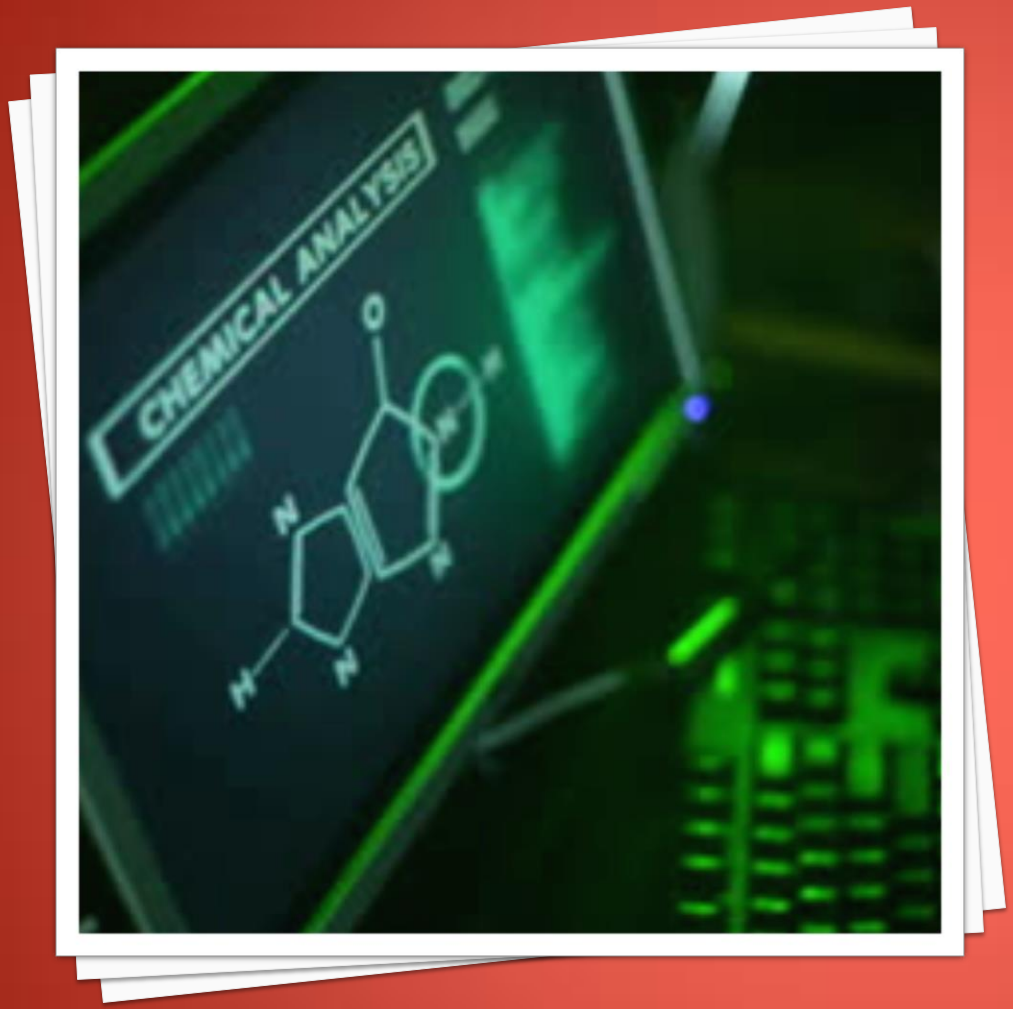
UIKTNT

UPORABA INFORMACIJSKO - KOMUNIKACIJSKIH TEHNOLOGIJ V NARAVOSLOVJU IN TEHNIKI

Doc. dr. Mojca Ciglarič, UL FRI
As. Vida Groznik, UL FRI
As. Dr. Darko Pevec, UL FRI



8

RAČUNALNIŠKA OMREŽJA

VSEBINA

- Uvod
- Delitev omrežij
- Omrežni protokoli
- Povezovanje omrežij
- Komunikacija med procesi
- Internet
- Dostop do Interneta
- Internetne aplikacije
- Modeli omrežij
- Varnost
- Iskanje podatkov na Internetu

UVOD

- Računalniško omrežje
  - med seboj povezani avtonomni računalniški sistemi,
  - potrebujemo jih za
    - prenašanje podatkov med računalniškimi sistemi in
    - delitev računalniških virov
  - za povezovanje računalniških sistemov potrebujemo primerno komunikacijsko opremo (strojno in programsko),

- Razlogi za razvoj računalniških omrežij
  - izmenjava podatkov med oddelki geografsko razpršene organizacije
  - preko omrežij imajo mnogi uporabniki dostop do
    - zmogljivih računalniških sistemov,
    - drage strojne opreme (barvni laserski tiskalniki),
    - drage programske opreme
  - razpršene podatkovne baze
    - hitrost dostopa, varnost podatkov, …
  - Komunikacija med ljudmi (e-pošta, klepet...)

DELITEV OMREŽIJ

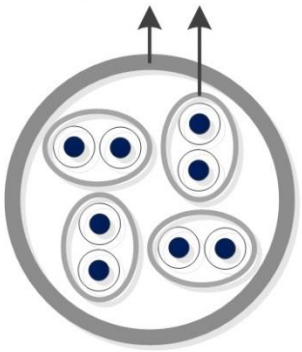
- Velikost omrežja:
  - lokalno omrežje, LAN (ang. local area network)
    - sistemi v takem omrežju so si geografsko dokaj blizu
    - za tako omrežje običajno skrbi ena sama organizacija
  - Prostrana omrežja, WAN (ang. wide area network)
    - omrežja, ki se razprostirajo po širokem geografskem področju, omrežne hrbtenice
- Javna (odprta) in zasebna (zaprta) omrežja
  - internet – javno omrežje
  - intranet – zasebno omrežje
- Glede na povezavo
  - Obstaja fizična povezava („žica“),
  - brezžična povezava

PRENOSNI MEDIJI 1/3

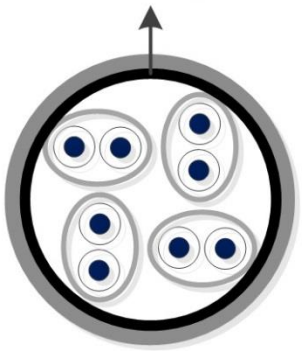
- Fizični prenos pomnilnih medijev
  - Kanal 512 kb/s, 10 min hoje, 2 GB baza
  - Omrežje: 8 ur, peš: 10 min!
- Parica in zvita parica (UTP)
  - Dve vzporedni izolirani bakreni žici
  - Zvita: manj interferenc, presluha ipd
  - 10 Gbps na krajše razdalje (lokalna omrežja),
  - Tudi Tbps...

PARICE

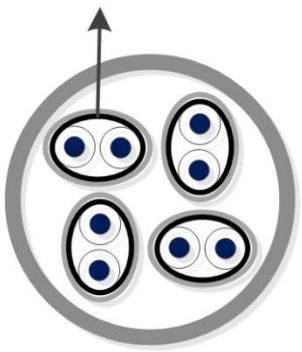
UTP
Izolacija iz umetne mase



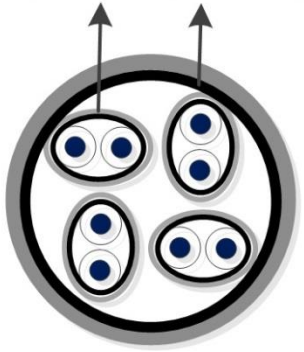
F/UTP
Oklop iz folije

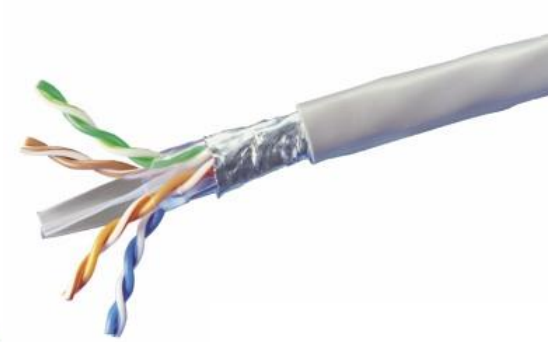


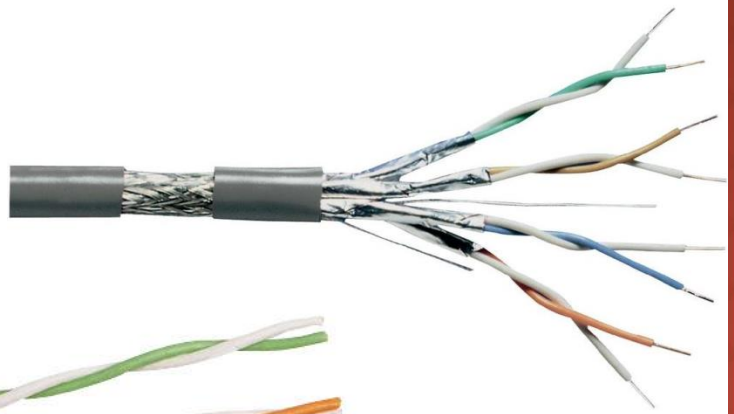
STP
Oklop iz folije

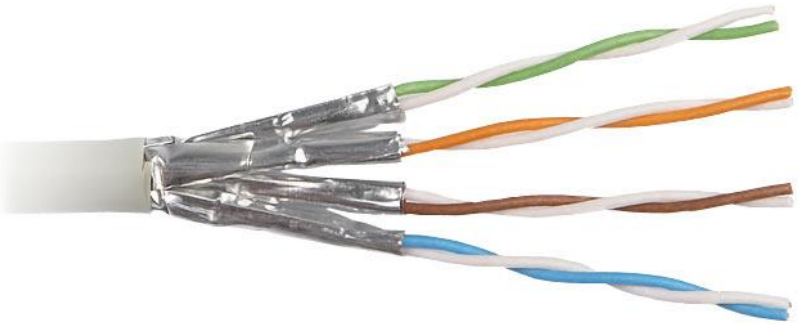


S/FTP
Oklop iz folije in pleten oklop









TIPI OKLOPLJENE PARICE

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

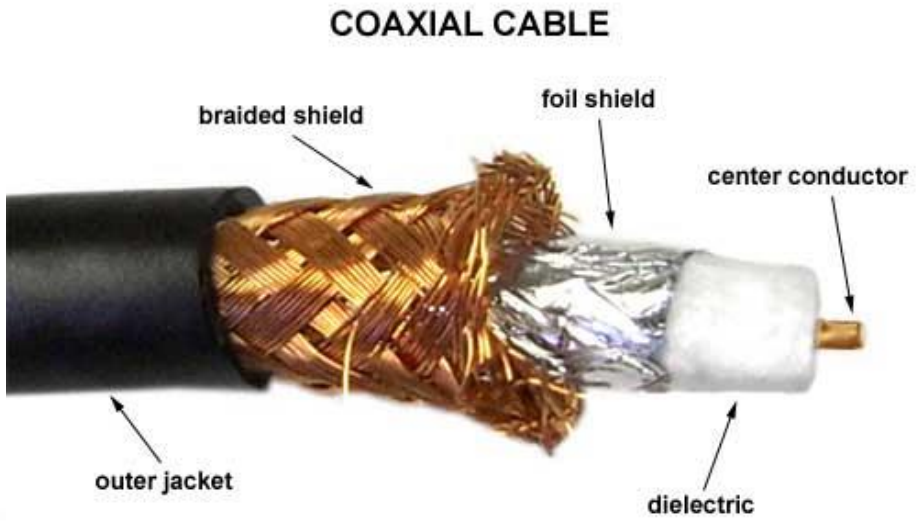
KATEGORIJE

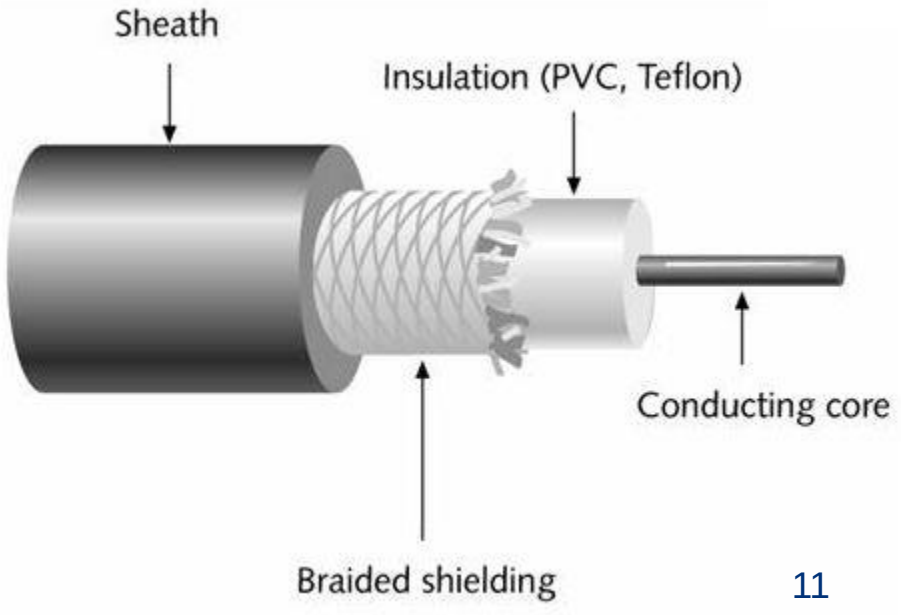
Category	Type	Frequency Bandwidth	Applications & Notes
Cat 1		0.4 MHz	Telephone and modem lines (not described in EIA/TIA recommendations and not suitable for modern systems).
Cat 2			Older Terminal Systems (not described in EIA/TIA recommendations and not suitable for modern systems).
Cat 3	UTP	16 MHz	10BASE-T & 100BASE-T4 Ethernet (Described in EIA/TIA-568. Not suitable for speeds > 16 Mbps. Commonly used for telephone cables).
Cat 4	UTP	20 MHz	16 Mbps Token Ring (Not commonly used these days)
Cat 5	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet (Commonly found in most of the LAN implementations)
Cat 5e	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet (Cat5 Enhanced. Same structure as Cat 5, but with better testing standards)
Cat 6	UTP	250 MHz	1000BASE-T Ethernet (SFS-EN 50173-1)
Cat 6e		250 MHz (500 MHz in some cases)	Not a standard; its a proprietary of cable manufacturers
Cat 6a		500 MHz	10GBASE-T Ethernet (ISO/IEC 11801:2002 Amendment 2)
Cat 7	S/FTP	600 MHz	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet. (Contains Four pairs, S/FTP : Shielded pairs, Braid-screened cable. ISO/IEC 11801 2nd Ed.)
Cat 7a		1000 MHz	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet. (Contains Four pairs, S/FTP : Shielded pairs, Braid-screened cable. ISO/IEC 11801 2nd Ed. Amendment 2)
Cat 8		1200 MHz	Under Development. (Four pairs, S/FTP: Shielded pairs, braid-screened cable. its a standard under development)

PRENOSNI MEDIJI 2/3

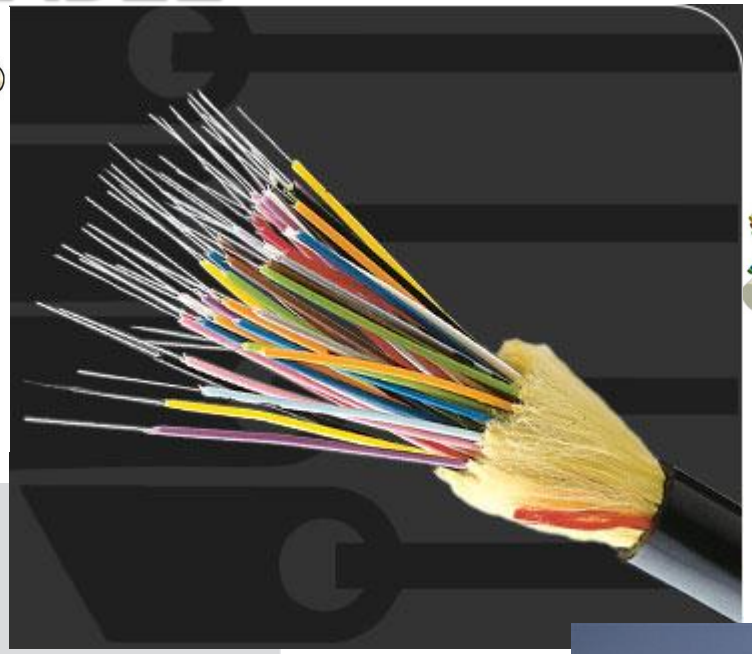
- Koaksialni kabel – do 2 Gbps
  - Bakrena žica, izolacija, oklop – drugi vodnik, še ena izolacija.
  - Odpornost proti motnjam, ni sevanja.
- Optično vlakno – Tera bps
  - Do 100 km brez ponavljalnikov
  - Mehanska občutljivost, zahtevno spajanje
  - WDM (Wavelength Division Multiplexing): za prenos 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)

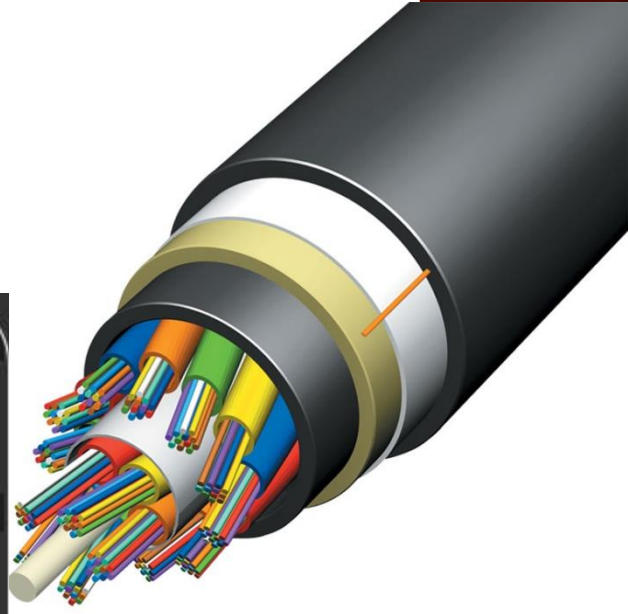
KOAKSIALNI KABEL

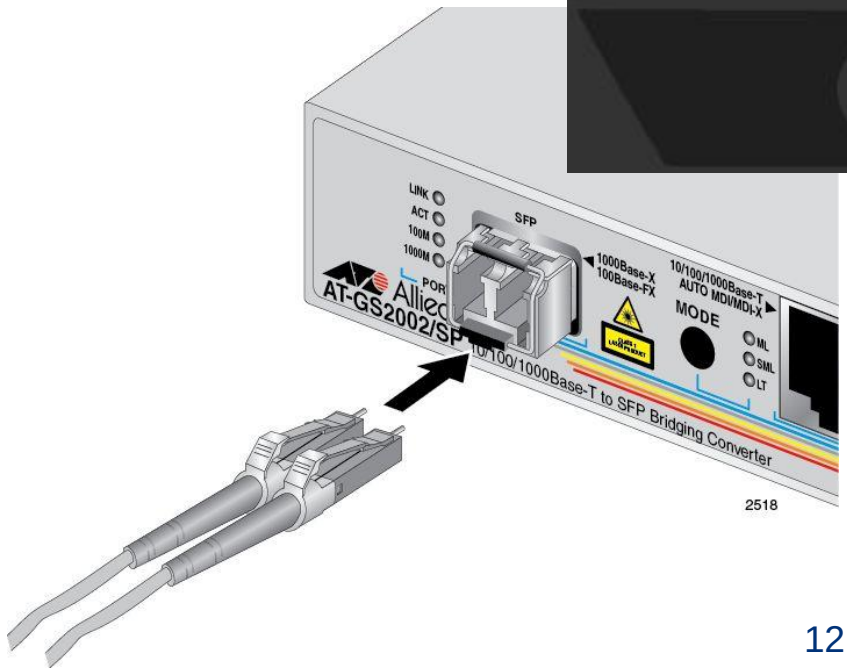




OPTIČNI KABEL





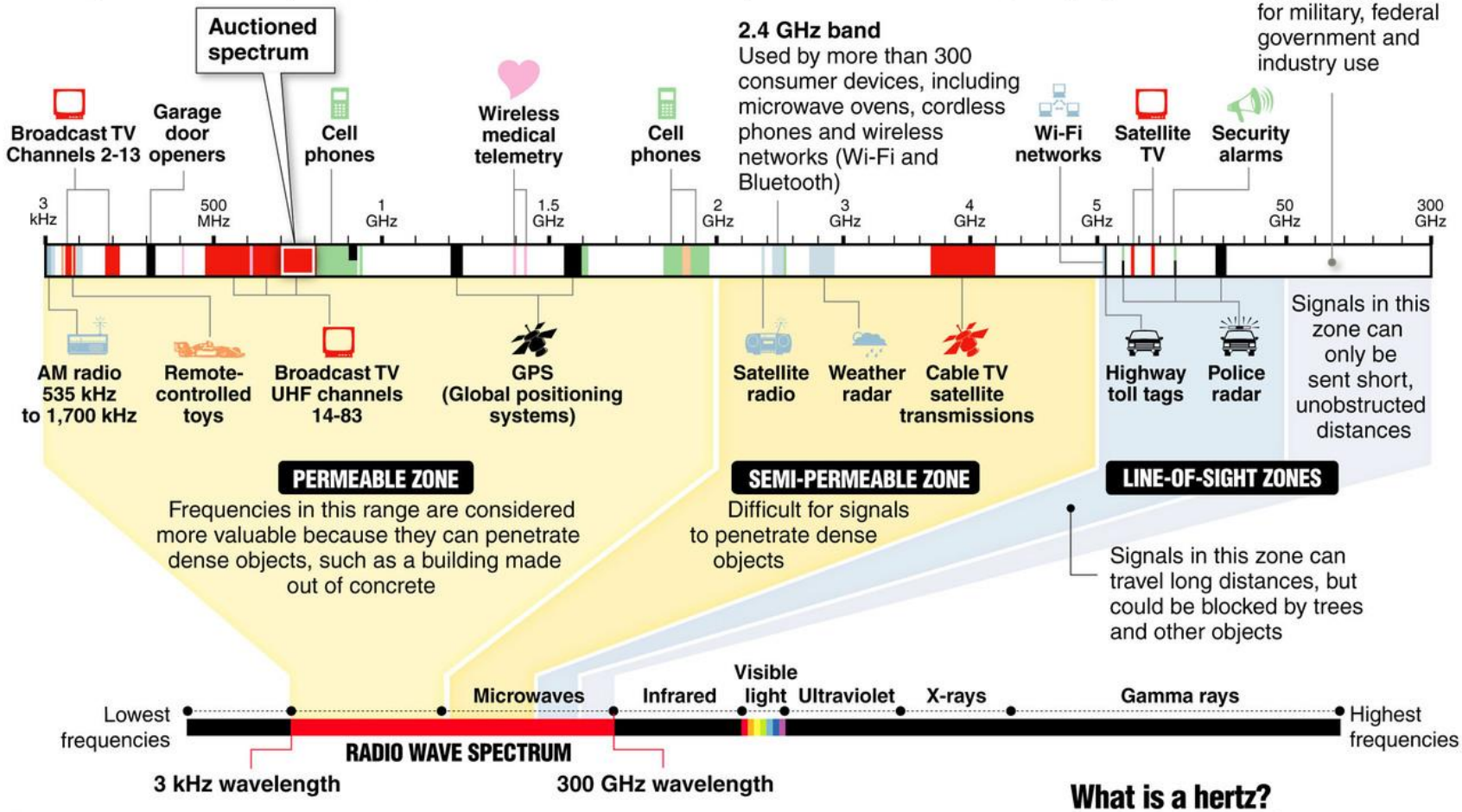


PRENOSNI MEDIJI 3/3

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

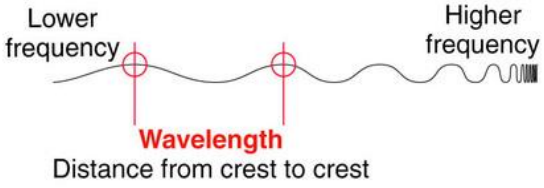
Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:



The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz



What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

1 kilohertz (kHz) = 1,000 hertz

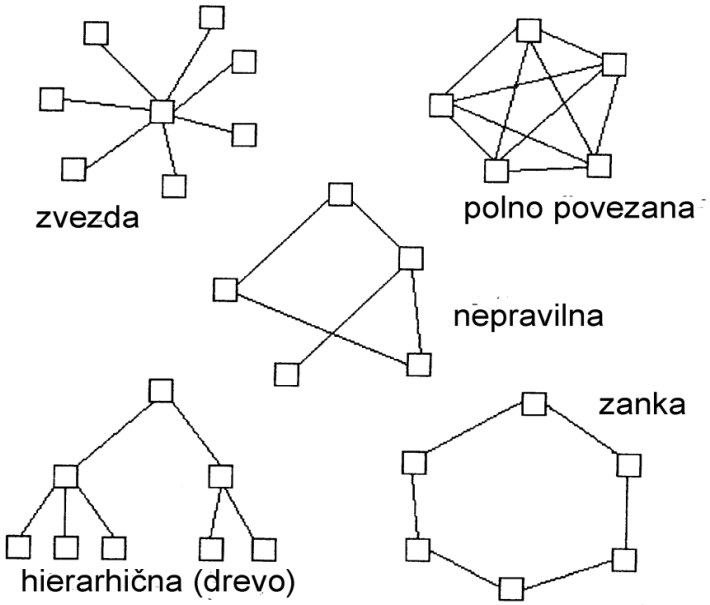
1 megahertz (MHz) = 1 million hertz

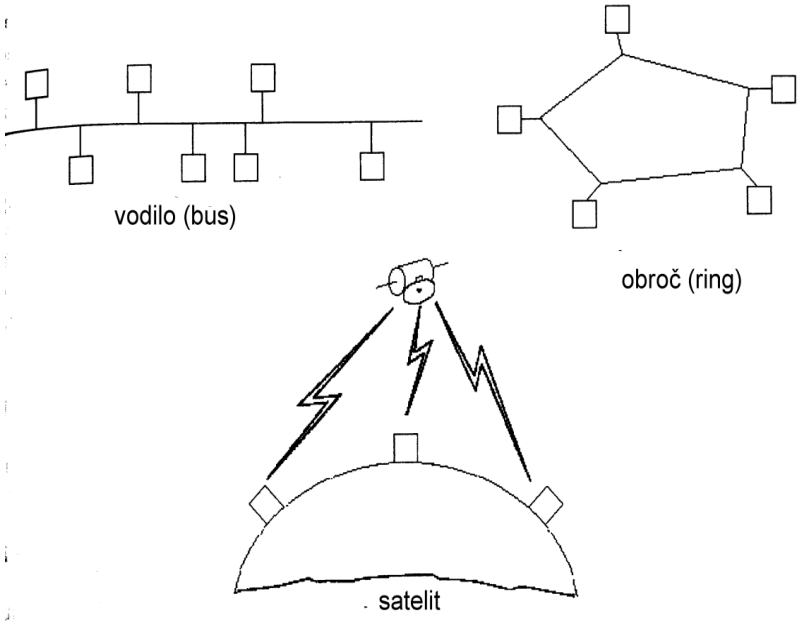
1 gigahertz (GHz) = 1 billion hertz

Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

DELITEV OMREŽIJ

- Topologija
  - Kanali tipa točka – točka
    - Komunikacija poteka samo med dvema napravama
    - Danes najpogostejši:
      - zvezda (LAN)
      - nepravilna (WAN)
  - Skupinski kanali
    - Več naprav si deli en kanal
    - vsak sistem sprejme vsa sporočila – potrebno je naslavljanje
    - Potreben je nadzor nad dostopom do kanala





OMREŽNI PROTOKOLI

Želimo zanesljivo delovanje omrežja.

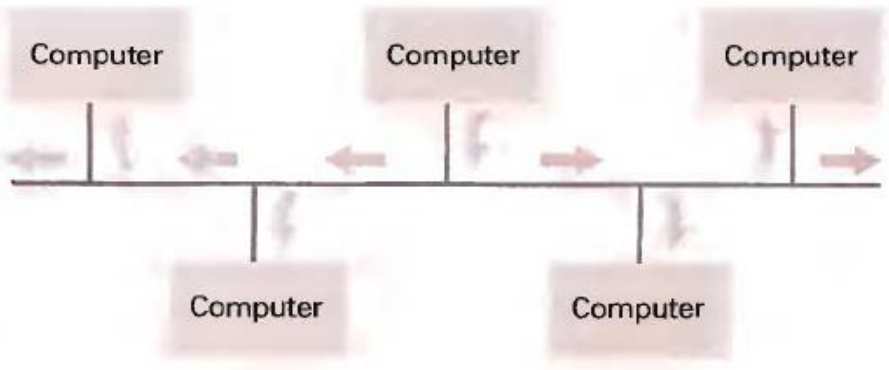
- Definirati je potrebno pravila o delovanju.
- **PROTOKOL** je zbirka pravil za komunikacijo:
  - Kdo lahko nekaj reče (odda sporočilo)
  - Kaj lahko reče
  - Kdaj lahko to reče
  - Kaj mora storiti, ko sprejme neko sporočilo
- Naprave morajo upoštevati protokol(e)

Primeri omrežnih protokolov: Ethernet, WiFi (IEEE 802.11 a/b/g/n), IP, TCP, UDP, SSL, http, POP3, ...

OMREŽNI PROTOKOLI

Protokol Ethernet – tehnologija za pošiljanje podatkov

- Teče na UTP žicah
- pravice za pošiljanje podatkov nadzoruje protokol tipa CSMA/CD (ang. Carrier Sense Multiple Access Collision Detection)
  - oddano sporočilo doseže vse računalnike v omrežju
  - vsi računalniki spremljajo sporočila, preberejo pa le tista, ki so namenjena njim
  - CS: poslušaj, preden spregovoriš
  - MA: vsi lahko govorijo hkrati (pride do trka)
  - CD: zaznavanje trkov (utihni, če govori kdo drug)
- oba računalnika neprestano spremljata pakete v omrežju,
  - ker opazita zmedo, počakata, da v omrežju ni več aktivnosti,
  - ponovno oddajanje sprožita po naključnem času (ne več hkrati)



STROJNI NASLOVI (FIZIČNI, MAC)

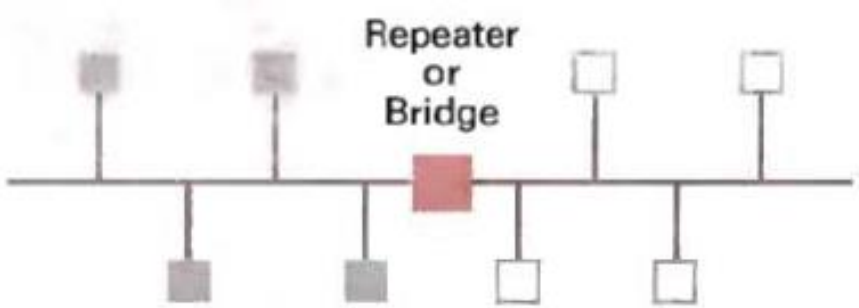
- To je naslov omrežnega adapterja, posamezni računalnik ima lahko več kot enega.
  - Npr. Ethernet, WiFI in Bluetooth
- 48 bitov oz. 12 šestnajstiških znakov, npr: 00-21-85-80-1A-B7
- Leva polovica: proizvajalec, desna: ID adapterja
- Standardi:
  - MAC-48 in EUI-48: sintaktično enaka. Uporaba: Ethernet, IEEE 802.11 (Wireless), Bluetooth,
  - EUI-64: 64-bitni, ima še dva dodatna byta za adapter. Uporaba: FireWire, IPv6, ZigBee (802.15.4)
- Posebni naslovi:
  - Broadcast FF:FF:FF:FF:FF:FF – namenjeno vsem.

POVEZOVANJE OMREŽIJ

- Lokalna omrežja povezujemo v večja omrežja in v internet)
- Omrežne naprave
  - Omrežna kartica (= vmesnik / adapter)
    - Samostojna
    - Lahko integrirana na matično ploščo
    - (10) / 100 / 1000 Mbit/s
    - Avtomatsko prilagajanje na hitrost omrežja

POVEZOVANJE OMREŽIJ - NAPRAVE

- Ojačevalnik (ang. repeater)
  - prenaša **vse** signale iz prvega omrežja v drugo in nazaj
  - tipična uporaba
    - združevanje omrežij, ki uporabljata različne medije za prenos signalov (žica in optično vlakno)
    - Za ojačenje signala v večjih omrežjih
- most (ang. bridge)
  - Ravno tako prenaša signale iz prvega omrežja v drugo in nazaj
  - prenaša **samo** tiste signale, ki so namenjeni v sosednje omrežje
    - promet znotraj omrežij lahko nemoteno poteka istočasno
- Danes ju redko srečamo.

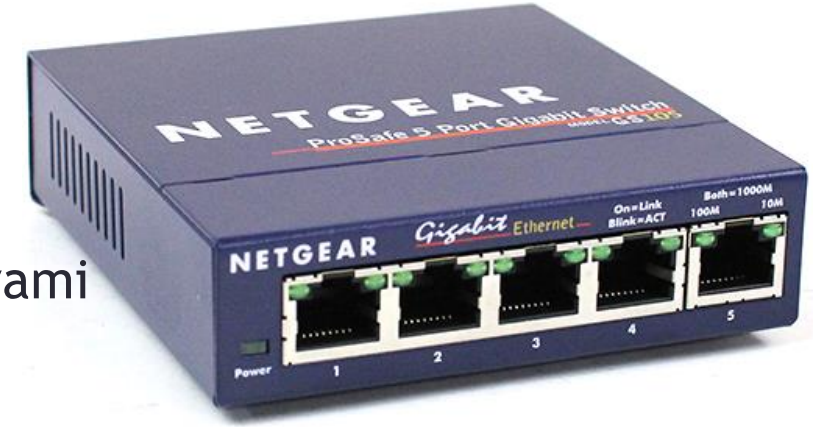


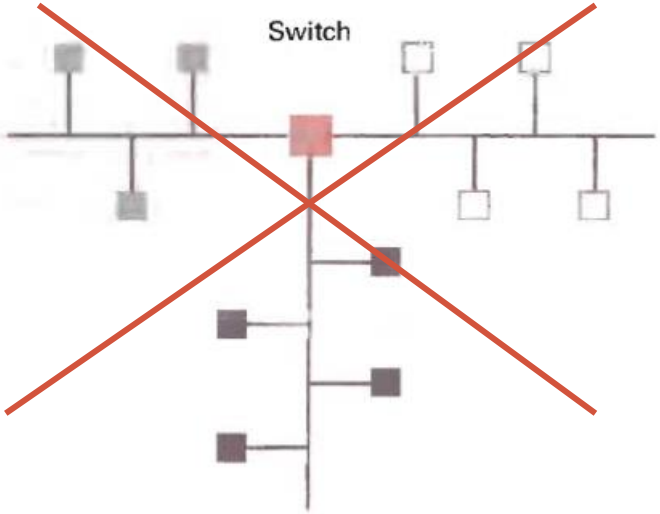
POVEZOVANJE OMREŽIJ - NAPRAVE

- Razdelilnik (ang. hub)
  - Povezuje več omrežij ali naprav
  - V bistvu je ojačevalnik z več povezavami
  - Prenaša **vsa** sporočila
  - Ne preprečuje kolizij, zato ga danes le redko še srečamo.

POVEZOVANJE OMREŽIJ - NAPRAVE

- Stikalo (ang. switch)
  - Deluje znotraj omrežja
  - je kot most z več povezavami
  - prenaša samo **potrebna** sporočila





STIKALO

- 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 (par: vmesnik – strojni naslov) in ga zapiše v tabelo.
  - Če ima ciljni naslov v tabeli, gre okvir na ta vmesnik
  - Sicer poplavi na vse vmesnike razen izvornega
- Ločuje kolizijske domene (vsak segment je svoja)
- Omogoča omrežje brez kolizij – vsak računalnik ima svojo dvosmerno povezavo (parico) do stikala.

POVEZOVANJE OMREŽIJ - NAPRAVE

Usmerjevalnik (ang. router) – več o tem kasneje!

- glavni namen je povezovanje krajevnih (LAN) in hrbtenic - prostranih omrežij (WAN)
- Primeri:
  - usmerjanje prometa med omrežji
  - povezava brezžičnega in žičnega omrežja
- NAT: računalnikov v omrežju LAN dostopa do interneta (WAN) z istim javnim IP naslovom
  - Ponovna (večkratna) uporaba istih zasebnih naslovov v različnih omrežjih

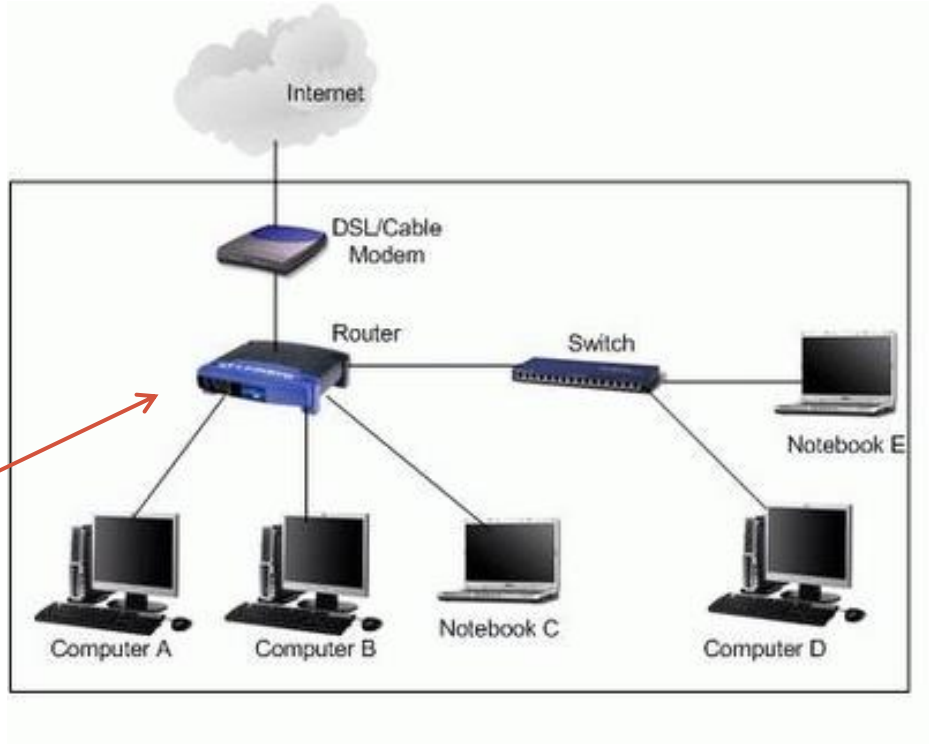
USMERJEVALNIK IN STIKALO

- Stikala: vsi vmesniki so v istem omrežju
- Usmerjevalnik: predstavlja mejo med omrežji. Vsak vmesnik je v drugem omrežju.

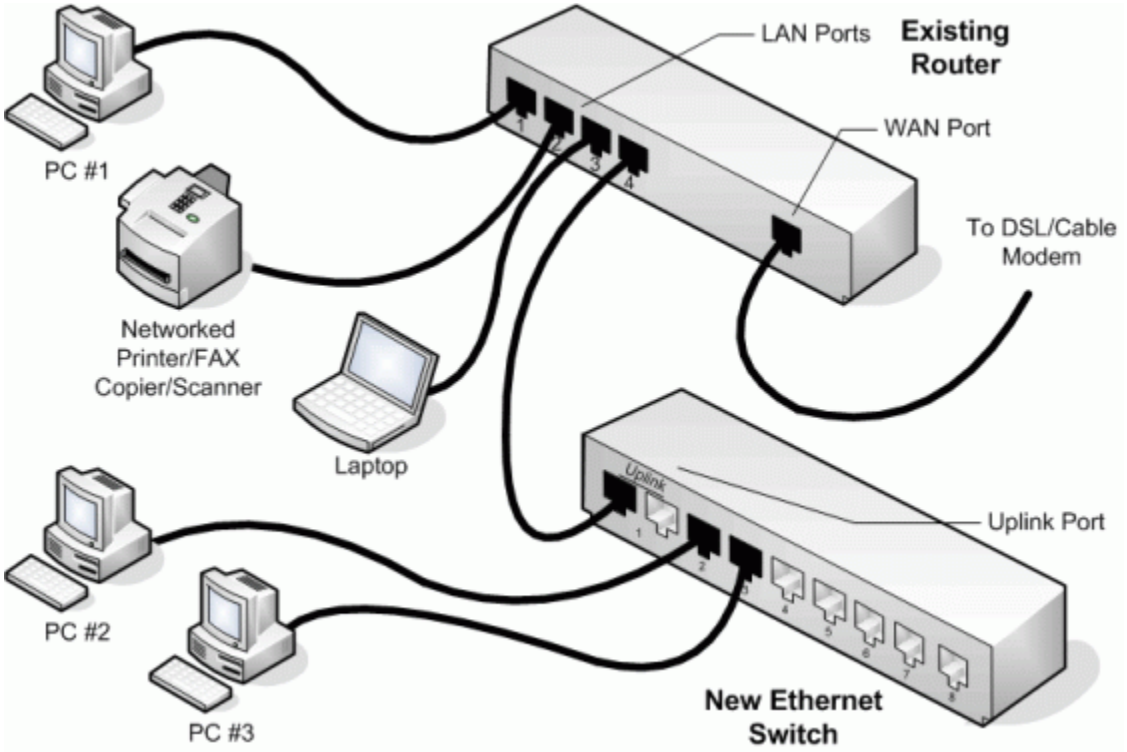
Internet –
javno omrežje

Domače (zasebno)
omrežje

Usmerjevalnik z 2
vmesnikoma in stikalo
s 4 vmesniki v eni škatli



USMERJEVALNIK IN STIKALO



ZAZNAVANJE IN ODPRAVLJANJE NAPAK

- Parnost: 1 bit. Samo zaznavanje enojnih napak.
- Parnost v 2 dimenzijah (vrstica + stolpec): zaznavanje in odpravljanje enojnih napak.
- Bolj kompliciranе formule za kontrolne vsote,
  - npr. Internet checksum (uporaba na omrežni intransportni 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). Zahtevnejše operacije (polinomske).

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
  - Primer: če je možna hitrost 10 Mb/s in imamo 10 priklopljenih naprav, bi v idealnem primeru vsaka oddajala s hitrostjo 1 Mb/s.
- Možne rešitve:
  - Razdeliti kanal, ni kolizij
  - Naključni dostop, dovoljene so kolizije, potrebno je obravnavanje kolizij.
  - Določeno je zaporedje dostopov posameznih naprav do medija, ni kolizij

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 (Code Division) – GSM omrežja,
  - WDM (Wavelength Division - optika)

KOLIZIJSKI PROTOKOLI (NAKLJUČNI DOSTOP) 1

- Določajo:
  - kako zaznati kolizijo
  - Kako ukrepati ob koliziji

- Prvi protokol: ALOHA - paket je ranljiv ves čas oddajanja
  - Preprost, nizka prepustnost (18%)
  - Kolizija: počaka naključen čas, nato spet odda

KOLIZIJSKI PROTOKOLI 2

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

NEKOLIZIJSKI PROTOKOLI - PROTOKOLI Z IZMENIČNIM DOSTOPOM

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

BREZŽIČNO OMREŽJE

Sestavljajo ga:

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

Ad hoc omrežje:

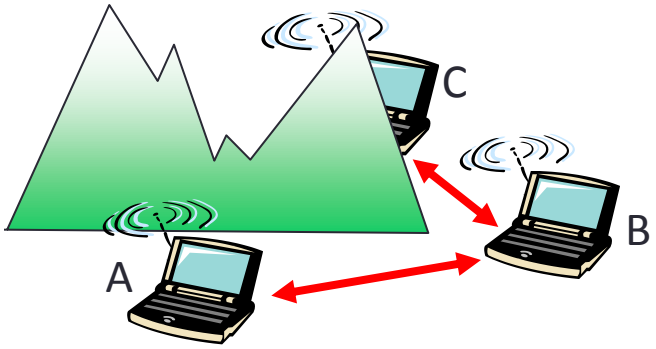
- Ni baznih postaj: pošiljanje le odjemalcem, ki so v dometu
- Vozlišča se lahko tudi organizirajo v omrežje z lastnim usmerjanjem (MANET – mobile ad hoc network; VANET – vehicular ad hoc network)

MESH (mreža): več skokov v brezžičnem omrežju, preden pride do ožičene infrastrukture (npr. WiFree Ljubljana)

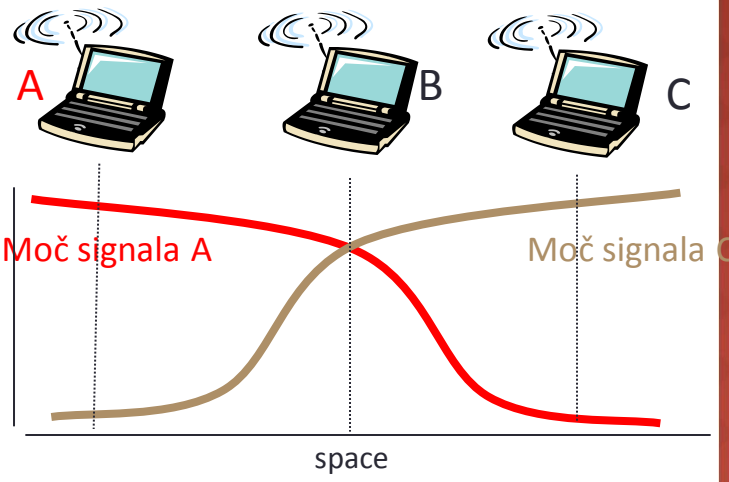
BREZŽIČNA POVEZAVA: LASTNOSTI IN TEŽAVE

- 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



STANDARDI IEEE 802.11 (WI-FI)

(ne se tega učiti na pamet!)

- 802.11a (krajše razdalje, do ca. 120 m), OFDM (FDMA)
  - 5-6 GHz, do 54 Mb/s (tipično 23)
- 802.11b (do ca. 140 m), OFDM
  - 2.4 do 5 GHz, do 11 Mb/s (tipično 4.5)
  - DSSS (direct sequence spread spectrum), ista koda
- 802.11g (do ca. 140 m), OFDM in DSSS
  - 2.4-5 GHz, do 54 Mb/s (tipično 19)
- 802.11n OFDM
  - 2.4-5 GHz, do 600Mb/s (150 na stream), do ca. 250 m
  - MIMO (multiple input, multiple output: uporabi tudi multipath signal); Channel bonding (do 4)
- 802.11ac („Wave 2“) - 5 GHz, do 8 vzporednih tokov, do 866Mb/s
- 802.11ad do 6.75 Gb/s (60 GHz, pasovna širina > 2GHz)
- 802.11 af, ah: ... (še v razvoju..)
- VSI: CSMA/CA, delovanje: ad hoc in bazne postaje

PRINCIPI DELOVANJA WLAN (WIFI)

- Uporaba na omejenih področjih (stavba)
- Prihodnost:
  - fiksna brezžična omrežja - npr. za last-mile širokopasovne povezave nekaj km
  - Mobilni telefon z WLAN + VOIP (poceni pogovor mimo operaterja 3G)
- 2.4 GHz področje: 11-14 kanalov različnih frekvenc (niso povsod vsi dovoljeni – regulativa). Administrator izbere kanal za AP. Uporabnik skenira kanale, ko išče AP.

PRINCIPI DELOVANJA WLAN

- **Mehanizem CSMA / CA:**
- **carrier sense (CS - poslušaj preden govoriš):**
  - posluša pred oddajo.
  - ni detekcije kolizij (med oddajanjem je sprejemnik izključen)
- **collision avoidance - izogibanje kolizijam (CA- vprašaj za dovoljenje, preden spregovoriš)**
  - Več algoritmov, npr. MACAW (Multiple Access Collision Avoidance for Wireless),
  - Postaja si "rezervira" kanal:
    - Odda RTS (request to send)
    - Prejme CTS (clear to send: vsebuuje podatek, katera naprava lahko oddaja in koliko časa lahko oddaja)
  - Šele po prejemu CTS odda podatke.
  - CTS slišijo vsi, zato počakajo in drugi ne oddajajo: kot posledica v podatkih ne pride do kolizij.

- **Uporablja se sprotno potrjevanje prejetih paketov (preden oddamo naslednji paket, počakamo na potrditev prejšnjega).**

PROTOKOL VKLJUČEVANJA V WLAN

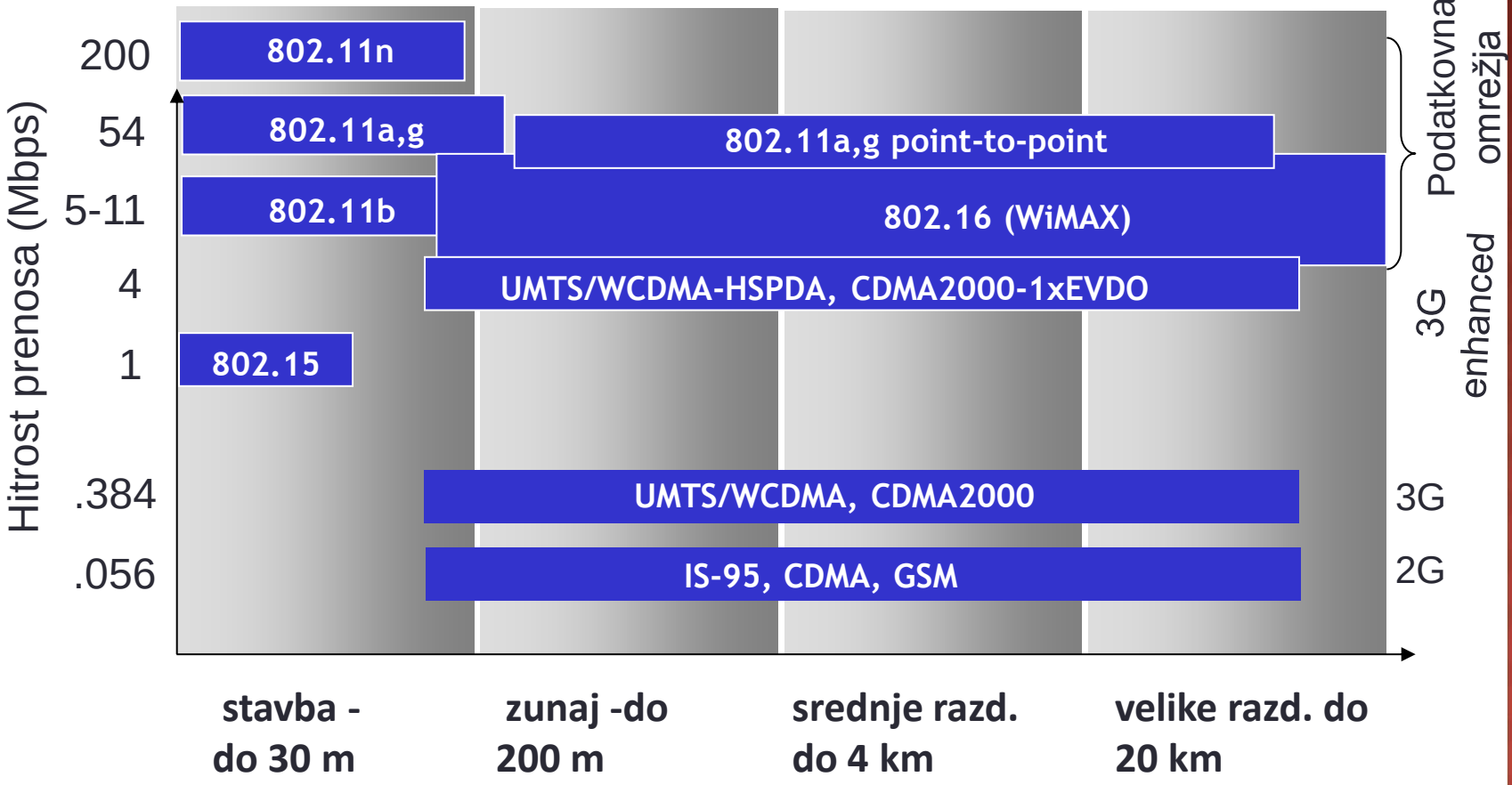
- **Postopek aktivne izbire pristopne točke** – *scanning* :
  - Probe (*Je v bližini kak AP?*)
  - Probe response (*Jaz sem AP*)
  - Association Request (*Rad bi se pridružil*)
  - Association Response (*Kar izvoli*)
- **Pasivna izbira** (passive scanning)
  - AP periodično oddaja *beacon frame (“Jaz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

STANDARDI IEEE 802.15 – OSEBNO OMREŽJE

- Razvoj iz Bluetooth specifikacije
  - 2.4 – 2.5 GHz, do 721 kb/s
  - 79 kanalov, TDM, frequency hopping
- IEEE 802.15.3-2003 (osnova): 11-55 Mb/s
  - 802.15.3-2009: 3 Gb/s
  - 802.15.6: BAN: Body Area Network (zdravje, zabava) – majhna moč in razd.
  - 802.15.7: VLC – visible light communication (uporablja svetlobo)
- PAN – personal area network: manj kot 10 m, uporaba namesto kablov (za miš, slušalke...)
- To je „ad hoc“ omrežje.
- Vloge naprav: gospodar in sužnji.
- Gospodar (npr. PC) mora sužnjem (npr. miški) dovoliti oddajanje

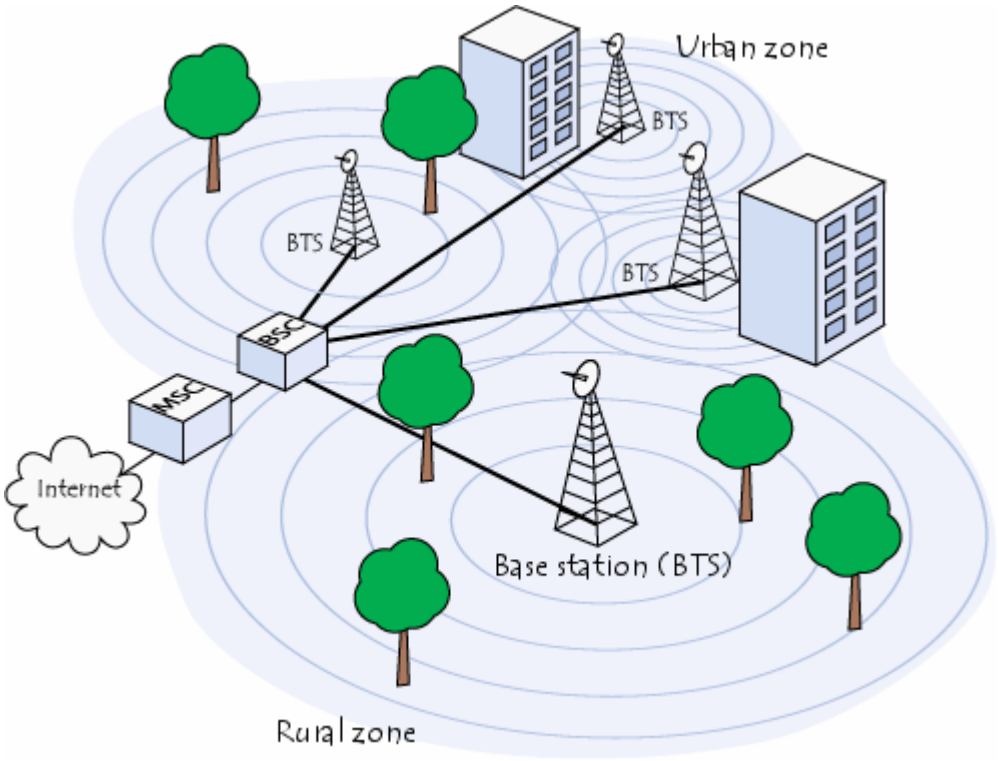
LTE

BREZŽIČNA OMREŽJA: PREGLED TEHNOLOGIJ



CELULARNA OMREŽJA

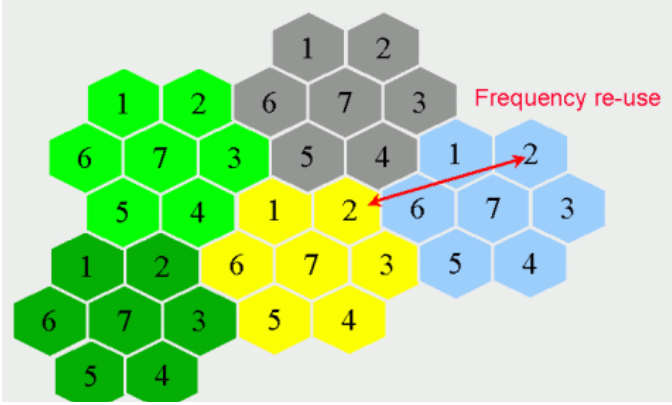
- Bazne postaje, mobilni uporabniki, žično omrežje



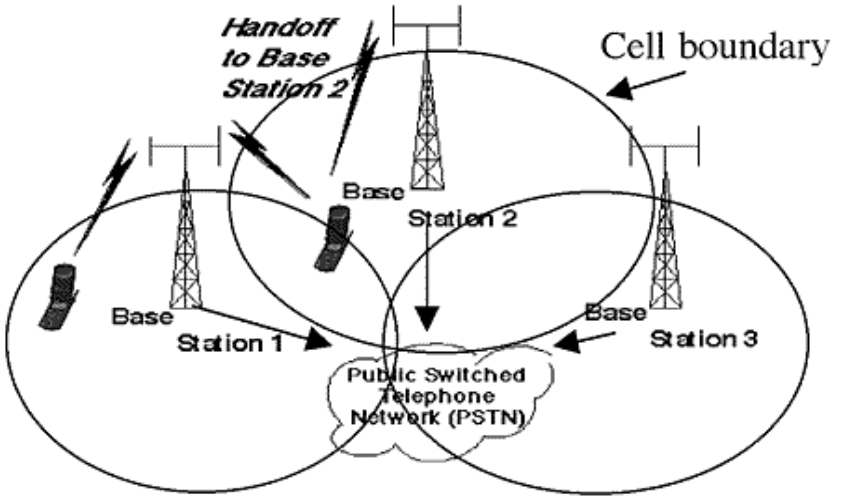
CELULARNA OMREŽJA

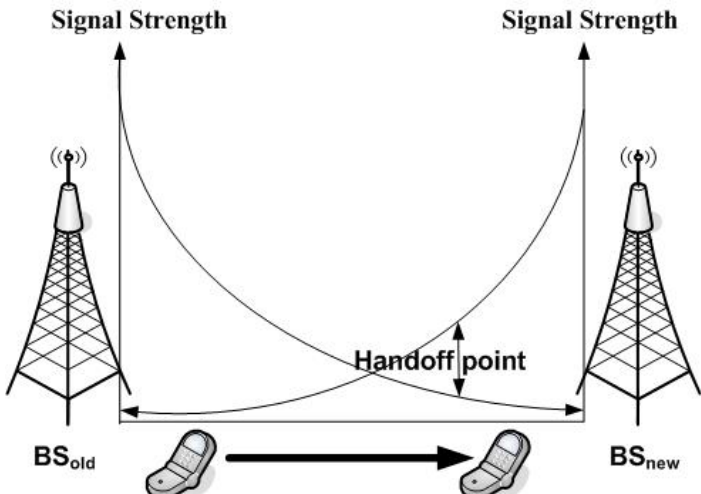
- Kombinacija FDMA/TDMA (GSM) ali CDMA
- Generacije
  - 1G: zvok (analogno - NMT)
  - 2G: zvok (GSM), FDMA+TDMA, podatki do 19 kb/s
  - 2.5G: zvok + podatki (GPRS, EDGE, CDMA) do 200 kb/s
  - 3G: UMTS, EDGE (2¾ G?), CDMA 2000, HSDPA/HSUPA, WCDMA, po standardu do 1-2 Mb/s, v praksi manj. (3.5G – tudi hitreje)
  - 4G: (LTE, Mobile WiMAX - Koreja) vseprisoten, gigabitne hitrosti (video, HDTV, telekonference), 100 Mb/s za veliko hitrost gibanja, 1 Gb/s za nizko hitrost (peš).

DELOVANJE CELULARNEGA OMREŽJA



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





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

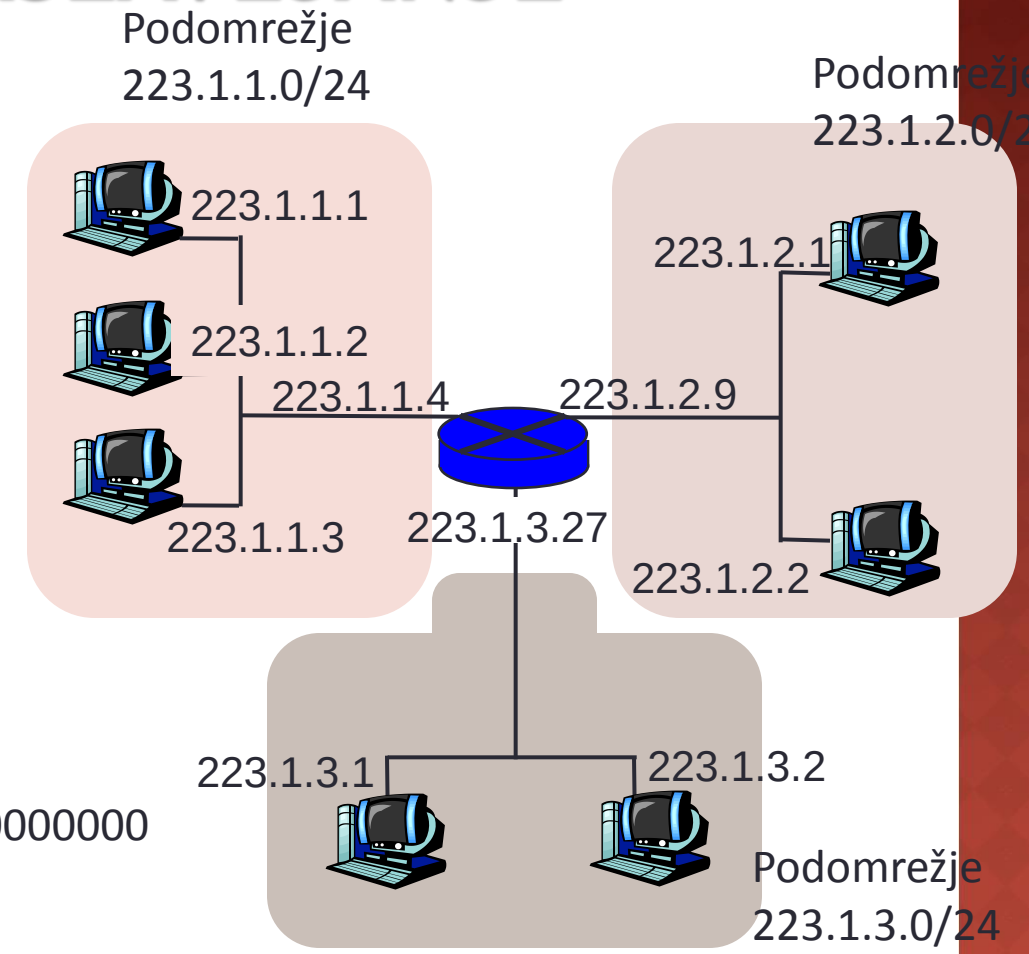
Usmerjevalnik ima na vsakem vmesniku drugo (pod)omrežje.

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...

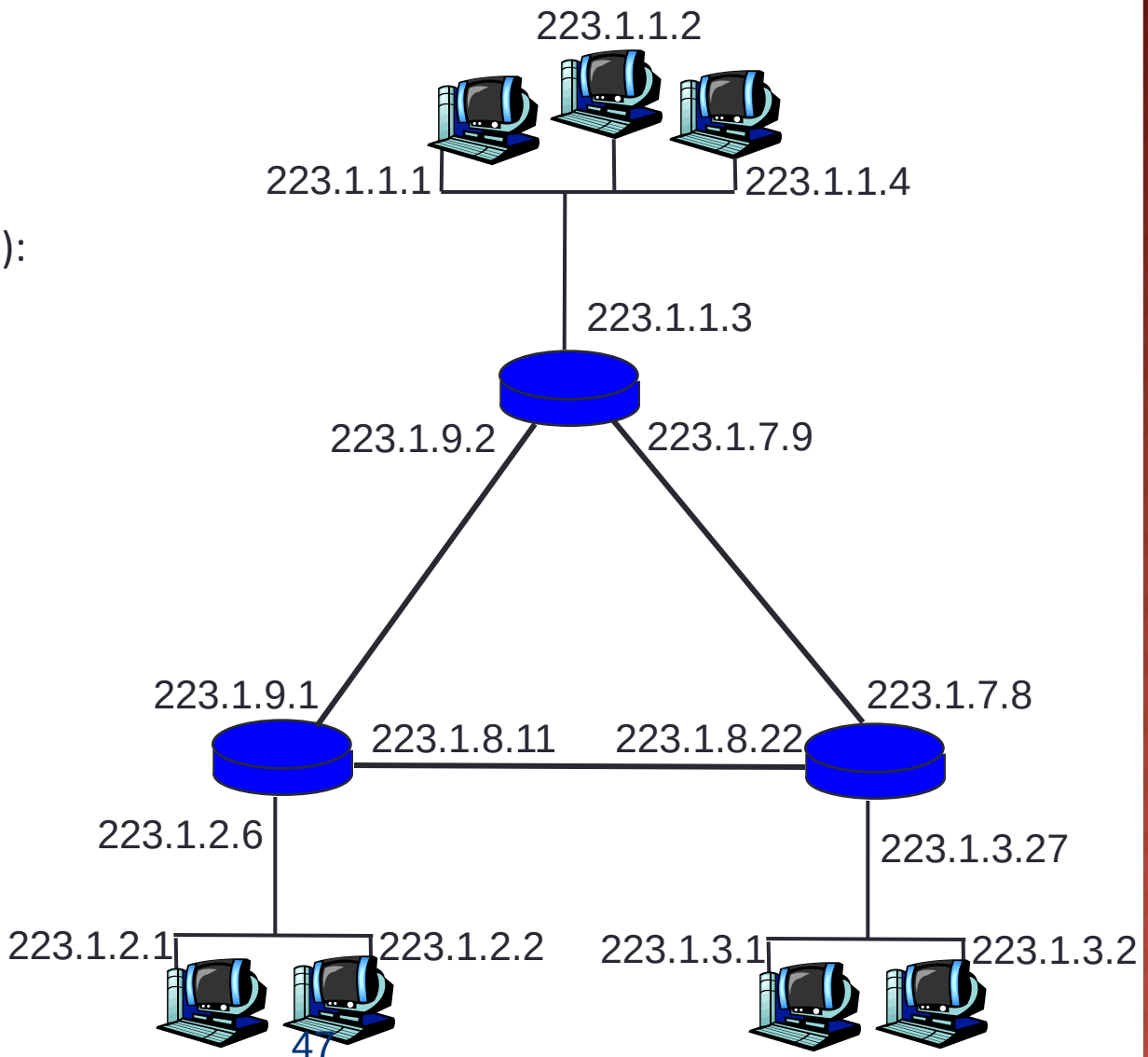


Znotraj (pod)omrežja ni usmerjevalnikov, so pa lahko stikala (switch) in razdelilniki (hub).

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



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.

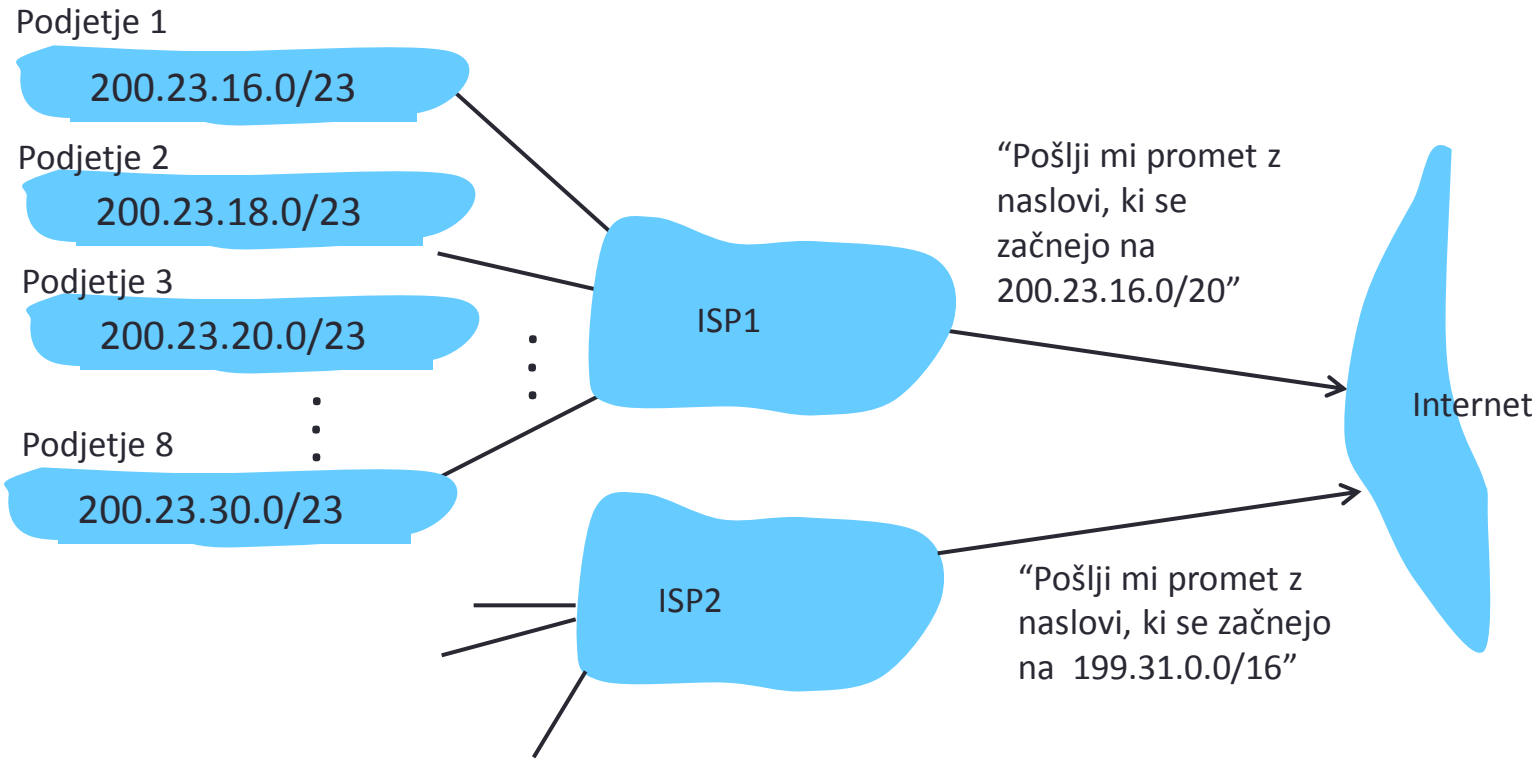
ISP-jev blok:	11001000 00010111 00010000 00000000	200.23.16.0/20
Podjetje1:	11001000 00010111 00010000 00000000	200.23.16.0/23
Podjetje2:	11001000 00010111 00010100 00000000	200.23.18.0/23
…	…	…

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

HIERARHIČNO NASLAVLJANJE

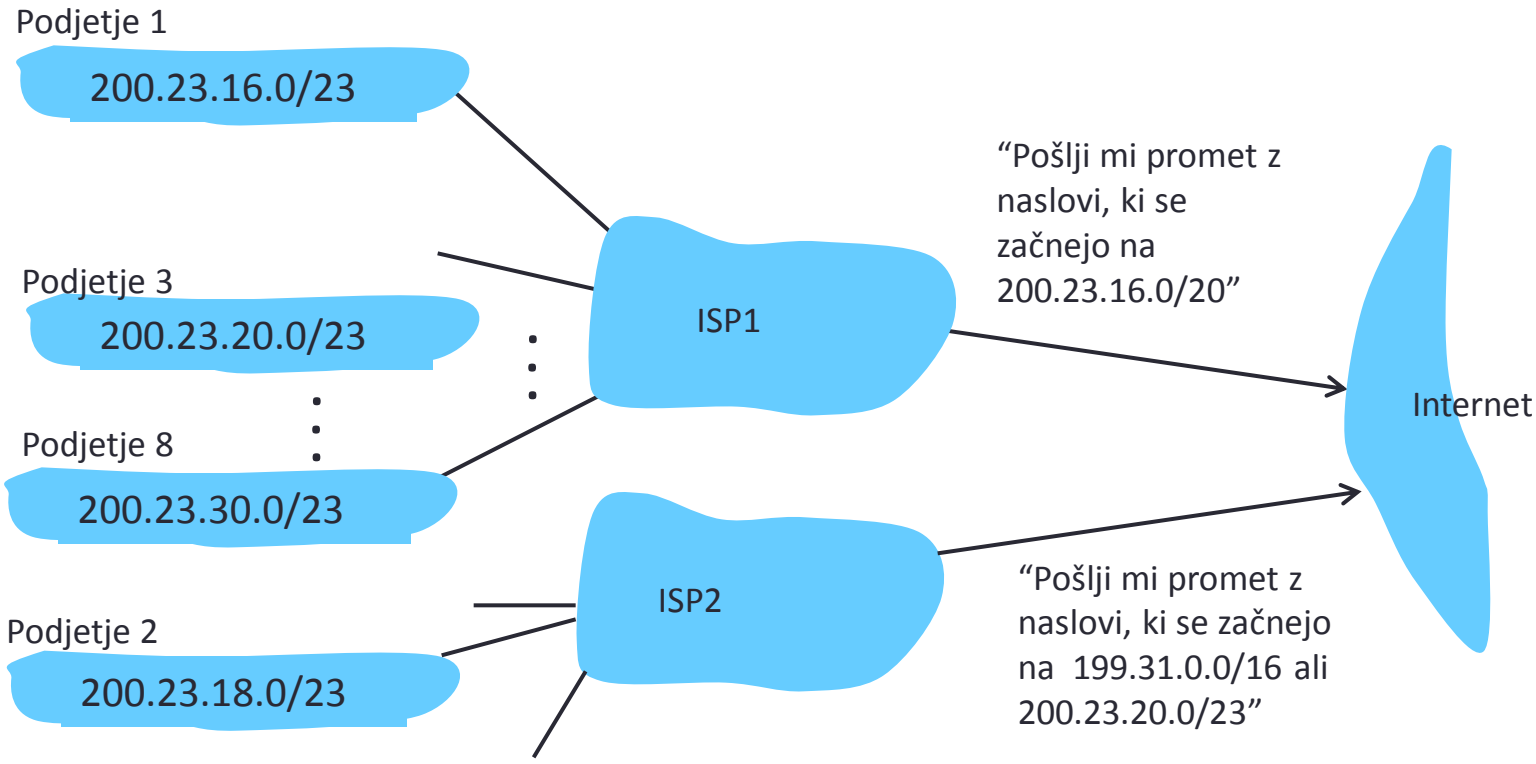
Pravilno dodeljevanje CIDR naslovov olajša usmerjanje!

Agregiranje ali sumarizacija naslovov – en prefiks za usmerjanje v več omrežij.

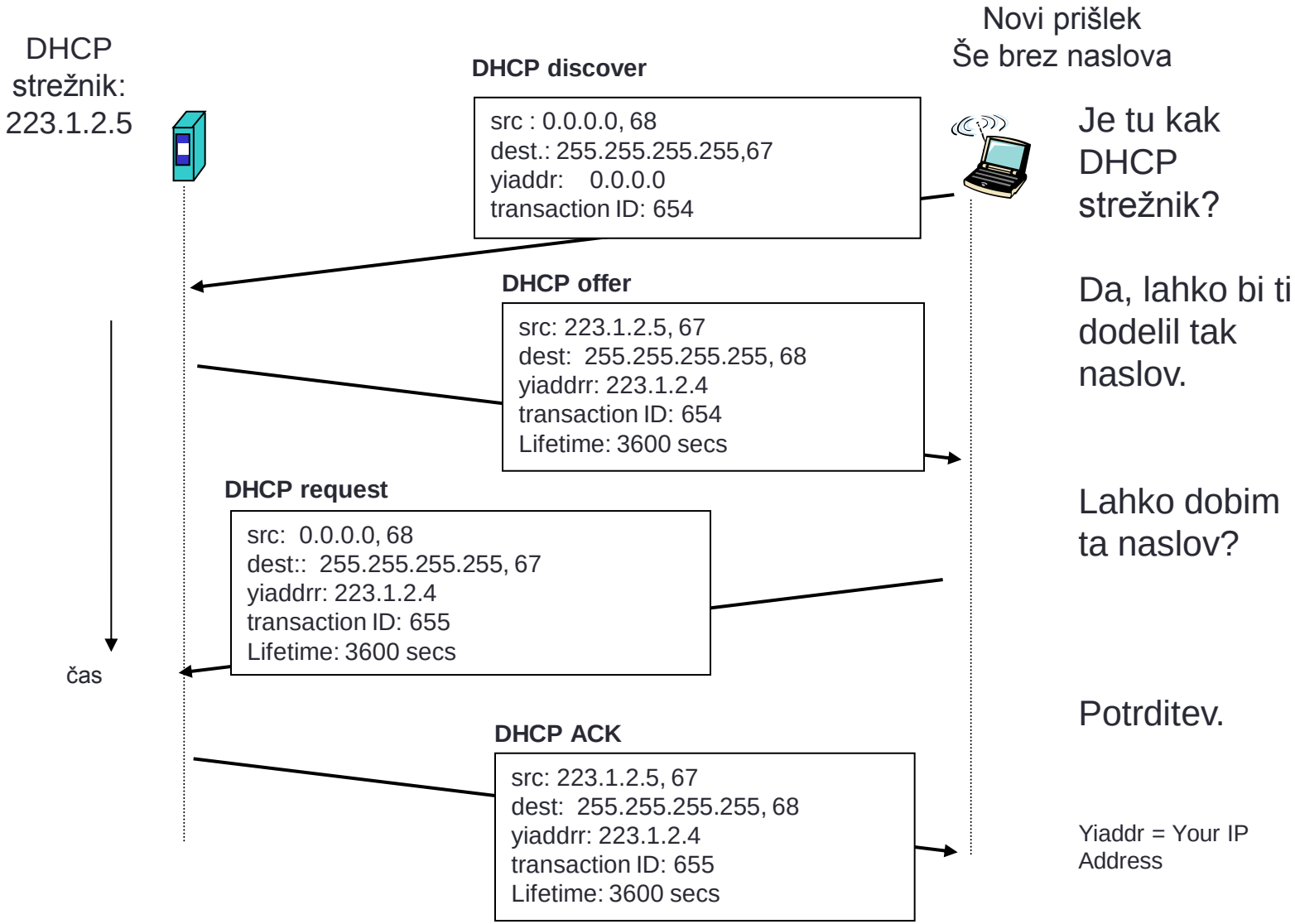


MANJ UČINKOVITO NASLAVLJANJE

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



DODELITEV NASLOVA S POMOČJO DHCP



Je tu kak DHCP strežnik?

Da, lahko bi ti dodelil tak naslov.

Lahko dobim ta naslov?

Potrditev.

Yiaddr = Your IP Address

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

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}

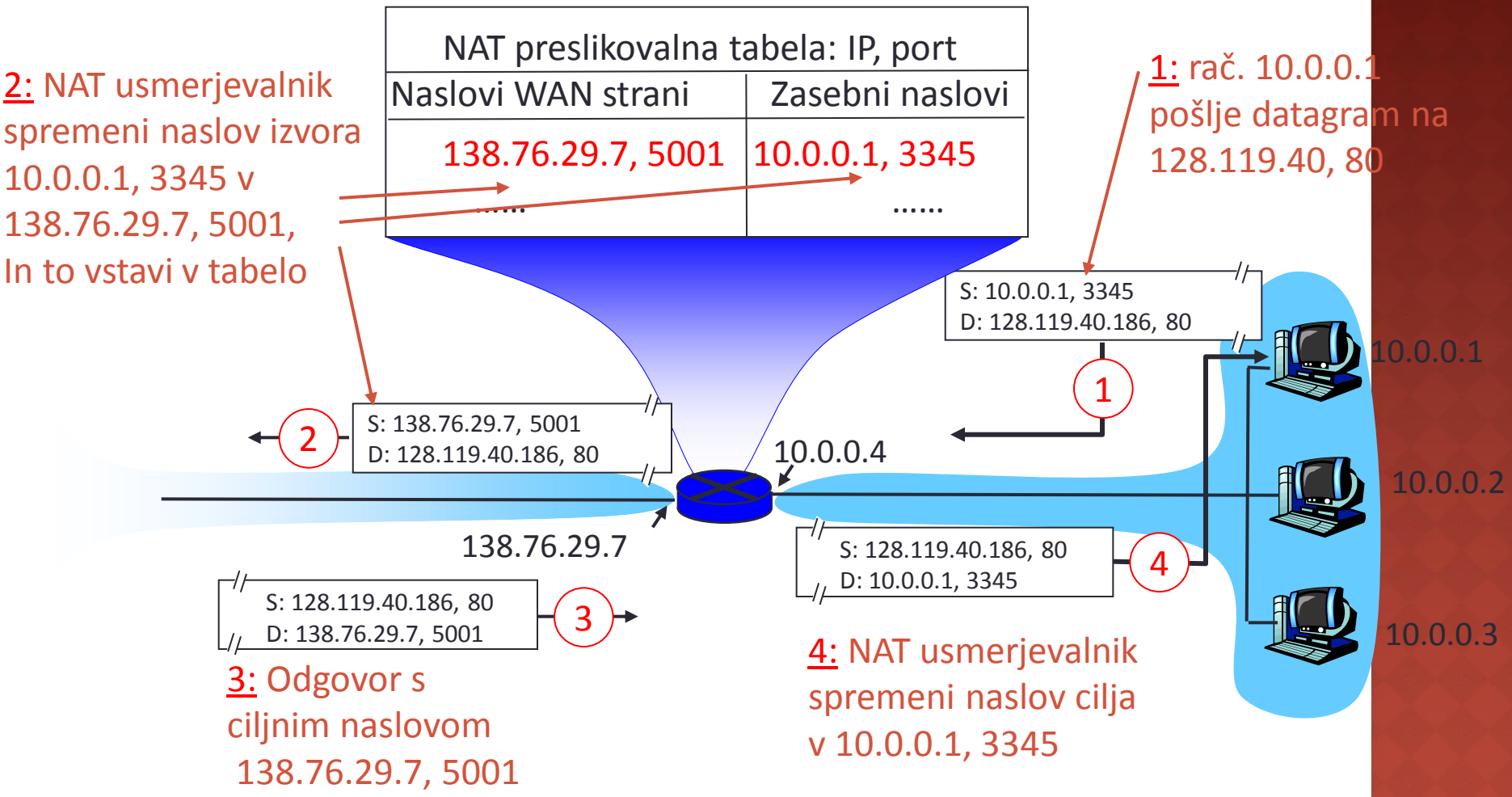
- Zasebni (notranji, interni) naslovi se uporabljajo le znotraj omrežja.
- Na NAT usmerjevalniku se naslov preslika v zunanji naslov.

NAT - NETWORK ADDRESS TRANSLATION

- 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

NAT/PAT


NAT preslikovalna tabela: IP, port
Naslovi WAN strani
Zasebni naslovi
138.76.29.7, 5001
10.0.0.1, 3345
.....
.....
2: NAT usmerjevalnik spremeni naslov izvora 10.0.0.1, 3345 v 138.76.29.7, 5001, In to vstavi v tabelo
1: rač. 10.0.0.1 pošlje datagram na 128.119.40, 80
S: 10.0.0.1, 3345
D: 128.119.40.186, 80
1
2
S: 138.76.29.7, 5001
D: 128.119.40.186, 80
10.0.0.4
138.76.29.7
10.0.0.1
10.0.0.2
10.0.0.3
S: 128.119.40.186, 80
D: 10.0.0.1, 3345
4
S: 128.119.40.186, 80
D: 138.76.29.7, 5001
3
3: Odgovor s ciljnim naslovom 138.76.29.7, 5001
4: NAT usmerjevalnik spremeni naslov cilja v 10.0.0.1, 3345

KRITIKA NAT-A

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

REŠITVE ZA PREHOD ČEZ NAT (NAT TRAVERSAL)

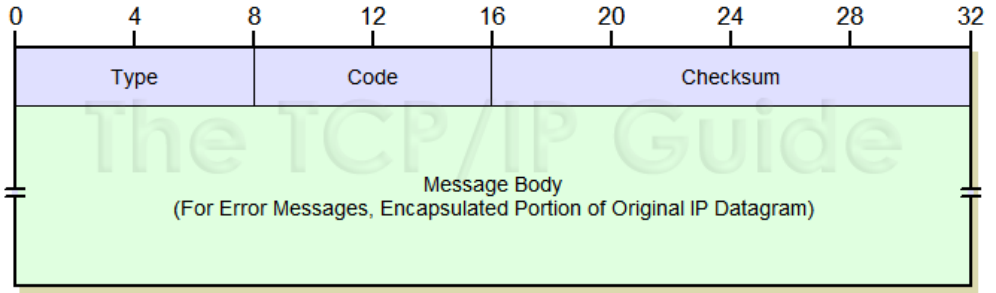
1. Statično konfiguriramo NAT – dodamo zapis v NAT tabelo (npr. 123.76.29.7, 2500 gre vedno v 10.0.0.1, 25000).
2. Universal Plug and Play (UPnP) Internet Gateway Device (IGD) protokol omogoča napravi za NATom ugotoviti zunanji IP naslov, in statične vnose v tabelo.
3. Prek posrednika: rač. za NAT-om ima stalno povezavo do posrednika, ki ni za NAT-om. Sogovornik vzpostavi povezavo s posrednikom. Posrednik posreduje promet med njima, ali pa signalizira prvemu, da vzpostavi povezavo do drugega.
   - *Connection reversal*: Peer A se poveže z B prek C-ja, s katerim ima B trenutno aktivno povezavo, in ga prosi, naj B vzpostavi povezavo z A.

ICMP (RFC 792)

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

ICMP SPOROČILA

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



TRACEROUTE

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

NAPADI NA ICMP

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

IPV6

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

PREDNOSTI IPV6

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

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

SINTAKSA IPV6 NASLOVA

- IPv6 naslov v binarni obliki :

```
00100000111011010000000001101001100000000000000000010111100111011
00000010101010100000000011111111111111000101000100111000101101O
```

- 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

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!

TRANSPORTNE STORITVE IN PROTOKOLI

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

KAJ POTREBUJE APLIKACIJA?

- Kako naj programer izbere transportni protokol?
  - Kaj nudi TCP in kaj UDP?
  - Analogija: 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

STORITVE TCP-JA

- Povezana storitev *(povezavno usmerjena, connection-oriented)*
  - 1.faza – rokovanje - handshaking: vzpostavljanje TCP povezave (kontrolna sporočila)
  - 2.faza – prenos podatkov (aplikacijskih sporočil, zapakiranih v TCP pakete), 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.

STORITVE UDP-JA

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

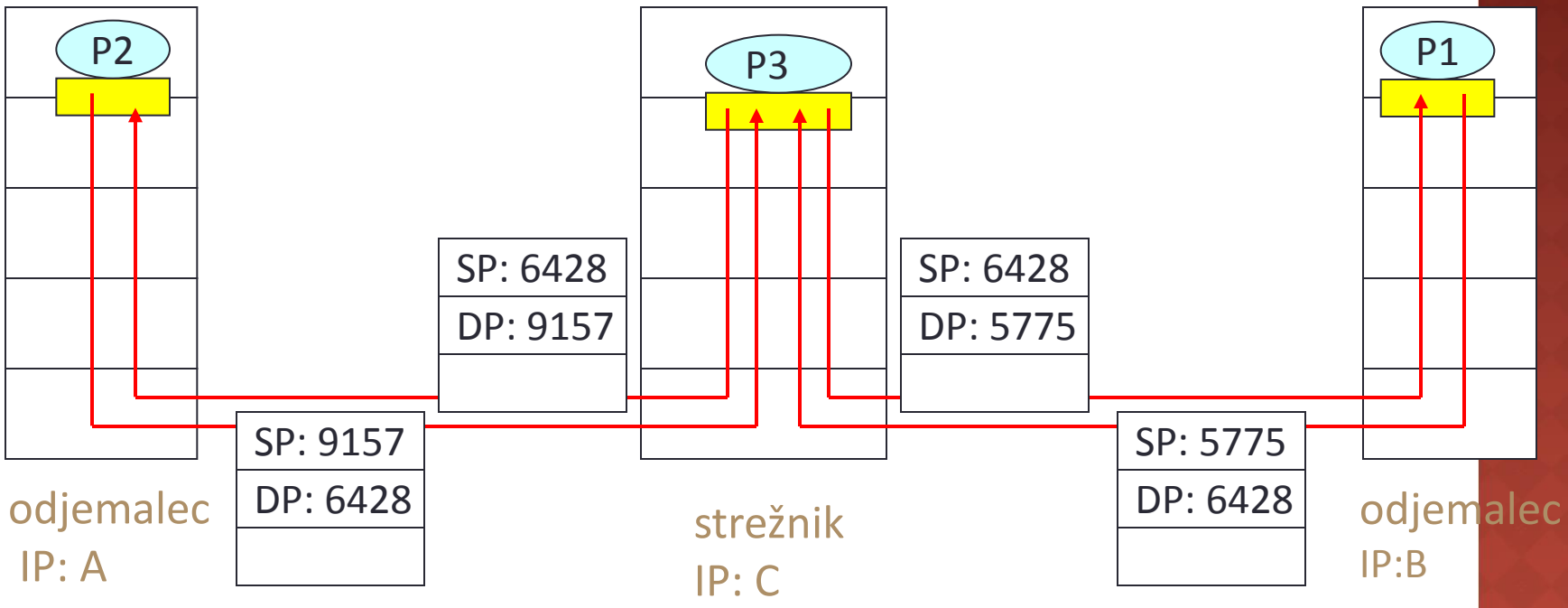
KAKO NASLOVITI PROCES NA DRUGI STRANI?

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

NASLAVLJANJE PROCESOV – KAKO?

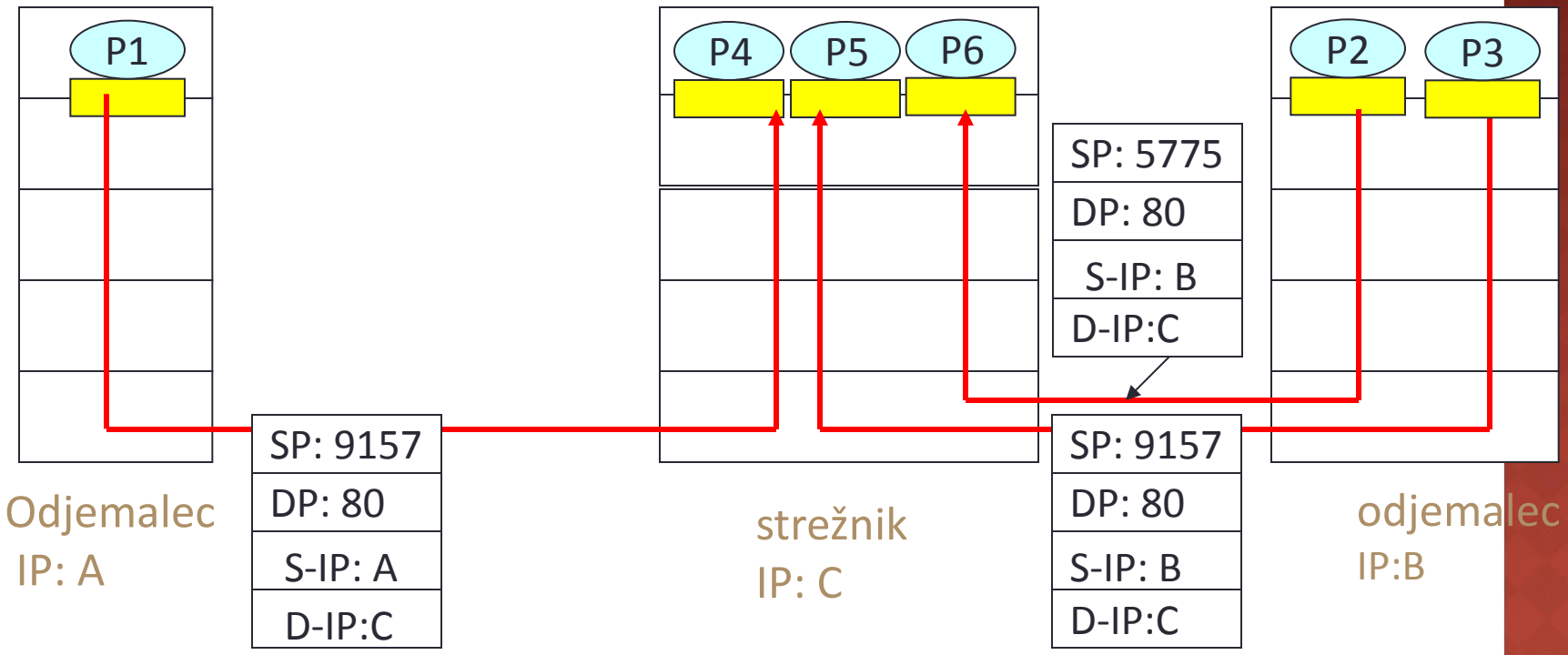
- IP paket ima IP naslova izvora in ponora
  - nosi en transportni segment
- Transportni segment ima št. vrat izvora in ponora
- Ciljni računalnik:
  - IP naslov + številka vrat → ugotovi pravi socket
- UDP vtič (končna točka) je določena s parom:
  - dest IP, dest port
  - UDP strežnik (sprejemnik) lahko sprejema iz različnih IP naslovov ali vrat hkrati
- TCP vtič:
  - source IP, source port, dest IP, dest port
  - Vsak proces ima lahko več vtičev (končnih točk)

UDP NASLAVLJANJE - PRIMER

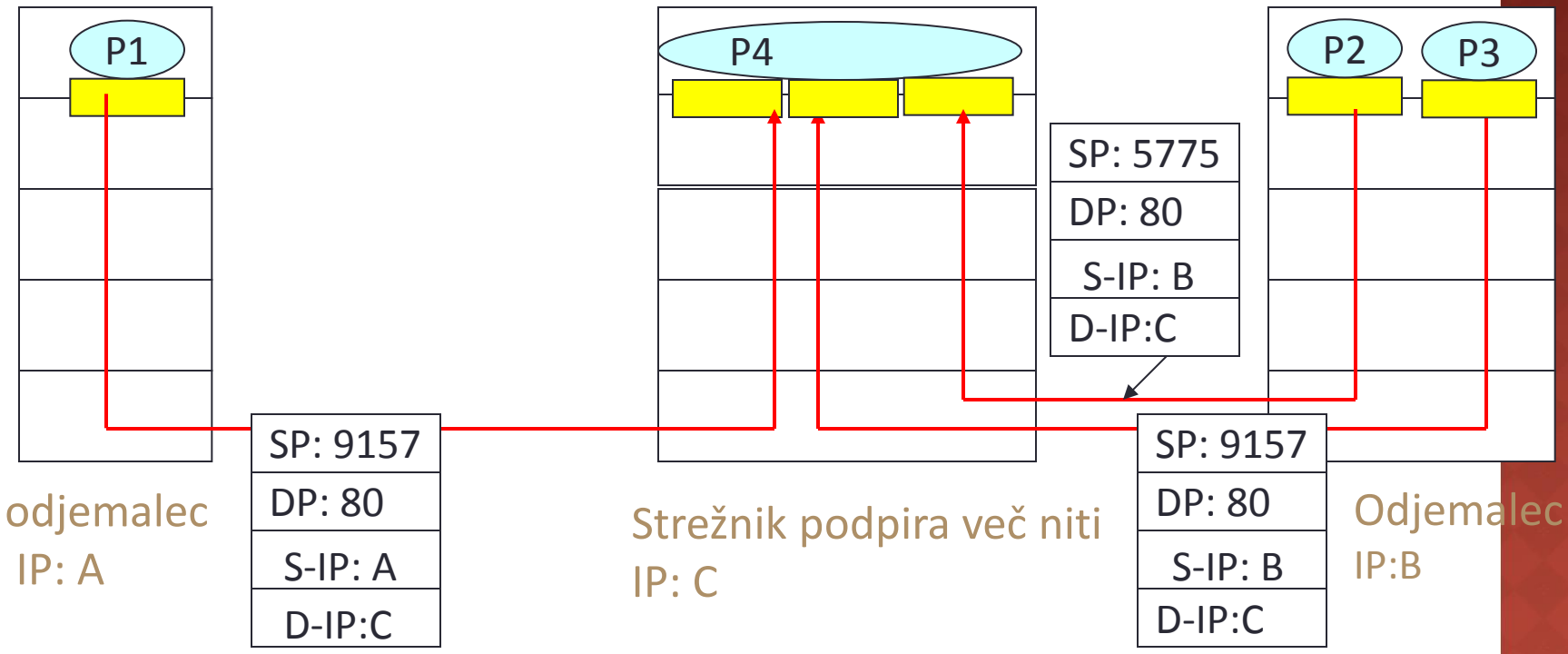


SP = source port (predstavlja naslov za odgovor)
DP = destination port

TCP NASLAVLJANJE - PRIMER



TCP NASLAVLJANJE - PRIMER Z NITMI



INTERNETNE APLIKACIJE

- Tradicionalne
  - elektronska pošta
  - prenos datotek
  - oddaljeni dostop do računalnikov
  - svetovni splet
- Novejše
  - internetna telefonija
  - oddajanje radijskega signala in televizijske slike
  - P2P

INTERNETNE APLIKACIJE: ELEKTRONSKA POŠTA

- ang. electronic mail, email
- ena najbolj uporabljanih aplikacij
- za elektronsko pošto skrbi poštni strežnik
  - računalnik z namensko programsko opremo
  - Uporabniški računalniki pošiljajo na poštni strežnik
  - poštni strežnik jo razpošilja na druge poštne strežnike
  - prejeta pošta je shranjena na ciljnem poštnem strežniku, dokler je uporabnik ne pobere
- Elektronski naslov:
  - Zgradba: oznaka_osebe@oznaka_strežnika
  - Primer: mojca.ciglaric@fri.uni-lj.si

INTERNETNE APLIKACIJE: ELEKTRONSKA POŠTA

- Protokoli
  - SMTP (ang. Simple Mail Transfer Protocol)
    - Oddajanje pošte na strežnik, komunikacija med strežniki
  - POP (ang. Post Office Protocol)
    - POP3
    - Za prevzem pošte s strežnika na svoj računalnik, kjer jo preberemo
    - Primerno predvsem, če za branje pošte uporabljamo en sam računalnik
  - IMAP (ang. Internet Message Access Protocol),
    - pošta se hrani na strežniku
    - Na strežniku rabimo veliko prostora
    - primerno, če za branje uporabljamo več računalnikov
    - Varnejši protokol – omogoča šifriran prenos
  - Exchange

INTERNETNE APLIKACIJE: PRENOS DATOTEK

- aplikacija tipa odjemalec - strežnik
  - poseben program,
  - Protokol razumejo tudi brskalniki
- protokol
  - FTP (ang. File Transfer protocol),
  - SFTP (ang. Secure FTP) – šifriran (varnejši prenos)
  - shrambe za datoteke
  - primer: ftp://ftp.arnes.si
- Novejši: sistemi „enak z enakim“ (P2P)
  - Bittorrent
  - eMule, eDonkey ...

INTERNETNE APLIKACIJE: ODDALJENI DOSTOP

- TELNET (ang. TELetype NETwork)
  - dostop na oddaljeni sistem v obliki ukazne vrstice
  - komunikacija ni šifrirana
    - prenašanje uporabniških imen in gesel ni varno!!!
- SSH (ang. Secure Shell)
  - dostop v obliki ukazne vrstice,
  - šifriranje sporočil
- RDP (ang. Remote Desktop Connection)
  - Microsoftov protokol za dostop do namizja oddaljenega računalnika

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- Aplikacija namenjena širjenju večpredstavnih vsebin po Internetu
  - ang. world wide web, www, w3
- Koncept nadbesedila (ang. hyper text)

  Nekoč besedilo in povezave, nato tudi drugi objekti: slike, zvok in video, ...
  - dokument (spletna stran), vsebuje povezave na druge dokumente (spletne strani)
    - z izbiro povezave se premaknemo na povezani dokument
    - povezani dokumenti so fizično lahko na kateremkoli računalniku v Internetu
    - spletna mesta (ang. websites) gostijo veliko število dokumentov

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- Izvedba
  - Programska oprema
    - spletni strežniki (ang. web servers)
    - odjemalci – brskalniki (ang. browsers)
  - Protokol za prenos dokumentov
    - HTTP (ang. Hyper Text Transfer Protocol)
    - HTTPS (ang. Hyper Text Transfer Protocol Secure)
  - Naslov dokumenta v spletu
    - Oblika URL (ang. Unified Resource Locator)
      - vključuje vso informacijo, potrebno za dostop do dokumenta

http://www.fri.uni-lj.si/si/osebje/270/oseba.html

protokol | spletni strežnik | mapa na strežniku | naziv dokumenta

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- HTML (ang. HyperText Markup Language)
  - besedilo je opremljeno s posebnimi simboli ali oznakami,
  - **ki določajo tip in posledično izgled besedila**
    - označbe so zapisane med znakoma <>
    - vsak dokument je sestavljen iz
      - glave med označbama <head> in </head> in
      - telesa med označbama <body> in </body>

```
<html>
<head>
<title> Demonstracija
</title>
</head>
<body>
<h1> Prvi poskus </h1>
<p> Pozdravljeni, to je naš prvi
spletni dokument. </p>
<p> Pritisnite
<a href="http://www.google.com">
tukaj
</a>
za premik na drugo spletno
stran.
</p>
</body>
</html>
```

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- Aktivnosti odjemalca in strežnika
  - Osnovne
    - Najprej v brskalnik vpišemo naslov URL strani, ki jo želimo odpreti
    - Brskalnik kot odjemalec bo prek protokola http prosil spletni strežnik, naveden v naslovu URL, da mu pošlje kopijo želene strani
    - Če stran obstaja, jo bo strežnik poslal brskalniku
    - Brskalnik nato prebere besedilo z označbami in jih pravilno prikaže na zaslonu
  - Dodatne aktivnosti
    - V primeru, da želena stran vsebuje animacije, mora strežnik poleg nadbesedila poslati tudi podatke, potrebne za izvedbo animacije. Animacijo nato izvede brskalnik pri uporabniku.
      - primer: animacije Flash, filmi, …
    - V primeru vpisovanja podatkov na internetno stran pa le-te obdela strežnik in glede na vnose prilagodi prikaz naslednjih strani
      - primer: iskalniki, obrazci za registracijo
  - Protokol http: zahteva, odgovor

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- Aktivnosti odjemalca in strežnika
  - Varnost in etičnost
    - odjemalci iz strežnikov lahko prenašajo kodo, ki jo nato izvajajo
    - odjemalci lahko zahtevajo izvajanje kode na strežniku
    - če nimamo ustreznih varoval, se izvede vse kar želi sogovornik
    - To je raj za zlonamerno kodo!!!

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- Sistemi za izvedbo aktivnosti
  - Na strani brskalnika (odjemalca)
    - JavaScript (Netscape Communications)
      - vključen v spletno stran,
      - prenese se hkrati s spletno stranjo
    - Java Applets (Sun Microsystems)
      - najprej se prenese spletna stran
      - nato se prenesejo še apleti, ki se izvedejo
    - Flash (Adobe)
      - Podobno kot Java Applets
      - Namenjen prikazu multimedijskih vsebin

INTERNETNE APLIKACIJE: SVETOVNI SPLET

- Sistemi za izvedbo aktivnosti
  - Na strani strežnika
    - CGI (Unix, ang. Common Gateway Interface) – malo zastarel
      - odjemalci so lahko zahtevali zagon programov na strežniku
    - Servlets (Sun Microsystems)
      - podobno kot CGI
    - Java Server Pages, JSP (Sun Microsystems)
      - primerno za pripravo prilagojenih spletnih strani (registracija, …)
      - podatki so shranjenina strežniku
    - Active Server Pages, ASP (Microsoft)
      - podobno kot JSP
      - predloge, iz katerih strežnik odjemalcu pripravi prilagojeno stran
    - Personal Home Page Hypertext Processor, PHP (odprto-kodno)
      - programski jezik namenjen izvajanju aktivnosti na strani strežnika
      - prilagojen za delo s spletnimi stranmi

MODELI OMREŽIJ: UVOD

- Pristojnosti komunikacijskih programov so razdeljene po plasteh

  - plast uporabnika
  - plast pošte
  - plast letalske družbe

  - uporabnik ne pozna detajlov delovanja pošte
  - pošta ne pozna podrobnosti delovanja letalske družbe

MODELI OMREŽIJ: STANDARDI

- Standardi določajo
  - plasti komunikacijskega procesa in
  - protokole znotraj vsake plasti

- Komunikacija poteka v več plasteh
  - sprememba nižje plasti (na primer fizične povezave) ne vpliva na višje plasti (na primer brskalnik)
  - za komunikacijo v omrežju lahko uporabljamo enostavne naprave, ki podpirajo samo nižje plasti

  - modeli lahko uporabljajo poljubno število plasti
  - več plasti, večja modularnost, bolj počasna omrežja

VARNOST

- Računalniki v omrežju so ogroženi
  - nepooblaščeni dostop, vandalizem
- Oblike napadov
  - Zlonamerna programska oprema (ang. malware)
    - lahko si jo nehote prenesemo na računalnik, kjer se nato izvaja
      - virusi, črvi, trojanski konji, vohljači, ribarjenje
    - računalnik lahko napade iz drugega računalnika
      - odpoved storitve, DOS (ang. denial of service)
      - neželena elektronska pošta
- Pogostost napadov
  - Za računalnik, priključen v Internet ocenjujejo, da doživi poskus napada vsakih 20 minut

VARNOST: OBLIKE NAPADOV

- Virus
  - integrira se v programe, ki so že na računalniku
  - pri izvajanju programa gostitelja se izvede tudi virus
  - namen izvajanja virusa je,
    - da se razširi še na druge programe v računalniku
    - zmanjša zmogljivosti računalnika
    - onemogoči izvajanje programov, pobriše podatke, …
- Črv
  - avtonomen program, ki se zna sam razpošiljati po omrežju
  - namen črva je lahko
    - samo razpošiljanje in s tem obremenjevanje omrežja
    - tudi bolj zlonamerne operacije

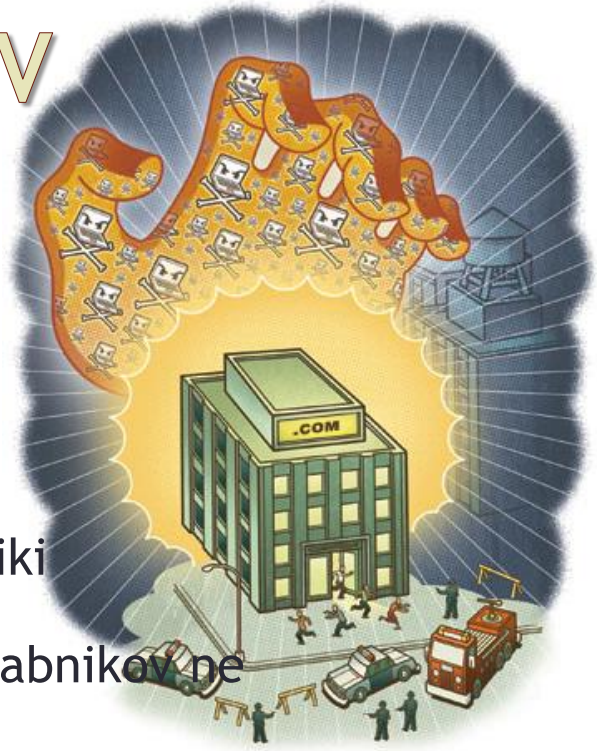
VARNOST: OBLIKE NAPADOV

- Trojanski konj
  - v računalnik ga namestimo sami kot sestavni del želenega programa (igra, orodje)
  - poleg osnovnih opravlja še dodatne funkcije, ki imajo lahko boleče posledice
  - izvajati se lahko začnejo takoj ali pa šele na točno določen dogodek (izbrani datum, …)
  - pogosto so sestavni del priponk v elektronskih sporočilih →**ne odpirajte priponk iz neznanih virov (exe, com, tudi doc, xls)**
- Vohljač
  - zbira podatke o aktivnostih, ki se izvajajo na računalniku
  - podatke pošilja pobudniku napada
  - kraja uporabniških imen, gesel, številk kreditnih kartic, …

VARNOST: OBLIKE NAPADOV

- Tehnika ribarjenja
  - podatke pridobivajo tako, da jih zahtevajo od uporabnika
  - uporabnika zavedejo z zelo podobno vsebino spletne strani, e-pošte in podobno in upajo, da bo kdo „prijel za vabo“
  - vabe se pošiljajo po elektronski pošti, v sporočilu je povezava na stran s podobnim izgledom in podobno vsebino
  - ang. fishing in phishing
  - primer: bančne prevare
    - “banka” zahteva, da naložite certifikat in vtipkate geslo!!!

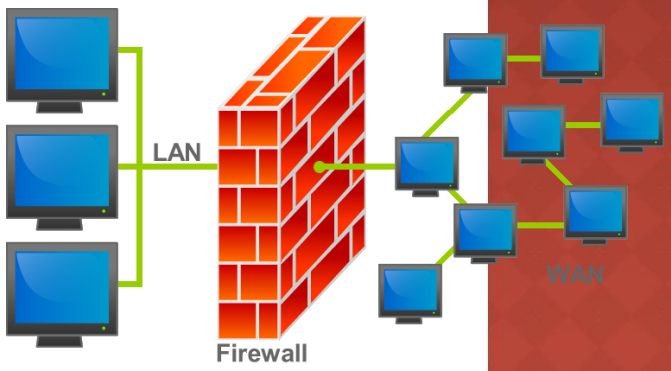
VARNOST: OBLIKE NAPADOV



- Odpoved storitve
  - ang. Denial Of Sevice, DOS
  - napadalec računalnik preobremeni
    - veliko število zahtev v kratkem času
    - Najprej okuži veliko računalnikov z ostalimi oblikami (črv, Trojanski konj)
    - Ob določenem dogodku vsi okuženi računalniki pošiljajo zahteve napadanemu strežniku
    - Če je teh zahtev veliko, zahteve pravih uporabnikov ne pridejo na vrsto.
  - pogosto so napadene velike računalniške korporacije
- Neželena elektronska pošta
  - ang. junk mail, spam
  - zloraba elektronskih sistemov za razpošiljanje pošte
  - predvsem nezaželena za bralca elektronskih sporočil
  - pogosto izhodišče za ostale oblike napadov

VARNOST: ZAŠČITA IN ZDRAVLJENJE

- Preventiva je najboljša kurativa!
- Nadzor prometa v omrežju
  - Sistemi „IP reputation“
  - požarni zid (ang. firewall) na domenskem prehodu
    - blokiranje odhodnih sporočil z določenimi ciljnimi naslovi
      - uporabnikom onemogočimo dostop do potencialno nevarnih strani
    - blokiranje dohodnih sporočil iz določenih naslovov
      - sporočila, ki jih pošiljajo nevarni strežniki, zavrne
    - blokirajo vsa dohodna sporočila, pri katerih je naslov pošiljatelja enak enemu od naslovov v notranjem omrežju
      - v tem primeru se napadalec pretvarja, da je običajni uporabnik
      - (ang. spoofing)
  - požarni zid na računalniku
    - program, ki blokira sporočila, ki jih ne potrebujejo nobeden od programov
    - če so zaprte vse “luknje”, napad ni mogoč,
    - primer: če na računalniku nimamo nameščenega spletnega strežnika, lahko vsa sporočila na vrata 80 zavrne



VARNOST: ZAŠČITA IN ZDRAVLJENJE

- Filtri za neželeno pošto
  - nameščeni na strežniku ali na odjemalcu
  - uporabljajo zapletene postopke za ločevanje želenih in neželenih sporočil
    - iskanje značilnih nizov znakov,
    - verjetnostna teorija,
    - umetna inteligenca

- Strežnik proxy - posrednik
  - varuje odjemalce pred zlonamernimi posegi strežnika
  - zlonamerni strežnik lahko analizira akcije odjemalcev in se tako seznani s strukturo omrežja, nato pripravi napad
  - med odjemalce in strežnik postavimo strežnik proxy
    - odjemalec komunicira s strežnikom proxy
    - strežnik proxy se do pravega strežnika obnaša kot odjemalec
    - pravi strežnik vedno vidi enega samega odjemalca

VARNOST: ZAŠČITA IN ZDRAVLJENJE

- Orodja za nadzor omrežja
  - specialna programska orodja, ki spremljajo aktivnost v omrežju
  - alarmiranje v primeru močno povečane aktivnost
  - poročanje o dogajanju na požarnih zidovih
- Protivirusni programi
  - namenjeni so zaznavanju in odstranjevanju najrazličnejših oblik napadov
  - podatkovne baze s podpisi virusov, črvov, Trojanskih konjev
  - nujno vzdrževanje podatkovnih baz s stalnim posodabljanjem
  - primeri:
    - AVG, NOD, Norton Antivirus, …

VARNOST: ZAŠČITA IN ZDRAVLJENJE

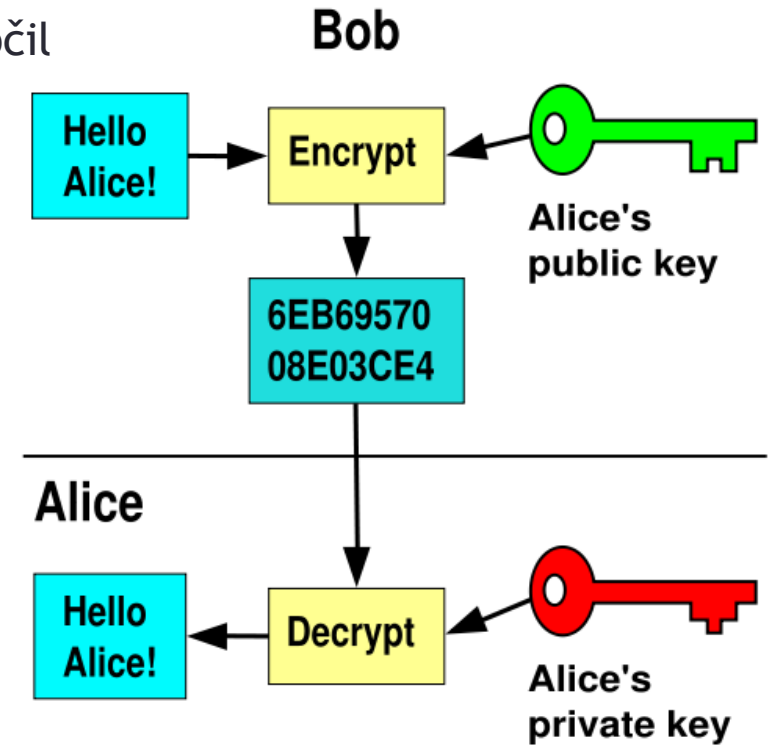
- Osnovni napotki
  - ne odpiramo priponk v elektronskih sporočilih nepoznanih pošiljateljev
  - z Interneta ne nalagamo programov katerih izvora ne poznamo,
  - ne odzivamo se na sporočila pop-up
  - računalnik po uporabi izklopimo iz Interneta ???

VARNOST: ŠIFRIRANJE SPOROČIL

- Cilj napadalcev je velikokrat dostop do podatkov na našem računalniku in okoriščanje z njimi
- Običajna zaščita:
  - uporabniško ime in geslo
  - z vohljanjem napadalec enostavno pride do obeh
  - potrebna je zaščita → šifriranje
- Internetne aplikacije
  - HTTP → HTTPS
  - FTP → SFTP
  - Telnet → SSH

VARNOST: ŠIFRIRANJE SPOROČIL

- Zaščita sporočil z javnim ključem
  - Kljub temu, da vemo, kako je sporočilo šifrirano, ga ne moremo odšifrirati
  - Sistem je zasnovan na dveh številčnih vrednostih (ključih)
    - javni ključ je namenjen šifriranju sporočil
    - zasebni ključ je namenjen za odšifriranje sporočil
  - Postopek
    - javni ključ razpošljemo vsem, ki želijo poslati sporočilo na ciljni sistem
    - pošiljatelj sporočilo šifrira z javnim ključem
    - morebitni napadalec ga ne more odšifrirati kljub temu, da pozna javni ključ
    - edini, ki sporočilo lahko odšifrira je ciljni sistem

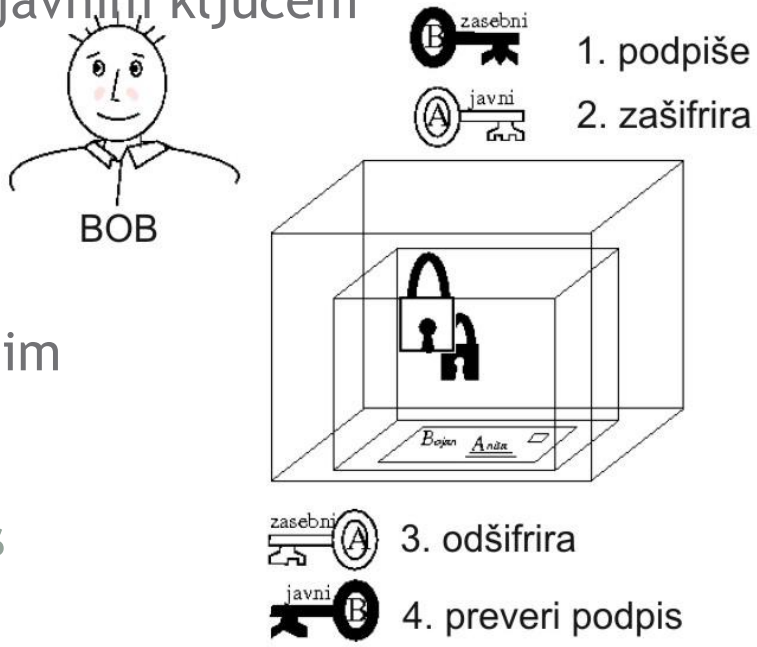


VARNOST: ŠIFRIRANJE SPOROČIL

- Zaščita sporočil z javnim ključem
  - Kako zagotoviti, da imamo pravi javni in zasebni ključ?
    certifikatni uradi
    - vzdržujejo liste certifikatov
    - certifikat je datoteka, ki vključuje ime stranke in njen javni ključ
    - organizacije zaradi večjega nadzora večinoma same izdajajo certifikate
  - Kako zagotoviti, da je pošiljatelj res pravi?
    avtentikacija sporočil
    - digitalni podpis
    - pošiljatelj sporočilo šifrira z zasebnim ključem
    - sprejemnik ga odšifrira z javnim ključem
    - odšifriranje je uspešno samo v primeru, ko javni ključ ustreza zasebnemu ključu

VARNOST: ŠIFRIRANJE SPOROČIL

- Zaščita sporočil z javnim ključem
  - Kako zagotoviti, da je pošiljatelj res pravi? avtentikacija sporočil
    - Primer: Bob pošlje Alice podpisano zasebno pismo
      1. **podpiše** ga s svojim zasebnim ključem
      2. **zašifrira** ga z Alicenim javnim ključem
      3. Alice ga **odšifrira** s svojim zasebnim ključem
      4. z Bobovim javnim ključem **preveri podpis**



VARNOST: ŠIFRIRANJE SPOROČIL

- Najbolj priljubljeni sistemi šifriranja z javnimi in zasebnimi ključi temeljijo na algoritmu RSA (avtorji River, Shamir, Adleman)
- PGP Corporation (ang. Pretty Good Privacy)
  - izdelava programskih modulov, ki uporabljajo RSA algoritme
  - kompatibilni so z večino programov za elektronsko pošto
  - zastonj za osebno in neprofitno rabo
  - Uporabnik lahko sam pripravi svoj zasebni in javni ključ
  - http://www.pgp.com