slike: GIF, JPEG, PNG
 - dokumenti: PDF, Postscript
 - multimedijiški dodaci: MPEG, QuickTime, WM
 - ...
- ◆ razni formati zasnovani na jeziku **Extensible Markup Language (XML)**
 - **XHTML** - HTML zapisan pomoću XML-a
 - vektorska grafika: SVG (Scalable Vector Graphics)
 - multimedijiške prezentacije: SMIL (Synchronized Multimedia Integration Language)
 - unos elektroničkim perom: Ink Markup Language (InkML)
 -

Komunikacijske mreže

12.11.2007

56 od 89

Uniform Resource Identifier - URI



URI – Uniform Resource Identifier
(uniformni identifikator resursa)

- ◆ **uniformni**: jednoobrazni način zapisa – propisan je oblik
- ◆ **identifikator**: sadrži informaciju nužnu za razlikovanje identificiranog resursa od svih ostalih (# identitet!)
- ◆ **resurs**: informacijski izvor; "bilo što" što se može identificirati URI-jem

Pojam **URI-ja** je središnji pojam u arhitekturi World-Wide Weba.
World Wide Web Consortium (W3C) definira WWW kao "informacijski prostor u kojem su predmeti od interesa identificirani URI-jima".

Komunikacijske mreže

12.11.2007

57 od 89

Architecture of the World Wide Web, Volume One

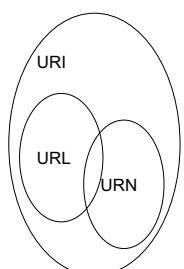
W3C Recommendation 15 December 2004

<http://www.w3.org/TR/webarc/>

Pojmovi: URI, URL i URN



- ◆ **URL – Uniform Resource Locator**
 - resurs se identificira preko svoje (mrežne) **lokacije**
 - npr. <http://161.53.19.1:8080>
- ◆ **URN – Uniform Resource Name**
 - stroži zahtjevi na trajnost: moraju se održavati čak i kad resurs koji identificiraju nestane
 - npr. <urn:ietf:rfc:2396>
- ◆ **URI** može biti ime, lokacija ili oboje



Komunikacijske mreže

12.11.2007

58 od 89

Razlika između URL-a i URN-a, analogija

URL odgovara poštanskoj adresi

- prof. X Y, FER, Unska 3, 10000 Zagreb, Hrvatska
- sadrži informaciju *kamo* dostaviti poruku
- ako se profesor Y preseli, adresa ne valja
- slično: pretplatički broj u fiksnoj telefoniji

URN odgovara JMBG-u

- jedinstven za osobu
- ne sadrži uputu gdje pronaći tu osobu
- nikad se neće koristiti za nešto drugo

Analiza uobičajenog URL-a



<http://www.fer.hr/predmet/kommre/>

shema URI-ja
pokazuje način
pristupa resursu;
npr., protokol HTTP

put - analizira ga poslužitelj
(određen pomoću *host name*)
kako bi dohvatio zadani resurs

host name – može sadržavati ime
(FQDN) ili IP adresu (računala ili
virtualnog) poslužitelja

Komunikacijske mreže

12.11.2007

59 od 89

RFC 3986 definira generičku sintaksu za primjenu u svim URI-shemama.

Primjeri



<http://www.fer.hr/predmet/kommre/>
<http://www.w3.org/TR/webarch/#identification>
<http://www.hr/wwwhr/arts/theatre/index.hr.html>
<http://google.com/search?q=telematika>
<mailto:telemat@tel.fer.hr>
<file:///c:/temp/>
<news:hr.org.fer>
<ftp://jdoe:jdoe@ftp.w3.org/>
[about:blank](#)
<urn:ietf:rfc:2396>

Komunikacijske mreže

12.11.2007

60 od 89

Komentar:

<http://www.fer.hr/predmet/kommre/>
-stranica predmeta (nije navedena puna staza do datoteke)
<http://www.w3.org/TR/webarch/#identification>
-lokalna adresa unutar resursa pomoću #
<http://www.hr/wwwhr/arts/theatre/index.hr.html>
-uri s potpunom stazom do datoteke
<http://google.com/search?q=telematika>
-primjer upita, dinamički generiran sadžaj
<mailto:telemat@tel.fer.hr>
-shema mailto, za e-poštu
<file:///c:/temp/>
- shema file, za pristup lokalnom datotečnom sustavu
<news:hr.org.fer>
-shema news, pristup USENET newsgrupama
<ftp://jdoe:jdoe@ftp.w3.org/>
-shema ftp, transfer datoteka
[about:blank](#)
-shema about, prazna stranica
<urn:ietf:rfc:2396>
\ shema urn

Protokol Hypertext Transfer Protocol (HTTP)



- ◆ aplikacijski protokol
- ◆ definira format i način razmjene poruka
 - tekstualan zapis, sličan formatu e-mail poruke i MIME standarda
- ◆ vrste poruka:
 - **zahtjev** ("metoda")
definira operaciju (metodu), resurs, protokol, npr. za dohvaćanje resursa:
<GET /index.html> [HTTP/1.0](#)
 - **odgovor** (ishod zahtjeva i sadržaj)
ishod zahtjeva (uspjeh, neuspjeh, greška,...) opisan statusnim kôdom, npr.:
[200 \(OK\)](#)
(na zahtjev GET) znači uspješan ishod, u tijelu odgovora dostavlja se sadržaj zatraženog resursa
 - [404 \(Not found\)](#) - neuspješan ishod

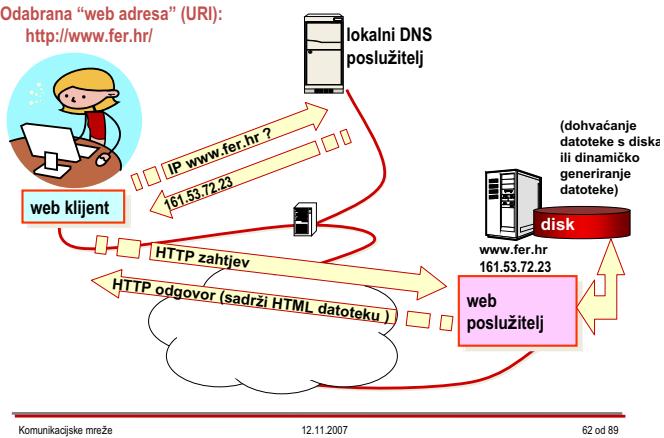
Komunikacijske mreže

12.11.2007

61 od 89

Komunikacija HTTP klijenta i poslužitelja

Odarvana "web adresa" (URI):
http://www.fer.hr/



Komunikacijske mreže

12.11.2007

62 od 89



Komunikacija HTTP klijenta i poslužitelja (opis)

1. proces www poslužitelja (uvijek) osluškuje TCP zahtjeve na dobro-poznatim vratima 80 (ako nije drugačije konfiguiran!)
2. koristeći klijentski program (preglednik), korisnik upisuje adresu traženog izvora (URI)
3. preglednik saznaće IP adresu poslužitelja putem upita na DNS
4. preglednik pokreće TCP vezu sa slobodno odabranih vrata na lokalnom računalu na IP adresu poslužitelja i TCP vrata 80 (port je "dobro-poznat")
5. nakon uspostave TCP veze, preglednik zahtijeva da mu poslužitelj pošalje dokument (HTTP-zahtjev)
6. poslužitelj šalje dokument(e) (HTTP-odgovor)
7. nakon uspješnog transfera, TCP veza se zatvara
8. preglednik prikazuje dokument (HTML) korisniku

Komunikacijske mreže

12.11.2007

63 od 89



Programska podrška

◆ Web klijent

- korisnički Web klijent – **preglednik** (engl. *browser*)
 - grafički ili tekstualno korisničko sučelje za prikaz Web stranice i navigaciju; novije verzije donose više mogućnosti
 - popularni preglednici: Netscape, Mozilla, Firefox, Internet Explorer, Opera, Lynx, ... (uglavnom besplatni)
- automatizirani Web klijent – **robot** ili pauk (engl. *spider, crawler*)
 - program koji samostalno pretražuje Web (ili neki njegov dio) radi prikupljanja podataka, npr. za tražilice

◆ Web poslužitelj

- popularni HTTP poslužitelji: Apache HTTP server (besplatan), Microsoft Internet Information Server
- dodatni aplikacijski poslužitelji

Komunikacijske mreže

12.11.2007

64 od 89



Druge tehnologije vezane uz Web

◆ usklađivanje Web stranica

- Cascading Style Sheets (**CSS**)
- Server Side Includes (**SSI**)

◆ klijentske tehnologije

- **Javascript**
- Java apleti (applets)
- za tehnologije koje nisu "ugrađene" koriste se *plug-in-ovi*

◆ poslužiteljske tehnologije

- Common Gateway Interface, **CGI**
- Java servleti, JavaServer Pages (**JSP**)
- Active Server Pages (**ASP**) - Microsoft
- Perl, PHP

Komunikacijske mreže

12.11.2007

65 od 89



Pristup raznim uslugama putem Weba

◆ "klasične" Internetske usluge

- tematski web portali
- pristup datotekama
- e-mail, webmail, archive mailing lista
- news, forumi, blogovi
- ...

◆ ostale usluge

- rezervacijski sustav (avio-karte, hoteli, ...)
- digitalna knjižnica, on-line publikacije
- osobno bankarstvo
- studentska služba (upis, prijava ispita, ...)
- ...

Komunikacijske mreže

12.11.2007

66 od 89



Sadržaj predavanja

◆ Osnove internetskih usluga

- usluge i aplikacijski protokoli
- modeli izvedbe usluga
- pronalaženje usluga
- programska podrška

◆ Odabrane internetske usluge i protokoli aplikacijskog sloja

- Sustav domenskih imena
- World Wide Web
- **Elektronička pošta**

Komunikacijske mreže

12.11.2007

67 od 89



Elektronička pošta



- ◆ elektronička pošta, e-pošta (engl. *electronic mail, e-mail*)
 - jedna od najstarijih internetskih usluga (od 1973. godine!)
 - omogućuje korisnicima slanje i primanje poruka i podataka putem Interneta korištenjem osobnih elektroničkih poštanskih adresa
- ◆ nekoliko aplikacijskih protokola: SMTP, POP, IMAP
- ◆ model izvedbe usluge: klijent-poslužitelj
- ◆ program klijenta:
 - koristi se za čitanje, pisanje i slanje pošte
- ◆ program poslužitelja:
 - prihvata odlaznu poštu od pošiljatelja, proslijeđuje odlaznu poštu prema odredišnom poslužitelju, prima dolaznu poštu svojih korisnika i dostavlja je u poštanski sandučić primatelja

Komunikacijske mreže

12.11.2007

68 od 89

RFC-ovi vezani za uslugu elektroničke pošte:

<http://www.imc.org/rfc.html>

Elektronička pošta: pregled sadržaja



- ◆ Zahtjevi usluge elektroničke pošte
- ◆ Arhitektura sustava
- ◆ Adresiranje
- ◆ Format poruke
- ◆ Transfer poruke
- ◆ Isporuka poruke krajnjem korisniku

Komunikacijske mreže

12.11.2007

69 od 89

Zahtjevi usluge - osnovne funkcije sustava



- ◆ stvaranje poruke
 - pisanje i uređivanje poruke elektroničke pošte
- ◆ predaja, transfer i isporuka poruke
 - prebacivanje poruke od pošiljatelja do primatelja
- ◆ predočavanje poruka
 - pregled pristiglih poruka (od koga, što, kada, ...)
- ◆ izvještavanje
 - je li poruka uspješno isporučena
- ◆ raspolaganje porukama
 - upravljanje elektroničkim poštanskim sandučićem
 - pohranjivanje, brisanje, proslijeđivanje, filtriranje, ..

Komunikacijske mreže

12.11.2007

70 od 89

Pitanja koja treba riješiti



- ◆ arhitektura sustava
 - klijenti i poslužitelji
- ◆ adresiranje - identifikacija primatelja pošte
 - “pohrani i proslijedi”
 - @
- ◆ format poruke
 - tekst
 - datoteke s drugim medijima (slike, audio, video) u izvornom obliku
- ◆ način povezivanja i komunikacije
 - standardni aplikacijski protokoli
 - SMTP
POP
IMAP

Komunikacijske mreže

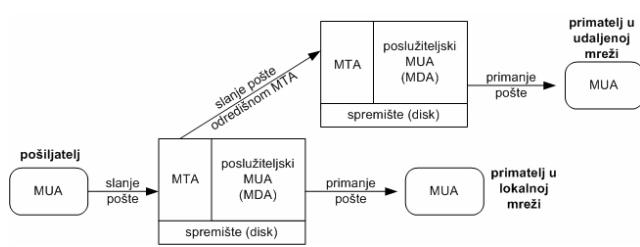
12.11.2007

71 od 89

Arhitektura sustava



- ◆ klijenti:
 - Mail User Agent – MUA
- ◆ poslužitelji čine sustav za dostavu elektroničke pošte:
 - Mail Transport Agent – MTA



Komunikacijske mreže

12.11.2007

72 od 89

Kratice:
MUA - Message User Agent
MTA - Message Transfer Agent
MDA - Message Delivery Agent

U postupku slanja i primanja pošte, program klijenta koristi se za čitanje, pisanje i slanje poruka elektroničke pošte. Program klijenta još se naziva i Message User Agent (MUA).

Poslužitelji su najčešće stalno spojeni na Internet i prihvataju poštu korisnika i prosleđuju je do primatelja. Programi poslužitelja koji usmjeravaju poruke elektroničke pošte nazivaju se Message Transfer Agents (MTA). MTA čeka na dolaznu poštu, koja može doći bilo od lokalnih korisnika, bilo od udaljenih MTA poslužitelja. Nakon što pregleda određenu adresu i ustanovi da je poruka namijenjena udaljenom korisniku, MTA će je proslediti određnom MTA. Ako je poruka namijenjena lokalnom korisniku, poslužiteljski MUA, često nazivan i Message Delivery Agent, će pohraniti poruku u poštanski sandučić lokalnog korisnika (*mailbox, mail spool*) kako bi je korisnik mogao pregledati.

U prijenos jedne poruke može biti uključeno više MTA entiteta. Svi poslužitelji kojima poruke prelaze na putu od izvođača do odredišta, nazivaju se mail relay.

Poстоje brojni klijentski programi za elektronički pošti: na Windows platformama poznati su *Thunderbird, Eudora, MS Outlook, Pegasus Mail* i ostali, dok se na Unix platformama koriste *Mail, mail, elm, mutt, pine* i drugi. Najpoznatiji MTA za Windows operacijski sustav je *Microsoft Exchange*, a na Unix sustavima koriste se *sendmail, qmail* i *postfix*.

Svaki korisnik ima svoju e-mail adresu, formata **korisnicko_ime@domena**, npr. marko@tel.fer.hr.

Znak @ odvaja lokalni dio, ime korisnika, od naziva domene korisnika. Domena izravno ili posredno identificira poslužitelja koji je zadužen za prihvatanje e-mail poruke. Na tom poslužitelju pokrenut je MTA, koji će, nakon što dobije poruku, analizom lokalnog dijela adrese odlučuti kojem korisniku mora dostaviti poruku.

Lokalni dio e-mail adrese može biti korisničko ime lokalnog korisnika, ali može biti i alias, koji može biti lakše pamtljiv od korisničkog imena. Administratori mail poslužitelja održavaju bazu podataka s podacima o aliasima i korisničkim računima, kojom će se MTA poslužiti po primitku poruke.

Primjer aliasa je: *webmaster@fer.hr*. Jedan alias može predstavljati više stvarnih korisnika (npr. marketing@tvrtka.hr).

Primjer: upit za MX (Mail Exchange) zapis za domenu carnet.hr
<http://centralops.net/asp/co/NsLookup.vbs.asp>

U odgovoru vidimo dva zapisa: mx2.carnet.hr i mail.carnet.hr.

Ako ima više poslužitelja, kao u ovom slučaju, parametar *preference* postavlja prioritet.

Adresiranje

- ◆ opći format adrese elektroničke pošte:

korisnicko_ime@domena

- domena – naziv domene ili potpuno kvalificirano domensko ime krajnjeg računala primatelja pošte

- korisnicko_ime – oznaka korisnika ili alias

primjeri:

- webmaster@fer.hr
- ivo.ivic@fer.hr
- marko@pc10.tel.fer.hr

- ◆ MTA mora saznati IP adresu računala koje prima elektroničku poštu za zadano odredište → DNS

Komunikacijske mreže

12.11.2007

73 od 89

DNS i e-mail

- ◆ DNS MX zapis – veza s domenskim dijelom e-mail adrese
- ◆ veza se ne uspostavlja s *domenom*, nego s poslužiteljem koji prima elektroničku poštu za tu domenu

- za istu domenu može postojati više primatelja pošte

primjer: carnet.hr

NsLookup

Query the DNS for resource records

domain	server	port	name	class	type	data	time to live
carnet.hr	70	53	carnet.hr	IN	MX	preference: 30 exchange: mx2.carnet.hr	14400s (4h)
carnet.hr			carnet.hr	IN	MX	preference: 10 exchange: mail.carnet.hr	14400s (4h)

Komunikacijske mreže

12.11.2007

74 od 89

Osnovni format poruke el. pošte

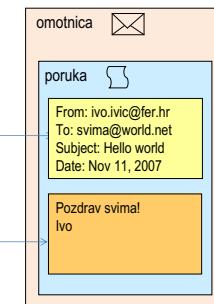
- ◆ osnovna specifikacija - RFC 822; kasnije proširena

omotnica

- služi za prijenos i dostavu
- korisnik je nikad ne vidi, jer ih koriste samo MTA

poruka

- zaglavje poruke - propisana polja
- tijelo poruke - izvorno samo 7-bitni ASCII tekst
- korisnik upisuje neka polja u zaglavljiju i sadržaj u tijelu poruke



Komunikacijske mreže

12.11.2007

75 od 89

Da bi poruka mogla biti ispravno isporučena korisniku, mora biti ispravno formatirana. Osnovna specifikacija zaglavlja poruke definirana je u **RFC 822**, koji opisuje sintaksu polja zaglavlja elektroničke pošte. Korisnici ne moraju voditi brigu oko formatiranja zaglavlja, jer se o tome brine MUA.

Zaglavljve poruke predstavlja niz linija oblika **polje: vrijednost_polja**. Najčešće korištena polja su: **To:**, **Cc:**, **Bcc:**, **From:**, **Reply-To:**, **Received:**, **Subject:**, **Date:** i slična.

Tijelo poruke sadrži sam tekst poruke, kako ga je unio korisnik.



Format poruke - zaglavljve

Neka često korištena polja u zaglavljju su:

- **To:** e-mail adresa primatelja
- **Cc:** e-mail adresa dodatnog primatelja kojem se šalje kopija poruke
- **Bcc:** e-mail adresa skrivenog primatelja
- **Subject:** predmet dopisivanja
- **Date:** datum i vrijeme slanja poruke
- **From:** e-mail adresa pošiljatelja
- **Received:** popis MTA po putu kojim je poruka prošla do odredišnog MTA.

upisuje korisnik

upisuje MUA ili MTA

Komunikacijske mreže

12.11.2007

76 od 89

Primjer

zaglavljve

```

Subject: Besplatan pristup bazi SAGE Publications u mjesecu studenom,
Probní pristup IEL/IEEE Xplore bazi podataka
From: "Subscriptions \ (FER e-Campus CMS v1\)" <donotreply@fer.hr>
Date: Thu, November 8, 2007 12:01 am
To: maja.matijasevic@fer.hr

Stranica: Obavijesti djalatnicima

Obavijesti: Kristijan Zimmer: Besplatan pristup bazi SAGE Publications u
mjesecu studenom
Objavljena obavijest
SAGE Publications ponudio je besplatan pristup svojoj cijelokupnoj bazi
koja uključuje preko 470 časopisa iz svih područja znanosti, tijekom
studenoga 2007.

tijelo poruke

....
```

--

(Ova e-mail poruka Vam je poslana jer su na odgovarajućim stranicama uključene opcije preplate na sadržaj i slanja obavijesti na e-mail. Ukoliko ne želite više primati ove poruke, molimo isključite opcije slanja obavijesti putem e-maila na dotičnim stranicama.)

Komunikacijske mreže 12.11.2007 77 od 89



Multi-purpose Internet Mail Extensions (MIME)

- ◆ cilj: razmjena teksta u jezicima s različitim znakovnim skupovima te razmjena ne-tekstualnih i višemedijskih poruka
- ne više samo 7bit-ASCII!
- slova s dijakriticima i akcentima (hrvatski, francuski, njemački, ...), ne-latinični znakovi (hebrejski, ruski, ...), slikovna pisma (kineski,...)
- višemedijski sadržaji (slike, glazba, video, ...)
- binarne datoteke (doc, zip, ...)
- podržani svi "poznati" standardni formati – MIME media type
- višedjelne poruke (engl. *multipart*)
- ◆ nova polja u zaglavljju
- Za pravilno formatiranje e-mail poruke u pravilu se brine klijentski program, tako da korisnik ne mora poznavati sintaksu zaglavlja.



Komunikacijske mreže

12.11.2007

78 od 89

Multi-purpose Internet Mail Extensions (RFC 2045-2049) omogućuje razmjenu podataka u jezicima s različitim znakovnim skupovima i raznjenu višemedijskih poruka između računala koje koriste Internet standarde za razmjenu pošte.

SMTP protokol ograničen je na prijenos 7-bitnog ASCII teksta s maksimalnom duljinom linije od 1000 znakova. Zbog toga SMTP ne može prenositi binarne datoteke, te se stoga pribegavalo raznim načinima kodiranja podataka. S obzirom da nacionalni znakovi imaju decimalnu vrijednost veću od 127, ni oni se nisu mogli prenositi SMTP protokolom. Standard MIME definiran je kako bi se nadvladali problemi u prijenosu poruka, uz zadržavanje kompatibilnosti s RFC 822 standardom. Dizajniran je tako da podržava minimum zajedničkih svojstava svih protokola koji su se koristili za prijenos poruka na Internetu, a nisu bili sasvim u skladu s RFC 821 specifikacijom.

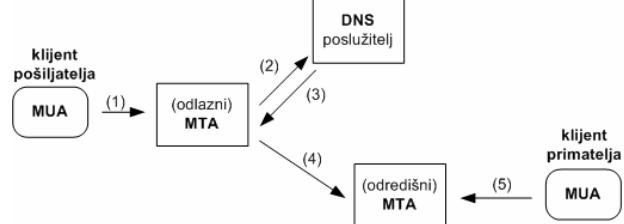
MIME pruža podršku za više objekata u jednoj poruci, za prijenos slika, zvuka, komprimiranih datoteka, postscript datoteka i svih ostalih datoteka koje nisu isključivo 7-bitni ASCII tekstovi. Standard podržava poznate tipove podataka (gif, jpeg, au...) te omogućuje definiranje vlastitih tipova podataka koji su dio poruke.

Popis poznatih formata održava IANA.

<http://www.iana.org/assignments/media-types/>

Standard definira nova polja zaglavlja: MIME-Version: određuje verziju MIME standarda kojoj odgovara poruka (trenutno 1.0). Polje Content-Type: definira vrstu podataka koji se u poruci prenose. Polje Content-Transfer-Encoding: definira način kodiranja podataka. Dodatna polja Content-ID: i Content-Description: mogu se koristiti za dodatni opis vrste poruke.

Mehanizam dostave poruka elektroničke pošte



Komunikacijske mreže

12.11.2007

79 od 89

Koraci prilikom dostave poruke elektroničke pošte ilustrirani su slikom:

(1) Korisnik koji šalje poštu pokreće svoj klijentski program (MUA), koji je podešen tako da poštu šalje preko odaljnog e-mail poslužitelja (MTA) na kojem je pokrenut prikladni poslužiteljski program za obradu zahtjeva. Nakon što korisnik napiše poruku, klijent će u poruku uključiti sva potrebna zaglavlja, na temelju podataka iz poruke (primatelj, predmet poruke) i konfiguracije MUA i poslati je odlaznom poslužitelju (MTA).

(2), (3) Odlazni poslužitelj prihvata poruku i analizira zaglavje kako bi odredio adresu odredišnog poslužitelja, pomoću upita na DNS.

(4) Nakon dobivenog odgovora od DNS poslužitelja, odlazni MTA uspostavlja vezu s odredišnim MTA, putem protokola SMTP, i prosjeduje mu e-mail poruku. Ako se odlazna poruka u tom trenutku ne može prosljediti, odlazni MTA je pohranjuje u svoj rep čekanja (mail spool), odakle će je pokušati prosljediti kasnije. Ovisno o konfiguraciji, odlazni MTA može, ali ne mora izvijestiti korisnika o privremenoj neisporučivosti poruke. Ukoliko se pak poruka uopće ne može isporučiti, npr. zbog pogrešne ili nepostojeciće adrese, ili pak nedostupnosti odredišnog MTA u nekom vremenskom razdoblju (npr. tri dana), korisnik će o tome u pravilu biti obavješten.

(5) Na dolaznoj strani, odredišni poslužitelj (odredišni MTA) će pregledati dospjelu poruku kako bi izdvojio lokalni dio e-mail adrese iz zaglavja poruke, te će prema tome spremiti poruku u poštanski pretinac korisnika – primatelj poruke. Primatelj može procitati dolaznu poštu bilo korištenjem svog klijenta (MUA), nakon autorizacije preko odgovarajućeg protokola (POP3, IMAP), bilo izravno iz poštanskog pretinca, preko interaktivne veze s poslužiteljem (telnet, ssh).

Aplikacijski protokoli korišteni prilikom dostave poruke elektroničke pošte su:

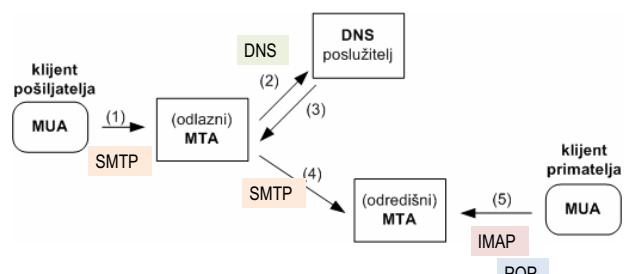
(1) Simple Mail Transfer Protocol (SMTP).

(2), (3) DNS.

(4) SMTP.

(5) Post Office Protocol (POP3) ili Internet Mail Access Protocol (IMAP).

Protokoli pri dostavi poruka elektroničke pošte



Komunikacijske mreže

12.11.2007

80 od 89

Simple Mail Transfer Protocol (SMTP)



- ◆ definiran još 1982. godine, u međuvremenu brojna proširenja
- ◆ standardni internetski aplikacijski protokol
- ◆ služi za slanje poruka elektroničke pošte i dostavu poruke do odredišnog poslužitelja (ne nužno i korisnika!)
- ◆ specificira format i način prijenosa poruka između dva računala
 - ne ovisi o mrežnom protokolu
 - omogućuje proslijedivanje poruka kroz raznovrsne mreže
- ◆ strogo definira sintaksu i redoslijed odvijanja transakcije
 - niz naredbi i odgovora
 - pošiljatelj šalje SMTP naredbu, na koju primatelj odgovara kodom koji može označavati uspjeh ili pogrešku.
 - na svaku naredbu pošiljatelj mora dobiti odgovor primatelja
 - tek se po primitku odgovora može nastaviti sljedeća faza

Komunikacijske mreže

12.11.2007

81 od 89

SMTP naredbe:

obavezne: HELO, MAIL, RCPT, DATA, RSET, VRFY, NOOP, QUIT

neobavezne: SEND, SOML, SAML, EXPN, HELP, TURN

Post Office Protocol v3 - POP3



- ◆ služi krajnjem korisniku za pristup poslužitelju
- ◆ definiran način na koji krajnji korisnik može dinamički pristupiti svom poštanskom sandučiću
- ◆ poruke se dohvaćaju s poslužitelja i spremaju lokalno na korisnikov disk
 - jednostavna manipulacija – "dohvati i obriši"
- ◆ sigurnosni problem – slanje lozinke za prijavu na sustav u otvorenom obliku, mogućnost "krađe" lozinke
- ◆ rješenje: proširenje protokola, Authenticated POP (APOP)
- ◆ noviji i napredniji protokol: IMAP

Komunikacijske mreže

12.11.2007

82 od 89

Protokol Post Office Protocol 3 (POP3) dohvaća poštu s udaljenog poslužitelja. Poslužitelj je najčešće pokrenut na portu 110. POP3 naredbe su obične naredbe pisane ASCII skupom znakova. Sastavljene su od ključnih riječi nakon kojih slijedi niz definiranih parametara a na kraju dolazi sekvenci "<CRLF>.<CRLF>." Naredbe mogu vratiti jednu ili više linija odgovora.

Ako se želi kriptografski zaštiti slanje korisničkog imena i lozinke za pristup POP poslužitelju, treba koristiti proširenje protokola Authenticated POP (APOP).

Internet Message Access Protocol – IMAP4rev1



- ◆ služi krajnjem korisniku za pristup poslužitelju
- ◆ složeniji od POP-a, nudi naprednije načine rukovanja porukama
- ◆ poruke ostaju na poslužitelju, a IMAP omogućuje da se s njima raspolaže jednakom kao da su na lokalnom računalu
 - parcijalno dohvaćanje i pristup MIME dijelovima poruke
 - kreiranje posebnih poštanskih pretinaca (*folder, mailbox*) na udaljenom poslužitelju
 - upravljanje pohranjenim porukama (pretraživanje, brisanje, mijenjanje) i premeštanje poruka iz jednog pretinca u drugi
 - moguće pretraživanje poruka prema definiranim kriterijima izravno na poslužitelju, bez dohvaćanja na lokalni disk
 - šifriranje komunikacije prilikom prijave na sustav
- ◆ pogodan za korisnike s pokretnim uređajima i one koji čitaju poruke s više računala (na poslu, kod kuće, na putu)

Komunikacijske mreže

12.11.2007

83 od 89

Protokol Internet Message Access Protocol v4 (IMAPv4) omogućuje klijentima pristup i manipulaciju nad udaljenim poštanskim pretincima. IMAP poslužitelj koristi dobro poznati port 143. IMAP protokol omogućuje kreiranje posebnih poštanskih pretinaca (*folder, mailbox*) na udaljenom poslužitelju, upravljanje pohranjenim porukama (pretraživanje, brisanje, mijenjanje) i premeštanje poruka iz jednog pretinca u drugi. Moguće je pretraživati poruke prema definiranim kriterijima izravno na udaljenom poslužitelju, a da se poruke ne dohvaćaju na lokalni disk.

Načini pristupa poštanskom sandučiću



- ◆ Stalni (*on-line model*)
 - veza s mail poslužiteljem uspostavljena je cijelo vrijeme dok se koristi MUA
 - način rada tipičan s računalima u LAN-u spojenom na Internet
- ◆ Povremeni (*off-line model*)
 - korisnik uspostavi vezu, prenese novu poštu na svoje računalo i prekine vezu
 - daljnji rad izvodi se lokalno, bez veze s poslužiteljem
 - način rada tipičan za protokol **POP**
- ◆ Odspojeni (engl. *disconnected*)
 - klijent uspostavlja vezu s poslužiteljem, pokupi nekoliko poruka u lokalni cache, pa prekine vezu
 - daljnja obrada odvija se lokalno, ali poruke ostaju na poslužitelju, te se po potrebi lokalni mailbox sinkronizira s centralnim, čim se ponovo uspostavi vezu.
 - način rada tipičan za protokol **IMAP**; odgovara korisnicima u pokretu

Komunikacijske mreže

12.11.2007

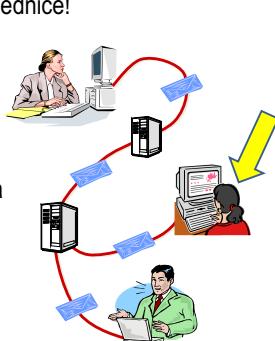
84 od 89

Zaštita privatnosti

- ◆ elektroničke poruke su kao razglednice!
- ◆ nema privatnosti

poželjno (nešto ili sve):

- ◆ šifriranje poruka
- ◆ provjera autentičnosti pošiljatelja
- ◆ garancija integriteta poruke
- ◆ neporecivost primitka
- ◆ Pretty Good Privacy (PGP)
 - primjena kriptografske zaštite metodom javnog ključa



Elektronička pošta nije zaštićena od neželjenog čitanja. Slanje elektroničke pošte je kao i slanje razglednice, svi koji imaju pristup do nje, mogu je pročitati. Na putu od pošiljatelja do primatelja, elektronička pošta prolazi kroz nekoliko mreža, usmjeritelja i mail poslužitelja. Na svakom od računala kroz koje prolazi, može je se presresti i pročitati. Čak ni jednom obrisana, pošta ne nestaje - moguće je da ostane arhivirana na disku radne organizacije, na nekom poslužitelju, na vlastitom disku, itd.

Poruke se mogu zaštiti korištenjem programa za šifriranje podataka. Najpopularniji program za tu namjenu je Pretty Good Privacy (PGP) kojeg je moguće besplatno skinuti s Weba. Takva zaštita funkcioniра na principu javnog i tajnog ključa. Prilikom prvog korištenja programa korisnik kreira svoj javni i privatni ključ, koji se kreiraju po posebnom algoritmu. Javni ključ može objaviti i on će služiti drugima za kriptografsku zaštitu poruke. Najčešće se javni ključevi objavljaju u posebnim imenicima na Webu ili se dodaju u potpis iz elektroničke poruke. Privatni ključ se ne smije djeleti s drugima. Korisnik koji šalje poruku, šifra je pomoći javnog ključa primatelja, a može je i digitalno potpisati svojim privatnim ključem. Primatelj će koristeći javni ključ pošiljatelja provjeriti autentičnost potpisa i pomoći svog privatnog ključa dešifrirati poruku. Uz dovoljno dugačak ključ i ispravno rukovanje ključevima, PGP se može smatrati neprobojnim.

Komunikacijske mreže

12.11.2007

85 od 89

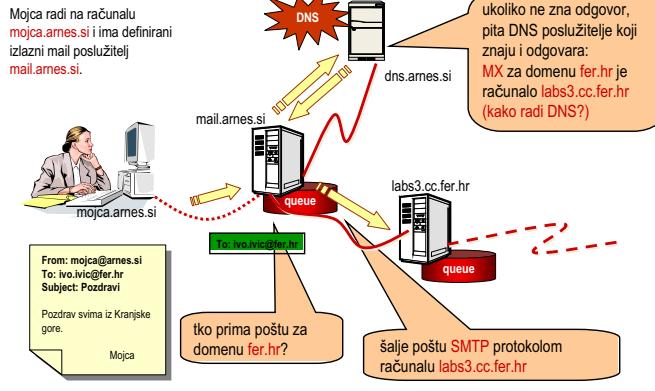
Primjer

Komunikacijske mreže

12.11.2007

86 od 89

Mehanizam slanja elektroničke pošte



Komunikacijske mreže

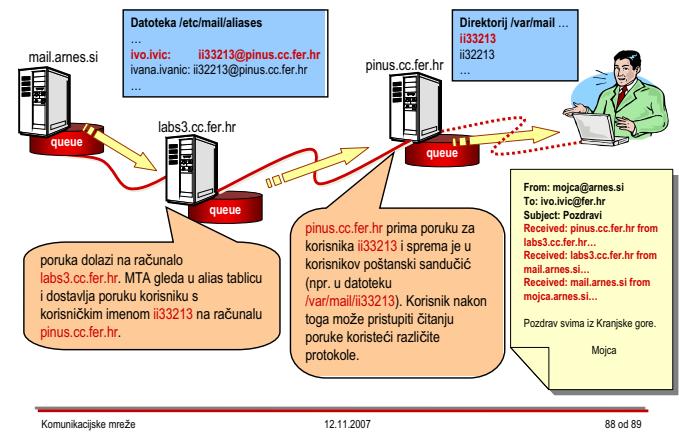
12.11.2007

87 od 89

Prijenos elektroničke pošte najčešće će obuhvaćati nekoliko koraka. Korisnik koji šalje poštu pokreće svoj MUA program, koji je podešen tako da poštu šalje preko e-mail poslužitelja MTA na kojem je pokrenut prikladan program za obradu zahtjeva. Nakon što napiše poruku, pošalje je preko mail poslužitelja (port 25). MUA će automatski u poruku uključiti sva potrebna zaglavja, na temelju podataka iz poruke (primatelj, predmet poruke) i konfiguracije MUA.

MTA prihvata poruku i analizira zaglavje kako bi odredio odredišni poslužitelj, te nakon dobivenog odgovora od DNS poslužitelja, uspostavlja vezu s odredišnim poslužiteljem putem SMTP protokola. Ukoliko se poruka ne može proslijediti, spremi se u lokalni rep čekanja (*mail spool*) i pokuša se proslijediti kasnije. Uobičajeno je da jedan MTA pruža uslugu elektroničke pošte većoj mreži računala. DNS sustav pruža mogućnost identifikacije takvog poslužitelja (MTA) putem mail exchanger (MX) zapisa, tako da se poruke adresirane na adresu domene (npr. ericsson.se) mogu isporučiti odgovarajućem računalu.

Mehanizam isporuke poruke



Komunikacijske mreže

12.11.2007

88 od 89

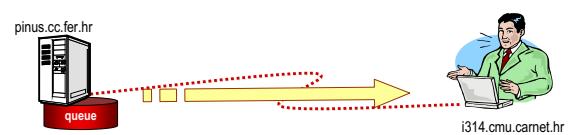
Odredišni poslužitelj pregledat će dospjelu poruku kako bi identificirao lokalni dio e-mail adrese iz zaglavja poruke, te će spremiti poruku u poštanski sandučić korisnika.

Primatelj će pročitati dolaznu poštu korištenjem svog MUA klijenta, nakon autorizacije preko odgovarajućeg protokola (POP3, IMAP) ili izravno iz poštanskog sandučića, ukoliko je uspostavio interaktivnu vezu s poslužiteljem (*telnet*, *ssh*).

Pristup poštanskom sandučiću

Tri uobičajena načina:

- ◆ korisnik može uspostaviti interaktivnu vezu s poslužiteljem (npr. *ssh*) i izravno pristupiti svom sandučiću
- ◆ pristup putem protokola Post Office Protocol (POP3)
- ◆ pristup putem protokola Internet Mail Access Protocol (IMAP)



Komunikacijske mreže

12.11.2007

89 od 89

Komunikacijske mreže

9.
Mrežna sigurnost: sigurnosni postupci

Ak.g. 2007./2008.

30.11.2007

Sadržaj predavanja

- ◆ **Komunikacijska sigurnost**
 - model komunikacijske sigurnosti
 - sigurnosne prijetnje u mrežama računala
 - poželjna svojstva komunikacijske sigurnosti
- ◆ Osnove kriptografije
 - ◆ Simetrične kriptografije
 - ◆ Kriptografija javnih ključeva
 - ◆ Digitalni potpisi
 - ◆ Poslovanje javnim ključevima

Komunikacijske mreže

30.11.2007

2 od 58

Model komunikacijske sigurnosti



Komunikacijske mreže

30.11.2007

3 od 58

Uobičajeni model koji se koristi prilikom definiranja komunikacijske sigurnosti prepostavlja jednosmjernu komunikaciju dva partnera, koju ugrožava neki treći. Kako je potpuno izomorfno radi li se pri tome o komunikaciji računala, vojnih zapovjednika, poslovnih partnera ili pak ljubavnika, obično se koristi neutralna situacija ovoga potonjega. U takvome modelu Alice želi komunicirati na "siguran" način sa svojim partnerom Bobom (Alice i Bob su uobičajena imena koja se u području računalne sigurnosti koriste radije nego suhoparni simboli A i B), ali pri tome postoji opasnost od potencijalnog uljeza Trudy (nadimak za Gertrude, ali i podsjetnik na njezinu "funkciju" uljeza, engl. inTRUDer). Trudy je naravno zakonita Bobova supruga koja ga želi uhvatiti "na djelu"; kako ona poslovno prislушкиje komunikaciju želeći sazнати što o vezi Alice i Boba, koji se put za uljeza koristi i oznaku Eve (dakle Eva, ali i "osoba koja prislушкиje", engl. EaVEsdropper).

U ovome modelu uljez Trudy može djelovati tako da (Ross i Kurose, 2007):

- prislушкиje, dakle "njuška" i bilježi upravljačke i podatkovne poruke na komunikacijskom kanalu te
- modificira, umeće ili briše bilo poruke ili njihov sadržaj (da bi napakostila Alice i Bobu).

Sigurnosne prijetnje u mrežama računala (1)



- ◆ **prislушкиvanje prijenosnog voda** (engl. tapping the wire): pristup nekriptiranim podacima i lozinkama
- ◆ **utjelovljivanje** (engl. impersonation): neovlašteni (engl. unauthorized) pristup podacima ili stvaranje neovlaštenih poruka e-pošte, naloga (engl. orders), itd.
- ◆ **uskraćivanje usluge** (engl. denial-of-service): učiniti mrežne resurse nefunkcionalnima
- ◆ **reprodukcijsko ponavljanje** (engl. replay) poruka: pristup informaciji u tranzitu i njezina promjena

Komunikacijske mreže

30.11.2007

4 od 58

U cilju kvarenja komunikacije partnera (Alice i Boba) uljez Trudy može djelovati na više načina, bilo pasivno ili aktivno. U prvom slučaju se radi samo o prisluskivanju, odnosno pristupu razmjenjivanim podacima uključujući i one "upravljačke", a u drugome su uljezove aktivnosti (još) ozbiljnije prirode i uzrokuju veću štetu partnerima u komunikaciji, jer zadire u razmjenjivane sadržaje (podatke) i njihovu modifikaciju. Tipično se spominje **utjelovljivanje**, odnosno "krada identiteta" jednog od partnera u komunikaciji.

Potrebno je uočiti da, osim neovlaštenog čitanja odnosno i raznih stupnjeva modificiranja razmjenjivanih podataka, uljez može djelovati u smislu kompromitiranja radne sposobnosti (i funkcionalnosti) računala spojenih na mrežu, što je naročito istaknuto za poslužitelje. Pri nabranju sigurnosnih prijetnji se stoga uključuju i takva djelovanja kao što su **uskraćivanje usluge** ili **ubacivanje virusa**.

Sigurnosne prijetnje u mrežama računala (2)



- ◆ pogodanje lozinki:
pristup informaciji i uslugama koje bi normalno bile uskraćene (napad rječnikom (engl. dictionary attack))
- ◆ pogodanje ključeva:
pristup kriptiranim podacima i lozinkama
~ napad grubom silom (engl. brute force attack)
- ◆ virusi:
uništavanje podataka

Poželjna svojstva komunikacijske sigurnosti



- ◆ povjerljivost (engl. confidentiality) ~ tajnost (engl. secrecy): razmjenjivane poruke trebaju biti razumljive samo pošiljatelju i namjeravanoj primatelju
- ◆ integritet poruke (engl. message integrity): osigurati da sadržaj komunikacije nije mijenjan prilikom prijenosa, bilo neprijateljskim djelovanjem ili slučajno
- ◆ ovjera krajnjih točaka (engl. end-point authentication): sposobnost utvrđivanja (autentičnosti) identiteta partnera u komunikaciji
- ◆ radna sigurnost (engl. operational security): (aktivno) suprotstavljanje napadima na mrežu računala neke organizacije
- ◆ neporecivost (engl. nonrepudiation): nemogućnost naknadnog odricanja prethodno odaslane poruke

Alice i Bob komuniciraju putem "nesigurnog" medija, pa je njihova želja osigurati povjerljivost komunikacije (dakle tajnost podataka koje razmjenjuju), tako da Trudy ne može razumjeti poruke koje očekivano presreće na komunikacijskom kanalu. Alice i Bob također žele biti sigurni da sadržaj razmjenjivanih poruka nije mijenjan prilikom prijenosa (tj. da je integritet poruka očuvan), a također i u identitet partnera s kojim komuniciraju. Stoga se poželjna svojstva *sigurne komunikacije* globalno definiraju putem skupa koji obuhvaća *povjerljivost* (ili tajnost), *integritet*, *ovjera* partnera te *radnu sigurnost*.

Neki autori posebno navode i svojstvo *neodicanja*, premda se to može interpretirati i kao utvrđivanje autentičnosti (sadržaja) razmjenjivanih poruka, što bi bila "ovjera poruka".

Osiguranje većine navedenih svojstava temelji se na postupcima *kriptiranja* (i naknadnog *dekriptiranja*) razmjenjivanih poruka i/ili njihovih dijelova.

Sadržaj predavanja



- ◆ Komunikacijska sigurnost
- ◆ Osnove kriptografije
 - model kriptiranja
 - zamjenske šifre
 - transpozicijske šifre
 - ključ za jednokratnu upotrebu
- ◆ Simetrične kriptografije
- ◆ Kriptografija javnih ključeva
- ◆ Digitalni potpisi
- ◆ Poslovanje javnim ključevima

Model kriptiranja

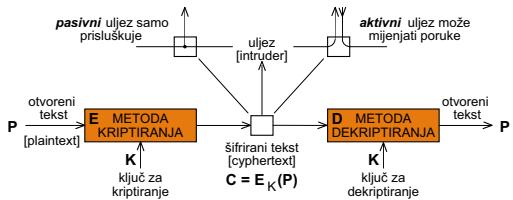


- ◆ kriptologija (engl. cryptology):
 - kriptografija (engl. cryptography): umješnost izmišljanja šifri
 - kriptoanaliza (engl. cryptoanalysis): umješnost razbijanja šifri
- ◆ metode kriptiranja: manipulacije nad izvornim tekstrom
 - šifra (engl. cypher): transformacija jedinice otvorenog teksta fiksne duljine pojedinih znakova ili bitova, bez obzira na lingvističku strukturu poruke
 - kod (engl. code): zamjena pojedine lingvističke jedinice promjenjive duljine (riječ ili simbol); ne koriste se više!

Osnovni mehanizam korišten u mrežnoj sigurnosti je zaštita (tajnosti ili povjerljivosti) razmjenjivanih podataka, pri čemu se koriste razne tehnike *kriptiranja*. *Kriptografija* je skup postupaka pretvorbe izvornih podataka u oblik koji je nečitljiv za uljeza, a *kriptoanaliza* skup postupaka "probijanja" tako zaštićenih sadržaja. *Kriptologija* je znanost o kriptiranju i dekriptiranju.

Radi potpunosti navode se i definicije *šifre* i *koda*. U današnje se vrijeme računalne potpore kriptiranju koriste samo šifre; to znači da se prilikom kriptiranja djeluje na podatke (bitove ili znakove/oktete).

Model kriptiranja



$$D_K(E_K(P)) = P$$

Komunikacijske mreže

30.11.2007

9 od 58

Formalno se postupak zaštite razmjenjivanih podataka kriptiranjem opisuje *modelom kriptiranja* (Tanenbaum, 2003) u kojem se opisuju koraci njihove transformacije. Ovo je model tradicionalne kriptografije, a osnovica je za računalne postupke kriptiranja. Izvorni se podaci koje treba zaštiti nazivaju se *otvorenii tekst*, a oni su zaštićeni naravno *šifrirani* ili *kriptirani tekst*; nazivi su srodnici području primjene (razne tekstovne poruke koje trebaju razmjenjivati vojni zapovjednici, diplomatice ili ljubavnici ☺).

Tradicionalna kriptografija prepostavlja da je metoda kriptiranja poznata te se tajnost postiže parametrom koji se pri tome koristi, a naziva se *ključ* (engl. key). Ključ je naravno tajan, a poželjno je da bude primjereno dugačak da bi osigurao željenu razinu zaštite. U stvari, što je ključ duži, zaštita je snaznija, jer se povećava broj mogućih kombinacija koje kriptoanalitičar mora ispitati radi probijanja zaštite.

Sa stanovišta kriptoanalitičara, problem probijanja zaštite ima tri stupnja težine:

1. problem *kriptiranog teksta* (engl. ciphertext-only), kad je raspoloživ upravo samo kriptirani tekst presretnute poruke;
2. problem *poznatog otvorenog teksta* (engl. known plaintext), kad postoje uskladeni dijelovi kriptiranog i otvorenog teksta;
3. problem *odabranog otvorenog teksta* (engl. chosen plaintext), kad kriptoanalitičar može (očito uspješno probijenim ključem) kriptirati odabrane dijelove otvorenog teksta.

Model kriptiranja



$$D_K(E_K(P)) = P$$

- ♦ **otvorenii tekst** (engl. plaintext): poruka koju treba kriptirati
- ♦ **ključ** (engl. key): parametar funkcije transformacije
- ♦ **šifrirani tekst** (engl. ciphertext), *kriptogram* (engl. cryptogram): rezultat procesa kriptiranja
- ♦ **uljez** (engl. intruder):
 - pasivni: samo sluša
 - aktivni: može ponoviti memorirane poruke, ubaciti svoje, ili modifirati valjane poruke

Komunikacijske mreže

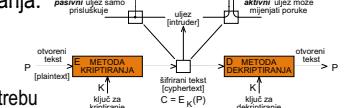
30.11.2007

10 od 58

Model kriptiranja



- ♦ **model kriptiranja** ~ simetrična šifra:
identični ključ za kriptiranje i dekriptiranje
- ♦ koriste se *poznate* metode kriptiranja:
teško izmišljati nove algoritme
- ♦ ključ tajan i lako promjenjiv:
duljina ključa osigurava neprobojnost šifre!
- ♦ tradicionalne metode kriptiranja:
 - zamjenske šifre
 - transpozicijske šifre
 - ključevi za jednokratnu upotrebu



Komunikacijske mreže

30.11.2007

11 od 58

Tradicionalna kriptografija je *simetrični* postupak, jer se za kriptiranje i za dekriptiranje koriste *identični* ključevi. Uobičajene su metode kriptiranja

- **zamjenske šifre** (engl. substitution cyphers),
- **transpozicijske šifre** (engl. transposition cyphers) i
- **ključevi za jednokratnu upotrebu** (engl. one-time pads).



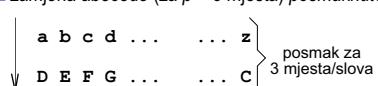
Zamjenske šifre



- ♦ **zamjenske šifre** (engl. substitution cyphers): zamjena znakova drugim znakovima

♦ Cezarova šifra:

- zamjena abecede (za $p = 3$ mjesta) posmknutom abecedom



- ključ = p

- popočenje: posmak za p mesta/slova

- kružno posmknuta abeceda:

lako probijanje

Komunikacijske mreže

30.11.2007

12 od 58

Navodno se već Gaj Julije Cezar koristio jednostavnijim oblikom zamjenske šifre koja se temeljila na zamjeni abecede drugom (*kružno, ciklički posmknutom* abecedom). Ključ je pri tome bio broj znakova za koje je nova abeceda posmknuta (započinje ne slovom "a", već nekim kasnijim; kod Cezarove šifre je to bilo slovo "d", pa je ključ upravo 3).

Naravno, nije teško probiti ovu šifru jednom kada se zna da je ključ broj znakova posmaka.

Jednoabecedna zamjena je složeniji (i nešto bolji) postupak, jer se svaki znak (bijektivno) preslikava u neki drugi. Ključ je nova ("ispremješana") abeceda. Kriptoanaliza se temelji na statističkim svojstvima jezika (pa je zgodno znati na kojem jeziku komuniciraju Alice i Bob, premda primjerice niti to ne bi puno pomoglo Japanki Trudy kad bi Alice i Bob zapravo bili Navajo indijanci ☺).

Višeabecedna zamjena je još složeniji postupak kriptiranja, jer se svako slovo kriptira drugom abecedom (i sve su te abecede zajedno s redoslijedom njihove izmjene ključ!). *Vigenèrova šifra* je pojednostavljena varijanta višeabecedne zamjene.

Zamjenske šifre



- ◆ **složenija zamjenska šifra**
~ *jednoabecedna zamjena* (engl. monoalphabetic substitution):
 - svaki se znak preslikava u neki drugi
 - ključ = niz slova koji odgovara cijeloj abecedi
- ◆ **kriptoanaliza** ~ statistička svojstva jezika:
učestalosti slova/digrama/trigrama/... u jeziku
- ◆ također kriptoanaliza *pogađanjem*:
vjerojatnija pojava riječi karakterističnih za pojedini kontekst

Komunikacijske mreže

30.11.2007

13 od 58

Zamjenske šifre



- ◆ **još složenija zamjenska šifra**
~ *višeabecedna zamjena* (engl. polyalphabetic substitution):
 - svako se slovo kriptira *drugom* abecedom
 - abecede se koriste *ciklički*
- ◆ jednostavna varijanta ~ *Vigenèrova šifra*:
matrica posmknutih abeceda (Cezarovih šifri)
- ◆ snažnija višeabecedna zamjena:
 - jednoabecedne zamjene *različite* od Cezarovih šifri
 - abecede postaju dio ključa pa su teže za pamćenje!

Komunikacijske mreže

30.11.2007

14 od 58

Primjer Vigenèrove šifre



- ◆ *Vigenèrova šifra*:

■ matrica posmknutih abeceda:	A B C D Z	redak A
tablica Cezarovih šifri	B C D E A	redak B
od kojih svaka započinje	C D E F B	redak C
sljedećim slovom

	Z A B C Y	redak Z

- (kratki) ključ određuje Cezarovu šifru iz koje se uzima zamjensko slovo

ključ: KINFA

K	I	N	F	A	K	I	N	F	A	K	I	N	F	A				
j	e	d	n	o	a	b	e	c	d	n	a	z	a	m	j	e	n	a
t	m	q	s	o	k	j	r	h	e	n	v	n	e	w	r	r	s	a

Komunikacijske mreže

30.11.2007

15 od 58

Kako je na primjeru pokazano, ključ Vigenerove šifre određuje iz kojeg retka posmknutih abeceda se uzima zamjenski znak tako što pojedina slova ključa predstavljaju prvo slovo odabrane abecede. Naravno, radi osiguranja jednoznačnosti, ključ (a to je riječ ili neka grupa slova) ne smije sadržavati više pojava istog slova.

Transpozicijske šifre



- ♦ **transpozicijske šifre:**
preuređenje redoslijeda slova otvorenog teksta tako da se izvorna slova ne prikrivaju
 - ♦ npr. **stupčana transpozicija**
 - kluč numerira stupce:
riječ/fraza u kojoj se slova ne ponavljaju
 - kriptoanaliza:
 - treba se znati da se radi o transpozicijskoj šifri
 - statistička svojstva jezika
 - odrediti broj stupaca iz vjerojatnost pojave nekih klučnih riječi
 - odrediti raspored stupaca pronašanje kluča

Komunikacijske mreže

30.11.2007

16 od 58

Umjesto zamjene pojedinih znakova izvornog otvorenog teksta nekim drugim znakovima, *transpozicijske šifre* provode njihovo temeljito "miješanje". Jednostavnija transpozicijska šifra je *stupčana transpozicija* (engl. columnar transposition) kod koje se otvoreni tekst zapisuje po recima (čime se tvori matrica znakova), a čita po stupcima. Redoslijed čitanja stupaca zadan je ključem, a to je rječ (ili fraza) čija slova svojim mjestom u normalnoj abecedi određuju redoslijed čitanja stupaca.

Kako se u ovoj šifri znakovi otvorenen teksta ne zamjenjuju drugim znakovima, lako je zaključiti radi li se o transpozicijskoj šifri, jer su učestalosti pojave pojedinih slova one ubičajene (ipak se i ovdje treba znati u kojem se jeziku odvija komunikacija Alice i Boba ☺). Kriptoanaliza dalje teče pogađanjem broja stupaca na temelju pogadanja pojave riječi karakterističnih za kontekst komunikacije (vjerojatnije je da će dva generala pisati o vojnim jedinicama, manevrima, oružju i sl., a poslovni ljudi o novcu, transakcijama i dionicama, negoli obratno). Konačno se pogada i ključ, odnosno redoslijed stupaca.

Primjer stupčane transpozicije



- ◆ stupčana transpozicija s 8 stupaca
(ključ ima 8 različitih slova)

ključ: VANGELIS
81632547

VANGELIS
81632547

transpozicijskasifratranspozicijeskasifra

criptirani tekst:
rcfpksst i

Komunikacijske mreže

30.11.2007

17 and 58

Transpozicjska šifra u primjeru može se interpretirati kao **blokovska šifra** (engl. block cipher), jer obrađuje **blok fiksne duljine** (ovdje blok od $8 \times 5 = 40$ znakova). Prema tome, može se govoriti da je "izlaz" šifre 2, 10, 18, 26, 34, 5, 13, 21, 29, 37, 4, ... (dakle najprije drugi stupac, pa peti stupac, pa četvrti itd.)

Ključevi za jednokratnu upotrebu



- ◆ *ključevi za jednokratnu upotrebu* (engl. one-time pads): moraju biti dulji od otvorenog teksta i *slučajni!*
 - ◆ neprobojna šifra, jer su svi su uzorci teksta dane duljine podjednako vjerojatni (teorija informacija)!
 - ◆ nedostaci postupka:
 - memoriranje ključa nemoguće
 - ograničenje duljine teksta
 - distribucija ključeva problematična
 - sinkronizacija u prijenosu

Komunikacijske mreže

30.11.2007

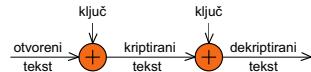
18 od 58

Ključevi za jednokratnu upotrebu se zasnivaju na principu poznatom iz teorije informacija: kombiniraju li se (operacijom EX-ILI) dva niza bitova, od kojih je jedan slučajan (i to je ključ), rezultat je također slučajan niz bitova. Snaga postupka leži u veličini (duljini) ključa, koji se ne smije ponavljati prilikom kriptiranja danog otvorenog teksta. Veličina ključa je i problem (ne može ga se lako pamti, njegova duljina ograničava duljinu otvorenog teksta, itd.). Moguće rješenje je generiranje ključa nekim algoritmom (primjerice sklopovski), ali se onda obično radi o pseudo-slučajnom ključu, i postoji ciklus ponavljanja bitova (jako veliki, ali ipak konačni).

Ključevi za jednokratnu upotrebu



- izvedba kombiniranjem (XOR) bitovne reprezentacije otvorenog teksta i ključa



- generiranje ključa:

- generator slučajnih brojeva:
obično generator pseudoslučajnih brojeva
(engl. Pseudo-Random Number Generator, PRNG)
~ generator sekvencije!
- povjesno ~ Vernamov postupak:
petlje bušene papirne trake čija se duljina razlikuju za jedan znak
- suvremeni pristup: kvantna kriptografija

Komunikacijske mreže

30.11.2007

19 od 58

Generator sekvencije je veliki posmačni register s povratnom vezom sa sklopovima EX-ILI (Peruško, Glavinić: *Digitalni sustavi*, 2005, str. 441-445; ponoviti!>.

Prvobitna izvedba se zasnivala na čitanju znakova iz nekoliko bušenih papirnih traka teleprintera (sprava koja se nekad koristila za prijenos telegrama ☺) koje su bile "zatvorene u sebe". Trake su se razlikovale za jedan znak, primjerice prva traka ima n znakova (pa je ciklus duljine n), druga $n+1$ (ciklus je duljine $n+1$), treća $n+2$ itd. Duljina tako generiranog ciklusa je $nx(n+1)x(n+2)x\dots$ znakova. Po inženjeru koji ju je prvi primijenio već tokom Prvog svjetskog rata, nazvana je Vernamov postupak.

Kvantna kriptografija



- generiranje ključa za jednokratnu upotrebu
- u optičkim komunikacijama:
polariziranje fotona putem dva polarizirajuća filtra (V i H)
- dva skupa polarizirajućih filtera:
 - s pravocrtnom bazom (engl. rectilinear basis)
 - s dijagonalnom bazom (engl. diagonal basis),
pod 45° u odnosu na pravocrtnu bazu
- postupak:
 - Alice → Bob: pridruživanje bitova (0, 1) i polarizacije (V, H)
 - Alice → Bob: ključ
 - Bob → Alice: baze korištene za pojedini bit
 - Alice → Bob: što je Bob ispravno primio; ispravno primljeni bitovi dio su ključa
- poslati > cca $2 \cdot l_{\text{ključa}}$ bitova, u prosjeku $\frac{1}{2}$ će biti ispravno primljeno

Komunikacijske mreže

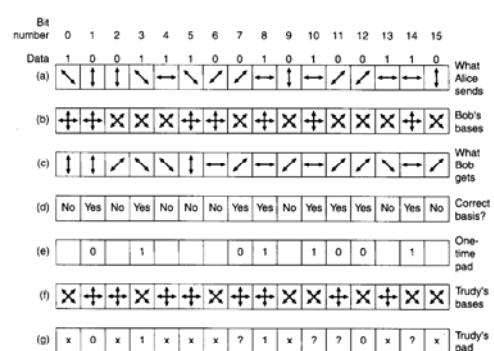
30.11.2007

20 od 58

Jedna mogućnost generiranja (i udaljene dostave) ključa za jednokratnu upotrebu jest kvantna kriptografija (engl. quantum cryptography). Primjenjuje se u optičkim komunikacijama, a zasniva se na polariziranju svjetlosnih impulsa (fotona) putem dva polarizirajuća filtra (za vertikalnu i horizontalnu polarizaciju). Ukoliko su osi filtra međusobno okomite, neće biti prijenosa fotona; inače je intenzitet svjetla proporcionalan kvadratu kosinusa kuta između osi filtra.

Alice (kao i Bob) koristi dva skupa polarizirajućih filtera: s pravocrtnom bazom (engl. rectilinear basis), koji se sastoji od vertikalnog i horizontalnog filtra te s dijagonalnom bazom (engl. diagonal basis), čiji su filtri u odnosu na one iz pravocrne baze rotirani za 45° . Za svaku bazu Alice odabire pridruživanje bitova (0 i 1) i polarizacije (V i H) te ih dojavljuje Bobu.

Primjer kvantne kriptografije (Tanenbaum)



Komunikacijske mreže

30.11.2007

21 od 58

Potom Alice šalje Bobu bitove ključa za jednokratnu upotrebu tako što nasumično koristi jednu ili drugu bazu. Bob naravno ne zna koju bazu koristiti za pojedini bit, pa je nasumično bira (primit će ispravni bit ako pogodi bazu). U slučaju odabira krive baze (filtr je polariziran pod 45° u odnosu na polarizaciju fotonu), svjetlosni impuls (foton) će se slučajno prebaciti u polarizaciju filtra ili u onu okomitu na nju tako da će neku bitovi biti ispravno prenijeti, a neki ne.

U sljedećem koraku Bob javlja Alice *koje je baze koristio* za pojedine bitove, a Alice mu potvrđuje *koje je bitove ispravno primio* (vrijednost bitova je i dalje nepoznata za uljeza!). Sada oboje znaju što je ispravno prenijeto, ali ne i Trudy čiji je izbor baza bio također slučajan, pa stoga drugačiji od Bobovog. Za bitove za koje se njezin odabir baza poklapa s Bobovim, ona zna vrijednost bitova, a za one za koje se taj odabir ne poklapa ona ih ne zna.

Ključ za jednokratnu upotrebu gradi se od ispravno prenijetih bitova; njih će u prosjeku biti upola manje od broja odaslanih, tako da Alice treba poslati bitovni niz nešto veći od dvostrukе duljine željenog ključa.



Sadržaj predavanja

- ◆ Komunikacijska sigurnost
- ◆ Osnove kriptografije
- ◆ **Simetrične kriptografije**
 - sklopovske implementacije kriptografskih algoritama
 - standard DES
 - drugi simetrični algoritmi
- ◆ Kriptografija javnih ključeva
- ◆ Digitalni potpisi
- ◆ Poslovanje javnim ključevima

Komunikacijske mreže

30.11.2007

22 od 58

Simetrična kriptografija



- ◆ tradicionalna kriptografija temelji se na *simetričnim* algoritmima: ključ za kriptiranje i dekriptiranje su identični!
 - ~ *tajni ključ* (engl. secret key)
- ◆ tipična primjena za kriptiranje pojedine sjednice (aplikacijskih procesa)
 - ~ "dijalog" ograničene duljine/trajanja
 - kako pojačati snagu kriptiranja?
 - kako ubrzati proces kriptiranja/dekriptiranja?

Komunikacijske mreže

30.11.2007

23 od 58

Simetrična kriptografija



- ◆ pojačati snagu kriptiranja *kaskadiranjem* većeg broja transformacija
 - ~ *produktna šifra* (engl. product cypher)
- ◆ tipično se koriste *blokovske šifre* (engl. block ciphers): kriptiranje n -bitnih blokova otvorenog teksta
- ◆ računalna izvedba tradicionalne kriptografije
 - ~ algoritam kriptiranja učiniti (vrlo) složenim:
 - sklopovska implementacija
 - ~ brzina
 - programska implementacija
 - ~ fleksibilnost

Komunikacijske mreže

30.11.2007

24 od 58

Pojavom računala mogućnost probijanja teksta kriptiranog tradicionalnim metodama dramatično se poboljšala (naročito probijanje "grubom silom"). Zato se napose u računalnom kontekstu primjenjuju metode pojačavanja zaštite podataka. Jedna je od tih metoda *kaskadiranje* većeg broja transformacija nad podacima, što se naziva *produktna šifra* (engl. product cipher). Tada je naravno "ključ" proširen, jer za svaki stupanj postoji potencijalno različiti ključ. Snaga zaštite leži upravo u toj činjenici.

Sklopovska implementacija (de)kriptiranja



- ◆ jednostavni (i vrlo brzi!) digitalni sklopovi
 - ~ *sklopovski algoritmi* (engl. hardware algorithms) kriptiranja
 - izvedba transpozicije *P-kutijom* (engl. P-box)
 - ~ permutacijska prospojna mreža
 - izvedba zamjena *S-kutijom* (engl. S-box)
 - ~ P-kutija + koder/dekoder
 - izvedba *produktne šifre* kaskadiranjem P-kutija i S-kutija, za različite grupe bitova

Komunikacijske mreže

30.11.2007

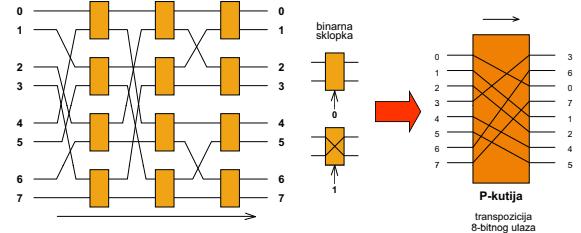
25 od 58

U skorije se vrijeme potreba (a i navika) komuniciranja proširila, pa danas postoji puno parova Alice i Boba čiju diskreciju želi kompromitirati nežaljena Trudy. Štoviše, Alice i Bob žele komunicirati i u stvarnom vremenu (npr. razgovarati telefonom, ali naravno putem zaštićenog kanala). Stoga se i kriptiranje i dekriptiranje mora obaviti u stvarnom vremenu, što neće ići bez primjene jednostavnih i brzih (digitalnih) sklopova. Neko ostvarenje algoritama sklopovskim putem naziva se općim imenom *sklopovski algoritam* (engl. hardware algorithm). Sklopovska se ostvarenja tradicionalnih algoritama kriptiranja i dekriptiranja temelje na primjeni kombinacijskog sklopa *prospojoine mreže*, koji svaki od 2^n ulaza jednoznačno prospaja na odgovarajući izlaz, sukladno primijenjenom upravljačkom uzorku.



Sklopovska implementacija

- ◆ izvedba P-kutije *prospojonom mrežom* (engl. interconnection network) temeljenom na "savršenom miješanju" (engl. perfect shuffle)



Komunikacijske mreže

30.11.2007

26 od 58

Pojavni su oblici *prospojonih mreža* (engl. interconnection networks) raznoliki, i ti su sklopovi u prošlosti vrlo temeljito obrađeni mahom i stoga što predstavljaju osnovicu za ostvarenja komutacijskih polja telefonskih centrala. Radi se o mrežama ostvarenim kaskadiranjem nekoliko stupnjeva *binarnih sklopki* (engl. binary switch), sklopa s dva ulaza i dva izlaza koji prospaja "direktno" ili "u križ", a izведенog dvama multipleksorima 2/1 (usp. Peruško, Glavinić: *Digitalni sustavi*, 2005, str. 323). Obično je ovisnost broja stupnjeva o broju ulaza (i izlaza) logaritamska (tj. broj_stupnjeva = $\log n$, ako je n broj ulaza).

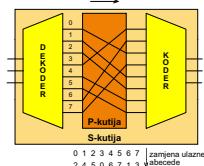
U primjenama kriptiranja koriste se *permutacijske prospojone mreže*, kod kojih se svaki ulaz jednoznačno povezuje s jednim izlazom (ulazi se "permutiraju"). Jedno moguće ostvarenje permutacijske prospojone mreže temelji se na algoritmu "savršenog miješanja" (engl. perfect shuffle), u analogiji s miješanjem igračih karata.

Očito je da permutacijska prospojoна mreža implementira transpoziciju (blokova od 2^n bitova) otvorenog teksta. Takav se sklop naziva *P-kutija* (engl. P-box) i predstavlja temelj za sklopovska ostvarenja složenijih sigurnosnih algoritama.

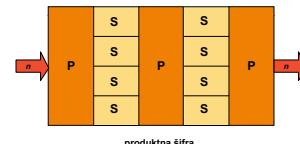


Sklopovska implementacija

- ◆ izvedba S-kutije



- ◆ izvedba produktne šifre



Komunikacijske mreže

30.11.2007

27 od 58

S-kutije (engl. S-boxes), koje se sastoje od P-kutija (za ostvarenje upravljanje permutacije ulaznog bloka bitova) te primjereno ulaznog kodera i izlaznog dekodera, ostvaruju zamjenu znakova ulazne abecede onim izlazne (u gornjem primjeru su radi jednostavnosti znakovi 3-bitni).

Producntna se šifra sklopovski ostvaruje odabranim kaskadiranjem stupnjeva P-kutija i S-kutija; radi povećanja složnosti kriptiranja koriste se različita grupiranja bitova na ulaz sklopa narunutih blokova otvorenog teksta.



Standard DES

- ◆ DES (engl. Data Encryption Standard), US NBS, 1977; izvorno IBM Lucifer
- ◆ produktna šifra temeljena na jednoabecednim zamjenama za 64-bitne blokove

■ 19 stupnjeva:

- 16 identičnih parametriziranih transformacija: tu je sva složenost algoritma
- parametar: 56-bitni ključ mijenja se za svaki stupanj rotacijom polovina
- zamjena lijeve i desne polovine 64-bitnog bloka
- završna transpozicija je inverz početne

■ dekriptiranje obrnutim redoslijedom

Komunikacijske mreže

30.11.2007

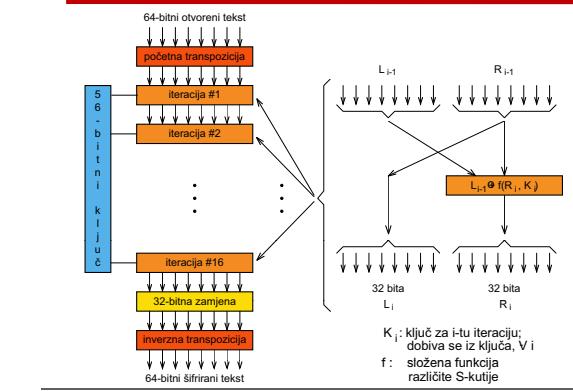
28 od 58

DES (engl. Data Encryption Standard) je jedan od prvih, najpoznatijih, (svojedobno) najšire korištenih i sigurno najkontroverznejih standarda zaštite. Razvijen je modifikacijom IBM-ove produktne šifre Lucifer (1972) koja je izvorno predviđala 128-bitovne ključeve. Izvjesno je vrijeme (do 1988.) DES bio standardna zaštita za "neklasificirane" (engl. unclassified) dokumente američke vlade, tj. dokumente koji nisu (prejerano) povjerljivi. U međuvremenu je široko prihvaćen u poslovnom svijetu, ali dodatno modificiran kako će se vidjeti na jednom od narednih slajdova.

Kontroverza vezana za DES leži u činjenici da je izvorni IBM-ov odabir 128-bitovnog ključa na zahtjev vladine agencije NSA (engl. National Security Agency) "skraćen" na samo 56 bita što rezultira mogućnošću probijanja kriptiranog teksta metodom grube sile. Također razlog izbora specifičnih S-kutija nije objavljen (što znači da su principi projektiranja tajni, a to je u suprotnosti s principima tradicionalne kriptografije). Ovo je rezultiralo stavom kriptoške javnosti da vlada namjerno pokušava ograničiti tajnost šifre, tako da je nitko osim njihovih službi ne može probiti.

DES je produktna šifra 64-bitovnih blokova teksta te se sastoji od 19 stupnjeva transformacija.

Sklopovska izvedba standarda DES



30.11.2007

29 od 58

Slika prikazuje blokovsku strukturu izvedbe DES:

- prvi i zadnji stupanj su transpozicije ulaznog 64-bitovnog blokova, s tim što je izlazni stupanj inverzna transpozicija ulazne;
- predzadnji stupanj zamjenjuje mesta (engl. swap) lijeva 32 bita i s desnim;
- 16 "unutarnjih" stupnjeva su transformacije polovina 64-bitovnog bloka: lijeva je polovina izlaza kopija desne ulazne, dok je desna polovina kombinacija (XOR po bitovima) lijeve i parametrizirane transformacije desne; za svaku od ovih 16 transformacija koristi se različiti ključ koji se izvodi iz 56-bitovnog.

Naravno, dekriptiranje se provodi istim ključem, s tim što su stupnjevi transformacija invertirani.

Problemi sa standardnom DES

- ♦ ključ je prekratak (samo 56 bita), pa ga se može probiti "grubom silom" (engl. brute force)
- ♦ dizajn sklopa DES nije objavljen
- ♦ ipak, snaga kriptiranja DES može se pojačati *kaskadiranjem* ~ "trostruki DES" (engl. Triple DES), IBM, 1979 (kasnije IS 8732)
- podrška već postojećim "jednostepenim" sustavima: EDE + ($K_1 = K_2$)
- podešiva moći kriptozaštite:
 - EDE/DED s 2 ključa (2·56 = 112 bitova)
 - EEE/DDD s 3 ključa (3·56 = 168 bitova)

Komunikacijske mreže

30.11.2007

30 od 58

Trostruki DES (engl. Triple DES) produktna je šifra dobivena kaskadiranjem tri DES čipa, što radikalno povećava snagu zaštite ($2 \times 56 = 112$ bita!). Koristi se dva ključa:

- prilikom kriptiranja je redoslijed transformacija teksta kriptiranje (K_1) – dekriptiranje (K_2) – kriptiranje (K_1);
- redoslijed transformacija kod dekriptiranja je obrnut.

Shema se može koristiti i sa DES sustavima s jednim ključem (uz $K_1 = K_2$), a također i s tri ($3 \times 56 = 168$ bita!) što se još uvijek smatra vrlo jakom zaštitom.

Standard AES

- ♦ novi standard, zamjena za DES:
AES (engl. Advanced Encryption Standard):

- zahtjevi na novi standard:
 - simetrična blokovska šifra
 - javno objelodanjeni dizajn
 - podrška ključevima duljine 128, 192 i 256 bita
 - moguće programske i sklopovske implementacije
 - javni ili nediskriminatorno licencirani algoritam
- Rijndael, NIST FIPS 197, 2001:
 - duljine ključeva i blokova u rasponu 128–256 bita, u koracima od po 32 bita
 - odabir duljina ključeva i blokova *nezavisna*
 - dizajn za sigurnost, ali i veliku brzinu!

Komunikacijske mreže

30.11.2007

31 od 58

AES (engl. Advanced Encryption Standard) je novi standard koji je razvije na "otvoreni" način – javno (da se ne bi smatralo da američka vlada ima svoje prste u nekom prikrivenom slabljenju njegove snage zaštite). Štoviše, objavljen je javni natječaj na kojem je pobijedio algoritam Rijndael (naziv prema dijelovima prezimena autora Daemena i Rijmena).

Drugi simetrični algoritmi



šifra	autor	duljina ključa	komentar
Blowfish	Schneier	1-448 bita	star i spor
DES	IBM	56 bita	preslab za suvremenu upotrebu
IDEA	Massey i Xuejia	128 bita	dobar ali patentiran
RC4	Rivest	1-2048 bita	oprez, neki su ključevi slabi
RC5	Rivest	128-256 bita	dobar ali patentiran
Rijndael	Daemen i Rijmen	128-256 bita	najbolji odabir
Serpent	Anderson, Biham i Knudsen	128-256 bita	vrlo jak
Triple DES	IBM	168 bita	drugi najbolji odabir
Twofish	Schneier	128-256 bita	vrlo jak, široko korišten

Komunikacijske mreže

30.11.2007

32 od 58

Tablični pregled trenutno korištenih simetričnih algoritama kriptiranja.

Sadržaj predavanja



- ◆ Komunikacijska sigurnost
- ◆ Osnove kriptografije
- ◆ Simetrične kriptografija
- ◆ **Kriptografija javnih ključeva**
 - asimetrična kriptografija
 - algoritam RSA
- ◆ Digitalni potpis
- ◆ Poslovanje javnim ključevima

Komunikacijske mreže

30.11.2007

33 od 58

Kriptografija javnih ključeva



- ◆ simetrični ključevi:
standardna upotreba u zaštiti sjednice aplikacijskih procesa
 - efikasni i efektivni
(jedan ključ za kriptiranje i dekriptiranje,
duljina ključa određuje snagu zaštite)
 - postoje brze implementacije (sklopovi)
- ◆ razmjena (dostava) sjedničkih (tajnih) ključeva?
 - sva zaštita leži u tajnosti ključa:
naročito zaštiti razmjenu ključeva
 - sjedničke ključeve treba dostaviti partnerima sigurne komunikacije

Komunikacijske mreže

30.11.2007

34 od 58

Simetrični ključevi se koriste za zaštitu *sjednice* aplikacijskih procesa, a često (ako je sjednica preduga) i samo *dijelova* sjednice (tajni se ključ mijenja u toku sjednice; ovo ovisi o sigurnosnom protokolu). Zbog toga je potrebno osigurati primjereni *sigurni* mehanizam razmjene tajnih ključeva, i to preko nesigurnog (nezaštićenog) komunikacijskog kanala.

Kriptografija javnih ključeva



- ◆ rješenje problema dostave sjedničkih (tajnih) ključeva:
kriptografija javnih ključeva (engl. public key cryptography),
Diffie & Hellman, 1976
 - razvijiti kriptiranje i dekriptiranje ~ *asimetrični* postupak
 - objaviti algoritam kriptiranja i odnosni ključ
 - više ne postoji problem dostave ključeva
- ◆ zadovoljiti sljedeće uvjete:
 - $D(E(P)) = P$
 E : algoritam kriptiranja, s *javnim* ključem za kriptiranje
 D : algoritam dekriptiranja, s *privatnim* ključem za dekriptiranje
 - izrazito je teško izvesti D iz E
 - E se ne može probiti metodom odabranog otvorenog teksta

Komunikacijske mreže

30.11.2007

35 od 58



Kriptografija javnih ključeva

- ◆ postupak kriptiranja i dekriptiranja:
 1. svaki partner razvija (E, D) i objavljuje E zajedno s pripadnim ključem:
 $A \sim E_A, B \sim E_B$
 2. kriptiranje: $A \rightarrow B: E_B(P_A)$
 $B \rightarrow A: E_A(P_B)$
 3. dekriptiranje: $A: D_A(E_A(P_B)) \equiv P_B$
 $B: D_B(E_B(P_A)) \equiv P_A$
- ◆ nalaženje prikladnih algoritama (E, D) koji zadovoljavaju zahtjeve metode?

Komunikacijske mreže

30.11.2007

36 od 58

Neki algoritmi javnih ključeva



- ◆ algoritam ruksaka (Merkle i Hellman, 1978):
privi korišteni, ne smatra se sigurnim
- ◆ faktorizacija velikih brojeva
(RSA - Rivest, Shamir i Adelman, 1978)
- ◆ izračunavanje diskretnih logaritama
(El Gamal, 1985; Schnorr, 1991)
- ◆ algoritmi temeljeni na eliptičkim krivuljama
(Menezes i Vanstone, 1993)
- ◆ najvažnije kategorije:
 - faktorizacija velikih brojeva
 - izračunavanje diskretnih logaritama modulo veliki prim-broj

Komunikacijske mreže

30.11.2007

37 od 58



Algoritam RSA

- ◆ MIT algoritam, algoritam RSA
(Rivest, Shamir, Adleman; MIT, 1978)
- ◆ svojstva:
 - vrlo snažan i siguran algoritam
 - glavni nedostatak:
 - za dobru sigurnost potrebni *dugi* ključevi (≥ 1024 bita):
izračunavanje je dosta spor!
 - primjer za kriptiranje tajnih ključeva za simetrične postupke,
prilikom njihove distribucije
 - zasniva se na teoriji brojeva:
nalaženje prim-brojeva ($> 10^{100}$) prilikom faktorizacije velikih brojeva

Komunikacijske mreže

30.11.2007

38 od 58

Algoritam RSA



- ◆ procjena CPU vremena za faktorizaciju na računalu s $t_{\text{instr}} = 1 \mu\text{s}$:
 - 200-znamenkasti broj: $\sim 4 \cdot 10^9$ godina
 - 500-znamenkasti broj: $\sim 10^{25}$ godina
- ◆ sigurnost zasnovana na vrlo velikom vremenu potrebnom za faktorizaciju:
 - ubrzanje primjerenom raspodjeljom posla na veliki broj (umreženih) računala
 - npr. eksperiment Atkinsa, Grafa i Leylanda, 1992:
1600 računala umreženih u Internet od 09/93 do 04/94 probili kriptozaštitu e-pošte PGP (RSA-129);
ipak se radi o kratkom ključu

Komunikacijske mreže

30.11.2007

39 od 58

Računalo s instrucijskim ciklusom $t_{\text{instr}} = 1 \mu\text{s}$ se tipično koristi radi usporedbe "brzine" algoritama. Naravno, radi se o uniprocesoru (nema paralelne obrade!).

Koraci algoritma RSA



1. odabratи dva velika prim-broja, p i q (tipično $> 10^{100}$)
2. izračunati $n = p \cdot q$ i $z = (p - 1) \cdot (q - 1)$
3. odabratи broj d koji je relativno prim u odnosu na z
4. naći broj e tako da je $e \cdot d = 1 \pmod{z}$
5. podijeliti otvoreni tekst u blokove P
tako da svaki od njih bude u intervalu $0 \leq P < n$
 \rightarrow k -bitni blokovi otvorenog teksta $\sim 2^k < n$
6. kriptiranje bloka P : $C = P^e \pmod{n}$
7. dekriptiranje C : $P = C^d \pmod{n}$
 \Rightarrow javni ključ = (e, n)
privatni ključ = (d, n)

Komunikacijske mreže

30.11.2007

40 od 58

Primjer kriptiranja algoritmom RSA



$$p = 3, q = 11 \Rightarrow n = 33, z = 20; \text{npr. } d = 7;$$

$$\frac{7 \cdot e}{20} = x + \frac{1}{20} \Rightarrow e = 3$$

$$C = P^3 \pmod{33}, P = C^7 \pmod{33}$$

	P	P^e	C $P^e \pmod{n}$	C^d	P $C^d \pmod{n}$	
K	11	1.331	11	19.487.171	11	K
I	9	729	3	2.187	9	I
N	14	2.744	5	78.125	14	N
F	6	216	18	612.220.032	6	F
A	1	1	1	1	1	A

Komunikacijske mreže

30.11.2007

41 od 58

Primjer je izrađen bez pomoći *modulo aritmetike*. Njenim korištenjem gornja su izračunavanja značajno jednostavnija.

Sadržaj predavanja



- ♦ Komunikacijska sigurnost
- ♦ Osnove kriptografije
- ♦ Simetrične kriptografije
- ♦ Kriptografija javnih ključeva
- ♦ **Digitalni potpisi**
 - potpsi sa simetričnim ključevima
 - potpsi s javnim ključevima
 - sažeci poruka
- ♦ Poslovanje javnim ključevima

Komunikacijske mreže

30.11.2007

42 od 58

Digitalni potpisi



- ♦ zamjena za vlastoručne potpise u porukama:

- sustav koji će podržati sljedeće zahtjeve:
 - primatelj može provjeriti identitet pošiljatelja
~ ovjera (engl. authentication) pošiljatelja
 - pošiljatelj ne može kasnije poreći sadržaj poruke
~ neporecivost (engl. nonrepudiation) poruke
 - primatelj nije mogao izmisliti poruku
- mogućnosti ostvarivanja digitalnih potpisa:
 - potpsi sa simetričnim ključem
 - potpsi s javnim ključem
 - sažeci poruka

Komunikacijske mreže

30.11.2007

43 od 58

Postoji nekoliko mogućnosti ostvarivanja digitalnih potpisa. Korištenje *sažetaka poruka* (engl. message digests) podržava izbjegavanje *preopterećivanja semantike*, jer odvaja utvrđivanje identiteta od osiguranja tajnosti podataka. Osim toga je obrada vezana za "digitalno potpisivanje" primjereno brža.

Potpisi sa simetričnim ključem



♦ postoji središnji autoritet kojem svi vjeruju:

- pošiljatelj šalje središnjem autoritetu kriptiranu poruku i još neke podatke
- središnji autoritet ustanovljuje identitet pošiljatelja:
 - dodaje informaciju o pošiljatelju kriptiranu svojim tajnim ključem
 - ~ potpisana poruka
 - proslijeđuje primatelju proširenu poruku kriptiranu primateljevim ključem

♦ primatelj:

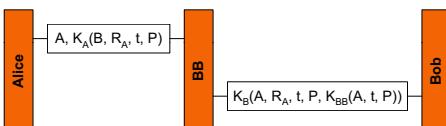
- može pročitati poruku
- siguran je u identitet pošiljatelja
- posjeduje potpis, koji on nije mogao izmisliti

Potpisi sa simetričnim ključem jednostavno su rješenje, ali tipično Alice i Bob ne bi htjeli imati još "nekog trećeg" kojemu trebaju sustavski vjerovati (a osim toga im "čita poštu").

Potpisi sa simetričnim ključem



- A, B: imena partnera; BB: bilježnik
K_A, K_B, K_{BB}: ključevi
R_A: slučajni broj; t: vremenska markica
K_{BB}(A, t, P): potpisana poruka



Preda ne toliko često, *bilježnik* (engl. notar) se koji puta naziva Nick (Nicholas ☺). Vidi se da bilježnik zaštićenim podacima koje proslijeđuje Bobu dodaje svoj *potpis* (kriptiran *njegovim* tajnim ključem K_{BB}) koji obuhvaća Aliceino ime, *vremensku markicu* (engl. time stamp), neki *slučajni broj* te samu poruku. Očito je postupak neefikasan, jer se poruka posve nepotrebno kriptira *dva puta*.

U ovom kontekstu je bilježnik prozvan "Velikim Bratom" ("Big Brother is watching you", poznata izreka iz romana 1984 Georgea Orwella).

Potpisi sa simetričnim ključem

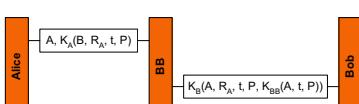


♦ osiguranje neporecivosti:

- BB prihvatio poruku, jer je kriptirana tajnim ključem K_A
- BB kriptirao podatke od A: K_{BB}(A, t, P)
Bob ih nije mogao izmisliti

♦ spriječavanje napada ponavljanjem (engl. replay attack):

- t ukazuje na "stare" poruke
- R_A ukazuje na već "iskorištene" poruke



Bilježnik BB (Veliki Brat) poznae Alicein tajni ključ, i taj je tajni ključ simetrični ključ njihove sjednice.

Smisao umetanja *vremenske markice* t i *slučajnog broja* R_A jest u ograničavanju mogućnosti organiziranja *napada ponavljanjem* (engl. replay attack). Trudy bi naime mogla snimati komunikaciju Alice i/ili Boba i naknadno se javiti jednomu od partnera ponavljanjem već odaslane poruke; vremenska markica ukazuje na vrijeme slanja poruke ("ostarjele" poruke su sumnjive!), a usporedbom upravo primljenog slučajnog broja s popisom prethodno primljenih Bob može ustanoviti da se radi o "potrošenoj poruci".

Potpisi s javnim ključem



- ◆ izbjegići potrebu korištenja središnjeg autoriteta kojem svi vjeruju (a koji im čita poruke!)
- ◆ od algoritma javnog ključa dodatno zahtijevati $E(D(P)) = P$
 - kriptiranje kod A: $E_B(D_A(P)) = C$
 - dekriptiranje kod B: $E_A(D_B(C)) = E_A(D_B(E_B(D_A(P)))) = P$
- ◆ neporicanje je zadovoljeno:
samo je A mogao kriptirati privatnim parametriziranim algoritmom D_A !
- ◆ problemi:
 - ako D_A nije više tajan? npr. ukraden je?
 - kako riješiti periodičko obnavljanje D_A (koji je E_A valjan?)

Komunikacijske mreže

30.11.2007

47 od 58

Zašto vjerovati Velikom Bratu BB, kad se sve može obaviti u vlastitoj režiji? Uvođenjem dodatnog zahtjeva (da kriptiranje javnim ključem nekog otvorenog teksta prethodno dekriptiranog privatnim daje izvorni otvoreni tekst) moguće je provesti *potpisivanje s javnim ključem*.

Neporicanje je u ovom postupku osigurano činjenicom da Bob ima u svojim rukama kako otvoreni tekst P, tako i taj isti tekst (de)kriptiran Aliceinim privatnim ključem (koji on nikako ne može posjedovati). Kako se D ne može izvesti iz E, očito je Bob u pravu. Problemi s ovom shemom digitalnog potpisivanja mogu nastati ako Alice ustvrdi da joj je D ukraden (znači nije više njen privatni ključ, pa je moguće zločesta Trudy mogla poslati poruku potpisu s D_A) ili je u međuvremenu provela periodičko obnavljanje D_A (pa naravno $D_A'(P) \neq D_A(P)$).

Sažeci poruka



- ◆ izbjegići kombiniranje dviju različitih funkcija (ovjere i tajnosti):
sažeci poruka (engl. message digests)
- ◆ jednosmjerna hash funkcija MD:
iz proizvoljno dugog dijela teksta generira bitovni niz fiksne duljine
- ◆ svojstva MD:
 - lako izračunati $MD(P)$
 - gotovo nemoguće izračunati P iz $MD(P)$
 - za dati P nemoguće izračunati $P' \sim MD(P') = MD(P)$:
osigurati da je $hash > 128$ bita
 - promjena od samo 1 bita daje vrlo različit rezultat:
hash mora "temeljito izmiješati" bitove

Komunikacijske mreže

30.11.2007

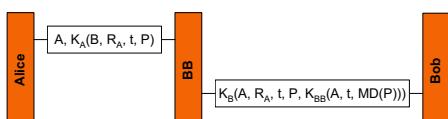
48 od 58

Sažeci poruka (engl. message digests) omogućuju potpisivanje poruke jedinstvenim kratkim uzorkom bitova fiksne duljine. Osim što se izbjegavanja dvostruko kriptiranje poruke otvorenog teksta, smanjena je i količina bitova koju treba prenosi mrežom. Sažeci poruka generiraju se primjenom jednosmjernih *funkcija miješanja* (engl. hash functions).

Sažeci poruka



- ◆ primjena sažetka poruke kod potpisa sa *simetričnim* ključem:
 - zamjena P s $MD(P)$:
 - brži su kako obrada (kriptiranje) tako i prijenos!
 - dekriptiranjem potpisane poruke $K_{BB}(A, t, MD(P))$:
uspoređuju se P i $MD(P)$



Komunikacijske mreže

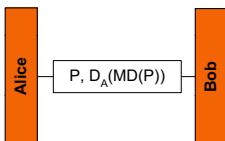
30.11.2007

49 od 58

Uočiti da kod potpisa sa *simetričnim* ključem i dalje Veliki Brat potpisuje poruku (premda puno kraćim sažetkom poruke) $K_{BB}(A, t, MD(P))$.

Sažeci poruka

- ◆ primjena sažetka poruke kod potpisa s *javnim* ključem:
 - kriptira se *samo* MD(P):
puno brža obrada (kriptiranje) i prijenos!
 - sigurno otkrivanje eventualne zamjene P s P' djelovanjem aktivnog uljeza provjeravanjem (kod B) uskladenosti P' i MD(P)



I kod potpisa s *javnim* ključem puno kraći sažetak poruke MD(P) zamjenjuje samu poruku MD(P).

Često korišteni sažeci poruka

- ◆ MD5, Rivest, 1992:
128-bitni sažetak dobiven miješanjem blokova od 512 bitova
- ◆ SHA-1 (engl. Secure Hash Algorithm), NIST, 1993:
160-bitni sažetak dobiven miješanjem blokova od 512 bitova



Sadržaj predavanja

- ◆ Komunikacijska sigurnost
- ◆ Osnove kriptografije
- ◆ Simetrične kriptografije
- ◆ Kriptografija javnih ključeva
- ◆ Digitalni potpisi
- ◆ **Poslovanje javnim ključevima**
 - certificiranje javnih ključeva
 - infrastruktura javnih ključeva

Poslovanje javnim ključevima

- ◆ sigurna komunikacija:
 - tajnost (povjerljivost) komunikacije kriptiranjem razmjenjivanih poruka
 - integritet razmjenjivanih poruka (digitalnim) potpisivanjem razmjenjivanih poruka
- ◆ tajnost sjednice osigurana sjedničkim (tajnim) ključevima;
razmjena sjedničkih (tajnih) ključeva kriptiranjem javnim ključevima
- ◆ problem *raspodjele* javnih ključeva, naročito za partnera koji se ne poznaju; postoji mogućnost ubacivanja uljeza u komunikaciju
~ *poslovanje javnim ključevima* (engl. public key management)

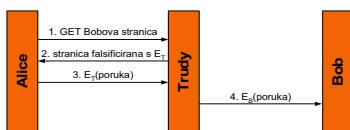


Sigurna je dostava/distribucija *simetričnih* (tajnih) ključeva osigurana njihovim kriptiranjem *asimetričnim* postupcima (javni-privatni ključ). Međutim, Alice treba biti sigurna u identitetu Boba prije no što kriptira svoju poruku njegovim javnim ključem. Trudy se, naime, može ubaciti u njihovu komunikaciju i *utjeloviti* (engl. impersonate) Boba, pa je sav trud oko uvođenja javnih ključeva uzaludan.

Prema tome, potrebno je razviti sustav sigurne distribucije javnih ključeva.

Poslovanje javnim ključevima

- ◆ mogućnost ubacivanja uljeza u komunikaciju partnera koji se ne poznaju



- ◆ centar za raspodjelu ključeva?

- podesivost (engl. scalability)
- raspoloživost

- ◆ certificiranje javnih ključeva

Prva, intuitivna i pomalo naivna, mogućnost organiziranja raspodjele javnih ključeva je formiranje centra za raspodjelu ključeva. To nažalost nije *podesivo* (engl. scalable) rješenje, za iole veće opterećenje postaje usko grlo, a također predstavlja i problem pouzdanosti (jedinstveni središnji element sustava) odnosno raspoloživosti (koliko je centar stvarno u radnom stanju).

Stoga se rješenje radije traži u sustavu *certificiranja* (potvrđivanja) javnih ključeva tako što se pojedini javni ključ vezuje za ime nekog entiteta. Certifikati su "izjave" o tom vezivanju, koje su digitalno potpisane.

Certificiranje javnih ključeva

- ◆ posebna organizacija ~ CA (engl. Certification Authority)

- *certificiranje*:

- povezivanje nekog javnog ključa s *imenom* (pojedinca, kompanije, itd.)

- *certifikat*:

- "izjava" o tome, potpisana privatnim ključem CA:
hash izjave kriptiran s D_{CA}
 - nije sam po sebi tajjan

- ◆ standard za certifikate: ITU-T X.509, 1988

- OSI imenovanje i adresiranje;
npr. /C=HR/O=FER/OU=ZEMRIS/CN=Vlado
 - kodiranje korištenjem OSI ASN.1
 - mogućnost korištenja imena prema DNS

Norma za formate certifikata je ITU-T X.509, a kodiranje pojedinih polja certifikata provodi se poznatim *zapisom apstraktnе sintakse ASN.1* (engl. Abstract Syntax Notation 1). U novije je vrijeme dozvoljeno korištenje DNS zapisa.

Certifikati prema X.509

- ◆ osnovna polja certifikata prema X.509:

polje	značenje
verzija	verzija X.509
serijski broj	serijski broj i ima CA jedinstveno identificiraju certifikat
algoritam potpisa	algoritam koji se koristi za potpisivanje certifikata
izdavatelj	ime CA prema X.509
razdoblje važenja	vremena početka i završetka važenja
ime subjekta	entitet čiji se ključ certificira
javni ključ	javni ključ subjekta i ID algoritma koji on koristi
ID izdavatelja	opcionali ID koji jedinstveno identificira izdavatelja certifikata
ID subjekta	opcionali ID koji jedinstveno identificira subjekt certifikata
proširenja	ima ih mnogo
potpis	potpis certifikata (potpisani privatnim ključem CA)

Poslovanje certifikatima

- ◆ pojedini CA ?

- performanse (opterećenje, raspoloživost)
 - odabir organizacije za vođenje CA

- ◆ poseban mehanizam:

- infrastruktura javnih ključeva PKI*
(engl. Public Key Infrastructure)

Predviđeni obim posla CA (koji naravno s porastom Interneta može samo rasti) navodi na formiranje hijerarhijske organizacije – *infrastrukture javnih ključeva* (engl. Public Key Infrastructure, PKI) – koja će obavljati zadaću certificiranja.

U ovome se (hijerarhijskom) kontekstu onda govori uspostavljanju "staze certificiranja", što implicira *lanac* certifikata koji siže do korijena strukture. Štoviše, utvrđuje se postojanje više takvih hijerarhija, čiji su (lokalni) korjeni obično upisani u suvremene *preglednike* (engl. browsers).

Infrastruktura javnih ključeva



- ◆ hijerarhija CA (najjednostavniji oblik):
viša razina certificira više CA niže razine
- ◆ *lanac povjerenja* (engl. chain of trust),
staza certificiranja (engl. certification path)
~ lanac certifikakata koji siže do korijena strukture
- ◆ postoji više (~ 100) korijena
~ više hijerarhija
- ◆ korjeni su prethodno upisani u Web preglednike
~ "sidra povjerenja" (engl. trust anchors)

Komunikacijske mreže

10.
Mrežna sigurnost: sigurnost u Internetu

Ak.g. 2007./2008.

8.12.2007

Popis mogućih napada na mrežnu sigurnost. Napadi se grubo mogu podijeliti na (i) napade na povjерljivost (tajnost) i integritet poruka, (ii) krađu identiteta partnera te (iii) kvarenje performansi mrežnih resursa.

Popis mogućih sigurnosnih problema u Internetu i pripadnih rješenja
(cf. A. Rodriguez et al.: *TCP/IP Tutorial and Technical Overview*, Seventh Edition, International Business Machines Corporation, August 2001, www.redbook.ibm.com/sg/redbooks/0243376.pdf)

Problem: Kako sprječiti prisluškače u čitanju poruka?

Rješenje: Kriptirati poruke, tipično korištenjem nekog djelejnog tajnog ključa. Tajni ključevi pružaju značajne prednosti u performansama nad kombinacijom javni-pravni ključevi.

Problem: Kako distribuirati ključeve na siguran način?

Rješenje: Koristiti različite tehnike kriptiranja, tipično javne-pravne ključeve.

Problem: Kako sprječiti da ključevi postanu zastariji, i kako zaštiti od pogodanja budućih ključeva probijanjem postojećih ključeva?

Rješenje: Često osvježavati ključeve i ne izvoditi nove ključeve iz starih (savršena tajnost unaprijed, engl. Perfect Forward Secrecy, PFS).

Problem: Kako sprječiti varalice u retransmisijski poruci (napad ponavljanjem)?

Rješenje: Koristiti redne brojke. Vremenske markice (engl. time stamps) su obično nepouzdane u sigurnosnim primjenama.

Problem: Kako se osigurati da poruka nije bila izmjenjena u tranzitu?

Rješenje: Koristiti sažetak ponuka, i to bilo hash ili jednosmjerno (engl. one-way) funkcije.

Problem: Kako osigurati da niti sažetak nije kompromitiran?

Rješenje: Koristiti digitalne potpisne kriptiranjem sažetaka poruke tajnim ili privatnim ključem (ovjera izvora, neodrancanje).

Problem: Kako osigurati da su poruka i potpis nastali kod željenog partnera?

Rješenje: Koristiti dvosmjerna rukovanja (two-way handshakes) koja uključuju kriptirane slučajne brojke (uzajamna ovjera).

Problem: Kako osigurati da su rukovanja razmijenjena s pravim partnerima (napad posrednikom, engl. man-in-the-middle attack)?

Rješenje: Koristiti digitalne certifikate (vezivanja javnih ključeva s trajnim identitetima, engl. permanent identities).

Problem: Kako sprječiti neprimjereno korištenje usluga inače primjerenog korisniku?

Rješenje: Koristiti model višešlojnog upravljanja pristupom.

Problem: Kako se zaštiti od virusa?

Rješenje: Ograničiti pristup vanjskim izvorima; izvršavati antivirusni SW na svakom poslužitelju i radnoj stanicu koja ima kontakte s vanjskim podacima, te često ažurirati taj SW.

Problem: Kako se zaštiti od neželjenih ili zlonamjernih poruka (napad uskraćivanjem usluge)?

Rješenje: Ograničiti pristup internoj mreži korištenjem filtra, "zastupnika" (engl. proxies), ovjere paketa, prikrivanja internih adresa i strukture imena, itd.

Sigurnosni problemi u Internetu



mogući napadi na mrežnu sigurnost (ponavljanje):

- ◆ prisluškivanje prijenosnog voda
- ◆ utjelovljivanje
- ◆ uskraćivanje usluge
- ◆ reprodukcija poruka
- ◆ pogodanje lozinki
- ◆ pogodanje ključeva
- ◆ virusi

Komunikacijske mreže

8.12.2007

2 od 59

Rješenja za sigurnosne probleme u Internetu



◆ zaštita tajnosti i integriteta poruka, utvrđivanje identiteta partnera:

- kriptiranje
- često osvježavanje ključeva, jaki ključevi, sprečavanje izvođenja (engl. deriving) budućih ključeva
- digitalni potpisi i certifikati

◆ zaštita mrežnih resursa:

- ovjera (engl. authentication) i ovlašćivanje (engl. authorization): zaštita od nedozvoljenog korištenja mrežnih resursa
- uzajamna ovjera partnera lozinkama za jednokratnu upotrebu (engl. one-time passwords) i dvosmjernim rukovanjem korištenjem slučajnih brojeva (engl. two-way random number handshakes)
- prikrivanje (engl. concealment) adrese: zaštita od napada uskraćivanjem usluga

Komunikacijske mreže

8.12.2007

3 od 59

Sadržaj predavanja



◆ Sigurnosna arhitektura Interneta

◆ Virtualne privatne mreže

◆ Sigurnosna stijena

◆ Sigurnosna arhitektura za IP – IPsec

◆ Sloj sigurnih priključaka SSL

◆ SET

◆ Protokoli ovjere

Komunikacijske mreže

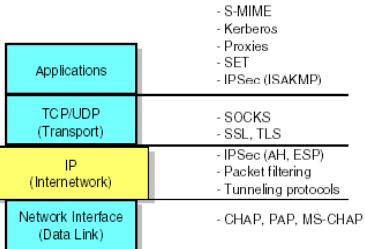
8.12.2007

4 od 59

Sigurnosna arhitektura Interneta



niz protokola i sustava koji se koriste radi pružanja različitih stupnjeva sigurnosnih usluga unutar Interneta:
uslojena arhitektura



Sigurnosna arhitektura Interneta



po slojevima različiti stupnjevi osiguranja sigurnosnih usluga u Internetu:

- IP filtriranje
- prevođenje mrežne adrese NAT
- sigurnosna arhitektura za IP
- SOCKS
- sloj sigurnih priključaka SSL
- aplikacijski zastupnici (engl. application proxies)
- sigurnosne stijene (engl. firewalls)
- Kerberos i drugi sustavi ovjere ~ AAA poslužitelji (engl. Authentication, Authorization and Accounting servers)
- sigurne elektroničke transakcije SET

Predma se u modelu OSI (engl. Open Systems Interconnection) mrežna sigurnost mahom promatra sa stanovišta *manipulacija nad podacima*, te stoga pripadna funkcionalnost pripada *predodžbenom sloju* (engl. presentation layer), sigurnosni se zahvat mogu provoditi i u nekim drugim slojevima, počevši od fizičkoga (OSI sloj 1). Unutar OSI razrađena je i odnosna sigurnosna arhitektura, s pregledom sigurnosnih usluga (po slojevima) utvrđenih u sklopu normi OSI te sigurnosnim postupcima koji ih implementiraju. Naravno, i u Internetu se radi to isto, iako na manje formalan način.

Sigurnosna arhitektura Interneta predviđa niz postupaka i protokola koji se izvršavaju u slojevima komunikacijskog modela TCP/IP. Primjerice, u aplikacijskom se sloju mogu izvršavati razne sigurnosne aplikacije (npr. sigurne elektroničke transakcije koje su temelj kartičnog poslovanja, ili *ovjera klijenata* koji žele pristupiti nekom poslužitelju), dok se u mrežnom sloju ostvaruju pretpostavke za izgradnju sigurnih privatnih (unutarnjih, korporacijskih) mreža nad javnom infrastrukturom, odnosno Internetom (*virtualne privatne mreže*), prejenjem paketa putem "tunela" zaštićenih sigurnosnim dodatkom protokola IP – IPsec.

U nastavku se obrađuje nekoliko sigurnosnih postupaka karakterističnih za internetsku okolinu, kao i pripadni sigurnosni protokoli.

Navedeni su neki od zahvata koji se koriste radi ostvarivanja sigurnosti u Internetu:

- IP filtriranje* je provjera i propuštanje paketa u skladu s tablicom dozvoljenih izvora i odredišta, koju provode ulazni i izlazni usmjeritelj sigurnosne stijene;
- prevođenje mrežne adrese* izvorno je postupak racionaliziranja korištenja IP adresa unutar IPv4, koji se pak može koristiti i kao tehnika prikidanja adresa unutar neke privatne mreže (intranet) u cilju sprečavanja napada uskraćivanjem usluga (tj. spriječavanja kompromitiranja radne sposobnosti poslužitelja);
- sigurnosna arhitektura za IP* (IPsec) je sigurnosni dodatak mrežnom protokolu IP, kojim se štiti integritet i povjerenljivost korisnih podataka paketa, odnosno i samoga zaglavja (pa stoga i informacije o izvoru i odredištu paketa);
- SOCKS* je standard za uspostavljanje *aplikacijskog spojnjog pristupa* unutar sigurnosne stijene, kojim se provjerava ovlaštenost korisnika u zaštićenoj privatnoj mreži za uspostavljanje spoja s nekim poslužiteljem u "vanjskoj" nezaštićenoj mreži; odnosno SOCKS poslužitelj djeluje kao "usmjeritelj aplikacijske razine" između klijenta i stvarnog (radnog) poslužitelja;
- sloj sigurnih priključaka* (SSL) osigurava sigurnost Webovskih transakcija (odnosno hipertekstovnih prijenosa, jer se mahom koristi kao sigurnosni protokol za inkapsulaciju HTTP poruka prije njihova dostavljanja protokolu TCP);
- aplikacijski zastupnici* (engl. application proxies, ili *aplikacijski spojni pristupi*, engl. application gateways) dijelovi su sigurnosne stijene koji provode analizu prometa i ispitivanje razmjerenih sadržaja;
- sigurnosne stijene* implementiraju jedinstvenu točku pristupa privatnoj (unutarnjoj, zaštićenoj) mreži, koja predstavlja "čuvana vrata" (engl. guarded gate) na kojima se filtrira promet paketa (IP filtriranje) za privatnu mrežu i iz nje, a također se provjerava sadržaj prenošenih poruka aplikacijske razine (npr. poruka e-pošte);
- sustavi ovjere* (od kojih je Kerberos jedan od najpopулarnijih) osiguravaju provjeru identiteta partnera u komunikaciji (mahom klijenata koji želi pristupiti resursima poslužitelja); ovde treba lučiti između ovjere (identifikacije korisnika) i autorizacije (njegove "ovlaštenosti") za korištenje nekih resursa (što se postiže u popisu prava pristupa pojedinim resursima), a često se naziva i *upravljanje pristupom* (engl. access control);
- posebno su za karakteristične (financijske) raspoložljive aplikacije, kakvo je primjerice kartično poslovanje (masovna i važna primjena ☺), razvijeni prikladni sigurnosni protokoli (koja što su sigurne elektroničke transakcije).

Značajniji internetski sigurnosni postupci i protokoli razrađuju se u nastavku, temeljeći se na osnovnim sigurnosnim postupcima kriptiranja podataka te zaštite njihova integriteta.

Sigurnosna arhitektura Interneta



	upravljanje pristupom	kriptiranje	ovjera	provjera integriteta	PFS(*)	prikrivanje adresе	praćenje sjednice
IP filtriranje	da	ne	ne	ne	ne	ne	ne
NAT	da	ne	ne	ne	ne	da	da
IPSec	da	da (paket)	da (paket)	da (paket)	da	da	ne
SOCKS	da	ne		ne	ne	da	da
SSL	da	da (podaci)	da (sustav-korisnik)	da		ne	da
aplikacijski zastupnici	da	normalno ne	da (korisnik)	da	normalno ne	da	da (spoj i podaci)
AAA poslužitelji	da (korisnik)	ne	da (korisnik)	ne	ne	ne	ne

(*) PFS (engl. Perfect Forward Secrecy): kompromitiranje prethodnih ključeva ne pruža korisnu informaciju za probijanje narednih; svaki novi ključ se izvodi neovisno o prethodnim

Tablica prikazuje sigurnosne usluge koje ostvaruju pojedini sigurnosni postupci i protokoli Interneta.

Sadržaj predavanja



- ◆ Sigurnosna arhitektura Interneta
- ◆ **Virtualne privatne mreže**
 - tuneliranje
 - prevodenje mrežne adrese
- ◆ Sigurnosna stijena
- ◆ Sigurnosna arhitektura za IP – IPsec
- ◆ Sloj sigurnih priključaka SSL
- ◆ SET
- ◆ Protokoli ovjere

Komunikacijske mreže

8.12.2007

8 od 59

Virtualne privatne mreže



- ◆ VPN (engl. Virtual Private Networks): vlastite (korporacijske) zaštićene mreže korištenjem postojeće javne internetske jezgre mreže
 - podrška unutarnjopravnoj i međukorporacijskoj komunikaciji
 - izbjegavanje troškova iznajmljivanja vodova i/ili kanala, ili nekih drugih usluga telekoma
 - pružanje sigurnosti tradicionalne privatne, samoadministrisane korporacijske mreže
- ◆ ostvarivanje VPN:
 - stvaranje sigurnog privatnog spoja putem nekog privatnog *tunela*
 - VPN rješenja trenutno temeljena na okolinama IPv4, s mogućnošću nadogradnje na IPv6 radi *osiguranje zajedničkog rada* (engl. interoperability) s budućim rješenjima

Komunikacijske mreže

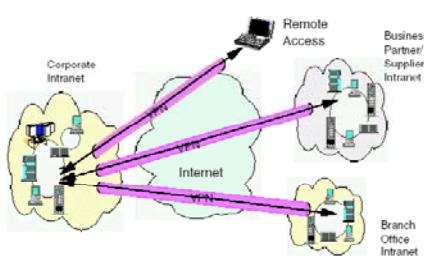
8.12.2007

9 od 59

Ekonomski i praktični razlozi ponukali su poslovne subjekte (naročito velike firme i korporacije) da napuste praksu izgradnje i korištenja vlastitih *privatnih* mreža računala (obično nad kanalima ili čak i fizičkim vodovima iznajmljenim od telekomunikacijskih operatera) u korist *virtualnih* privatnih mreža izgrađenih nad "zaštićenim kanalima" postojeće mrežne infrastrukture kakva je primjerice Internet.

Takve su virtualne mreže zasnovane na *tunelima* (usporedivo s prijevozom automobila ili kamiona vlakovima) koji su naravno "osigurani" primjerenim sigurnosnim protokolima kakav je IPsec.

Virtualne privatne mreže



Komunikacijske mreže

8.12.2007

10 od 59

VPN se gradi iznad Interneta, i nije nužno stacionarnog tipa; njezina je korist naročito u pružanju sigurne komunikacije s korporacijskim poslužiteljima za *dislocirane* namještenike (koji su *pokretni*, dakle na putu).

Tuneliranje



- ◆ *tuneliranje* (engl. tunneling): specijalni slučaj povezivanja podmreža, kad su partnerska radna računala (engl. hosts) na mreži istog tipa!
- ◆ primjena (inače): povezivanje LANova putem WAN-a:
 - WAN djeluje poput serijske linije = tunel
 - LAN paket iz MAC okvira → WAN paket (korisni teret)
 - otprema na drugi kraj WAN
 - LAN paket iz WAN paketa → MAC okvir
 - način izgradnje virtualnih privatnih mreža, VPN
- ◆ *tunel* je "virtualna serijska linija" i može se prikladno zaštiti (primjerice protokolom IPsec)

Komunikacijske mreže

8.12.2007

11 od 59

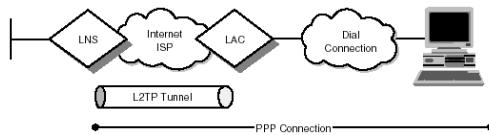
Radi podrške ostvarivanju tunela (naročito) za pokretne korisnike funkcionalnost internetskog podatkovnog pristupnog protokola PPP (engl. Point-to-Point Protocol) proširuje se (pod)protokolom L2TP (engl. Layer 2 Tunneling Protocol). Time se uspostavlja internetski *virtualni link* (poveznica) između računala pokretnog korisnika (klijent) i zaštićenog korporacijskog poslužitelja. Korisnik je na Internet priključen biranom linijom.



Tuneliranje

tunel se gradi preko Interneta, izvršavanjem protokola L2TP (engl. Layer 2 Tunneling Protocol), i to između:

- koncentratora pristupa L2TP, LAC (engl. L2TP Access Concentrator), na klijentskoj strani tunela
- mrežnog poslužitelja L2TP, LNS (engl. Network Server), na poslužiteljskoj strani tunela



Komunikacijske mreže

8.12.2007

12 od 59

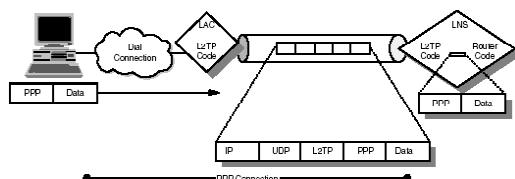
Aktivne su naprave koje su krajne točke tunela (na "obodu" Interneta) koncentrator pristupa LAC i mrežni poslužitelj LNS.



Tuneliranje

L2TP tunel ~ inkapsulacija L2TP:

- okviri L2TP inkapsulirani u segment UDP
- segmenti UDP inkapsulirani u paket IP



Komunikacijske mreže

8.12.2007

13 od 59

Inkapsulacija prema L2TP utvrđuje umetanje okvira PPP, primjereno "obuhvaćenog" okvirom L2TP, u segment UDP koji se dalje prenosi Internetom.



Prevodenje mrežne adrese

- ♦ izvorno zahvat uveden radi nedostatka IP adresa u IPv4: odvojiti adresiranje unutar zatvorene cjeline (npr. intranet) od onog u Internetu
- ♦ prevodenje adresa: *prevoditelj mrežnih adresa* (engl. NAT box)
- ♦ *sigurnosna* primjena:
 - odvajanje privatne mreže od Interneta, kada nije na raspolaganju primjerena sigurnosna stijena
 - privatne (unutarnje) IP adrese *nisu objavljene* u Internetu: zaštita poslužitelja od napada uskraćivanja usluga

Komunikacijske mreže

8.12.2007

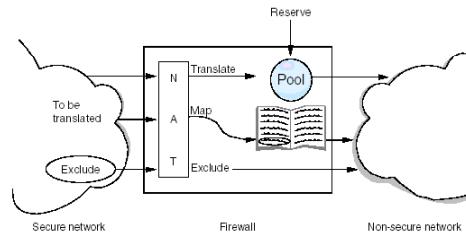
14 od 59

Prevoditelj mrežnih adresa korisnicima izgleda kao "normalni" usmjeritelj koji proslijeđuje IP pakete. Za izlazne IP pakete (one koji "izlaze" iz privatne mreže) se izvorišna adresa nakon uspješne provjere ("smiju" li izići i biti proslijeđeni na navedenu odredišnu IP adresu?) prevodi u jednu rezerviranu vanjsku ("globalnu") i obratno (propušta se onaj paket čija se odredišna adresa koristi u NAT).



Prevodenje mrežne adrese

- konfiguracija prevoditelj mrežnih adresa:



Komunikacijske mreže

8.12.2007

15 od 59

Sadržaj predavanja



- Sigurnosna arhitektura Interneta
- Virtualne privatne mreže
- Sigurnosna stijena**
 - komponente sigurnosne stijene
 - sigurnosna politika
- Sigurnosna arhitektura za IP – IPsec
- Sloj sigurnih priključaka SSL
- SET
- Protokoli ovjere

Komunikacijske mreže

8.12.2007

16 od 59

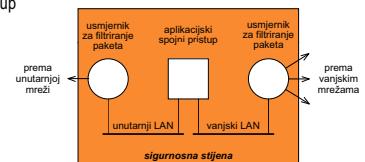
Sigurnosna stijena



"vatrozid" (engl. firewall):

mehanizam ostvarivanja nadzora nad pristupom privatnoj mreži:

- jedinstvena točka pristupa: može se lakše nadzirati
- više tipova ~ zahtijevana moć zaštite i uključena HW/SW oprema
- komponente (općenito):
 - usmjeritelji za filtriranje paketa
 - aplikacijski spojni pristup



Komunikacijske mreže

8.12.2007

17 od 59

Sigurnosne stijene (engl. firewall) sustavi su (ili grupe sustava) koji nameću utvrđenu sigurnosnu politiku između neke sigurne privatne (unutarnje, zaštićene) mreže i nesigurne (vanjske) mreže kakva je Internet te na taj način štite privatnu mrežu od sigurnosnih napada "izvana".

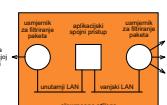
Sigurnosne stijene utvrđuju informaciju, odnosno usluge, kojima se izvana može pristupiti, kao i tko smije pristupiti vanjskim informacijama, odnosno uslugama.



Komponente sigurnosne stijene

- usmjeritelji za filtriranje paketa:

- izlazni promet: usmjeritelj na unutarnjem LANu
- ulazni promet: usmjeritelj na vanjskom LANu
- tablice filtriranja:
 - prihvativi izvori/odredišta
 - izvori/odredišta koji se blokiraju
 - prepostavljena (engl. default) pravila za postupanje u slučaju prometa različitog od gornjeg



Komunikacijske mreže

8.12.2007

18 od 59

Usmjeritelji za filtriranje paketa (engl. packet-filtering router) donose odluke o poslijedivanju paketa na temelju informacija iz zaglavja (izvorna/odredišna IP adresa, TCP/UDP pristupi, tipovi ICMP poruka, informacija o inkapsuliranom protokolu). Oni provode:

- filtriranje prema usluzi: promatraju se *standardni* pristupi (engl. ports) TCP/UDP, a n'estandardni se pristupi obrađuju s oprezom (npr. NSF koristi RPC, kod kojeg se pristupi dodjeljuju spojevima *dinamički*);
- filtriranje prema izvoru/odredištu: promatraju se IP adrese izvora i odredišta; primjerice, poznat je stroj na kojem se izvršava poslužiteljska aplikacija;
- napredno filtriranje: primjerice, provjeravaju se opcije zaglavja paketa IP, posmak (engl. offset) segmenata, itd.

Aplikacijski spojni pristup ostvaruje funkciju "zastupnika" ("opunomoćenika", engl. proxy), obavljajući višu razinu nadzora nad prometom između dvije mreže tako što prati i filtrira sadržaj neke usluge.

Zastupnik djeluje kao poslužitelj za klijenta, a kao klijent za poslužitelja, čime se između klijenta i poslužitelja gradi *virtualni* spoj; za partnerne koji komuniciraju zastupnik je *transparentan*! Njegova je funkcionalnost vezana za upravljanje razmjenom podataka na aplikacijskoj razini, bilježenje (engl. logging) poslužitelja koje je klijent posjetio i ostvarivanje snažnije ovjera korisnika.

Prijenosni spojni pristup (engl. circuit-level gateway) može također biti komponenta jednostavnijih sigurnosnih stijena. Podržava "prijenos" (engl. relay) prijenosnih (engl. transport) spojeva bez dodatne obrade paketa ili filtriranja time također ostvarujući *transparentni* spojni pristup:

- pruža podršku većem broju aplikacija nad TCP/IP ili UDP/IP, bez dodatnih modifikacija na klijentskoj strani aplikacije;
- koristi se uglavnom za *izlazni* spoj (prema nesigurnoj mreži), dok se primjerice aplikacijski spojni pristup koristi za oba smjera!

Tipičan primjer funkcionalnosti prijenosnog spojnog pristupa je standard SOCKS (djeluje kao "usmjeritelj aplikacijske razine" između klijenta i stvarnog (radnog) poslužitelja).

Dvije su moguće sigurnosne politike koje može provoditi sigurnosna stijena:

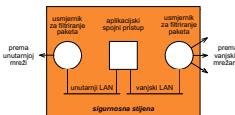
- "uskraćeno je sve što nije posebno dozvoljeno", i
- "dozvoljeno je sve što nije posebno uskraćeno".

Komponente sigurnosne stijene



♦ aplikacijski spojni pristup

- djeluje na *aplikacijskoj* razini:
 - analiza prometa između distribuiranih aplikacija
 - eventualno i ispitivanje sadržaja
- npr. spojni pristup za elektroničku poštu: ispitivanje zaglavja poruka, veličine poruka, sadržaja poruka



Komunikacijske mreže

8.12.2007

19 od 59

Sigurnosne politike u sigurnosnoj stijeni



♦ uskraćeno je sve što nije posebno dozvoljeno: najsigurnija metoda!

- blokiranje cijelokupnog prometa između dvije mreže osim za usluge i aplikacije koje su eksplicitno dozvoljene (a omogućio ih je administrator)
- svaka željena usluga i aplikacija treba se pojedinačno implementirati
- ne dozvoljava se niti jedna usluga i aplikacija koja bi mogla biti potencijalni proboci u sigurnosnoj stijeni
- restrikтивnije i manje pogodno s gledišta korisnika

♦ dozvoljeno je sve što nije posebno uskraćeno:

- omogućen sav promet između dvije mreže osim za one usluge i aplikacije koje su uskraćene
- svaka usluga ili aplikacija koja nije od povjerenja (engl. untrusted) ili je i potencijalno štetna (engl. harmful) treba se pojedinačno uskratiti
- za korisnike fleksibilna i pogodna metoda, ali potencijalno može prouzrokovati ozbiljne sigurnosne probleme

Komunikacijske mreže

8.12.2007

20 od 59

Sadržaj predavanja



♦ Sigurnosna arhitektura Interneta

♦ Virtualne privatne mreže

♦ Sigurnosna stijena

♦ **Sigurnosna arhitektura za IP – IPsec**

- protokol IKE
 - načini korištenja IPsec
 - zaglavja protokola IPsec
- ♦ Sloj sigurnih priključaka SSL
- ♦ SET
- ♦ Protokoli ovjere

Komunikacijske mreže

8.12.2007

21 od 59

Sigurnosna arhitektura za IP

"sigurnost za IP" (engl. IP security, IPsec)
(RFC 2401, 2402, 2406): sigurnosni dodatak za IP

- okvir za višestruke usluge, algoritme i zrnatost
- dva glavna dijela:
 - opis *zaglavja* za prijenos sigurnosne informacije
 - protokol za poslovanje ključevima IKE
(engl. Internet Key Management Exchange)
- kriptiranje:
 - temeljeno na kriptografiji *simetričnih* ključeva (bolje performanse)
 - korištenje pri (samo) prijenosu ili tuneliranju
 - "prazni algoritam" (engl. null algorithm):
isključivanje računski zahtjevnog kriptiranja

Komunikacijske mreže

8.12.2007

22 od 59



Sigurnosni se mehanizmi u Internetu mahom ostvaruju bilo u aplikacijskom sloju, čime se osigurava zaštita "s kraja na kraj" (krajnje su točke upravo pristupi aplikacijskim procesima u udaljenim radnim računalima), ili u mrežnom, pa se zaštita (npr. ovjera i/ili kriptiranje paketa) provodi bez uključivanja korisnika (tj aplikacijskih procesa).

U prvome slučaju, kriptiranje i provjeru integriteta provode aplikacijski procesi, što zasigurno pruža bolja sigurnost, jer se obuhvaća *sakriveno* moguće manipuliranje između aplikacijskih procesa, uključivo ona *unutar* operacijskih sustava. Naravno, ugradnja sigurnosnih mehanizama zahtijeva modifikacije postojećih aplikacija. S druge strane, kada se sigurnost ostvaruje u mrežnom sloju, ovjera i/ili kriptiranje paketa obavlja se *bez* uključivanja korisnika, što ima barem dvije prednosti [Tanenbaum, 2003]:

- tipični korisnici ionako ne razumiju sigurnosne probleme i ne bi mogli ispravno koristiti sigurnosne mehanizme;
- izbjegava se potreba modificiranja postojećih programa.

Navedeno je potaklo razvoj standarda za sigurnost mrežnog sloja – *sigurnosnu arhitekturu za IP* (IPsec), s ciljem da se pruži pomoć u ostvarivanju sigurnosti svim korisnicima, a s druge strane to ne sprječava primjenu specifičnih sigurnosnih zahvata u aplikacijskom sloju.

Trenutno (podaci iz 12/2005) je aktualna verzija 2 – IPsec ver. 2.

Protokol IPsec



◆ spojno orijentirani:

- "spoj" ~ *sigurnosno udruživanje SA* (engl. security association):
- ključ se utvrđuje i koristi *samo* izvjesno vrijeme
 - ~ neka vrsta spoja
 - amortiziranje troškova uspostavljanja udruživanja preko mnogo paketa
- ◆ ostvarivanje sigurnosnog udruživanja SA:
- jednosmjerni (engl. simplex) spoj s pridruženim *sigurnosnim identifikatorom* (engl. security identifier):
 - identifikatori unutar paketa
 - prisjeće paketa inicira *pregledavanje* (engl. look up) ključeva i drugih relevantnih informacija
 - sigurni promet u *oba smjera*: dva sigurnosna udruživanja

Komunikacijske mreže

8.12.2007

23 od 59

Sigurnosna je arhitektura Interneta implementirana protokolom IPsec. Utvrđeno je dvojako korištenje IPsec:

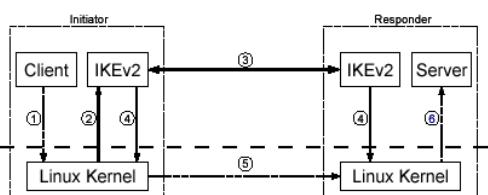
- u *prijenosnom* načinu, radi osiguranja integriteta ili i tajnosti podataka prenošenih unutar paketa IP;
- u *tunelskom* načinu, kad se *potpuno* kriptira izvorni paket IP (korisni podaci – segment TCP, ali i zaglavlj), a osigurava se i integritet tako kriptiranog paketa.

IPsec je spojno orijentirani protokol, s time što je "spoj" sigurna sjednica koja se naziva *sigurnosno udruživanje* (engl. security association, SA). SA se štiti *tajnim* (simetričnim) ključem, koji se utvrđuje prethodnim pregovaranjem partnera.

Protokol IKE



- ◆ *protokol IKE* (Internet Key Exchange):
poslovanje (generiranje i osvježavanje) sjedničkim ključevima i
sigurnosnim udruživanjima
~ dosta složena procedura



Komunikacijske mreže

8.12.2007

24 od 59

Koraci pregovaranja unutar protokola IKE (operacijski je sustav Linux).

Načini korištenja IPsec



- ♦ **prijenosni način** (engl. transport mode):
umetanje **zaglavljiva IPsec** iza zaglavlja IP
 - promjena polja protokola u zaglavljiju IP (zaglavljje IPsec *prije* zaglavlja TCP)
 - sigurnosna informacija (identifikator SA, novi *sigurnosni* redni broj paketa, provjera integriteta korisnog tereta)
- ♦ **tunelski način** (engl. tunnel mode):
inkapsuliranje **cijelog IP paketa** u tijelo *novog* IP paketa s *novim* zaglavljem IP, što pruža višestruke koristi:
 - tunel završava na lokaciji različitoj od odredišne:
 - transparentnost sigurnosnih aktivnosti za radna računala intraneta
 - obavlja ih sigurnosni spojni pristup – sigurnosna stijena [firewall]
 - agregiranje skupa TCP spojeva:
 - jedan kriptirani tok
 - sprječavanje uljeza u provođenju *analyze prometa*

Za razliku od prijenosnog načina, u tunelskom se načinu kriptira i ovjerava *cijeli izvorni paket IP*.

Formati zaglavlja IPsec



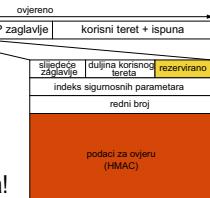
- ♦ **zaglavlje AH** (engl. Authentication Header):
osigurava samo integritet podataka
- ♦ **zaglavlje ESP** (engl. Encapsulating Security Payload):
 - izvorno samo tajnost podataka, naknadno proširen provjерom integriteta
 - efikasniji, očekuje se postupna zamjena AH njime

U posljednje se vrijeme napušta zaglavje ovjere AH u korist zaglavlja ESP.

Zaglavlje AH



- ♦ provjera integriteta
- ♦ sigurnost od *napada ponavljanjem* (engl. antireplay security)
- ♦ **ne i tajnost:** nema kriptiranja podataka!
- ♦ korištenje u *prijenosnom načinu*:
 - za IPv4: između zaglavlja IP (sa svim opcijama) i zaglavlja TCP
 - za IPv6: samo još jedno **zaglavlje proširenja**
 - polje korisnog tereta:
ispuniti na neku specifičnu duljinu, radi provođenja algoritma ovjere



Zaglavlje AH



polje	značenje
sljedeće zaglavlje	vrijednost polja protokola u zaglavljiju IP <i>prije</i> zamjene s 51 (sljedi zaglavlje AH); u većini slučajeva slijedi kod za TCP (6)
duljina korisnog tereta	(broj 32-bitnih riječi zaglavlja AH) – 2
indeks sigurnosnih parametara	identifikator spoja koji se umeće radi ukazivanja na neki specifični zapis u primateljevoj bazi podataka; taj zapis sadrži dijeljeni ključ koji se koristi u ovom spoju kao i drugu informaciju o spaju
redni broj	numeriranje svih paketa koji se šalju unutar jednog SA; svaki paket dobiva <i>jedinstveni</i> redni broj, uključujući i retransmisijske (premda redni broj TCP ostaje isti!), radi otkrivanja napada ponavljanjem ako se iscripi prostor rednih brojeva 2^{32} , u smislu nastavka komunikacije potrebno je uspostaviti novi SA
podaci za ovjerenje (HMAC)	polje promjenjive duljine s digitalnim potpisom korisnog tereta; pri uspostavljanju SA partnerske strane pregovaraju o algoritmu potpisa koji će se koristiti, a normalno se, radi poboljšanja performansi, koriste simetrični algoritmi

Objašnjenje pojedinih polja zaglavljia AH.

Zaglavljie AH



računanje digitalnog potpisa korištenjem *dijeljenog ključa: hash* (*cijeli paket, dijeljeni ključ*):

- dijeljeni ključ prethodno utvrđen pregovaranje partnera
- provjerom integriteta *nepromjenjivih* polja zaglavljia IP (npr. IP adresa izvora) onemogućeno falsificiranja izvora paketa
- ubrzanje postupka
- shema HMAC (engl. Hashed Message Authentication Code)

Komunikacijske mreže

8.12.2007

29 od 59

Zaglavljie ESP



◆ prijenosni način



◆ tunelski način



Komunikacijske mreže

8.12.2007

30 od 59

Zaglavljie ESP koristi se u oba načina – prijenosnom i tunelskom. Stoga je i razumljivo da se pomalo napušta korištenje zaglavljia AH u smislu ekonomičnosti korištenja različitih mehanizama. Dodatno, zaglavljie ESP uz ovjeru podataka (osiguranje integriteta podataka) ostvaruje i povjerljivost prijenosa.

Zaglavljie ESP



◆ format zaglavljia ESP: dvije ili tri 32-bitne riječi

- indeks sigurnosnih parametara
- redni broj
- vektor *inicijalizacije*, koristi se kod kriptiranje, a ispušta kod primjene *praznog kriptiranja*

◆ provjera integriteta putem HMAC:

- nakon korisnog tereta
- implementacije su sklopovske: HMAC SE računa prilikom slanja bitova, i naknadno se dodaje *na kraj* paketa

Usluge i algoritmi IPsec



◆ više *usluga*: zadovoljavanja specifičnih potreba odgovara troškovima dodatne obrade

◆ *osnovne usluge*:

- tajnost (povjerljivost) podataka
- integritet podataka
- zaštita od napada ponavljanjem (uljez ponavlja neku konverzaciju)

◆ više *algoritama*:

opstanak okvira IPsec i u slučaju promjene algoritama, po kompromitiranju duže korištenih algoritama

Komunikacijske mreže

8.12.2007

31 od 59

Komunikacijske mreže

8.12.2007

32 od 59

Sadržaj predavanja

- ◆ Sigurnosna arhitektura Interneta
- ◆ Virtualne privatne mreže
- ◆ Sigurnosna stijena
- ◆ Sigurnosna arhitektura za IP – IPsec
- ◆ **Sloj sigurnih priključaka SSL**
 - protokol rukovanja
 - protokol SSL zapisa
- ◆ SET
- ◆ Protokoli ovjere



Komunikacijske mreže

8.12.2007

33 od 59

Sloj sigurnih priključaka SSL

(engl. Secure Sockets Layer):
de facto sigurnosni protokol, izvorno vlasnički protokol
Netscape Communications Corp.

- podrška sigurnom obavljanju financijskih transakcija putem Weba (nabava kreditnom karticom, on-line bankarstvo itd.)
- sigurni spoj između dva priključka:
 - pregovaranje klijenta i poslužitelja o parametrima
 - uzajamna ovjera klijenta i poslužitelja
 - tajna komunikacija
 - zaštita integriteta podataka



Komunikacijske mreže

8.12.2007

34 od 59

Sigurnosni programski paket koji se ugrađuje u *preglednike* (engl. browsers), a razvila ga je tvrtka Netscape. U međuvremenu je postao toliko popularan da se koristi i u suparničkom pregledniku Internet Explorer.

Sloj sigurnih priključaka SSL

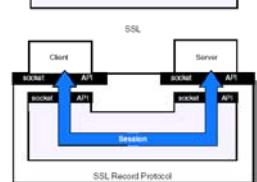
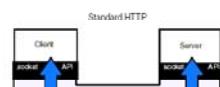
- ◆ između aplikacije (tipično HTTP) i prijenosa (TCP):
 - HTTP nad SSL: HTTPS (engl. Secure HTTP)
 - katkad s novim ID pristupom 443, umjesto standardnog 80
- ◆ zadaće SSL:
 - uspostavljanje sigurnog spoja
 - kompresija i kriptiranje podataka
- ◆ više verzija,
s puno različitih algoritama
i opcija

aplikacija (HTTP)
sigurnost (SSL)
prijenos (TCP)
mreža (IP)
podatkovna veza (PPP)
fizička veza (modem, ADSL, CATV)

SSL se smješta između aplikacijskog i prijenosnog (transportnog) sloja. Kako pruža alternativni pristup (ID = 443), nad njim je moguće na sigurni način izvršavati i druge internetske aplikacije.

Sloj sigurnih priključaka SSL

- dva (pod)protokolna sloja
- **protokol SSL rukovanja**
(engl. SSL Handshake Protocol): početna ovjera i prijenos ključeva za kriptiranje
 - **protokol SSL zapisa**
(engl. SSL Record Protocol): prijenos podataka



Komunikacijske mreže

8.12.2007

36 od 59

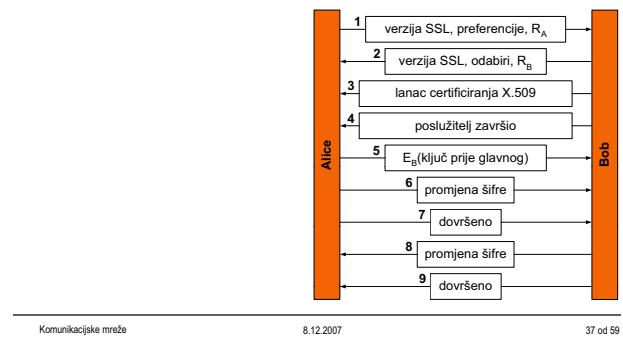
SSL se sastoji od dva protokolna sloja:

- niži sloj obuhvaća protokol za prijenos podataka, koji može koristiti više prethodno utvrđenih kombinacija šifri i ovjera;
- viši je sloj ostvaren protokolom za početnu ovjeru i razmjenu ključeva.

Na slici je SSL prikazan kao da pruža (posebno) sučelje priključka (engl. socket interface) za raspodijeljene aplikacije; u stvarnosti ovo sučelje priključka dolazi već ugrađeno unutar SSL programskog paketa te ne pruža API (engl. Application Program Interface) koje bi moglo koristiti druge aplikacije.

Protokol rukovanja SSL

protokol početnog rukovanja SSL
~ uspostavljanje (sigurnog) spoja



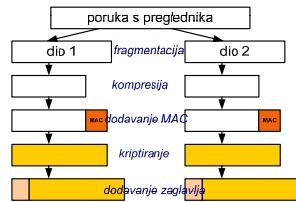
Koraci protokola početnog rukovanja SSL:

1. Alice (klijent) → Bob (poslužitelj): zahtjev za uspostavljanje spoja sa sigurnosnim parametrima (verzija SSL, preferencije u pogledu algoritama kompresije i kriptiranja); također se šalje nonce (slučajno odabrani veliki broj) R_A ;
2. Alice ← Bob: Bob bira algoritme te šalje svoj nonce R_B ;
3. Alice ← Bob: Bob šalje svoj certifikat s javnim ključem ili, alternativno, ako certifikat nije potpisao neki poznati CA, lanac certifikata; on može poslati još koju poruku (npr. zahtjev za certifikat s javnim ključem od Alice);
4. Alice ← Bob: Bob predaje komunikaciju Alice;
5. Alice → Bob: Alice odabire slučajni 384-bitovni "ključ prije glavnog" (engl. premaster key) i šalje ga Bobu kriptiranog njegovim javnim ključem E_B ; stvari sjednički ključ generira se iz ključa prije glavnog i oba noncea (R_A i R_B);
6. Alice → Bob: Alice javlja Bobu da se prebaci na novu šifru i...
7. Alice → Bob: ... da je dovršila (pod)protokol uspostavljanja sigurnog spoja (odnosno početno rukovanje);
8. Alice ← Bob: Bob potvrđuje promjenu šifre i...
9. Alice ← Bob: ... dovršavanje početnog rukovanja.

Protokol SSL zapisa

prijenos podataka:

- razbijanje poruka s preglednika (engl. browser) u jedinice od 16K
- svaka se jedinica komprimira odvojeno
- dodaje se MAC (engl. Message Authentication Code):
hash (tipično MD5) komprimirane poruke
i ulančanog tajnog ključa
prethodno izvedenog
iz oba noncea
i ključa prije glavnog
- sve se kriptira
dogovorenim
simetričnim algoritmom kriptiranja
- dodaje se zaglavje



Slijedi prijenos podataka sigurnim spojem:

- preduge se poruke s preglednika fragmentiraju te se svaka odvojeno komprimira (ako je odabrana ova opcija);
- komprimirani se fragmenti potpisuju i kriptiraju (prethodno dogovorenim simetričnim postupkom) zajedno s potpisom;
- tako kriptirani fragmenti, kojima je dodano zaglavje, šalju se putem TCP spoja.

Ostali protokoli temeljeni na SSL

- ◆ sigurnost prijenosnog sloja (engl. Transport Layer Security, TLS):
 - de iure (IETF) normiranje vlasničkog standarda SSL, RFC 2246 (TLS 1.0 ~ SSL 3.0)
 - između SSL i TLS (ipak) postoje male razlike koje priječe potpunu sposobnost suradnje (engl. interoperability)
- ◆ sigurni MIME (engl. Secure Multipurpose Internet Mail Extension, S-MIME):
 - interpretira se kao posebna vrsta protokola sličnog SSL
 - koristi se u zaštiti poruka e-pošte (kriptiranje, digitalni potpis)
 - zasniva se na tehnologiji javnih ključeva te koristi certifikate prema X.509 za utvrđivanje identiteta partnera
 - implementira se u udaljenim radnim računalima, ali ne i u usmjeriteljima ili sigurnosnim stijenama

Koji se puta TLS 1.0 označava i kao SSL 3.1.

Sadržaj predavanja



- ◆ Sigurnosna arhitektura Interneta
- ◆ Virtualne privatne mreže
- ◆ Sigurnosna stijena
- ◆ Sigurnosna arhitektura za IP – IPsec
- ◆ Sloj sigurnih priključaka SSL
- ◆ **SET**
- ◆ Protokoli ovjere

Komunikacijske mreže

8.12.2007

40 od 59

Sigurne elektroničke transakcije



(engl. Secure Electronic Transactions), SET:
rezultat dogovora MasterCard i Visa radi utvrđivanja *jedinstvenog* elektroničkog sustava kreditnih kartica:

- protokol SET transakcija:
specificiran veći broj transakcija za nabavu, ovjeru, obrat plaćanja (engl. payment reversal), itd.
- shema certificiranja:
hijerarhija certifikacijske strukture
- spojni pristup plaćanja stjecatelju (engl. acquirer payment gateway)
pruža dobro definirano i sigurno sučelje između trgovca (na Internetu) i kartične mreže (engl. bank card network) koju koriste stjecatelj i izdavatelj

Komunikacijske mreže

8.12.2007

41 od 59

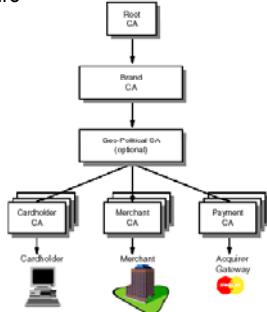
Uloge (engl. roles) unutar specifikacije SET (prema Rodriguez *et al.*, vidi prethodnu referencu):

- trgovac* (engl. merchant): prodavač robe, usluga ili informacija;
- stjecatelj* (engl. acquirer): organizacija koja pruža kartičnu uslugu (npr. MasterCard ili Visa);
- izdavatelj* (engl. issuer) kreditne kartice kupcu (engl. purchaser); obično je to banka ili slična finansijska ustanova;
- klijent* – posjednik kreditne kartice (engl. cardholder): "Web surfer" koji kupuje putem Weba;
- spojni pristup plaćanja stjecatelju* (engl. acquirer payment gateway);
- certifikacijski autoritet*.

Sigurne elektroničke transakcije



hijerarhija certifikacijske strukture



Komunikacijske mreže

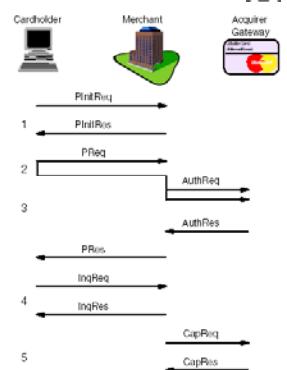
8.12.2007

42 od 59

SET transakcija



tipične elektroničke
(engl. online) nabave:
svaka se *transakcija*
sastoji od *para* zahtjev-odziv



Komunikacijske mreže

8.12.2007

43 od 59

SET transakcija



- ◆ *PInitReq, PInitRes*: inicijalizacija sustava
- ◆ *PReq, PRes*: narudžba (engl. purchase order); stvarni zahtjev korisnika za kupovinu; kombinacija dvije poruke:
 - nalog za narudžbu (engl. order instruction, OI): šalje se trgovcu kao otvoreni tekst
 - nalog za nabavu (engl. purchase instruction, PI):
 - trgovac prenosi PI spojnjom pristupa plaćanja kriptirano javnim klijem stjecatelja: trgovac je ne može pročitati!
 - u PI je uključen hash OI:
OI i PI se mogu manipulirati samo kao par
 - broj kartice je sadržan samo u PI
 - OI se obično šalje nakon odobrenja stjecatelja

Komunikacijske mreže

8.12.2007

44 od 59

SET transakcija



- ◆ *AuthReq, AuthRes*: autorizacija (engl. ovlašćivanje); putem spojnjog pristupa plaćanja trgovac traži od stjecatelja da autorizira zahtjev
 - poruka uključuje opis nabave i cijenu, a također i PI iz narudžbe koju je korisnik prethodno poslao: stjecatelj zna da se trgovac i kupac slažu o onome što se kupuje i o cijeni
 - po primitu zahtjeva stjecatelj koristi postojeću kartičnu mrežu za njegovu autorizaciju te vraća primjereni odgovor

Komunikacijske mreže

8.12.2007

45 od 59

SET transakcija



- ◆ *InqReq, InqRes*: raspitivanje; korisnik može poželjeti znati kako se odvija njegov zahtjev
- ◆ *CapReq, CapRes*: prijenos novca (engl. capture); stvarni nalog stjecatelju da prenese prethodno ovlašteni iznos na svoj račun; može se ugraditi i kao dio zahtjeva/odziva autorizacije, ali ima situacija kad trgovac preuzima novac kasnije (npr. pri isporuci dobara putem pošte)

Komunikacijske mreže

8.12.2007

46 od 59

Sadržaj predavanja



- ◆ Sigurnosna arhitektura Interneta
- ◆ Virtualne privatne mreže
- ◆ Sigurnosna stijena
- ◆ Sigurnosna arhitektura za IP – IPsec
- ◆ Sloj sigurnih priključaka SSL
- ◆ SET
- ◆ **Protokoli ovjere**
 - općeniti model ovjere
 - ovjera dijeljenim tajnim ključem
 - Diffie-Hellmanova razmjena ključa
 - ovjera korištenjem centra za raspodjelu ključeva
 - usluga mrežne ovjere Kerberos

Komunikacijske mreže

8.12.2007

47 od 59

Općeniti model ovjere



- ◆ kontekst obrade: model klijent–poslužitelj
 - klijent Alice: začetnik (inicijator, engl. initiator), započinje sigurnosnu transakciju
 - poslužitelj Bob: odzivnik (engl. responder)
 - centar za raspodjelu ključeva KDC (engl. Key Distribution Center): entitet od povjerenja (engl. trusted KDC), "od kojeg se očekuje da bude pošten" [Tanenbaum] ~ "Big Brother" ☺
- ◆ po završetku izvršavanja protokola ovjere:
 - stranke sigurne u identitetu partnera
 - uspostavljen sigurni tajni sjednički ključ (engl. session key) za nastavak konverzacije ~ razmjenje podataka

Komunikacijske mreže

8.12.2007

48 od 59

Postupkom ovjere ustanavljuje se identitet partnera (najčešće klijenta koji se poslužitelju prijavljuje radi pribavljanja neke obrade). Klijent započinje (inicira) sigurnosnu transakciju, a poslužitelj odgovara na njegove upite. Naravno, inicijator je poznat Alice, dok je odzivnik poznati Bob. Osim njih dvoje, u ovaj okvir ulazi i centar za raspodjelu ključeva, entitet iz porodice Velike Braće ☺.

U razmjeni poruka između Alice i Boba, odnosno Alice i KDC, želi se uplesti zločesta Trudy, i to nizom različitih vrsta napada (primjerice presretanjem poruka, nijihovom izmjenom ili ponavljanjem).

Po uspješnom dovršenju postupka ovjere, stranke su sigurne u identitetu partnera te je uspostavljen sigurni tajni sjednički ključ za nastavak konverzacije, odnosno razmjenje podataka.

Općeniti model ovjere



- ♦ ovjera dijeljenim tajnim ključem, protokoli izazova i odziva: partneri prethodno posjeduju (dijeljeni) ključ
- ♦ ovjera korištenjem centra za raspodjelu ključeva KDC: izbjegći potrebu za poslovanjem ključevima
 - ~ bolje performanse za veći broj različitih partnera

Komunikacijske mreže

8.12.2007

49 od 59

Ovjera dijeljenim tajnim ključem

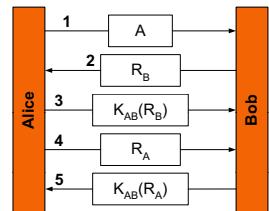


(engl. shared secret key),
protokoli izazova i odziva (engl. challenge-response)

- ♦ partneri prethodno posjeduju (dijeljeni) ključ

- ♦ protokol:

- "izazov" (engl. challenge): neki veliki slučajni broj (engl. nonce)
- generiranje dijeljenog ključa: npr. Diffie-Hellmanova razmjena ključa
- osjetljivost na napad zrcaljenjem (engl. reflection attack)



Komunikacijske mreže

8.12.2007

50 od 59

Ovjera protokolima izazova i odziva zasniva se na razmjeni (velikih) slučajnih brojeva (engl. nonces) koje partner transformira na prethodno dogovoren način, u ovom slučaju prethodno dogovorenim dijeljenim tajnim ključem. Na slajdu je prikazana dvosmerna ovjera. Dijeljeni se ključ može generirati Diffie-Hellmanovom razmjenom (vidi slijedeći slajd).

Napad zrcaljenjem zasniva se na snimanju prometa između Alice i Bob, čime se prikupljuju identitet te nonce i njegova pojava kriptirana dijeljenim ključem. Naknadnim ponavljanjem tih poruka Trudy može zaobići postupak ovjere ako legalni partner prihvata višestruko uspostavljanje sjednica (usp. Tanenbaum: *Computer Networks*, 4th Ed., 2003, 787-790).

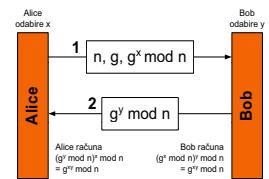
Diffie-Hellmanova razmjena ključa



♦ generiranje dijeljenog ključa (1976), temelji se na nemogućnosti računanja diskretnih logaritama mod veliki prim broj

- ♦ protokol:

- Alice i Bob se trebaju dogovoriti o dva velika broja n i g (mogu biti objavljeni):
 - n i $(n-1)/2$ su prim brojevi
 - vrijede izvjesni uvjeti za g
- tajni ključ je $g^{xy} \text{ mod } n$
- osjetljivost na napad posrednikom (engl. man-in-the middle attack, bucket brigade attack)



Komunikacijske mreže

8.12.2007

51 od 59

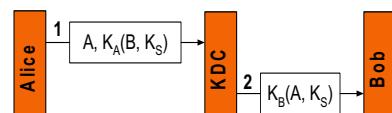
Ukoliko Trudy može prekinuti direktnu komunikaciju Alice i Boba, ona može utjeloviti Boba u komunikaciji s Alice, a Alice u komunikaciji s Bobom. U tom će smislu ona dogovoriti ključ koji dijeli s Alice te onaj koji dijeli s Bobom i tako ne samo pasivno, već i aktivno, moći djelovati na komunikaciju Alice i Boba.

Ovjera korištenjem centra za raspodjelu ključeva



izbjegći potrebu za poslovanjem ključevima:
bolje performanse za veći broj različitih partnera

- KDC i stranke posjeduju prethodno utvrđene tajne ključeve



- napad ponavljanjem
- primjeri protokola:
Needham-Schroederov protokol ovjere;
Otway-Reesov protokol ovjere;
Kerberos

Komunikacijske mreže

8.12.2007

52 od 59

Ovjera korištenjem KDC je efikasn postupak, jer ovjera partnera i poslovanje tajnim ključevima ide putem KDC; prepostavka je da svaki partner ima prethodno utvrđen tajni ključ za komunikaciju s KDC. Na slajdu je prikazana najjednostavnija izvedba protokola koja je osjetljiva na napad ponavljanjem: Trudy prati komunikaciju KDC i Boba te onu između Alice i Boba kriptiranu tajnim ključem K_S , te je naknadno ponavlja (možda i više puta). Očito bi pomogla vremenska informacija o trenutku slanja pojedinih poruka (vremenska markica, engl. time stamp), odnosno razmjena nonceova. I ovim se slučajevima mogu konstruirati situacije kada postupak ne pruža dovoljnu zaštitu od djelovanja uljeza (lokálni satovi Alice i Bob nisu točno sinkronizirani pa se dozvoljava izvjesna tolerancija u protokolu, što Trudy naravno koristi; nonceovi se ne smiju nikad više koristiti, jer marna Trudy može pratiti komunikaciju kroz duži period vremena). Kombinacija vremenske markice i noncea može ograničiti valjanost noncea, uz usložnjavanje protokola.

Rješenje je uvođenje koncepta *ulaznice* (engl. ticket), podataka koje KDC kriptira tajnim ključem odzivnika (Boba), a uključuje identitet inicijatora (Alice) i sjednički ključ za Alice i Boba. Tom ulaznicom se potom Alice identificira kod Boba. U međusobnoj komunikaciji kriptirano sjedničkim ključem, Alice i Bob razmjenjuju nove nonceove (izazovi), koje vraćaju transformirane (pa se tako sprječava napad ponavljanjem). Ovo je gruba skica Needham-Schroederov protokola ovjere čija je varijanta protokol Kerberos.

Usluga mrežne ovjere Kerberos



(engl. Kerberos Network Authentication Service),
J. G. Steiner, B. C. Neuman, J. I. Schiller, MIT, 1988

- mahom ovjera radi sprječavanja lažnih (engl. fraudulent) zahtjeva i odgovora korisnika i poslužitelja
- može se dodati informacija za ovlašćivanje (engl. authorization)
- varijanta Needham-Schroederovog protokola ovjere; bitna je razlika uvođenje *sinkronizacije* satova partnera ("labavo sinkronizirani sat" u radnim stanicama)

Usluga mrežne ovjere Kerberos



- ♦ široka primjena (npr. MS Windows 2000, Qualcomm Eudora):
 - Kerberos, verzija 4:
najčešće korištena u industriji
 - Kerberos, verzija 5:
predloženi standard Interneta, RFC 1510
 - podrška velikom rasponu računala,
od radnih stanica (tipično!) do poslužitelja
- ♦ povjerljivi podaci ili operacije visokog rizika:
potrebna *dodatačna* sigurnosna obrada

Arhitektura sustava Kerberos



- ♦ *klijent*: radna stanica Alice
- ♦ *tri poslužitelja* ~ pas Kerberos iz grčke mitologije:
 - *poslužitelj ovjere KAS* (engl. Kerberos Authentication Server); sličan KDC, ovjerava korisnike prilikom prijave (engl. login):
 - dijeli "privatni" tajni ključ sa *svakim* od korisnika
 - provjerava korisnike prilikom prijave
 - *poslužitelj dodjele ulaznica TGS* (engl. Ticket Granting Server); dodjeljuje *ulaznice* (engl. tickets), kao dokaze identiteta, za željenu uslugu na stvarnom radnom poslužitelju
 - (stvarni) radni (aplikacijski) poslužitelj Bob

Postupak ovjere u sustavu Kerberos



- ♦ (koraci 1 i 2) Alice ↔ KAS:
KAS dodjeljuje Alice tajni sjednički ključ (za sjednicu ovjere) i *ulaznicu* za uslugu TGS
- ♦ (koraci 3 i 4) Alice (s ulaznicom) ↔ TGS (traži ulaznice za Boba):
TGS dodjeljuje Alice ulaznicu i tajni sjednički ključ za sjednicu razmjene podataka
- ♦ (koraci 5 i 6) Alice (s ulaznicom koja je parametrizirana kriptiranom vremenskom markicom) ↔ Bob:
Bob odgovara *svojom* kriptiranom vremenskom markicom
- ♦ ishođena ulaznica za uslugu TGS vrijedi za pristupe na siguran način i *na preostale poslužitelje* u mreži!

Opis aktivnosti po koracima postupka prikazanog u vremenskom dijagramu na sljedećem slajdu.

Postupak ovjere u sustavu Kerberos



K_A : tajni ključ Alice-KAS

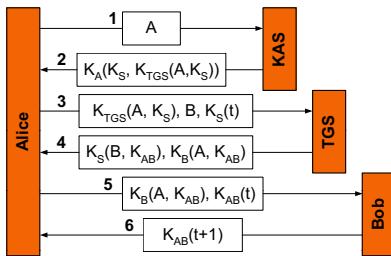
K_S : tajni ključ KAS-TGS

$K_B(A, K_{AB})$: ulaznica za Boba

K_B : tajni ključ TGS-Bob

$K_{TGS}(A, K_S)$: ulaznica za TGS

K_{AB} : zajednički (tajni) ključ Alice i Boba



Komentar koraka u postupku ovjere Kerberos:

1. Alice se identificira (otvorenim tekstom) KASu, radeći na *javnoj* radnoj stanicici;
2. KAS odgovara ulaznicom za TGS $K_{TGS}(A, K_S)$ i sjedničkim ključem za komunikaciju Alice-TGS K_S , sve kriptirano dijeljenim ključem Alice i KAS K_A ;
3. Alice se identificira ulaznicom za TGS i izražava želju za komunikacijom s Bobom; također šalje vremensku markicu t kriptiranu s K_S ;
4. TGS dodjeljuje Alice ulaznicu za Boba $K_B(A, K_{AB})$, također i sjednički ključ K_{AB} , kriptiran s K_S ; Alice može utvrditi da je identifikator Boba ispravno kriptiran; Trudy je sprjećena u ponavljanju poruke, jer je t kriptirana s K_S pa ne može zamjeniti t sa svježijom t'; u svakom slučaju, ako i ponovi poruku s $K_S(t)$, od TGS-a će dobiti poruku 4 što ne može probiti jer ne zna K_S ;
5. Alice se javlja Bobu korištenjem ulaznice $K_B(A, K_{AB})$ te ga izaziva novom vremenskom markicom;
6. Bob modifcira tu vremensku markicu i odgovara na izazov.

Jednom ovjerena kod KAS, Alice se može javiti TGSu radi dodjele ulaznice za neki drugi poslužitelj (npr. poruka 3'). Prema tome, nakon ovjere kod KAS, Alice može pristupiti svim poslužiteljima nekog odsječka mreže čiji je ovjerovatelj upravo KAS.

Postupak ovjere u sustavu Kerberos



- ◆ za korištenje usluge potrebna je *ulaznica*:
 - početna se ulaznica dobiva od KAS; to je ulaznica za TGS
 - ulaznice za sve radne poslužitelje mreže dobivaju se od TGS
- ◆ svakoj ulaznici pridružen je odnosni sjednički ključ
- ◆ poslužitelj održava povijest prethodnih zahtjeva klijenata radi odbacivanje ponovljenih zahtjeva

IPsec

dodatni slajdovi

Načini rada (vrijedi i za AH i za ESP protokol)

izvorni IP datagram



- transportni način: štiti podatke protokola viših slojeva (od transp. na više)

paket zaštićen transportnim načinom



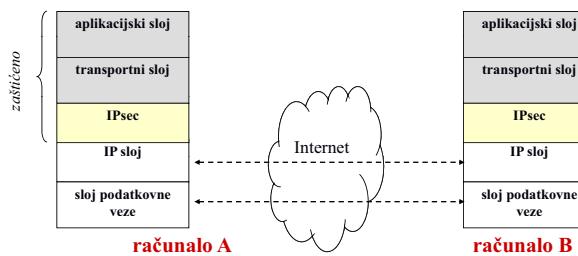
- tunelirani način: primjena SA na tunel; štiti cijeli izvorni IP paket

paket zaštićen tuneliranim načinom



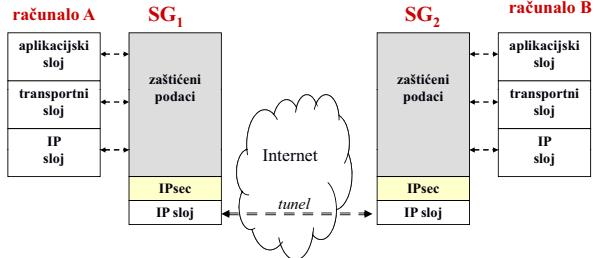
Transportni način, primjer uporabe

- krajnje točke: krajnje računalo – krajnje računalo



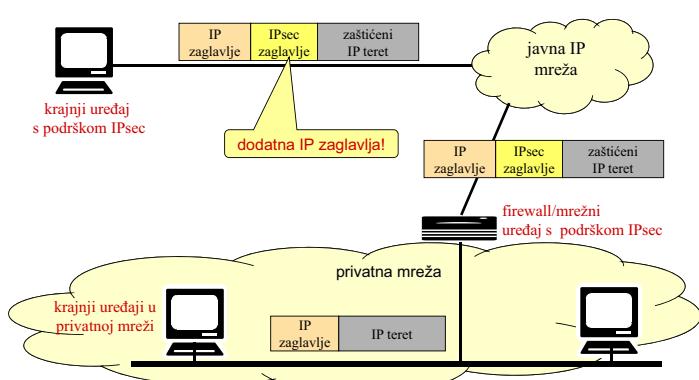
Tunelirani način, primjer uporabe

- krajnje točke: krajnje računalo – mrežni uređaj (A-SG₂) ili između dva mrežna uređaja (SG₁-SG₂)



SG = Security Gateway (sigurnosni prilaz)

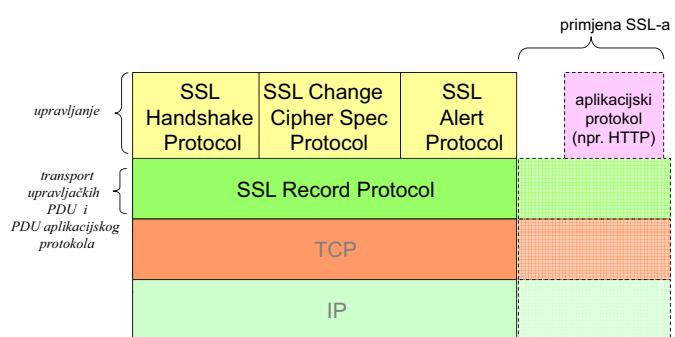
Primjer: Sigurna komunikacija uz IPsec



Secure Socket Layer (SSLv3)

dodatni slajdovi

Arhitektura SSL-a



Protokoli u arhitekturi SSL-a (1/2)

- arhitekturu SSL-a čine četiri protokola
- **SSL Record Protocol**
 - osigurava povjerljivost i cjeleovitost poruke; ovija poruke protokola višeg sloja
 - poruka višeg sloja se fragmentira i komprimira, na nju se dodaje kôd za vjerodostojnost poruke (*Message Authentication Code*), sve se zajedno šifriira i na kraju dodaje SSL Record zaglavljive

SSL Record zaglavlje

šifrirani sadržaj (npr. HTTP poruka)

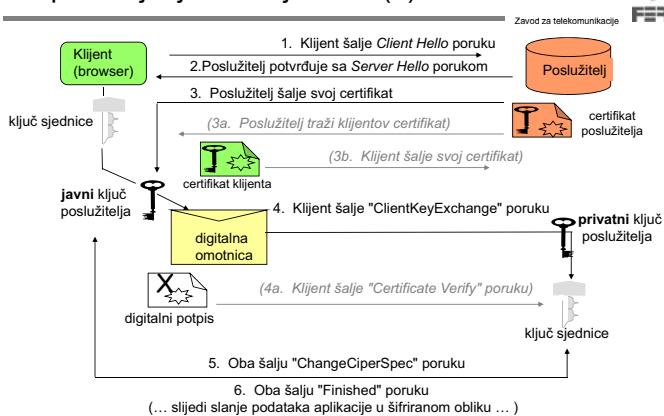
Protokoli u arhitekturi SSL-a (2/2)

- **SSL Change Cipher Spec Protocol**
 - služi za osvježavanja skupa šifri za SSL vezu
- **SSL Alert Protocol**
 - služi za slanje poruka s upozorenjima drugoj strani (indikacija za prekid SSL sjednice ako je sigurnost narušena)
- **SSL Handshake Protocol**
 - služi za uspostavljanje SSL sjednice i dogovor o parametrima sigurne veze

Uspostavljanje SSL sjednice (1)

1. Klijent (preglednik) otvara vezu prema poslužitelju šaljući poruku "ClientHello", koja sadrži klijentovu verziju SSL-a i moguće metode šifriranja i kompresije
2. Poslužitelj odgovara porukom "ServerHello", koja sadrži identifikator sjednice, te odabранe metode šifriranja i kompresije
3. Poslužitelj šalje svoj certifikat klijentu kako bi dokazao svoju vjerodostojnost
4. Klijent šalje poruku "ClientKeyExchange" sa simetričnim klučem, koju šifrija javnim klučem poslužitelja
5. Poslužitelj i klijent šalju poruku "ChangeCipherSpec", koja pokazuje spremnost za početak slanja šifriranih podataka
6. Klijent i poslužitelj šalju "Finished" poruke koje sadrže kriptografsku zaštitnu sumu cijele komunikacije do te točke (dokaz cjeleovitosti) i nakon toga počinje slanje podataka aplikacije

Uspostavljanje SSL sjednice (2)



Secure Electronic Transactions (SET)

dodatajni slajdovi

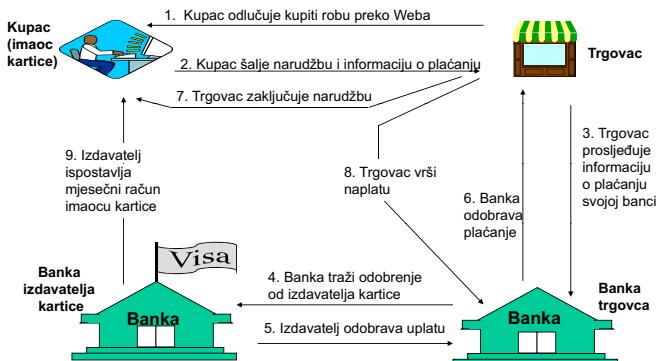
Secure Electronic Transactions (SET)

- Secure Electronic Transactions - SET je otvorena specifikacija za sigurne transakcije korištenjem kreditnih kartica preko javne mreže
- razvili su ga tvrtke Visa i Mastercard
- temelji se na primjeni digitalnog potpisa i certifikata
- šifriranje se vrši na razini poruke, a ne na razini veze; rješenje potpuno neovisno o mreži
- sigurnosne usluge:
 - vjerodostojnost - identitet svih stranaka u transakciji
 - povjерljivost - transakcija je šifrirana, zaštićena od prisluškivanja
 - cjelovitost poruke - ne može se promijeniti broj kartice niti iznos plaćanja
 - dvostruki potpis: povjерljivost prema posrednicima i zaštita od nepoštenih trgovaca preko nepovjerenosti plaćenog primitka iznosa
- slaba primjena u praksi

Funkcionalnost SET-a

- SET protokol osigurava sve funkcije kao u klasičnom kartičnom poslovanju (npr. registraciju vlasnika kartice i trgovca, autorizaciju plaćanja, uplatu, vraćanje novca, kredit i sl.)
 - SET omogućuje interaktivne transakcije i one s naknadnom obradom
-

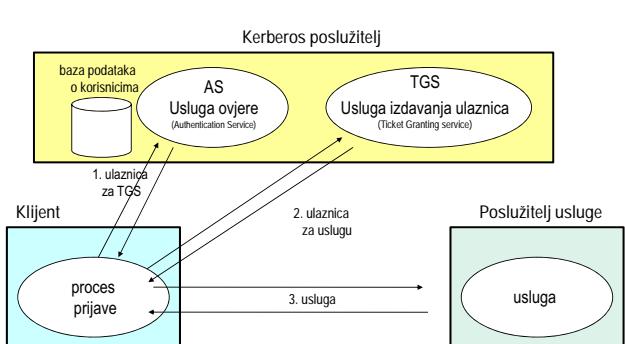
SET - obavljanje transakcije



Kerberos

dodatajni slajdovi

Arhitektura Kerberos sustava



Komunikacijske mreže

11. Javne mreže

Ak.g. 2007./2008.

17.12.2007.

Sadržaj predavanja

- ◆ Model mreže
- ◆ Fiksne (nepokretne) javne mreže
 - Javna telefonska mreža
 - Digitalna mreža integriranih usluga
 - Signalizacija u mreži
- ◆ Javna pokretna mreža
 - Evolucija sustava pokretnih telekomunikacija
 - GSM – Globalni sustav pokretnih komunikacija
 - Komunikacija porukama
 - GPRS, EDGE, UMTS
 - Daljnji razvoj pokretnih mreža
- ◆ Inteligentna mreža

Komunikacijske mreže

17.12.2007.

2 od 56

Javna mreža (engl. public network)

- ◆ Mreža dostupna korisnicima s ugovornim odnosom s mrežnim operatorom (engl. network operator)

Komunikacijske mreže

17.12.2007.

3 od 56

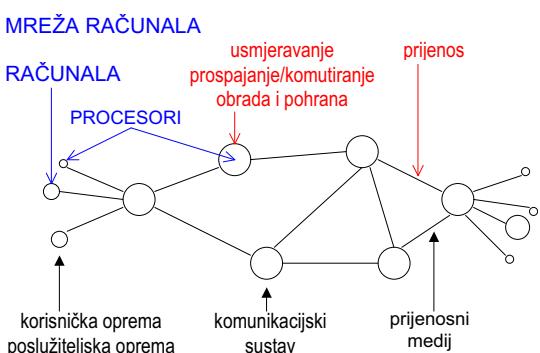
U javnim mrežama pravo na usluge stječe se temeljem ugovornog odnosa s mrežnim operatorom. Preplatniku je omogućeno komuniciranje s preplatnicima i korisnicima vlastite ili drugih mreža te davaljima usluga (engl. *service provider*) u zemlji i inozemstvu, bez vremenskih i prostornih ograničenja. Privatne mreže povezuju se s javnim mrežama, uz ograničenja određena namjenom privatne mreže.

S motrišta vlasništva, javne su mreže u manjinskom, većinskom ili potpunom privatnom vlasništvu, a privatne mreže u državnom (npr. akademska i istraživačka mreža), ili privatnom vlasništvu (npr. bankovna mreža).

Izvedba javnih mreža uključuje, uz Internet, fiksne (nepokretne) mreže:

- javna komutirana telefonska mreža (engl. *Public Switched Telephone Network*, PSTN)
- digitalna mreža integriranih usluga (engl. *Integrated Services Digital Network*, ISDN) te pokretnе mreže:
- globalni sustav pokretnih komunikacija (engl. *Global System for Mobile communications*, GSM), s proširenjima za komunikaciju podacima: opća paketska radijska usluga (engl. *General Packet Radio Service*, GPRS) i poboljšane brzine prijenosa podataka (engl. *Enhanced Data rates for Global Evolution*, EDGE),
- opći pokretni telekomunikacijski sustav (engl. *Universal Mobile Telecommunication System*, UMTS)

Prikaz mreže



Komunikacijske mreže

17.12.2007.

4 od 56

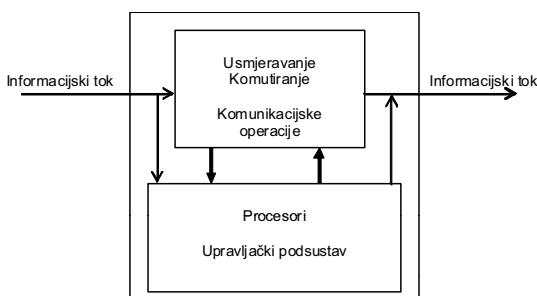
U mreži se razlikuju krajnji čvorovi koji predočuju korisničku i poslužiteljsku opremu te međusobno povezani mrežni čvorovi koji predočuju komunikacijske sustave. Mrežni čvorovi na koje su priključeni ili s kojima su povezani krajnji čvorovi nazivaju se pristupnim čvorovima.

Komunikacijski sustavi provode operacije s informacijskim tokovima u mreži. Oni ih usmjeravaju kroz mrežu (engl. *routing*), prospajaju, odnosno komutiraju (engl. *switching*) sa svojim ulazima na svoje izlaze, po potrebi obrađuju i pohranjuju. Kako poslužuju više ili mnogo korisnika, ovisno o namjeni i veličini mreže, u pravilu su većeg ili velikog kapaciteta, a moraju omogućiti unaprjeđenje postojećih usluga i aplikacija, kao i uvođenje novih. Stoga su komunikacijski sustavi procesorski upravljeni, a njihovi upravljački sustavi sadrže mnoštvo procesora s različitim zadatacama.

Pojam korisnika (engl. *user*) obuhvaća osobe te različite uređaje i sustave priključene na mrežu. „Korisnik“ upotrebljava mrežu za informacijske i komunikacijske usluge i aplikacije. Korisnička oprema koja omogućuje različite informacijske i komunikacijske usluge (npr. pokretni telefon), isto tako sadrži jedan ili nekoliko procesora, a mnoge usluge i aplikacije korisnici izvode izravno sa svog računala.

Sve današnje komunikacijske mreže u svojim krajnjim i mrežnim čvorovima sadrže računala ili procesore, tako da velikih konceptualnih razlika između komunikacijske mreže, ili, u užem smislu mreže računala (engl *computer network*) nema.

Prikaz komunikacijskog sustava



Komunikacijske mreže

17.12.2007.

5 od 56

Informacijski tokovi u mreži



Komunikacijske mreže

17.12.2007.

6 od 56

Komunikacijski sustav sadrži upravljački podsustav koji upravlja operacijama s informacijskim tokovima koje se u sustavu provode, npr. usmjeravanjem paketa ili komutiranjem kanala.

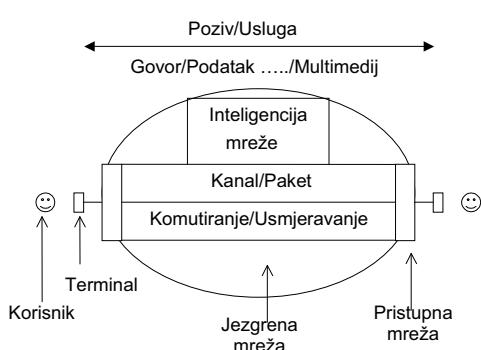
Generiranje, predaja, komutiranje, usmjeravanje, obrada, pohranjivanje, prijenos, prepoznavanje, prijam i drugi postupci s informacijskim tokovima određeni su procesima u terminalima, čvorovima i mreži te komunikacijom među njima. Svim procesima potrebno je upravljati, tako da se korisničkom informacijskom toku pridružuje upravljački informacijski tok koji se često naziva signalizacijom.

Pojam "terminal" odnosi se na krajnji uređaj koji se u različitim mrežama različito naziva, npr. krajnji sustav u Internetu, korisnička oprema u pokretnoj mreži itd.

Različite operacije s informacijskim tokovima nastoje se izvesti ujedinstveno, na zajedničkoj osnovi, što se naziva integracijom postupaka. Preduvjeti za to su digitalni signal kao nositelj informacije te procesorsko i programsko upravljanje kao sustavna potpora svim postupcima.

S obzirom na izvore i odredišta informacije te njene oblike važna je komunikacija govorom, podacima, tekstom, zvukom i slikom te jedinstven pristup informacijskim procesima u terminalu, čvoru i mreži, što opisuje integraciju oblika informacije. Sredstvo za distribuciju i prikaz informacije naziva se medijem. Medij je povezan s čovjekovom percepцијom okoline (sluh, vid, opip, okus, miris). Izravno se na različite načine može predočiti samo zvuk i sliku, a sve ostalo se opisuje podacima.

Model mreže



Komunikacijske mreže

17.12.2007.

7 od 56

Razlikuju se dva dijela mreže – pristupna mreža (Access Network) i jezgrena mreža (Core Network). Pristupna mreža obuhvaća opremu za povezivanje korisničkog terminala na mrežu, tj. pristupni čvor i prijenosni sustav između korisničkog terminala i pristupnog čvora. Jezgrena mreža obuhvaća čvorove koji međusobno povezuju pristupne čvorove te čvorove za povezivanje s drugim mrežama.

Sadržaj predavanja

- ◆ Model mreže
- ◆ Javna fiksna (nepokretna) mreža
 - Javna telefonska mreža
 - Digitalna mreža integriranih usluga
 - Signalizacija u mreži
- ◆ Javna pokretna mreža
 - Evolucija sustava pokretnih telekomunikacija
 - GSM – Globalni sustav pokretnih komunikacija
 - Komunikacija porukama
 - GPRS, EDGE, UMTS
- ◆ Inteligentna mreža

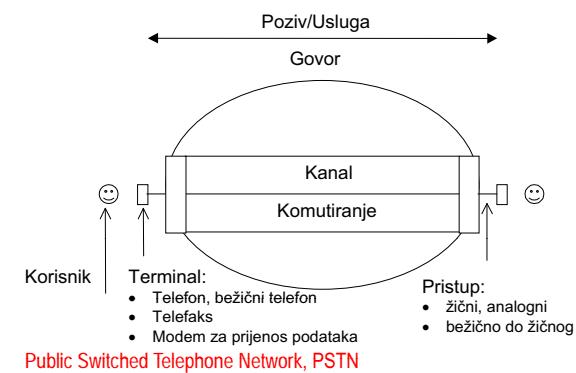
Komunikacijske mreže

17.12.2007.

8 od 56



Javna telefonska mreža



Komunikacijske mreže

17.12.2007.

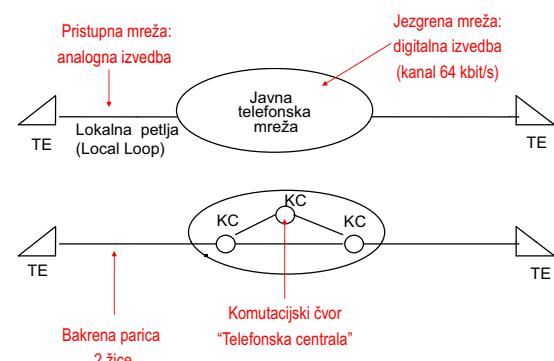
9 od 56

Javna telefonska mreža, punim nazivom javna komutirana telefonska mreža (PSTN - Public Switched Telephone Network) mreža je za govornu komunikaciju. Javna je telefonska mreža najrasprostranjenija globalna fiksna mreža.

Telefonska mreža radi na načelu komutacije kanala tako da se korisnicima, na njihov zahtjev, dodjeljuju kanali i drugi resursi mreže potrebni za ostvarivanje veze. Kad se telefonska mreža rabi za prijenos podataka, to se obavlja u govornom kanalu, primjenom modema.

Korisnički terminal – telefonski aparat pristupa mreži žično, a na zaključenje telefonske linije može se spojiti i bežični telefon (CT – Cordless Telephone).

Organizacija javne telefonske mreže



Komunikacijske mreže

17.12.2007.

10 od 56

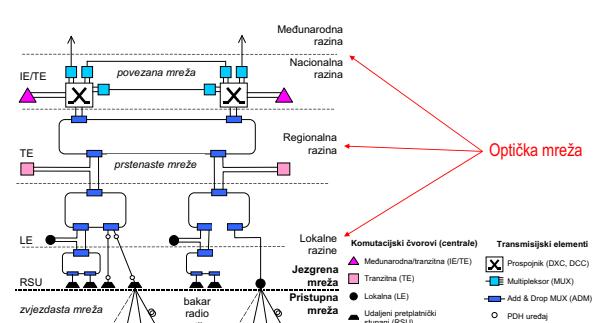
Terminali (TE) putem kojih korisnici ostvaruju svoje komunikacijske zahtjeve su telefoni priključeni su na čvorove mreže, komutacijske centre ili centrale (KC), koji obavljaju funkcije prospajanja-komutiranja i druge funkcije vezane uz pozive i usluge. Komutacijski centri na koje se priključuju telefonski aparati nazivaju se pristupnim ili lokalnim centralama (Local Exchange), a čvorovi koji ih međusobno povezuju tranzitnim centralama (Transit Exchange).

Prikључivanje telefona na lokalnu centralu izvedeno je dvožičnim vodičem – paricom (engl. pair), a taj se dio prijenosnog medija naziva lokalnom petljom (Local Loop) ili korisničkom petljom (Subscriber Loop). To je jedini dio telefonske mreže analognog izvedbe!

Jezgrena mreža je potpuno digitalna, a temelji se na kanalima kapaciteta 64 kbit/s.

Telefonski se aparati za poslovne potrebe neke tvrtke ili institucije mogu povezati na tzv. kućnu centralu (PBX – Private Branch Exchange) koja se spaja na lokalnu centralu. U tom se slučaju interni pozivi obavljaju bez posredovanja javne mreže.

Javna telefonska mreža u Republici Hrvatskoj

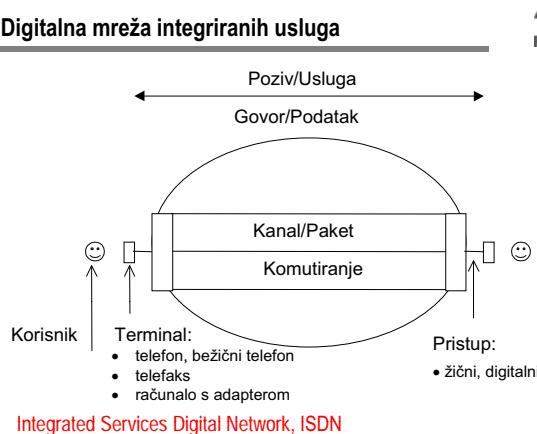


Komunikacijske mreže

17.12.2007.

11 od 56

Digitalna mreža integriranih usluga



Komunikacijske mreže

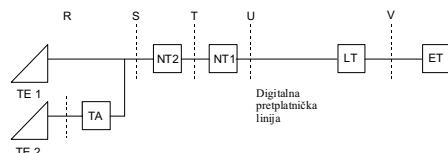
17.12.2007.

12 od 56

ISDN funkcijeske skupine i referentne točke

Funkcijeske skupine:

- terminalska oprema (TE - Terminal Equipment),
- terminalski adapter (TA - Terminal Adapter),
- mrežno zaključenje (NT - Network Termination),
- linjsko zaključenje (LT - Line Termination),
- komutacijsko zaključenje (ET - Exchange Termination).



Komunikacijske mreže

17.12.2007.

13 od 56

Digitalna mreža integriranih usluga sadrži funkcijeske skupine kojima se ostvaruje korisnički pristup, a između kojih su definirane referentne točke. Funkcijeske skupine su sljedeće:

- terminalska oprema (TE - Terminal Equipment),
- terminalski adapter (TA - Terminal Adapter), te
- mrežno zaključenje (NT - Network Termination).
- linjsko zaključenje (LT - Line Termination), te
- komutacijsko zaključenje (ET - Exchange Termination).

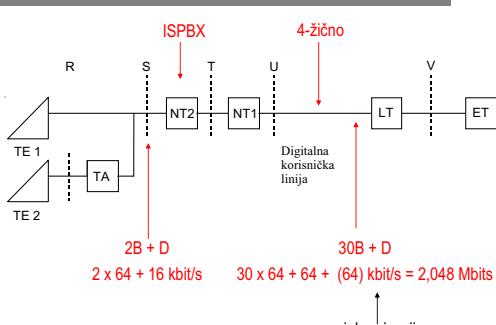
Komutacijsko i linjsko zaključenje se izvode u sastavu pristupnog komutacijskog čvora ISDN mreže.

Terminalska oprema (terminal) može biti u potpunosti prilagođena radu u ISDN mreži i kao takva može se izravno priključiti na mrežno zaključenje (terminal vrste TE1). Terminal koji nije prilagođen radu u ISDN mreži priključuje se posredstvom terminalskog adaptora (terminal vrste TE2).

Mrežno zaključenje povezuje terminalsku opremu na digitalnu preplatničku liniju (DSL – Digital Subscriber Line). Primjenjuje se podjela funkcija mrežnog zaključenja na osnovne (NT1) i složene (NT2). Osnovne funkcije obuhvaćaju fizički sloj i sloj podatkovne poveznice modela OSI. Složene funkcije obuhvaćaju više slojeva modela OSI, a najčešće se izvode kao poslovni komutacijski čvor, tj. integrirana kućna centrala (ISPBX - ISDN Private Branch Exchange).

Referentne točke R (između TE2 i TA), S (između TE1 ili TA i NT), T (između NT2 i NT1), U

Primarni pristup



Komunikacijske mreže

17.12.2007.

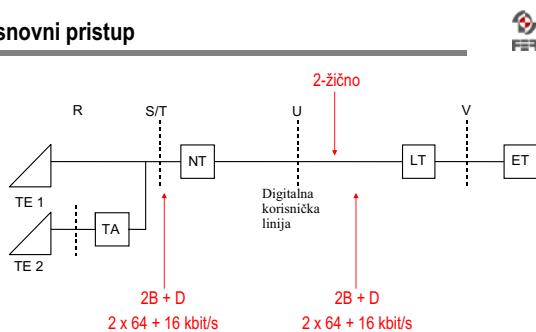
14 od 56

U ISDN-u primjenjuju se dvije vrste kanala, B i D. Informacijski kanal, nazvan B kanal, namijenjen je prijenosu različitih digitaliziranih izvornih oblika korisničke informacije (govor, podatak, slika, itd.). Brzina prijenosa B kanalom iznosi 64 kbit/s. Signalizacijski kanal naziva se D kanalom i osnovna mu je namjena prijenos signalizacijske informacije potrebne za upravljanje pozivom i uslugama na relaciji korisnik - mreža. D kanal može se koristiti i predviđen je, uz signalizaciju, za prijenos podataka komutacijom paketa, izmjenju kratkih poruka između korisnika, te prijenos telemetrijskih podataka niskih brzina (npr. očitanje el. brojila).

Na S točki uvek je na raspolaganju 2B+D kanala odnosno $2 \times 64 + 16 = 144$ kbit/s. Stvarna brzina prijenosa bita je veća, jer su potreben dodatni bitovi za adresiranje i zaštitno kodiranje tako da u S točki iznosi 192 kbit/s.

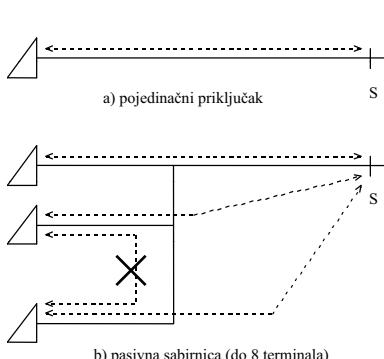
Primarni pristup koji obuhvaća sve funkcijeske skupine namijenjen je većem poslovnom sustavu koji zahtjeva međusobnu komunikaciju korisnika bez izlaza na javnu mrežu, odnosno funkcije kućne centralne. Primarni pristup u točki U raspolaže s 30 informacijskim kanala i jednim signalizacijskim kanalom, što odgovara opisu s 30B+D kanala. Primarni pristup dobio je naziv po primarnom vremenskom multiplexu od 32 kanala po 64 kbit/s, s ukupnom brzinom prijenosa 2,048 Mbit/s na digitalnoj preplatničkoj liniji. 30 kanala su informacijski B kanali, jedan je signalizacijski D kanal, a još jedan služi za sinkronizaciju. Glede fizičkog medija, rabi se četverožični spoj (2 parice), što je uobičajeno rješenje za primarni multipleks.

Osnovni pristup



Basic Rate Access, BRA

Priklučak korisnika



Osnovni pristup namijenjen je kućnom (u stanu) ili manjem poslovnom (u uredu) priključku, tako da funkcije mrežnog zaključenja reducirane na osnovne, pa točke S i T koinkidiraju.

Za takve potrebe osigurava se jedan signalizacijski kanal i dva informacijska kanala (2B+D) u točki U. Kod osnovnog pristupa brzina prijenosa D kanalom na digitalnoj korisničkoj liniji iznosi 16 kbit/s.

Osnovni pristup izvodi se dvožično do mreže, zamjenom opreme na postojećoj dvožičnoj telefonskoj instalaciji!

Signalizacija u mreži

- Da bi se uspostavila, održavala i prekinula veza za potrebe **korisničkog informacijskog toka**, potreban je dodatni, **upravljački informacijski tok** kojim se izmjenjuju informacije o adresama korisnika (pozivni broj), stanju korisnika (slobodan/zauzet, dostupan/nedostupan), dijelovima mreže koji sudjeluju u vezi i sl.
- Upravljačku ili signalizacijsku informaciju većim dijelom stvaraju i rabe sustavi u mreži, a pravila izmjene upravljačke informacije opisana su **signalizacijskim protokolima**.

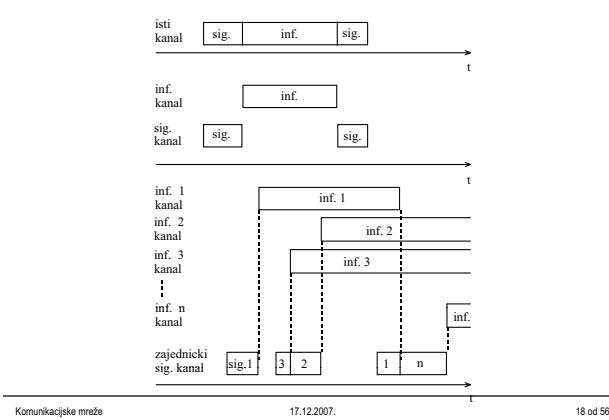
U mreži treba ostvariti komunikaciju između krajnjih čvorova, preko jednog ili više međučvorova. Između korisnika i mreže, odnosno čvora mreže na kojeg je korisnik priključen, te između čvorova u mreži izmjenjuje se upravljačka informacija.

Izmjena upravljačke informacije kojom se ostvaruje usklađeno odvijanje i nadzor procesa poziva i usluga naziva se signalizacijom, a pravila i protokoli izmjene signalizacijske informacije nazivaju se signalizacijskim sustavima.

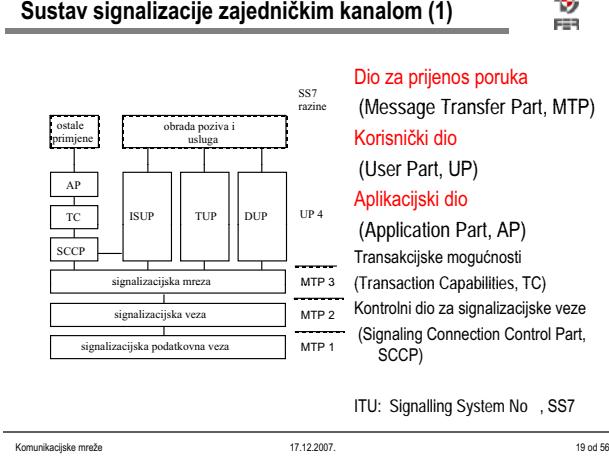
Postoje dvije vrste signalizacijskih sustava:

- signalizacijski sustav na sučelju korisnik-mreža koji služi za izmjenu upravljačke informacije između korisničkog terminala i čvora mreže na kojeg je priključen,
- mrežni signalizacijski sustav koji rješava izmjenu upravljačke informacije između čvorova u mreži.

Prijenos signalizacijske informacije



Sustav signalizacije zajedničkim kanalom (1)



Sustav signalizacije zajedničkim kanalom (2)

Primjer korisničkog dijela (UP):

- Integrirani korisnički dio (Integrated Services User Part, ISUP) za telefonsku i ISDN mrežu

Primjeri aplikacijskih dijelova (AP):

- Pokretni aplikacijski dio (Mobile Application Part, MAP) za pokretnu mrežu
- Inteligentni aplikacijski dio (Intelligent Network Application Part, INAP) za usluge inteligentne mreže

Ova tri dijela se primjenjuju u mrežama u Republici Hrvatskoj.

Tri su načina prijenosa signalizacijske informacije:

- istim kanalom kojim se prenosi korisnička informacija,
- posebnim kanalom, odvojeno od korisničke informacije,
- posebnim kanalom, zajedničkim za skupinu kanala kojima se prenosi korisnička informacija.

Ako se signalizacijska informacija prenosi istim kanalom kojim se prenosi korisnička informacija, tada se kanal koristi u vremenskoj podjeli (npr. upravljačka informacija prenos se prije i nakon korisničke informacije). Takva je situacija kod analognog priključka telefonskog aparata gdje se prvo izmjenjuje upravljačka informacija (podizanje slušalice, znamenke biranja, pozivanje, javljanje), zatim se obavљa govorna komunikacija (korisnička informacija) i na kraju ponovno prenosi upravljačka informacija (spuštanje slušalice, prekidanje veze).

Signalizacija se u digitalnim mrežama prenosi posebnim kanalima, tako da kod digitalnog korisničkog priključka na sučelju korisnik-mreža razlikujemo informacijski kanal i signalizacijski kanal koji se prenose istim fizičkim medijem u vremenskoj podjeli. Npr. u ISDN-u to su B informacijski kanali i D signalizacijski kanal.

Za mrežne signalizacijske sustave najpovoljniji je zajednički signalizacijski kanal. Tada signalizacijski kanal poslužuje u vremenskoj podjeli više ili mnogo korisničkih kanala.

Sustav signalizacije zajedničkim kanalom (CCS - Common Channel Signalling) sadrži tri dijela:

- dio za prijenos poruka (MTP - Message Transfer Part, MTP) kojim se ostvaruje prijenos signalizacijskih poruka,
- korisnički dio (UP – User Part) kojim se rješava upravljačka informacija za pojedinu vrstu poziva usluga na raspolažanju korisnicima.
- aplikacijski dio (AP – Application Part) kojim se rješava upravljačka informacija za posebne primjene.

MTP sadrži tri razine koje odgovaraju nižim slojevima OSI modela.

Razina 1: Signalizacijska podatkovna poveznica (Signalling data link) - odgovara fizičkom sloju OSI modela. Signalizacijski kanal je, kao i svi ostali kanali, digitalan, strukturiran s 8 bita i osigurava brzinu prijenosa 64 kbit/s.

Razina 2: Signalizacijska poveznica (Signalling link) - odgovara sloju podatkovne poveznice OSI modela. Informacijske jedinice koje prenose upravljačku informaciju (npr. birani broj pozvanog korisnika, stanje pozvanog korisnika) između čvorova mreže nazivaju se signalizacijske poruke.

Razina 3: Signalizacijska mreža (Signalling network) - odgovara sloju mreže OSI modela, sadrži funkcije neophodne za povezivanje čvorova u cilju izmjene signalizacijskih poruka, uključujući

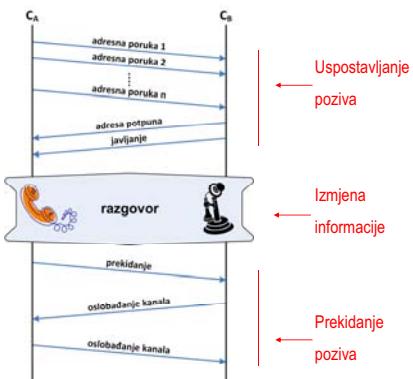
Razlike u vrsti mreže i usluga očituju se u rješenju korisničkog dijela signalizacijskog sustava. Korisnički dio (UP - User Part) na razini 4 ovisi o vrsti mreže i mogućim oblicima informacije.

- Korisnički dio izvodi se samo u čvorovima na koje su priključeni korisnici. Korisnički dio može biti
- integrirani korisnički dio (ISUP - Integrated Services User Part), ako je riječ o signalizaciji za potrebe ISDN i telefonske mreže te komunikaciji govorom i/ili podacima,
 - telefonski korisnički dio (TUP - Telephony User Part), ako je riječ o signalizaciji za potrebe telefonske mreže i komunikaciji govorom,
 - podatkovni korisnički dio (DUP - Data User Part), ako je riječ o signalizaciji za potrebe komunikacije govorom,

Ovi korisnički dijelovi surađuju s funkcijama obrade poziva i usluga. Glede usporedbi s OSI modelom može se reći da korisnički dijelovi odgovaraju sloju primjene, a da su funkcije slojeva transporta, sjednice i prikaza sadržane u sloju primjene, slično kao u internetskom modelu.

U situacijama kad se ne može jednostavno povezati poziv ili usluga sa signalizacijskom informacijom (npr. u inteligentnoj mreži, u pokretnoj mreži) ili poziva uopće nema (npr. ako se prenose podaci o mjerjenjima prometa ili pristupa bazama podataka za potrebe upravljanja mreže), rabe tzv. aplikacijski dijelovi (AP - Application Part) koji trebaju potporu za transakcije tipa upit-odgovor (TC - Transaction Capability) i dodatnu kontrolu signalizacijskih veza (SCCP - Signalling Connection Control Part).

Primjer: izmjena signalizacijskih poruka



Komunikacijske mreže

17.12.2007.

21 od 56

Poziv:

Generički pojam koji se odnosi na uspostavljanje, održavanje i prekidanje veze između pozivajuće i pozvane stranke (korisnika) u cilju izmjene informacije. Poziv predočuje združivanje dva ili više korisnika ili korisnika i mreže koje se ostvaruje uporabom mrežnih mogućnosti.

Usluga:

Ono što nudi mreža svojim korisnicima za ispunjenje posebnih komunikacijskih zahtjeva.

Sadržaj predavanja



- ◆ Model mreže
- ◆ Fiksne (nepokretne) javne mreže
 - Javna telefonska mreža
 - Digitalna mreža integriranih usluga
 - Signalizacija u mreži
- ◆ Javna pokretna mreža
 - Evolucija sustava pokretnih telekomunikacija
 - GSM – Globalni sustav pokretnih komunikacija
 - Komunikacija porukama
 - GPRS, EDGE, UMTS
 - Daljnji razvoj pokretnih mreža
- ◆ Inteligentna mreža

Komunikacijske mreže

17.12.2007.

22 od 56

Telekomunikacije u pokretu



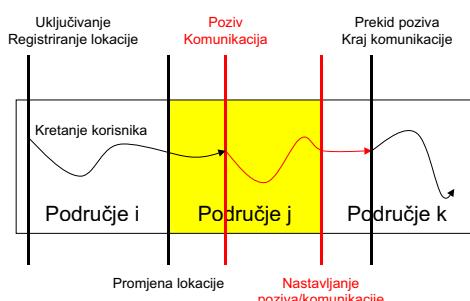
Cilj

- ◆ komunikacija govorom, podacima i s više medija za stacionarne i pokretnе korisnike bez vremenskih i prostornih ograničenja uporabom jedne adrese - pozivnog broja

Prepostavke

- ◆ pokretnjivost terminala, osoba i usluga

Model pokretnjivosti



Komunikacijske mreže

17.12.2007.

24 od 56

Korisnik se kreće sa svojim terminalom i pritom prolazi različita područja. Područja mogu biti određena prostorno ili zemljopisno (npr. pokrivanje radijskim signalom) te administrativno (npr. Internet domena).

Prigodom uključivanja terminala treba registrirati njegovu lokaciju i početi pratiti kretanje (područje i). Kad korisnik priđe granicu između dva područja treba ustanoviti promjenu lokacije (područje j). U nekom trenutku pokreće se poziv i ostvari komunikacija, a korisnik nastavlja kretanje. Pri prijelazu u novo područje treba nastaviti poziv odnosno komunikaciju (područje k). Obično se kretanje prati preciznije tijekom komunikacije nego dok je terminal samo uključen. Po završetku komunikacije terminal ostaje uključen te se nastavlja s praćenjem kretanja. Registriranje lokacije uključenog terminala olakšava uspostavljanje poziva, jer time područje u koje treba uputiti poziv postaje poznato unaprijed.

Komunikacija u pokretu zahtjeva funkcije upravljanja pokretnjivošću. One iziskuju dodatnu upravljačku informaciju (signalizaciju) između terminala i mreže koja se izmjenjuje i kad terminal nije aktivran. Podsetimo da se u fiksnoj mreži signalizacija izmjenjuje samo tijekom poziva.

Pokretna mreža



Mobile Network

- ♦ **Javna mreža** u kojoj se pristup zasniva na **radijskoj komunikaciji** koja omogućuje pokretljivost korisničke opreme – terminala na području pokrivanja radijskim signalom
- ♦ **Jezgrena mreža**
 - Izvodi se kao fiksna mreža
- ♦ **Pristupna mreža**
 - Radijska pristupna mreža temeljena na sustavu ćelija

Komunikacijske mreže

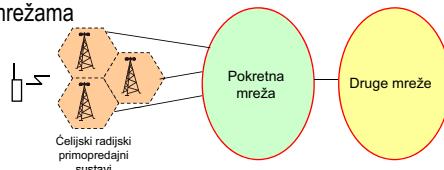
17.12.2007.

25 od 56

Opća arhitektura pokretnе mreže



- ♦ **Ćelijski radijski primopredajni sustav**
 - Ćelijom (engl. cell) se naziva područje pokriveno jednim radijskim primopredajnim sustavom
- ♦ **Čvorovi za povezivanje unutar pokretnе mreže i s drugim mrežama**



Komunikacijske mreže

17.12.2007.

26 od 56

Prva generacija - NMT



- ♦ Generacije sustava
 - U svim generacijama **višestruki pristup** – više korisnika pristupa skupini komunikacijskih kanala
- ♦ **Prva generacija 1G**
 - Analogni sustavi
 - Višestruki pristup u **frekvencijskoj** podjeli (Frequency Division Multiple Access FDMA)
 - posebne frekvencije svakom komunikacijskom kanalu
 - različiti frekvencijski pojasevi dodjeljuju za komunikaciju od mreže prema terminalu (down link) i komunikaciju od terminala prema mreži (up link).
 - Sustav NMT (Nordic Mobile Telephony)
 - RH: Mobitel 099 (1987.g.) – 98,000 pretplatnika 1998.g., nije više u uporabi

Komunikacijske mreže

17.12.2007.

27 od 56

Višestruki pristup u frekvencijskoj podjeli ostvaruje se dodjelom posebne frekvencije svakom komunikacijskom kanalu. Obično se različiti frekvencijski pojasevi dodjeljuju za komunikaciju od mreže prema terminalu (down link) i komunikaciju od terminala prema mreži (up link).

Druga generacija - GSM



- ♦ **Druga generacija 2G**
 - Digitalni sustavi
 - Višestruki pristup u **vremenskoj** podjeli (Time Division Multiple Access TDMA), 124 frekvencije x 8 kanala = 992 kanala
 - GSM (Global System for Mobile communications), GSM-900/DCS-1800 (Digital Communication System)
 - **Prijenos govora dominantan**
 - **Komutacija kanala**
 - 2,5G – GPRS, EDGE
 - podaci
 - **GPRS:** $14,4 \times 8 = 115,2 \text{ kbit/s}$
 - **EDGE:** $48 \times 8 = 384 \text{ kbit/s}$

Komunikacijske mreže

17.12.2007.

28 od 56

Višestruki pristup u vremenskoj podjeli omogućuje da se na svakoj prijenosnoj frekvenciji izvede više kanala u vremenskoj podjeli, tako da ukupan broj kanala odgovara umnošku broja frekvencija i broja vremenskih kanala.

Treća generacija - UMTS

♦ Treća generacija 3G

- Međunarodne pokretne telekomunikacije 2000 (International Mobile Telecommunications IMT-2000)
- Europa: Opći pokretni telekomunikacijski sustav (Universal Mobile Telecommunications System, UMTS)
- Širokopojasni višestruki pristup u kodnoj podjeli (ideband Code Division Multiple Access, WCDMA)

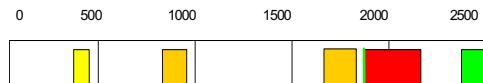
Komunikacijske mreže

17.12.2007.

29 od 56



Frekvencijski spektar



♦ Ograničeni resurs – ograničeni broj mreža!

♦ Kontrolirana dodjela i naplata (licence, koncesije)

♦ Slobodna uporaba:

1880-1900 MHz: bežični telefon (DECT – Digital Enhanced Cordless Telecommunications)

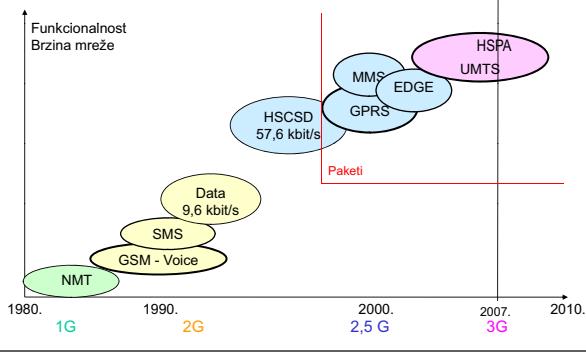
2400-2500 MHz: ad-hoc komunikacija, WLAN (ISM – Industrial Scientific Medical)

Komunikacijske mreže

17.12.2007.

30 od 56

Evolucija mreže



Komunikacijske mreže

17.12.2007.

31 od 56



GSM

Globalni sustav pokretnih komunikacija
(Global System for Mobile communication)

Ćelijska struktura (Cellular)

♦ optimum: pokrivenost/iskoristivost frekvencija

Višestruki pristup u vremenskoj podjeli

♦ TDMA (Time Division Multiple Access)

♦ 124 frekvencije x 8 kanala = 992 kanala

Prometni i kontrolni kanali

♦ odvajanje korisničke i upravljačke informacije (signalizacije)

Komunikacijske mreže

17.12.2007.

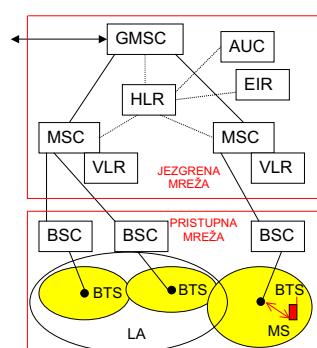
32 od 56

GSM mreža pokriva područje radijskim signalom na ćelijskom načelu. Ćelijom se naziva područje koje pokriva jedan radijski primopredajni sustav. Ćelijska struktura omoguće dobru iskoristivost raspoloživih frekvencija, jer se u susjednim ćelijama rabe različite, a u udaljenim ćelijama iste frekvencije.

GSM je digitalni sustav u kojem se višestruki pristup ostvaruje u vremenskoj podjeli tako da se na svakoj od 128 frekvencija raspoloživo 8 kanala, ukupno 992.

Korisnička informacija prenosi se prometnim kanalima, a upravljačka informacija posebnim kontrolnim kanalima.

Arhitektura mreže GSM



Komunikacijske mreže

17.12.2007.

33 od 56

GSM mreža sadrži prilazni pokretni komutacijski centar, GMSC, preko kojeg se povezuje s drugim mrežama i preko kojeg se pristupa GSM mreži te pokretnе komutacijske centre, MSC. Oni povezuju GMSC i sustave baznih postaja, BSS. BSS se sastoji od dva dijela, kontrolnog, BSC i primopredajnog, BTS. Jedan BSC upravlja s više BTS-ova koji sadrže antenski sustav. Područje pokrivanja radijskim signalom jednog BTS-a naziva se ćelija. Skup ćelija koje pripadaju jednom MSC-u naziva se lokacijsko područje (LA- Location Area).

Korisnički terminal (npr. pokretni telefon) naziva se općenito pokretnom postajom, MS. Domaći lokacijski registar, HLR, sadrži sve podatke o domaćim (vlastitim) preplatnicima i uslugama koje koriste te o njihovoj trenutnoj lokaciji, ukoliko je poznata.

Gostujući lokacijski registar (lokacijski registar posjetitelja), VLR, sadrži podatke o preplatnicima koji su trenutno u lokacijskom području dotičnog MSC-a. Podatke o trenutnoj lokaciji preplatnika VLR dojavljuje HLR-u njegove domaće mreže.

Centar za provjeru autentičnosti, AUC, sadrži autentifikacijski ključ s kojim se provjerava preplatnik pri svakom pozivu.

Registrar identifikacije opreme, EIR, sadrži podatke o MS-u s kojima se može provjeriti da li je u vlasništvu preplatnika.

Prigodom zasnivanja preplatničkog odnosa u HLR se zapisuju međunarodna identifikacija pokretnog preplatnika, IMSI, pozivni broj pokretnе postaje, MSISDN, autentifikacijski ključ, Ki te popis usluga i mogućnosti kojim raspolaže preplatnik (uslužni profil). U MS se stavlja modul preplatničkog identiteta, SIM, koji sadrži IMSI i Ki. MS je zaštićen osobnim identifikacijskim brojem, PIN, kojim se uključuje. Odblokiranje SIM-a nakon tri pogrešna unosa PIN-a provodi se s ključem za odblokiranje (PUK - PIN Unblocking Key).

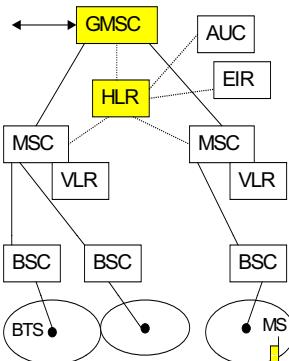
Serijski broj MS upisuje se u EIR kako bi se mogla provesti provjera identiteta opreme. EIR je opcionalna mogućnost GSM-a.

IMSI je identifikacijski broj koji jednoznačno određuje GSM mrežu i preplatnika, a kojeg se koristi za sustavske operacije u mreži i između različitih GSM mreža.

MSISDN je preplatnikov pozivni broj (npr. 091 xxx xx xx ili 098 xx xx xx).

Ki je jednoznačni autentifikacijski ključ zapisan u MS i HLR koji omogućuje provjeru preplatnika prije početka poziva. Ukoliko se ključevi ne podudaraju, poziv se odbacuje

Preplata



U HLR:

- MSISDN (Mobile Station ISDN) - pozivni broj
- IMSI (International Mobile Subscriber Identification)
- Ki (Authentication Key) - autentifikacijski ključ
- popis dopuštenih usluga

U MS:

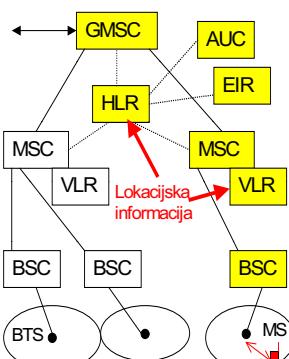
- SIM (Subscriber Identity Module) s IMSI i Ki
- zaštita s PIN (Personal Identification Number)

Komunikacijske mreže

17.12.2007.

34 od 56

Uključivanje, registracija i pozivanje



Uključivanje/isključivanje (Attachment/Deattachment)

- prati se stanje MS

Registracija (Registration)

- nakon uključivanja MS, periodički, kod promjene lokacije
- provjera autentičnosti (AUC) i identiteta opreme (EIR)
- lokacijska informacija u VLR i HLR

Pozivanje (Paging)

- traženje MS

Komunikacijske mreže

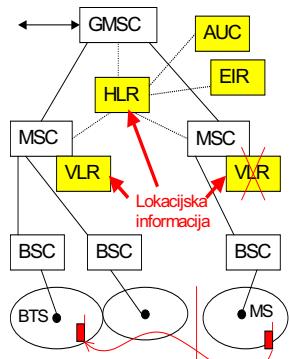
17.12.2007.

35 od 56

Mreža nadzire uključivanje i isključivanje MS. Nakon uključivanja, MS se otkriva u ćeliji u kojoj se trenutno nalazi, provjerava se autentičnost i identitet opreme te u VLR-u registrira lokacijska informacija. Nakon toga VLR obavještava domaći HLR o lokaciji preplatnika. Tako se mreža unaprijed priprema za pozive, jer će znati odakle može krenuti odlazni poziv, odnosno kamo treba usmjeriti dolazni poziv. Registracija se obnavlja periodički te kod promjene lokacije. Mreža može tražiti MS tako da ga pozove i čeka odziv.

Izključivanjem MS gubi se lokacijska informacija i MS prestaje biti dostupan.

Lociranje, prebacivanje poziva i prelaženje



Lociranje

- utvrđivanje potrebe za prebacivanjem uključene MS u drugu ćeliju (signal/šum)
- promjena lokacijske informacije kad se mijenja LA

Prebacivanje poziva (Call Handover)

- nastavljavanje poziva pri promjeni kanala/ćelije

Prelazanje (Roaming)

- komunikacija u drugim mrežama (ne samo vlastitoj)

Komunikacijske mreže

17.12.2007.

36 od 56

Lociranjem se naziva postupak kojim se uključeni MS prebacuje iz jedne ćelije u drugu. Kriterij je kvaliteta signala, tj. odnos signal/šum. Ukoliko je neko područje pokriveno s više GSM mreža, MS će odabratи onu s najboljom kvalitetom signala. Stoga je tehničko rješenje sustava baznih postaja važno za "privlačenje" gostujućih pretplatnika.

Svaki započeti poziv mora se nastaviti pri promjeni kanala, odnosno ćelije.

MS može ostvariti komunikaciju u vlastitoj (domaćoj) mreži i u drugim mrežama s kojima je operator domaće mreže sklopio ugovor o kretanju.

Upravljanje pokretljivošću



Domaći lokacijski registar

(HLR - Home Location Register)

- ◆ Trajni zapis pretplatničkih podataka vlastitih pretplatnika
- ◆ Trenutna lokacija vlastitih pretplatnika

Posjetiteljski lokacijski registar

(VLR - Visitor Location Register)

- ◆ Privremeni zapis dijela pretplatničkih podataka vlastitih i tuđih pretplatnika koji su trenutno u lokacijskom području
- ◆ Tuđi pretplatnici se poslužuju temeljem ugovora o prelaženju između mreža

Komunikacijske mreže

17.12.2007.

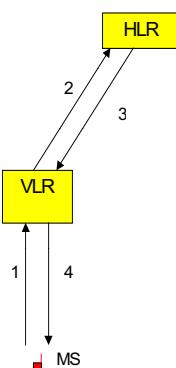
37 od 56

Registracija u vlastitoj mreži



Signalizacija:

- 1 - zahtjev za registracijom
- 2 - registracijska poruka
- 3 - pretplatnički podaci
- 4 - uspješna registracija



Komunikacijske mreže

17.12.2007.

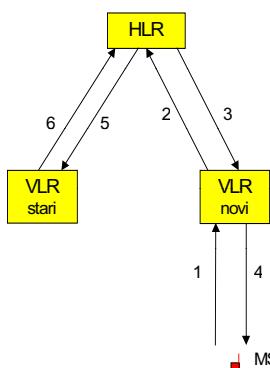
38 od 63

Promjena lokacije u vlastitoj mreži



Signalizacija (nepoznat stari VLR):

- 1 - zahtjev za registracijom
- 2 - registracijska poruka
- 3 - pretplatnički podaci
- 4 - uspješna registracija
- 5 - deregistracijska poruka
- 6 - potvrda deregistracije

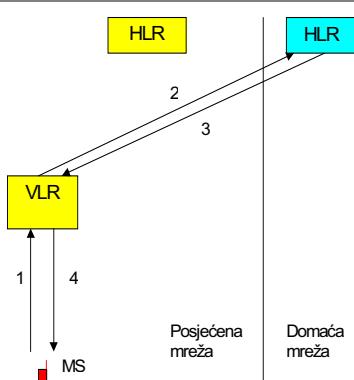


Komunikacijske mreže

17.12.2007.

39 od 63

Registracija u posjećenoj mreži



Komunikacijske mreže

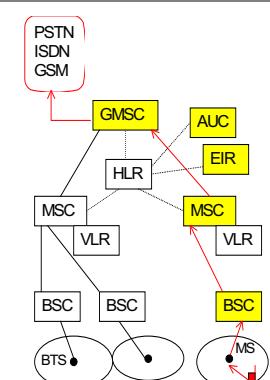
17.12.2007.

40 od 56

Odlazni poziv



- ◆ MS traži kanal
- ◆ provjera autentičnosti (AUC) i identiteta opreme (EIR)
- ◆ propajanje poziva BTS - BSC - MSC - GMSC - druga mreža
- ◆ kriptografska zaštita tijekom prijenosa

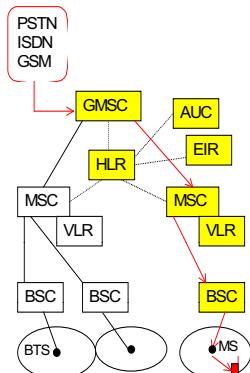


Komunikacijske mreže

17.12.2007.

41 od 56

Dolazni poziv



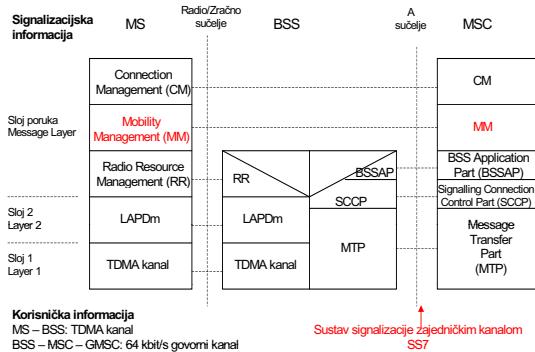
- GMSC od HLR traži lokacijsku informaciju (LA) za MS
- HLR - VLR izmjenjuju podatke o pozvanom MS
- MSC prenosi svim BSC (BTS) u LA zahtjev za pozivanjem MS
- provjera autentičnosti (AUC) i identiteta opreme (EIR)
- prospajanje, kriptografska zaštita tijekom prijenosa

Komunikacijske mreže

17.12.2007.

42 od 56

GSM – komunikacijski protokoli



Komunikacijske mreže

17.12.2007.

43 od 56

GSM protokoli viših slojeva

- podsloj za upravljanje radijskim resursima (RR - Radio Resource Management Sublayer): uspostavljanje fizičke veze preko radio kanala za prijenos signalizacije između MS i BSS
 - podsloj upravljanja pokretljivošću (MM - Mobility Management Sublayer): uspostavljanje, održavanje i prekidanje veze, uključivanje, lociranje, isključivanje između MS i MSC
 - podsloj upravljanja vezom (CM - Connection Management Sublayer): dodatne usluge i SMS između MS i MSC
 - BSS aplikacijski dio (BSSAP - BSS Application Part): aplikacijski dio u sustavu signalizacije br. 7 za GSM
 - kontrolni dio za signalizacijsku vezu (SCCP - Signaling Connection Control Part) i dio za prijenos poruka (MTP - Message Transfer Part): standardni dio sustava signalizacije br. 7
- BSS procesi**
- BSS Management Application Process (BSSMAP): procedure između BSS i MSC koje zahtijevaju interpretaciju/obradu informacija vezanih uz poziv te upravljanje radio resursima
 - Direct Transfer Application Process (DTAP): transparentni prijenos informacija između MS i MSC za upravljanje pokretljivošću i vezom

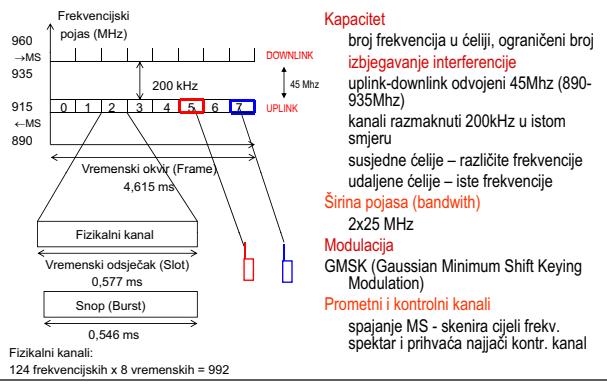
Fizički kanali u GSM mreži ostvaruju se vremenskom podjelom kojom se formira okvir (frame) s osam vremenskih kanala na svakoj od 124 dodijeljenih frekvencija koje su međusobno razmaknute za 200 kHz.

Fizički kanal odgovara jednom odsječku (slot) trajanja 0,577 ms kojim se prenosi snop bita (burst) trajanja 0,546 ms. Snop sadrži 114 kriptiranih (sigurnosno zaštićenih) korisnih bita i 48 dodatnih bita. Fizički kanali služe za prijenos korisničke informacije.

Govor se prenosi digitalno, s kodiranjem govornih blokova kojim se postiže brzina prijenosa 13 kbit/s. Rabi se modulacijski postupak GMSK (Gaussian Minimum Shift Keying).

Uz fizičke kanale formiraju se i logički kanali, tako da se stvaraju multi okviri od 26 ili 51 okvira. Logički kanali služe za prijenos kontrolne informacije.

GSM - fizički kanal



Komunikacijske mreže

17.12.2007.

44 od 56

Komunikacija porukama

SMS (Short Message Service)

- Usluga kratkih poruka (do 160 znakova)

EMS (Enhanced Messaging Service)

- Obogaćena usluga izmjene poruka (točkaste slike, kratke melodije)

MMS (Multi Media Messaging)

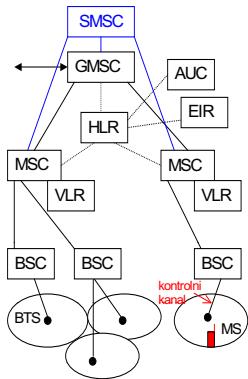
- Izmjena višemedijskih poruka (bogati sadržaj)

Komunikacijske mreže

17.12.2007.

45 od 56

Usluga kratkih poruka



SMS (i EMS)

- Poruke se prenose kontrolnim kanalom u pristupnoj mreži
- Poruke prihvata, pohranjuje i proslijeđuje SMSC (SMS Centre)

Komunikacijske mreže

17.12.2007.

46 od 56

Uz govor se GSM mrežom mogu prenositi podaci u govornom kanalu brzinom do 9,6 kbit/s, a uz učinkovitije kodiranje do 14,4 kbit/s. Rješenje je ekvivalentno onome u telefonskoj mreži.

Osim toga može se komunicirati kratkim porukama (SMS) kojima rukuje posebni centar, SMSC, usmjeravajući ih od izvođenog prema određenom MS. Pojedini GSM sustavi raspolažu rješenjima za ulančavanje poruka kojima se više kratkih poruka ograničenih na 160 znakova stapaaju u jednu dulju.

Kratke poruke se prenose kanalom SDDCH (Stand Alone Dedicated Control Channel) koji je namijenjen za signalizaciju i kratke poruke.

GPRS



Opće paketske radijske usluge (General Packet Radio Services)

Obilježja

- paketizirani podaci u mreži GSM
- pristup IP zasnovanim mrežama - Internetu
- brzina prijenosa ovisna kodiranju podataka, tj. o kodnoj shemi (npr. 14,4 kbit/s) i broju kanala za komunikaciju paketima (1-8, tipično 2-4)
- Između 2. i 3. generacije – **2,5 G**

Komunikacijske mreže

17.12.2007.

47 od 56

Pojavom pokretnog Interneta potrebno je omogućiti pristup i rad u Internetu preko pokretnog telefona i drugih pokretnih terminala. Kako se u tom slučaju radi o komunikaciji podacima preko bežičnog pristupa, odnosno o usnopljenom prometu, potrebno je omogućiti prijenos podataka komutacijom paketa. GPRS upravo omogućava komutaciju paketa unutar postojeće GSM arhitekture, dakle radi se o proširenju GSM arhitekture sa sljedećim značajkama za operatera:

- bolje karakteristike prilikom bežičnog prijenosa podataka,
- korak bliže trećoj generaciji usluga,
- brzo i jednostavno dodavanje čvorova koji omogućavaju komutaciju paketa u postojeću GSM infrastrukturu,
- bolja iskoristivost kanala u odnosu na prijenos podataka komutacijom kanala.

Sa gledišta krajnjeg korisnika GPRS omogućava:

- povezanost s Internetom ili Intranetom preko pokretnog terminala (pokretni Internet ili Intranet),
- stalnu vezu s IP,
- povećanje brzine komuniciranja do 115 kbit/s,
- brzi pristup mreži,
- naplata prema primljenom/poslanom volumenu podataka, a ne prema trajanju komunikacije.

EDGE



Poboljšane brzine prijenosa podataka (Enhanced Data Rates for Global Evolution)

Obilježja

- paketizirani podaci u GSM/GPRS mreži
- pristup IP zasnovanim mrežama - Internetu
- veće brzine prijenosa (384 kbit/s)
- Između 2. i 3. generacije – **2,5 G**

Komunikacijske mreže

17.12.2007.

48 od 56

UMTS



Opći pokretni telekomunikacijski sustav (Universal Mobile Telecommunications System)

Obilježja

- do 144 kbit/s u svim uvjetima, do 384 kbit/s na otvorenom prostoru, do 2 Mbit/s u zatvorenom prostoru
- kanali i paketi, više istodobnih usluga

Komunikacijske mreže

17.12.2007.

49 od 56

Brzine prijenosa i zone pokrivanja:

- do 144 kbit/s: udaljeni krajevi, slaba naseljenost, velika brzina kretanja (do 1000 km/h) - Svjetska ćelija,
- 144 - 384 kbit/s: prigradska područja, srednja naseljenost, brzina kretanja 120-500 km/h - Makro ćelija,
- 384 - 2048 kbit/s: gradsko područje, velika naseljenost, brzina kretanja do 120 km/h - Mikro ćelija,
- 2048 kbit/s: zatvoreni prostor, veoma velika gustoća korisnika, mirovanje ili hodanje - Piko ćelija.

Usluge:

- od uskopojasnih (govor) do širokopojasnih (multimedij u stvarnom vremenu),
- brza komutacija paketa (pretraživanje WWW, isporuka informacija, udaljeni i bežični pristup Internetu/Intranetu),
- unificirano rukovanje porukama (e-mail, ...),
- pokretna trgovina,
- pokretni ured.

Daljnji razvoj pokretnih mreža (1)



Brzi paketski pristup

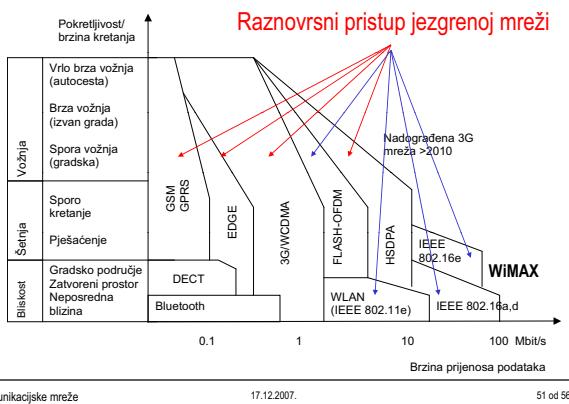
(HSPA – High Speed Packet Access)

- ♦ Brzi paketski pristup silazno (HSDPA – High Speed Downlink Packet Access)
 - Teorijski 14,4 Mbit/s, očekivano 3,6 Mbit/s, praktički 1,8 Mbit/s
 - Uvođenje započelo 2006.
- ♦ Brzi paketski pristup uzlazno (HSUPA – High Speed Uplink Packet Access)
 - Uvođenje započinje u 2007.

Daljnji razvoj pokretnih mreža (2)



Raznovrsni pristup jezgrenoj mreži



Sadržaj predavanja



- ♦ Model mreže
- ♦ Fiksne (nepokretnе) javne mreže
 - Javna telefonska mreža
 - Digitalna mreža integriranih usluga
 - Signalizacija u mreži
- ♦ Javna pokretna mreža
 - Evolucija sustava pokretnih telekomunikacija
 - GSM – Globalni sustav pokretnih komunikacija
 - Komunikacija porukama
 - GPRS, EDGE, UMTS
 - Daljnji razvoj pokretnih mreža
- ♦ Inteligentna mreža

Inteligentna mreža



Intelligent Network, IN

Prepoznavanje i posluživanje informacijskih i komunikacijskih zahtjeva na način koji korisnika odvaja od poznavanja mreže i usluga.

"Inteligencija" mreže:

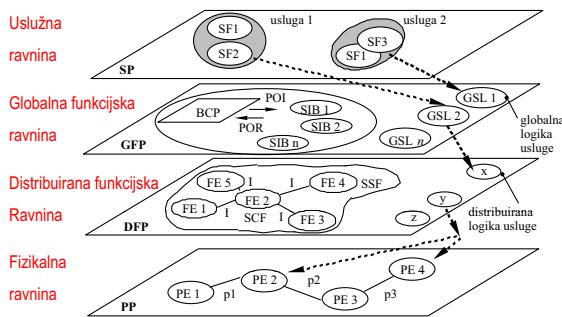
- ♦ više "znanja" o korisnicima i njihovim zahtjevima te
- ♦ više "znanja" o trenutnim mogućnostima mreže i davaljela usluga.

Primjena koncepta intelligentne mreže u svim mrežama:

- ♦ PSTN, ISDN, pokretna mreža,

Koncepcionalni model sastoji se od četiri ravnine (plane) od kojih svaka predstavlja drukčiji "pogled" na inteligentnu mrežu.

Koncepciji model inteligentne mreže



Komunikacijske mreže

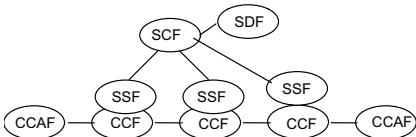
17.12.2007.

54 od 56

Funkcijalni entiteti



- upravljanje pristupom pozivu (CCAF - Call Control Access Function) - pristup korisniku i interakcija s mrežom,
- upravljanje pozivom (CCF - Call Control Function) - obrada poziva
- komutiranje usluga (SSF - Service Switching Function) - proširenje poziva uslugama
- upravljanje usluga (SCF - Service Control Function) - usklajivanje poziva sa zahtjevima za uslugama, uz uključivanje dodatnih funkcijalnih entiteta za ostvarenje usluge
- podaci o usluga (SDF - Service Data Function)

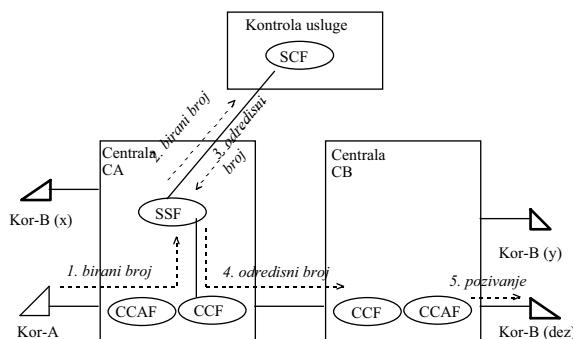


Komunikacijske mreže

17.12.2007.

55 od 56

Primjer usluge: besplatni poziv (Freephone)



Komunikacijske mreže

17.12.2007.

56 od 56

Ravnina usluga (SP - Service Plane) određuje pogled isključivo sa strane usluga, bez informacija o načinu izvedbe usluge u mreži, na način kako uslugu vidi korisnik. Svaka usluga (S - Service) sastoji se od jedne ili više odlike usluge (SF - Service Feature).

Globalna funkcijalna ravnina (GFP - Global Functional Plane) opisuje cijelu inteligentnu mrežu kao jedan entitet. U njoj su sadržani osnovna obrada poziva (BCP - Basic Call Processing) i blokovi neovisni o usluzi (SIB - Service Independent Building Block). Osnovna obrada poziva je također blok neovisan o uslugama koji se povezuje s ostalima preko točaka započinjanja (POI - Point Of Initiation) i točaka povratka (POR - Point Of Return) u poziv.

U globalnoj funkcijalnoj ravnini dodjeljuje se svakom dijelu usluge globalna logika usluge (GSL - Global Service Logic), jedna ili više njih. GSL opisuje koji su blokovi neovisni o uslugama uključeni u zadanu uslugu, kako su međusobno povezani i na koje su točke započinjanja i vraćanja povezani.

Distribuirana funkcijalna ravnina (DFP - Distributed Functional Plane) opisuje distribuiranu strukturu inteligentne mreže. U njoj funkcijalni entiteti (FE - Function Entity) izvode različite akcije. Blok neovisan o usluzi se izvodi slijedom odabralih akcija u funkcijalnim entitetima pri čemu se po potrebi izmjenjuju informacije između entiteta.

U distribuiranoj funkcijalnoj ravnini svaki GSL prikazuje se jednom ili više distribuiranih logika usluge (DSL - Distributed Service Logic). DSL su programi koji se pridružuju se funkcijalnim entitetima, a sadrže funkcije upravljanja uslugama.

Fizikalna ravnina (PP - Physical Plane) modelira fizikalnu strukturu inteligentne mreže. Sadrži fizikalne entitete (PE - Physical Entity) i protokole za njihovo povezivanje. Svaki funkcijalni entitet se izvodi u nekom fizikalnom entitetu (npr. terminal, komutacijski čvor, usmjeritelj).

Programi logike usluga se u fizikalnoj ravnini dodjeljuju i izvode na fizikalnim entitetima koji sadrže funkcijalne entitete s funkcijama upravljanja uslugama.

Ključni problem su funkcije tako da će se detaljnije obraditi samo funkcijalni entiteti. Funkcijalnim entitetom smatra se skupina funkcija na jednoj lokaciji potrebnih za izvedbu usluge. Dva funkcijalna entiteta komuniciraju informacijskim tokom. Za izvedbu usluga definirani su sljedeći osnovni entiteti:

- funkcijalni entitet za upravljanje pristupom pozivu (CCAF - Call Control Access Function) koji omogućuje pristup korisniku i njegovu interakciju s mrežom
- funkcijalni entitet za upravljanje pozivom (CCF - Call Control Function) koji ostvaruje obradu poziva i vezu
- funkcijalni entitet za komutiranje usluga (SSF - Service Switching Function) koji proširuje pozive uslugama
- funkcijalni entitet za upravljanje usluga (SCF - Service Control Function) koji uskladjuje upravljanje pozivom sa zahtjevima za uslugama, a pritom može uključivati i dodatne funkcijalne entitete potrebne za ostvarenje usluge
- funkcijalni entitet za podatke o usluga (SDF - Service Data Function) koji osigurava podatke potrebne za izvedbu usluge i

Za stvaranje usluga, njihovo uvođenje u mrežu i operativno vođenje potrebni su i drugi entiteti.

Usluga je zamišljena tako da pozivajući korisnik ne snosi troškove, nego pozvani korisnik koji je ujedno davatelj usluge. Njegov je poslovni interes da omogući takvu komunikaciju (npr. nabavka zrakoplovnih karata) te nastoji poslužiti čim više takvih poziva i obaviti čim više poslova. Drugo što je važno za tu uslugu jest pozivanje davaljatelja usluge jedinstvenim brojem, a svaki poziv će se usmjeriti prema njegovoj poslovničkoj koja je npr. trenutno najmanje opterećena.

Pozivajući korisnik Kor-A bira broj usluge, a kako to više nije pozivni broj odredišta, funkcijalni entiteti koji se bave "običnim" pozivom (CCAF i CCF) u njegovoj centrali CA će proslijediti poziv funkciji komutiranja usluge (SSF) koja će ga usmjeriti funkciji kontrole usluge (SCF) kako bi se provelo prevođenje biranog broja u odredišni broj na kojem će poziv završiti. SCF će pritom primijeniti dogovorenopravilo odabira odredišta (npr. navečer samo dežurnoj poslovnicu) i odrediti odredišni broj Kor-B(dez).

Odredišni pozivni broj će se vratiti u centralu i funkcije kontrole poziva nastaviti poziv prema dobivenoj odredišnoj adresi Kor B(dez). Očevidno je da je upravljanje uslugom složenije s motrišta mreže, a za korisnika jednostavnije. U ovom primjeru poziv nije završio na bližem odredištu Kor-B nego na odredištu koje ga može poslužiti. Troškovi poziva teretit će davaljatelja usluge, a ne pozivajućeg korisnika.

U intelligentnoj mreži se javlja veći tok signalizacijske informacije i drugi način rukovanja s njom. Tipične su transakcijske operacije zasnovane na konceptu upit-odgovor, što se rješava u sustavu signalizacije zajedničkim kanalom s aplikacijskim dijelom INAP.

Komunikacijske mreže

12.
Pristup Internetu

Ak.g. 2007./2008.

7.1.2008.

Sadržaj predavanja

- ◆ Uvod
- ◆ Korisnici Interneta i davaljci internetske usluge
- ◆ Modeli pristupa i rješenja
 - Protokol PPP
 - Pretvorba mrežnih adresa
- ◆ Fiksni pristup Internetu
 - telefonska mreža, ISDN
 - širokopojasni pristup: ADSL, kabelska televizija
- ◆ Pokretni pristup Internetu
 - GSM, GPRS, EDGE
 - UMTS, HSPA

Komunikacijske mreže

7.1.2008.

2 od 45

Uvod (1)

Pristup Internetu (engl. Internet Access):

- ◆ spajanje krajnjeg sustava (engl. End System), npr. računala kojim se izvode usluge i aplikacije (engl. host) ili drugog uređaja, na Internet

Ostvarivanje pristupa Internetu:

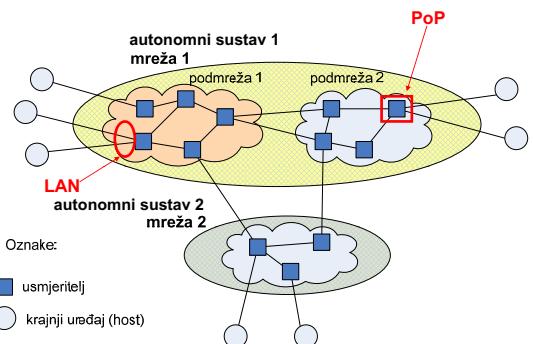
- ◆ lokalnom mrežom koja je dio/podmreža autonomnog sustava Interneta ili
- ◆ povezivanjem do točke u autonomnom sustavu putem koje se spaja na Internet – točka prisutnosti IP-a (engl. IP Point of Presence, IP PoP ili kraće PoP)

Komunikacijske mreže

7.1.2008.

3 od 45

Uvod (2)



Komunikacijske mreže

7.1.2008.

4 od 45

Korisnici Interneta

Mali korisnici

- kućni (domaćinstva) i manji poslovni, s nekoliko računala,
- manje brzine prijenosa, nema potrebe za stalnim pristupom, asimetrični promet (odlazni << dolazni),
- nema potrebe za stalnom IP adresom.

Srednji korisnici

- poslovni, s lokalnom mrežom, do nekoliko desetaka računala,
- veće brzine prijenosa, stalni pristup,
- uglavnom nema potrebe za stalnom IP adresom.

Veliki korisnici

- poslovni, s lokalnom mrežom/mrežama, mnogo računala,
- velike brzine prijenosa u oba smjera,
- stalna IP adresa, obično više IP adresa.

Komunikacijske mreže

7.1.2008.

5 od 45

Pristup Internetu uključuje tri skupine sudionika:

- krajnji korisnike,
- davaljci usluga (engl. Service Provider) i
- davaljci usluge pristupa Internetu (engl. Internet Access Provider).

Krajnji korisnici osim usluge pristupa Internetu, uglavnom traže i telefoniju, a sve više i televiziju. Davatelji usluga kao osnovnu uslugu nude internetsku uslugu (engl. Internet Service Provider, ISP) uz korištenje raznih sadržaja (npr. web, e-pošta, glazba, video, pričanice i sl.), a mogu pružati i druge usluge, kao npr. pristup bazama podataka, ili uslugu virtualne privatne mreže. Davatelji usluge povezivanja, kao što sam naziv kaže, vrše povezivanje krajnjih korisnika s davaljima usluga. ISP je u pravilu i davaljci usluge pristupa Internetu.

Najvažnija obilježja usluge pristupa Internetu su trajanje veze i kvaliteta. S motrišta trajanja veze razlikujemo korisnike kojima je potreban stalni pristup Internetu i one koji se priključuju povremeno, odn. putem veze po pozivu ("dial-up"). Oni prvi su najčešće poslovni korisnici, dok su oni drugi najčešće kućni korisnici. Kvaliteta pristupa najčešće se opisuje parametrima brzine prijenosa i rasploživosti.

Davatelj internetske usluge (1)



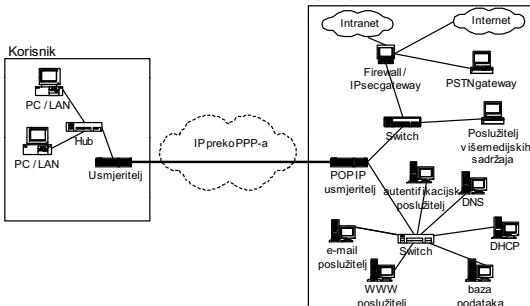
ISP (Internet Service Provider):

- ♦ usluga pristupa Internetu i druge internetske usluge:
 - elektronička pošta,
 - web portal,
 - udomljavanje web sadržaja (engl. web hosting),
 - datotečni poslužitelj,
 - registracija domene i drugo.
- ♦ točka pristupa Internetu: točka prisutnosti (Pop)
 - izvedeno, PoP je usmjeritelj na kojem se korisnici spajaju, putem kojeg pristupaju poslužiteljima ISP-a i povezuju se drugim korisnicima istog ISP-a ili korisnicima drugih mreža

Onima koje posebno zanima Internet s motrišta odnosa tehnologije i tržišta preporuča se knjiga:

A: Bažant, Ž. Car, G. Gledec, D. Jevtić, G. Ježić, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, Z. Skočir : Telekomunikacije – tehnologija i tržište, Element, Zagreb, 2007.

Davatelj internetske usluge (2)



Modeli pristupa (1)



Izravni pristup Internetu putem lokalne mreže (podmreža autonomnog sustava)

Usluge i aplikacije
TCP, UDP
IP
LLC
MAC
Fizikalni sloj

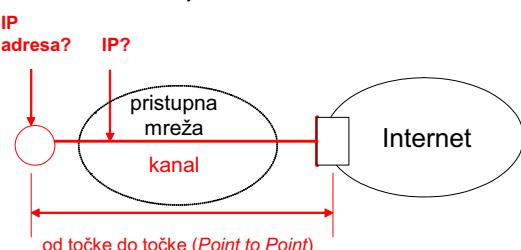
- ♦ krajnji sustav komunicira paketski s drugim krajnjim sustavima i usmjeriteljem kojim se povezuje s drugim mrežama
- ♦ IP datagram se prenosi u polju podataka okvira podatkovne poveznice, npr. Ethernetskog okvira

Modeli pristupa (2)



Pristup Internetu kanalom kroz drugu mrežu:

- ♦ od točke na kojoj je krajnji sustav do točke putem koje se spaja na Internet
- ♦ problem: dovesti IP i dodijeliti IP adresu



Protokol PPP (1)



PPP

(Point to Point Protocol)

Usluge i aplikacije
TCP, UDP
IP
PPP
Fizikalni sloj

- ♦ prijenos paketa kanalom od točke na kojoj je krajnji sustav do točke u autonomnom sustavu kojom se ostvaruje pristup Internetu
- ♦ IP datagram se prenosi u polju podataka okvira protokola PPP
- ♦ fizikalni sloj: kanal u pristupnoj mreži

Point-to-Point Protocol (PPP) je standardni internetski protokol za transport datagrama različitih mrežnih protokola preko veze od točke do točke. Specifikacija PPP-a je STD-51 koji uključuje RFC 1661 i RFC 1662, a u RFC 2153 (Vendor Extensions) se opisuje opći mehanizam za proširenja od strane proizvođača.

PPP kao podloga za IP omogućuje primjenu različitih mreža i prijenosnih medija za pristup Internet. Nadalje, PPP je otvoren i prema i IPv6.

Protokol PPP (2)

- ◆ protokol sloja podatkovne poveznice kojim se ostvaruje prijenos paketa dvostravnim kanalom
- ◆ bit-orientirani protokol
- ◆ izveden iz protokola HDLC (High-level Data Link Control):
 - struktura okvira
 - kodiranje adresnog i kontrolnog polja
- ◆ dodatna funkcionalnost:
 - dinamička dodjela IP adresa
 - ovjera (utvrđivanje autentičnosti)

Format PPP okvira se temelji na ISO High Level Data Link Control (HDLC) protokolu, kako je opisano u RFC 1662, "PPP in HDLC-like Framing".

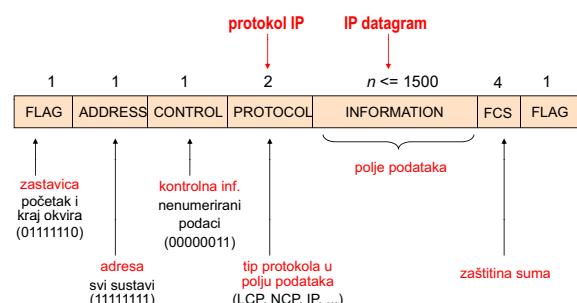
Komunikacijske mreže

7.1.2008.

11 od 45



Format PPP okvira



Komunikacijske mreže

7.1.2008.

12 od 45



Zastavica – 01111110

označava početak i kraj okvira

može se koristiti jedna zastavica za kraj jednog i početak sljedećeg okvira)

Adresa – 11111111

uvijek ima istu vrijednost jer ne treba adresirati kod komunikacije od točke do točke
11111111 u protokolu HDLC označava sve sustave na poveznici

Kontrolno polje – 00000011

uvijek ima istu vrijednost

00000011 u protokolu HDLC označava nenumerirane podatke (ne označava se slijed
jedinica podataka potreban za kontrolu toka i pogrešaka)

Protokol

označava protokol mrežnog sloja koji se smješta (enkapsulira) u PPP okvir

0021 znači da sadrži IP datagram

C021 znači da sadrži LCP

8021 znači da sadrži NCP

Podaci – varijabilna duljina, maksimalno 1500 okteta

FCS – zaštutna suma okvira (Frame Check Sequence)

računa se za sva polja, osim zastavica i samog FCS-a

Komponente protokola PPP

Protokol za kontrolu poveznice

(engl. Link Control Protocol, LCP)

- ◆ konfiguriranje, uspostavljanje, ispitivanje i raskidanje podatkovne poveznice

Mrežni kontrolni protokol

(engl. Network Control Protocol, NCP)

- ◆ neovisno konfiguriranje i uspostavljanje pojedinih protokola mrežnog sloja
- ◆ više NCP-ova, posebni NCP za svaki mrežni protokol
- ◆ IPCP (IP Control Protocol)

Komunikacijske mreže

7.1.2008.

13 od 45



Danas je aktualan širokopojasni pristup (engl. Broadband Access), odnosno pristup Internetu većim brzinama prijenosa podataka.

Pojam "širokopojasnost" različito se tretira u pojedinim izvorima, posebice onima koji se bave statističkim pokazateljima razvijenosti mreža i usluga.

Tako npr. Europska unija pod tim pojmom razumijeva 144 kbit/s što se postiže već ISDN-om.

Rigidnja tehnička definicija ITU govori o 2,048 Mbit/s, odnosno brzini prijenosa primarnog vremenskog multipleksa (32 x 64 kbit/s).

S uporabnog motrišta, širokopojasnim se može smatrati nekoliko stotina kbit/s (npr. kao kod ADSL-a).



Dodjela IP adrese (1)

Javna IP adresa:

- ♦ jedinstvena adresa unutar globalnog internetskog adresnog prostora
- ♦ ograničenja adresnog prostora IPv4 onemogućuju dobivanje jedinstvene adrese za sve potrebe

Privatna IP adresa:

- ♦ adresa unutar privatnog adresnog prostora
- ♦ ne omogućuje adresiranje i usmjeravanje u Internetu

Prevođenje mrežnih adresa javna ↔ privatna:

NAT (Network Address Translation)

Dodjela IP adrese (2)



Statička dodjela javne IP adrese

- ♦ stalna IP adresa
- ♦ dodjeljuje sustavima za koje treba omogućiti globalni pristup (mrežni sustavi, poslužiteljski sustavi) i ovisno o raspoloživom adresnom prostoru korisničkim krajnjim sustavima

Dinamička dodjela javne IP adrese

- ♦ privremena IP adresa
- ♦ dodjeljuje se korisnicima na zahtjev, prigodom pristupanja Internetu

Prevođenje IP adresa (1)



m:n prevođenje

- ♦ m privatnih prevodi se u n javnih adresa:
 - svakom od m pretplatnika ISP-a dodjeljuje se jedna od raspoloživih javnih IP adresa ($m < n$)
 - svakom od m pretplatnika operatora pokretnе mreže dodjeljuje se jedna od raspoloživih javnih IP adresa za pristup Internetu ($m < n$)
- ♦ način prevođenja:
 - statički: privatnoj adresi dodjeljuje se uvijek ista javna adresa
 - dinamički: privatnoj adresi dodjeljuje se svaki put neka druga javna adresa (primjenjuju ISP i operator pokretnе mreže)

Prevođenje IP adresa (2)



m:1 prevođenje

- ♦ m (najčešće) privatnih pretvara se u jednu javnu adresu:
 - svakom od m korisnika privatne mreže dodjeljuje se ista javna IP adresa
 - svi sustavi u privatnoj mreži pristupaju Internetu preko jedne IP adrese (sigurnost: maskiranje interne strukture mreže otežava neovlaštene upade)
- ♦ istodobne izlazne veze postižu se uporabom različitih vrata (portova) namijenjenih za NAT
- ♦ postupak u NAT-u:
 - izvođačna IP adresa zamjenjuje se javnom IP adresom
 - izvođačna vrata zamjenjuju se NAT vratima

Pristup Internetu iz telefonske mreže (1)



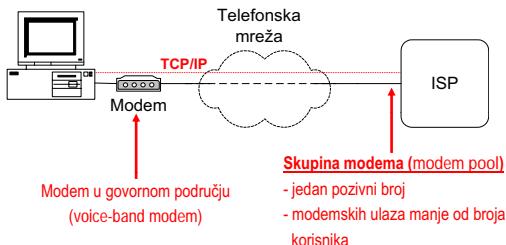
Koristi se javna komutirana telefonska mreža:

- ♦ analogni prijenos pretplatničkom petljom (engl. Subscriber line, SL),
- ♦ prijenos podataka u govornom kanalu, primjena modema (modulator demodulator) na koji se priključuje računalo
- ♦ komunikacija u frekvencijskom pojasu 0 - 4kHz,
- ♦ maksimalna brzina prijenosa 56 kbit/s,
- ♦ nemogućnost istovremenog prijenosa govora i podataka,
- ♦ pristup Internetu vezom ostvarenom pozivom, odnosno "biranjem" ("dial-up")

Pristup Internetu iz telefonske mreže (2)

Postupak:

1. modem poziva broj davnatelja internetske usluge (ISP)
2. PPP uspostavlja vezu (do 56 kbit/s)
3. računalu se dinamički dodjeljuje privremena IP adresa



Komunikacijske mreže

7.1.2008.

23 od 45

Pristup računalu na Internetu preko veze po pozivu ("dial-up").

Takva veza uspostavlja se na zahtjev korisnika, i koristi privremenu, telefonsku ili ISDN vezu. Korisnikovo računalo ponaša kao da je izravno spojeno na Internet, odr. mogu se koristiti sve usluge i aplikacije. S korisnikovog gledišta, osim po pitanju brzine, nema razlike u odnosu na računalo na LAN-u, trajno povezano

Postupak pristupanja Internetu započinje na zahtjev korisnika, tj. pokretanjem programa za uspostavu veze s davnateljem internetske usluge. Računalo preko modema ili ISDN adaptera naziva odgovarajući pozivni broj. Nakon odziva na strani davnatelja internetske usluge i uspostave telefonske ili ISDN veze, program protokola sloja podatkovne poveznice (PPP) uspostavlja podatkovnu poveznicu. Računalu se dinamički dodjeljuje privremena IP adresa, nakon čega TCP/IP programska potpora omogućuje sve internetske usluge i aplikacije.

Pristup Internetu ISDN-om (1)

Osnovni pristup (2B + D):

- ◆ digitalni prijenos digitalnom preplatničkom linijom (engl. Digital Subscriber line, DSL),
- ◆ prijenos podataka u B kanalu, priključak računala na terminalski adapter (engl. Terminal Adapter, TA), obično izveden u sklopu mrežnog zaključenja (engl. Network Termination, NT)
- ◆ maksimalna brzina prijenosa 128 kbit/s (2B)
- ◆ mogućnost istovremenog prijenosa govora i podataka, svakog u svojem B kanalu
- ◆ pristup Internetu vezom ostvarenom pozivom ("dial-up")

Komunikacijske mreže

7.1.2008.

24 od 45

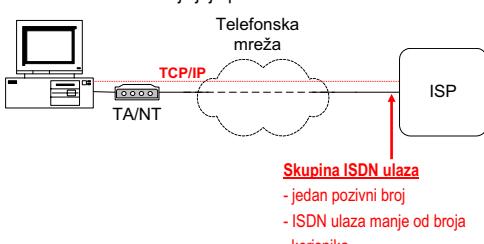
Pristup računalu na Internetu preko veze po pozivu ("dial-up").

Takva veza uspostavlja se na zahtjev korisnika, i koristi privremenu, telefonsku ili ISDN vezu. Koncepcijski nema razlike između telefonske mreže i ISDN-a!

Pristup Internetu ISDN-om (2)

Postupak:

1. računalo poziva broj davnatelja internetske usluge (ISP)
2. PPP uspostavlja vezu (do 128 kbit/s)
3. računalu se dinamički dodjeljuje privremena IP adresa



Komunikacijske mreže

7.1.2008.

25 od 45

Koncepcijski nema razlike između pristupa putem telefonske mreže i ISDN-a!

Asimetrična digitalna preplatnička linija



ADSL (Asynchronous Digital Subscriber Line):

- ◆ izvodi se paricom u pristupnom dijelu telefonske mreže
- ◆ asimetrični prijenos:
 - dolazni smjer – veća maksimalna brzina (8 Mbit/s, do 3 km)
 - odlazni smjer – manja maksimalna brzina (640 kbit/s, do 3 km)
 - osjetljiv na kvalitetu izvedbe i duljinu parice, te broj parica u kabelu s digitalnim prijenosom
- ◆ mogućnost istovremenog prijenosa govora i podataka
- ◆ stalna povezanost (nije potrebno uspostavljati vezu pozivom)
- ◆ **ADSL2 (12 Mbit/s, 1 Mbit/s), do 1,5 km**
- ◆ **ADSL2+ (x Mbit/s, 1 Mbit/s), do 1,5 km**

Komunikacijske mreže

7.1.2008.

26 od 45

U Republici Hrvatskoj su lokalne petlje pretežno do 1,5 km duljine, tako da se uz osnovni ADSL mogu primjenjivati i naprednije inačice, ADSL2 i ADSL2+.

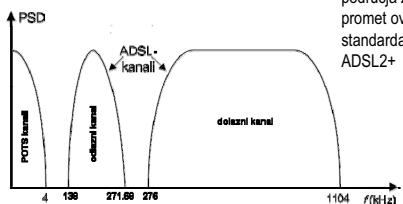
ADSL – frekvenčijski spektar



Tri frekvenčska područja za ADSL:

- 0 - 4 kHz – analogni telefonija
138 – 271.68 kHz – odlazni promet
276 kHz – 1104 kHz – dolazni promet

Napomena: Frekvenčska područja za odlazni i dolazni promet ovisna su o inačici standarda (ADSL, ADSL2, ADSL2+)



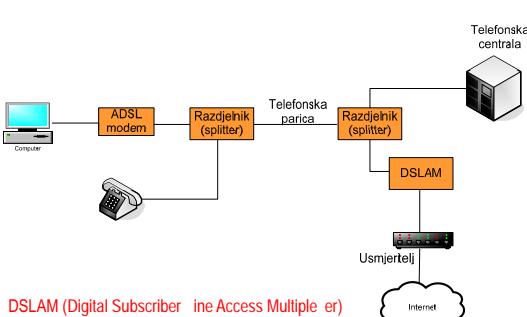
Komunikacijske mreže

7.1.2008.

27 od 45

POTS (Plain Ordinary Telephony Service) – Naziv za "uobičajenu" uslugu telefonske mreže.

Arhitektura ADSL-a



DSLM (Digital Subscriber Line Access Multiple er)
multiplesira veći broj ADSL veza na brzu vezu
prema Internetu

Komunikacijske mreže

7.1.2008.

28 od 45

Kabelski pristup Internetu



Koristi se infrastruktura kabelske televizije:

- ◆ izvodi se koaksijalnim kabelom ("kabelski modem")
- ◆ asimetrični prijenos:
 - dolazni smjer – veća maksimalna brzina (do 30 Mbit/s)
 - odlazni smjer – manja maksimalna brzina (manje od 1 Mbit/s)
- ◆ topologija sabirnice:
 - problem dijeljenog medija: brzina ovisi o broju korisnika
 - problem sigurnosti podataka
- ◆ mogućnost istovremenog prijenosa TV programa, podataka i govora
- ◆ stalna povezanost (nije potrebno uspostavljati vezu pozivom)

Komunikacijske mreže

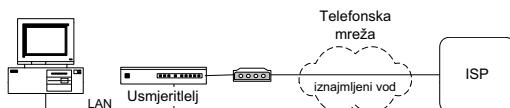
7.1.2008.

29 od 45

Iznajmljeni vod

Zakup voda od mrežnog operatora:

- ◆ stalni pristup Internetu za velike korisnike (poduzeća, ustanove, davaljili usluga)
- ◆ moguć odabir brzine prijenosa
- ◆ cijena ovisna o brzini prijenosa (bit/s) i udaljenosti (km)
- ◆ stalna povezanost (nije potrebno uspostavljati vezu pozivom)



Komunikacijske mreže

7.1.2008.

30 od 45

Povezivanje na Internet je putem trajne IP veze.

Takva veza najbolje je, ali i najskuplje rješenje. Trajna IP veza ostvaruje se preko iznajmljenog voda veće ili velike brzine, npr. 2 Mbit/s, i 34 Mbit/s i više. Na strani korisnika najčešće se nalazi lokalna mreža, a dodatna oprema uključuje usmjeritelj i drugu mrežnu opremu.

Postavljanje i konfiguracija mrežne opreme na korisnikovoj lokaciji, kao i stalno održavanje, relativno je složeno i traži stručnost, znanje i vrijeme. Zbog toga, kao i zbog visoke cijene, za takvo se rješenje uglavnom odlučuju poslovni korisnici.

Ostale širokopojasne pristupne tehnologije

Optička pristupna mreža (pasivna):

- Optička nit do stana (engl. Fiber To The Home, FTTH)
- Optička nit do zgrade (engl. Fiber To The Building, FTTB)
- Optička nit do pločnika (engl. Fiber To The Curb)
- Optička nit do kabinetra (engl. Fiber To The Cabinet, FTTCab)

Hibridna optičko-koaksijalna mreža

- HFC (Hybrid Fiber Coax)

Bežična pristupna mreža

- Wi-Fi (WLAN) - IEEE 802.11
- WiMAX (Wireless Metropolitan Area Network) - IEEE 802.16

Satelitski pristup

- Dial-up (odlazno) + satelitska veza (dolazno)

Komunikacijske mreže

7.1.2008.

31 od 45

Pristup Internetu iz pokretne mreže

Pokretni Internet (Mobile Internet)

- ◆ pristup i rad u Internetu preko pokretnog telefona i druge pokretne korisničke opreme (prijenosno računalo, ručno računalo, ...)
- ◆ komunikacija podacima preko pokretnog pristupa
- ◆ "normalne" ili posebne internetske aplikacije
- ◆ pokretno poslovanje (m-business)

Pristup Internetu:

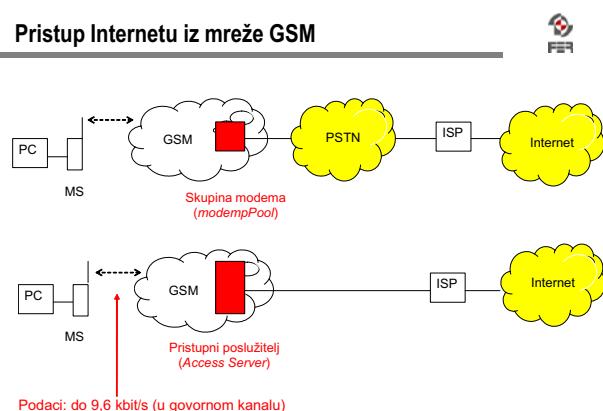
- ◆ kanalski: GSM
- ◆ paketski: GPRS, EDGE, UMTS, HSPA

Komunikacijske mreže

7.1.2008.

32 od 45

Pristup Internetu iz mreže GSM



Komunikacijske mreže

7.1.2008.

33 od 45

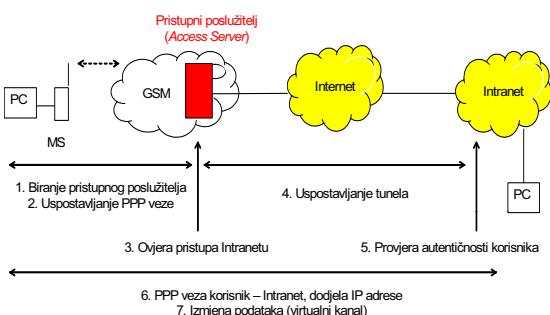
GSM - PSTN - Internet

- GSM operator nije ISP (Internet Service Provider),
- skupina modema na izlazu iz GSM mreže koji se dodjeljuju podatkovnom pozivu,
- > 20 s za uspostavljanje veze,
- GSM operator plaća PSTN troškove,
- bez mogućnosti uvođenja usluga s dodanom vrijednosti.

GSM - Internet

- GSM operator je ISP (Internet Service Provider),
- podatkovni pozivi završavaju u GSM mreži na pristupnom poslužitelju (Access Server),
- digitalna prosojenost s kraja na kraj,
- < 10 s za uspostavljanja veze,
- mogućnost uvođenja nekih usluga s dodanom vrijednosti.

Primjer: pristup Intranetu iz mreže GSM



Komunikacijske mreže

7.1.2008.

34 od 45

Paketska komunikacija u pokretnoj mreži

Proširenje mreže GSM:

- paketski podatkovni kanali na radijskom sučelju
- potporni čvorovi za pristup Internetu i IP zasnovanim mrežama
- rješenja:
 - Opće paketske radijske usluge (engl. General Packet Radio Services, GPRS), n x 14,4 kbit/s (do 115,2 kbit/s)
 - Poboljšane brzine prijenosa podataka (engl. Enhanced Data Rates or Global Evolution, EDGE), n x 48 kbit/s (do 384 kbit/s)

Mreža UMTS:

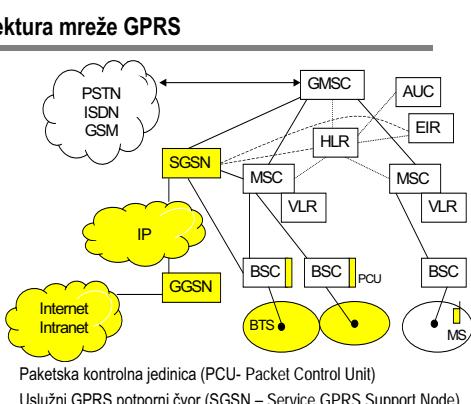
- Kanalski dio (govor) i paketski dio (podatak), do 2 Mbit/s

Komunikacijske mreže

7.1.2008.

35 od 45

Arhitektura mreže GPRS



Komunikacijske mreže

7.1.2008.

36 od 45

GSM - Internet - Intranet

- pristup Intranetu odvija se u koracima kojima se postupno gradi pristupna veza na temelju PPP protokola (Point to Point Protocol)
- tako se može ostvariti virtualna privatna mreža (VPN - Virtual Private Network) koja rabi Internet kao transportnu mrežu kroz koju se tuneliraju paketi između GSM mreže i Intraneta.

Pojavom pokretnog Interneta potrebno je omogućiti pristup i rad u Internetu preko pokretnog telefona i druge pokretne opreme. Kako se u tom slučaju radi o komunikaciji podataka preko bežičnog pristupa, odnosno o usnopljenom prometu, potrebno je omogućiti prijenos podataka komutacijom paketa. GPRS omogućava komutaciju paketa unutar postojeće GSM arhitekture, dakle radi se o proširenju GSM arhitekture sa sljedećim značajkama za operatera:

- bolje karakteristike prilikom bežičnog prijenosa podataka,
- korak bliže trećoj generaciji mreža,
- brzo i jednostavno dodavanje čvorova koji omogućavaju komutaciju paketa u postojeću GSM infrastrukturu,
- bolja iskoristivost kanala u odnosu na prijenos podataka komutacijom kanala.

S gledišta krajnjeg korisnika GPRS omogućava:

- povezanost s Internetom ili Intranetom preko pokretnog terminala (pokretni Internet ili Intranet),
- stalnu vezu s IP,
- povećanje brzine komuniciranja,
- brzi pristup mreži,
- naplata prema primljenom/poslanom volumenu podataka, a ne prema trajanju komunikacije.

Novi čvorovi:

- Serving GPRS Support Node (SGSN) - uslužni GPRS potporni čvor,
- Gateway GPRS Support Node (GGSN) - prilazni GPRS potporni čvor.

Proširenje BSC: paketska kontrolna jedinica (PCU - Packet Control Unit).

SGSN poslužuje korisnika, odnosno rukuje prometom korisnikovih paketiziranih podataka unutar zemljopisnog područja. Povezuje BSS i GGSN čvorove. Područje mreže koje pokriva jedan SGSN čvor naziva se područjem usmjeravanja (RA - Routing Area). Njegove zadaće su:

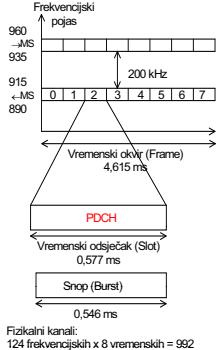
- usmjeravanje paketa iz/u RA od/prema MS
- kriptografska zaštita i provjera autentičnosti
- prikupljanje podataka za naplatu.

GGSN proslijeđuje podatke, odnosno povezuje korisnika sa drugim GPRS i ostalim podatkovnim mrežama. Njegove zadaće su:

- sučelje prema vanjskim IP mrežama
- pridruživanje korisnika SGSN-u
- prikupljanje podataka za naplatu

Čvorovi SGSN i GGSN su međusobno povezani mrežnim IP protokolom.

GPRS - fizički kanal za prijenos paketa



PDCH (Packet Data Channel)

- ◆ vremenski odsječak (GSM kanal) dodijeljen paketskoj komunikaciji
- ◆ svaki PDCH mogu rabiti svi korisnici u ćeliji
- ◆ jedan korisnik može rabiti više PDCH
- ◆ broj PDCH u ćeliji: fiksni ili se mijenja dinamički (npr. do 4)

Komunikacijske mreže

7.1.2008.

37 od 45

GPRS fizički kanal na radijskom sučelju isti je kanal koji osigurava GSM. Vremenski odsječak koji se dodjeli paketskom prijenosu naziva se paketski podatkovni kanal (PDCH).

U svakoj se ćeliji broj PDCH kanala, odnosno omjer GSM i GPRS fizičkih kanala određuje na temelju očekivanog prometa. Broj PDCH može biti fiksni ili se dinamički prilagođavati stvarnom prometu. U tom slučaju se mogu postaviti granične vrijednosti broja PDCH kanala. Kako je broj kanala u ćeliji konstantan, povećanje GPRS kanala smanjuje broj raspoloživih GSM kanala i obrnuto.

Svaki kanal omogućuje brzinu prijenosa podataka ovisno o primjenjenoj kodnoj shemi. U uporabi je kanal s 14,4 kbit/s. Kad bi se svih 8 PDCH dodijelilo jednom korisniku raspolagao bi brzinom 115,2 kbit/s što je za taj slučaj i najveća brzina koju osigurava GPRS.

GPRS potporni čvorovi



Uslužni (SGSN)

- ◆ usmjeravanje paketa od/prema MS
- ◆ upravljanje pokretljivošću i upravljanje logičkom vezom prema MS

Prilazni (GGSN)

- ◆ sučelje prema vanjskim IP mrežama
- ◆ pridruživanje korisnika SGSN-u
- ◆ (DNS, DHCP, NAT)

Isto rješenje za paketsku komunikaciju kao GPRS imaju i EDGE i UMTS!

Komunikacijske mreže

7.1.2008.

38 od 45

Uslužni GPRS potporni čvor SGSN je odgovoran za usmjeravanje paketa od/prema pokretnim postajama MS unutar svojeg područja pokrivanja. Poslužuje sve GPRS korisnike koji su locirani unutar SGSN područja usmjeravanja RA. GPRS korisnik može biti poslužen od strane bilo kojeg SGSN u mreži ovisno o lokaciji. Podaci se usmjeravaju od SGSN prema BSC i preko BTS do pokretnе postaje MS.

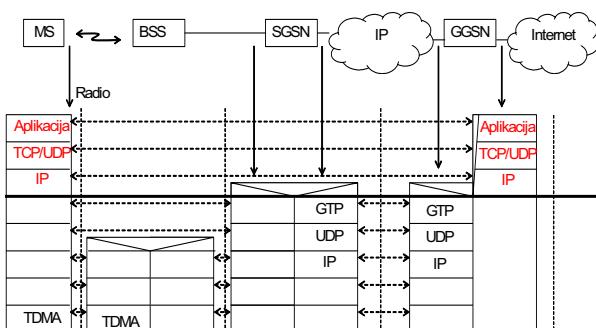
Sučelje Gs između MSC i SGSN je odgovorno za koordinaciju signalizacije za terminale koji imaju moćnost komutacije kanala i komutacije paketa.

HLR sadrži podatke o GPRS pretplatnicima i informacije o usmjeravanju. Svakom pretplatniku dodjeljuje jednog ili više GGSN elemenata.

BSC sadrži novu funkcionalnost za paketsku kontrolu kanala, paketsku kontrolnu jedinicu PCU i novu funkcionalnost za upravljanje pokretljivošću.

GGSN predstavlja sučelje prema drugim GPRS mrežama, ali isto tako i prema vanjskim IP mrežama. Kako bi omogućio komunikaciju s različitim mrežama, GGSN vrši translaciju formata podataka, signalizacijskih protokola i adresne informacije. Usmjerava promet određenom SGSN čvoru i vrši konverziju protokola. Može sadržavati DNS, DHCP i NAT funkcije.

Pristup Internetu iz mreže GPRS (1)



Komunikacijske mreže

7.1.2008.

39 od 45

Osnovna je zamisao "privesti" Internetske protokole (aplikacijski, TCP/UDP, IP) do MS.

Kod pristupa Internetu, paketi od SSGN prema GGSN i obratno tuneliraju za što je odgovoran GTP (GPRS Tunneling Protocol). Pritom se rabi UDP transportni protokol. U tom slučaju ne "gleda" se sadržaj paketa već se oni samo propuštaju prema odredištu. Dakle, paketi od MS dolaze do SGSN gdje se ovijaju (encapsulate) što im omogućava tuneliranje i takvi se propuštaju prema GGSN i dalje prema Internetu. Odredišni SGSN razvija (decapsulate) dobivene pakete od GGSN i šalje ih odredišnom MS.

S motrišta korisnika svi slojevi i protokoli ispod IP protokola između radijskog i ostalih sučelja služe kao prijenosni sloj (bearer) kojim se korisnički terminal bežično, u pokretu, spaja na Internet.

Pristup Internetu iz mreže GPRS (2)

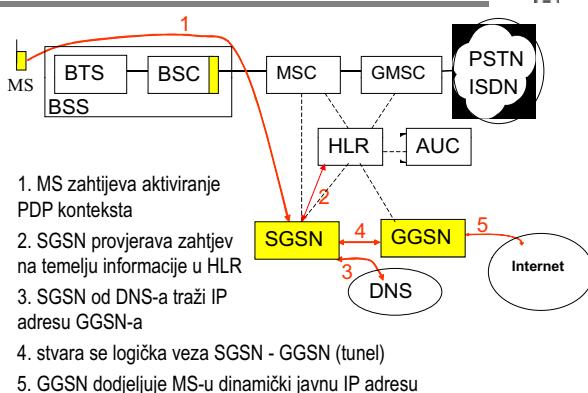


Komunikacija na relaciji korisnička oprema – GGSN:

- ◆ Parametri veze sadržani u PDP kontekstu (Packet Data Protocol Context) koji je pohranjen u korisničkoj opremi (GPRS: Mobile Station, MS), HLR-u, SGSN-u i GGSN-u
- ◆ PDP kontekst aktivira se pri uključivanju korisničke opreme ili komandom prije početka komunikacije
- ◆ GGSN dodjeljuje IP adresu korisničkoj opremi tijekom aktiviranja PDP konteksta:
 - privatna IP adresa se primjenjuje unutar vlastite mreže,
 - javna IP adresa se primjenjuje za vanjsku komunikaciju

PDP context između ostalih parametara sadrži i informacije o usmjeravanju paketa između MS i GGSN.

Pristup Internetu iz mreže GPRS (3)



Prigodom spajanja na Internet potrebno je aktivirati PDP kontekst. U njemu su zapisane karakteristike veze, mrežna adresa, pristupna točka i kvaliteta usluge. Postupak izgleda ovako:

1. MS zahtijeva aktiviranje PDP konteksta.
2. SGSN provjerava zahtjev i uspoređuje ga s pretplatničkim informacijama (mogućnostima) zapisanim u HLR.
3. SGSN od DNS-a traži IP adresu pristupne točke preko koje se pristupa Internetu, DNS šalje IP adresu GGSN-a.
4. Stvara se logička veza, odnosno tunel između SGSN i GGSN pomoću GTP protokola.
5. GGSN dinamički dodjeljuje javnu IP adresu MS-u kao bi se ostvarila komunikacija između MS-a i Interneta.

Opći pokretni telekomunikacijski sustav

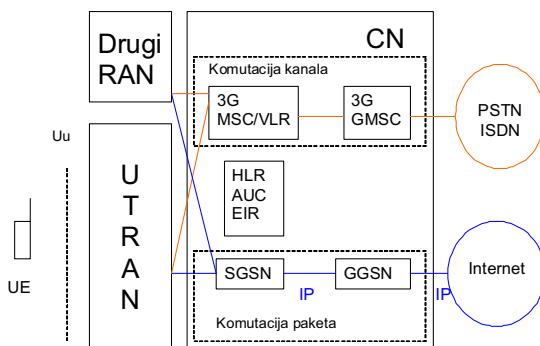


UMTS (Universal Mobile Telecommunications System)

Obilježja

- ◆ terminalska i osobna pokretljivost
- ◆ širokopojasni pristup Internetu u pokretu: do 144 kbit/s u svim uvjetima, do 384 kbit/s na otvorenom prostoru, do 2 Mbit/s u zatvorenom prostoru
- ◆ kanali i paketi, više istodobnih usluga
- ◆ simetrični i asimetrični prijenos
- ◆ kvaliteta govora usporediva s onom u fiksnoj mreži
- ◆ integracija s fiksnom mrežom, koegzistencija s 2. generacijom (GSM)

Arhitektura mreže UMTS



Arhitektura mreže UMTS, 3GPP Release R99.

Uvođenjem UMTS-a uz neku postojeću mrežu javljaju se dvije pristupne mreže - UTRAN i RAN (Radio Access Network) postojeće mreže (GSM, GSM/GPRS, GSM/EDGE).

Da bi se postiglo međudjelovanje (interoperability) dviju mreža na razini pristupa, npr. GSM-a i UMTS-a, treba omogućiti prebacivanje radijskog pristupa iz GSM u UMTS i obratno (inter-system handover). To se postiže distribucijom informacija o WCMA radijskom pristupu kroz TDMA i obrnuto, u smjeru prema pokretnoj postaji (MS), odnosno korisničkoj opremi (UE).

Međudjelovanje na razini jezgrene mreže (CN - Core Network) zahtijeva njezinu evoluciju, s posebnim rješenjima za dio s komutacijom kanala i dio s komutacijom paketa.

U kanalskom dijelu dograđuju se MSC/VLR i HLR/AUC/EIR kako bi mogli poslužiti 2G i 3G korisnike.

U paketskom dijelu koji je preuzet iz GPRS-a, mijenja se funkcionalnost SGSN-a. Naime, u GPRS-u SGSN rješava samostalno upravljanje pokretljivošću. U UMTS-u za upravljanje pokretljivošću nadležni su RNC i SGSN, pri čemu RNC obrađuje promjenu ćelije.

IP kao transportni mehanizam završava na SGSN-u, kao u GPRS-u.

Brza paketska komunikacija u pokretnoj mreži



HSPA (High Speed Packet Access)

Nadogradnja radijske pristupne mreže UMTS

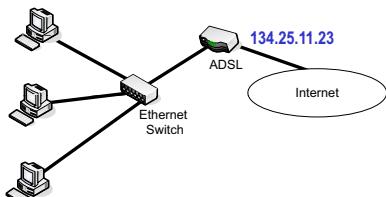
- ◆ Brzi paketski pristup u dolaznom smjeru, HSDPA (High Speed Downlink Packet Access)
 - višestruko ubrzanje prijenosa podataka u dolaznom smjeru, do 10 Mbit/s
- ◆ Brzi paketski pristup u odlaznom smjeru, HSUPA (High Speed Uplink Packet Access)
 - višestruko ubrzanje prijenosa podataka u odlaznom smjeru, od 2 do 5 Mbit/s

Razmisiliti o rješenju ...



Korisnik s tri računala spojena na Ethernet komutator povezan je na Internet primjenom ADSL-a. ISP dodjeljuje korisniku samo jednu javnu IP adresu (134.25.11.23).

Što treba napraviti da bi sva tri računala mogla pristupiti Internetu?



Komunikacijske mreže

13.
Akademika i korporacijska mreža

Ak.g. 2007./2008.

9.1.2008.

Sadržaj predavanja

- ◆ Korporacijska mreža: rješenje 4. domaće zadaće
- ◆ Akademska mreža
 - Mreže zavodskih laboratorija
 - Fast Ethernet
 - Giga Ethernet
 - WLAN
 - Mreža FER-a
 - Mreža CARNet
 - Mreža GEANT2
- ◆ Izazovi Interneta

Komunikacijske mreže

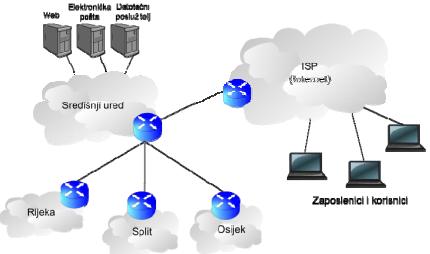
9.1.2008.

2 od 52

Korporacijska mreža: rješenje 4. domaće zadaće

Inicijalno konceptualno rješenje

- ◆ Način spajanja podružnica
 - Iznajmljeni vod
 - VPN
- ◆ Pristup središnjeg ureda Internetu
 - ADSL
 - Stalni vod na Internet (VPN)
- ◆ Pristup korisnika i zaposlenika
 - ADSL
 - UMTS
 - Bežična mreža
 - Modemski ulazi



Komunikacijske mreže

9.1.2008.

4 od 52

Modeliranje sigurnosne prijetnje

- ◆ Cilj je odrediti što napadači imaju na raspolaganju
 - Pretpostavke
 - Mreža je u potpunosti pod kontrolom napadača
 - Usmjeritelji su pod kontrolom napadača
 - Niti jedan mrežni i računalni element tvrtke nije pod kontrolom napadača
- ◆ Sigurnosne prijetnje
 - Prisluškivanje
 - Utjelovljenje
 - Lažiranje paketa
 - Lažiranje poruka elektroničke pošte
 - Napad uskraćivanjem usluge
 - MITM (Man-in-the-Middle) napad
 - Pretraživanje (scanning) u potrazi za ranjivostima

Komunikacijske mreže

9.1.2008.

5 od 52

Tehnologije za zaštitu (1)

- ◆ Komunikacija podružnica i središnjeg ureda
 - Postavljanje vatrozida neposredno prije svih usmjeritelja
 - Usmjeritelji ne smiju vidjeti promet između podružnica
 - VPN (IPsec)
 - Privatnost, integritet i autentičnost
- ◆ Spajanje središnjeg ureda na Internet
 - Korištenje vatrozida za zaštitu unutarnje mreže
 - Istovremeno služi i za nadzor tko/što smije van na Internet
 - Izdvajanje poslužitelja dostupnih izvana u posebnu zonu
 - "Demilitarizirana zona" (DMZ)
 - Datotečnom poslužitelju se ne može pristupiti izvana

Komunikacijske mreže

9.1.2008.

6 od 52

Tehnologije za zaštitu (2)



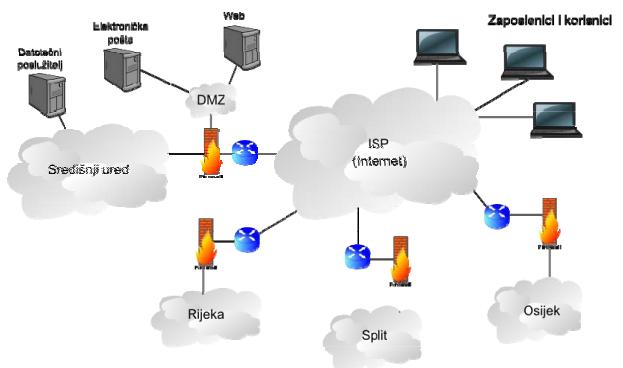
- ◆ Pristup zaposlenika korporacijskoj mreži
 - Upotreba VPN pristupa
 - Klijent na operacijskom sustavu zaposleničkog računala
- ◆ Pristup zaposlenika elektroničkoj pošti
 - Isključivo putem SSL-a
- ◆ Pristup zaposlenika Web poslužiteljima
 - Pristup putem SSL-a (bez ovjere/autentifikacije)
 - Ovjera klijenta za poslovnu aplikaciju

Komunikacijske mreže

9.1.2008.

7 od 52

Konačno rješenje



Komunikacijske mreže

9.1.2008.

8 od 52

Najčešće pogreške u rješenjima zadaća



- ◆ Usmjeritelji (uglavnom) ne obavljaju funkciju VPN-a
- ◆ DoS napadi su općenito napadi zauzimanja **bilo kakvih** (ograničenih) resursa
 - Ne samo poslužitelja!
- ◆ Ne navoditi konkretnе proizvode (točne karakteristike)
 - To bi više bio dio izvedbenog prijedloga
- ◆ Nepotrebno navoditi načine spajanja klijenata kada su izvan tvrtke

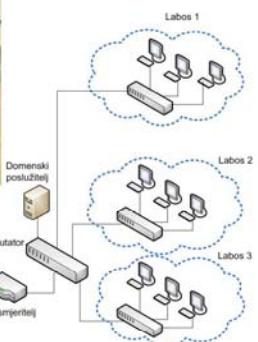
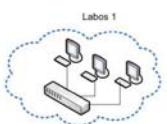
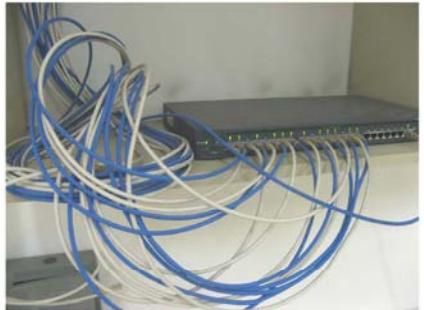
Komunikacijske mreže

9.1.2008.

9 od 52

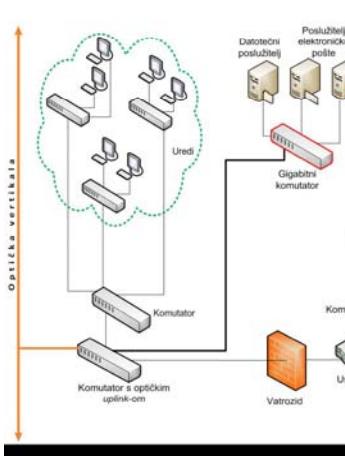
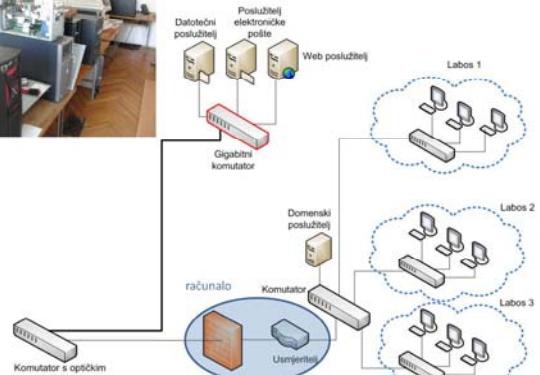
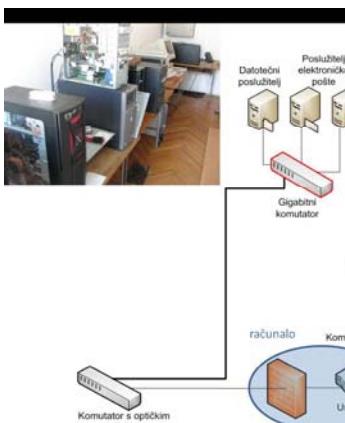
Akademска mrežа





optički uplink

Komutator s optičkim uplink-om



Fast Ethernet

- ◆ Zajednički naziv za skup Ethernet standarda koji omogućuju prijenosne brzine do 100 Mbit/s
 - standard uveden 1995.

Vrste prijenosnih medija

- 100BASE-T2
 - Korištenje dviju parica UTP kategorije 3
- 100BASE-T4
 - Korištenje četiriju parica UTP kategorije 3
- 100BASE-TX
 - Korištenje dviju parica UTP kategorije 5/5e
- 100BASE-FX i 100BASE-SX
 - Korištenje dviju optičkih niti
- 100BASE-BX
 - Korištenje jedne optičke niti

Komunikacijske mreže

9.1.2008.



12 od 52

Gigabitni Ethernet

- ◆ Gigabit Ethernet (GbE, standard uveden 1998.)
 - Omogućuje prijenosne brzine do 1 Gbit/s kod pristupne metode CSMA/CD
 - 1000BASE-T (specificira uporabu četiri parice)
 - 1000BASE-X (specificira uporabu optičkih niti)

10 Gigabit Ethernet (10GbE, uveden 2006.)

- UTP (Cat 6) i optika
- Isključivo full-duplex (ethernet komutatori)

100 Gigabit Ethernet (100GbE, standard u razvoju)

- Isključivo optika

Komunikacijske mreže

9.1.2008.

13 od 52

Primjena WLAN-a

- ◆ Proširenje žičnih lokalnih mreža (LAN)
 - Npr., WLAN na FER-u
- ◆ Povezivanje LAN-ova na manjim udaljenostima
 - Npr., povezivanje dvije poslovnice usmjerjenim bežičnim link-om
- ◆ Omogućena ograničena pokretljivost korisnika u radu
 - Npr., audio strujanje na pokretnom uređaju (iPAQ, ...)
- ◆ U situacijama neprikladnog ili neizvedivog ožičenja
 - Kulturno-povijesni objekti, skijališta, kampovi, itd.

Komunikacijske mreže

9.1.2008.

14 od 52



Komponente WLAN-a

- ◆ Pokretne ili fiksne radne stanice
 - Prijenosno računalo
 - Stolno računalo opremljeno bežičnom mrežnom karticom
- ◆ Pristupne točke (Access Point, AP)
 - Veza između bežičnog i žičanog dijela mreže
 - Komunikacija između stanica obavlja se isključivo putem pristupne točke (izuzetak ad-hoc WLAN-ovi)
- ◆ Distribucijski sustavi
 - Povezuje veći broj pristupnih točaka
 - Najčešće žičani LAN
- ◆ Bežični medij
 - Radijski prijenos (RF)
 - (Infracrveni prijenos, IR)

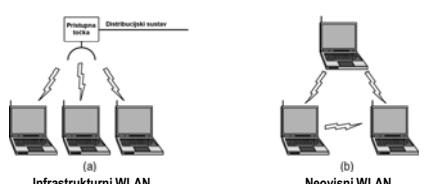
Komunikacijske mreže

9.1.2008.

15 od 52

Topologije WLAN-a

- ◆ Infrastrukturni WLAN
 - Komunikacija između krajnjih uređaja obavlja se isključivo putem pristupne točke (stanice ne mogu izravno komunicirati)
 - Veće područje pokrivanja
- ◆ Neovisni (ad-hoc) WLAN
 - Stanice komuniciraju izravno (nema pristupne točke)
 - Manje područje pokrivanja u odnosu na infrastrukturni WLAN



Komunikacijske mreže

9.1.2008.

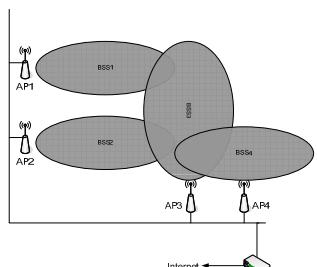
16 od 52



16 od 52

Povezivanje više pristupnih točaka

- ◆ BSS (Basic Service Set)
 - Osnovni element mreže prema standardu 802.11 (skup stanica koje međusobno komuniciraju)
 - Jedinstvena oznaka BSSID
- ◆ BSS omogućava ograničeno područje pokrivanja (Basic Service Area)
 - Područje unutar kojeg članovi BSS-a mogu međusobno komunicirati
 - Cca. 10-20 m u zgradama, 100 m na otvorenom
- ◆ ESS (Extended Service Set)
 - Više BSS-ova povezanih distribucijskim sustavom s ciljem pokrivanja većeg područja
 - Stanice unutar jednog ESS-a mogu međusobno komunicirati
 - SSID - identifikacija ESS-a
 - Pristupne točke moraju razmjenjivati podatke o spojenim stanicama - koristi se protokol IAPP (Inter-Access Point Protocol)



Komunikacijske mreže

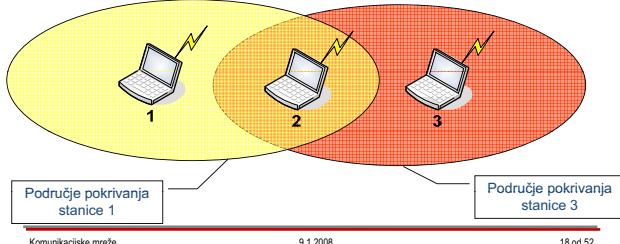
9.1.2008.

17 od 52



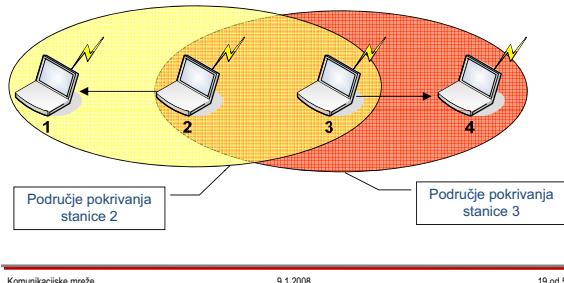
Problem skrivene stanice (hidden station problem)

- Stanice 1 i 3 ne mogu komunicirati (izvan dosega su)
- Stanice 1 i 3 žele poslati okvir stanici 2
 - CS mehanizmi stanica 1 i 3 zaključuće da je medij slobodan
 - Stanice 1 i 3 šalju okvir i dolazi do sudara
- Stanica 1 je skrivena za stanicu 3 i obratno



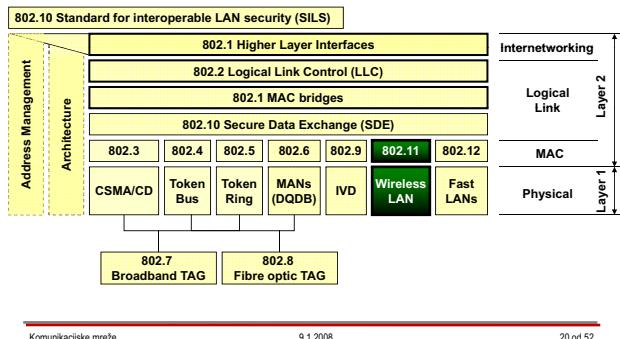
Problem izložene stанице (exposed station problem)

- Stanica 2 šalje podatke stanicu 1
- Stanica 3 želi poslati podatke stanicu 4
 - CS mehanizam zaključuje da je medij zauzet te odgađa slanje



Standard IEEE 802.11

- Odbor IEEE 802, grupa 11 (<http://www.ieee802.org/11/>)



802.11 MAC - podsloj pristupa mediju (1)

- MAC podsloj kontrolira i određuje kada korisnik može poslati podatke na medij
- Tri načina pristupa mediju**
 - Distribuirani** (Distributed Coordination Function, DCF)
 - Koristi se metoda pristupa CSMA/CA
 - CS (Carrier Sense) - stanica osluškuje medij
 - MA (Multiple Access) - više stanica dijeli isti medij
 - CA (Collision Avoidance) - izbjegavanje kolizija
 - Distribuirani s ugradenim protokolom "rukovanja"** (DCF RTS/CTS)
 - Razmjenjuju se upravljački okviri RTS (Request to Send) i CTS (Clear to Send)
 - Centralizirani** (Point Coordination Function, PCF)
 - Pristupna točka vrši prozivanje stanica, nema natjecanja za medij
 - Pogodno za stvarno-vremenske aplikacije

Komunikacijske mreže 9.1.2008. 21 od 52

802.11 MAC - podsloj pristupa mediju (2)

- Nedostaci DCF-a**
 - Povećanjem broja stanica koje se natječu za medij povećava se broj kolizija, te se smanjuje brzina prijenosa podataka
 - Nema prioritizacije prometa
 - Stanica koja zauzme medij može ga zauzimati neograničeno dugo (problem sa sporim stanicama)
- DCF RTS/CTS se najčešće koristi u praksi
- PCF se vrlo rijetko koristi u praksi
 - Vrlo mali broj komercijalnih pristupnih točaka omogućava PCF

Komunikacijske mreže

9.1.2008.

22 od 52

Protokol CSMA/CA (1)

- Detekcija nosioca (CS, Carrier Sensing)**
 - Utvrdjuje da li je medij slobodan
 - Fizički CS
 - Izveden sklopovski
 - Problem istovremenog odašiljanja i primanja signala
 - Skupo
- Virtualni CS**
 - Primjena NAV (Network Allocation Vector) vektora
 - U zaglavju okvira postoji polje kojim se definira predviđeno trajanje zauzeća medija
 - Stanica postavlja NAV vektor na vrijednost u ms, koliko smatra da će zauzimati medij
 - Ostale stanice mijere vrijeme od vrijednosti NAV vektora do 0

Komunikacijske mreže

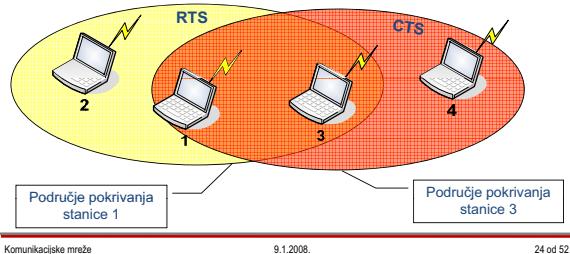
9.1.2008.

23 od 52

Protokol CSMA/CA (2)



- Izbjegavanje kolizija (CA, Collision Avoidance)
 - Razmjena okvira RTS (Request to Send) i CTS (Clear To Send)
 - Oba okvira sadrže informaciju o predviđenom trajanju zauzeća medija



Sigurnost podataka u WLAN-u (1)



- Podaci koji se prenose lako su dostupni jer se komunikacija odvija zrakom
- Zaštita podataka je najvažniji preduvjet široke primjene bežičnih LAN-ova
- Šifriranje
 - Postupak modifikacije poslanih podataka, tako da su nerazumljivi svima koji nemaju informaciju o načinu dekripcije
- Ovjera/autentifikacija
 - Postupak provjere korisnika - da li je korisnik zaista onaj za koga se izdaje?

Komunikacijske mreže 9.1.2008. 25 od 52

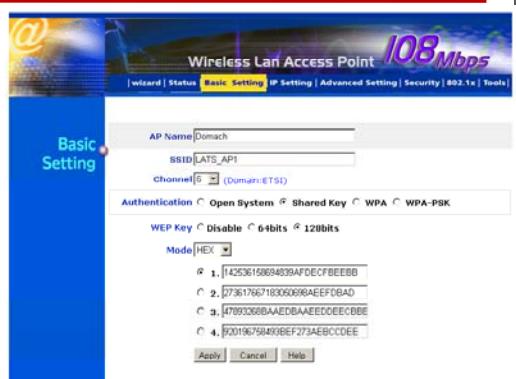
Sigurnost podataka u WLAN-u (2)



- Filtriranje MAC adresa - najprimitivnija metoda restrikcije pristupa WLAN-u
 - Na pristupnoj točki definira se popis MAC adresa svih pokretnih stanica koje se smiju spojiti na AP
- WEP (Wired Equivalent Privacy)
 - Standard za enkripciju podataka izведен na MAC sloju 802.11 mrežnih uređaja
 - Kriptiranje se obavlja bit po bit, obje strane u komunikaciji (mrežna kartica i AP) moraju koristiti isti ključ
 - Problem velikog broja korisnika i pristupnih točaka
 - Nepouzdan način zaštite - ručna distribucija ključeva, mogućnost probijanja velika

Komunikacijske mreže 9.1.2008. 26 od 52

WEP - primjer konfiguracije AP-a



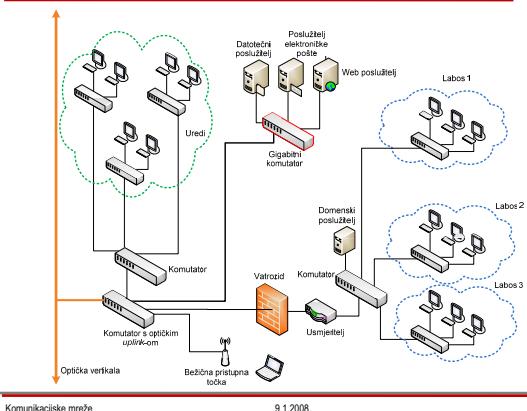
Alternative WEP-u



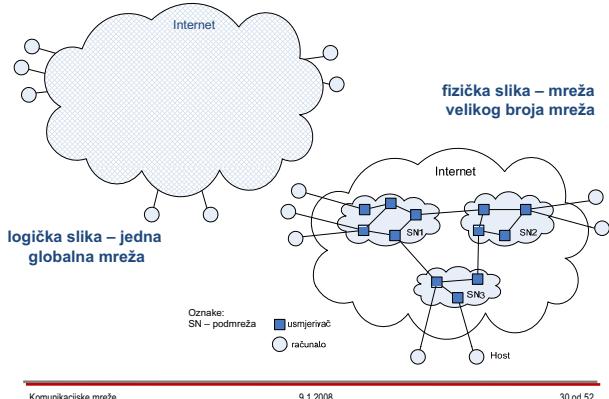
- WPA (Wi-Fi Protected Access), WEP2
 - Riješeni problemi WEP-a
 - Poboljšana enkripcija, 2 metode ovjere korisnika
- WPA2 (IEEE 802.11i)
 - Trenutno najpouzdanija metoda zaštite od neovlaštenog pristupa 802.11 LAN-ovima

Komunikacijske mreže 9.1.2008. 28 od 52

Primjer zavodske mreže



Logička i fizička slika Internet mreže

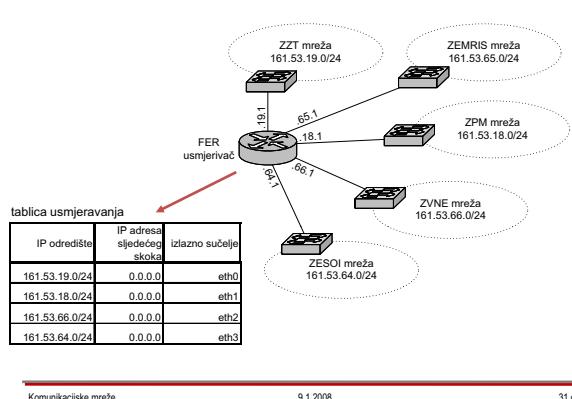


Komunikacijske mreže

9.1.2008.

30 od 52

Arhitektura Interneta – kroz primjere

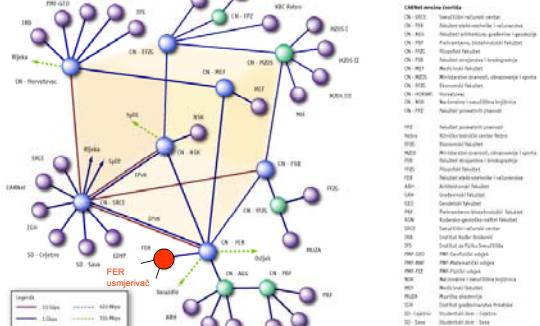


Komunikacijske mreže

9.1.2008.

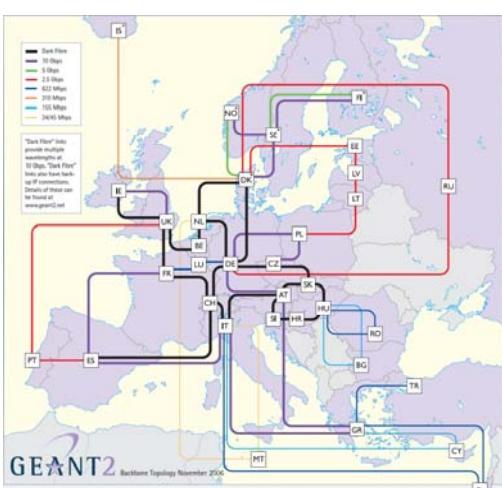
31 od 52

Stanje zagrebačkog dijela CARNet mreže Od rujna 2004.

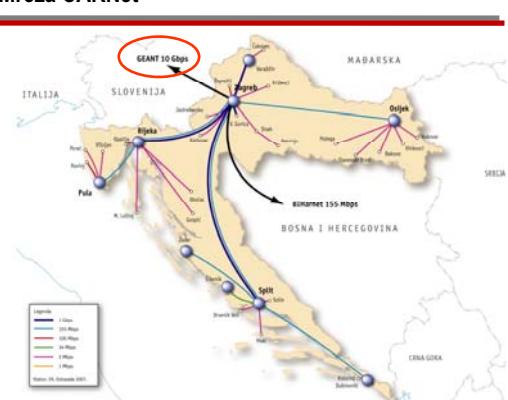


Europska istraživačko-ekdukacijska mreža

Topologija okosnice mreže GEANT2



Mreža CARNet



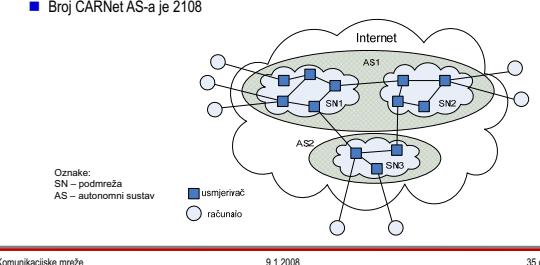
Komunikacijske mreže

9.1.2008.

33 od 52

Autonomni sustav

- Skup IP mreža i usmjerivača u nadležnosti jedne organizacije koja samostalno određuje kako se provodi usmjeravanje unutar sustava te kako se, s obzirom na usmjeravanje, sustav ponaša prema ostatku Internet mreže
- Svakom autonomnom sustavu (AS) organizacija IANA dodjeljuje jedinstveni broj
 - Broj CARNet AS-a je 2108

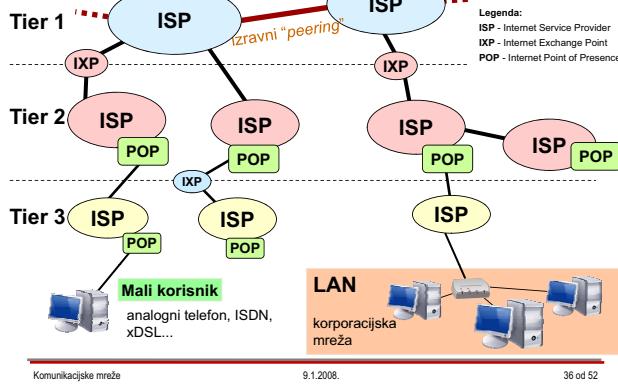


Komunikacijske mreže

9.1.2008.

35 od 52

Internet hijerarhija



Croatian Internet eXchange – CIX

- ◆ 19 članica (www.cix.hr)

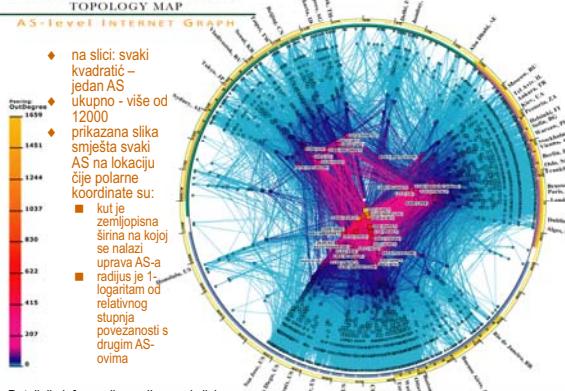
	CARNet	Iskon	Metronet	VIP-NET	Optima	HRT	HEP	VM-Mreže	Vojateli	Amis
CARNet	+	+	+	+	+	+	+	+	-	-
Iskon	+	-	+	+	+	-	-	-	-	-
Metronet	+	-	+	+	-	-	-	-	+	-
VIP-NET	+	+	+	-	+	?	?	+	+	?
Optima	+	+	+	+	-	?	?	+	+	?
HRT	+	+	-	?	?	-	?	+	?	?

Nepotpuna tablica "peering" ugovora

Oznake:
"+" postoji peering
"-" ne postoji peering
"?" nepoznato

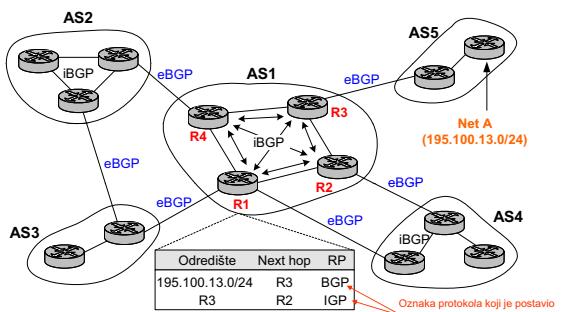
Komunikacijske mreže 9.1.2008. 37 od 52

IPv4 INTERNET



Usmjeravanje između AS-ova – BGP

Svi autonomi sustavi koriste Border Gateway Protocol (BGP) i to verziju 4.



Izazovi Interneta

Internet nekada

- ◆ (Relativno) mali broj korisnika
- ◆ Sigurna okolina
- ◆ Simetrični linkovi relativno malih brzina
- ◆ Udaljen rad na velikim računalima (Mainframe)

Internet danas



◆ Nove vrste i novi koncepti mreža

- Pokretne i bežične mreže (UMTS, WLAN)
- Asimetrična povezanost (UMTS, xDSL)
- Više-gigabitni linkovi (10GbE)

◆ Jeftin pristup Internetu

◆ Nedostatak IPv4 adresa

- Pokretni uređaji

◆ Višemedijski sadržaj

◆ Poslovanje tvrtki na Internetu

- Pouzdanost



Temeljni principi Interneta

◆ Internet se temelji na jednostavnim principima

- Sva "inteligencija" mora biti izvan mreže
 - End-to-End design principle
- Svi uređaji priključeni na Internet moraju imati jedinstvenu i stalnu IP adresu

◆ Uvođenje novih aplikacija i usluga je jednostavno

◆ Danas se ti principi sve više krše

- Vatrozidovi, NAT uređaji, posrednički poslužitelji (proxy), ...

Problem s IP adresama



◆ IP adrese imaju dvostruku funkciju

- Identifikator
 - Određuju s kim komuniciramo
- Lokator
 - Određuju gdje se nalazi odredište

◆ Razlog je korištenje IP adresa u mrežnom, transportnom i aplikacijskom sloju

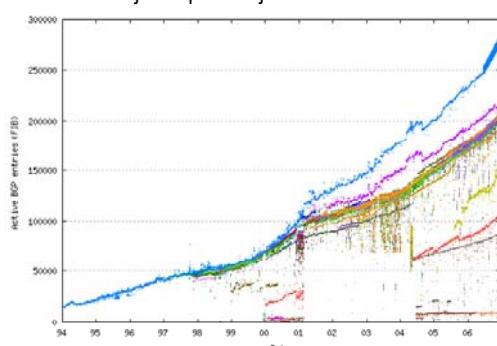
◆ Problemi za

- Višepristupnost (Multihoming)
- Pokretljivost
- Renumeračiju



Rast Interneta (1)

◆ Rast Interneta je eksponencijalan



Rast Interneta (2)



◆ Problemi za postojeće usmjerivače

- Nisu predviđeni za takva opterećenja
- IPv6 može pogoršati situaciju
 - Više mogućih adresa – još veće tablice usmjeravanja
- Projektiranje nove opreme potencijalno preskupo

◆ Istraživanje u okviru grupe RRG

- Routing Research Group
- Primjer je prijedlog LISP
 - Locator ID Separation Protocol
- Temelji prijedloga
 - Razdvajanje funkcionalnosti IP adresa
 - Predviđeno postupno uvođenje



Novosti u IPv6

◆ Moguće adresiranje većeg broja umreženih uređaja i sustava (adresa 128 bitova)

◆ Pojednostavljen format zaglavja, uvedena dodatna zaglavla, moguća nova zaglavla

◆ Pojednostavljenovo usmjeravanje

◆ Sigurnosni mehanizmi na mrežnom sloju (IPsec)

◆ Pokretljivost (Mobile IP)

◆ Kvaliteta usluge (prijenos u stvarnom vremenu)

Višepristupnost

◆ Ciljevi

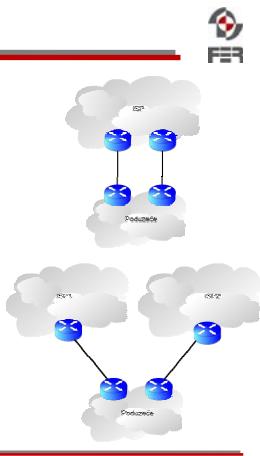
- Postići nezavisnost od pojedinog ISP-a
- Ostvariti veću dostupnost i propusnost

◆ Problemi s jednim ISP-om

- Ne postižemo potuni učinak
 - Još uvek ovisimo o jednom ISP-u
- Upotreba NAT-a unosi dodatne probleme

◆ Problemi s više ISP-ova

- Opterećenje na sustav usmjeravanja u jezgri Interneta
 - Ako koristimo IP adrese jednog ISP-a
- Zahtjev za nezavisnim IP adresama i AS brojem
 - Značajni troškovi
- NAT je uvek značajan problem



Komunikacijske mreže

9.1.2008.

48 od 52

"Klasični" IP, bez pokretljivosti

Aplikacija

HTTP, FTP, Telnet, SMP, SNMP, NFS, ...

Transport

TCP, UDP, RTP

Mreža

IPv4, ICMP, IGMP, ...

Prijenos

Podatkovna veza
Fizikalni sloj

- Identifikacija čvora i mreže
- Određivanje priključne točke
- Usmjeravanje datagrama prema odredištu (IP adresa)

Komunikacijske mreže

9.1.2008.

49 od 52

IPv4 - Mobile IP

Aplikacija
HTTP, FTP, Telnet, SMP, SNMP, NFS, ...
Transport
TCP, UDP, RTP
Mreža
IPv4, ICMP, IGMP, ...
Prijenos
Podatkovna veza Fizikalni sloj

- "Klasični" IP:
 - Pokretni korisnik/čvor zahtijevač bi promjenju IP adresu, s poslijedicama na transport i aplikacije
- Mobile IP:
 - Zadržati stalnu IP adresu
 - Uvođenje novih funkcijskih entiteta i trenutne adrese
 - Ne mijenjati programsku podršku u usmjeriteljima

Komunikacijske mreže

9.1.2008.

50 od 52

Razvoj novih transportnih protokola

◆ TCP (i UDP) u upotrebi skoro 30 godina

- Mnoštvo istraživanja i optimizacija
- Ipak, neke nedostatke nije moguće ispraviti

◆ Novi transportni protokoli

■ Alternativa TCP-u: SCTP

- Višepristupnost, sačuvane granice poruka, više tokova (streams) unutar jedne asocijacije (veze)

■ Alternativa UDP-u: DCCP

- Bespojni protokol s kontrolom zagruženja
- Kontrola zagruženja je vrlo bitan i složen element

Komunikacijske mreže

9.1.2008.

51 od 52

Još nekoliko otvorenih pitanja u Internetu...

◆ Osiguranje stabilne povezanosti Interneta

- Problemi s oscilacijama i ispadima linkova

◆ Osiguranje kvalitete usluge u Internetu

- Diferencirane usluge (Differentiated Services, DiffServ)
- Integrirane usluge (Integrated Services, IntServ)

◆ Uvođenje telefonije

- SIP (Session Initiation Protocol)

◆ Distribucija video materijala

- Znatan rast u zadnje vrijeme (YouTube)
- Veliko opterećenje na infrastrukturu

Komunikacijske mreže

9.1.2008.

52 od 52