Univerza
v Ljubljani

Pedagoška
fakulteta

Računalniške komunikacije

Uvod, primer komunikacije, ping, traceroute, lookup, arp

Nosilec predmeta: dr. Jože Rugelj
joze.rugelj@pef.uni-lj.si
Asistent: Matej Zapušek

Virtualna učilnica

- Virtualna učilnica:
  - http://ucilnica.pef.uni-lj.si

- Ključ za učilnico: RK1415

Obveznosti študentov

- 1 kolokvij: za pozitivno oceno je potrebno pisati več kot 50%.
- Pozitivno ocenjen kolokvij lahko nadomesti pisni del izpita.
- Če študent z oceno iz kolokvija ni zadovoljen, lahko vseeno opravlja pisni del izpita. Upošteva se boljša ocena.

Obveznosti študentov

- Pozitivna ocena na pisnem izpitu oz. pozitivna ocena kolokvija je pogoj za pristop k ustnemu delu izpita.

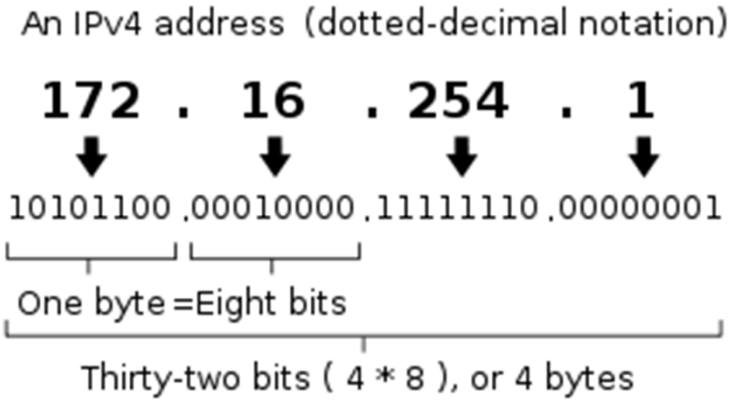
- Če je ustni del izpita ocenjen negativno, je treba ponovno opravljati pisni del izpita

Študijska literatura

- A. Tanenbaum: Computer Networks, 4rd ed., Prentice Hall
- T. Vidmar: Računalniške komunikacije
- D.E. Comer: Internetworking with TCP/IP, vol. 1,2,3,Prentice Hall
- O. Kirch: Linux Network administrator guide, O'Reilly & Assoc.

IP naslov

- Protokol zadolžen za logično naslavljanje
- Sistemski položaj naprave v omrežju (podobno kot hišni naslov)
- Število je 32bitno, zapisano v obliki 4 osembitnih polj (okteti) zapisanih v desetiški obliki



IP naslov

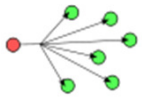
- Vsak IP ima dva dela:
  - Omrežno predpono ali omrežno identifikacijo (net ID)
    - Vsi gostitelji na istem omrežju omrežju imajo dodeljeno isto omrežno identifikacijsko oznako, ki je enolično določena
  - Gostiteljevo identifikacijo (host ID)
- Razdeljeni v kategorije (A,B,C,D,E)
  - Kategorija A (8b Network, 24b Host)

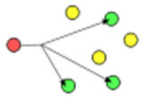
  - Kategorija B (16b Network, 16b Host)

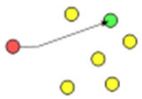
IP naslov

- Kategorija C (24b Network, 8b Host)

- A,B,C kategorije namenjene unicast naslavljanju


broadcast


multicast


unicast

- Kategorija D - multicasting
- Kategorija E – raziskovalni nameni IETF (The Internet Engineering Task Force)

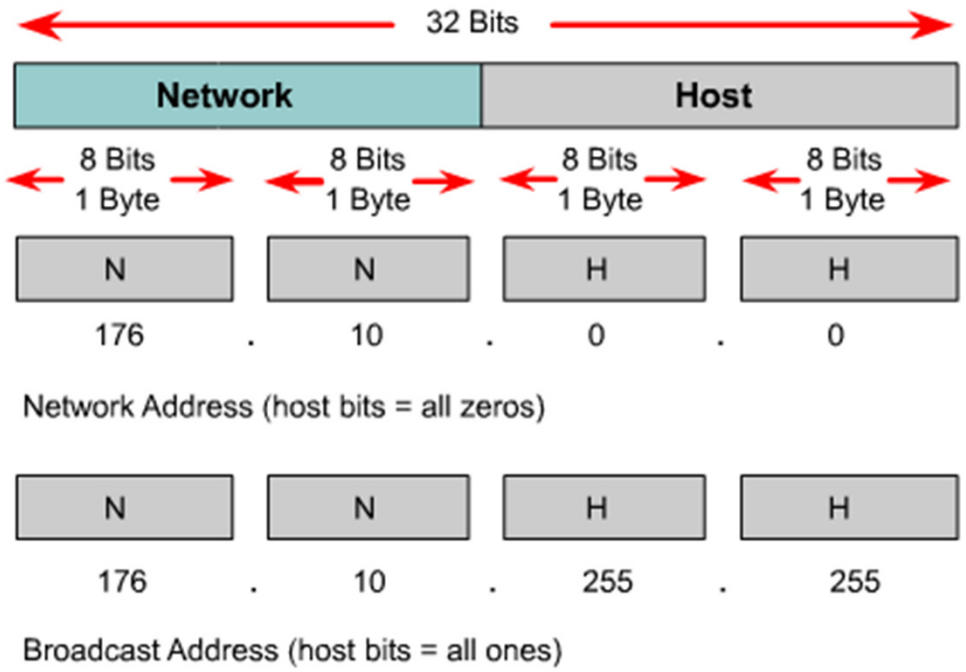
IP naslov

Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class A	0	0-127	8	126	16,777,216
Class B	10	128-191	16	16,384	65,536
Class C	110	192-223	24	2,097,152	254
Class D	1110	224-239	28	N/A	N/A

Rezervirani IP naslovi:

- Nekateri naslovi za gostitelje so rezervirani in jih ne moremo dodeliti napravam v omrežju.
- IP naslov, ki ima na vseh bitih v gostiteljevem delu IP naslova vrednost 0 je rezerviran za **naslov omrežja** (identificira omrežje).
- IP naslov, ki ima na vseh bitih v gostiteljevem delu IP naslova vrednost 1 je rezerviran za **broadcast naslov**.

IP naslov


32 Bits
Network
Host
8 Bits
1 Byte
8 Bits
1 Byte
8 Bits
1 Byte
8 Bits
1 Byte
N
N
H
H
176 . 10 . 0 . 0
Network Address (host bits = all zeros)
N
N
H
H
176 . 10 . 255 . 255
Broadcast Address (host bits = all ones)

Privatni IP naslovi

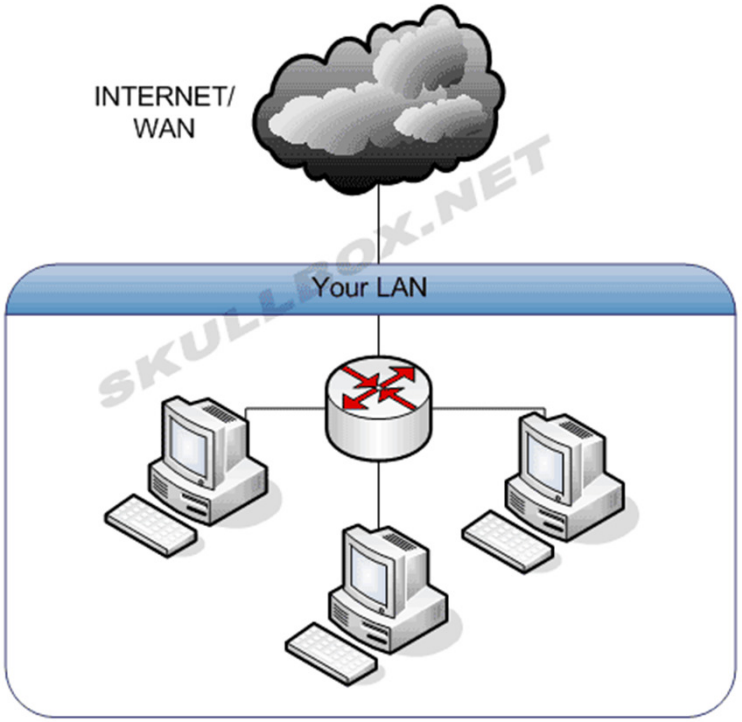
- Javno omrežje
  - naprave morajo imeti različne IP naslove
  - Taki IP naslovi so globalni in standardizirani
- Problem pomankanja IP naslovov!
- Rešitev: privatni IP naslovi
  - The Internet Assigned Numbers Authority (IANA) rezervirala naslove za uporabo v privatnih omrežjih
  - V omrežju internet se ti naslovi ne uporabljajo (se ne usmerjajo)
  - Za povezavo privatnega omrežja z internetom je potrebno uporabiti NAT.

NAT (Network address translation)

- Proces spreminjanja informacije o mrežnih naslovih v paketih, ki potujejo preko usmerjevalnika z namenom spreminjanja naslovnega prostora.

- Omogoča:
  - Napravam povezanim v privatno omrežje uporabo enega javnega IP naslova.
  - Povezava LAN – WAN
  - DHCP
  - Varnost (omejuje promet)

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16



Statični, dinamični IP naslovi

- **Statični** naslov je ob vsaki vzpostavitvi povezave isti.
- Lastnosti (+/-):
  - (+) možnost vzpostavitve strežnika
  - (+) poenostavljen oddaljen dostop do računalnika
  - Dostopanje do virov (IP, poleg username+pass. Npr. Web of Science)
  - (-) manjša varnost
  - (-) včasih so potrebne "ročne" nastavitve
  - (-) ni vedno dostopna možnost (nekateri ponudniki tega ne omogočajo)

Statični, dinamični IP naslovi

- **Dinamični** naslov se po vsaki prekinitivi in vzpostavitvi povezave spremeni.
- Lastnosti (+/-):
  - (+) vse potrebne podatke računalnik pridobi od DHCP-strežnika, zato ni potrebna nobena "ročna" namestitev s strani uporabnika,
  - (+) manjša verjetnost vdora ali drugih oblik nadlegovanja, saj je IP-naslov vsakič drugačen,
  - (+) cenejša možnost, saj mnogo ponudnikov to obračunava kot dodatno storitev;
  - (-) neustrezna izbira, kadar želimo vzpostaviti lasten strežnik in
  - (-) če imamo dostop do določenega strežnika omejen z IP-naslovom (npr. dostop do strežnika, kjer se je treba predstaviti tudi z IP-naslovom, ne le z uporabniškim imenom in geslom).

ARP (Adress resolution protocol)

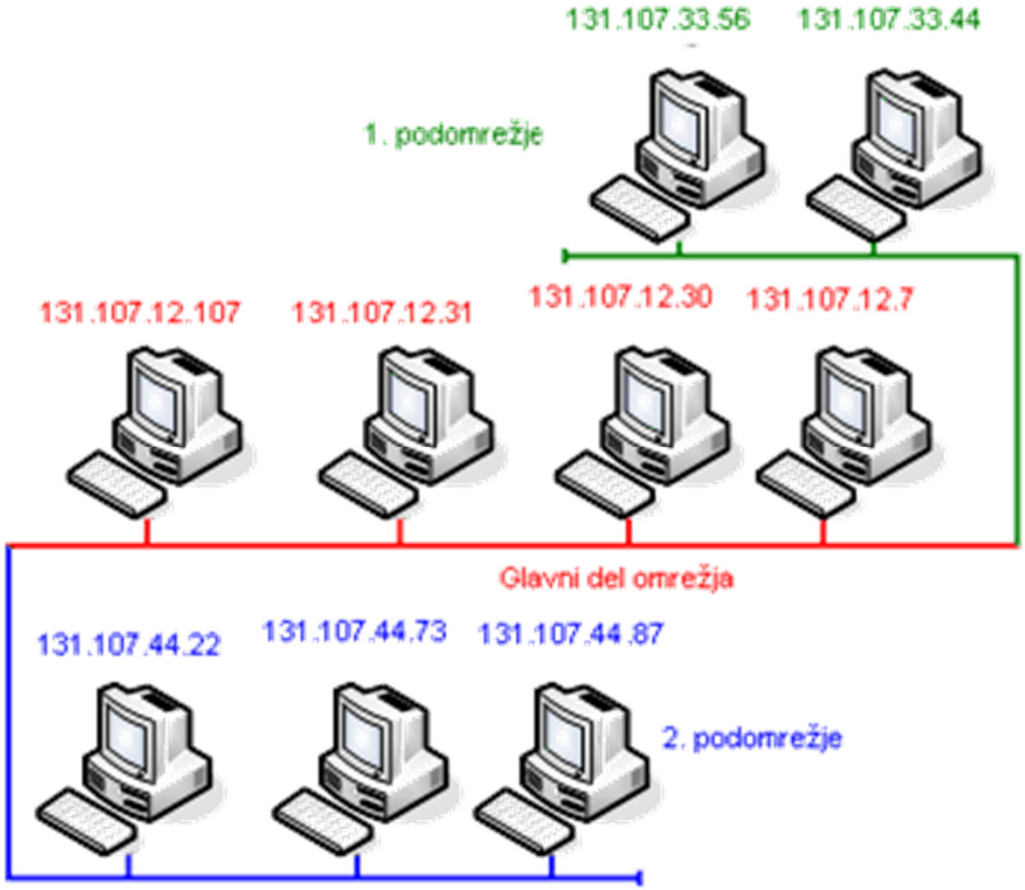
- Pridobitev neznanega L2 naslova iz znanega L3 naslova.
- Ko naprava A pošlje paket napravi B, pozna svoj IP naslov in IP naslov naprave, kamor pošilja. Ker protokol na L2 ne razume teh naslovov (MAC ali strojni naslov) je nujno potrebno prevesti IP naprave B v njen MAC address.

- Kako to naredi?
  - Najprej pogleda, če ima v svoji ARP tabeli informacijo o MAC naslovu naslovnega gostitelja. Če ne najde, potem:
  - Naprava A z razpršenim oddajanjem pošlje poizvedbo, kdo je naprava, ki se skriva pod IP naslovom naslovnega gostitelja?
  - Naprava B sliši ARP zahtevo, ker je to njen IP vrne svoj MAC naslov, druge naprave zahtevo ignorirajo.
  - Izvorni gostitelj posodobi svojo ARP tabelo

- Kaj če se pošlje sporočilo napravi, ki je v drugem omrežju kot pošiljajoča naprava? (Proxy ARP)
  - Ko router dobi zahtevo preko razpršenega oddajanja iz omrežnega dela ugotovi, da gre za napravo na drugem omrežju.
  - Router oddajanja ne spusti naprej (router ustavi razpršeno oddajanje, ga ne posreduje)
  - Router javi nazaj svoj MAC naslov
  - Ko router dobi paket s svojim MAC naslovom izbriše L2 podatke
  - Kot source uporabi svoj MAC naslov, za destination pa MAC naslov usmerjevalnika, ki mu bo posredoval paketke

Podomrežja

- Zakaj?
  - Razdelitev lokalnih omrežij
  - Večje število omrežij
  - Varnost
    - Dostop do drugega podomrežja le preko routerja.
    - Access list – določila kdo lahko dostopa do podomrežja
- Kako?
  - Gostiteljeve bite uporabimo kot bite omrežja


131.107.33.56
131.107.33.44
1. podomrežje
131.107.12.107
131.107.12.31
131.107.12.30
131.107.12.7
Glavni del omrežja
131.107.44.22
131.107.44.73
131.107.44.87
2. podomrežje

Podomrežja

- Pričnemo pri MSBju gostitelja (bit najbližje mrežnemu delu) in si **sposodimo** toliko bitov, kot jih potrebujemo za realizacijo podomrežij
- Naslovi podomrežja vsebujejo:

  mrežni + podomrežni + gostiteljev del

- Kreiranje podomrežji je interna funkcija LAN-a.
- Na zunaj je LAN videti kot enotno, nerazdeljeno omrežje.

Podomrežja

- Določitev št. bitov v procesu kreiranja podomrežji odvisna od max. št. gostiteljev na enem podomrežju.
- Zadnja dva bita IP naslova ne moreta biti nikoli določena podomrežju (katerakoli kategorija)
- Formule za določitev št. uporabljenih bitov:
  - 2^št. sposojenih bitov – 2 = št. podomrežij
  - 2^št. preostalih bitov gostitelja – 2 = št. Uporabnikov
  - Zakaj **-2** ? (samih ničel oz. enic gostitelju ne smemo prirediti)

Maska podomrežja

- Maska podomrežja pove routerju v katerem omrežju in podomrežju se nahaja gostitelj in določa kolikšen del IP naslova je namenjen omrežnemu delu in kolikšen gostiteljevemu.
- Kako dobimo masko podomrežja:
  - Določimo na koliko podomrežij bo razdeljeno omrežje. Število pretvorimo v dvojiški sistem.
  - Preštejemo št. bitov. Npr. če potrebujemo 6 podomrežij je dvojiška vrednost 110, za kar potrebujemo 3 bite
  - Za vrednost števila bitov (v tem primeru 3) dodamo enice za LSBjem omrežnega dela, ki je zapisan s samimi enicami.
  - Gostiteljev del je sestavljen iz samih ničel
  - Pretvorimo nazaj v desetiško vrednost

Maska podomrežja

- Primer:

Example of a Class C Subnet

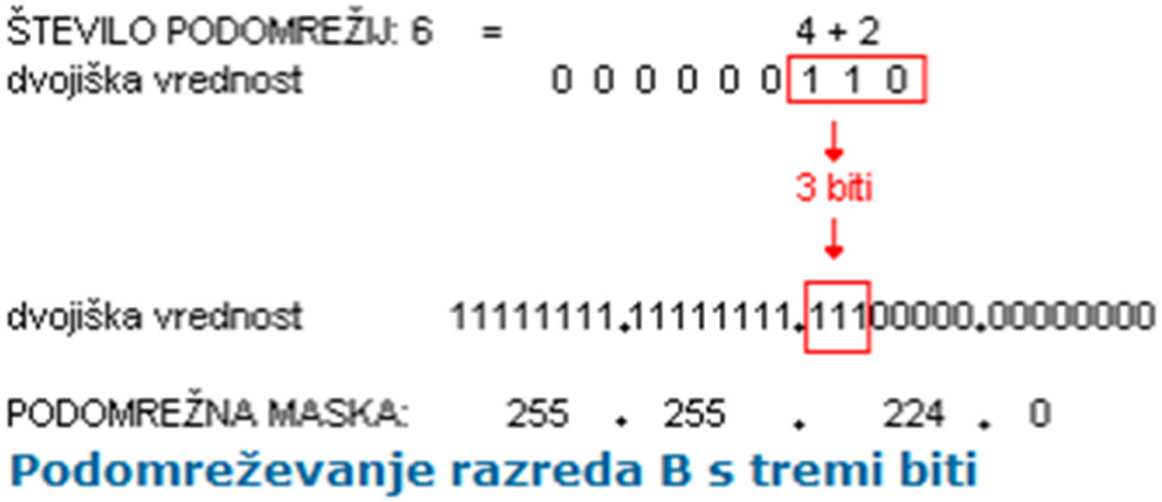
Number of Subnets	6			
Binary Value	0 0 0 0 0 0 1 1	0		
				4 + 2 = 6
Convert to Decimal	11111111	11111111	11111111	11100000
Subnet Mask =	255 .	255 .	255 .	224
198.53.147.45	11000110	00110101	10010011	00101101
255.255.255.224	11111111	11111111	11111111	11100000
	11000110	00110101	10010011	00100000
	198	53	147	32

Host Address Range

198.53.147.33 to 198.53.147.62

00100000

6 Subnets 30 Hosts



Podomreževanje razreda B s tremi biti

DHCP

- *Dynamic Host Configuration Protocol*
- omrežni protokol za dinamično nastavitev gostiteljevih parametrov.
- Dinamično dodeljuje napravam IP naslove iz določenega obsega.
- Sestoji iz 3 komponent:
  - Odjemalca (večina TCP/IP implementacij ima DHCP odjemalce vgrajene v sistem).
  - Strežnika (aplikacija, ki teče na računalniku in daje usluge odjemalcem, vgrajena v skoraj vse strežniške distribucije OS)
  - Protokola, ki komunicira med njima.
- DHCP strežniki in odjemalci niso odvisni od platforme.

DHCP

- Ključna naloga: dodeljevanje IP naslovov

- Načini:
  - ***Ročna nastavitev:*** Administrator nastavi določen IP vsaki postaji na DHCP strežniku in strežnik nato posreduje ta naslov.
  - ***Samodejna nastavitev:*** DHCP strežnik zagotavlja odjemalcem IP naslove, ki se nahajajo v množici, odjemalci jih dobijo v stalno uporabo.
  - ***Dinamična nastavitev:*** DHCP strežnik zagotavlja odjemalcem IP naslove, ki se nahajajo v množici. Odjemalci morajo periodično obveščati strežnik o uporabi tega naslova. V primeru ne odziva odjemalca, se naslov vrne v množico neoddanih naslovov.

Privzeti prehod (default gateway)

- Kaj je gateway?
  - Naprava v omrežju, katere vloga je povezovanje z drugimi omrežji
  - Usmerjevalna naprava, ki ve kako usmerjati promet med omrežji in podomrežji
  - Potreba po določitvi poti (pot definiramo kot seznam naslovov vozlišč preko katerih mora iti paket, da pride do svoje končne lokacije)
  - Gateway ne ve točne poti za vsak paket (za nekatere da), ve pa vsaj poti do drugih gatewayev katerim jih posreduje
  - "Po domače": Če hočemo v (pod)omrežju poslati nekaj na napravo, ki ni v tem (pod)omrežju to storimo preko gatewaya.

Privzeti prehod (default gateway)

- Kaj pa privzeti prehod?
  - Privzeti prehod je na istem podomrežju kot računalnik preko katerega se povezujemo
  - Računalnik ga uporabi vedno, kadar želi dostopati do računalnika, ki ni v tem podomrežju
  - To je ponavadi IP routerja, ki ga dobimo od ISPja
- Kako vidimo kakšen je naš "default gateway":
  - *Start*
  - *cmd*
  - *ipconfig*

PING

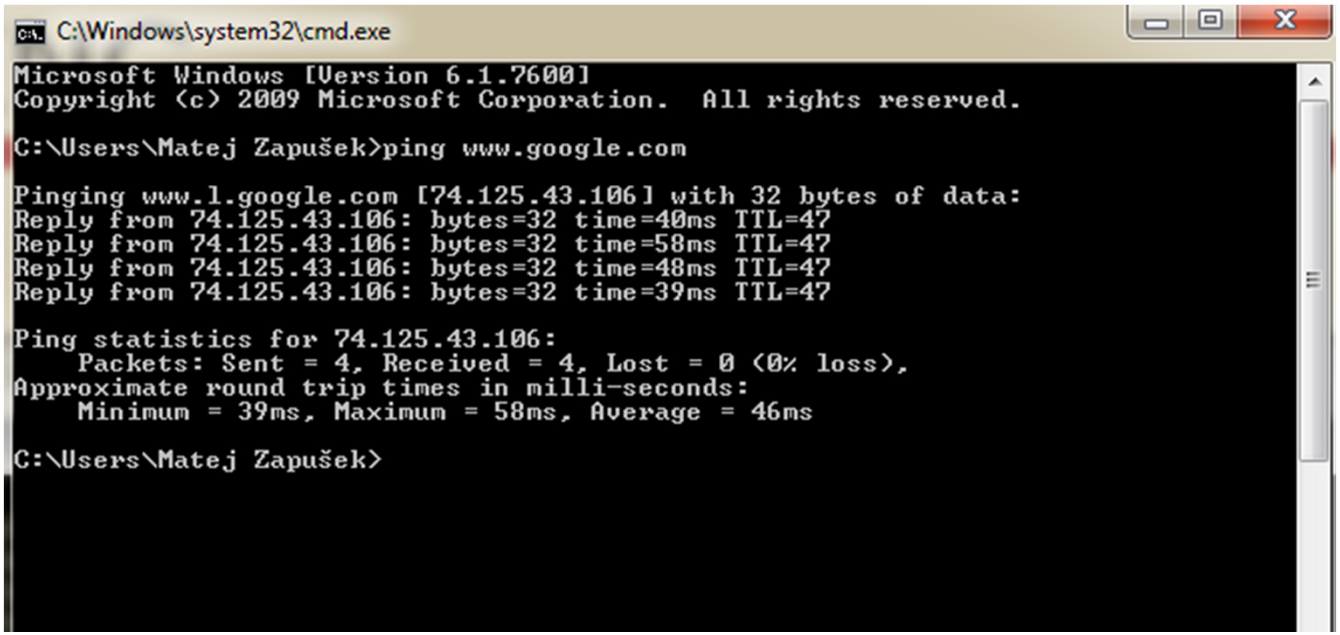
- Uporaba:
  - Dosegljivost gostitelja preko IP omrežja.
  - Samotestiranje mrežne kartice
  - Test zakasnitve (latency) – čas, ki ga porabi prvi bit od klienta do strežnika
- Delovanje:
  - Pošiljanje ICMP paketov
  - Poslušanje odgovora (tudi v obliki ICMP paketa) – imenujemo PONG

ICMP paket

ICMP packet

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
IP Header (160 bits OR 20 Bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (64+ bits OR 8+ Bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

PING


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Matej Zapušek>ping www.google.com
Pinging www.l.google.com [74.125.43.106] with 32 bytes of data:
Reply from 74.125.43.106: bytes=32 time=40ms TTL=47
Reply from 74.125.43.106: bytes=32 time=58ms TTL=47
Reply from 74.125.43.106: bytes=32 time=48ms TTL=47
Reply from 74.125.43.106: bytes=32 time=39ms TTL=47
Ping statistics for 74.125.43.106:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 39ms, Maximum = 58ms, Average = 46ms
C:\Users\Matej Zapušek>

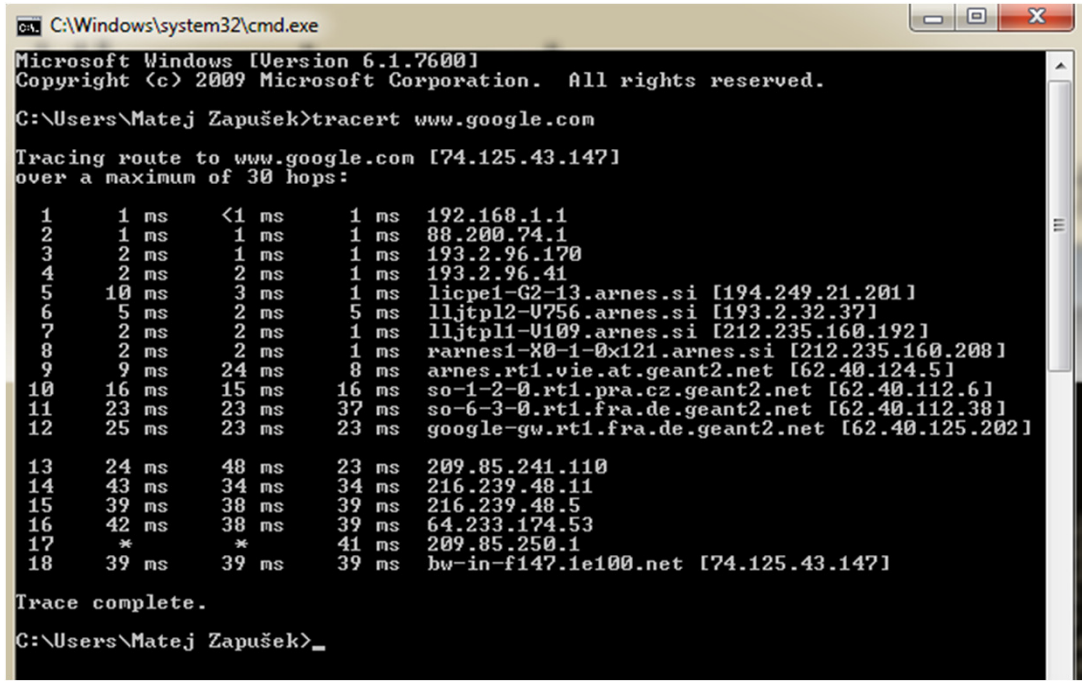
PING

- Pridobljeni podatki:
  - round-trip delay time (RTT) – čas potovanja paketka do strežnika in nazaj k nam.
  - Koliko paketkov se je izgubilo (packet loss)
  - Statistični povzetek o:
    - Paketkih poslanih iz strežnika k nam
    - Min., maks., povpr. RTT
- Zanimivosti:
  - Ping flood:
    - Denial of service attack
    - Strežnik “zasujemo” z ICMP paketki
  - Ping of death:
    - Pošiljanje nepravilno oblikovanega ICMPja.

TRACEROUTE

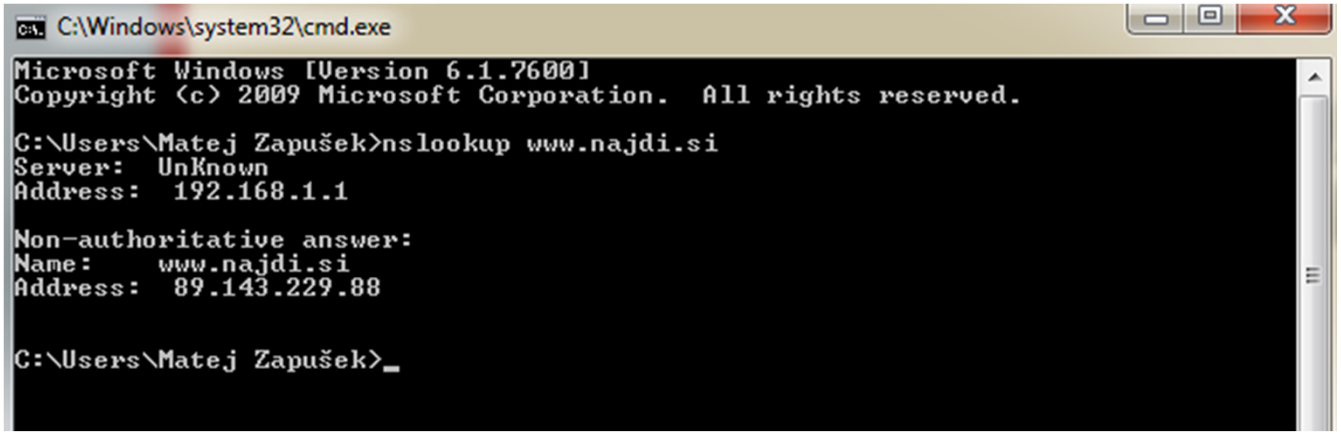
- Ukaz: tracert
- Pokaže pot do iskanega strežnika
- Možni parametri:
  - -d: ne pridobiva imen domen od DNS strežnikov, izvedba ukaza je tako hitrejša.
  - -h: maximum hops (največje število korakov na poti do destinacije, ki jih opravi)
  - -w timeout: čaka za vrednost timeouta na odgovor routerja.
- Delovanje:
  - Izvorni računalnik tvori niz (v tracert oz. navadno 3) UDP datagramov na neveljaven port host-a.
  - Vsak datagram ima parameter TTL, ki se povečuje za ena ob doseganju vmesnih destinacij. V prvem koraku nastavi TTL = 1 in pošlje datagram, v drugem je TTL = 2, itd. Ko router sprejme datagram, zmanjša TTL za ena.

- Če TTL enak 0, tedaj proces na routerju tvori obvestilo o "napaki" v obliki ICMP sporočila (obvestilo: Time Exceeded Message), ki ga pošlje nazaj.
- Iz tega obvestila izračuna čas in IP routerja od katerega je dobil sporočilo.



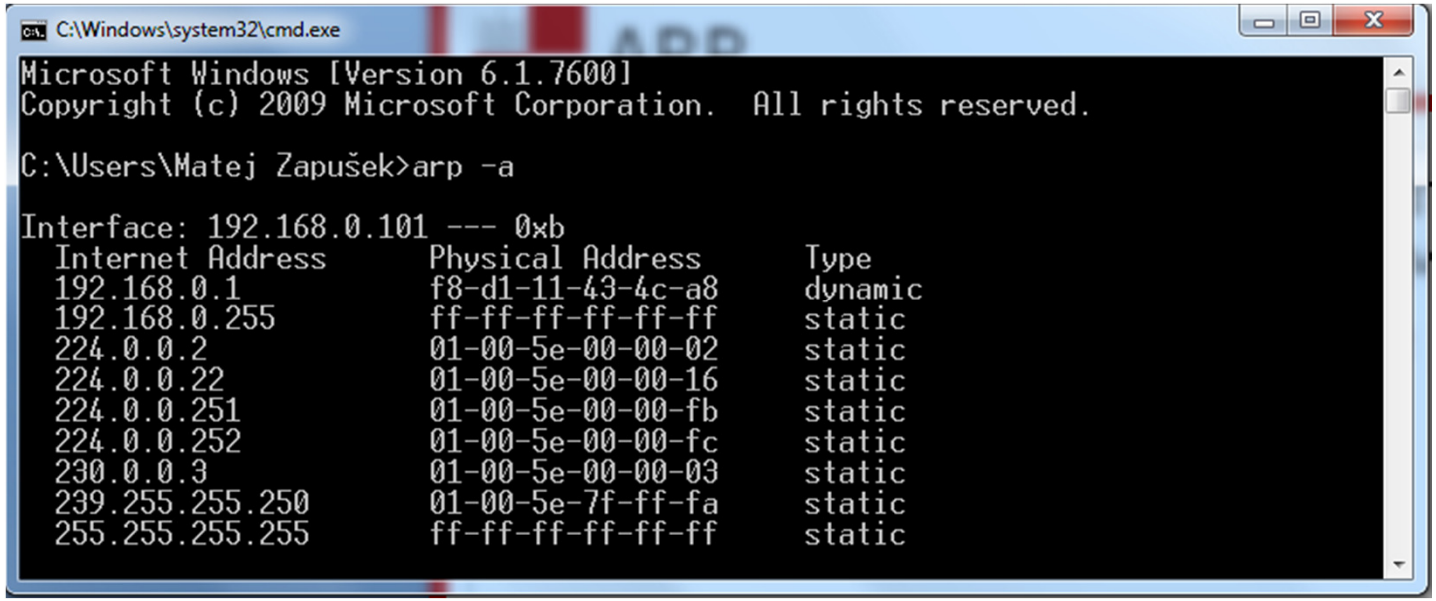
NSLOOKUP

- Nslookup je ukaz, ki najde ime strežnika iz njegovega IP naslova ali IP strežnika iz njegovega imena.



Podatki o ARP poizvedbah

- Preko ukaza *arp –a* pogledamo povezave med IP naslovi in MAC naslovi, ki smo jih na zadnje pridobili.



Vprašanja, ki jih rešujemo…

- Če so problemi, potem skušamo odgovoriti na:
  - Ali imamo dodeljen IP naslov?
  - Ali lahko pingamo ostale računalnike v podomrežju?
  - Ali je default router v routing tabeli?
  - Lahko pingamo IP naslov od default routerja (privzeti prehod)?
  - Ali lahko pingamo po IP naslovih računalnike, ki jih dosegamo preko routerja?
  - Ali je dobro shranjeno ime DNS-ja (ali je pravilno vpisano)?
  - A lahko pingamo IP naslov od DNS-ja?
  - Ali lahko pingamo ostale računalnike po imenih?

Naloga

- Zaženi CMD. Uporabi funkcije PING, TRACEROUTE in NSLOOKUP za naslednje strežnike:

  - Berkeley.edu
  - Mit.edu
  - Vu.nl
  - www.usyd.edu.au
  - www.uct.ac.za
  - www.pef.uni-lj.si

  Poglej kako potujejo paketki pri posameznem primeru. Razmisli, kaj povedo ti podatki.

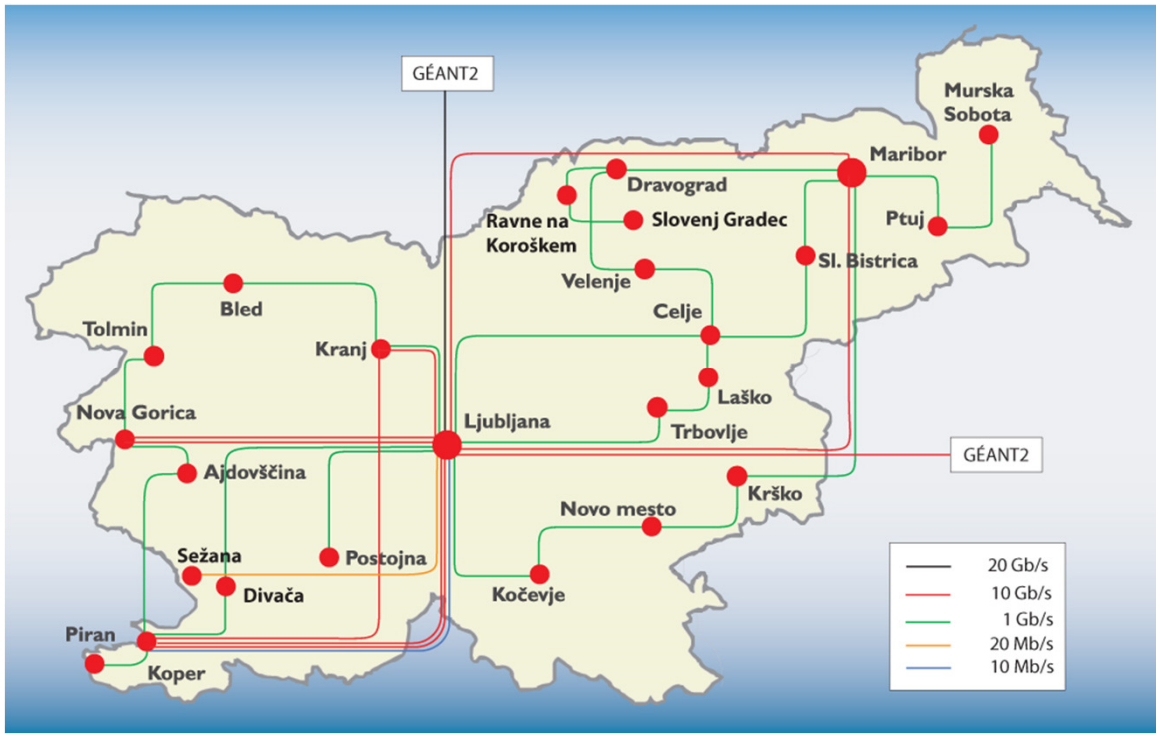
  Uporabite funkcijo traceroute večkrat za isto domeno in poglejte ali je izpis oz. pot potovanja paketkov vedno enaka.

Arnes

- Arnes - Akademska in raziskovalna mreža Slovenije
- Zavod, ki zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture.
- Arnes gradi, vzdržuje in upravlja infrastrukturo, ki povezuje univerze, inštitute, raziskovalne laboratorije, muzeje, šole, baze podatkov in digitalne knjižnice.
- V omrežje ARNES je povezanih več kot 1000 slovenskih organizacij, storitve Arnesa pa na tak način uporablja blizu 200.000 ljudi.
- Mednarodna povezljivost z izobraževalnimi in raziskovalnimi omrežji drugih držav je zagotovljena preko več desetgigabitnega omrežja GÉANT2, ki ga sofinancira Evropska komisija.

Arnes – topologija omrežja

Komunikacijsko omrežje ARNES je sestavljeno iz **hrbtenice** (angl. **backbone**) omrežja, ki povezuje kraje po Sloveniji, in strank omrežja, ki so priključene na hrbtenico ARNES na njenih vozliščih. Hrbtenica omrežja je povezana v tuja omrežja preko mednarodnih vodov.



GÉANT2

- visoko zmogljiva širokopasovna povezava
- Namenjena raziskovalnim in izobraževalnim ustanovam v Evropi
- Direktno povezuje 34 evropski držav med seboj in v druge regije
- “srce” globalnega raziskovalnega omrežja

GÉANT2 - topologija

- http://www.geant2.net/upload/pdf/GN2_Topology_Feb_09.pdf

Omrežje na PeF

- Omrežje Metulj povezano z omrežjem Arnes preko 3 vodov.
- Preko vozlišča na EF povezani na omrežje Metulj.
- Iz EF z optično povezavo do PeF (routerji v P020)
- Z optiko do vsakega nadstropja
- V vsakem nadstropju SWITCH in z UTP kablom povezava s kabineti.

Zanimive povezave

- TJPing
  program za pinganje, ipd.
  http://www.topjimmy.net/tjs/

- Spletna stran za pinganje, ipd.
  http://www.ping.eu/