Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

RAČUNALNIŠKE KOMUNIKACIJE
Uvod, Povezovanje
(IKS, 1.-3. poglavje)

UVOD

- Informacijski sistem
- (Tele)komunikacijski sistem
- INFORMACIJSKO-KOMUNIKACIJSKI sistem - IKS
- STORITEV: funkcionalnost sistema, ki uporabniku omogoča izpolnitev neke zahteve.
- Primeri storitev

Storitve

Integrirani sistemi

▼

Integrirane storitve

Uporabnika ne zanima izvedba storitve:
TRANSPARENTNOST

Osnovni pojmi 1/2

- Podatek: zapis dejstva
- Informacija: interpretacija podatka
- Večja vrednost informacije, če je dogodek manj verjeten.
- Komunikacija: proces prenašanja podatkov (za shranjevanje ali interpretacijo).
- Signal: zapis (dela) podatka v obliki, primerni za prenos po prenosnem mediju

Primer

- Predstavitev (prevajanje)
- Konverzija sporočilo-signali
- Vmesniki med plastmi

Osnovni pojmi 2/2

- Informacijski sistem: obdeluje podatke (omogoča interpretacijo).
  - Vnos, obdelava, prikaz podatkov.
- Komunikacijski sistem: omogoča komunikacijo.

Izvor podatkov

- Primera
  - človek
  - merilni inštrument
- Oddajna informacijska točka – vmesnik med informacijskim in komunikacijskim sistemom.
  - Podatki – sporočilo.
- Sprejemna informacijska točka
  - Sporočilo – podatki.

7

IKS

- Kompleksen
- Multidisciplinaren:
  - Prenosne naprave
  - Telekomunikacije
  - Računalništvo
  - Informatika
  - Elektrotehnika
  - Psihologija (uporabniki!)
  - ...

8

Prenosni sistemi

- Analogni
  - 1830: Telegraf (pike črte 3bit/s)
  - 1890: Telefon, 1892: tel. centrala - preklapljanje
  - 1950: 595 Mb/s, 1978: 8 Gb/s
- Digitalni
  - 1970: X.25 9600 bit/s
  - 1980: ISDN 2 x 64 kbit/s
  - 1990: 10 - 100 Mb/s
  - Danes: 100 Gb/s, 1 Tb/s

9

Storitve

- Interaktivne (omejena zakasnitev)
- Večpredstavne (zagotovljena kapaciteta): govor - zvok, video
- Podatkovne (klasične): poljuben prenosni kanal.
  - BREZIZGUBNO OMREŽJE: poljubno število zvez
- Storitve v realnem času (tel. kanal):
  - IZGUBNO OMREŽJE: omejeno število zvez
- Mobilnost

10

Integrirane storitve

- Radio, televizija, video na zahtevo
- Pozivnik, brezvrvični telefon, mobilni telefon
- Telex, email, javni podatki ...

11

POVEZOVANJE

- Končni uporabnik
- IKS

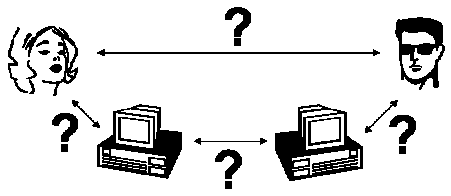
- Delovno mesto: večpredstavni terminal
- Uporabniško okolje: še aplikacije.

- Informacijski del: povezovanje ljudi in tehnologije
- Komunikacijski del: povezovanje tehnologije

12

Povezovanje

- Uporabnik – uporabnik
- Uporabnik – računalnik
- Računalnik - računalnik



13

Povezovanje uporabnikov

- Uporabnik odda podatke.
  - Podatki so (shranjeni, potujejo, ...) v sistemu
- Uporabnik sprejme podatke.
- Oblika podatkov: govor, slika, besedilo ...

14

Informacijski sistem

- Pomaga uporabniku pri delu s podatki. Je (podatkovni) model realnega sveta.
- Nudi orodja za delo s podatki.
- Povezovanje uporabnikov:
  - Informacijske funkcije (za delo s podatki)
  - Komunikacijske funkcije (za prenos podatkov)

15

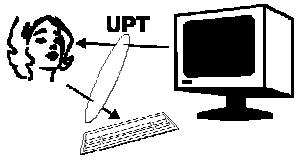
Povezovanje uporabnik - računalnik

- Uporabnik: človek, ki komunicira z IKS prek vhodno izhodnih enot.
- Uporabnik izkorišča vire IKS:
  - Procesiranje (izvajanje)
  - Aplikacije (nadgradnja procesiranja)
  - Podatki
  - Komunikacijske storitve

16

Pristopna točka

- VMESNIK med uporabnikom in viri = pristopna točka (UPT),
- uporabniški vmesnik: posredovanje ukazov sistemu



17

Povezovanje računalniških sistemov

Struktura računalniškega sistema:

- Sistemski elementi
  - Strojna oprema
  - Sistemska programska oprema
  - Sistemski podatki
- Uporabniški elementi
  - Uporabniška programska oprema
  - Uporabniške podatkovne strukture

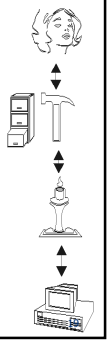
18

Povezave pri lokalni uporabi

Računalnik ne dostopa do omrežja.

POVEZAVE:
Vertikalne - fizične

Uporabnik
UPT
Aplikacija
Pod. baza
NADZOR
Operacijski sistem
NADZOR
Strojna oprema



Povezave pri oddaljenem dostopu

Računalnik dostopa do omrežja.

POVEZAVE:
Vertikalne – fizične
in
Horizontalne - logične

20

PLASTI

Funkcionalni sklopi IKS so večplastni.

- Uporabniška plast: poslovanje
- Aplikacijska plast: informacijska podpora delovnemu mestu.
- Transportna plast: omrežje
  - Usmerjanje od izvora do ponora
- Povezavna plast: prenosni medij
  - Prenos podatkov med napravami

21

Vertikalne povezave

- Višja plast zahteva storitev od nižje plasti.
- Nižja plast izvede storitev.
  - Lahko zahteva izvedbo kake druge storitve od še nižje plasti

22

Horizontalne povezave

- Logične povezave med procesi iste plasti.
- Ti procesi se izvajajo v okviru različnih delovnih mest!

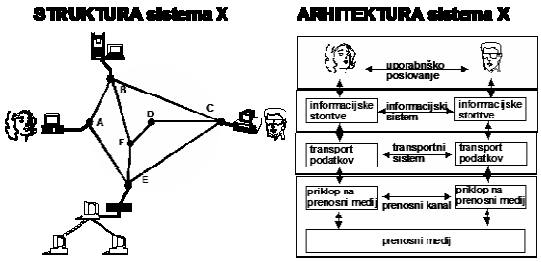
23

Arhitektura in struktura

- Arhitektura opredeljuje
  - Plasti, njihovo funkcijo in hierarhijo
  - Logične povezave
- Struktura opredeljuje
  - Topologijo sistema
  - Izvedbo vertikalnih povezav
  - Fizične zmogljivosti sistema

24

Arhitektura in struktura



Arhitektura in struktura

NALOGA:

- Obvladovanje razpršenih virov
- Prijaznost do uporabnika

Razpršenost in porazdeljenost

- Razpršenost (decentralizacija)
  - Opisuje fizično ali logično lokacijo virov (opreme, podatkov, nadzora).
- Porazdeljenost (distribuiranost)
  - Značilnost sistema - opisuje rezultanto razpršenosti podatkovnih, procesnih in nadzornih virov

Kje se nahajajo plasti?

- Informacijska:
  - aplikacija na uporabniškem računalniku
- Transportna, omrežna in prenosna:
  - na uporabniškem računalniku
  - na usmerjevalnikih

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Tipi povezovanja in standardizacija plasti (IKS, 4.+5. poglavje)

Zaprti in odprti sistemi

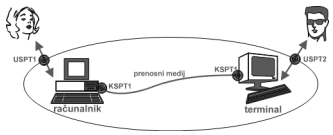
- Iniciativa pri povezovanju:
  - Uporabniki
  - Proizvajalci
- Težave (združljivost)
- Rešitev – ločen komunikacijski sistem, TSPT

Tipi povezovanja

- Terminalski dostop
- Oddaljen (omrežni) dostop do računalnika
- Oddaljen dostop do podatkov
- Sodelovanje oddaljenih aplikacij

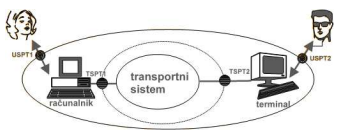
Terminalski ali lokalni dostop

- Lokalni računalnik: vsi viri v enem računalniku
- Terminali so povezani prek V/I (npr. serijska povezava)
- Ni transportne plasti (priključek na interna vodila ali prek KSPT)!
- Nabor storitev
- Lokalna prijava



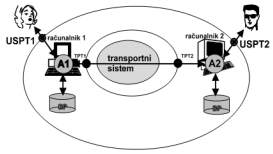
Oddaljen dostop

- Vmes je omrežje
- Transportni sistem
- Vzpostavitev povezave
- Oddaljena prijava
- (Aplikacija)



Oddaljene aplikacije

- Uporabnik se prijavi le v svojo aplikacijo
- Ta poskrbi za dostop do lokalne in v sodelovanju z oddaljeno aplikacijo še do oddaljene podatkovne baze.
  - Kooperativnost
  - Konkurenčne situacije
  - Transparentnost!



Računalniški sistem

- VIRI:
  - Strojna oprema
  - Procesorske zmogljivosti
  - Nadzorni sistem
  - Podatki (podatkovna baza)
- Fizične in logične povezave
- Vodilo (naslovno, podatkovno, kontrolno)
- Strojna oprema
  - Centralni del (CPE, pomnilnik, krmilniki)
  - Periferni del (periferne enote – disk, zaslon, miš…)

7

Vrste povezav med viri

- TESNA: z naslovnim, podatkovnim in kontrolnim vodilom
- OHLAPNA: s podatkovnimi in kontrolnimi vodili (V/I kanal)
- OMREŽNA: podatkovno vodilo (serijsko ali tudi paralelno)

8

Zmogljivosti (1/2)

- Transakcija
- Posel: vsebinsko zaporedje transkacij
- Proces: viri, ki sodelujejo pri izvedbi zahteve

- Odzivni čas
- Prepustnost: št. trans. oz. poslov / čas
- Dostopnost: več uporabnikom, do več sistemov
- Obremenljivost: prilagajanje številu zahtev

9

Zmogljivosti (2/2)

- Adaptivnost (prilagodljivost): prilagajanje virov (števila, količine…) poslom
- Zanesljivost omrežja: v vsakem trenutku dostopnost vsakemu uporabniku
- Razpoložljivost: čas delovanja / čas (>99.8%)
- Modularnost (razširljivost): sposobnost fleksibilne rasti in konfiguriranja
- Cena: strojna oprema + vzpostavitev + obratovalni stroški. Cena / zmogljivost.

10

Standardizacija plasti

- Horizontalno - logično
- Vertikalno – fizično

povezovanje

- Višja plast zahteva izvedbo storitve od nižje plasti.
- Nižja plast funkcionira kot strežnik.
- Podobni problemi kot v sistemih odjemalec – strežnik.

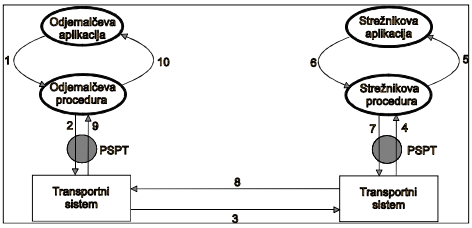
11

Odjemalec - strežnik

- Odjemalec: proces, ki potrebuje izvedbo neke storitve
- Strežnik: proces, ki je sposoben izvesti storitev
- Zahteva – odgovor: transakcija
- Primer: program-podprogram

12

Klic oddaljene procedure



- Transparentnost
- Formatiranje parametri ⇔ sporočilo

13

Izredne situacije

- Izpad strežnika ali transportnega sistema
  - Odjemalec čaka (reset)- največ enkrat
  - Časovna kontrola –
  - Ponovni klic – vsaj enkrat
  - Odgovor: zadnji od mnogih

14

Izredne situacije

Izpad odjemalca (strežniški proces sirota)

- Iztrebljanje otrok, ko se odjemalec ponovno zbudi
- Nežno iztrebljanje
- Omejen čas za odgovor strežnika (prosi za nov interval)
- Reinkarnacija (odjemalec oznani novo epoho)

15

Splošne lastnosti plasti

- Strukturiranje sorodnih problemov
  - Informacijski sistem (razpršitev virov)
  - Transportni sistem (tvorjenje, prenos in transformacija sporočil)
  - Prenosni sistem (sporočilo →signali, prenos)

16

Definicija plasti

- Skupina storitev, specifična obravnava
- Natančno opredeljena funkcionalnost
- Minimalen pretok med plastmi
- Ustrezno število plasti
- Kompatibilno s standardizacijo

17

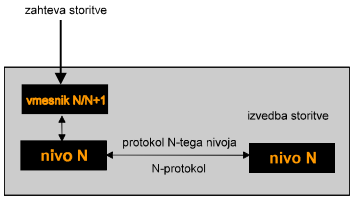
Delovanje plasti

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

18

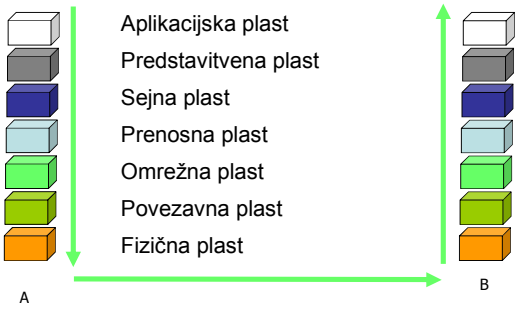
Entitetni par

- Par procesov, ki komunicirata na isti plasti – na različnih straneh.
- Kaj pa, če je več plasti?



19

ISO OSI model



20

Fizična plast

- prenos bitov po komunikacijskem kanalu (baker – optika – brezžično)
  - Kodiranje
  - Multipleksiranje

21

Povezavna plast

- Asinhrona, sinhrona komunikacija
- Zaznavanje in odpravljanje napak (pariteta, CRC, kontrolne vsote)
- Okvirjanje, kontrola pretoka

22

Omrežna plast

- Preklapljanje (povezavne in nepovezavne storitve)
- Usmerjanje
- Izogibanje zamašitvam

23

Transportna in sejna plast

- Transportna: Učinkovit, zanesljiv prenos podatkov od izvora do ponora (povezavno, nepovezavno)
- Sejna: pogosto je vgrajena v aplikacije. Logično povezovanje oddaljenih procesov / aplikacij.

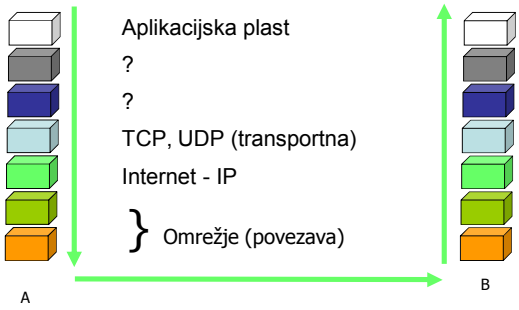
24

Predstavitvena in aplikacijska plast

- Predstavitvena
  - Sintaksa in semantika podatkov
  - Kodiranje, kompresija, varnost
- Aplikacijska
  - Standardne storitve – telnet, FTP, SMTP, SNMP, HTTP...
  - Nestandardne storitve

25

TCP/IP model



26

Primerjava modelov

- TCP/IP: prilagodljiv, fleksibilen, obilje storitev in izdelkov, izvor v računalništvu, nesistematičen, *de facto* (najprej izvedba, potem standard)
- ISO OSI: kompleksen, rigiden sistematičen vseobsegajoč, izvor v TK, *de iure* (najprej standard, potem izvedba), pomanjkanje izdelkov – izvedb, zamira.

- ISO: mednarodna organizacija za standardizacijo
- OSI: Open System Interconnection

27

Kakovost storitve

- Storitev
  - S potrditvijo (oddajnik prejme potrditev) - zanesljiva
  - Brez potrditve (oddajnik upa, da vse OK) - nezanesljiva

28

Kakovost storitve

- Storitev
  - Povezana (najprej vzpostavi logični kanal)
    - Paket ne potrebuje naslova
    - Ohranja se vrstni red
    - Faze: vzpostavljanje, prenos, rušenje
  - Nepovezana
    - Podatki gredo po različnih poteh (naslov!)
    - Ni vzpostavljanja in rušenja
    - Vrstni red ni zagotovljen
- Zanesljive in nezanesljive lahko izvedemo povezano ali nepovezano

29

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Omrežna plast

Vsebina

Delovanje storitev omrežne plasti

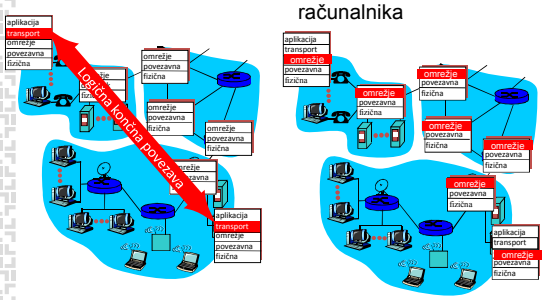
- Virtualne zveze in datagramske povezave
- Usmerjevalniki
- IP protokol: format, naslavljanje, ICMP, IPv6
- Usmerjevalni algoritmi
- Usmerjanje v Internetu, broadcast in multicast

Omrežna plast

- Omrežni protokoli so v **vsakem** računalniku in usmerjevalniku!
- NALOGE
  - Prenos segmenta od izvornega do ciljnega računalnika.
  - Pošiljatelj: enkapsulacija segmentov v IP datagrame
  - Prejemnik: izluščenje in predaja segmentov transportni palsti

Transportna in omrežna plast

- Od procesa do procesa
- Od računalnika do računalnika



Ključni funkciji

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

Model omrežnih storitev

Kaj omrežna plast lahko zagotovi transportni plasti?

- Zagotovljena dostava paketa
- Zgornje, z navzgor omejeno zakasnitvijo

Za posamezen paket

- Dostava paketov v pravem zaporedju
- Zagotovljena spodnja meja pasovne širine
- Čas med prejemom dveh paketov je le malo (navzgor omejeno) različen od časa med njuno oddajo – ***jitter***.

Za zaporedje paketov

Internet: best –effort, ni nobenih zagotovil ☹

Primer ATM: več modelov storitev

- Za različne povezave lahko vzamemo različne modele.

Omrežje	Model	Zagotavlja? Pas. širina	Izguba	Vr. red	Čas	Zamašitev-obvestilo
Internet	best effort	ne	ne	ne	ne	Ne (izguba)
ATM	CBR	Konstant.	da	da	da	Ni zamašitev
ATM	ABR	minimalna	ne	da	ne	da (CI)

Available bit rate

Constant bit rate

7

Povezavne in nepovezavne storitve

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

8

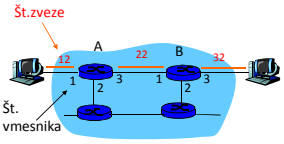
Virtualne zveze

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

9

Virtualna zveza: primer

Povezovalna tabela: usmerjevalnik ima podatke o stanju zvez – podatke, potrebne za posredovanje.



A

Vhodni vmesnik	Vhodna št.zveze	Izhodni vmesnik	Izhodna št. zveze
1	12	3	22
2	63	1	18
3	7	2	17
...	...	...	...

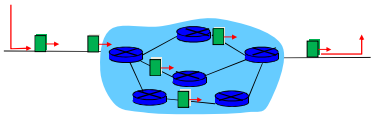
B

Vhodni vmesnik	Vhodna št.zveze	Izhodni vmesnik	Izhodna št. zveze
1	22	3	32
1	34	2	23
2	4	1	55
...	...	...	...

10

Datagramsko omrežje

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



11

Posredovalna tabela v datagramskem omrežju

- Če je 32-bitni naslov: 4 mrd. različnih naslovov!
- V tabeli uporabimo rang naslovov, npr:

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

12

Posredovalna tabela v datagramskem omrežju

- Če je 32-bitni naslov: 4 mrd. različnih naslovov!
- V tabeli uporabimo rang naslovov, npr:

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

- Ujemanje najdaljše predpone (longest prefix match)

13

Primer: ujemanje najdaljše predpone

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

Ciljni naslov	Vmesnik povezave
11001000 00010111 00010	0
11001000 00010111 00011000	1
11001000 00010111 00011	2
sicer	3

Učinkovitost: če so veliki bloki zaporednih naslovov za posamezno izhodno povezavo (krajši prefiksi, krajše tabele)

14

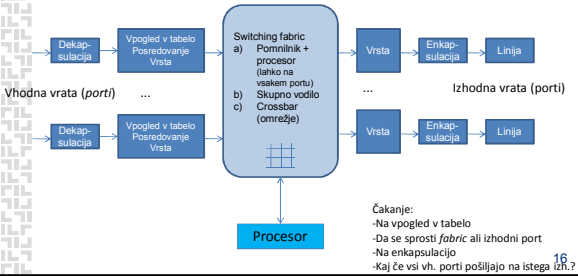
Primerjava datagramskega in omrežja z virtualnimi zvezami

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

15

Usmerjevalnik

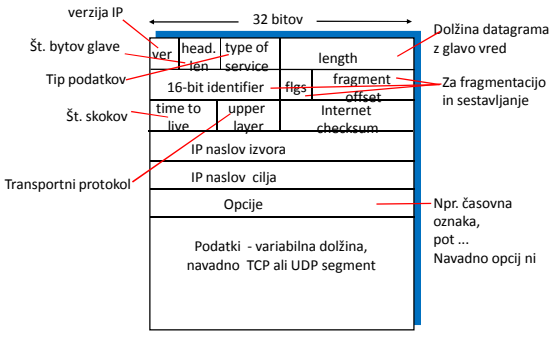
- Težava: usmerjanje (pravilno: preklapljanje!) izvajati s hitrostjo vhodne povezave.



Čakanje:
-Na vpogled v tabelo
-Da se sprosti *fabric* ali izhodni port
-Na enkapsulacijo
-Kaj če vsi vh. porti pošiljajo na istega izh.?

16

IP – internet protokol: format IPv4 datagrama



17

Režija

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

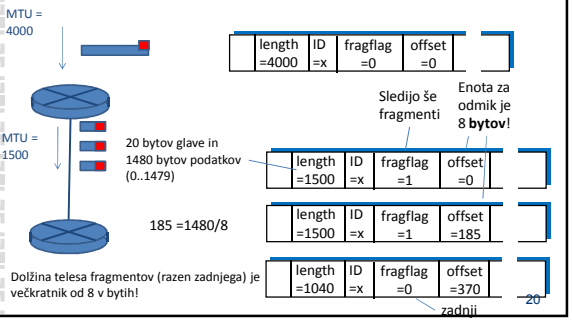
18

Fragmentacija

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

Fragmentacija: primer

- Datagram 4000 bytov, MTU 1500 bytov



Napad teardrop

- Spada med DoS napade
  - (Denial of Service – napad z onemogočanjem storitve)
- Napadalec: fragmentirani paketi z namerno napačnimi odmiki/dolžinami (prekrivanje).
- Pri sestavljanju se ciljni sistem zmede in (lahko) sesuje – napaka v kodi TCP/IP sklada!
- Občutljivi: Win 3.1, Win95, WinNT, Linux do 2.1.63

IPv4 naslavljanje

- Vmesnik: povezuje računalnik ali usmerjevalnik s fizično linijo (interface).
- IPv4 naslov je 32-bitni **ID vmesnika.**
- Koliko vmesnikov ima navadno računalnik in koliko usmerjevalnik?

Primer IPv4 naslova:

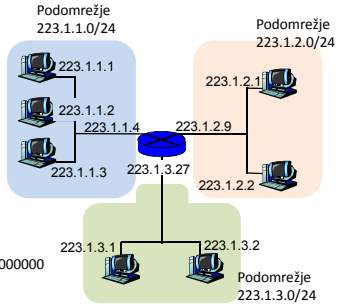
11011111 00000001 00000001 00000001

Desetiški zapis: 223.1.1.1

Podomrežje

- IP naslov: naslov omrežja | naslov naprave
- (Pod)omrežje je množica vmesnikov,
  - ki imajo enak naslov omrežja,
  - med seboj so dosegljivi brez posredovanja usmerjevalnika.
- Maska podomrežja določa dolžino naslova (pod)omrežja.
  - Maska je 32-bitni niz, ki ima enice na mestih, ki označujejo naslov omrežja, na ostalih so ničle.
  - Npr. maska /25 pomeni, da je prvih 25 bitov naslov omrežja, zadnjih (desnih) 7 pa naslov naprave.
  - Primer: 11111111 11111111 11111111 10000000 ali 255.255.255.128

Primer - naslavljanje



Usmerjevalnik ima na vsakem vmesniku drugo (pod)omrežje.

223.1.1.0/24 : levih 24 bitov (MSB) označuje naslov (prefix) omrežja, ostali naslov naprave.

Maska podomrežja /24:

11111111 11111111 11111111 00000000 oziroma 255.255.255.0

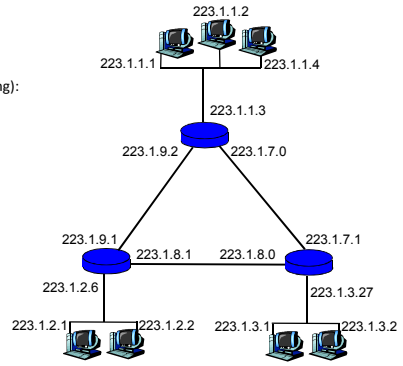
Maska je lahko poljubno dolga, npr. /17 ali /25...

Znotraj (pod)omrežja ni usmerjevalnikov, so pa lahko stikala (switch) in razdelilniki (hub).

Koliko je podomrežij?

Prefiksna ali CIDR notacija (classless inter-domain routing): 223.1.1.0/24

Broadcast naslov: same enice. Velja za omrežje in napravo. Pošilja se vsem v omrežju, usmerjevalnik ga ne posreduje naprej. 233.1.1.255 255.255.255.255



25

Dodeljevanje IP naslovov

- Naprava:
  - Administrator vpiše naslov (fiksen) ali
  - DHCP strežnik dodeli naslov (dinamičen)
- Omrežje podjetja:
  - Ponudnik dostopa do interneta (ISP) dodeli del svojega naslovnega prostora.

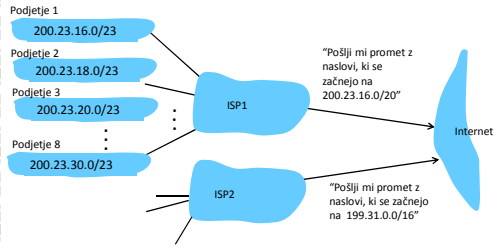
ISP-jev blok:	11001000 00010111 00010000 00000000	200.23.16.0/20
Podjetje1:	11001000 00010111 00010000 00000000	200.23.16.0/23
Podjetje2:	11001000 00010111 00010100 00000000	200.23.18.0/23
…	…	…

- ISP: ICANN dodeli naslovni prostor
  - Internet Corporation for Assigned Names and Numbers, www.icann.org

26

Hierarhično naslavljanje

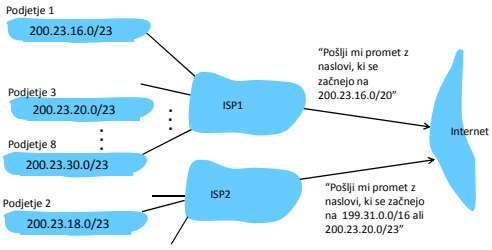
Pravilno dodeljevanje CIDR naslovov olajša usmerjanje!
Agregiranje ali sumarizacija naslovov – en prefiks za usmerjanje v več omrežij.



27

Manj učinkovito naslavljanje

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



28

NAT – Network Address Translation (RFC 2663,3022)

- Pomanjkanje IPv4 naslovnega prostora
- Zasebni naslovni prostor, RFC 1918

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

- Zasebni (notranji, interni) naslovi se uporabljajo le znotraj omrežja.
- Na NAT usmerjevalniku se naslov preslika v zunanji naslov.

29

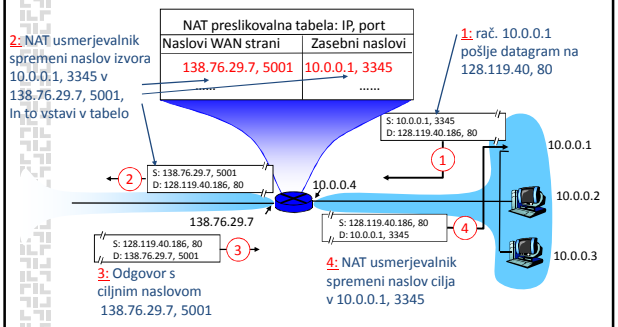
NAT - možnosti

- N notranjih, N zunanjih naslovov
- N notranjih, M zunanjih naslovov, M<N
- N notranjih, 1 zunanji naslov (npr. domača omrežja) : NAT usmerjevalnik in celo omrežje za njim navzven izgleda kot ena naprava.

- NAT usmerjevalnik:
  - Zamenja naslov izhodnega datagrama
  - Zapomni si preslikavo (par notranji + zunanji naslov)
  - Zamenja naslov vhodnega datagrama

30

NAT/PAT



Kritika NAT-a

- Usmerjevalniki – 3.plast: naj ne bi imeli opravka s 4. plastjo (porti)!!!
- Port je namenjen za naslavljanje procesov, ne računalnikov.
- Težava s strežniki na notranji strani (poslušajo na dogovorjenih vratih – well known port).
- Pomanjkanje naslovov: raje uporabi IPv6!
- Krši end-to-end argument (za aplikacije naj bi bilo omrežje transparentno): npr. P2P načrtovalci morajo programirati tudi za primer NATa.
- Peer B za NAT-om ne more sprejemati povezav, ker nima fiksnega naslova in ga ne more objaviti. Lahko le sam zahteva povezave. Težava, če sta oba za NAT-om!
  - *Connection reversal*: Peer A se poveže z B prek C-ja, s katerim ima B trenutno aktivno povezavo, in ga prosi, naj B vzpostavi povezavo z A.

ICMP (RFC 792)

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

ICMP sporočila

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

Traceroute

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

IPv6

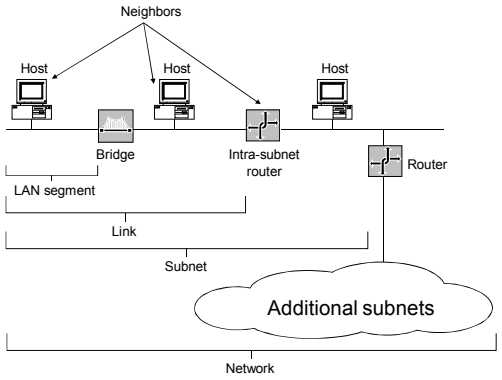
- Motivacija:
  - večji naslovni prostor je potreben – 128 bitov
  - Format glave – hitrejše usmerjanje
  - Glava – omogoča QoS
- Ipv6 datagram:
  - Fiksna glava 40 bytov
  - Fragmentacija ni dovoljena

Prednosti IPv6

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

37

IP v6 terminologija



38

Naslovni prostor IPv6

- 128-bitni naslovni prostor
  - 340,282,366,920,938,463,463,374,607,431,768,211,456 naslovov (3.4×10^{38})
  - 6.65×10^{23} naslovov na m^2 zemljine površine !!!
- Zato imamo lahko fleksibilno večnivojsko hierarhijo (naslavljanje, usmerjanje)
- Tipičen unicast naslov:
  - 64 bitov: ID podomrežja
  - 64 bitov: ID vmesnika

39

Sintaksa IPv6 naslova

- IPv6 naslov v binarni obliki :

  `0010000111011010000000001101001100000000000000000101111001111011`
  `0000001010101010000000001111111111111111000101000100111000101101O`

- Razdeljen na osem 16-bitnih skupin:

  `0010000111011010  0000000011010011  0000000000000000  0010111100111011`
  `0000001010101010  0000000011111111  1111111000101000  1001110001011010`

- Zapisan šestnajstiško, ločeno z dvopičji
  21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
- Vodilne ničle v vsaki skupini lahko izpustimo:
  21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

40

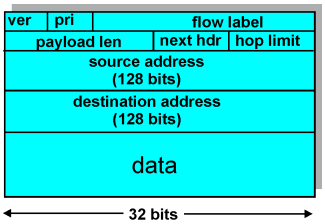
Kompresija ničel v zapisu naslova

- Dolga zaporedja samih ničel
- Zaporedje 16-bitnih blokov iz samih ničel lahko zapišemo kot dve dvopičji ::
- Primer
  - FE80:0:0:0:2AA:FF:FE9A:4CA2 ali krajše FE80::2AA:FF:FE9A:4CA2
  - FF02:0:0:0:0:0:0:2 ali krajše FF02::2
- To ne velja za dele blokov – cel blok mora biti 0
  - FF02:30:0:0:0:0:0:5 ni isto kot FF02:3::5,
  - lahko pa zapišemo FF02:30::5.
- Kompatibilnost z v4 naslovi: spredaj dodamo ničle
  - 193.2.72.1 → ::193.2.72.1
  - Lahko pustimo tudi pike iz v4 naslova!

41

IPv6 format datagrama

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



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

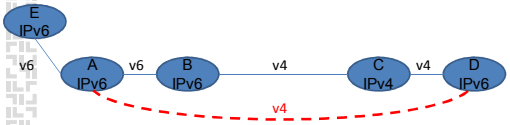
ICMP v6 – dodatne funkcije, npr. sporočilo Packet Too Big.

42

Prehod IPv4 – IPv6

Ne bo se zgodil čez noč!

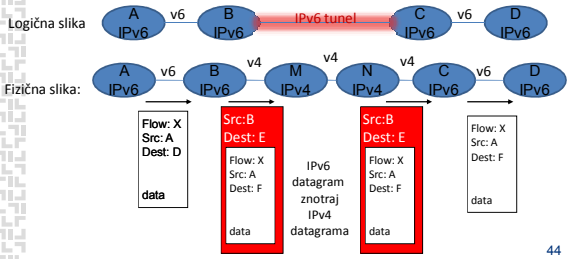
- Dual-stack: usmerjevalnik pozna v4 in v6. Z v6-enabled "govori" v6, z ostalimi pa v4.
  - Kako to ugotovi? DNS vrne v6 ali v4 naslov. DNS mora biti že na v6!
  - Če je na poti med dvema v6 vozliščema kakšno v4, se bo promet vmes pretvarjal v v4; v6-specifična polja se bodo izgubila!



43

Prehod IPv4-IPv6

- Tuneliranje: IPv6 datagram zapakiramo v enega ali več IPv4 datagramov kot podatke.



44

Usmerjanje

- Abstraktni model:
  - teorija grafov, vozlišča, povezave.
- Algoritmi za iskanje najkrajše (najcenejše) poti
  - to je naloga usmerjevalnih algoritmov.

45

Principi

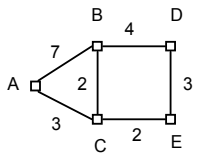
- Statično (neadaptivno) ali dinamično (adaptivno)
  - ali upošteva trenutne razmere v omrežju in jim prilagaja usmerjanje prometa?
- Po eni poti ali po več poteh
  - ali gredo v nekem trenutku vsi paketi z istim ciljem po isti poti?
- Globalno (centralizirano) ali porazdeljeno
  - Ali so pri izračunu poti znani podatki za celo omrežje?
- Možne so vse kombinacije.
- OPTIMALNO usmerjanje: enakomerno obremenjene povezave.
  - Vsebovanost krajših optimalnih poti v daljši
  - Drevo ponora (sink tree)

46

Usmerjanje po najkrajši poti

Glede na

- čas,
- ceno,
- število skokov...

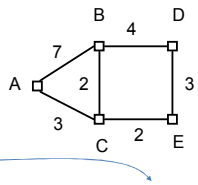


47

Usmerjanje po najkrajši poti

Glede na

- čas,
- ceno,
- število skokov...



Usmerjevalna tabela za vozlišče A
-zakasnitev
-št. skokov

- statično
- po eni poti

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

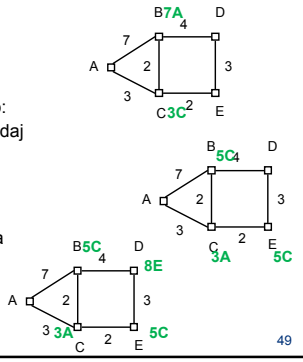
AB	ACB (5)
AC	AC (3)
AD	ACED (8)
AE	ACE (5)

48

Usmerjanje po najkrajši poti: Dijkstrin algoritem za iskanje najkr. poti

Iščemo pot A-E.

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



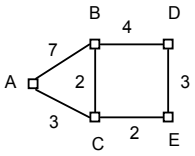
49

Usmerjanje po več poteh

- Določen delež paketov za vsako izmed možnih poti.
- Ponekod je lahko možna le ena pot.
- Paketi lahko blodijo – preprečiti!

Usmerjevalna tabela za vozlišče A:

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



- statično
- po več poteh

50

Centralizirano usmerjanje

- Glavno vozlišče (*master, koordinator*)
- Zbira podatke o razmerah v omrežju
- Izračuna tabele in jih razpošlje
- Alternativa: vsi razpošiljajo podatke, vsak zae izračunava globalno usmerjanje (link state routing)
- TEŽAVA: velika omrežja s hitrimi spremembami

- dinamično
- lahko po eni ali po več poteh

51

Izolirano usmerjanje

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

52

Porazdeljeno usmerjanje

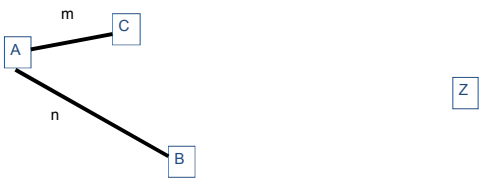
- Vsako vozlišče pozna razdaljo do svojih sosedov.
- Vsakih T čas. enot si izmenjajo usmerjevalne tabele.
- Potem pregledajo in prilagodijo svoje tabele.

- Lastnosti:
  - Dobre novice se širijo hitro, slabe počasi (počasi konvergira).
  - Problem štetja do neskončnosti.

53

Porazdeljeno usmerjanje

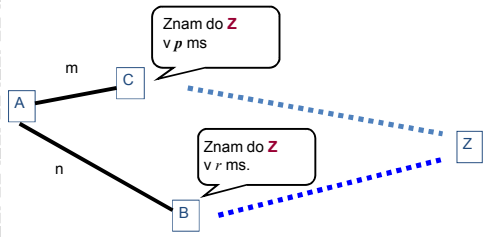
Vozlišče A pozna razdaljo (čas) do C in B.



54

Porazdeljeno usmerjanje

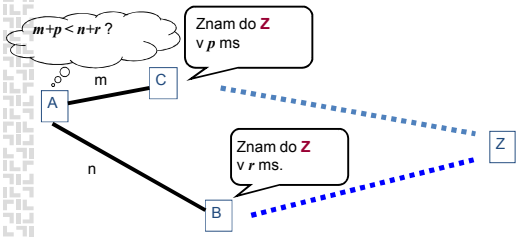
Vozlišče A pozna razdaljo (čas) do C in B.



55

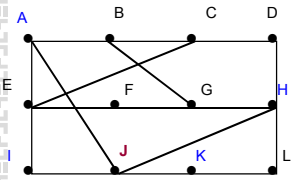
Porazdeljeno usmerjanje

Vozlišče A pozna razdaljo (čas) do C in B.



56

Porazdeljeno usmerjanje



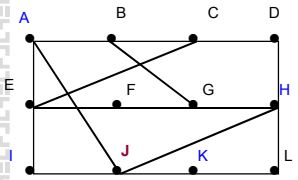
JA: 8 JH: 12

JI: 10 JK: 6

57

Porazdeljeno usmerjanje

J dobi tabele od sosedov. Poišči njegovo novo tabelo!



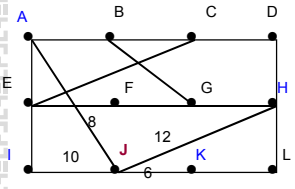
JA: 8 JH: 12

JI: 10 JK: 6

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

58

Porazdeljeno usmerjanje -rešitev



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

Kaj če se ob naslednji izmenjavi podatki od sosedov spremenijo?
•Daljši čas (ali pretrgana pov.)
•Krajši čas
Vnos zamenjamo, če najdemo boljšo pot.

59

Porazdeljeno usmerjanje ali usmerjanje z vektorjem razdalj

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

60

Usmerjanje glede na stanje povezav

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

- **V praksi**: OSPF; IS-IS (interdomain).

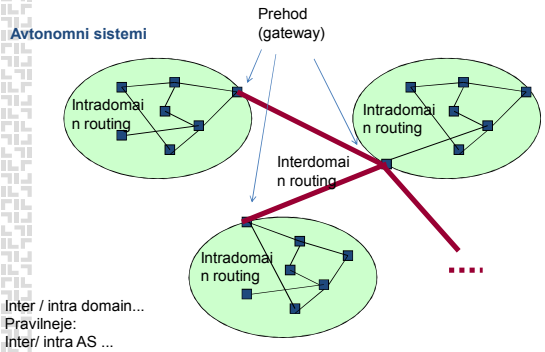
61

Usmerjanje v internetu

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

62

Internet



Inter / intra domain...
Pravilneje:
Inter/ intra AS ...

63

Usmerjanje med avtonomnimi sistemi

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

64

Usmerjanje iz AS

- Če je v AS le en prehod:
  - promet, namenjen iz AS, se usmerja na ta prehod
- Če je več kot en prehod:
  - Na katerega naj se usmerja promet, namenjen iz AS?

1. Usmerjevalnik ugotovi, da je več prehodov do X.
2. Iz intra-AS ugotovi, do katerega prehoda pride najceneje
3. Hot potato: promet usmeri na najcenejšega
4. Doda ta podatek v svojo posredovalno tabelo

65

BGP

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

66

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Transportna plast

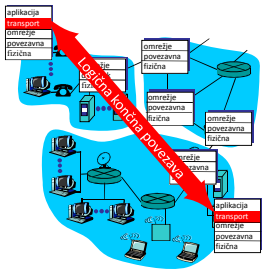
Pregled

- Storitve transportne plasti
- (De-)multipleksiranje
- UDP
- TCP in zanesljiv prenos
- TCP in nadzor zamašitev (zasičenje - congestion control)

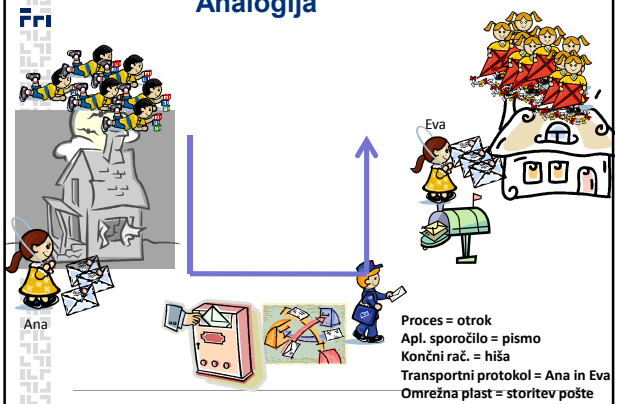
Transportne storitve in protokoli

- Logična komunikacija med aplikacijskimi procesi
- Transportni procesi tečejo v KONČNIH sistemih
- Naloga:
  - Sprejem sporočila od aplikacije
  - Sporočilo -> segmenti -> omrežna plast
  - Sprejem PDUjev od omrežne plasti
  - Sestavljenje segmentov v sporočilo
  - Predaja aplikacijski plasti
- Internet: ni zagotovitve pasovne širine ali zakasnitve
  - TCP (vzp. povezave, kontrola pretoka in zamašitev)
  - UDP (best effort)

Logična povezava



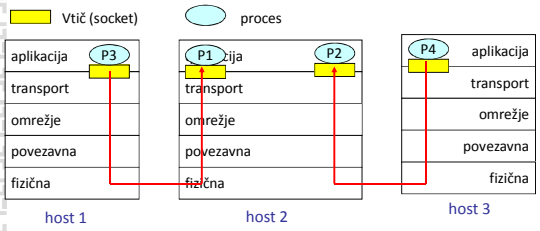
Analogija



Proces = otrok
Apl. sporočilo = pismo
Končni rač. = hiša
Transportni protokol = Ana in Eva
Omrežna plast = storitev pošte

(De-)multipleksiranje – kaj je?

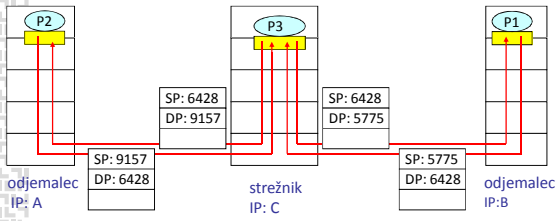
- Pošiljatelj: pobira iz več vtičev, doda glavo
- Sprejemnik: segmente razdeli ustreznim vtičem



(De-)multipleksiranje – kako?

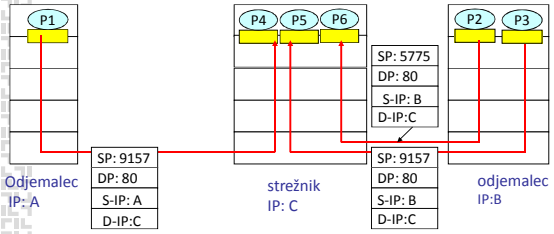
- IP datagram: IP naslova izvora in ponora
  - nosi en transportni segment
- Transportni segment: št. Vrat izvora in ponora
- Ciljni računalnik:
  - IP naslov + številka vrat → ugotovi pravi socket
- UDP vtič določen s parom: (dest IP, dest port)
  - Lahko sprejema iz različnih IP naslovov ali vrat
- TCP vtič: (source IP, source port, dest IP, dest port)
  - En proces ima lahko več vtičev

Nepovezavno demux.-primer

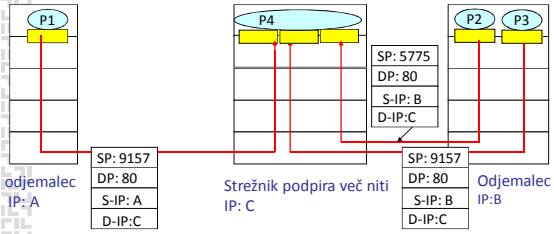


SP = source port (predstavlja naslov za odgovor)
DP = destination port

Povezavno demux.-primer



Povezavno demux.- primer z nitmi



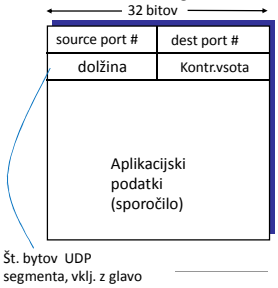
UDP – User Datagram Protocol

- RFC 768 - minimalna funkcionalnost
- Storitev po najboljših močeh (best effort):
  - Možno izgubljanje, napačen vrstni red
- Nepovezavni: ni rokovanja, vsak datagram potuje posebej (UDP segment = datagram)
- Prednosti:
  - Ni zakasnitve rokovanja
  - Preprost, ni treba vzdrževati stanja (obe strani)
  - Majhna glava
  - Ni kontrole zamašitev – lahko hitro oddaja

UDP

- Uporaba: večpredstavnost
  - Tolerira izgube
  - Hitrost!
- DNS, SNMP
- Zanesljiv prenos:
  - Zanesljivost se zagotovi na apl. plasti

UDP: format datagrama



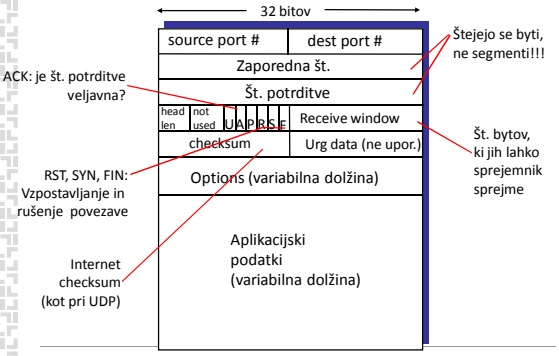
Zanesljiv prenos podatkov (potrjevanje)

- Zanesljiv kanal (ni pokvarjenih, izgubljenih pak.)
- Nezanesljiv kanal
  - ACK, NACK, detekcija napak
  - Izguba, okvara ACK, NACK
  - Zap. št. paketov, duplikati
  - Časovne kontrole
  - Stop and wait (sprotno)
  - Go-back-N, selective repeat: tekoče
  - NACK-free protokol: namesto NACK pošlje ACK za zadnjega pravilnega (ACK5, ACK5 velja kot NACK6)

TCP

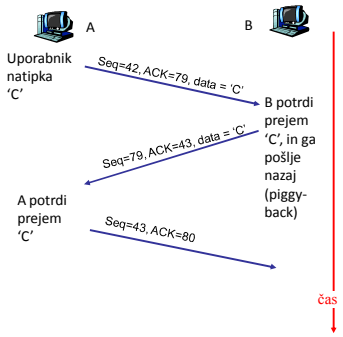
- RFC 793, 1122, 1323, 2018, 2581
- Lastnosti
  - En sprejemnik, en oddajnik
  - Zanesljiv, urejen tok
  - Sprejemni in oddajni "TCP bufferji"
  - "cev" od izvora do ponora, nadzor pretoka in zamašitev
  - Oddajnik ne "zasuje" sprejemnika
  - Full duplex, max. velikost segmenta
  - Povezavno usmerjen (rokovanje)

TCP segment



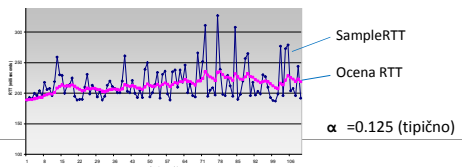
Primer

- Delček telnet seje: strežnik vrača vtipkane črke nazaj, šele potem jih uporabnik vidi na zaslonu.



Čas vrnitve

- Čas vrnitve - RTT (Round trip time)
- Interval za časovno kontrolo > povprečni RTT !
- TCP meri čas do ACK (SampleRTT) in računa gibajoče povprečje.
- **`Ocena RTT' = OcenaRTT(1-α) + α*SampleRTT`**



Interval za časovno kontrolo

- Če čas vrnitve bolj niha, naj bo večja 'rezerva'.

```
OdmikRTT' = (1 - β) OdmikRTT +
            β * |SampleRTT - OcenaRTT|
```

β = 0.25 (tipično)

```
TimeoutInterval = OcenaRTT + 4*OdmikRTT
```

- **Fast retransmit**: ponovna oddaja segmenta preden poteče časovna kontrola, če dobi 3x ACK za isti segment.

TCP: zanesljiv prenos

ACK (posredno), časovne kontrole, tekoče pošiljanje

osnova = začetna zap. št. ; *nasl* = začetna zap.št.

Če sprejme podatke od aplikacije:

- Naredi TCP segment *nasl*, sproži timer
- Segment preda IP-ju, *nasl* = *nasl* + dolžina podatkov

Če poteče timer za segment y

- Ponovno odda segment y
- sproži timer

Če sprejme potrditev za segment y

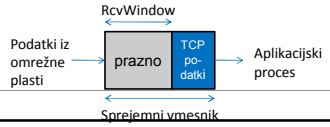
- Če y > *osnova*: /* potrditev zaporedja do vklj.y */
  Zbriši timer za segmente y < *nasl*; *osnova* = y
- Sicer /* duplikat že prejete potrditve */
  poveča števec duplikatov ACK za y; če je ta že = 3, ponovi segment y in ponastavi timer zanj
  /* to je TCP fast retransmit*/

TCP potrditve (RFC 1122, 2581)

Dogodek pri sprejemniku	Odziv sprejemnika
Sprejem naslednjega segmenta, prejšnji že potrjen	Zakasnjen ACK. Po max. 500 ms potrdi, če ni nasl. sprejema.
Isto, a prejšnji nepotrjen.	Kumulativni ACK – potrdi oba.
Sprejem segmenta s previsoko št. (vrzel!)	Takoj potrdi zadnji v zaporedju sprejeti segment (pošlje duplikat).
Sprejem segmenta z najnižjo številko iz vrzeli (polnjenje vrzeli)	Takoj potrdi segment.

TCP: kontrola pretoka

- Aplikacija bere iz sprejemnega vmesnika (receive buffer) – lahko počasi.
- Prejemnik:
  - **RcvWindow** polje v glavi segmenta: sem vpiše količino praznega prosotora v spr. Vmesniku
- Pošiljatelj nastavi širino okna na **RcvWindow**



TCP: vzpostavljanje povezave

Trojno rokovanje (three-way handshake)

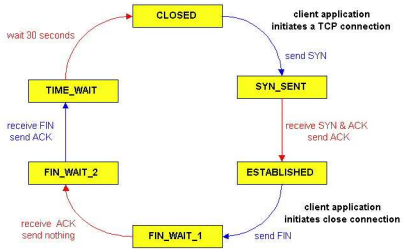
1. Odjemalec pošlje TCP SYN segment
   - Začetna št. odj. segmenta, brez podatkov
2. Strežnik vrne SYNACK segment
   - Začetna št. str. segmenta; alocira buffer
3. Odjemalec vrne ACK, lahko že s podatki

TCP: rušenje povezave

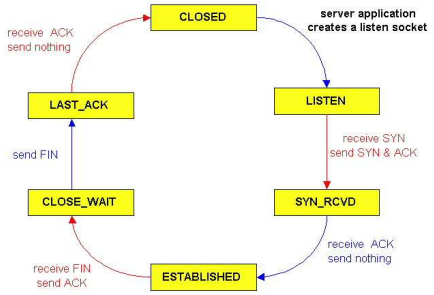
Odjemalec zapre socket:

1. Odjemalec pošlje TCP FIN segment.
2. Strežnik potrdi z ACK, zapre pov., pošlje FIN.
3. Odjemalec potrdi FIN z ACK.
   - Čaka kratek čas; če sprejme FIN, potrdi z ACK.
4. Strežnik sprejme ACK, končano.

Življenski cikel odjemalca



Življenjski cikel strežnika

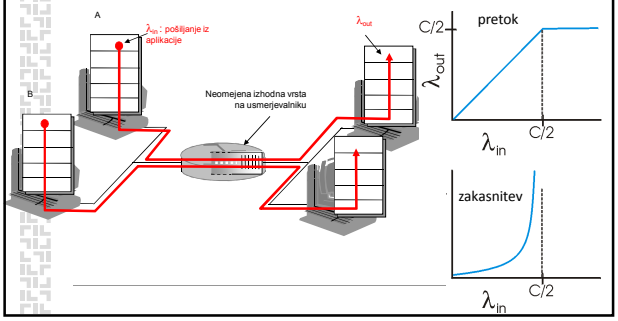


Nadzor zamašitev (congestion)

- Ni isto kot nadzor pretoka!
- Zamašitev: preveč virov naenkrat pošilja preveč podatkov (prehitro) za dano omrežje.
- Posledica:
  - izguba segmentov (prelivi),
  - velike zakasnitve (dolge vrste na usmerjevalnikih)

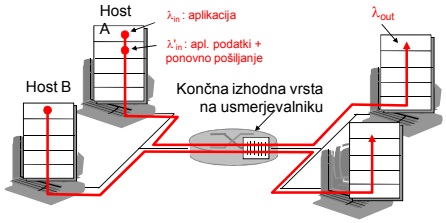
Zamašitev – primer 1

- Dva pošiljatelja, neskončna vrsta



Zamašitev – primer 2

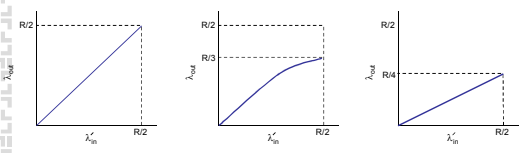
- Končna vrsta in ponovna pošiljanja segmentov



Zamašitev – primer 2

a. Če bi vedeli, kdaj je prostor v vrsti, ne bi bilo izgub: segment oddamo le, ko je prostor (ni možno v praksi)
b. Dogajajo se izgube paketov in ponovna pošiljanja
c. ponovna pošiljanja tudi zaradi velikih zakasnitev

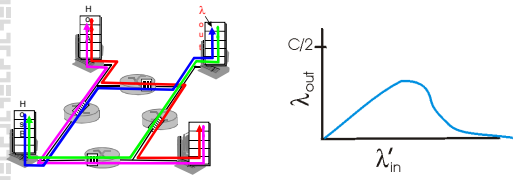
Več dela omrežja za manjši učinek. Nepotrebne ponovitve.



a. b. c.

Zamašitev – primer 3

- Daljše poti: če se paket izgubi na *n*-tem skoku, so bili zaman vsi dotedanji prenosi!



Nadzor zamašitev - pristopi

1. TCP: Odvisno le od **končnih sistemov**: opazijo izgubo ali zakasnitve.
2. Lahko pa pomaga tudi **omrežje**:
   - Usmerjevalnik nastavi kak bit (SNA, DECnet, ATM)
   - Usmerjevalnik sproči sprejemljivo hitrost oddajanja

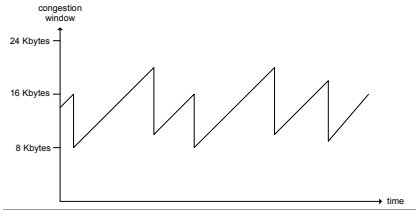
- Primer ATM: kontrolna RM celica (resource mgmt.)
  - Pošiljatelj jih oddaja med podatkovnimi
  - ATM stikalo lahko nastavi NI (no increase – ne povečuj prometa) ali CI (congestion indication – zmanjšaj) bit
  - Prejemnik vrne RM celice nespremenjene oddajniku

TCP: nadzor zamašitev

- Dinamični vrednosti **`CongWin`** (zamašitveno okno) in **`treshold`** – prag.
- Hitrost pošiljanja ≈ **`CongWin/RTT`** bytov/s
- Pošiljatelj: izguba (č.k. ali 3 duplikati ACK) → zmanjša **`CongWin`**

TCP AIMD

- Additive Increase: CongWin se vsak RTT poveča za 1 max. velikost segmenta, če ni napak.
- Multiplicative Decrease: ob izgubi (3 duplikati ACK) zamašitveno okno prepolovimo.



Žagasta oblika

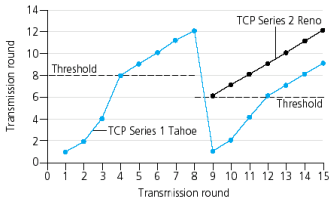
Počasen začetek – TCP Slow Start

- Ob vzpostavitvi povezave: **`CongWin`** = 1 segment
  - Primer: če MSS = 500 bytov in RTT = 100 ms, potem je začetna hitrost 39 kbps.
- Povečuj hitrost eksponentno (**`CongWin`***2 vsak RTT – ob prejemu ACK) do prve izgube (tu nastavi **prag**)

Nadaljnja izboljšava:

- Po treh duplikatih ACK razpolovi **`CongWin`**, okno nato povečuj linearno (za 1) – cong. avoidance
- Po timeoutu postavi **`CongWin`** = 1 , nato naj raste eksponentno do praga (slow start), nato linearno.

TCP različice

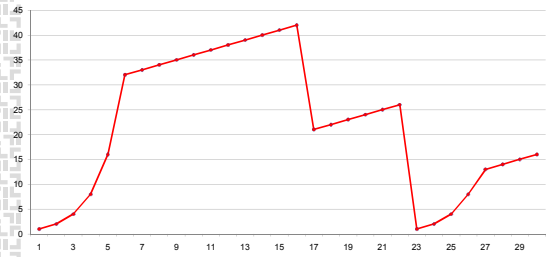


- TCP Tahoe: osnovna verzija
- TCP Reno: ni toliko čakanja po č.k. – *fast recovery:* preskoči *slow start* fazo. Ima tudi fast retransmit.
- TCP Vegas: izogibanje zamašitvam – ko se RTT poveča, se zmanjša **`CongWin`**.

Povzetek nadzora zamašitev

- **`CongWin`** < prag: slow start (eksponentna rast)
- **`CongWin`** > prag: congestion avoidance (linearna rast)
- 3 duplikati ACK:
  prag = **`CongWin`**/2, **`CongWin`** = prag.
- Timeout: Prag = **`CongWin`**/2, **`CongWin`** = 1

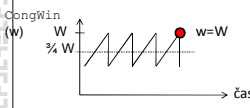
Primer: TCP Reno



Kdaj je počasen začetek in kdaj izogibanje zamašitvam?
Kdaj so bili 3 duplikati ACK in kdaj timeout?
Kakšen je bil prag na začetku, kakšen ob T=18, in T=24?
Kdaj je bil poslan 70. segment?
Če bi pri T=26 imeli 3 duplikate ACK, kako bi določili prag in CongWin?

Kakšen je povprečen pretok?

- Pretok = CongWin/RTT



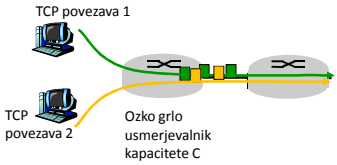
- Predpostavimo: W in RTT sta ~ konstantna. Potem pretok niha med W/(2 RTT) in W/RTT.
- Povprečen pretok = ¾ W/RTT

Primer

- Max. segment (MSS) = 1500 bytov
- RTT = 100 ms
- Če želimo 10 Gb/s pretoka: **`CongWin`** mora biti povprečno 83!
- Možno je izračunati, da za ta pretok lahko izgubimo le $2*10^{-10}$ segmentov!

Je TCP pravičen?

- Cilj: Vsaka od N TCP sej po isti povezavi s kapaciteto C naj bi dobila C/N .



Pravičen ?

- TCP sam: DA
- Več paralelnih TCP povezav za isto aplikacijo in ena povezava za drugo aplikacijo: z vidika aplikacije NI pravičen
- UDP in TCP po istem omrežju: ni pravično do TCP (UDP pošilja brez omejitev pretoka)

Sklep

- Principi za transportnimi storitvami
  - (de)multipleksiranje
  - Zanesljiv prenos
  - Kontrola pretoka in zamašitev
- TCP in UDP

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Aplikacijska plast

Omrežne aplikacije so razlog za obstoj omrežij!

Omrežne aplikacije

- 80. leta: tekstovne (e-pošta, oddaljen dostop, prenos datotek, novice, klepet)
- Sredi 90. let: aplikacija SPLET
- Večpredstavne aplikacije: pretočni video, spletni radio, spletni telefon, video konference...
- Večuporabniške omrežne igre
- Okrog 2000: IM (takojšnje sporočanje) in P2P izmenjava datotek
- Kaj je "*killer*" aplikacija?

Temeljna načela omrežnih aplikacij

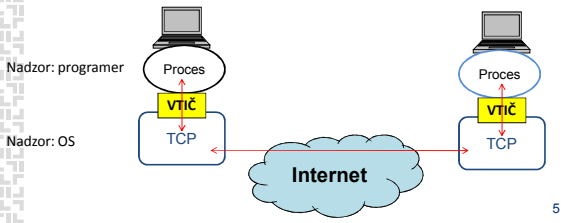
- Teče na več **končnih** napravah
- Več (različnih?) programov / procesov
- Primera:
  - spletni strežnik in odjemalec: strežnik ves čas dostopen, lahko farma; znan naslov. Odjemalci so lahko nedostopni, med sabo direktno ne komunicirajo.
  - P2P: člani so lahko nedostopni. Robustnost, skalabilnost. Hibridni pristop. Upravljanje je težko.

Komunikacija med procesi

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

Vtiči (socket)

- Vtič je vstopna točka v proces.
- Vtič je **vmesnik** (API) med aplikacijsko in transportno plastjo.



Kako nasloviti proces na drugi strani?

- **Naslov naprave** (host address): IP številka
- **Naslov procesa** (znotraj naprave): številka vrat
- Znane aplikacije uporabljajo znane številke vrat 0-1023 (t.i. *well-known port*), npr.
  - Spletni strežnik: 80
  - Poštni strežnik SMTP: 25
  - Imenski strežnik: 53
  - IRC strežnik: 194
- Več: `www.iana.org`

Protokoli aplikacijske plasti

- Protokol določa **pravila za izmenjavo sporočil**.
  - Vrste sporočil (npr. zahteva, odgovor, potrditev...)
  - Zgradbo sporočila (polja, meje med polji...)
  - Pomen sporočila (kaj je v nekem polju)
  - Kdaj in kako proces oddaja sporočila in kako reagira na prejeta sporočila
- Javni (odprti) protokoli, npr. HTTP (RFC 2616)
  - Specifikacije (RFC): www.ietf.org
- Lastniški (zaprti) protokoli, npr. Skype

7

Kaj potrebuje aplikacija?

- Kako izbrati transportni protokol?
  - Kaj nudi TCP in kaj UDP?
  - Vlak ali letalo? Avtobus ali kolo?
- Bistveno
  - Zanesljiv prenos podatkov ali tolerira izgubo?
  - Zagotovljeno pasovno širino? (aplikacije, občutljive na pasovno širino / elastične aplikacije)
  - Čas: omejena ali neomejena zakasnitev

8

Dopolnite...

Aplikacija	Izguba	Pasovna širina	Časovna občutljivost
Prenos datotek			
E-pošta			
Zvok/ slika v realnem času		Zvok: nekaj kb/s- 1Mb/s Slika: 10kb/s – 5 Mb/s	Nekaj 100 ms
Shranjen zvok/ slika			
Interaktivne igre			
IM			

9

Dopolnite...

Aplikacija	Izguba	Pasovna širina	Časovna občutljivost
Prenos datotek	NE	Elastična	NE
E-pošta	NE	Elastična	NE
Zvok/ slika v realnem času	DA	Zvok: nekaj kb/s- 1Mb/s Slika: 10kb/s – 5 Mb/s	Nekaj 100 ms
Shranjen zvok/ slika	DA	-II-	Nekaj s
Interaktivne igre	? (DA)	1-10 kb/s	Nekaj 100 ms
IM	NE	Elastična	? (DA)

10

Storitve TCP-ja

- Povezana storitev *(povezavno usmerjena, connection-oriented)*
  - 1.faza - handshaking: vzpostavljanje TCP povezave (kontrolna sporočila)
  - 2.faza – prenos aplikacijskih sporočil, popolnoma dvosmerna povezava
  - 3.faza – rušenje povezave
- Zanesljiv prenos: brez napak, v pravem zaporedju.
- Nadzor zamašitev *(congestion control)*
- NE zagotavlja kapacitete ali zg. meje zakasnitve.

11

Storitve UDP-ja

- Hiter, učinkovit, lahek, minimalističen
- Nepovezaven – brez “rokovanja”
- Ni garancije dostave, ne zagotavlja vrstnega reda
- Nima nadzora zamašitev

12

Uporaba

- **TCP**: SMTP, Telnet, HTTP, FTP, ...
- **UDP ali TCP**: SIP, pretočne aplikacije,..
- **Tipično UDP**: DNS, SNMP, RIP (usmerjanje), telefon (zaprti protokoli)...

13

Splet in HTTP

- Kar hočeš, kadar hočeš – na zahtevo.
- Specifikaciji
  - RFC 1945 (HTTP 1.0),
  - RFC 2616 (HTTP 1.1)
- Odjemalec: http zahteva (request) gre prek vtiča (socket interface) v transportni sistem.
- Strežnik: http odgovor (response).
- TCP poskrbi za potrditve, ponovitve, vrstni red.
- Protokol brez stanj (stateless).

14

HTTP povezave

- Nonpersistent (minljive, ne trajne):
  - Za vsak objekt se vzpostavi nova TCP povezava (zamudno zaradi rokovanja, obremenjuje strežnik)
- Persistent (trajne):
  - Strežnik pusti po pošiljanju povezavo še odprto, po njej lahko pošlje še več datotek
    - Brez cevovodov: odjemalec da novo zahtevo, ko prejme prejšnji objekt
    - S cevovodi: odjemalec da novo zahtevo, ko naleti na referenco na nov objekt (privzeti način).

15

Format sporočila: zahteva

```
Metoda URL Verzija
Ime polja: vrednost
...
Ime polja: vrednost
[prazna vrstica]
TELO
```

Statusna vrstica

Vrstice glave (header lines)

```
GET /sem/ocene.htm HTTP/1.1
Host: marvin.fri.uni-lj.si
Connection: close
...
```

16

HTTP zahteva - metode

- GET: zahteva objekta
- POST: zahteva objekta + deli objekta imajo poslane vrednosti (html forms)
- Obrazec lahko uporabi tudi metodo GET, vrednosti parametrov pa pošilja kot podaljšan naslov (`www.google.si/search?q=html`)
- HEAD: zahteva za HTTP odgovor, vendar brez zahtevanega objekta (razhroščevanje)
- PUT (HTTP 1.1) – upload na strežnik
- DELETE (HTTP 1.1) – brisanje s strežnika

17

Format sporočila: odgovor

```
Verzija Status Opis
Ime polja: vrednost
...
Ime polja: vrednost
[prazna vrsta]
TELO
```

Statusna vrstica

Vrstice glave (header lines)

```
HTTP/1.1 200 OK
Connection: close
Date: Mon, 05 Nov 2007 12:18:23 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: ...
Content-Length: 6534
Content-Type: text/html
```

18

HTTP status

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

19

HTTP vrstice glave

- Odjemalec: glava zahteve - odvisne so od
  - Odjemalca
  - Verzije HTTP
  - Jezika ...
- Strežnik: glava odgovora - odvisne so od
  - Zahteve
  - Verzije
  - Konfiguracije strežnika ...

20

Piškotki

- Specifikacija RFC 2109
- Strežnik brez piškotkov ne loči zahtev različnih odjemalcev.
- Sestavni deli
  - Piškotkova vrstica v glavi zahteve
  - Piškotkova vrstica v glavi odgovora
  - Odjemalčeva datoteka piškotkov
  - Strežnikova zaledna podatkovna zbirka

21

Scenarij uporabe

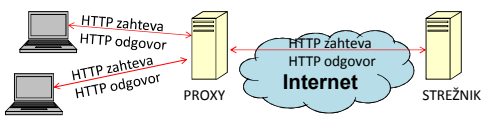
- Odjemalec: HTTP zahteva brez piškotkove vrstice
- HTTP odgovor z vrstico `Set-cookie:1234567` (ID)
- Odjemalec: dopolni datoteko piškotkov in vse naslednje zahteve s piškotkovo vrstico.
- Strežnik shranjuje podatke o uporabniku...

- Nad plastjo HTTP (brez stanj) se ustvari sejna plast (s stanji).
- Bogatejša uporabniška izkušnja, sporno glede zasebnosti.

22

Posredniški strežnik

- Web cache, proxy server (navadno pri ISP-ju)
- Odgovarja na zahteve namesto strežnikov.
- Ima svoje kopije spletnih strani (samo sveže).
- Ustrezno konfiguriran odjemalec!
- Če proxy strani nima pri sebi, jo zahteva od pravega strežnika.



23

Zakaj posredniki?

- Manj prometa
- Hitrejši odgovor odjemalcu
- Ozka grla

- Pogojna zahteva (je pomnjena stran zastarela?)
  - metoda **Conditional GET**
  - vrstica glave:
    `If-modified-since: Wed, 31 Oct 2007 09:32:22`
  - Strežnik pošlje novo stran ali
    `HTTP/1.1 304 Not Modified` (prazno telo)

24

Prenos datotek - FTP

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

25

FTP: sporočila

- RFC 959. Nadzorna povezava: 7-bitni ASCII
- Ukazi

  `USER ime; PASS geslo; LIST`

  `RETR ime_dat` (retireve = get)

  `STOR ime_dat` (store = put)
- (Nekateri) odgovori strežnika

  331 Username OK, password required

  125 Data connection open, transfer starting

  452 Error writing file

  425 Can't open data connection

26

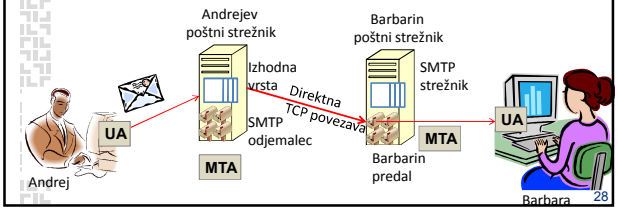
Elektronska pošta

- Poštni strežniki
  - Poštni predali (vhodna pošta)
  - Izhodna vrsta sporočil
- Odjemalski programi (UA): tekstovni, grafični
- Protokol za prenos sporočil (SMTP)
- Pošiljatelj – pošiljateljev UA – pošiljateljev strežnik – prejemnikov strežnik – prejemnikov UA – prejemnik.
- Kaj če pošiljateljev strežnik ni dosegljiv?

27

SMTP

- RFC 2821. Protokol je star več kot 30 let!
- 7-bitni ASCII (tudi za telo sporočila)
- Binarne priponke je potrebno prekodirati v ASCII. In na prejemni strani nazaj v binarno.



28

SMTP

- Odjemalec: SMTP strežnik, ki pošilja sporočilo
- Strežnik: SMTP strežnik, ki sprejema sporočilo
- Povezava na vrata 25

1. Aplikacijsko rokovanje
   - Medsebojna predstavitev
   - Odjemalec: e-mail naslov pošiljatelja in prejemnika
2. Prenos sporočila (lahko več po isti povezavi)
3. Rušenje TCP povezave

29

Primer - SMTP ukazi

```
S: 220 fri.uni-lj.si          strežnik se predstavi
O: HELO email.si              odjemalec se predstavi
S: 250 Hello email.si, pleased to meet you
O: MAIL FROM: <miha@email.si>
S: 250 miha@email.si ... Sender ok
O: RCPT TO:<mojcac@fri.uni-lj.si>
S: 250 <mojcac@fri.uni-lj.si> ... Recipient ok
O: DATA
S: 354 Enter mail, end with "." on a line by itself
O: Zdravo, Mojca!
O: Nujno me poklici, ko prides domov, LP Miha.
O: .
S: 250 Message accepted for delivery.
O: QUIT                       ali pa zopet MAIL FROM: <...
S: 221 fri.uni-lj.si closing connection
```

30

Format sporočila (RFC 822, 2822)

```
Ime polja: vrednost
...
Ime polja : vrednost
[prazna vrsta]
Telo sporočila
```

```
From: miha@email.si
To: mojcac@fri.uni-lj.si
Subject: Poklici me

Zdravo, Mojca!
Nujno me poklici, ko
prides domov, LP Miha.
```

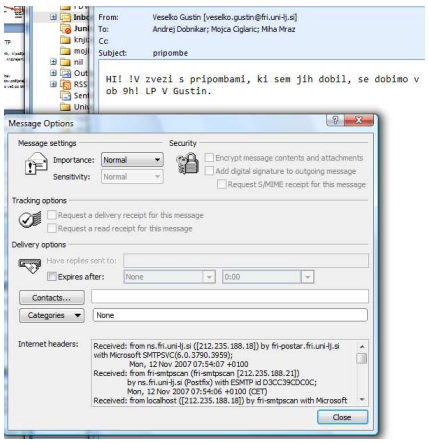
Vrstice glave
(header lines)

Pomembno: razlika med SMTP ukazi in polji v glavi!

Prejemni strežnik

- V glavo doda vrstico Received
- Teh vrstic je lahko več (npr. če se pošta posreduje - forward)

```
Received: from fri.uni-lj.si by
  gmail.com;
   4 Nov 2007 15:29:42 GMT
Received: from email.si by fri.uni-lj.si;
   4 Nov 2007 15:27:33 GMT
```

Celotna glava prejšnjega sporočila...

```
Received: from ns.fri.uni-lj.si ([212.235.188.18]) by fri-postar.fri.uni-lj.si with Microsoft
    SMTPSVC(6.0.3790.3959);
    Mon, 12 Nov 2007 07:54:07 +0100
Received: from fri-smtpscan (fri-smtpscan [212.235.188.21])
    by ns.fri.uni-lj.si (Postfix) with ESMTP id D3CC39CDC0C; Mon, 12 Nov 2007 07:54:06 +0100 (CET)
Received: from localhost ([212.235.188.18]) by fri-smtpscan with Microsoft SMTPSVC(6.0.3790.0);
    Mon, 12 Nov 2007 07:54:05 +0100
X-Virus-Scanned: amavisd-new at fri.uni-lj.si
Received: from ns.fri.uni-lj.si ([127.0.0.1])
    by localhost (ns.fri.uni-lj.si [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id LBI165vdxDib; Mon, 12 Nov 2007 07:54:04 +0100 (CET)
Received: from fri.uni-lj.si (lra-3.fri.uni-lj.si [193.2.76.71])
    by ns.fri.uni-lj.si (Postfix) with ESMTP id D61259CDC0C;  Mon, 12 Nov 2007 07:54:03 +0100 (CET)
Message-ID: <4737F884.9080703@fri.uni-lj.si>
Date: Mon, 12 Nov 2007 07:53:56 +0100
From: Veselko Gustin <veselko.gustin@fri.uni-lj.si>
Organization: University og Ljubljana, Faculty of Computer and Information Science
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: <andrej.dobnikar@fri.uni-lj.si>,  Mojca Ciglaric <mojca.ciglaric@fri.uni-lj.si>, <miha.mraz@fri.uni-lj.si>
Subject: pripombe
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
X-OriginalArrivalTime: 12 Nov 2007 06:54:05.0541 (UTC) FILETIME=[D0E7F150:01C824F8]
Return-Path: veselko.gustin@fri.uni-lj.si
```


MIME razširitve sporočila

- Multipurpose Internet Mail Extensions
- RFC 2045 in 2046: razširitvi starega RFC 822.
- ČŠŽÁÃÇÊËΩξ☺ , večprestavna sporočila
- Nova polja glave

```
MIME-Version:
Content-Type:
Content-Transfer-Encoding:
```


Kodiranje (Encoding)

- Quoted-printable
  - Za (8-bitni) tekst z malo ne-angleškimi znaki. Berljivo.

```
Subject: =?iso-8859-
2?Q?RE:_Obisk_na_va=B9i_=B9oli?=
```

- Base 64
  - Abeceda iz 64 znakov (A-Z, a-z, 0-9, “+” in “/”)
  - 3x8 bitov → 4x6 bitov→ 4 ASCII znaki
  - Velika režija (137% + 814 bitov glava)
- Binary (novejši RFC 3030)
- Primer: jpg priponka (decode, jpeg dekompresija)

Primerjava SMTP in HTTP

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

37

Dostop do poštnega predala

Včasih: oddaljen dostop do strežnika (telnet), nato neposredno branje iz poštnega predala...

Danes

- Dohodna pošta: POP3, IMAP ali HTTP dostop
  - PULL (prenos pošte k sebi)
- Pošiljanje odhodne pošte na strežnik: SMTP
  - PUSH

38

POP3

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

39

POP3 ukazi - primer

```
S: +OK POP3 server ready
O: user mojcac            uporabnik se predstavi
S: +OK
O: pass tralala           nezaščiteno!
S: +OK user successfully logged on     (ali pa –ERR)

O: list
S: 1 678                  1. sporočilo je veliko 678 bytov
S: .                      Ni več sporočil...
O: retr 1                 prenesi sporočilo 1
S: (tralala hopsasa ...)
S: .
O: dele 1                 briši sporočilo 1
O: quit
S: +OK POP3 server signing off
```

40

IMAP in HTTP

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

41

DNS

- IP številka ali znano ime (www.google.com)?
- Bistvena omrežna funkcionanost, ne direktno za uporabnika. RFC 1034, 1035, ...
- DNS vključuje
  - Porazdeljeno podatkovno zbirko
  - Protokol za poizvedovanje po njej
- Storitve
  - Preslikava med imeni in IP številkami
  - Aliasi (več imen za isto IP številko) hostov in poštnih strežnikov
  - Porazdeljevanje bremena (več IP številk za isto ime)

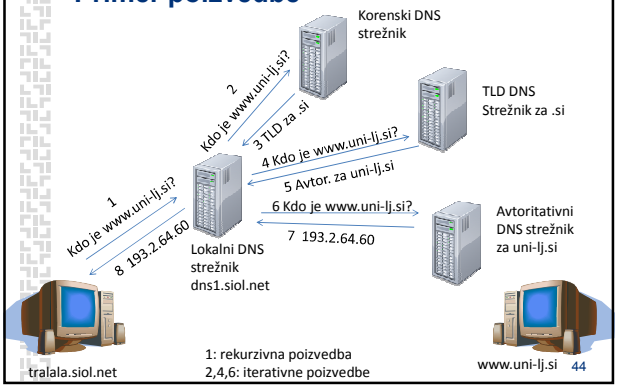
42

Organizacija

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

43

Primer poizvedbe



1: rekurzivna poizvedba
2,4,6: iterativne poizvedbe

44

DNS caching

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

45

DNS zapisi

- RR = Resource Record (Name, Value, Type, TTL)
- TTL: kdaj zapis izbrisati
- Type = A: Name - ime rač., Value – IP številka
- Type = NS: Name – ime domene, Value – ime avtoritativnega DNS strežnika.
- Type = CNAME: Name – alias ime, Value – pravo (kanonično) ime
- Type = MX: Name – alias poštnega strežnika, Value – pravo (kanonično) ime poštnega strežnika

46

DNS strežniki in zapisi

- Avtoritativni DNS strežnik ima zapise tipa A za vse "svoje" gostitelje.
- Ne-avtoritativni DNS strežnik **`(dns1.siol.net)`**
  - ima *lahko* zapis tipa A (cache!) za nekega gostitelja **`(www.uni-lj.si, 193.2.64.60, A)`**
  - Ima NS zapis za domeno tega gostitelja **`(uni-lj.si, dns1.uni-lj.si, NS)`**
  - Ima A zapis za DNS strežnik te domene **`(dns1.uni-lj.si, 193.2.64.45, A)`**

47

DNS sporočila

- Poizvedba in odgovor. Format je enak.
- Glava 12 bytov, več polj
  - ID sporočila 16 bitov
- Poizvedba (ime, tip, npr. A/MX)
- Odgovor (RR zapisi za ime)
- Avtoritete (zapisi drugih avt. strežnikov)
- Dodatni podatki

- nslookup

48

Kako raste DNS zbirka podatkov?

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

49

Storitev aplikacijske plasti je še več...

- **Standardne**
  - Oddaljen dostop (telnet, RFC15 → RFC 854 in drugi),
  - Novice (NNTP, RFC 977, 3977 in drugi)
  - Imenik (LDAP)...
- **Nestandardne**
  - Iskanje,
  - P2P izmenjava datotek
  - ...
- **Podporne** (sejna + predstavitvena plast po OSI)
  - Predstavitev podatkov (preslikave med kodnimi tabelami, ASN.1)
  - Stiskanje (jpeg, mpeg...)
  - Zaščita vsebine (kriptiranje...)
  - Logično povezovanje aplikacijskih procesov – vodenje seje
  - ...

50

Nestandardne storitve: npr. P2P

- Osrednji strežnik (Napster)
- Popolna enakost (osnovna Gnutella, Kazaa)
  - Poplavljanje poizvedb
  - Omejeno poplavljanje
- Popolna enakost + super vozlišča (Gnutella, Kazaa danes)
  - Prioritete uporabnikov, paralelno pretakanje, čakalne vrste zahtev
- Podobno: eMule, eDonkey
- BitTorrent: iskanje je ločeno od prenašanja

51

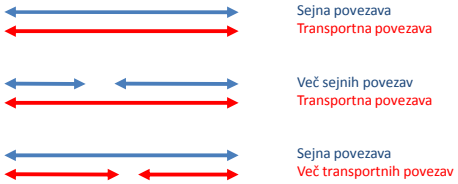
Podporne storitve sejne plasti

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

52

Sejna in transportna povezava

- Možni odnosi:



- Multipleksiranje se izvaja na nižjih plasteh.

53

OSI: struktura seje

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

54

OSI: funkcije sejne plasti

Različni nivoji kakovosti sejne storitve! Funkcionalni sklopi:

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

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

55

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Zaščita in kriptiranje

UVOD (1/3)

- Varnost - kaj je, kdo je ogrožen, kaj ga ogroža?
- Varovanje: preprečevanje možnih nevarnosti
- Ranljivost: šibka točka sistema
- Organizacijski del je danes **pomembnejši** od tehnološkega!
- Dve področji varnosti:
  - **Zanesljivost**: zagotavljanje razmer za delovanje storitev in normalno delo uporabnikov
  - **Zaščita**: onemogočanje nelegalne uporabe sistema
- Oboje lokalno ali razpršeno, zanima nas bolj razpršeno.
- Nadzor!
- Vloge: nadzornik/upravljalec, vzdrževalec, napadalec, uporabnik

Zagotavljanje zanesljivosti (2/3)

- **Ustrezen nadzor**: zbiranje podatkov o delovanju, stanju, uporabi sistema. Dnevniki.
- **Upravljanje**: ukrepanje na podlagi zbranih podatkov.
- Alarmi.Diagnostika. Načrtovanje. Administracija.
- **Orodja**: imeniki, seznami in kazala. SNMP. Poslovna pravila.
- Načrtovanje zmogljivosti in razvoja sistema, primerno testiranje in uvajanje.
- **Razpršena zaščita**. Integriteta povezav, virov, vsebine, uporabnikov, sporočil.

Zaščita in kriptiranje (3/3)

- Kriptiranje: skrivanje vsebine
- Zgodovinski kriptografski postopki
- Simetrični algortimi (DES, AES)
- Asimetrični algoritmi (RSA, ECC)
- Kriptoanaliza (razbijanje)

Varna komunikacija

- Zaupnost – kdo sme prebrati? (enkripcija)
- Avtentikacija – dokaži, da si res ti,
- (Identifikacija – povej, kdo si - brez dokaza)
- Integriteta sporočila – je bilo med prenosom spremenjeno?
- Preprečevanje zanikanja (nonrepudiation) – res si poslal / res si prejel.
- Razpoložljivost in nadzor dostopa – preprečevanje nelegitimne rabe virov (avtorizacija – ugotavljanje, ali nekaj smeš storiti)
- Pomembno je tudi beleženje vseh dogodkov (dostopov, ...)

Pregled celotne vsebine varnosti

- Kriptografija
- Mehanizmi in protokoli (avtentikacija, integriteta...)
- PKI: infrastruktura javnih ključev
- Omrežje – zgradba in požarne pregrade

Pregled vsebine

- Zagotavljanje avtentičnosti
  - Tipični protokoli
  - Tipični napadi
  - Izvedba v PKI
- Integriteta sporočil
- Distribucija ključev in organizacija PKI

Problemi

- Poznamo kriptografske metode
  - simetrične,
  - asimetrične.
- Kako ugotoviti, s kom ZARES komuniciram? AVTENTIKACIJA
- Kako se prepričati, da sporočilo med prenosom ni bilo spremenjeno? INTEGRITETA
- Kako distribuirati javne ključe?

Avtentikacija

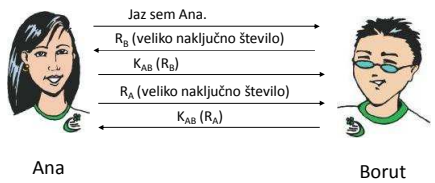
- Če vem, kdo si, ti dovolim več:
  - Se pogovarjam s tabo
  - Dostop do podatkov (avtorizacija)
  - Ti zaupam (verjamem)
- Osebna izkaznica, geslo, kreditna kartica
- To omogoča tudi PKI (infrastruktura javnega ključa) .

Avtentikacija

- Prepričamo se, da je naš sogovornik res tisti, za kogar se izdaja.
  - Izziv-odgovor
  - Zaupamo tretji strani
  - Avtentikacija z javnim ključem

Protokol izziv-odgovor

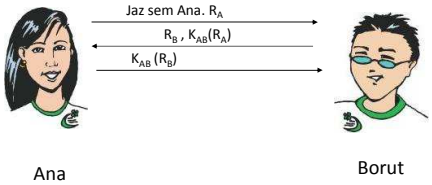
- *Challenge-Response* ali *Shared Secret*
  - Dvosmerna avtentikacija. K_{AB} je vnaprej znan.
- Primer:



Protokol izziv-odgovor

Malo skrajšan primer:

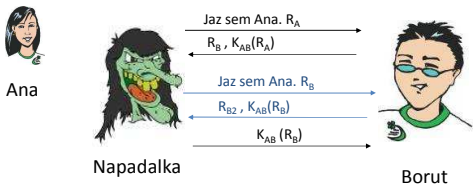
- Je varen?



Protokol izziv-odgovor

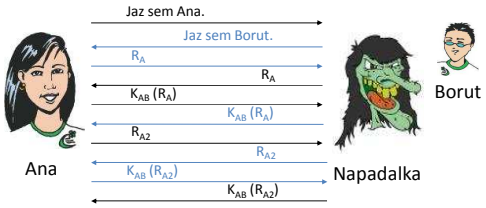
Malo skrajšan primer

- Napad z zrcaljenjem(reflection attack) – če B omogoča več sej hkrati.



Protokol izziv-odgovor

- Napad z zrcaljenjem na prvi protokol:

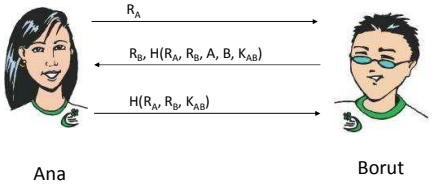


Varen protokol izziv-odgovor

- TEŽKO!
- Pravila:
  - Iniciator naj prvi dokaže svojo identiteto.
  - Za dokaz naj uporabljata različne ključe (K_{AB} in K_{BA})
  - Izziva (R) naj bosta različna (npr. sodo-liho št.)
  - Informacija iz ene seje nekoristna v drugi seji.

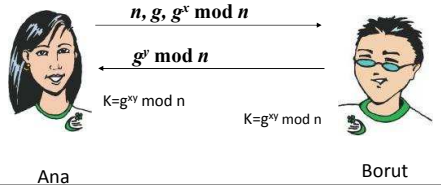
Varen protokol za avtentikacijo

- Uporablja zgoščevalne funkcije (digitalni izvleček)!



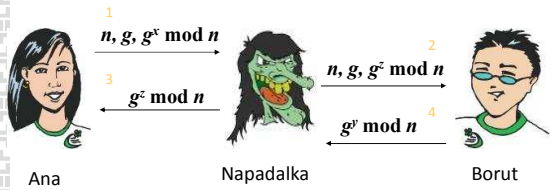
Diffie-Hellman izmenjava ključev

- Kako si pred avtentikacijo izmenjata K_{AB}?
- Najprej izbereta n in g – javno.
- Eden izbere x, drugi y – tajno.



Diffie-Hellman izmenjava ključev

- Napad z vrivanjem (man in the middle attack).

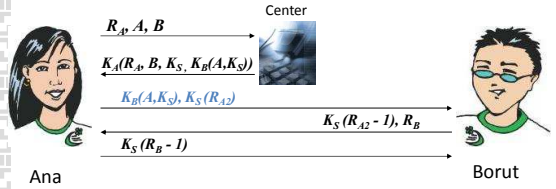


Center za distribucijo ključev

- Težava: upravljanje in organizacija ključev.
- Center pozna vse tajne ključe. Zaupanje!
- Možen napad: replay attack – napad s posneto sejo.
  - Nepooblaščena ponovitev legalne seje (npr. plačilo računa).
  - Rešitev: časovno označevanje in/ali izziv R v vsakem sporočilu

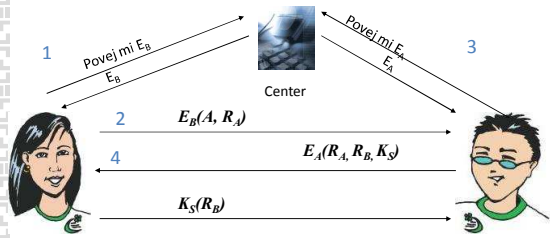
Center za distribucijo ključev

- Needham-Schroeder:
- Če napadalec dobi star K_S, še vedno lahko napade na 3. koraku (replay)!



Avtentikacija v PKI

- Varno, če zaupamo centru.



Integriteta

- Kako vem, da ni bilo sporočilo med prenosom spremenjeno?

Zgoščevalne funkcije (digitalni izvleček)

- Prstni odtis (hash) sporočila m: $f = h(m)$
- m je sporočilo variabilne dolžine
- f je kratek (omejena dolžina!).
- Kolizija: različna sporočila imajo lahko enak digitalni izvleček odtis.

Dobra funkcija

- Pri vseh možnih vhodnih vrednostih je frekvenca vseh rezultatov enaka.
- Majhna sprememba sporočila povzroči veliko spremembo podpisa.
- Zelo težko najti kolizijo!
- Take funkcije imenujemo *cryptographic hash value, digital fingerprint, footprint, message digest (MD), cryptographic checksum.*

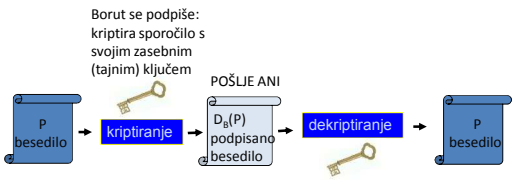
Način delovanja

- Preproste bitne operacije brez ključa
- Podobno simetrični kriptografiji
- Delitev sporočila v bloke, procesiranje v ciklih
- MD4 (podlaga za SHA-1) in MD5 – 128 bitov
- SHA-1 (trenutno najpomembnejši!) – 160 bitov (SHA-256, SHA-512)
- Zgoščevalna funkcija s ključem: MAC (Message Authenticy Check)
- Napad: rojstnodnevni – birthday attack (iskanje kolizije).

Elektronski podpis

- Elektronski podpis mora omogočati troje:
  - Možno preveriti podpis (prejemnik)
  - Ni ga možno ponarediti (prejemnik ali tretja oseba)
  - Ni možno zanikati podpisa (pošiljatelj)
- Podpisan dokument P: $D_A(P)$

Podpis podatkov



Če želimo ohraniti tudi zaupnost sporočila, ga je treba po podpisu še kriptirati z Aninim javnim ključem E_A.
Sam podpis ne zagotavlja zaupnosti, saj je E_B javni ključ, ki ga lahko dobi kdorkoli!

Ana: preveri podpis - dekriptira z Borutovim javnim ključem: $E_B(D_B(P))$

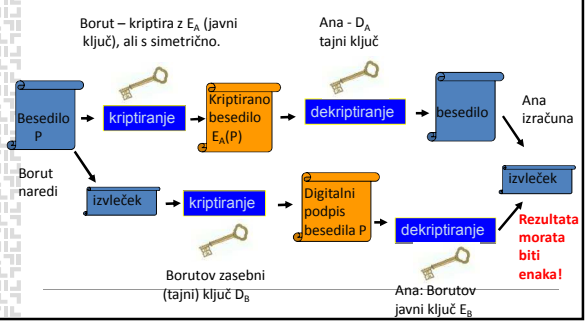
Digitalni certifikat (ali elektronsko potrdilo)

- Zaupanja vredna avtoriteta (certifikatna agencija - CA) - pri nas so kvalificirani **NLB, Pošta, SiGen, Halcom.**
- CA mora imeti dobro definirana pravila (politiko) izdajanja certifikatov (kdo, kako, pod kakšnimi pogoji ga lahko dobi).
  - Primer: http://postarca.posta.si/files/postarca/politika_fizicne_kartica_v1.pdf
- CA podpiše osebne podatke – "vizitko": to je digitalno potrdilo ali certifikat, je časovno omejen.
- Tega nato uporabljamo za avtentikacijo.

Integriteta sporočila

- Sporočilo
- Izvleček
- Podpis
- (Kriptiranje) - po želji

Zagotavljanje identičnosti sporočila (izvleček)



Protokola SSL (Secure Sockets Layer) in TLS (Transport Layer Security)

- Aplikaciji nudi varen kanal, overjanje strežnika in izmenjavo sejnih ključev.
- Leži nad transportno plastjo.
- Aplikacija se ga zaveda (zna uporabljati).
- Tipična uporaba:
  - na aplikacijski plasti za HTTP (https), FTP, SMTP, NNTP, SIP
  - Za tuneliranje celotnega omrežnega sklada – VPN nad transportno plastjo

Delovanje SSL/TLS

- Odjemalec: **ClientHello** (max. verzija TLS, naključno št., seznam podprtih kriptografskih p., izvlečkov in kompresij)
- TLS strežnik: **ServerHello** (izbrana verzija TLS, naključno št., izbrane metode iz seznama)
- TLS strežnik: svoje **digitalno potrdilo** [lahko tudi zahteva potrdilo od odjemalca]
- Odjemalec lahko preveri potrdilo.
- Na podlagi naključnih št. izračunata ključe.
- Komunikacija: simetrično kriptirana sporočila, dodan MAC (odtis sporočila)

Tipični algoritmi SSL/TLS

- Izmenjava ključev: RSA, Diffie-Hellman, PSK...
- Simetrično kriptiranje: RC4, 3-DES, AES, Camellia (starejši SSL: tudi DES, RC2, IDEA).
- Digitalni izvleček: MD5, SHA-1

Pregled celotne vsebine varnosti

- Kriptografija ☑
- Mehanizmi in protokoli (avtentikacija, integriteta) ☑
- PKI
- Omrežje – zgradba in požarne pregrade
- Kratek pregled napadov in preprečevanja

PKI

- Začetki: 1976 (Diffie, Hellman)
- Kriptografija
  - Asimetrična (javni in zasebni - tajni ključ)
  - Simetrična (samo en ključ – mora biti skriven) – hitrejša (faktor 1000)
- Asimetrični ključi:
  - Ključ E zaklene podatek
  - Ključ D (samo ta ključ!) podatek odklene
  - Lahko tudi zaklene D in odklene E.

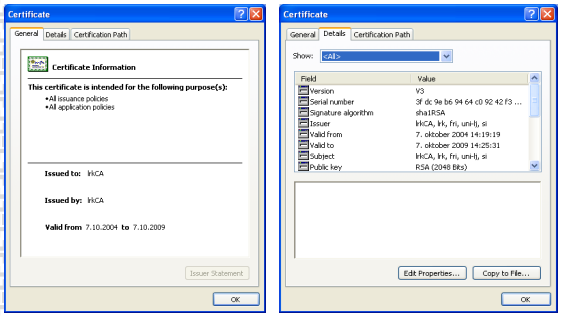
X.509

- X.509 v3: ITU-T / IETF PKI standard
  - Format certifikata
  - Postopek preverjanja veljavnosti certifikata
  - CRL
- Zahteva hierarhijo CA

Upravljanje z javnimi ključi

- Distribucija javnega ključa prek spleta:
  napad s prestrezanjem - man in the middle
- CA
  - Garantira, da ključ pripada določeni entiteti.
- Certifikat (digitalno potrdilo):
  - Podatki o lastniku
  - Javni ključ
  - Ostali podatki
  - **Izvleček in podpis s strani CA**

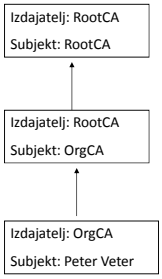
Certifikat - primer



Preverjanje certifikata

- Izdajatelj CA
- Preverimo lahko
  - Integriteto certifikata
  - Identiteto lastnika
  - Izdajateljev javni ključ in podpis
- Veriga zaupanja!

Veriga zaupanja



- Korenska avtoriteta
- Organizacijska CA
- Uporabnik

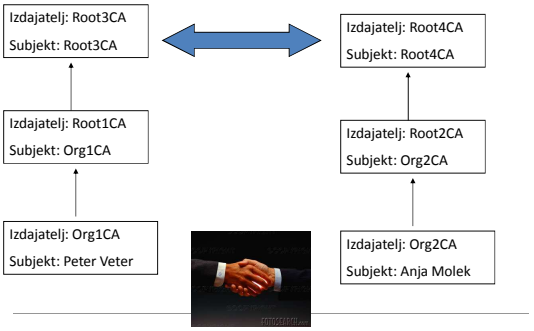
Veriga zaupanja

- Na vrhu je avtoriteta, ki ji eksplicitno zaupam.
- Samo-podpisan certifikat; varovanje!
- Eksplicitno lahko zaupamo tudi komurkoli nižje v verigi.

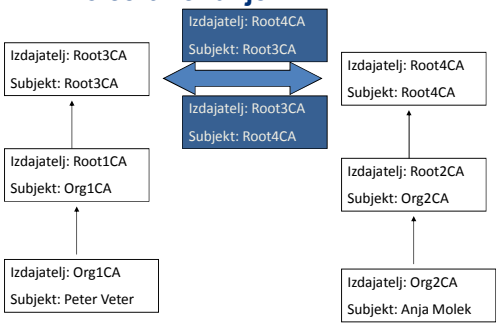
Veriga zaupanja

- Komu zaupata oba? Nikomur ?
  - Par novih certifikatov, vsakomu iz druge hierarhije
  - Navzkrižno certificiranje (CA)

Križno certificiranje



Križno certificiranje



CRL - ČRNA LISTA

- Certificate Revocation List
- Sporne certifikate je potrebno preklicati! Npr. če
  - Ukraden
  - Menjava službe
  - Tajni ključ ogrožen
- CRL: podpis CA in čas (veljavnost)
- ARL – Authority Revocation List (koren)
- Validacija – tudi CRL

PKCS –standardi (RSA lab.)

- PKCS #7 – Cryptographic Message Syntax (kako podpisati in kriptirati)
- PKCS #8 – Format shranjevanja ključa
- PKCS #10 – Format zahteve za certifikat
- PKCS #11 – Dostop do kripto naprave
- PKCS #12 – Zasebni ključi, certifikati, CRL

RFC

- RFC 3369 – Cryptographic Message Syntax
- RFC 3280 – X.509 PKI, certifikat in CRL profil.
- RFC 2315 = PKCS #7 – kako podpisati in kriptirati

Pregled celotne vsebine varnosti

- Kriptografija ☑
- Mehanizmi in protokoli (avtentikacija, integriteta...) ☑
- PKI ☑
- Omrežje – zgradba in požarne pregrade

Temeljna vprašanja

- KDO SI? (identifikacija)
- ALI RES? (avtentikacija – overjanje: kako naj vemo, da si res ta?)
- KAJ SMEM? (avtorizacija)
- ALI SI RES POSLAL TAKE PODATKE? (integriteta)
- ALI NI TEGA NIHČE DRUG VIDEL? (zaupnost)
- KAJ SE JE ZGODILO? (beleženje – logging)
- Ne-zanikanje (pošiljatelj lahko dokaže, da je nekaj poslal; prejemnik prejema ne more zanikati)

Varna komunikacija

- Zaupnost – kdo sme prebrati? (enkripcija)
- Avtentikacija – dokaži, da si res ti,
- (Identifikacija – povej, kdo si - brez dokaza)
- Integriteta sporočila – je bilo med prenosom spremenjeno?
- Preprečevanje zanikanja (nonrepudiation) – res si poslal / res si prejel.
- Razpoložljivost in nadzor dostopa – preprečevanje nelegitimne rabe virov (avtorizacija – ugotavljanje, ali nekaj smeš storiti)

- Pomembno je tudi beleženje vseh dogodkov (dostopov, ...)

Zaščita

- Sporočilo med prenosom po IKS ščitimo z uporabo enkripcije.
- Skrivamo algoritem (?)
  - PROBLEM: nov algoritem za vsakega uporabnika
  - PROBLEM: težko dokazovanje varnosti
- Skrivamo ključ
  - Enak algoritem za vse uporabnike
  - Algoritem je lahko javen

Napadalci in vdiralci

- Upravljalci in nadzorniki
- Sodelavci – prijatelji, ki poznajo geslo
- Državne službe
- Neznanci, na primer:
  - Tatovi, kriminalci
  - Vandali
  - Hekerji, skriptni otroci
  - Beli in črni klobuki
  - Bivši zaposleni
- Socialni inženiring

Kriptiranje

- Čimbolj otežiti delo potencialnim napadalcem in vdiralcem.
- Pošiljatelj - sporočilo P:
  - izbrana metoda kriptiranja in
  - ustrezen enkripcijski ključ E:
  - kriptogram E(P): napadalec ga ne razume.
- Prejemnik:
  - Dekripcijski ključ D
  - D(E(P)) = P

Napadalci

- PASIVNI posluša.
  - Mora izvajati dekripcijo
- AKTIVNI spreminja vsebino, generira nova sporočila.
  - Mora izvajati dekripcijo
  - Mora izvajati enkripcijo

Varen sistem

- Varnostna politika je formalni zapis varnostnih mehanizmov in drugih pravil, ki jih morajo upoštevati vsi posamezniki z dostopom do opreme, prostorov in informacij.
- Vzpostavitev: ORGANIZACIJSKI ali TEHNIČNI problem?
- Težave:
  - organizacijske,
  - cenovne,
  - pravne,
  - politične,
  - družbene.
- Višji nivo varnosti pomeni manj svobode za uporabnika!

Standardi

- ISO/IEC 27000 serija (prej 17799 ter BS 7799) :
  - ISMS – Information Security Management System
  - najboljše prakse z nadgradnjo
  - osnova certificiranja
- Slovenske različice (SIST)
  - Sistemi za upravljanje varovanja informacij – Specifikacija z napotki za uporabo
  - Informacijska tehnologija – Kodeks upravljanja varovanja informacij

ISO 27001; Sistem upravljanja varovanja informacij

- 10 bistvenih poglavij, za vsako so določeni cilji, vsak cilj nadziramo s pomočjo kontrolnih točk.
  - skupno 36 ciljev,
  - 127 nadzorstev

Primeri poglavij, ciljev, kontrol

- Fizična zaščita in zaščita okolja
  - Varovana območja
    - kontrole fizičnega dostopa (npr. beležimo čas prihoda in odhoda, identifikacija z magnetno kartico)
  - Varovanje opreme
    - Namestitev in zaščita pred krajo, ognjem, prahom…
    - Oskrba z energijo (UPS, generator)
- Upravljanje s komunikacijami in produkcijo
  - Zaščita pred zlonamerno programsko opremo
    - Namestitev in posodabljanje protivirusnih programov…
  - Ravnanje z nosilci podatkov in njihovo varovanje
    - Brisanje podatkov, sežiganje zastarelih nosilcev
  - Varovanje e-pošte

Kriptografske metode

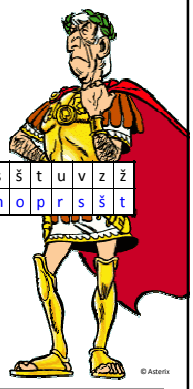
- Po načinu
  - Substitucijske: posamezne črke ali dele besedila nadomestimo z drugimi.
  - Transpozicijske: spreminjamo vrstni red znakov, besed, stavkov…
- Po lastnostih ključa
  - Simetrične: E=D, ključ mora biti tajen.
  - Asimetrične: E≠D, E je lahko javen, D mora biti tajen.

Klasične metode: Cezar

- Cezarjev kriptogram: substitucija.
- JULUA = ?

a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž
u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t

- 25 možnih ključev
- Razbijemo ga v največ 25 poskusih!



Razbijanje substitucijskega kriptograma

- Razbijanje na osnovi poznanega besedila (npr. “please login”) – že v 1. poskusu!
  - Zato kriptiramo le vsebino, ne cele komunikacije
- Statistika jezika (črke, besede, dvo- ali tročrkovni sklopi) – potrebno je daljše besedilo.
- Poznavanje vsebine (semantika) olajša razbijanje – iščemo pričakovane korene besed ipd.
- Knjiga – primer razbijanja!

Vigenèr-jev kriptogram – večabecedno kriptiranje

- Preprost ključ
- Statistika jezika in semantika postaneta nemočni
- Viegenerjeva matrika: vse Cezarjeve abecede.

a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž
b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a
c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b
č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c
d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č

(in tako dalje še 20 vrstic…)

- Ključ = niz D črk, vsaki pripada ena vrstica (enaka 1. črka).
- Z abecedo n-te črke gesla kriptiramo n-to, n+D-to, n+2D-to … črko sporočila.

Vigenèr-jev kriptogram (primer)

- Geslo: računalniške komunikacije
- Sporočilo: Junija vsi izpiti na žalost odpadejo, razen pri ekonomiki, septembra pa bo spet vse po starem.

r	a	č	u	n	a	l	n	i	š	k	e	k	o	m	u	n	i	k	a	c	i	j	e
j	u	n	i	j	a	v	s	i	i	z	p	i	t	i	n	a	ž	a	l	o	s	t	o
d	p	a	d	e	j	o	r	a	z	e	n	p	r	i	e	k	o	n	o	m	i	k	i
S	e	p	t	e	m	b	r	a	p	a	b	o	s	p	e	t	v	s	e	p	o	s	t
a	r	e	m																				

- Prvi stolpec črk kriptiramo z 18. abecedo, itd.

Porterjev kriptogram

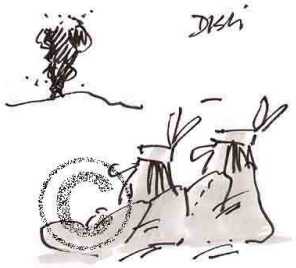
- Kriptiramo po 2 znaka hkrati.
- Simboli so v tabeli – vrstica za en, stolpec za drugi znak.

	a	b	c	č	d	e	f	g	h	i	j	k	l	m
a														
b														
c														
č											…	it	d	…
d														

- npr. KAČA =

Kodiranje

- Cel znak ali besedo nadomestimo z drugo.
- Ni splošnega pravila za zamenjave.
- Ključ predstavlja cela kodna tabela.



"Bugger! I was just about to crack his code, when he burnt his blanket."

Transpozicijski kriptogram

- Znake ali dele besedila premestimo!
- Ključ ima vse črke različne (npr. KOPRIVA).
- Oštevilčimo ključ po abecedi.
- Zapišemo stolpce glede na številke.

k	o	p	r	i	v	a
3	4	5	6	2	7	1
J	u	n	i	j	a	n
ž	a	l	o	s	t	v
s	i	i	z	p	i	t
i	o	d	p	a	d	e
j	o	b	l	a	b	l

Klasične metode - povzetek

- Klasične metode – zgolj za razumevanje.
- Znakovno usmerjene – kriptiramo črko po črko (včasih tudi po besedah).
- Z računalniki jih ni težko razbijati.
- Sodobne računalniške metode so bitno usmerjene.

Simetrične kriptografske metode

- DES
- AES
- IDEA
- RC4
- Misty

Osnovni elementi simetričnih metod

- Transpozicija (P-škatla, ključ)
  - Permutacija
  - Redukcija
  - Ekspanzija
- Substitucija (S-škatla, tabele)
  - Dekoder n/2^n (poljuben n-bitni vhod ⟶ same 0 in 1 enica – po tabeli)
  - Permutacija
  - Koder 2^n/n (obratno kot dekoder – po tabeli)

DES

- Simetričen.
- Hiter (strojna implementacija).
- Kaskada zaporednih permutacij, substitucij in še nekaterih operacij.
- Deluje nad 64-bitnimi binarnimi bloki.
- Ključ je 56-biten.
- Težave z distribucijo ključa!
- Sum bližnjice…
- Več – podrobno: na vajah!

Distribucija ključa

- Lokalno izračunavanje k
  - Tajna funkcija za generiranje, npr. $P(x) = ax^3 + bx^2 + cx + k$
  - Za spremembo ključa pošljemo 3 točke polinoma: $(x_1, P(x_1))$, $(x_2, P(x_2))$, $(x_3, P(x_3))$
  - Prejemnik lahko izračuna k.
- Metoda "puzzles" za časovno občutljive podatke
  - ključ na videz skrajšamo (dogovorjeno zaporedje
  - Pošljemo veliko ključev, prejemnik enega izbere in razbije, sporoči njegovo zaporedno številko.
  - Pošlje kriptirano besedilo, ki je varno še za čas razbijanja.

Metoda enkratnega ključa

- Ključ je daljši kot besedilo.
- Ekskluzivni ALI (xor): (A xor B) xor B = A
- Enkripcija: P xor E = E(P)
- Dekripcija: D(E(P)) = E(P) xor E
  = (P xor E) xor E = P
- Težava: potrebno je generirati poljubno dolg ključ (na obeh straneh! - sinhronizacija)

Veriženje

- DES = velik substitucijski kriptogram!

M	O	J	C	A		S	I
J	A	N	E	Z		S	I
P	E	T	E	R		S	I

T		1	0	0	0	0	0
T		3	0	0	0	0	0
T			3	2	0	0	0

- Možno je zamenjati posamezne kriptirane bloke z drugimi, tudi če ne poznamo ključa.

Enkripcijski stroj (veriženje)

Metoda enkratnega ključa ima težave s ključi.

- Kompromis: Naslednji blok sporočila najprej XOR-kriptiramo s prejšnjim DES-kriptiranim blokom, šele nato ga damo v DES škatlo.
- $C_N=E(P_N \text{ XOR } C_{N-1})$

NAPAD Z GROBO SILO

Ključ	Oseba	Mala skupina	Razisk. omrežje	Veliko podjetje	Vojska
40	Dnevi	Ure	Minute	Mili-sekunde	Mikro-sekunde
56	Leta	Tedni	Dnevi	Minute	Mili-sekunde
64					
80					
128					

Ocene tehnologije iz leta 2000!

NAPAD Z GROBO SILO

Ključ	Oseba	Mala skupina	Razisk. omrežje	Veliko podjetje	Vojska
40	Dnevi	Ure	Minute	Mili-sekunde	Mikro-sekunde
56	Leta	Tedni	Dnevi	Minute	Mili-sekunde
64	Tisočletja	Stoletja	Desetletja	Ure	Sekunde
80					
128					

Ocene tehnologije iz leta 2000!

NAPAD Z GROBO SILO

Ključ	Oseba	Mala skupina	Razisk. omrežje	Veliko podjetje	Vojska
40	Dnevi	Ure	Minute	Mili-sekunde	Mikro-sekunde
56	Leta	Tedni	Dnevi	Minute	Mili-sekunde
64	Tisočletja	Stoletja	Desetletja	Ure	Sekunde
80	∞	∞	Tisočletja	Stoletja	Dnevi
128	∞	∞	∞	∞	∞

Ocene tehnologije iz leta 2000!

Napad na DES z grobo silo

- DES - challenge
- Začetek 1998: v 39 dneh
- Sredi 1998: v 56 urah z računalnikom za 250.000 €
- 1999: v 22 urah s 100.000 prostovoljci – uporabniki Interneta

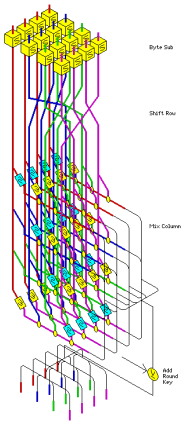
Trojni DES

- 3 x kriptiranje
- 3 x počasnejši
- 2^{56} x varnejši za napad z grobo silo

- Enkripcija: E(K1) – D(K2) – E(K1)
- Dekripcija: D(K1) – E(K2) – D(K1)
- 112 bitov je dovolj varno.
- EDE namesto EEE: za kompatibilnost med DES in 3-DES (3-DES rač. nastavi K2 = K1)

AES: simetričen

- Advanced Encryption Standard
- Rijndael: kriptografski algoritem (Daemen, Rijmen)
- Hiter, varen
- Blok dolg 256 (16 8-bitnih znakov)
- Ključ dolg različno (128, 196, 256)
- Dekripcija: v obratni smeri ali z drugimi tabelami.

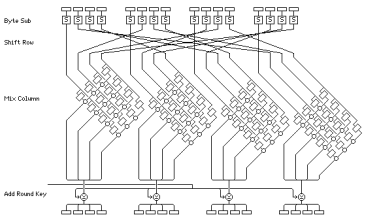


AES: osnovne operacije

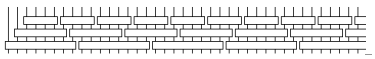
- Byte sub: Substitucija (S-škatla)
- Shift row: mešanje vrstic (P-škatla)
- Mix column: mešanje stolpcev – substitucija, ki temelji na aritmetiki končnih polj.
- Add round key – substitucija: XOR trenutnega bloka z delom ekspandiranega ključa.

AES: simetričen

Shema z drugega zornega kota:



Možno sestavljati različne dolžine ključev kot lego kocke:



Drugi simetrični algoritmi

- IDEA, 1990 (International Data Encription Algorithm)
  - Podoben DES-u, brez večjih slabosti
  - Uporaba v PGP (+ triple DES +CAST)
- RC2 (Rivest Cipher 2)
  - Eden od algoritmov S/MIME
  - Spremenljiva dolžina ključa
- CAST (imena avtorjev) –(v PGP)
  - RFC2144: določene S-škatle in 128-bitni ključ
  - RFC2612: CAST-256 s spremenljivo dolžino ključa
- Skipjack, Misty
- ...

Asimetrična kriptografija

- E in D različna!
- E je lahko javen, D mora biti tajen.
  - D(E(P)) = P
  - Iz P in E(P) je nemogoče ugotoviti D.
  - Iz E je nemogoče ugotoviti D.

RSA

- Izberemo p,q: veliki praštevili (1024 bitov)

  $n = pq$

  $z = (p-1)(q-1)$
- Izberemo d: nima skupnih deliteljev z *z*.
- Izberemo e: $ed \bmod z = 1$
- P → $C=P^e \bmod n$ *kriptiranje*
- C → $P=C^d \bmod n$ *dekriptiranje*
- *Ni težav z distribucijo. Počasnost.*

Elektronski podpis

- To je medsebojno identificiranje uporabnikov.
- Potreben pogoj: D(E(P) = E(D(P))
- Oddajnik sporočilu doda informacijo, ki je značilna samo zanj.
- Za podpis se navadno uporabi le kratek niz P (nekaj 100 bitov): lahko digitalni izvleček.
  - Ime in priimek
  - EMŠO, davčna, vpisna številka, …
  - Podjetje
  - Datum in ura podpisa

Elektronski podpis z RSA

- Pogoj: E(D(P))=D(E(P))
- Podpis: informacija, lastna samo podpisniku: D; D(P) je podpisano besedilo.
- Peter: E_P, D_P
- Vesna: E_V, D_V

- P="Peter Klepec" → podpisano:$D_P(P)$
- Enkripcija: $E_V(D_P(P))$ → sledi prenos.
- Dekripcija: $D_V(E_V(D_P(P)) = D_P(P)$
- Preverjanje podpisa: $E_P(D_P(P)) = P$

Tajenje podpisa

- Če podpisnik zamenja ključ, lahko taji svoje prejšnje podpise!
- NOTAR: uporabnik deponira svoje podatke skupaj s časom njihove veljavnosti
- Notar vzdržuje tudi historiat.
- Notarju zaupamo!
- Ko prejmemo podpisano sporočilo, preverimo podpis pri notarju.

Načini uporabe bločnih kriptosistemov

- CBC (Cypher Block Chaining) – veriženje:
  - Pred kriptiranjem se vsak blok XOR-a s prejšnjim kriptiranim blokom.
- PCBC (Propagating CBC) – upošteva več prejšnjih P in C blokov
- CFB (cipher Feedback) – zelo podobno.Omogoča tudi kode za popravljanje napak (napačen bit na istoležnem mestu).
- CTR (counter) – za vzporedno kriptiranje več blokov hkrati.

- Inicializacijski vektor: težave!

Integriteta sporočila

- Ali je bilo sporočilo med prenosom spremenjeno?
- Digitalni izvleček sporočila Z(P)
- Z(P) podpišemo in pošljemo skupaj s sporočilom.

Zgoščevalne funkcije

- Prstni odtis (hash) sporočila *m: f = h(m)*
- *m* je poljubno dolgo sporočilo
- *f* je kratek (omejene dolžine!).
- Kolizija: različna sporočila imajo enak prstni odtis.

Dobra zg. funkcija

- Pri vseh možnih vhodnih vrednostih je frekvenca vseh rezultatov enaka.
- Majhna sprememba sporočila povzroči veliko spremembo podpisa.
- Zelo težko najti drugačno vhodno vrednost za isti podpis (kolizijo)!
- Take funkcije imenujemo *cryptographic hash value, digital fingerprint, footprint, message digest (MD), cryptographic checksum*.

Način delovanja

- Preproste bitne operacije brez ključa
- Podobno simetrični kriptografiji
- Delitev sporočila v bloke
- Procesiranje blokov v več ciklih
- SHA-1 (trenutno najpomembnejši!) – 160 bitov
- MD4 (podlaga za SHA-1) in MD5 – 128 bitov
- Zgoščevalna funkcija s ključem: MAC (Message Authenticy Check)

Generatorji

- Naključni generatorji, vgrajeni v OS, prevajalnik, … : statistično dobro porazdeljeni
- Generator naključnih števil
  - Čas med dostopi do diska
  - Vnosi s tipkovnice
  - Premiki miške
  - Strojni: spremembe napetosti
- Generator praštevil
  - Temelji na zgornjem
  - Preverja delitelje

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Protokoli

Splošni protokoli

- Odkrivanje in odpravljanje napak
- Nadzor pretoka

- Oddajnik: ali je sprejemnik dobil podatke? Pravilne?
- Oddajnik: ali pošiljam prehitro?
- Sprejemnik: ponoviti oddajo.

Potrjevanje

- SPROTNO POTRJEVANJE: oddajnik po vsaki oddani PPE čaka na potrditev `(stop-and-wait)`
- TEKOČE POŠILJANJE: oddajnik ne čaka na sprotne potrditve.

- NEPOSREDNO: ACK, NACK
- POSREDNO: ACK

Potrjevanje

- Neposredno: ACK, NACK
- Posredno: ACK

- Sprotno potrjevanje: naslednji paket se pošlje po prejemu potrditve.
- Tekoče pošiljanje: ne čaka se na potrditve.

Potrjevanje

	SPROTNO	TEKOČE pošiljanje
NEPOSREDNO	✓	✓
POSREDNO	✓	✓

Parametri

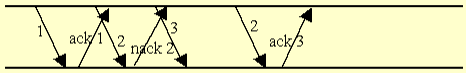
- Časovna kontrola oddajnika
- Časovna kontrola sprejemnika (izpad odd.)
- Število ponovitev PPE
- Število ponovitev potrditve
- Zaporedna številka paketa (večkratne oddaje)

Potrjevanje

- Tekoče neposredno
  - Potrjevanje bloka (zaporedja):
    ACK(N) potrdi vse do N
  - Po oddaji NACK(N) ni ACK, dokler N ni pravilno sprejet.
- Tekoče posredno
  - Ni potrjevanja bloka.
  - ACK(N-1), ACK(N+1) ⇨ namesto NACK(N)

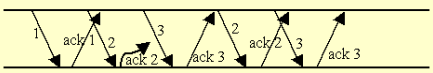
7

- Za kašno potrjevanje gre?



8

- Za kakšno potrjevanje gre na spodnji sliki?



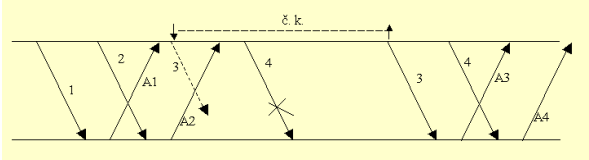
9

Primer

- Pošiljamo sekvenco 5 paketov.
- Možni zapleti:
  - Paket se popači.
  - Paket se izgubi.
  - Potrditev se izgubi.
- Vse različice potrjevanja.

10

- Za kakšno potrjevanje gre?



11

Potrjevanje

- Vrste
  - Oddajnik: oddani, še nepotrjeni paketi
  - Sprejemnik: sprejeti, še nepotrjeni paketi
- Sprejemnik
  - Odpravljanje duplikatov
  - Sortiranje
- Ponavljanje zaporedja (*go back n*) – ponovimo vse PPE od napake dalje.
  - Ohranja vrstni red.
  - Pri tekočem – posredno in neposredno potrjevanje.

12

Primer

- Pri tekočem pošiljanju 6 paketov uporabljamo posredno potrjevanje brez ponavljanja zaporedja.
- Kakšna je shema prenosov, če se izgubita 1. in 3. paket, po ponovitvi pa še potrditev 1. paketa?
- Širina okna naj bo 4.

13

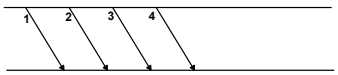
Kontrola pretoka

- Uravnavanje intenzivnosti pošiljanja.
- Eksplicitna: X-on/X-off
  - X-off: nehaj
  - X-on: nadaljuj
- Implicitna: drseče okno (*sliding window*)
  - Širina okna = N
  - Največ N nepotrjenih PPE

14

Kontrola pretoka
Protokoli z drsečim oknom

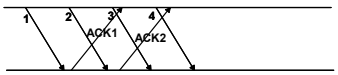
Širina okna = 4



15

Kontrola pretoka
Protokoli z drsečim oknom

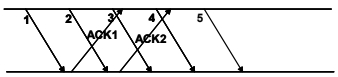
Širina okna = 4



16

Kontrola pretoka
Protokoli z drsečim oknom

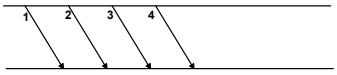
Širina okna = 4



17

Kontrola pretoka
Protokoli z drsečim oknom

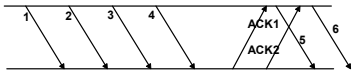
Širina okna = 4



18

Kontrola pretoka
Protokoli z drsečim oknom

Širina okna = 4

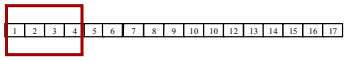


19

Kontrola pretoka
Protokoli z drsečim oknom

Širina okna = 4

Drsenje okna:



20

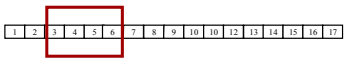
Kontrola pretoka
Protokoli z drsečim oknom

Širina okna = 4

21

Kontrola pretoka
Protokoli z drsečim oknom

Širina okna = 4

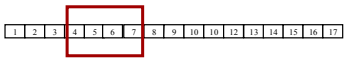


22

Kontrola pretoka
Protokoli z drsečim oknom

Širina okna = 4

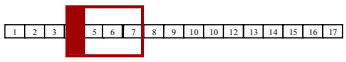
Zapiranje okna:



23

Kontrola pretoka
Protokoli z drsečim oknom

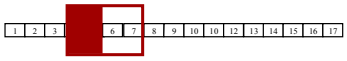
Širina okna = 4



24

Kontrola pretoka
Protokoli z drsečim oknom

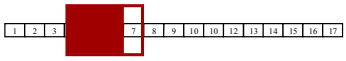
Širina okna = 4



25

Kontrola pretoka
Protokoli z drsečim oknom

Širina okna = 4



26

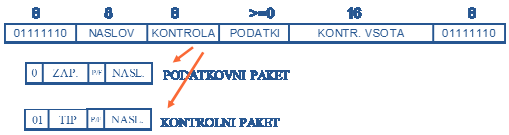
Potrjevanje
Primeri protokolov 2.plasti - HDLC

- HDLC = High-level Data Link Control (X.25)
  Sorodniki: SDLC, ADCCP, LAP, LAPB
- FORMAT OKVIRJA

- KONTROLA

27

Potrjevanje
Primeri protokolov 2.plasti - HDLC



TIPI KONTROLNIH PPE:

- 00 = receive ready (ACK)
- 01 = reject (NACK) od številke vključno NASL.
- 10 = receive not ready = Ack do NASL.-1 + Počakaj!
- 11 = selective reject (NACK) samo za NASL.

28

Potrjevanje
Primeri protokolov 2.plasti - PPP

PPP = Point-to-Point Protocol

- Metoda okvirjanja + detekcija napak
- LCP (Link Control Protocol) za vzpostavljanje, preizkušanje in sproščanje povezav
- Več NCP (Network Control Protocol) za več tipov omrežnih protokolov (IP, Novell - IPX, AppleTalk ...)

29

Potrjevanje
Primeri protokolov 2.plasti - PPP

SCENARIJ UPORABE

- Fizična povezava modem – modem ali usm. ISP-ja
- LCP – pogajanje o PPP parametrih povezave
- NCP – konfiguriranje omrežne plasti (npr. dodelitev IP številke)
- NCP – sproščanje omrežne povezave (npr. IP številke)
- LCP – prekine podatkovno povezavo
- Modem – prekine telefonsko povezavo

30

Potrjevanje
Primeri protokolov 2.plasti - PPP

PPP okvir

Zastavica	Naslov	Kontrola	Protokol	Podatki	Kontr.vsota	Zastavica
01111110	11111111	00000011	1 ali 2 byta	variabilno	2 ali 4 byti	01111110

Vsi poslušajo

Protokol omr.plasti

Neoštevilčen okvir (na nezanesljivih omrežjih se tu uporablja zap.št.)

31

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

PROTOKOLI
Načrtovanje, analiza, testiranje

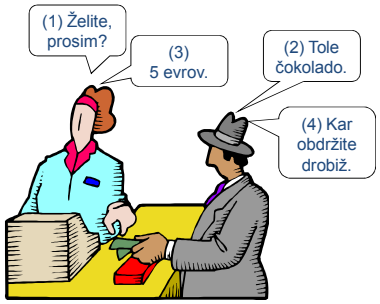
Protokoli

- PROTOKOL: zbirka pravil za komuniciranje.

33

Protokoli

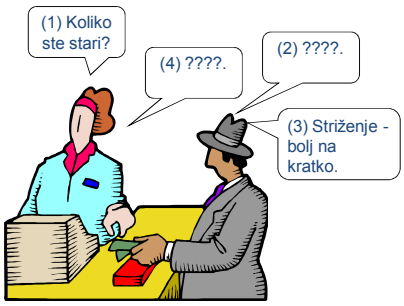
PRIMER



34

Protokoli

PRIMER
(napake
v protokolu!)



35

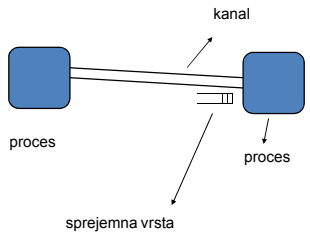
Protokoli

- PROCES: mrežna točka v sistemu
- Procesi komunicirajo prek kanalov.
- KANAL
  - Dvosmerni – kolizijski / nekolizijski
  - Izmenično dvosmerni
  - Enosmerni

36

Protokoli

Preprost sistem z dvema procesoma



37

Protokoli

- DOGODEK:
  - Proces A v stanju X sprejme sporočilo p od procesa B in preide v stanje Y
- Formalni zapis dogodka:
  - A(X, +p(B), Y)
- Vrste dogodkov
  - Sprejemni +
  - Oddajni -
  - Lokalni #

38

Protokoli

- STANJE procesa
- Začetno stanje
- Prehodi med stanji ⇔dogodki

39

Protokoli

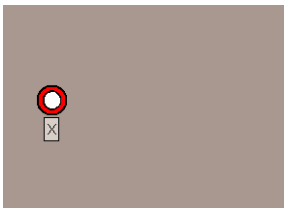
- Model: končni avtomat
- VSAK PROCES ima svoj avtomat.

40

Protokoli

- PRIMER AVTOMATA za proces A

začetno stanje

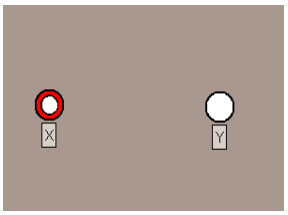


41

Protokoli

- PRIMER AVTOMATA za proces A

še eno stanje

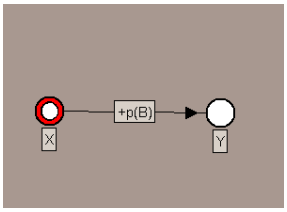


42

Protokoli

- PRIMER AVTOMATA za proces A

dogodek (prehod med stanji)



43

PRIMER

- Procesa A in B: oba lahko zahtevata povezavo, ruši pa jo lahko le A.
- Po 2 stanji
  - P (povezan)
  - N (nepovezan)
- Sporočili
  - p (poveži)
  - r (ruši povezavo)
- Nariši oba avtomata.
- Navedi vse možne dogodke.

44

Protokoli – testiranje
metoda PGSS

PGSS = Perturbiranje Globalnih Stanj Sistema

- N: število procesov
- Globalno stanje: matrika N x N
  - $[i,i]$: trenutno stanje procesa i
  - $[i,j]$: vsebina sprejemne vrste od procesa i k procesu j
- Začetno globalno stanje:
  - Vsi procesi so v začetnih stanjih
  - Vse vrste so prazne

45

Protokoli – testiranje
metoda PGSS

- Iščemo vse možne dogodke, ki se lahko zgodijo v začetnem globalnem stanju.
- Dogodek ⇨ novo globalno stanje
  - Sprememba stanja enega procesa
  - Sprememba vsebine čakalne vrste (nobene / ene / več)
- Drevo globalnih stanj sistema

46

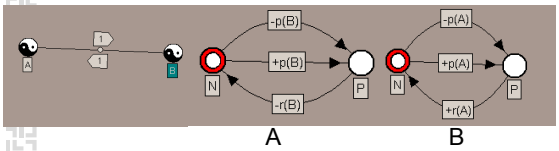
Protokoli – testiranje
metoda PGSS

- Listi drevesa:
  - "že videna" globalna stanja
  - Napake
    - PV – polna vrsta
    - NS – nedefiniran sprejem
    - SO – smrtni objem
- Mrtva koda (dogodek, ki se ne more zgoditi)
- Stabilno globalno stanje (vse vrste so prazne)

47

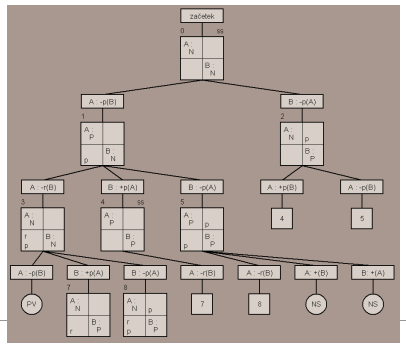
Protokoli – testiranje
metoda PGSS

Primer: PGSS za prejšnji protokol



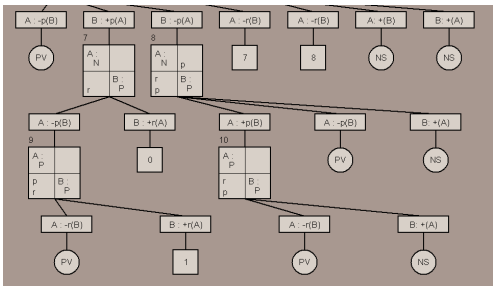
48

Protokoli – testiranje



Protokoli – testiranje

metoda PGSS



Protokoli – testiranje

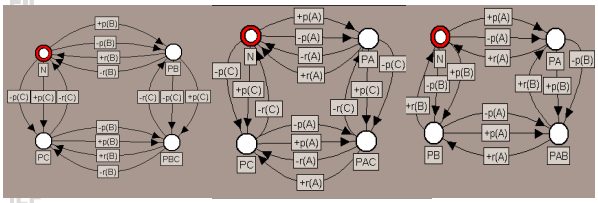
metoda PGSS

Primer:

- 3 procesi (A, B, C)
- VSAK: povezan z enim, povezan z drugim, povezan z obema, nepovezan
- Vsi lahko vzpostavljajo zvezo, rušita pa jo le A in B.
- Sporočili p, r
- Nariši avtomate, testiraj.

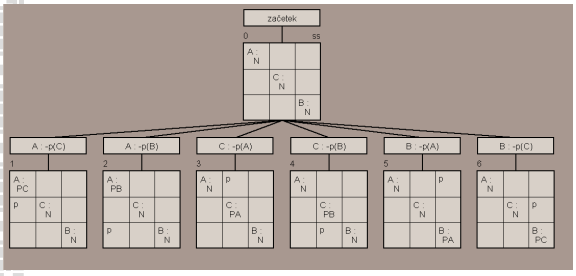
Protokoli – testiranje

metoda PGSS



Protokoli – testiranje

metoda PGSS



Protokoli – testiranje

metoda PGSS

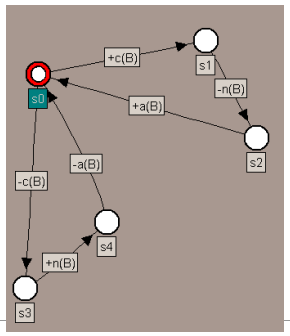
Primer:

- 2 procesa (A, B)
- Simetrična avtomata.
- Prvi pokliče drugega, ta mu pošlje nazaj neko število. Prvi potrdi.
- Hkratna vzpostavitev: prevlada tisti, ki je poslal večje število. Če sta števili enaki, se zveza ruši.

Naloga - avtomat

Osnovna funkcionalnost:
Odjemalec:
- Oddam zahtevo
- Sprejmemem *n*
- Oddam potrditev

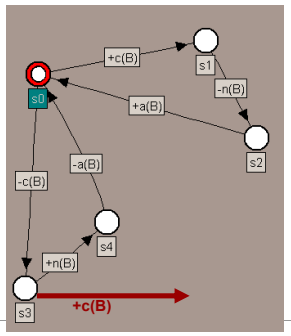
Strežnik:
- Sprejmem zahtevo
- Oddam *n*
- Sprejmem potrditev



55

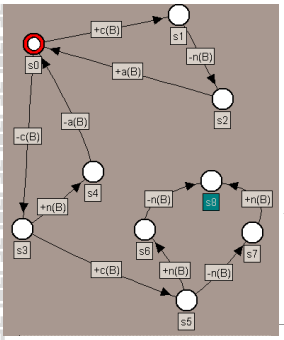
Naloga - avtomat

Konflikt:
- Oddam zahtevo
- Sprejmemem zahtevo
- ???



56

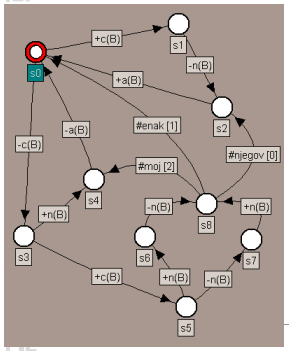
Naloga - avtomat



Reševanje konflikta in izmenjava števil

57

Naloga - avtomat

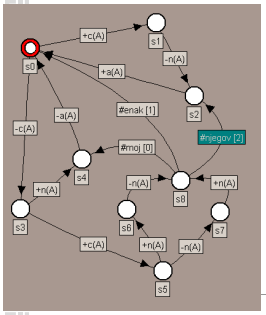


Lokalni dogodek:

Prehod med stanji brez sprejema ali oddaje

58

Naloga - avtomat

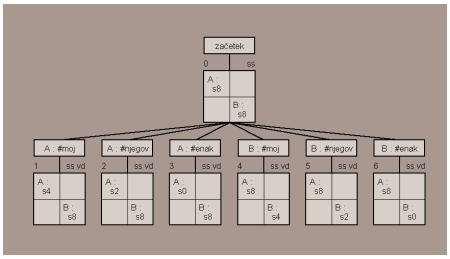


VEZANI DOGODKI:

0 - A:#njegov in B:#moj
1 - A:#enak in B:#enak
2 - A:#moj in B:#njegov

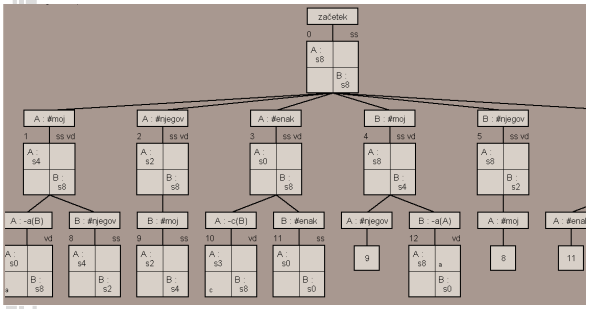
59

Naloga - poudarki



60

Naloga – poudarki



61

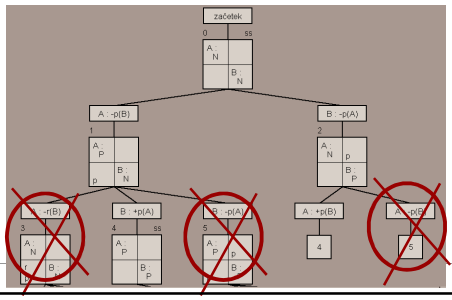
Protokoli – testiranje
POSEBNE LASTNOSTI

- Prioriteta sprejema pred oddajo
  "Raje sprejemam kot oddajam"
- Prioriteta oddaje pred sprejemom
  "Raje oddajam kot sprejemam"
- *Velja lahko*
  - *za sistem kot celoto*
  - *za posamezen proces*

62

Protokoli – testiranje
POSEBNE LASTNOSTI

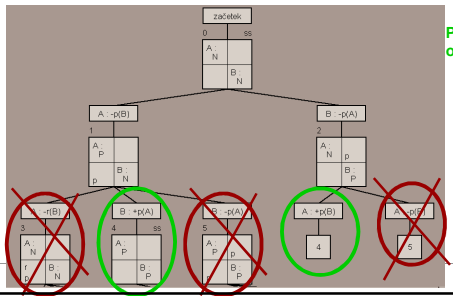
- Prioriteta sprejema pred oddajo



63

Protokoli – testiranje
POSEBNE LASTNOSTI

- Prioriteta sprejema pred oddajo



Prioriteta oddaje

64

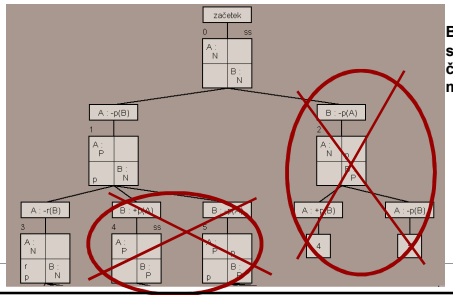
Protokoli – testiranje
POSEBNE LASTNOSTI

- Hierarhija procesov – raje imamo, da akcije izvaja A kot B (potreben je centralni nadzor)
  - Samo na nivoju sistema kot celote
- Hierarhija procesov – raje komuniciramo z A kot z B (vsaj 3 procesi)
  - Na nivoju sistema kot celote: vsi raje komunicirajo z A kot z B. (ustvari se "lestvica" – npr. A B C)
  - Na nivoju posameznih procesov: C raje komunicira z A kot z B, B pa raje sC kot z A.

65

Protokoli – testiranje
POSEBNE LASTNOSTI

- Hierarhija procesov – raje imamo, da akcije izvaja A kot B (centralni nadzornik)

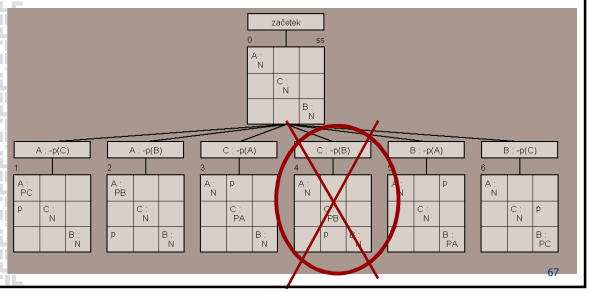


B deluje samo, če A ne more.

66

Protokoli – testiranje
POSEBNE LASTNOSTI

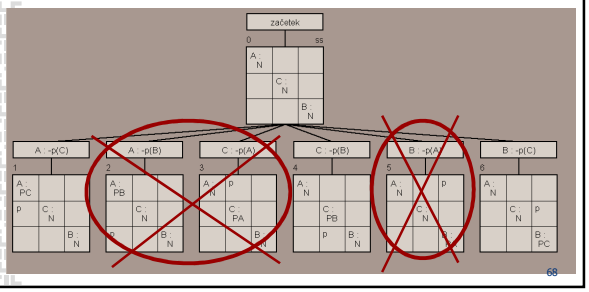
- Hierarhija procesov – C se raje pogovarja z A kot z B



67

Protokoli – testiranje
POSEBNE LASTNOSTI

- Hierarhija procesov – lestvica C B A



68

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Povezavna in fizična plast

Vsebina

- Pregled storitev
  - Zaznavanje in popravljanje napak
  - Multiple access: dostop do skupnega medija
  - Naslavljanje
  - Zanesljiv prenos podatkov, kontrola pretoka – med sosednimi vozlišči
- Pregled tehnologij
  - Npr. Ethernet, IEEE 802.11 (Wi-Fi), Frame Relay,
  - Različni protokoli povezavne plasti nudijo različne storitve (npr. zanesljiv prenos da / ne)

Prenosni sistem

- Povezavna plast (OSI)
- Fizična plast (OSI)

} Prenosna plast (TCP/IP)

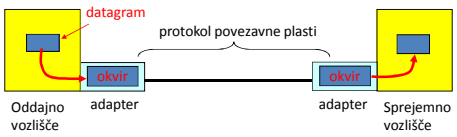
- **Prenosni kanal**: naprava, ki lahko prenese paket (okvir) po mediju.

Povezavna plast

- Vozlišče: računalnik, usmerjevalnik
- Povezava (link) povezuje dve sosedni vozlišči
- Paket povezavne plasti je OKVIR.
- Okvir enkapsulira datagram.

- NALOGA povezavne plasti:
  - Prenos okvirja po povezavi med sosednima vozliščema .

Komunikacija med adapterji



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

Zaznavanje in odpravljanje napak

- Parnost: 1 bit. Samo zaznavanje enojnih napak.
- Parnost v 2 dimenzijah (vrstica + stolpec): zaznavanje in odpravljanje enojnih napak.
- Internetna kontrolna vsota (uporaba le na transportni plast: telo datagrama je zaporedje 16-bitnih števil. Njihova vsota (eniški komplement) gre v glavo datagrama.
- CRC: n-bitov za rezultat – detekcija napak do n bitov (in nekaterih večjih)

Protokoli za dostop do skupinskega medija

- Multiple Access. Kolizija.
- Isti kanal se uporablja tudi za koordinacijo.
- Idealni protokol:
  - Eno vozlišče oddaja: hitrost H
  - M vozlišč oddaja: vsako s hitrostjo H/M
- Možne rešitve:
  - Razdeliti kanal, ni kolizij
  - Naključni dostop, dovoljene kolizije
  - Določeno zaporedje dostopov, ni kolizij

7

Delitev kanala

- TDMA: Time Division Multiple Access
  - V vsakem "krogu" vsaka postaja dobi enak časovni interval (1 paket)
  - Neizkoriščeni intervali
- FDMA: Frequency Division Multiple Access
  - Vsaka postaja ima svoj fiksen frekvenčni pas
  - Neizkoriščen čas
- Pošteno in učinkovito pri visoki obremenitvi, pri nizki neizkoriščenost kanala.
- CDMA, WDM (pride na vrsto kasneje)

8

Kolizijski protokoli (naključni dostop) 1

- Določajo:
  - kako zaznati kolizijo
  - Kako ukrepati ob koliziji
- ALOHA: paket je ranljiv ves čas oddajanja
  - Preprost, nizka prepustnost (18%)
  - Kolizija: počaka naključen čas, nato spet odda
- Razsekana ALOHA: čas je razsekan na delčke
  - Sinhronizacija, boljša prepustnost (37%)
  - Paket je ranljiv le v začetku oddajanja
  - Kolizija: z verjetnostjo *p* odda v naslednjem intervalu

9

Kolizijski protokoli 2

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

10

Nekolizijski protokoli

- Namesto faze boja za medij je faza rezervacije.
  - Rezervacijski paket obišče vse postaje, te vanj zapišejo svoj ID (prijava za oddajo)
  - Nato postaje oddajajo po določenem **vrstnem redu.**
  - **Vodilo in obroč z žetonom (**FDDI, Token Ring)

11

Naslavljanje

- MAC naslovi (LAN naslov, fizični naslov)
  - 48 bitov, npr: 58-32-D7-FA-20-B6
  - Identificira adapter znotraj (pod)omrežja
  - Prenosljivi, nehierarhični, nespremenljivi
  - MAC naslov izvora in ponora sta v glavi okvirja
  - Broadcast: FF-FF-FF-FF-FF-FF
- ARP – Address Resolution Protocol
  - Preslikava IP – MAC naslov
  - Vsako vozlišče ima ARP tabelo (IP – MAC – TTL)

12

ARP protokol

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

- Ni potreben administrator ☺

Če je iskani naslov zunaj omrežja...

- Na ARP poizvedbo za naslov zunaj omrežja odgovori usmerjevalnik R – prehod v B-jevo omrežje, s svojim MAC naslovom.
- Ko R prejme okvir od A, pogleda ciljni IP naslov.
- R naredi ARP poizvedbo v omrežje B.
- R pošlje okvir na novi ciljni MAC naslov.

ARP spoofing (ARP poisoning)

- Okvir z lažnim izvornim MAC naslovom – "naj mislijo, da sem jaz npr. prehod"
- Posledica v zastrupljeni ARP tabeli:
  - Napadalčev MAC naslov – legalen IP naslov
- Napadalec
  - Pasiven: posluša in posreduje promet naprej
  - Aktiven: spreminja in posreduje promet naprej (napad man-in-the-middle).
  - DOS napad: napadalec poveže IP naslov prehoda žrtve z neveljavnim MAC naslovom.

ARP spoofing

- Preprečevanje
  - Fiksni zapisi v ARP tabelah (ročni vnosi)
  - DHCP snooping: pozna MAC naslove na linkih in preverja vsak ARP paket, če ustreza (Cisco)
  - ArpWatch: program, ki opozarja na spremembe ARP tabel (npr. Mail administratorju)
- Legalna uporaba: npr. redundančna infrastruktura (rezervni strežnik, če glavni odpove)...

DHCP stradanje

- Napadalec: broadcast veliko zahtev za DHCP naslov iz lažnih MAC naslovov.
- DHCP strežnik: zmanjka naslovov
  - DOS napad (uporabnik ne dobi naslova)
  - Napadalec lahko zdaj postavi lažni DHCP strežnik

- Preprečevanje:
  - DHCP avtentikacija (RFC 3118)
  - Omejevanje števila različnih MAC naslovov na posam. Vmesniku stikala ali usmerjevalnika

Še več napadov ...

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

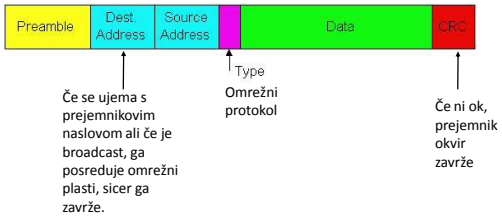
Ethernet

- Topologija: vodilo (včasih), zvezda (danes).
- Hub – razdelilnik signala (na fizični plasti)
- Stikalo: preklaplja okvirje na podlagi MAC naslova (na povezavni plasti)
- [Usmerjevalnik: na podlagi IP naslova – na omrežni plasti]
- 10BaseT, 100 BaseT, Gb/s, 10 Gb/s

19

Ethernet okvir

- Preambula: 7 x 10101010 in 1 x 10101011
  - Da se sinhronizirata uri oddajnika in prejemnika



20

Storitev

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

21

Hub - razdelilnik

- Deluje na 1. plasti
- Možna večja razdalja med vozlišči, če je vmes hub (deluje kot ojačevalec signala)
- Ne ločuje kolizijskih domen – vsi segmenti so ena, razdelilnik le ponavlja signal
- Ne more povezovati segmentov različnih hitrosti

22

Stikalo

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

23

Primerjava

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

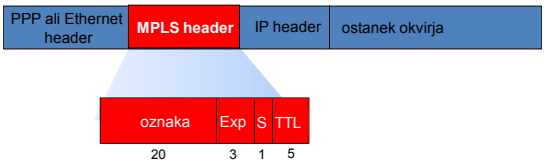
24

PPP

- En pošiljatelj, en prejemnik, MAC naslovi nepotrebni
- Klicna povezava, ISDN
- Naloge:
  - Okvirjanje, detekcija napak
  - Preverjanje povezave, pogajanje o omrežnih naslovih
- Ni potrebno:
  - Korekcija napak, ponovno pošiljanje, pravo zaporedje
  - Kontrola pretoka
- Byte stuffing: 01111110 označuje začetek in konec okvirja. Če je isti niz v podatkih, vrinemo še enega. Če prejemnik zazna dva zapored, enega zavrže.

MPLS

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



MPLS usmerjanje

- "Label-switched" usmerjevalnik
- Posredovanje paketov glede na oznako
- MPLS tabela je drugačna od usmerjevalne

  (v IP usmerjanju npr. določanje poti glede na izvor prometa ne bi bilo možno)
- Potreben je signalizacijski protokol za vzpostavljanje poti (RSVP – Resource ReSerVation Protocol, RFC 2205)
- Dobra združljivost z IP-usmerjevalniki

Brezžično omrežje

Sestavljajo ga:

- Bazne postaje, povezane v ožičeno omrežje
- Brezžični odjemalci (prenosnik, dlančnik, telefon,...)
- Brezžične povezave

Ad hoc omrežje:

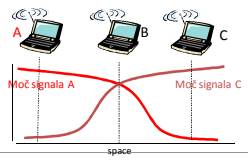
- Ni baznih postaj
- Pošiljanje le odjemalcem, ki so v dometu
- Vozlišča se lahko tudi organizirajo v omrežje z lastnim usmerjanjem

Brezžična povezava: lastnosti in težave

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

A in C sta v interferenci pri B

A in C se ne slišita



CDMA

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

Standardi IEEE 802.11 (Wi-Fi)

- 802.11b (do ca. 140 m)
  - 2.4 do 5 GHz, do 11 Mb/s (tipično 4.5)
  - DSSS (direct sequence spread spectrum), ista koda
- 802.11a (krajše razdalje, do ca. 120 m)
  - 5-6 GHz, do 54 Mb/s (tipično 23)
- 802.11g (do ca. 140 m)
  - 2.4-5 GHz, do 54 Mb/s (tipično 19)
- 802.11n (predlog; predvidoma bo l. 2009)
  - 2.4-5 GHz, do 248 Mb/s (tipično 74), do ca. 250 m

- VSI: CSMA/CA, delovanje: ad hoc in bazne postaje

31

Principi delovanja WLAN

- Uporaba na omejenih področjih (stavba)
- Prihodnost:
  - fiksna brezžična omrežja - npr. WiMax za last-mile širokopasovne povezave do 30 km, do 40 Mb/s
  - Mobilni telefon z WLAN + VOIP (poceni pogovor mimo operaterja 3G)
- 802.11b: 11 kanalov različnih frekvenc

32

Principi delovanja WLAN

- CSMA/CA
  - **carrier sense:**
    - posluša pred oddajo.
    - ni detekcije kolizij (med oddajanjem je sprejemnik izključen)
  - **collision avoidance**
    - Več algoritmov, npr. MACAW (Multiple Access Collision Avoidance for Wireless),
    - Postaja si "rezervira" kanal:
      - Odda RTS (request to send)
      - Prejme CTS (clear to send) - majhna paketa
    - Šele po prejemu CTS odda podatke.
    - V podatkih ni kolizij

33

Protokol vključevanja v WLAN

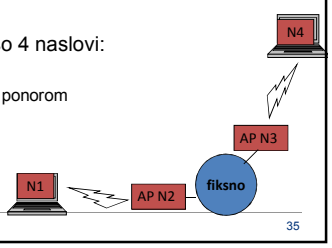
- **Postopek aktivne izbire pristopne točke** – *scanning* :
  - Probe (*Je v bližini kak AP?*)
  - Probe response (*Jaz sem AP*)
  - Association Request (*Rad bi se pridružil*)
  - Association Response (*Kar izvoli*)
- **Pasivna izbira** (passive scanning)
  - AP periodično oddaja *beacon frame ("Jaz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

34

WLAN: Format okvirja

Kontrola, 16 bitov (ali je ad hoc omrežje?)
Izvor in ponor, vsak do 48 bitov (ad hoc)
Podatki, do 2312 bitov
CRC, 32 bitov
Če ni ad hoc omrežje, so 4 naslovi:

- N1: končni ponor
- N2: AP pred končnim ponorom
- N3: AP pri izvoru
- N4: izvor



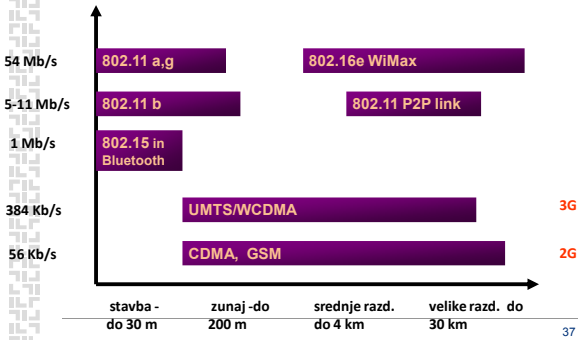
35

IEEE 802.15 – osebno omrežje

- PAN – personal area network
- Razvoj iz Bluetooth specifikacije
  - 2.4 – 2.5 GHz, do 721 kb/s
- Manj kot 10 m, namesto kablov (miš, slušalke...)
- Ad hoc omrežje. (Bluetooth ima lahko tudi AP).
- Gospodar in sužnji: gospodar (npr. PC) mora sužnjem (npr. miški) dovoliti oddajanje

36

Brezžična omrežja: tehnologije



Celularna omrežja

- Bazne postaje, mobilni uporabniki, ožičeno omrežje
- Kombinacija FDMA/TDMA (GSM) ali CDMA
- Generacije
  - 1G: zvok (analogno - NMT)
  - 2G: zvok (GSM), podatki do 19 kb/s
  - 2.5G: zvok + podatki (GPRS, EDGE, CDMA) do 200 kb/s
  - 3G: UMTS, CDMA 2000, HSDPA, WCDMA, po standardu do 1-2 Mb/s, v praksi manj.
  - 4G: pretočni video (NTT DoCoMo – Japonska, WCDMA). Vsepovsod brezžični dostop, nevidno preklapljanje med omrežji, brez prekinitve sej, visoke kapacitete (video, TV), brezplačno. ☺

Delovanje celularnega omrežja

- Omrežje: bazna postaja pokriva svojo "celico" (uporablja okrog 200 kanalov)
- Mobilni terminal poišče celico z najmočnejšim signalom in se prijavi.
- Bazna postaja obvesti o prijavi lokalno centralo, ta pa matično.
- Ko pride klic, se ta usmeri v ustrezno celico.
- Če jakost signala pade, se terminal preklopi na drugo celico.
- Podatkovni prenos: še vedno drag in počasen.

Zagotavljanje mobilnosti

- pri omrežjih mobilne telefonije so podobni problemi kot pri zagotavljanju mobilnosti v IP (vgrajeno v IPv6).

- Domače omrežje, domači agent, stalni naslov
- Gosteče omrežje, gosteči naslov, domači agent gostečega omrežja
- Sogovornik želi komunicirati z "nomadom".
- Usmerjanje – 3 možnosti:

Usmerjanje – 3 možnosti

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

Tipi prenosnih sistemov

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

Kodiranje

- Prenosni kanal: kodiranje
  - Digitalni: z diskretnimi vrednostmi (npr. dva napetostna nivoja)
  - Analogni: z analognimi signali (zvezno spreminjanje vrednosti)
- Naprave: digitalne ali analogne
- Omrežja: digitalna ali analogna
- Kje nastopi potreba po konverziji?

Fizična plast

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

Prenosni medij

- Frekvenčna karakteristika: kakšne frekvence lahko prenese (od-do).
  - Govor: 300 do 7000 Hz
  - Telefonski kanal: 500 do 3600 Hz
  - Hi-fi oprema: 100 do 20.000 Hz
- Prenos signala: Fourierova analiza (vsota osnovnega signala in višjih harmonskih komponent).
- Čimveč višjih komponent se lahko prenese, tem bolj lepo pravokoten bo signal (vsota).

Prenos digitalnih podatkov po analognem kanalu

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

Modulacija

- **Amplitudna** modulacija:
  - Glasen pisk: 0
  - Tih pisk: 1
- **Frekvenčna** modulacija:
  - Visok pisk: 0
  - Nizek pisk: 1
- **Fazna**: sprememba faze za določen fazni kot pomeni spremembo signala.

Kvadratna modulacija

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

Prenos analognih podatkov po digitalnem kanalu

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

Prenosni mediji 1/3

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

Prenosni mediji 2/3

- Koaksialni kabel – do 2 Gbps
  - Bakrena žica, izolacija, oklop – drugi vodnik, še ena izolacija.
  - Odpornost proti motnjam, ni sevanja.
- Optično vlakno – Tera bps
  - Do 100 km brez ponavljalnikov
  - Mehanska občutljivost, zahtevno spajanje
  - WDM (Wavelength Division Multiplexing): za prenos več signalov po enem vlaknu uporabimo več valovnih dolžin (barv) svetlobe – to je v bistvu isto kot FDM!
  - Veliko dobrih lastnosti
  - V začetku le omrežne hrbtenice, danes tudi “last mile” povezave (FTTH)

Prenosni mediji 3/3

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

Digitalna telefonija

- PDH (skoraj sinhrona digitalna hierarhija)
- SDH (sinhrona)
- Sonet
- ISDN in B-ISDN (optika, ATM)