

Komunikacijski protokoli in omrežna varnost

Uvod in ponovitev osnov predmeta

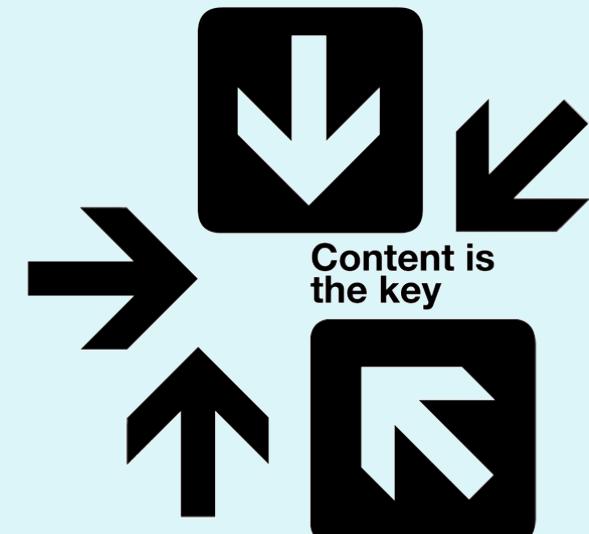
Komunikacijski protokoli in omrežna varnost

- **Profesor:**
dr. Andrej Brodnik (Ljubljana)
- **Asistent:**
as. dr. Gašper Fele Žorž
- **Izvedba predmeta:**
 - 3 ure predavanj - 2 dela, 2 uri laboratorijskih vaj tedensko
 - kontakt: e-mail, govorilne ure, forum na strani predmeta



Vsebina predmeta

- ponovitev osnov računalniških komunikacij (ISO/OSI, TCP/IP, protokoli, storitve, varnost),
- zagon stroja
- nadzor in upravljanje omrežij,
- razpošiljanje (*multicasting*),
- aplikacije v stvarnem času,
- varnost: avtentikacija, avtorizacija, beleženje, varni prenos, VPN, certificiranje, požarni zidovi, IDS sistemi,
- podatki za delovanje omrežja, LDAP,
- IEEE 802.



Vsebina predmeta - okvirni načrt

teden	predavanje	DN	LAB
3.10.	Uvod v predmet	1	
10.10.	Zagon računalnika, omrežna konfiguracija	1	
17.10.	Nadzor in upravljanje omrežij	1	
24.10.	<i>vabljeni predavanji</i>		
31.10.	<<< dan spomina na mrtve >>>		
7.11.	Promet in aplikacije v stvarnem času	2	
14.11.	Razpošiljanje	2	
21.11.	Razpošiljanje	2	
28.11.	KOLOKVIJ 1		LAB1
5.12.	Varnostni elementi omrežij	3	
12.12.	Avtentikacija, avtorizacija in beleženje (AAA)	3	
19.12.	Avtentikacija, avtorizacija in beleženje (AAA)	3, 4	
26.12.	<<< božično – novoletni prazniki >>>		
2. 1.	Podatki za delovanje omrežja (LDAP)	4	
9.1.	Družina IEEE 802	4	
16.1.	<i>rezerva / priprava na kolokvij</i>		
23.1.	KOLOKVIJ 2		LAB2

Obveznosti predmeta

Končna ocena (≥ 50):

- 4 domače naloge: 20%
 - laboratorijski nalogi 40%
 - pisni izpit ali 2 kolokvija: 40%
- 100%

Obveznosti:

- RFC: povzetek v slovenščini, 2 x pregled, popravek
- domače naloge ≥ 40 , vsaka domača naloga ≥ 20
- seminarski nalogi ≥ 40 , vsaka seminarska naloga ≥ 20
- pisni izpit ≥ 50 , vsak od kolokvijev ≥ 40

Obveznosti predmeta

Pri oceni se še upošteva:

- sodelovanje na forumih
- dopolnjevanje RFCjev
- pomoč kolegom
- ...

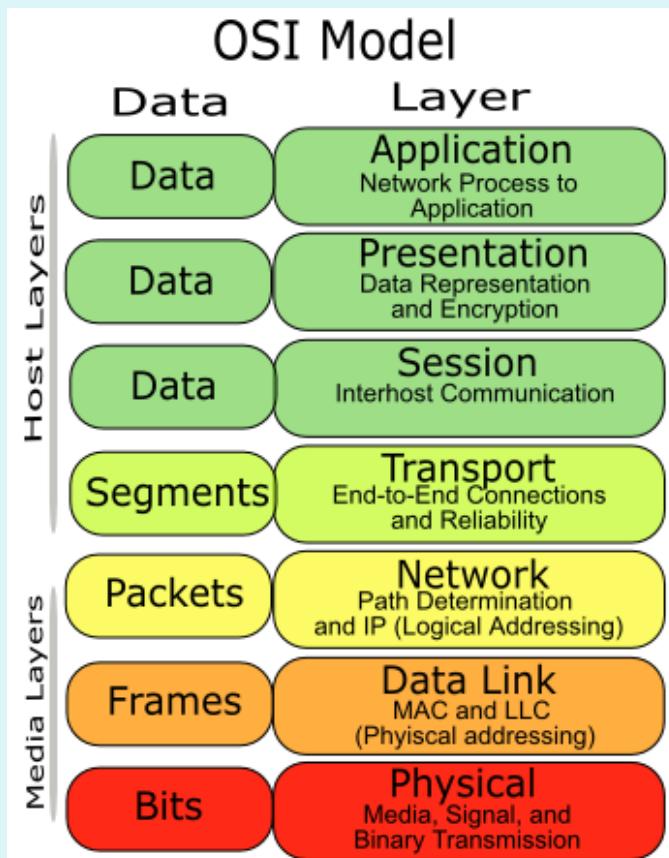
Literatura

- J. F. Kurose, K. W. Ross: Computer Networking, 5th edition, Addison-Wesley, 2010.
- A. Farrel: The Internet and Its Protocols: A Comparative Approach, Morgan Kaufmann, 2004.
- E. Cole: Network Security Bible, Wiley, 2nd edition, 2009.
- Mani Subramanian: Network Management: An introduction to principles and practice, Addison Wesley Longman, 2000
- RFCji
- ...

Ponovitev osnov računalniških komunikacij

ISO/OSI model

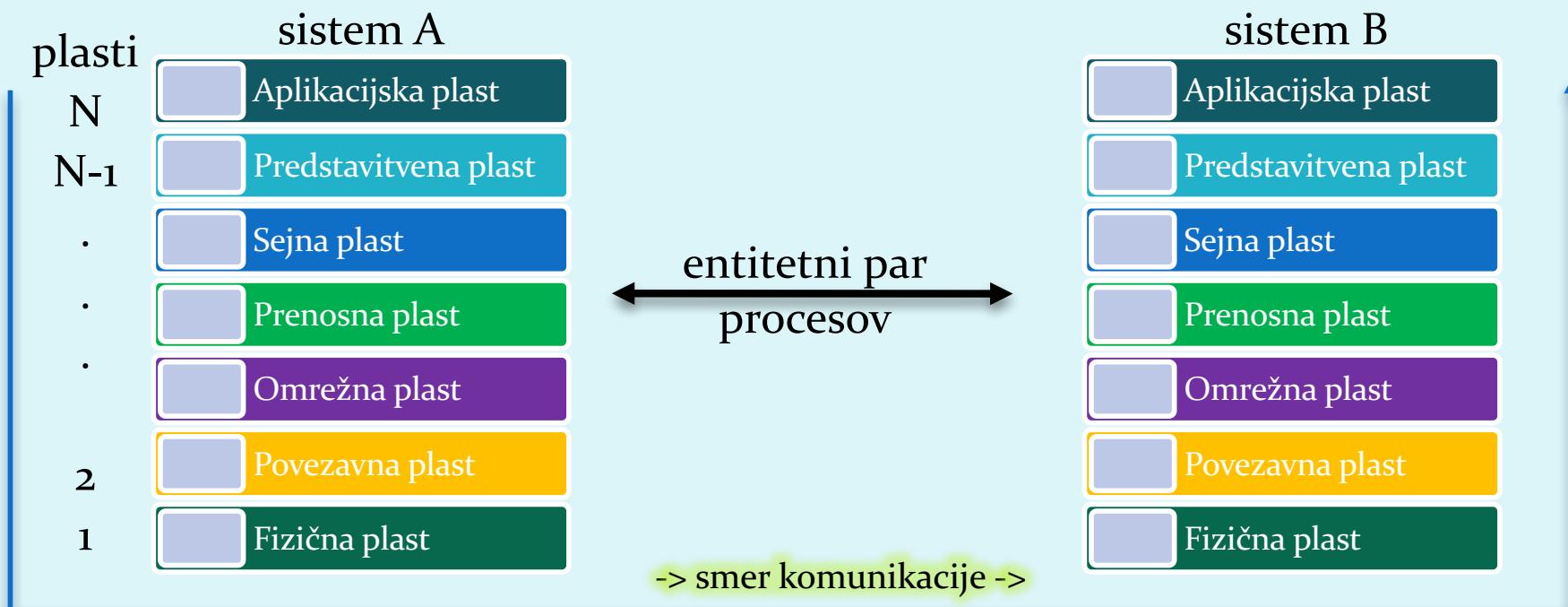
- model vsebuje 7 plasti, ki definirajo sloje sorodnih funkcij komunikacijskega sistema



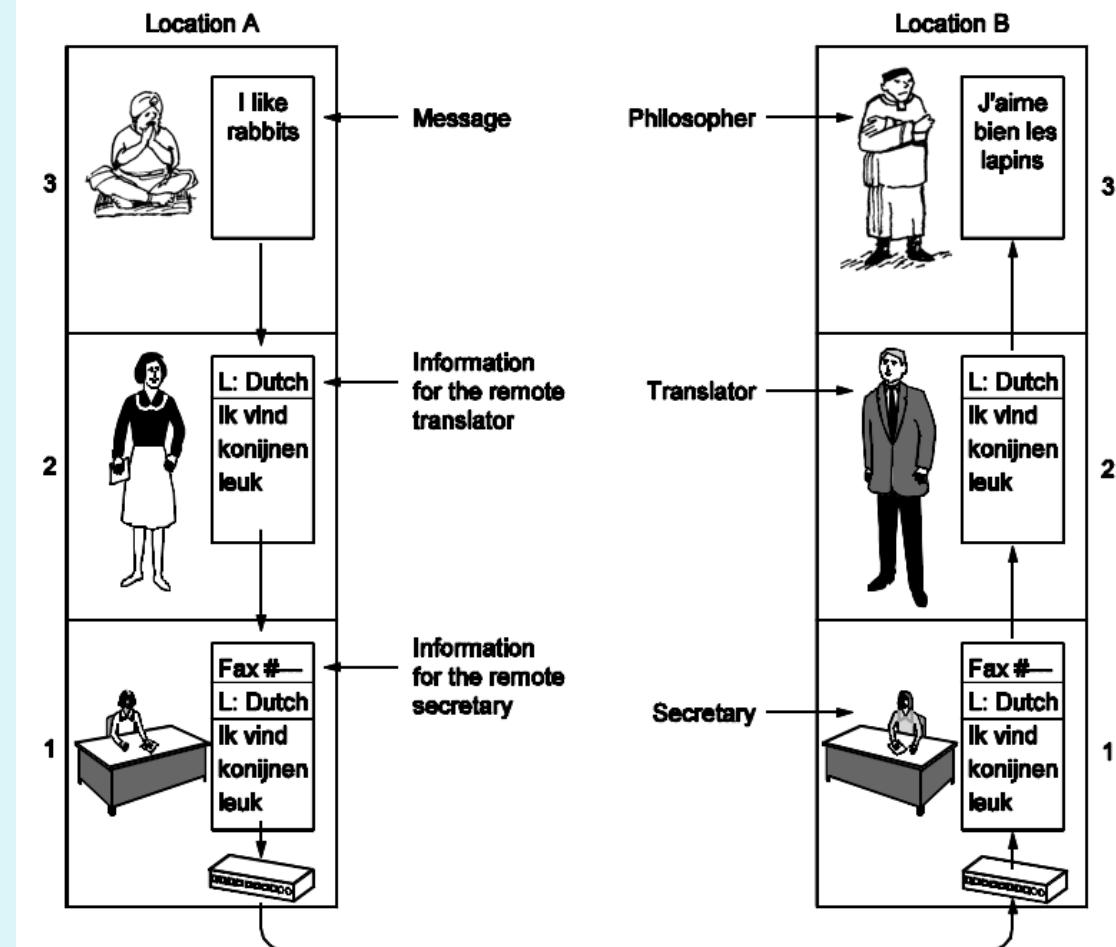
aplikacijska plast
predstavitevna plast
sejna plast
transportna plast
omrežna plast
povezavna plast
fizična plast

ISO/OSI model

- plast N nudi storitve (streže) plasti N+1
- plast N zahteva storitve (odjema) od plasti N-1,
- protokol: pravila komuniciranja med istoležnima procesoma,
- entitetni par: par procesov, ki komunicira na isti plasti



Analogija: pogovor med dvema filozofoma

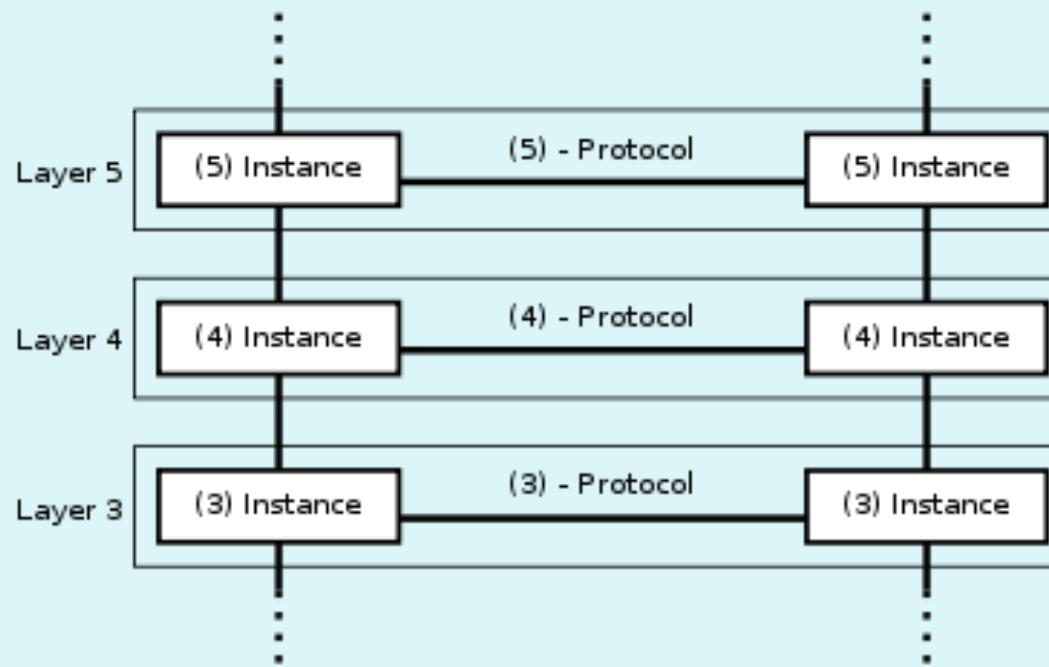


- Zakaj plasti?
 - sistematična zasnova zgradbe sistema,
 - sprememba implementacije dela sistema je neodvisna od ostalega sistema

ISO/OSI model

In še drugače:

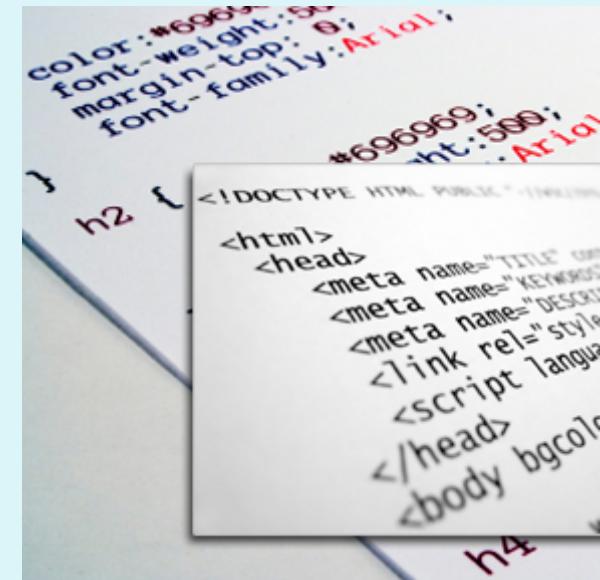
- vsaka plast ima svoje protokole (= jezik, s katerim se pogovarja istoležni entitetni par procesov),
- protokoli so specifični za storitve, ki jih plast zagotavlja.



OSI plasti: podrobneje

- **Aplikacijska plast**

- najbližja uporabniku,
- omogoča interakcijo aplikacije z omrežnimi storitvami,
- standardne storitve: telnet, FTP, SMTP, SNMP, HTTP



OSI plasti

- **Predstavitevna plast**

- določa pomen podatkov med entitetnima paroma aplikacijske plasti,
- sintaksa in semantika,
- določa kodiranje, kompresijo podatkov, varnostne mehanizme

- **Sejna plast**

- nadzor pogovora (množice povezav) med aplikacijama,
- logično povezovanje med aplikacijami,
- običajno vgrajena v aplikacije.

OSI plasti

- **Transportna plast** (enota: SEGMENT)

- učinkovit, zanesljiv in transparenten prenos podatkov med uporabnikoma; te storitve zagotavlja višjim plastem,
- mehanizmi: kontrola pretoka, segmentacija, kontrola napak,
- povezavni, nepovezavni prenosi,
- TCP, UDP, IPSec, GRE, L2TP, PPP

The TCP Segment Format



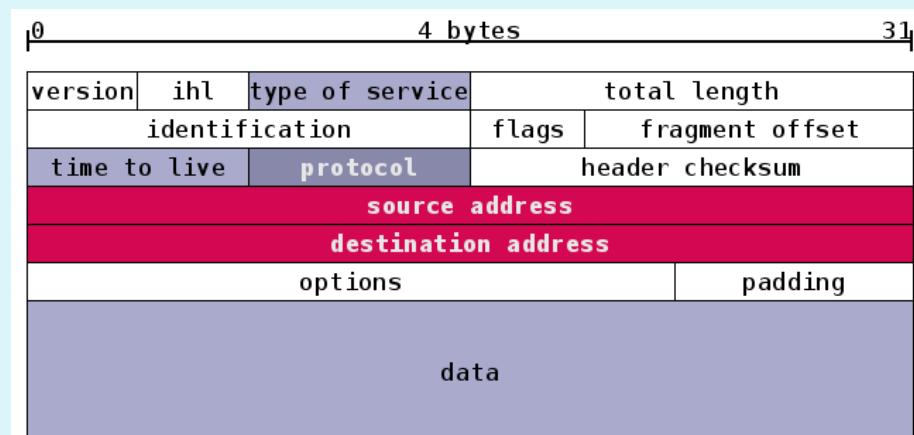
The UDP Segment Format



OSI plasti

- **Omrežna plast** (enota: PAKET)

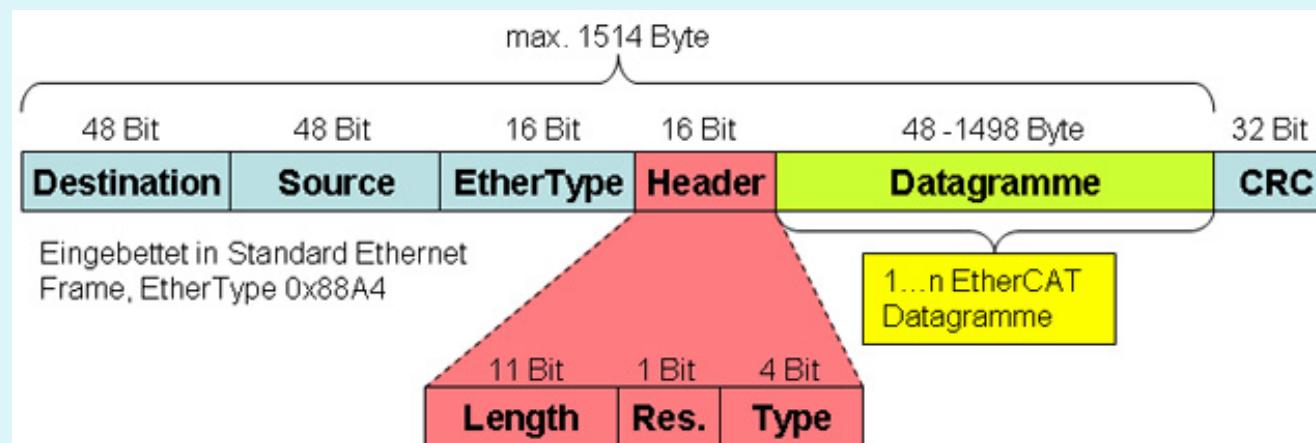
- usmerjanje (povezavne in nepovezavne storitve)
- prenos paketov od izvornega do ciljnega računalnika,
- lahko zagotavlja: zagotovljeno dostavo, pravilno zaporedje, fragmentacijo, izogibanje zamašitvam,
- usmerjanje, usmerjevalniki, usmerjevalni algoritmi,
- protokoli: IP, ICMP, IPSec, IGMP, IPX



OSI plasti

- **Povezavna plast** (enota: OKVIR)

- asinhrona/sinhrona komunikacija,
- fizično naslavljjanje: npr MAC naslov,
- zaznavanje in odpravljanje napak (pariteta, CRC, checksum)
- kontrola pretoka, okvirjanje
- protokoli: Ethernet, PPP, Frame Relay



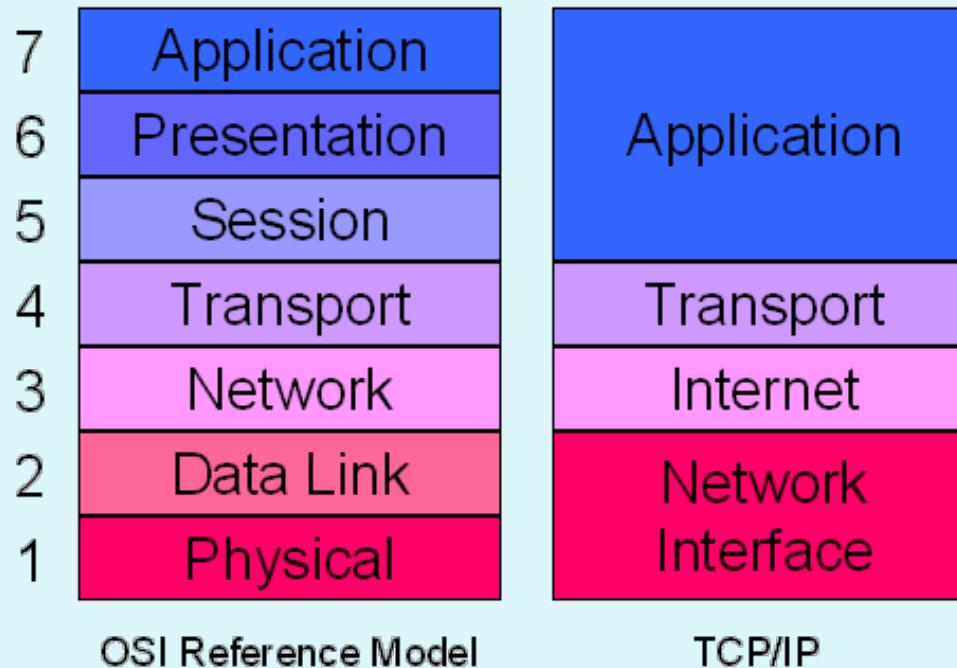
OSI plasti

- **Fizična plast**

- prenos bitov po kanalu (baker/optika/brezžično),
- digitalni, analogni medij,
- UTP, optika, koaksialni kabli, brezžična omrežja,
- RS-232, T1, E1, 802.11b/g, USB, Bluetooth



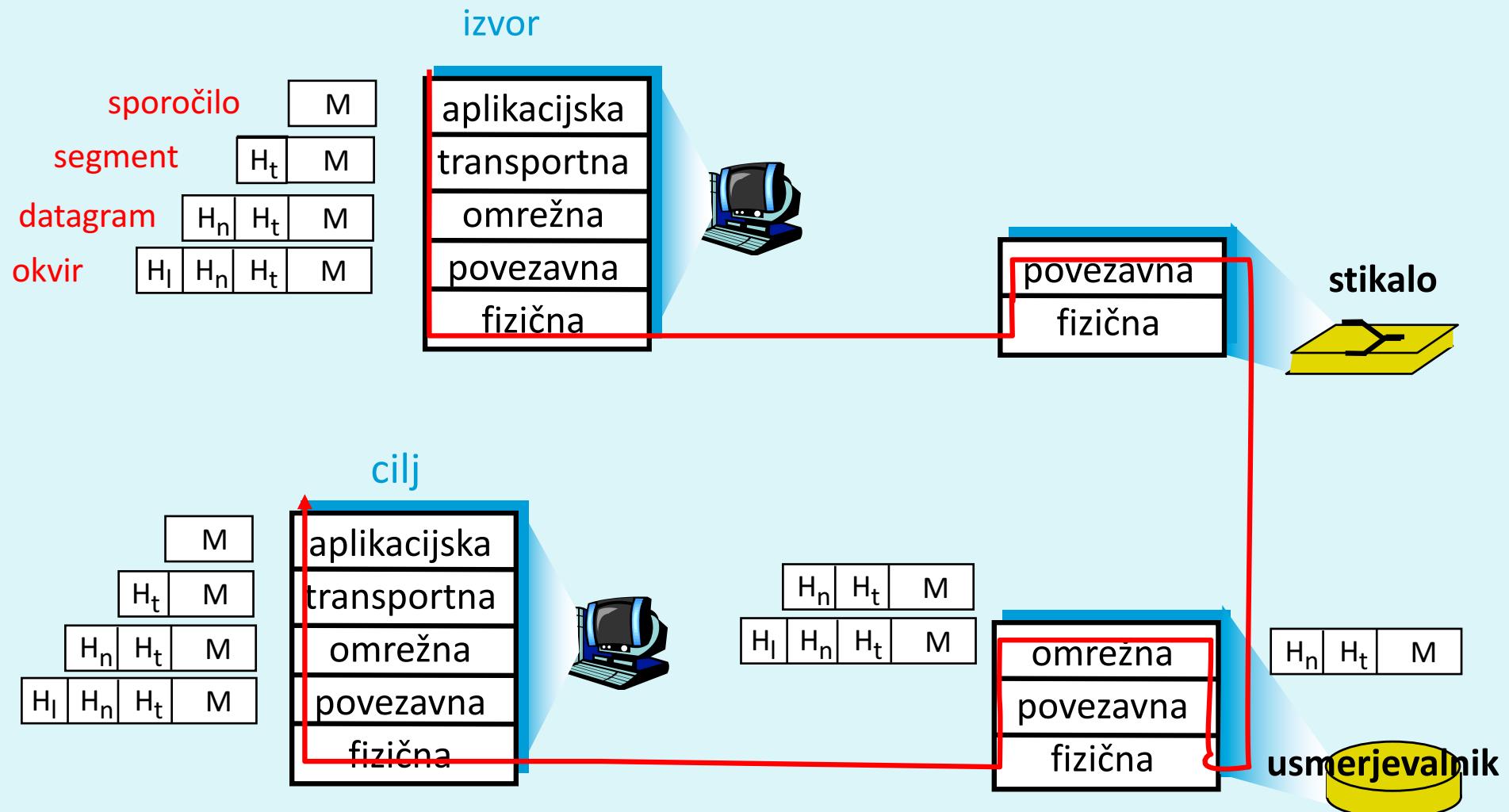
OSI model in model TCP/IP



Primerjava modelov:

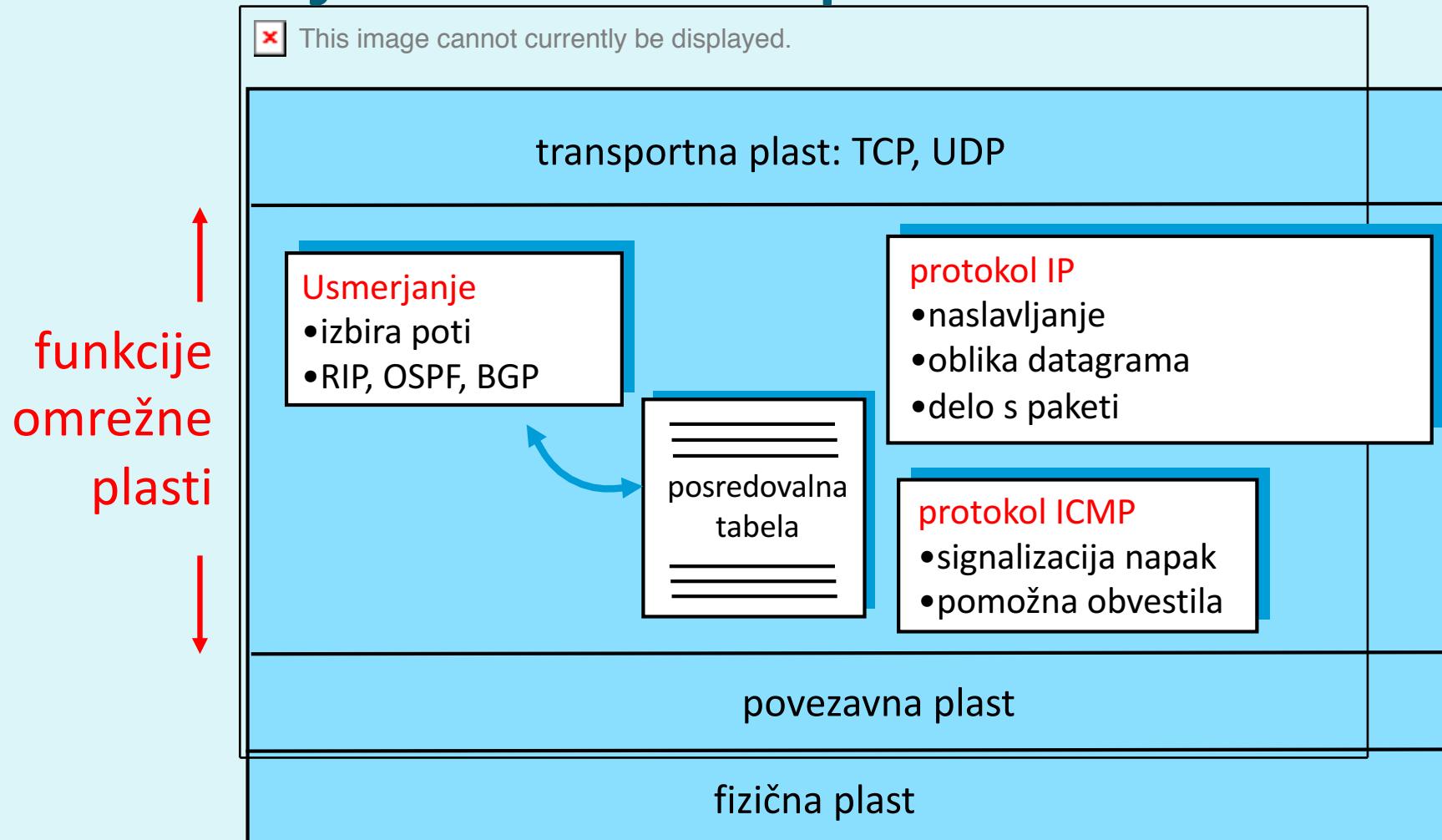
- ISO OSI: **de iure**, teoretičen, sistematičen, pomanjkanje implementacij (izdelkov),
- TCP/IP: **de facto**, prilagodljiv, nesistematičen, fleksibilen, veliko izdelkov

Enkapsulacija



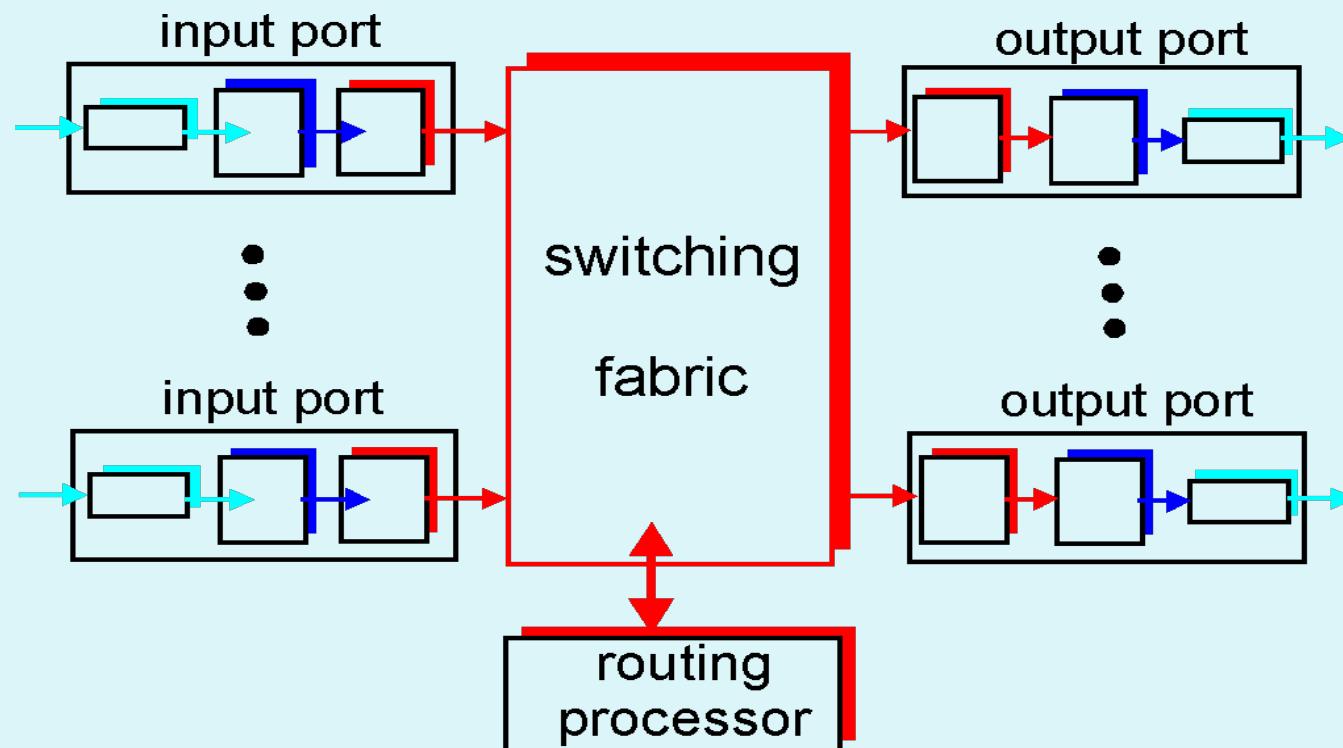
Omrežna in transportna plast: podrobneje

Omrežna plast: Funkcije omrežne plasti



Omrežna plast: Usmerjevalniki

- uporaba usmerjevalnih (*routing*) protokolov (RIP, OSPF, BGP)
- posredovanje (*forwarding*) datagramov med vhodnimi in izhodnimi vrti



Omrežna plast: Primerjava aktivne opreme

- **usmerjevalnik (router):**

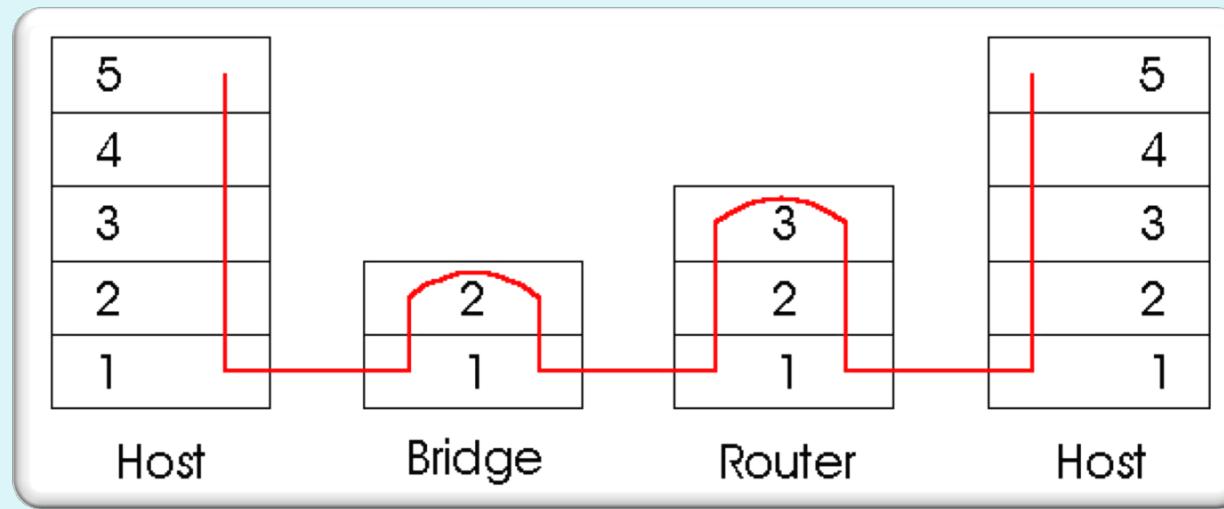
- naprava, ki deluje na OMREŽNI plasti
- vzdržujejo usmerjevalne tabele, izvajajo usmerjevalne algoritme,

- **stikalo (switch):**

- naprava, ki deluje na POVEZAVNI plasti,
- vzdržujejo tabele za preklapljanje, izvajajo filtriranje in odkrivanje omrežja

- **povezovališče (hub):**

- naprava, ki deluje na fizični plasti, danes niso več v rabi



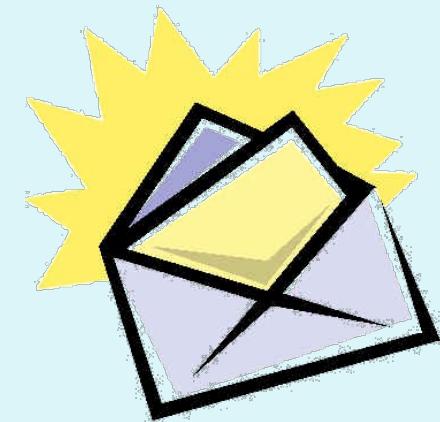
Omrežna plast: IPv4

- protokol na omrežni (3.) plasti OSI modela
- **IPv4 naslov** je 32 bitni naslov vmesnika. Primer:

11000001 00000010 00000001 01000010

ali

193.2.1.66



- **Podomrežje** je množica IP naslovov, ki so med seboj dosegljivi brez posredovanja usmerjevalnika. Maska (32 bitov) določa del IP naslova, ki predstavlja naslov podomrežja. Primer:

11111111 11111111 11110000 00000000 (255.255.255.240)

pomeni, da prvih 20 bitov IP naslova predstavlja naslov omrežja, preostalih 12 pa naslov vmesnika.

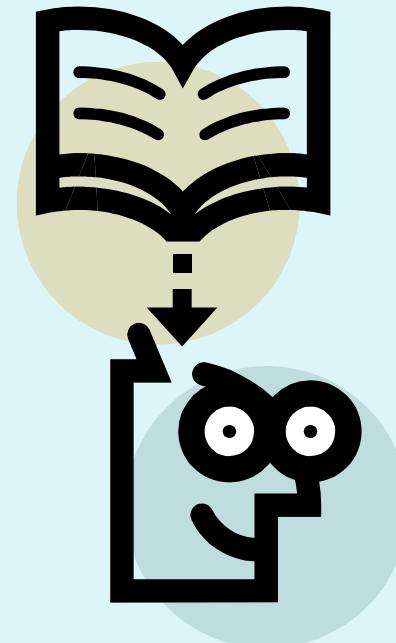
Omrežna plast: Vaja!

- Podana sta IP naslov nekega vmesnika in maska podomrežja:

193.90.230.25 /20

Kakšen je naslov podomrežja?

Kakšen je naslov vmesnika?



Omrežna plast: IPv6

- **Prednosti:**

- večji naslovni prostor: 128 bitov
- hitro usmerjanje in posredovanje ter QoS omogoča že format glave, fragmentacije ni,
- implementacija IPSec znotraj IPv6 obvezna.

- **Naslov:** sestavljen iz 64 bitov za ID podomrežja + 64 bitov za ID vmesnika

001000011011010 000000011010011 0000000000000000 001011100111011
0000001010101010 0000000011111111 111111000101000 1001110001011010

Zapisan šestnajstško, ločeno z dvopičji

21DA:00D3:0000:0000:02AA:00FF:FE28:9C5A

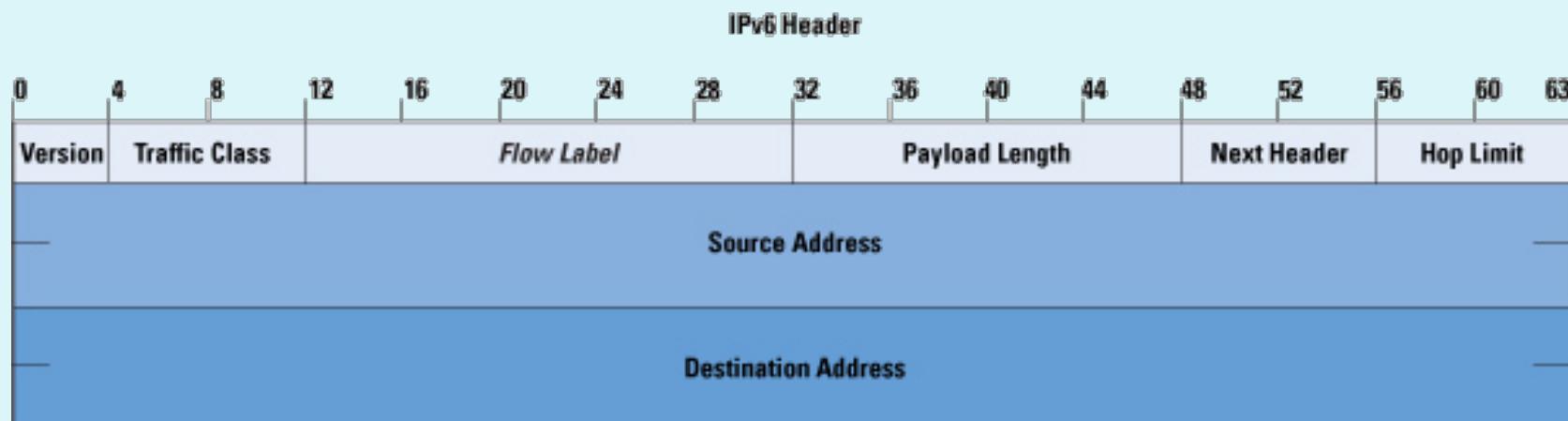
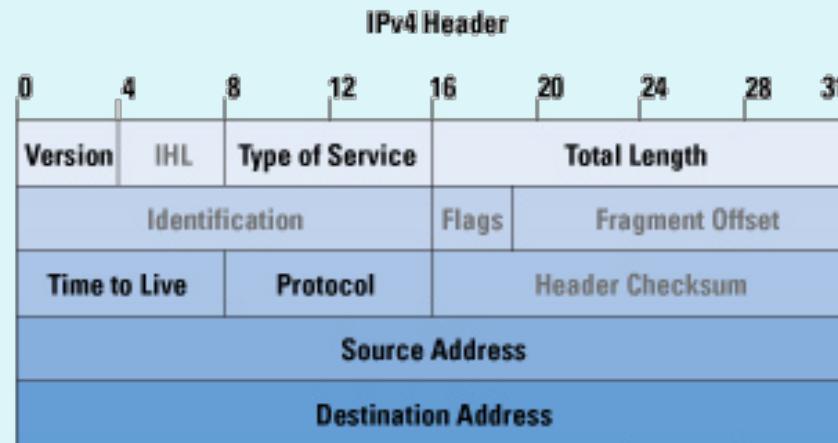
ali (brez vodilnih ničel)

21DA:D3:0:0:2AA:FF:FE28:9C5A

ali (izpustimo bloke ničel)

21DA:D3::2AA:FF:FE28:9C5A

Omrežna plast: Primerjava IPv4 in IPv6



Omrežna plast:

IPv6 - načini naslavljjanja

- **UNICAST:**

naslavljanje posameznega omrežnega vmesnika



- **MULTICAST:**

naslavljanje skupine omrežnih vmesnikov, dostava vsem vmesnikom v množici

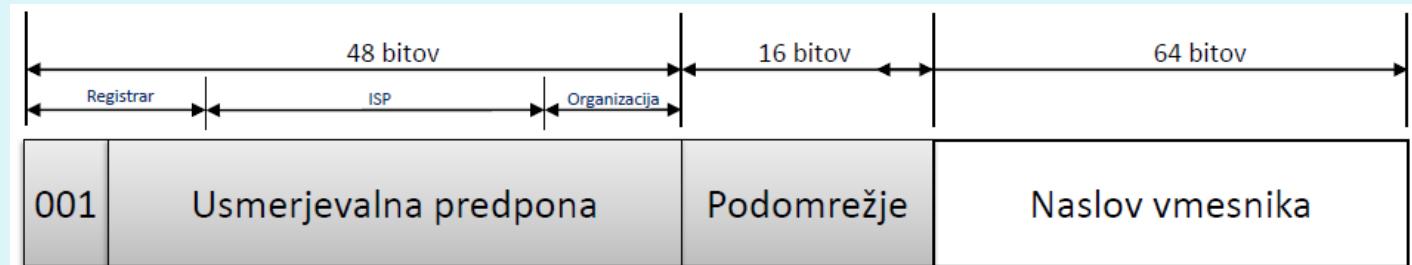
- **ANYCAST:**

je naslov množice vmesnikov, dostava se izvede enemu (najbližjemu?) vmesniku iz te množice

Vsak vmesnik ima lahko več naslovov različnih tipov.
(BROADCAST naslovov - v IPv6 ni več!)

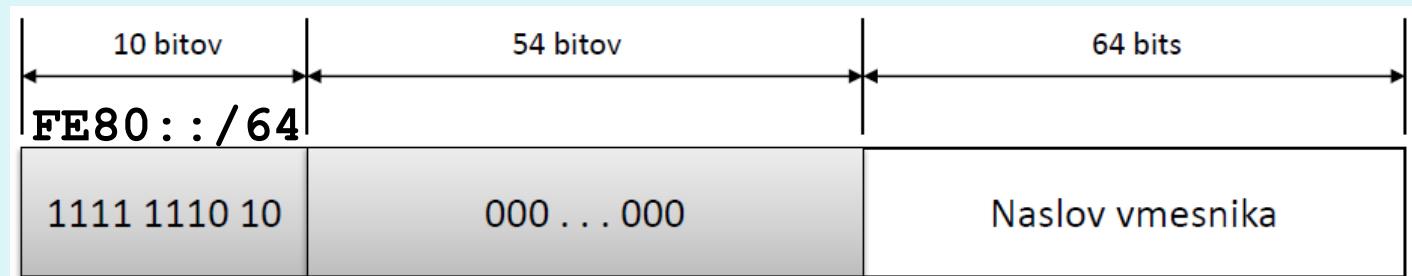
Omrežna plast: IPv6 - vrste unicast naslovov

1.) **globalni unicast** (= javni naslovi)



2.) **posebni naslovi** (localhost ::1, ne definiran o::o, IPv4 naslovi)

3.) **link-local naslovi** (znotraj 1 povezave, adhoc omrežja)

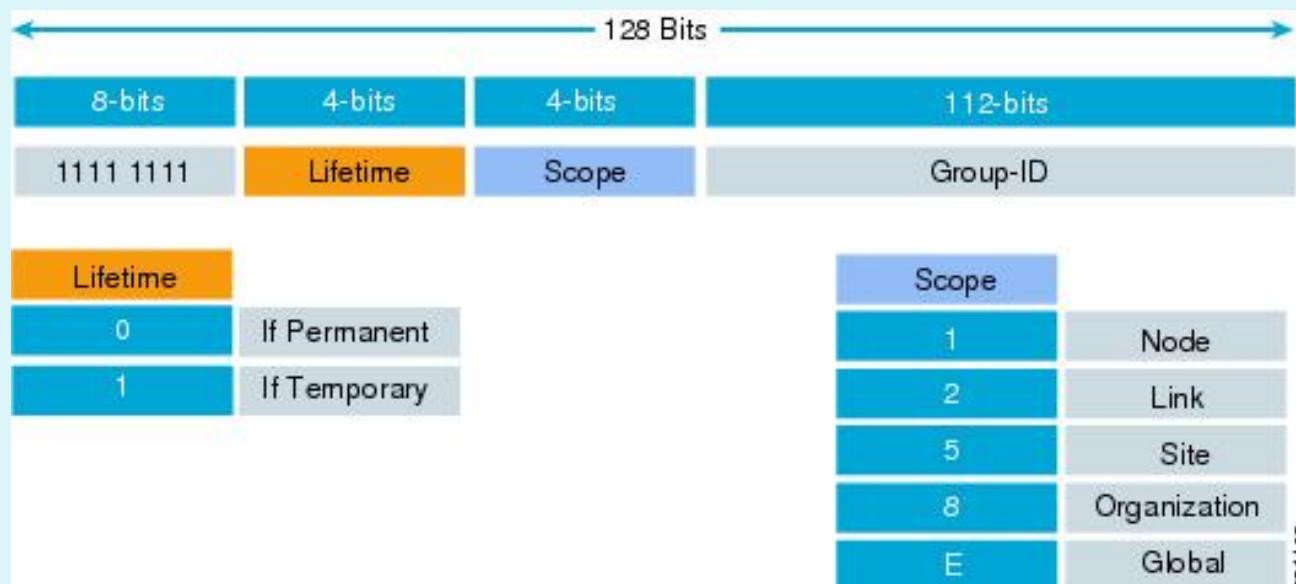


4.) **site-local** (=privatni naslovi, znotraj org., se ne usmerjajo, FEC0::/10)

5.) **unique-local** (=zasebni naslovi, dodeli registrar, znotraj org. se ne usmerjajo, so bolje strukturirani, FC00::/7)

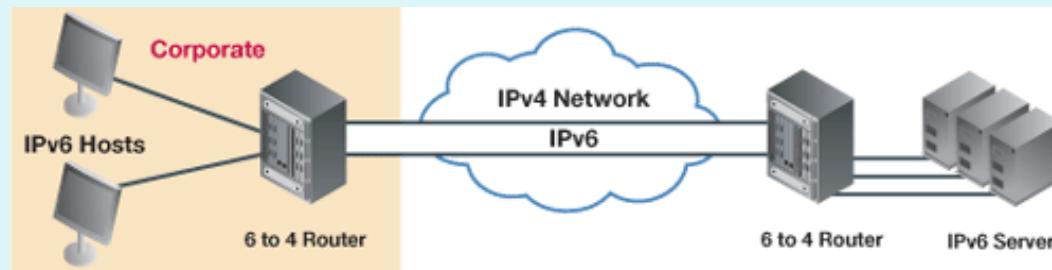
Omrežna plast: IPv6 – razpošiljanje (*multicast*)

- 1.) FF02::1 (link local: vsi VMESNIKI)
- 2.) FF02::2 (link local: vsi USMERJEVALNIKI)
- 3.) Struktura naslova:



Omrežna plast: IPv6 v omrežjih IPv4

- 1.) **dvojni sklad (dual-stack):** usmerjevalniki poznajo IPv4 in IPv6. Z možnimi govorji IPv6, z ostalimi pa IPv4.
- 2.) **tuneliranje:** IPv6 paket zapakiramo v enega ali več IPv4 paketov kot podatke.



Omrežna plast: Usmerjanje

- **NAČINI**

- statično / dinamično (upoštevanje razmer v omrežju)
- centralizirano / porazdeljeno (glede na poznavanje stanja celega omrežja)
- po eni poti / po več poteh

- **IMPLEMENTACIJE:**

- z vektorjem razdalj (RIP, IGRP, EIGRP)
- glede na stanje omrežja (OSPF, IS-IS)



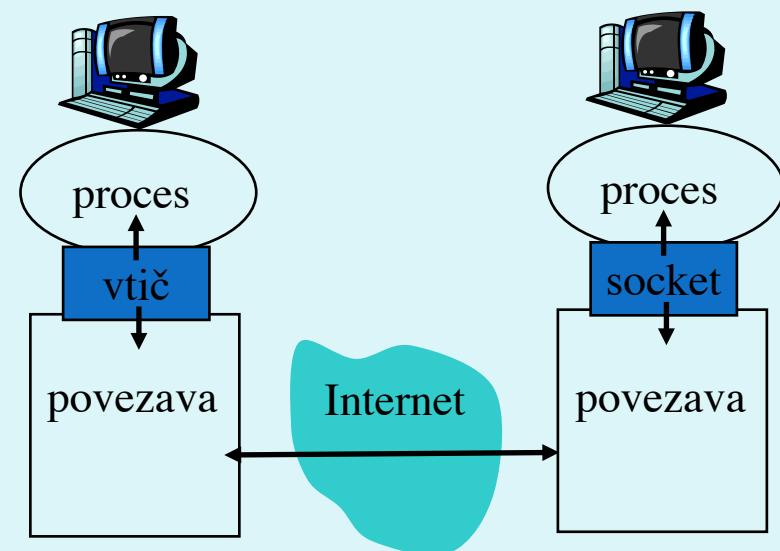
Transportna plast: Funkcionalnosti

- **Naloga:**

- Sprejem sporočila od aplikacije
- Sestavljenje segmentov v sporočilo za omrežno plast
- Predaja aplikacijski plasti

- **Vtič**

- vmesnik med transportno in aplikacijsko plastjo,
- proces naslovimo z IP številko in številko vrat
(www: 80, SMTP: 25, DNS: 53, POP3: 110).



Transportna plast:

Povezavno in nepovezavno

- **Povezavna in nepovezavna komunikacija**

- TCP in UDP; ter ostali protokoli
- vzpostavitev, prenos, podiranje – povezave



- **Potrjevanje**

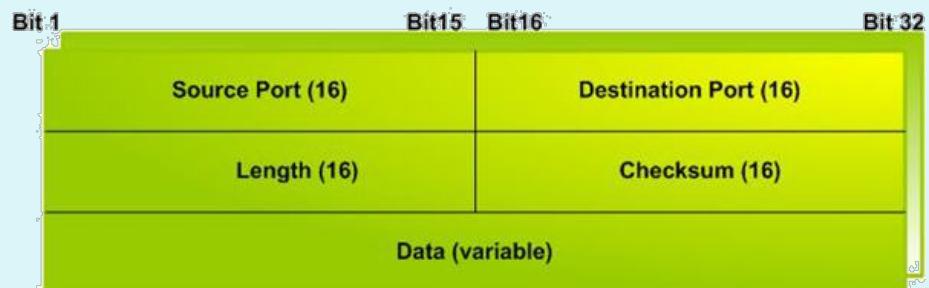
- v protokolu (TCP)
- v aplikaciji (UDP)
- neposredno (ACK in NACK)
- posredno (samo ACK, sklepamo na podlagi številk paketov)
- sprotno potrjevanje: naslednji paket se pošlje šele po prejemu potrditve
- tekoče pošiljanje: ne čaka se na potrditve.

Transportna plast: TCP in UDP

The TCP Segment Format



The UDP Segment Format



Aplikacijska plast:

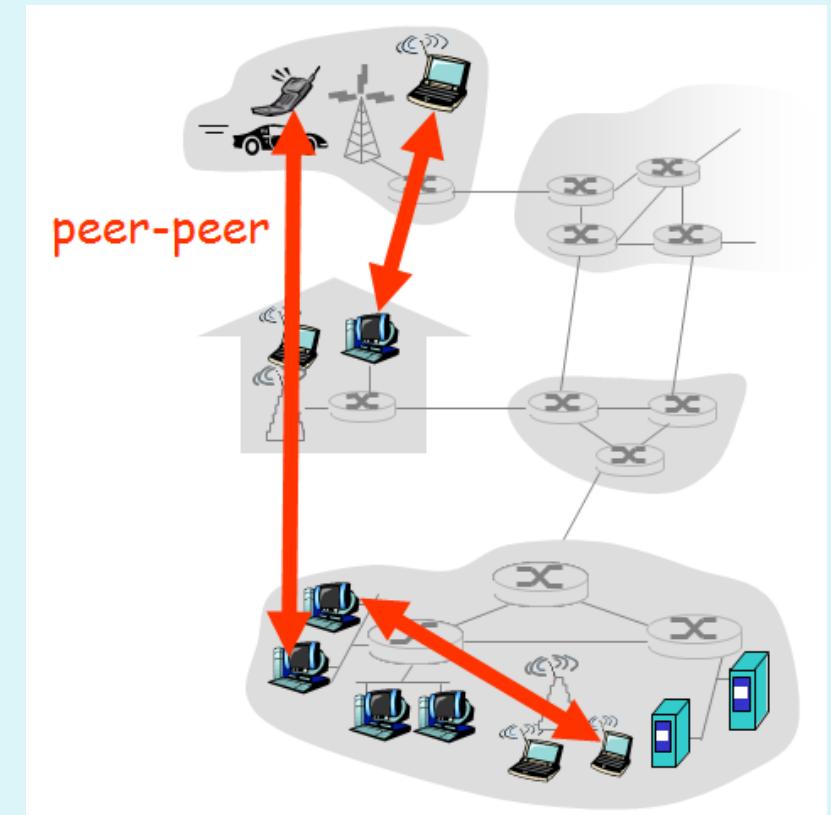
- **Klasične storitve – odjemalec-strežnik**

- telnet, ssh; rdesktop
- ftp, sftp
- WWW in HTTP,
- SMTP, POP₃, IMAP, MAPI
- DNS,
- SNMP, LDAP, RADIUS, ...
- ...

Aplikacijska plast:

- **Novejše storitve – P2P:**

- komunikacija poljubnih dveh končnih sistemov,
- strežniki niso nenehno prižgani,
- prekinjene povezave / spremembe IP naslovov,
- primeri: BitTorrent, Skype

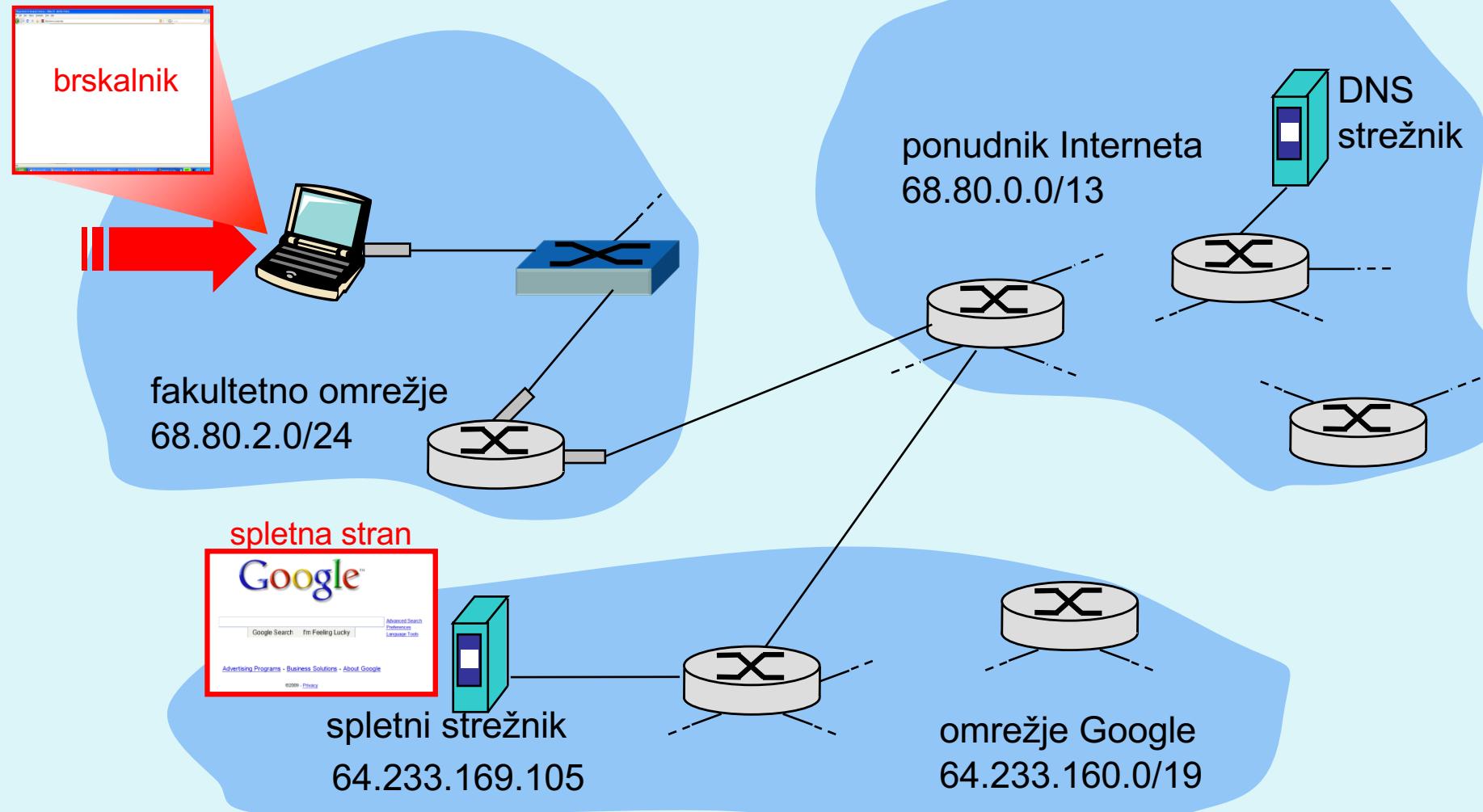


Omrežna in transportna plast: Iz preteklosti za prihodnost

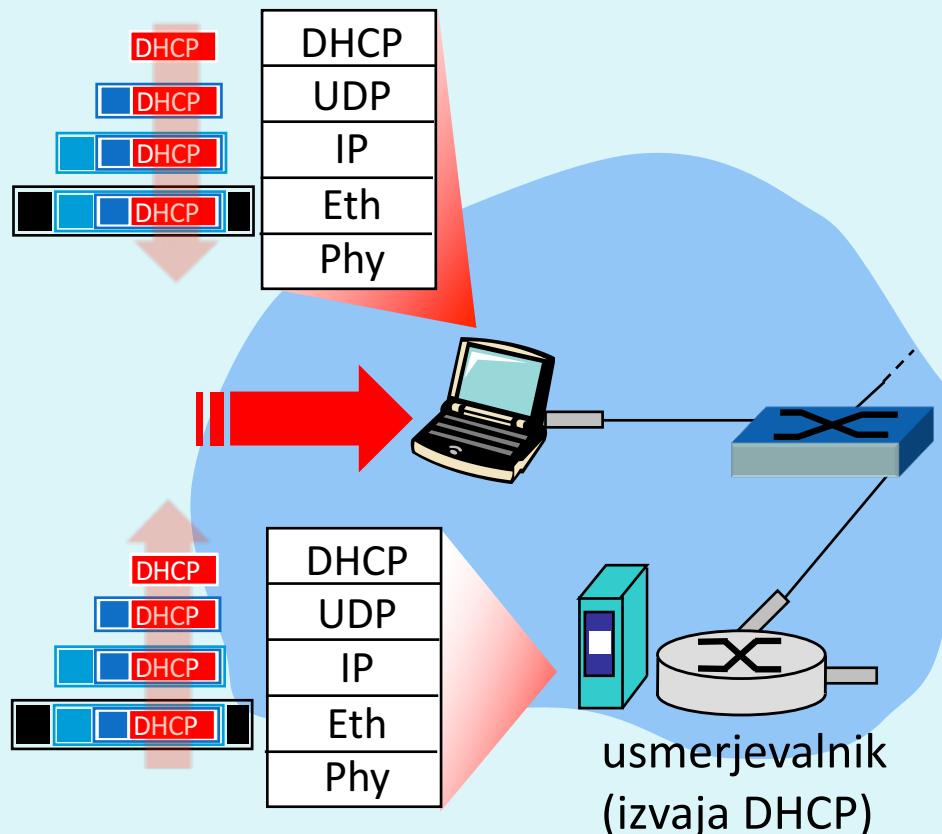
- **Problem:** pomanjkanje IPv4 naslovov
 - izkoristek zasebnih naslovnih prostorov
 - NAT prehodi – običajno hkrati požarni zidovi
 - preprosto v odjemalec-strežnik sistemih
 - v P2P potrebujemo preslikovalni naslov v zunanjem svetu
- V IPv6 NAT prehodi niso potrebni

Primer komunikacije

Primer komunikacije: spletno brskanje

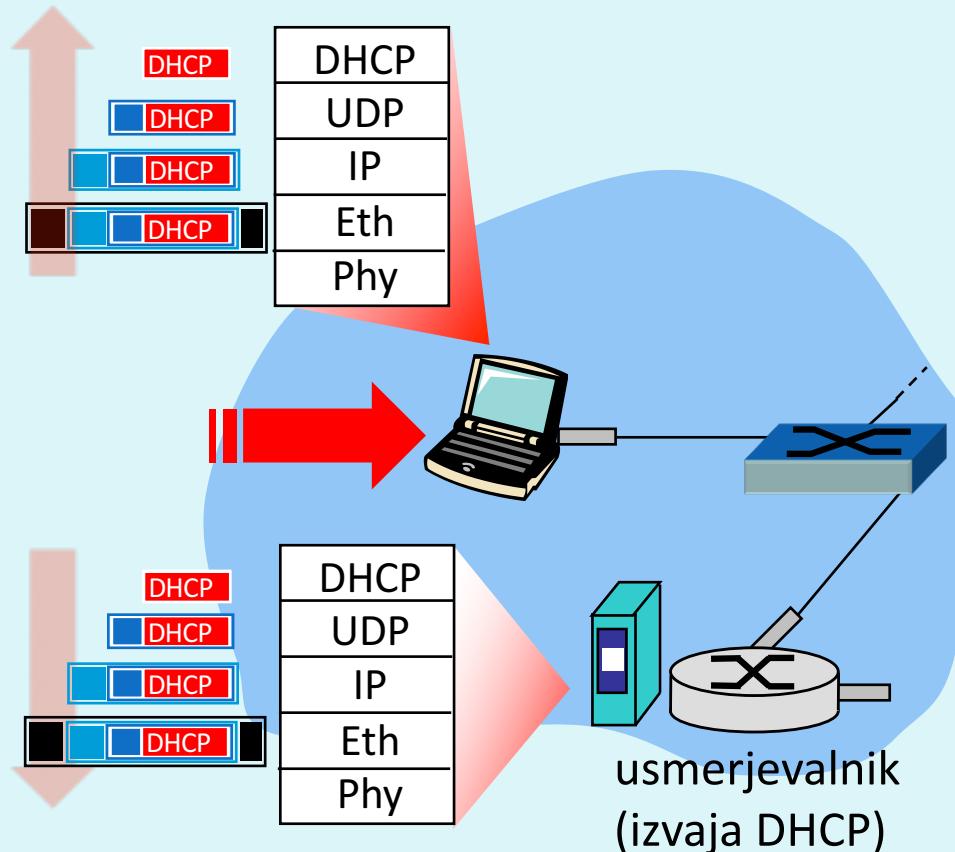


Primer komunikacije: spletno brskanje



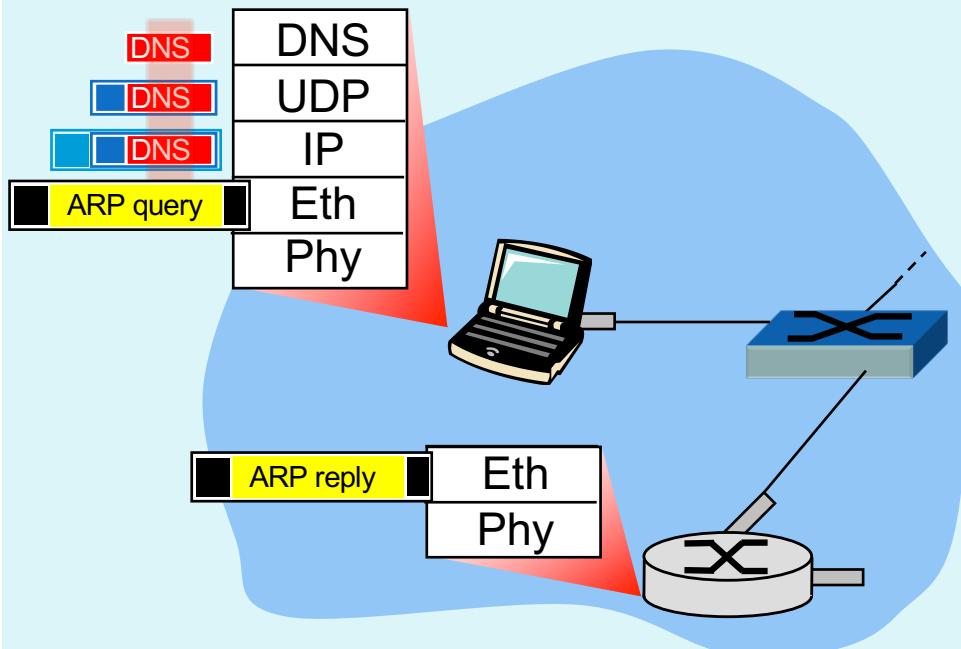
- notesnik ob priklopu na omrežje potrebuje **IP naslov** in podatke prehoda ter DNS strežnika: uporabi torej **DHCP**,
- zahteva DHCP se **enkapsulira**: UDP -> IP -> 802.1 Ethernet
- ethernet okvir se **odda** (*broadcast*) na omrežje, prejme ga usmerjevalnik, ki opravlja nalogu DHCP strežnika
- DHCP strežnik **prebere** vsebino DHCP zahteve

Primer komunikacije: spletno brskanje



- DHCP strežnik odgovori odjemalcu (notesniku) s paketom **DHCP ACK**, ki vsebuje njegov IP naslov ter naslove prehoda in DNS strežnika,
- odgovor **enkapsulira** DHCP strežnik (usmerjevalnik) in ga posreduje odjemalcu, ki ga **dekapsulira**,
- DHCP odjemalec dobi odgovor DHCP ACK,
- rezultat: odjemalec je pripravljen na komunikacijo.

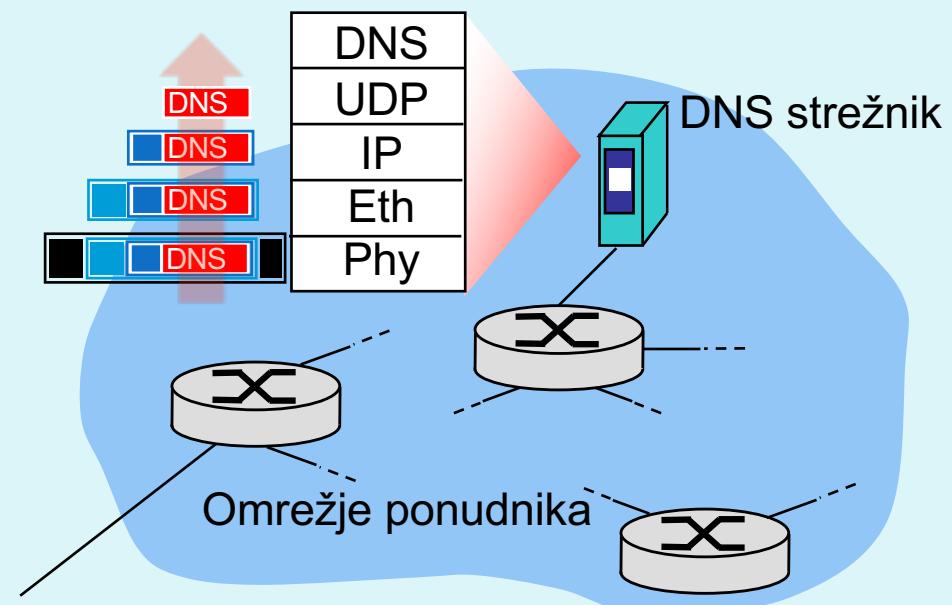
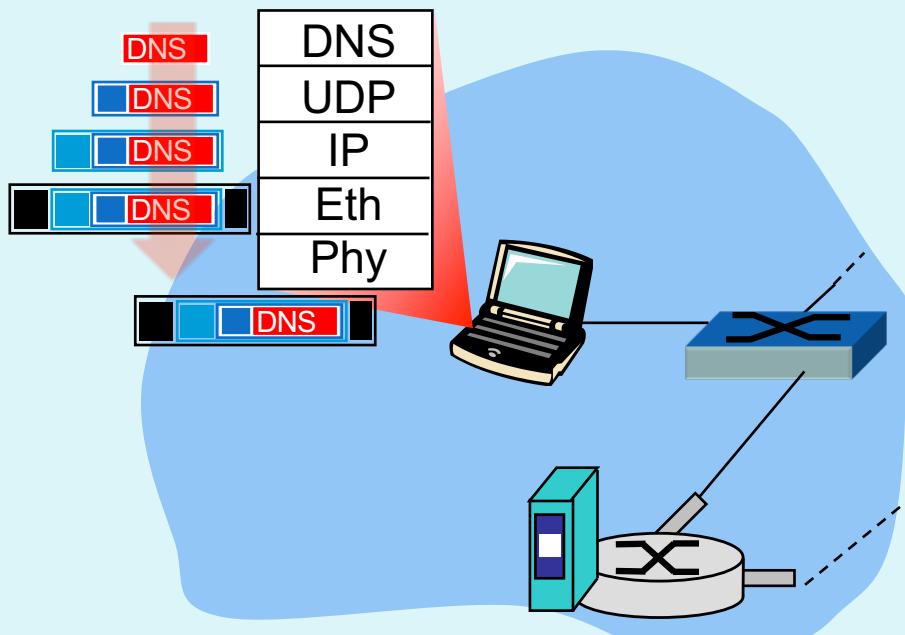
Primer komunikacije: spletno brskanje



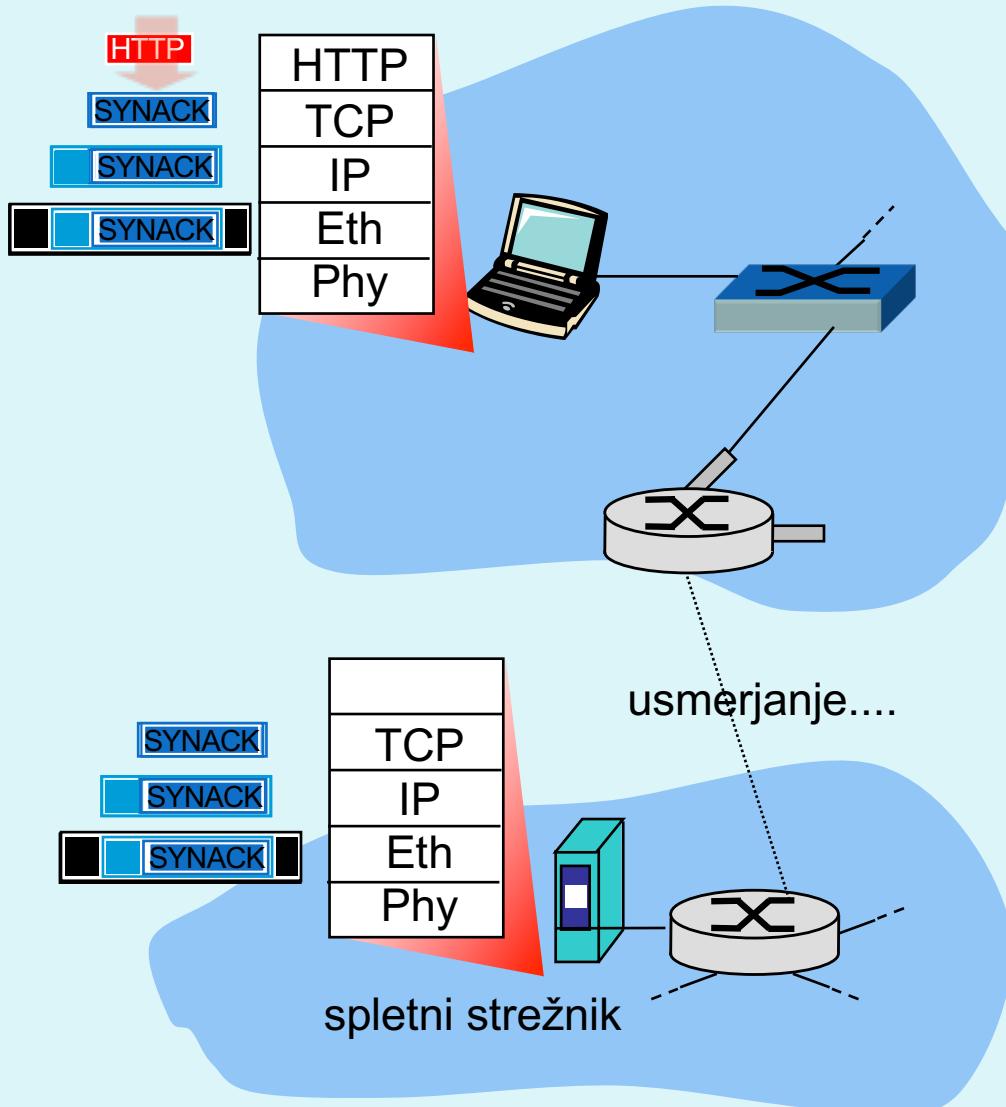
- pred pošiljanjem zahtevka HTTP, potrebujemo IP naslov strežnika www.google.com: **uporabi DNS**,
- enkapsulacija zahtevka DNS: UDP -> IP -> Ethernet. Potrebujemo MAC naslov usmerjevalnika: **uporabi ARP**
- razpošljemo **zahtevek ARP**, usmerjevalnik odgovori z **ARP odgovorom**, ki hrani njegov MAC naslov,
- klient sedaj pozna MAC naslov prehoda, ki mu lahko **pošlje DNS zahtevk**.

Primer komunikacije: spletno brskanje

- IP datagram z **zahetvkom DNS** se posreduje usmerjevalniku
- IP datagram se posreduje **DNS strežniku**, ki je v omrežju ponudnika (z uporabo usmerjevalnih protokolov RIP, OSPF, IS-IS ali BGP),
- DNS strežnik **dekapsulira** zahtevek in posreduje uporabniku IP naslov spletnega strežnika www.google.com

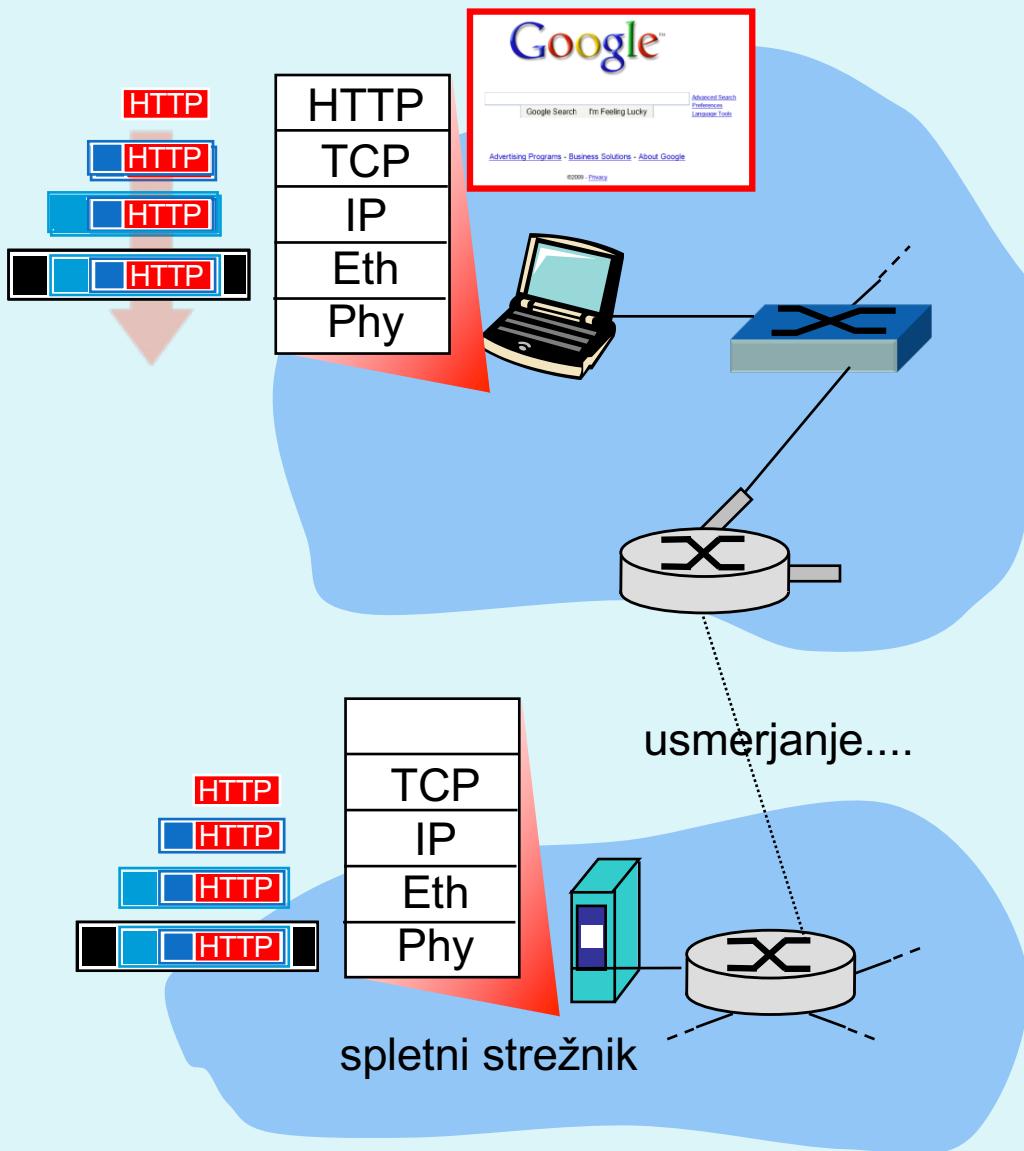


Primer komunikacije: spletno brskanje



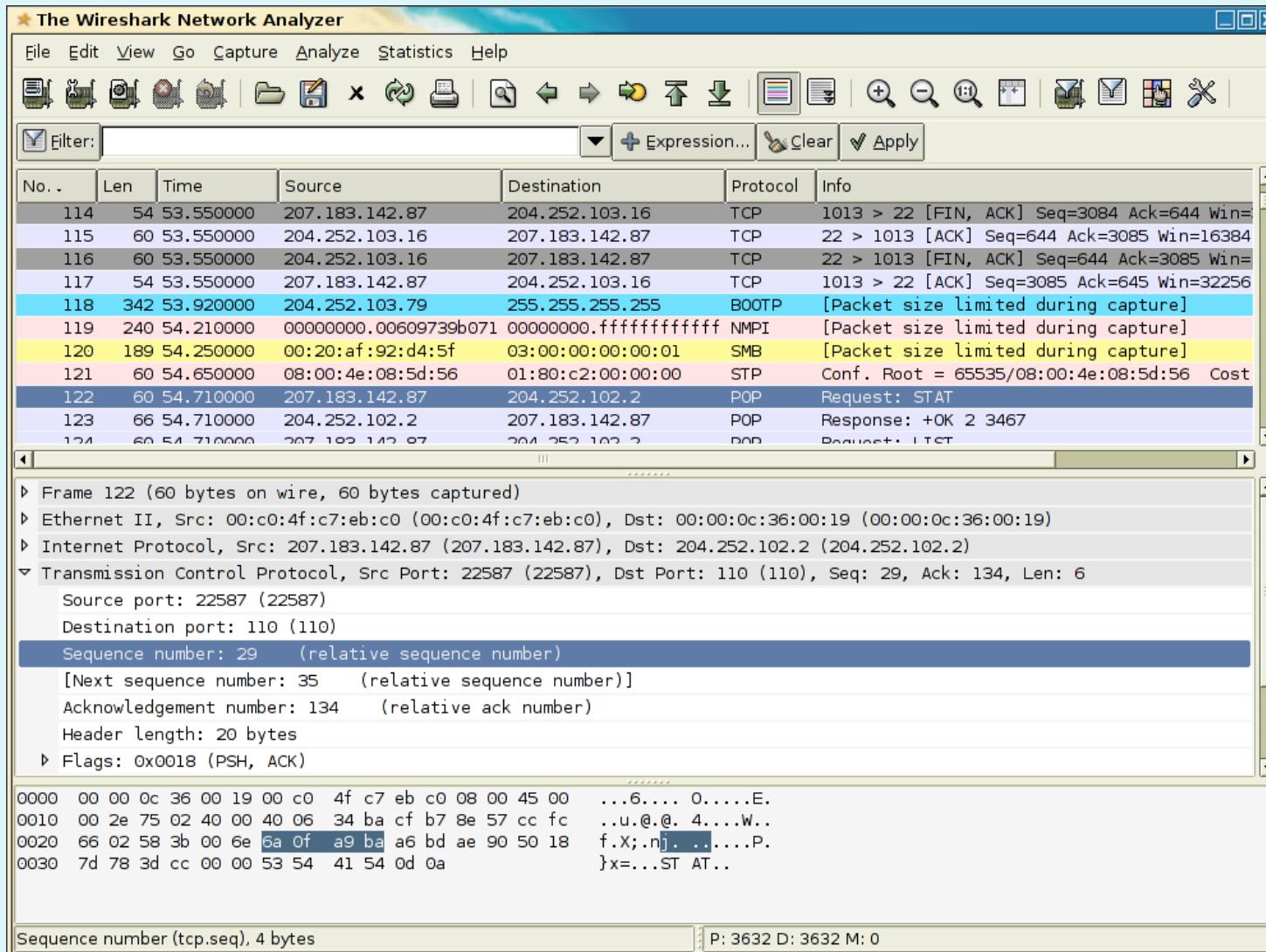
- za pošiljanje **HTTP zahtevka**, odjemalec najprej naslovi **TCP vtič** spletnega strežnika,
- **TCP SYN** segment se preko omrežja usmeri do spletnega strežnika
- spletni strežnik odgovori s **TCP SYNACK** (potrditev rokovanja),
- sedaj je **TCP povezava vzpostavljena!**

Primer komunikacije: spletno brskanje



- **HTTP zahtevek** se pošlje na **TCP vtič** spletnega strežnika,
- **IP datagram**, ki vsebuje spletno zahtevo po strani www.google.com se usmeri k spletnemu strežniku
- spletni strežnik odgovori s **HTTP REPLY**, ki vsebuje vsebino strani
- IP datagram s stranjo se usmeri h klientu,
- **WWW stran je kočno prikazana!**

Zajem podatkov iz omrežja



Zajem podatkov iz omrežja: primer DHCP

zahtevek

Message type: **Boot Request (1)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) **DHCP Message Type = DHCP Request**
Option: (61) Client identifier
Length: 7; Value: 010016D323688A;
Hardware type: Ethernet
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
Length: 11; Value: 010F03062C2E2F1F21F92B
1 = Subnet Mask; 15 = Domain Name
3 = Router; 6 = Domain Name Server
44 = NetBIOS over TCP/IP Name Server
.....

odgovor

Message type: **Boot Reply (2)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
Length: 12; Value: 445747E2445749F244574092;
IP Address: 68.87.71.226;
IP Address: 68.87.73.242;
IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."

Omrežna varnost



Omrežna varnost

- **Je področje, ki:**

- analizira možnosti vdorov v sisteme,
- načrtuje tehnikе obrambe pred napadi,
- snuje varne arhitekture, ki so odporne pred vdori.

- **Internet ni bil snovan ozirajoč se na varnost!**

- vizija interneta je sprva bila: „To je skupina ljudi, ki si med seboj zaupajo in je priključena na skupno omrežje“
- pri izdelavi protokola so ga proizvajalci delali z metodologijo „krpanja“,
- varnostne mehanizme je potrebno upoštevati na vseh plasteh OSI modela.

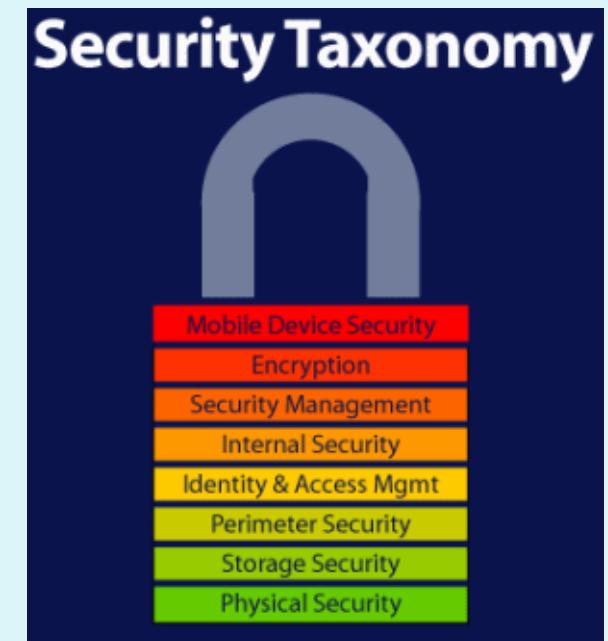
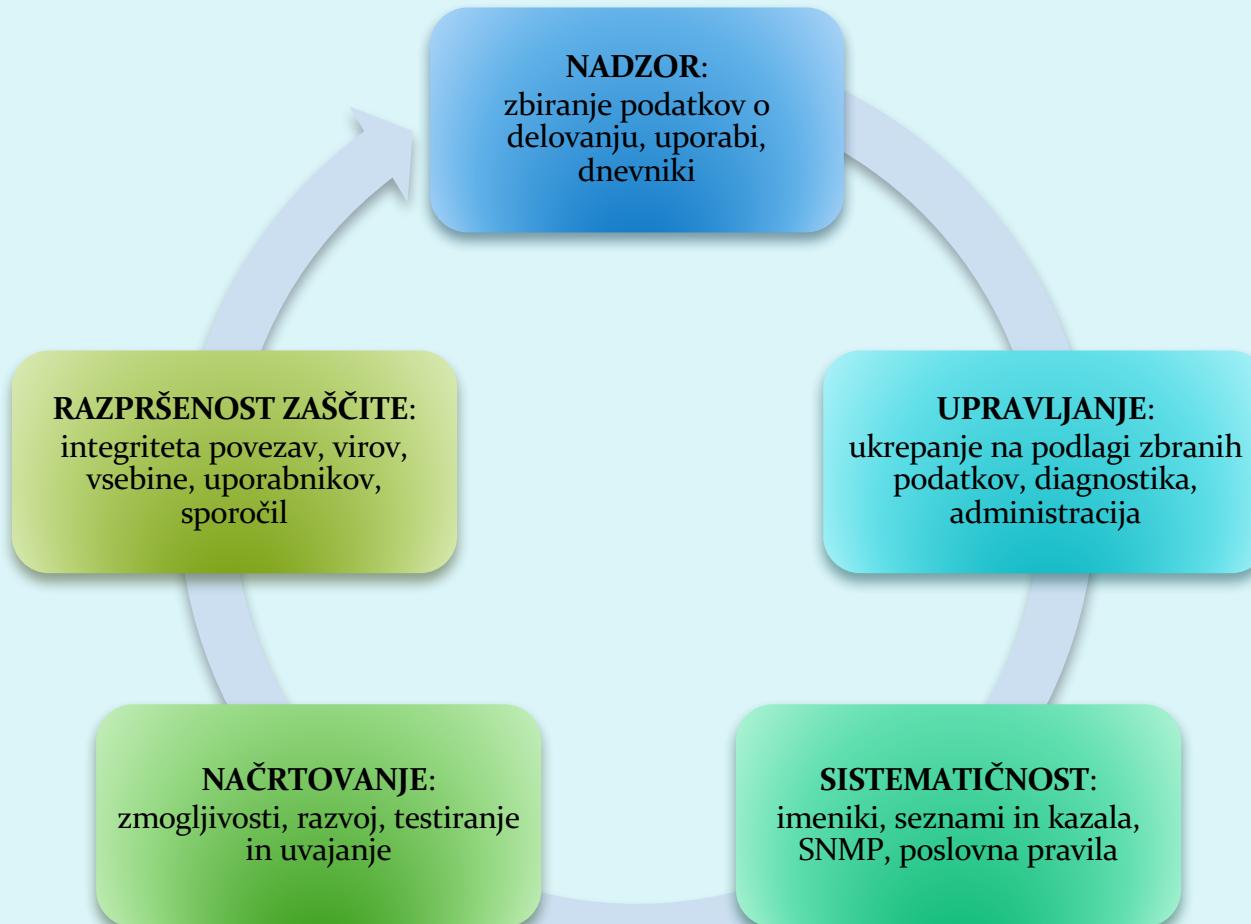
Kako lahko vdiralec škoduje sistemu?

Ima veliko možnih pristopov in tehnik!

- **prisluškovanje:** prestrezanje sporočil,
- aktivno **ponarejanje** sporočil v neki komunikaciji,
- **kraja identitete (impersonacija):** ponaredi lahko izvorni naslov ali poljubno drugo vsebino paketa,
- **prevzem povezave (hijacking):** odstrani pravega pošiljatelja ali prejemnika iz komunikacije in prevzame njegovo vlogo,
- **onemogočanje nudenja storitve (denial of service):** onemogoči uporabo regularne storitve (npr. s tem, da jo preobremenim)



Varnost: zagotavljanje zanesljivosti



Elementi varne komunikacije

- **Zaupnost** – kdo sme prebrati? (enkripcija)
- **Avtentikacija (authentication)** – dokaži, da si res ti (identifikacija – povej, kdo si, brez dokaza)
- **Razpoložljivost in nadzor dostopa** – preprečevanje nelegitimne rabe virov (*avtorizacija (authorization)* – ugotavljanje, ali nekaj smeš storiti, *beleženje (accounting)* – kaj je kdo uporabljal)
- **Integriteta sporočila** – je bilo med prenosom spremenjeno?
- **Onemogočanje zanikanja (nonrepudiation)** – res si poslal / res si prejel.
- V praksi:
 - požarne pregrade, zaznava vdorov (*intrusion detection*) sistemi,
 - varnost na aplikacijski, transportni, omrežni in povezavni plasti

Avtentikacija

Prepričamo se o dejanski identiteti osebe - sogovornika v komunikaciji.

PRISTOPI:

- izziv-odgovor (*Challenge-response*),
- zaupamo tretji strani,
- avtentikacija s sistemom javnih ključev.



Zaupnost sporočil: kriptiranje (zakrivanje) vsebine

Je način obrambe pred **pasivnimi** vdiralci (prisluškovlci) in **aktivnimi** vdiralci (ponarejevalci).

Sporočilo **P** **kriptiramo** s ključem **E()** - dobimo **kriptogram E(P)**. Kriptogram **E(P)** predelamo v izvorno obliko s ključem **D()**, dobimo izvorno sporočilo **D(E(P))=P**.

Vrste metod:

- **substitucijske** (menjava znakov) / **transpozicijske** (vrstni red znakov)
- **simetrične ($E=D$)**, npr. DES, AES) / **asimetrične ($E \neq D$)**, npr. RSA, ECC)

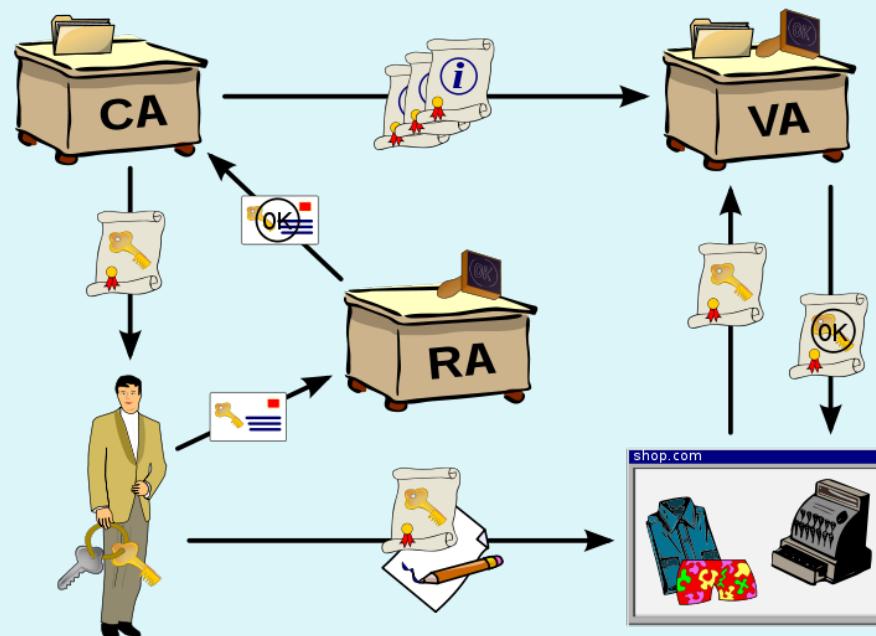
Vrste kriptografije

- Kriptografija uporablja ključe
 - kriptirni algoritem je običajno znan vsem,
 - tajni so le ključi
 - kriptiranje: skrivanje vsebine
 - kriptoanaliza („razbijanje“ kode)
- Kriptografija z javnimi ključi
 - $E() \neq D()$: dva ključa – javni in zasebni
- Simetrična kriptografija
 - $E() = D()$: samo en ključ
- Zgoščevalne funkcije – niso kriptografija
 - ne uporabljajo ključev. Kako so lahko koristne?

$$\begin{aligned} & \frac{x^2(y f(2x + 40)\bar{x})y_1 + e_2(x)y_2 + e_3(x)y_3}{(x+1)} \\ &= \left(\frac{x(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right) \\ &= \left(\frac{(x-1)(x-2)}{2}\right)1 + (x(x-1))0 \neq \left(\frac{x(x-1)}{2}\right)^2 \\ & f_p(x, y) \\ & \frac{y^2(y + 6x + x^2)^4(x + 7x^2 + 8x^3)^2(y + 9x + 6)^4(x + 1)}{1)(x + 6)^4(x + 9)^4} \\ & -9b + \sqrt{3}\sqrt{4a^3 + 27b^2}(y^3 + 6x)^2(y + 10x + 5)^2(x + 1) \\ & 2^{11/3}3^{2/3}x(x + 6)^2(y + 9x + 6)^2 \\ & + \frac{(1 - i\sqrt{3})(-9b + \sqrt{3}\sqrt[3]{4a^3 + 27b^2})^{1/3}}{2^{4/3}3^{1/3}x + 9} \\ & (y + 8x)^2(y + 7x + 4)^4(y + 1) \end{aligned}$$

Kriptografija z javnimi ključi

- **PKI (Public Key Infrastructure)** je sistem, ki opredeljuje izdelavo, upravljanje, distribucijo, shranjevanje in preklic digitalnih certifikatov.
- Uporabnike avtenticiramo s pomočjo javnih ključev, ki so overovljeni s strani certifikacijske agencije (*certificate authority, CA*).

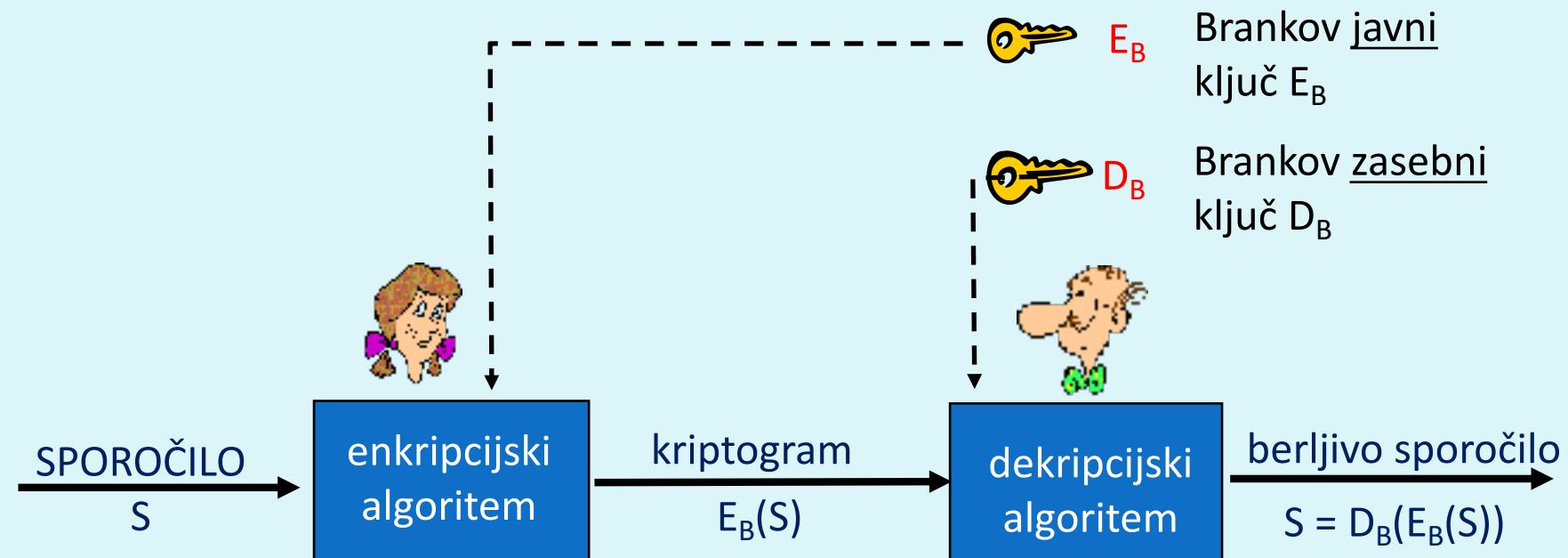


Kriptografija z javnimi ključi

- Algoritmi za kriptiranje z javnimi ključi so asimetrični, E=enkripcijski ključ, D=dekripcijski ključ, velja $E \neq D$
- Ključa **E** in **D** morata izpolnjevati naslednje zahteve glede kriptiranja sporočila **S**:
 1. $D(E(S)) = D(E(S)) = S$
 2. Iz znanih **S** in **E(S)** mora biti nemogoče ugotoviti **D**.
 3. Iz **E** mora biti zelo težko / nemogoče ugotoviti **D**.
- Najbolj znan algoritem je **RSA** (Rivest, Shamir, Adelman). RSA uporablja velika praštevila za določitev D in E, postopek kriptiranja/dekriptiranja pa je enak računanju ostanka pri deljenju s produktom teh praštevil.

Problem: distribucija ključev, počasnost.

Kriptografija z javnimi ključi



Zakaj je RSA varen?

- Denimo, da poznamo javni ključ neke osebe (določen z dvojico števil (n, e)). Za ugotavljanje zasebnega ključa moramo poznati delitelje števila n . Iskanje deliteljev nekega velikega števila pa je težko ali neizvedljivo z današnjimi računskimi kapacitetami.
- Kako poiskati dovolj velika praštevila?
 - večkrat izvedemo „ugibanje“: generiramo veliko število, nato ga testiramo, ali je praštevilo,
 - za testiranje praštevil obstajajo danes učinkoviti algoritmi.

Integriteta

- **Integriteta uporabnikov:** dokazuje, kdo je sporočilo poslal in da sporočilo bere le pravi prejemnik. Sporočilo S , ki ga uporabnik A pošlje B kriptiramo

in odkriptiramo:

$$E_A(D_A(S)) = S$$

$$\begin{aligned} E_B(D_A(S)) &= \text{XXX} \\ D_B(\text{XXX}) &= D_B(E_B(D_A(S))) = D_A(S); \end{aligned}$$

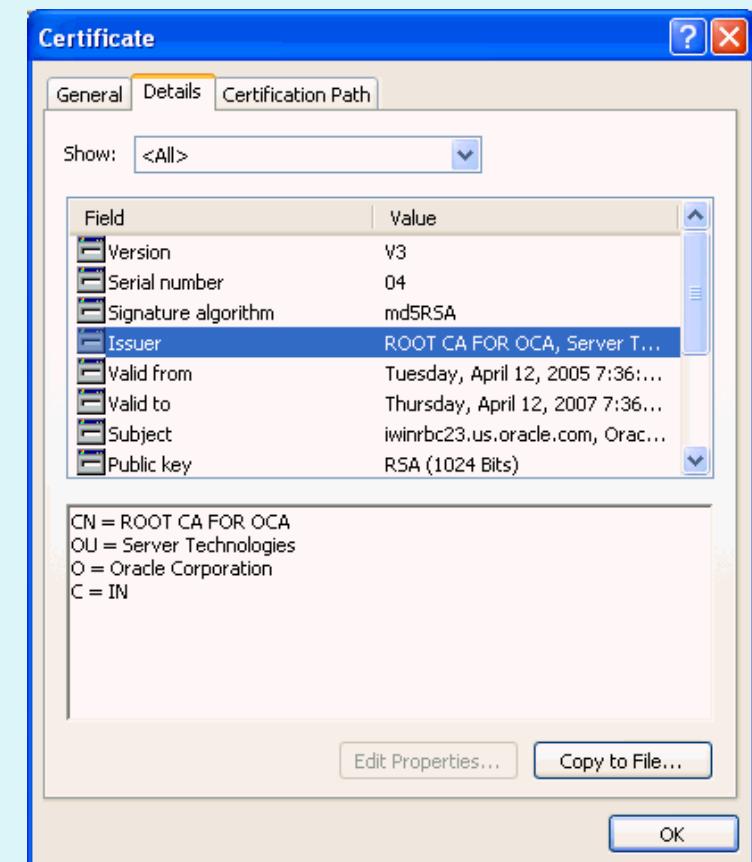
- **Integriteta sporočila:** dokazuje, da sporočilo (tudi nekriptirano!) ni bilo spremenjeno. Uporablja se zgoščevalne funkcij, ki izračunajo podpis sporočila $\text{sig}(S)$. To vrednost podpišemo z mehanizmom elektronskega podpisa

$$D_A(\text{sig}(S)) = \text{sss}$$

in sss pošljemo skupaj s (kriptiranim) originalnih sporočilom XXX : (XXX, sss) Prejemnik odkriptira XXX v S , ponovno izračuna $\text{sig}(S)$ in preveri, ali $\text{sss} = \text{sig}(S)$.

Certifikati

- Sistem PKI vsebuje certifikacijske agencije (angl. certification authority), ki izdajajo, hranijo in preklicujejo certifikate.
- Certifikati so definirani s standardom X.509 (RFC 2459)
- Certifikat vsebuje
 - naziv izdajatelja,
 - ime osebe, naslov, ime domene in druge osebne podatke,
 - javni ključ lastnika,
 - digitalni podpis (podpisan z zasebnim ključem izdajatelja),



Naslednjič gremo naprej!

- priključitev računalnika na omrežje
- zagon računalnika: protokola DHCP in BOOTP
- arhitektura strežnik – odjemalec,
- protokol: delovanje, njegove funkcije,
- sled protokola

