

Tru64: Mreža i servisi

Dinko Korunić
v1.0, travanj 2005.



O predavaču

- višegodišnji vanjski suradnik časopisa Mrež@, vlastita kolumna "Digitalna radionica - Linux", itd.
- vanjski suradnik SRCE-a: forenzike provaljenih sustava, izgradnja sistemskih paketa, helpdesk za sistemce, sigurnost Unix baziranih sustava, predavač, itd.
- sigurnosni ekspert pri InfoMAR d.o.o.

Tijekom prezentacije

- **ako što nije jasno - pitajte i tražite objašnjenje!**
- **ako što nije točno - ispravite!** greške su moguće i česte, posebice za prvu verziju
- **diskusija** je poželjna i produktivna
- **ako je prebrzo - tražite da se uspori!**
- **ako je pak presporo i uspavljuje vas - lako se ubrza** sa sadržajem
- **podijelimo** zajedno vlastita iskustva

Dio I: Uvod u mreže



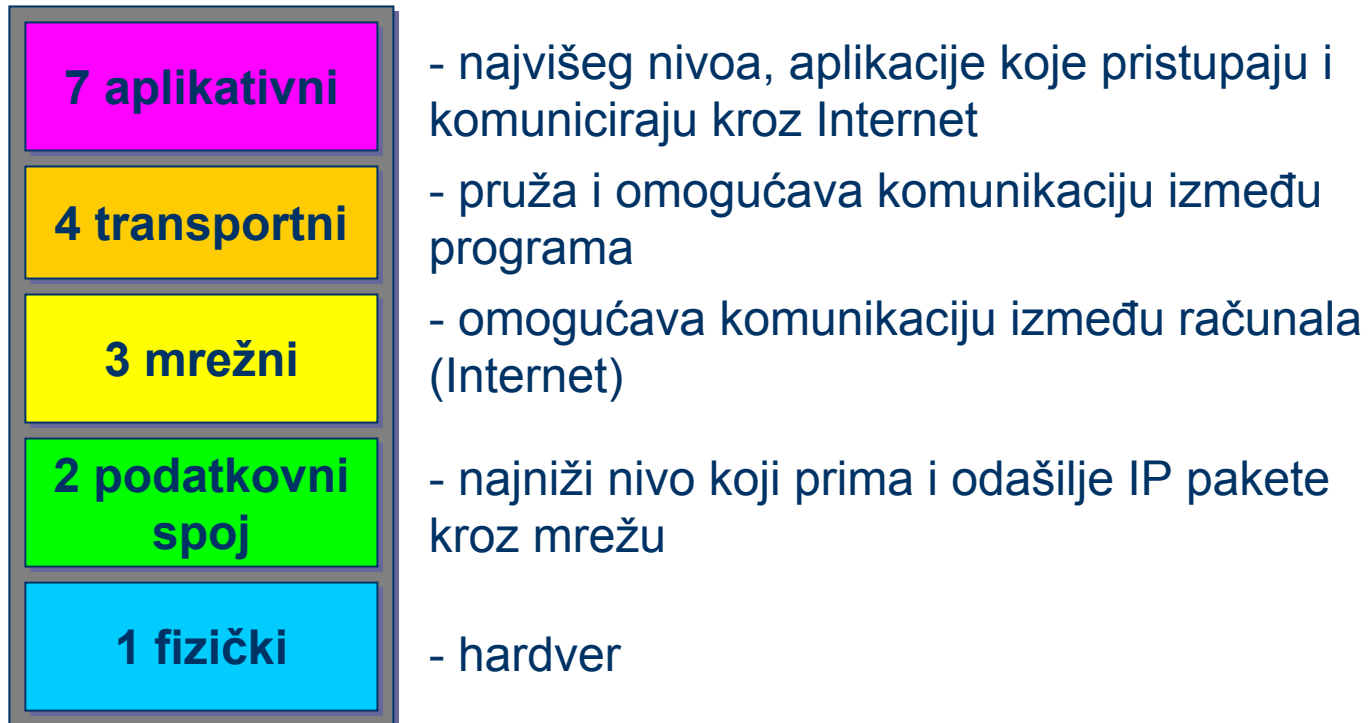
Protokoli

- radi međusobnog komuniciranja
- nužna standardizacija - 2+ uređaja moraju se slagati u protokolu
- protokol = niz pravila kako se se razmjenjuju informacije
- ISO razvio teoretski OSI model
- OSI - mnogima referenca za razvoj
- IPv4 - prihvaćeni protokol za Internet komunikaciju: 32bit - 4 okteta tvore adresu

Internet

- niz heterogenih, miješanih mreža
- sigurnosni problem
- komunikacija kroz IPv4 i IPv6 (te treba postati općeprihvaćena zamjena) protokol
- IPv4
 - općeprihvaćen
 - premalo adresa
 - problem lažiranja adresa
 - nema krypto i sigurnosnih mogućnosti

TCP/IP DARPA model - u uporabi



OSI model - referentni, teorijski



- najvišeg nivoa, aplikacije koje koriste mrežu
- funkcije trebaju programima kad koriste mrežu (npr. prezentacija podataka, ASCII, ...)
- sloj koji sinkronizira aplikacije na transportni sloj
- pruža pravila komunikacije između odredišnog računala i izvorišnog računala
- mreža - definira stazu (kako izvor tako i odredište) kojom će proći podatci
- sučelje između mrežnog softvera i fizičkog uređaja
- fizički uređaj

OSI i mrežne komponente

- L7 - aplikativni i L6 - prezentacijski:
 - konverteri protokola
- L5 - sjednički i L4 - transportni:
 - prilaz (gateway)
- L3 - mrežni:
 - usmjerivač
- L2 - podatkovni spoj:
 - preklopnici, mostovi
- L1 - fizički:
 - koncentratori, obnavljač

Usporedba DARPA-OSI

- DARPA
 - slaba/nikakva pouzdanost spoja
 - transportni sloj vrši detekciju grešaka i oporavak
 - oslanja se na IH u mrežnim protokolima, usmjeravanju i mrežnom upravljanju
- OSI
 - softver (protokol) detektira i rješava greške na svim nivoima
 - protokol garantira uspješni i točni prijenos
 - računala ne sudjeluju dodatno u mrežnim događanjima
 - nadležni ISP se bavi usmjeravanjem, upravljanjem, itd

Ethernet - kratko i još kraće

- mrežna tehnologija bazirana na okvirima (frame) za realizaciju LAN mreža
- definirano kabliranje i signali na fizičkom, te formati okvira i protokoli za pristup mediju (podatkovni spoj)
- najčešće u vidu 802.3: maksimalna dužina segmenta 500m, maksimalno računala 1024, najveći paket 1518 bajtova...
- jedna od najpoznatijih LAN realizacija (nekad TokenRing, FDDI, ARCNET)

Ethernet - još malo

- CSMA/CD
 - izbjegavanje kolizije random vremenima i eksponencijalnim povećanjem čekanja
- MAC adresa:
 - hardverska jedinstvena 48bitna adresa ugrađena u uređaj
 - MAC-48: 3 grupe po 4 heksadecimalne znamenke, razdijeljene znakom .
 - EUI-64: 6 grupa po 2 hex znamenke, odvojene sa znakom : ili znakom -

Dio II: Uvod u TCP/IP mreže



Internet protokol

- skup komunikacijskih protokola - pravila za slanje poruka i formate poruka
- implementiraju stog protokola (softverska implementacija) za Internet
- alternativno ime TCP/IP po dva najvažnija: Transmission Control Protocol i Internet Protocol
- ne mogu se svi dijelovi jednoznačno preslikati u OSI

Internet

- niz konvencija i fizičkih prospoja koji omogućavaju spajanje hardverski različitih mreža u koordiniran skup
- korisnici se spajaju iz svojih mreža u centralnu mrežu neovisno o tipu originalne mreže i komuniciraju međusobno
- protokoli su dokumentirani u RFC-ovima!
- danas je mreža vrlo narasla - granica su 32bitne adrese

Administracija Interneta

- RIR - Regional Internet Registry:
 - organizacija za registraciju/alokaciju IPv4, IPv6 adresa i AS brojeva
 - postoji po 1 za svaki dio svijeta
 - vršno IANA - Internet Assigned Numbers Authority - dodjeljuje /8 adrese RIRovima
 - ARIN - Sjeverna Amerika
 - RIPE - Europa
 - APNIC - Azija i Pacifik
 - LACNIC - Latinoamerika i Karibi

Internet protokoli

- 7 - aplikacijski nivo:
 - HTTP, SMTP, SNMP, FTP, Telnet, SSH, SCP, NFS, RTSP
- 6 - prezentacijski nivo:
 - XDR, ASN.1, SMB, AFP
- 5 - sjednički nivo:
 - TLS, SSH, RPC, NetBIOS, ASP
- 4 - transportni nivo:
 - TCP, UDP, RTP, SCTP, SPX, ATP

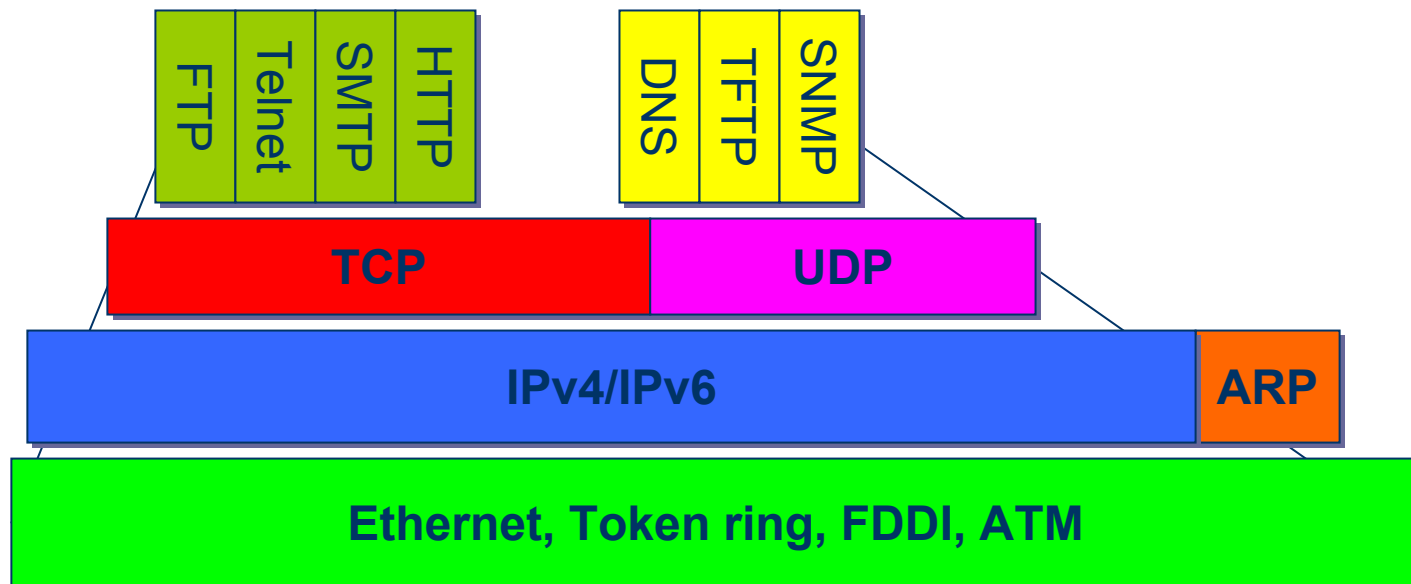
Internet protokoli (2)

- 3 - mrežni nivo:
 - IPv4, IPv6, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IPX, DDP
- 2 - podatkovni spoj:
 - Ethernet, Token ring, PPP, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI
- 1 - fizički spoj:
 - fizički mediji - struja, radio, laser
 - tehnike kodiranja
 - T1, E1

Internet protokoli - završno

- vršna tri sloja OSI modela (aplikativni, prezentacijski i sjednički) - smatraju se jedinstvenim aplikativnim nivoom (L7) u TCP/IP setu
- uglavnom nema jedinstvenog sjedničkog sloja - individualne aplikacije imaju dotičnu funkciju
- primjer L7: HTTP, FTP, DNS, ali i BGP i RIP koji mogu biti i L3

IP složenac u praksi



L3 protokoli - IPv4

- standardni i osnovni protokol na Internetu
- RFC 791
- 32-bitne adrese:
 - ograničeno na 4,294,967,296 adresa
 - dobar dio rezerviran za posebne namjene - multicast, lokalne mreže, itd
 - budućnost - očigledni manjak adresa
 - obično u točka-decimalnoj notaciji:
207.142.131.235

IPv4 adrese (1)

- originalno
 - samo su imale 8-bitni mrežni broj
 - prepoznavanje mreže po tom broju
 - ostatak davao adresu računala - samo 256 mreža
- host adrese sa svim 0 ili 1 su broadcast - poruke svim računalima u mreži istovremeno
- adrese sa 127. su lokalno računalo (loopback)
- klase - moguće prepoznati po prvom polju

IPv4 adrese (2)

- IPv4 adresa - sastoji se od mrežnog i host dijela

klasa	vodeći bitovi	mrežni dio	host dio
klasa A	0	7 (128)	24 (16,777,214)
klasa B	10	14 (16,384)	16 (65,535)
klasa C	110	21 (2,097,152)	8 (256)
klasa D (mcast)	111	-	-
klasa E (rezerv.)	-	-	-

IPv4 adrese (3)

tip	polje1	polje1	polje1	polje1
rezervirano	0			
klasa A	1-126	host dio		
rezervirano	127			
klasa B	128 - 191.254			
klasa C	192 - 223.254.254		host dio	
klasa D	224-239	mcast ID (28bit)		
rezervirano	240-255			

IPv4 adrese (4)

- rezervirane klase:
 - 0.0.0.0/8 - prazno, A klasa, 16M adresa
 - 10.0.0.0/8 - privatne, A, 16M
 - 127.0.0.0/8 - localhost, A, 16M
 - 169.254.0.0/16 - M\$ APIPA, B, 64k
 - 172.16.0.0/12 - privatne, B, 1M
 - 192.0.2.0/24 - dokumentacija i primjeri, C, 256
 - 192.88.99.0/24 - IPv6 prema IPv4, C, 256
 - 192.168.0.0/16 - privatne, C, 64k
 - 198.18.0.0/15 - mjerenje brzine, C, 128k
 - 224.0.0.0/4 - multicast, D, 256M
 - 240.0.0.0/4 - rezervirano, E, 256M

IPv4 subnetiranje

- dijeljenje mreže u manje podmreže
 - bolje performanse - manje broadcasta
 - sigurnije - lakše se izolira problem
- IPv4 tada ima 3 dijela:
 - mrežni dio, subnet dio i ostatak za računalo
- mrežna maska
 - maska bitova koja odvaja bitove mreže od bitova za samo računalo
 - subnet routing - svi prefiksi nisu usmjerljivi
 - CIDR: /32 (računalo), /24 (C), /16 (B), /8 (A)

CIDR

- Classless Inter-Domain Routing
- način na koji se IPv4 adrese interpretiraju
- efikasnije korištenje adresa, strožija hijerarhija, odbacivanje "klasa", agregacija prefiksa (jednostavnije usmjeravanje)
- koriste se VLSM (variable length subnet masks) da se alokira IP adresa po potrebi, a ne po općenitom mrežnom pravilu (fiksne dužine mrežnog dijela, npr.) - primjenjivo rekurzivno!

CIDR (2)

- RFC 1518, 1519
- novi sustav - usmjerivanje bez klasa (classless routing)
- spajanje usmjerivačkih prefiksa (routing prefix aggregation) - 16 slijednih /24 mreža se spajaju u jedinstvenu /20 rutu, od kojih se 2 slijedne mogu spajati u jednu /19, itd.
- notacija:
 - 192.168.0.0/24 - 256 adresa, 192.168.0.0-255
 - 192.168.0.0/22 - 1024 adresa, 192.168.0.0-3.255

L3 protokoli - IPv6

- nova generacija IP
- IPv4 = $4E+9$ adresa, IPv6 = $3.4E+38$ adresa
- NAT - djelomično rješenje, nije P2P
- ekstenzije - mobilnost, QoS, privatnost
- 128bit adrese: 64bit mrežni prefiks, 64bit host dio (od MAC adrese):
 - 4 grupe hex brojeva
 - npr. 2001:0db8:85a3:0000:1319:8a2e:0370:7344
 - ili 2001:0db8:85a3::1319:8a2e:0370:7344

IPv6 (2)

- moguće zapisati i IPv4 adresu u IPv6:
 - ::ffff:192.168.89.9
- specijalne adrese:
 - ::/128 - bilo koja adresa (sve!)
 - ::1/128 - loopback
 - ::/96 - IPv4 kompatibilna adresa
 - ::ffff/96 - IPv4 mapirana adresa
 - fe80::/10 - prefiks - samo u lokalnom fiz. stroju
 - fec0::/10 - prefiks - samo unutar organizacije
 - ff00::/8 - multicast prefiks

L3 protokoli - ARP

- Address Resolution Protocol - pronalaženje MAC (Ethernet) adrese iz IP adrese
- pošiljatelj broadcasta ARP paket koji sadrži IP adresu traženog računala i osluškuje odgovor sa MAC adresom (odgovara bilo dotično računalo bilo neko drugo - proxy ARP, ARP spoofing)
- svako računalo sadrži međuspremnik sa mehanizmima zastarijevanja
- za dobivanje MACa za nekoliko L3 protokola
- RFC 826

L4 protokoli - TCP

- konekcijski orijentiran, tokovski, orijentiran oko bajtova (8-bitni tok)
- RFC 793
- garantira uspješnost prijenosa i redosljed
- garantira razlikovanje odredišnih servisa
- IP pruža samo pakete, ali ne i pouzdane cjevovodne konekcije - transportni sloj!
- ovisno o MTU (Maximum Transmission Unit) se tok dijeli na segmente koji putuju kao IP

L4 protokoli - TCP (2)

- svaki bajt ima slijedni broj - osiguranje od gubitka i garancija ispravnog redoslijeda
- šalje se priznanica za primljene bajtove
- retransmisija ako se ne dobije priznanica u dogledno vrijeme
- bajtovi zaštićeni zaštitnom 16bit sumom
- tri faze stvaranja konekcije:
 - uspostava, prijenos i zatvaranje konekcije
- rukovanje u 3 smjera, zatvaranje u 4 smjera

L4 protokoli - TCP (3)

- TCP portovi:
 - brojevi za identifikaciju aplikacija koje primaju ili šalju
 - svaka strana ima 16bitni nepredznačeni broj
 - grupe: standardni, registrirani i dinamički/privatni
 - IANA: standardni = sistemski/root procesi (0-1023), registrirani - 1024 - 49151
 - datoteka **/etc/services**, npr.
- TCP - koristi ga 95% IP paketa, CPU intenzivan, loš za RT upotrebe i visokih latencija, zagušenje

L4 protokoli - UDP

- User Datagram Protocol
- programi šalju kratke poruke - datagrame
- nema pouzdanosti i garancije redoslijeda
- brži, efikasniji, jednostavniji, manje latencije
- RFC 768
- nema stanja poruke - jednostavna IP datagram nadogradnja sa multipleksiranjem aplikacije i zaštitnim sumama
- nema detekcije zagušenja i gubitka

L4 protokoli - ICMP

- Internet Control Message Protocol
- za slanje poruke o grešci - generira ga OS kao odgovor na greške u IP datagramima, te za dijagnostičke i usmjerivačke potrebe
- ne koriste ga mrežne aplikacije direktno (osim npr. ping i slično)
- RFC 792, 1122
- IPv6 verzija - ICMPv6

L4 protokoli - ICMP (2)

- stvaraju se u IP sloju, uglavnom od normalnog IP datagrama koji je uzrokovao grešku, a takav paket se enkapsulira sa novim IP zaglavljem i šalje nazad
- primjeri:
 - 0 - echo reply, 3 - destination unreachable, 4 - source quench, 5 - redirect message, 6 - alternate host address, 8 - echo request, 9 - router advertisement, 10 - router solicitation, 11 - time exceeded, 12 - parameter problem, 13 - timestamp, itd.

L7 protokoli - Telnet

- generalni, dvosmjerni, 8bitni komun. protokol
- klijent/server, tcp/23
- RFC 854, 855
- sigurnosni problemi:
 - zastarjelo, rupe
 - nema enkripcije, čisti tekst pa i za lozinke
 - nema autentifikacijske sheme, nema provjere integriteta paketa
- za debug ostalih TCP cleartext protokola

L7 protokoli - HTTP

- HyperText Transfer Protocol
- standardni način razmjena informacija na W3
- namjena je slanje i primanje HTML stranica
- RFC 2616 - HTTP/1.1
- zahtjev/odgovor (RR) protokol između klijenta i poslužitelja, tcp/80, nema stanja!
- riječi: GET, POST, PUT, DELETE, HEAD, TRACE, CONNECT
- serveri: Apache, Boa, Thttpd, Squid, IIS

L7 protokoli - SMTP

- Simple Mail Transfer Protocol
- standardni način razmjene e-mailova
- tekstualni protokol, tcp/80
- RFC 2821, 2822, 1869, 1891
- SMTP server za domenu - MX ili A zapis
- riječi: HELO, MAIL FROM, RCPT TO, DATA
- poslužitelji: Sendmail, Postfix, Qmail, Exim
- spamming problem...
- uzimanje pošte - protokoli POP3 ili IMAP

L7 protokoli - FTP

- File Transfer Protocol
- 8-bitni klijent/server protokol, visoke latencije
- tcp/20 (podatkovni) i tcp/21 (kontrolni)
- problem aktivni/pasivni, čisti tekst za kontrolni, zastarjeli dizajn
- riječi: user, bye, binary, cd, get, put, prompt...
- RFC 0959
- danas se koristi SFTP ili SCP
- poslužitelji: VsFTPd, ProFTPd, WuFTPd

L7 protokoli - SSH

- Secure Shell - i protokol i program
- zamjena za telnet, rlogin i rsh
- enkriptirana komunikacija, tuneliranje, prosljeđivanje X11 konekcija, itd
- protokoli - SSH1 i SSH2 (sigurniji, kvalitetniji)
- tcp/22
- poslužitelji: OpenSSH, SSH

L7 protokoli - SNMP

- Simple Network Management Protocol
- nadzor mrežnih i inih uređaja:
- hijerarhija:
 - glavni agenti - svaki čvor sa IP adresom parsira i formatira protokol
 - podagenti - ako ima više podsustava, glavni mu prenosi zahtjev na koji ovaj odgovara
 - nadzorne stanice - klijenti koji traže i spremaju informacije o stanju
- riječi GET, SET, TRAP

L7 protokoli - SNMP (2)

- tri verzije protokola: v1, v2 i v3
- udp/161 (agenti) i udp/162 (klijent, manager)
- SNMP v1: RFC 1065, 1066, 1067
- SNMP v2p: RFC 1441, 1452
- SNMP v2c: RFC 1901, 1908
- SNMP v2u: RFC 1909, 1910
- SNMP v3: RFC 3411, 3418
- koegzistencija: RFC 3584

L7 protokoli - LDAP

- Lightweight Directory Access Protocol
- jednostavniji (usporedi sa DAP) protokol za korištenje X.500 imeničkih direktorija
- LDAP direktorij - objekti u X.500, konformiraju se po shemama, stroga hijerarhijska struktura
- moguće držati raznolike podatke (DNS npr.)
- tcp/389, udp/389
- RFC 1777, 1778, 3377, 2307, itd.
- poslužitelji: OpenLDAP

L7 protokoli - DOMAIN

- Domain Name Protocol
- udp/53 (ili tcp/53, za veće pakete i XFR)
- hijerarhijski DNS sustav
 - distribuirano skladište informacija o simboličkim imenima računala i domena
 - povezivanje simbolička labela - IP adresa
 - povezivanje IP adresa - simbolička labela
- poslužitelji: Bind8, Bind9, DJBDNS

L7 protokol - DHCP

- klijent-server protokol
- DHCP poslužitelj daje informacije DHCP klijentima
 - podatke o IP mrežnim parametrima, alokaciju adrese, itd
- RFC 2131, 2136
- alokacija adresa:
 - manualna - kroz MAC adrese
 - automatska - prva slobodna se za stalno dodjeljuje klijentu
 - dinamička - automatska + ponovno iskorištenje

L7 protokol - DHCP (2)

- dinamičko dodjeljivanje:
 - raspon IP adresa
 - na svakom klijentu TCP/IP softver traži adresu (broadcast)
- DHCP server može pružati:
 - adrese DNS poslužitelja, DNS ime, IP adresu prilaza (gateway), broadcast adresu, maska pod mreže, vrijeme isticanja ARP spremnika, MTU za uređaj, NIS(+) poslužitelje, NIS(+) domenu, NTP poslužitelje, SMTP poslužitelje, TFTP poslužitelje, WINS poslužitelje

L7 protokol - DHCP (3)

- portovi:
 - 67/udp - za poslužitelj
 - 68/udp - za klijenta
- princip rada:
 - DISCOVER - klijent broadcasta (odredište 255.255.255.255) na lokalnoj fizičkoj mreži u potrazi za poslužiteljima
 - usmjerivač može i ne mora prosljeđivati DHCP pakete na druge podmreže

L7 protokol - DHCP (3)

- OFFER - poslužitelj iz konfiguracije i klijentove MAC adrese određuje IP adresu i nudi je klijentu
- REQUEST - klijent odabire konfiguraciju iz ponuđenih paketa i traži IP adresu
- ACKNOWLEDGE - klijent odobrava adresu i šalje broadcast odluke na lokalnoj podmreži; od klijenta se očekuje da se rekonfigurira u skladu sa dogovorom
- danas - vrlo prošireno, jednostavno korištenje, radi na mnogo OS-ova, moguće različite primjene

L7 protokol - NTP

- Network Time Protocol
- sinkronizacija sata računala ili uređaja kroz preklapane mreže sa nestalnim latencijama
- čisti UDP - udp/123
- NTPv4 - održava vrijeme unutar 10ms oscilacija kroz standardni Internet
- NTP servis - kako na poslužitelju tako i na klijentima, no moguće imati i periodičke klijente

L7 protokol - NTP (2)

- hijerarhijski sustav:
 - stratum 1 - direktno spojeni na GPS, radio uređaje, atomske satove, itd.
 - stratum 2 - spojeni na stratum 1
- RFC 1361, 1769 i 2030, 1305
- postoji (skupi!) hardver ali i standardni ntpd/xntpd softver
- osigurava točno vrijeme i na "lošim" sistemskim satovima - točni logovi!

Dio III: TCP/IP komunikacija



Socket

- **socket** (priključnica)
 - osnovna struktura, skup (IPaddr, protokol, port)
 - krajnja točka komunikacije između dva procesa
 - veže se na port (vrata) - datoteka **/etc/services** ima popis IANA dozvoljenih i registiranih portova
 - jedinstveno je adresirljiva je kroz mrežnu adresu (IP) i broj porta
 - predstavlja sučelje između same aplikacije i TCP/IP nivoa/protokola
 - danas se koriste BSD socketi

Socket komunikacija

- danas standard
- klijent/server model:
 - server - čeka na zahtjeve, pruža servis
 - klijent - traži servis
- staza komunikacije:
 - po 2 socketa po komunikaciji
 - klijentov IP + klijentski port
 - serverov IP + serverski port

Socket komunikacija (2)

- pojednostavljeno ostvarivanje ftp konekcije na ftpd poslužitelj kroz socket komunikaciju



- prikaz svih aktivnih konekcija - naredba **netstat**
- primjer: `netstat -a`

Paket

- fundamentalna jedinica informacije u svim modernim računalnim mrežama
- datagram - može i ne mora biti paket; samodovoljan, dovoljno informacija u zaglavlju da prolazi i dolazi kroz mrežu neovisno o ostalima
- zaglavlje paketa - informacije o izvorištu i odredištu, potencijalno i ruti
- podatkovni dio paketa - informacije koje šalje pošiljatelj (izvorište)

Usmjerivanje

- routing - osnovni L3 koncept
- načini pronalaženja staze gdje informacija (i možda paketi) mogu biti poslani
- automatsko usmjerivanje
 - autonomne mreže
 - pronalaženje najbolje staze, rješavanje blokiranja i ispada
- prosljeđivanje
 - prosljeđivanje logički adresiranih paketa iz podmreža prema cilju

TCP/IP usmjeravanje

- host, router, gateway
- direktno usmjeravanje:
 - prijenos paketa direktno od računala do drugog
 - obavlja se koristeći fizičku transmisiju
 - ARP do finalnog odredišta
 - 1. određivanje fizičke adrese iz IP adrese koristeći ARP spremnik
 - 2. enkapsulacija paketa u fizički okvir koristeći MAC adresu
 - 3. slanje okvira kroz hardversko sučelje

TCP/IP usmjeravanje (2)

- indirektno usmjeravanje:
 - prijenos paketa kroz mrežu koja nije lokalna računalo, kroz routere
 - ARP do idućeg računala
 - 1. enkapsulacija paketa u fizički okvir i slanje direktno nadređenom računalo iz tablice usmjeravanja
 - 2. usmjerivački softver uzima paket i usmjerivačke rutine određuju kamo dalje poslati
 - 3. paket se šalje kroz iduću fizičku mrežu

TCP/IP usmjeravanje (3)

- usmjerivač:
 - 1. paket stiže
 - 2. IP softver pronalazi odredišnu IP adresu
 - 3. vrši se usmjeravanje koristeći podudaranje u najvećem broju bitova sa tablicom usmjeravanja
- tablice usmjeravanja:
 - podaci o mrežama i računalima
 - mogu se ručno unositi, a mogu biti i automatski distribuirane...
 - odluka o usmjeravanju - ovisi o tablicama

Tablice usmjeravanja

odredišna adresa	adresa idućeg koraka
mreža1	direktna isporuka
mreža2	vrata1
mreža3	vrata2

- manipuliranje rutama:
 - servis **routerd** - dinamičko upravljanje i distribucija (danas se koristi Quagga - OSPF, BGP, RIP, RIPNG, OSPFv6)
 - naredba **route**

Naredba route

- naredba **route**:
 - naredbe:
 - add - dodavanje ruta
 - flush - brisanje svih ruta
 - delete - brisanje zadane rute
 - monitor - nadzor nad promjenama ruta
 - zastavice:
 - -n - ne radi DNS rezoluciju imena (samo numerika)
 - -v - dodatni detalji
 - -q - "tihi" rad

Naredba route (2)

- default route
 - standardna ruta koja se primjenjuje kad niti jedno drugo pravilo (pravilo podudaranja najviše bitova) ne odgovara
- moguće definirati rute za pojedina računala (npr. gateway)
- primjeri:
 - `route add default 128.32.0.120`
 - `route add -host mickey 128.32.0.120 - hopcount 2`
 - `route delete -host mickey 128.32.0.120`

Naredba route (3)

- primjeri:

- `route add -precedence 1 -host milan
128.32.0.130`
- `route change -oldgateway 128.32.0.130 -
oldinterface le0 -host milan
128.32.10.131`
- `route add -net 212.232.32/22
128.32.0.130`
- `route add -host 219.67.129.16
219.67.122.41 -dev tu1`
- `route delete -net 219.84.6 219.84.6.79 -
olddev fta0`

Mrežne konf. datoteke

- **/etc/hosts**

- lokalno popisana baza DNS - IPaddr
- uglavnom za slučajeve kad DNS ne radi
- format: IP FQDN alias

- **/etc/inetd.conf**

- konfiguracija inet servisa
- zastarjelo, danas se ne koristi
- konfigurira niz servisa koji ne osluškuju stalno
- format: servis tip protokol čekanje korisnik staza argumenti

Mrežne konf. datoteke (2)

- **/etc/networks**

- popis mreža i njihovih simboličkih imena
- olakšava administriranje
- npr. za naredbu route
- format: ime IPmreža alias

- **/etc/protocols**

- popisuje Internet protokole koje računalo/poslužitelj obično razumije
- format: ime broj standardninaziv

Mrežne konf. datoteke (3)

- **/etc/services**
 - popisuje IANA definirane i rezervirane portove za pojedine servise
 - format: servis port/protokol
- zastarjelo:
 - **/etc/hosts.equiv**,
 - **\$HOME/.rhosts**, itd.

Dio IV: Postavljanje TCP/IP mreže



Priprema

- 1. koji su mrežni uređaji u računalu
 - naredba **netstat** - mrežne informacije: po uređaju, izgubljeni paketi, memorija, adrese, tablice usmjeravanja, usmjerivačke statistike i statistike po uređaju, protokolu, itd.
 - primjer: `netstat -i`
- 2. FQDN računala - domena i simboličko ime
 - naredba **hostname**
 - pregled **/etc/hosts** datoteke

Priprema (2)

- 3. IP adresu računala i mrežnu masku
 - prikazuje naredba **ifconfig**: konfiguriranje mrežnih uređaja i parametara, prikaz, aliasi, NetRAIN, itd.
 - primjer: `ifconfig -a`
- 4. imena i IP adrese ostalih važnijih čvorova
 - datoteka **/etc/hosts**
 - datoteka **/etc/resolv.conf**
- 5. statičke rute na računalu
 - datoteka **/etc/routes**
 - naredba **route**

Postavljanje mreže

- naredba **netsetup**
 - više se ne koristi, postoji na starim sustavima
- naredba **sysman**
 - opće upravljanje sustavom - usporedi sa AIX Smit
 - smanjuje mogućnost greške, pojednostavljuje upravljanje, korisno za neiskusne sistemce
 - npr. sysman -menu
 - datoteke **/etc/rc.config*** - dodatno naredba **rcmgr**
- alternativno - ručno editiranje!
 - ifconfig, route i ostatak

Radni zadatak

- pronaći, isprobati i istražiti naredbe (man stranice):
 - ifconfig, route, sysman, netstat
- pronaći i pregledati konfiguracijske datoteke:
 - hosts, resolv.conf, rc.config, routes, networks, services, protocols, inetd.conf

Dio V: Korištenje TCP/IP mreže



Naredba ssh

- **ssh** - zamjenjuje nekadašnji rlogin
- pristup udaljenom računalu koje ima sshd
- sintaksa:
 - ssh [-l korisnik] poslužitelj [naredba]
 - ...
- mogućnosti:
 - redirekcija portova i tuneli, X11 prosljeđivanje, itd
 - udaljeno izvršavanje naredbi
 - prijenos datoteka (naredbe **scp** i **sftp**)

Naredba ssh (2)

- najvažniji parametri:
 - -l - korisnik
 - +X, -X, +x, -x - kontrola X11 tunela
 - +C, -C - kontrola kompresije
 - -v - više informacija tijekom spajana
 - -f - pozadinski način rada (neinteraktivno)
 - -L, -R - stvaranje tunela
 - -4, -6 - IPv4 i IPv6 način rada

Naredba ssh (3)

- kontrolni kodovi:
 - ~. - prekid konekcije
 - ~^Z - suspendiranje konekcije
 - ~~ - slanje znaka ~
- primjeri:
 - ssh -l kreator server1
 - ssh server1 ls -al
 - ssh +X +C kreator@server2 xemacs
 - ssh -f -L 9696:localhost:6667
posluzitelj

Naredba scp

- **scp** - dodatak na ssh, zamjena za rcp, prijenos datoteka
- sintaksa:
 - scp [korisnik@] poslužitelj datoteka ...
[[korisnik@] poslužitelj] datoteka-ili-direktorij
 - ...
- sigurno kopiranje - kroz tunel
- parametri:
 - -p - čuva dozvole, attribute, itd.
 - -d - odredište mora biti direktorij

Naredba scp (2)

- parametri:
 - -u - emulira način rada naredbe **mv**
 - -4, -6 - IPv4 i IPv6
 - -r - rekurzivno kopiranje
- primjeri:
 - scp lokalna_datoteka
korisnik@posluzitelj: /neki/direktorij
 - scp
korisnik@posluzitelj2: /direktorij/dat
oteka /direktorij/za/datoteku

Naredba telnet

- **telnet** - omogućava spajanje na telnet poslužitelje, debuggiranje mrežnih servisa
- sintaksa:
 - telnet [-dfx] [-l korisnik] [racunalo] [port]
- parametri:
 - -f, -x - enkripcija i autentifikacija za Kerberos
 - -l - šalje korisnika za varijablu \$USER
- dva moguća načina rada
 - komandni (naredbeni) i interaktivni (udaljeni rad)

Naredba telnet (2)

- u naredbeni moguće doći escape znakom ^] iz interaktivnog načina
- naredbeni način:
 - ? i help - pomoć
 - close - zatvori konekciju ali ne izlazi iz telneta
 - open - otvori konekciju prema računalu
 - quit - zatvara konekciju i izlazi
 - status - vraća status
- primjeri:
 - telnet localhost 25

Naredba ftp

- **ftp** - spajanje na udaljeni poslužitelj, izvršavanje naredbi, prijenos datoteka
- sintaksa:
 - ftp [-dginptvx] [racunalo]
- parametri:
 - -g - ne dozvoljava korištenje zamjenskih znakova
 - -i - isključuje interaktivni način rada
 - -n - onemogućava automatski login pri spajanju
 - -v - daje detaljne informacije o statusu, paketima...

Naredba ftp (2)

- naredbe:
 - ! - izvršava naredbu pod ljuškom
 - ? - daje pomoć
 - append - nadostavlja željenu datoteku na udaljenu datoteku
 - ascii - postavlja način prijenosa u 7-bit ASCII
 - binary - postavlja način prijenosa u 8-bit (npr. za binarne datoteke)
 - bye, quit - završetak rada
 - close - zatvara konekciju, ali ne izlazi iz klijenta

Naredba ftp (3)

- naredbe:
 - lcd - lokalna promjena direktorija
 - get - uzima udaljenu datoteku i sprema lokalno
 - put - uzima lokalnu datoteku i sprema udaljeno
 - mget - uzima nekoliko datoteka i sprema lokalno
 - mdelete - briše nekoliko datoteka...
 - mput - stavlja nekoliko datoteka..
 - open - otvara konekciju prema željenom računalu
 - prompt - omogućava i onemogućava interaktivni rad (ftp pita za svaku datoteku)

Naredba ftp (4)

- naredbe:
 - rename - preimenovanje datoteke
 - pwd - ispis trenutnog direktorija
 - cd - promjena direktorija udaljeno
 - user - identifikacija korisnika
- primjeri:
 - ftp localhost
 - get .. put.. delete..

Naredba sftp

- **sftp** - kvalitetnija zamjena za ftp, koristi ssh poslužitelj
- sintaksa:
 - sftp [korisnik@] racunalo [port]
- naredbe identične kao za ftp
- primjer:
 - sftp korisnik@posluzitelj
 - get.. put.. binary.. cd..

Naredba tftp

- **tftp** - pruža usluge TFTP servisa
- sintaksa:
 - tftp [poslužitelj] [port]
- minimalno okruženje, minimalne naredbe (usporedi sa **ftp**)
 - ascii, binary, connect, get, put, mode, quit, status
- obično iskoristivo za mrežnu opremu
- manjak autorizacije, sigurnosti, itd

Dodatak

- korisne GNU naredbe/programi:
 - curl, wget - http/ftp konzolski klijent za preuzimanje sadržaja
 - w3m, lynx, links - Web preglednici
 - netcat - kopiranje bez autorizacije
 - redir - redirekcija portova
 - lsof, fuser - pregled otvorenih datoteka, portova, itd

Radni zadatak

- pročitati manual stranice za
 - telnet, ssh, sftp, scp, ftp, tftp
- isprobati korištenje dotičnih naredbi u skladu sa naučenim parametrima i primjerima
- isprobati primjere iz Compaq/Digital literature

Dio VI: Korištenje TCP/IP alata



Naredba ping

- **ping** - popularni mrežni alat za detekciju mogućih problema, općenito mjerenje latencija i sl.
- šalje ICMP ECHO_REQUEST paket, čeka ICMP ECHO_RESPONSE od računala ili njegovog gw
- sintaksa:
 - ping [-cqv...] [-s velicina] [-i vrijeme] [-p uzorak] racunalo

Naredba ping (2)

- parametri:
 - -c - šalje željeni broj paketa
 - -i - čeka željeni broj sekundi prije slanja paketa
 - -q - ništa ne ispisuje osim rezultata
 - -s - šalje pakete željene veličine
 - -v - detaljni ispis
 - -p - šalje pakete sa određenim uzorkom
 - -f - brzinsko mjerenje (oprez!)
 - -r - zaobilazi tablice usmjeravanja

Naredba ping (3)

- prekida se sa ^C
- primjeri:
 - `ping 161.53.2.130`
 - `ping -p ff 127.0.0.1`
 - `ping -c 5 10.0.0.1`
- ne daje nužno ispravne rezultate!
- ICMP često zabranjen!
- današnje alternative:
 - TCP ping, UDP ping, bing

Naredba arp

- **arp** - prikazivanje ili modifikacije nad ARP tablicama
- sintaksa:
 - arp [-adf...] [-s] ime [...]
- parametri:
 - -a - prikazuje sve ARP unose
 - -d - briše unos za željeno računalo
 - -f - čita ARP unose iz datoteke i unosi u sustav
 - -g - šalje "nepotrebni" ARP paket

Naredba arp (2)

- parametri:
 - -n - prikazuje unose bez DNS rezolucije (korisno!)
 - -s - ručni unos ARP adrese (izbjegavati)
 - -i - ispis uređaja sa kojim se ARP unos povezuje
- primjeri:
 - `arp -a -n -i`
 - `arp pero`
 - `arp -s pero 08:00:2b:0f:44:24 temp`
 - `arp -f datoteka`

Naredba ifconfig

- **ifconfig** - konfiguracija i ispis mrežnih parametara
- uz **route** jedna od najvažnijih naredbi
- pri podizanju systemske skripte koriste ifconfig za postavljanje mrežnih parametara svakog uređaja (ln0, sl0, lo0, ics0, ee0, itd.)
- sintaksa:
 - ifconfig uređaj [adresna_obitelj] [adresa[/maska] [odredisna_adresa]] [parametri]

Naredba ifconfig (2)

- argumenti:
 - uređaj - fizički uređaj, moguće vidjeti sa netstat -i
 - adresna obitelj - protokol, npr. inet, inet6
 - adresa - nova adresa
- dodatni argumenti:
 - -a - ispisuje podatke o svim uređajima
 - -d - ... samo o ugašenim uređajima
 - -l - ... samo o konfiguriranim uređajima
 - -u - ... samo o uređajima koji su aktivni
 - -v - ispisuje dodatne informacije o uređajima

Naredba ifconfig (3)

- mijenjanjem adrese:
 - ne ostaje pohranjena stara vrijednost
 - nova je privremena do podizanja sustava
 - treba restartati sve mrežne servise - jer oni imaju staru adresu!
- parametri:
 - add - stvara, modificira set NetRAIN adaptera
 - alias - aliasiranje uređaja
 - arp - omogućava korištenje ARP (standardno)
 - broadcast - postavlja broadcast adresu

Naredba ifconfig (4)

- delete - miče adresu
- down - proglašava uređaj neaktivnim
- filter - omogućava filtriranje na razini jezgre (datoteka **/etc/ifaccess.conf**)
- metric - postavlja metriku (routing daemoni) za uređaj
- netmask - postavlja mrežnu masku
- promisc - stavlja mrežnu karticu u promiscuous način rada
- up - proglašava uređaj aktivnim
- abort - prekida sve TCP konekcije

Naredba ifconfig (5)

- primjeri:

- `ifconfig ee0`
- `ifconfig lo0 inet 127.0.0.1 up arp`
- `ifconfig ee0 161.53.2.1/22`
- `ifconfig sl0 down delete abort`
- `ifconfig nr1 add ee0,ee1`
- `ifconfig nr1 inet 161.53.116.8`
- `ifconfig nr1 remove ee0`
- `ifconfig nr1 remove`
- `ifconfig ee0 alias 161.53.2.2/24`

Naredba netstat

- **netstat** - prikazuje sve mrežne informacije: o uređajima, sustavu, konekcijama, itd
- iznimno važna naredba!
- sintaksa:
 - netstat [parametri] [-f adresna obitelj] [-p protokol] [interval]
 - ... kompliciranija sintaksa, vidjeti man stranice ...
- parametri:
 - -a - ispisuje stanja socketa

Naredba netstat (2)

- parametri:
 - -f - adresne obitelji: inet, inet6, unix, all, any
 - -g - statistike od podizanja sustava do trenutnog vremena
 - -H - ARP tablica, imitira **arp** naredbu (arp -a)
 - -i - stanja trenutno konfiguriranih uređaja, MAC adrese, itd.
 - -l - informacije o željenom uređaju
 - -M - ispisuje multicast usmjerivačke informacije
 - -n - ispisuje informacije čisto numerički

Naredba netstat (3)

- parametri:
 - -p - statistike po traženom protokolu (datoteka **/etc/protocols**)
 - -r - tablice usmjerivanja (kao naredba **route**)
 - -s - statistike za tablicu usmjerivanja
 - -d - ispisuje broj ispuštenih/odbačenih paketa, nužno je specificirati i uređaj
- izlazne informacije:
 - Iface, MTU, addr, Ipkts, Ierrs, Opkts, Oerrs, col, drop, timer

Naredba netstat (4)

- oznake ruta:
 - c - klonirana ruta
 - C - klonirana ruta kroz **route** naredbu
 - D - dinamički generirana kroz redirekciju
 - f - fragmentiranje nije dozvoljeno
 - G - ruta prema gatewayu
 - H - ruta prema računalu
 - I - ruta sa informacijama o spojnom sloju
 - L - povratna ruta (loopback)
 - m - mobilni IPv6

Naredba netstat (5)

- oznake ruta:
 - -M - modificirana od redirekcije
 - -p - stalna ruta, ne može se modificirati
 - -R - ruta za odbacivanje paketa
 - -U - aktivna ruta
- primjeri:
 - netstat -i
 - netstat -rn
 - netstat -a

Naredba rcmgr

- **rcmgr** - služi konfiguriranju mrežnih varijabli
- datoteke **/etc/rc.config**,
/etc/rc.config.common i **/etc/rc.config.site**
- konfiguriranje sustava pri dizanju
- obično ih koriste **/sbin/init.d** skripte (SystemV
i BSD style init razlike)
- mreža se može konfigurirati kroz ručne
naredbe (ne ostaje zapamćeno), **sysman** ili
rcmgr

Naredba rcmgr (2)

- korištenje.
 - set variabla vrijednost - u datoteke i u memoriju
 - get varijabla - traži iz datoteka
 - mget variabla* - dobavlja grupu parametara
 - delete varijabla - briše varijable
- parametri (za cluster):
 - -c - radi grupne promjene (**rc.config.common**)
 - -s - radi grupne promjene (**rc.config.site**)
 - -h - radi lokalne promjene (poštuje hijerarhiju)
 - -n - radi lokalne promjene

Naredba rcmgr (3)

- samostalni sustav:
 - **rc.config** i **rc.config.common**
- cluster:
 - **rc.config.common** - među svim računalima
 - **rc.config** - za svako računalo posebno
 - **rc.config.site** - grupno, nestandardno
- redosljed pretraživanja:
 - **rc.config, rc.config.common, rc.config.site**

Naredba rcmgr (4)

- varijable:
 - HOSTNAME
 - IFCONFIG_0
 - MAX_NETDEVS
 - itd.
- primjeri:
 - `rcmgr mget | more`
 - `rcmgr get NUM_NETCONFIG`
 - `rcmgr set IFCONFIG_0 161.53.2.130
netmask 255.255.255.0`

Dodatni korisni programi

- nisu nužno dio standardne Tru64 distribucije:
 - konzolski:
 - tcpdump
 - lsof
 - iptraf
 - traceroute
 - tracepath
 - grafički:
 - darkstat
 - ntop

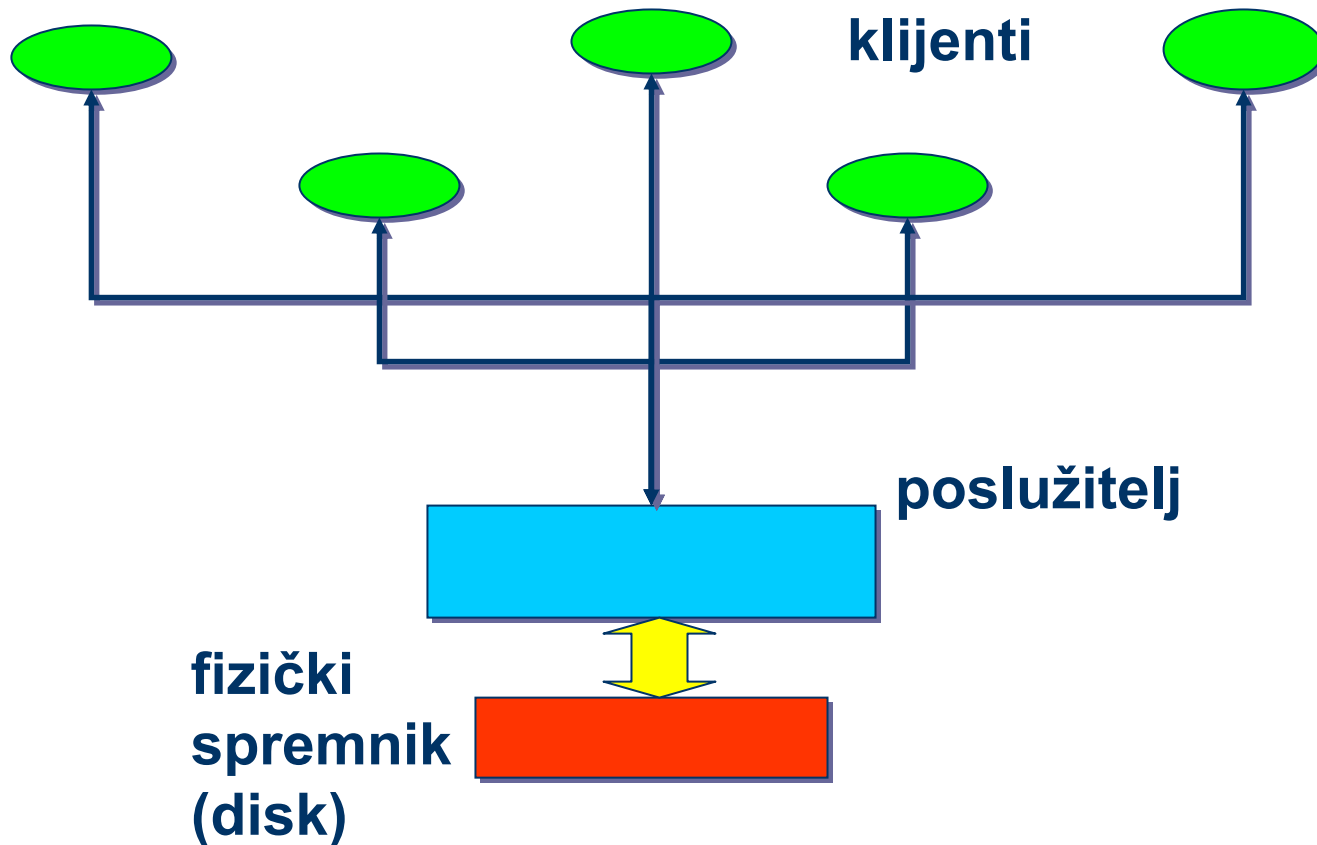
Radni zadatak

- pročitati manual stranice za naredbe:
 - arp, ping, ifconfig, route, rcmgr, netstat
- isprobati primjere sa slajdova i iz manual stranica
- saznati na poslužitelju aktualne mrežne parametre, provjeriti servise i ARP spremnik, saznati rc varijable i njihove vrijednosti

Dio VII: NFS



Prikaz



Uvod

- razvio Sun Microsystems 1984
- RFC 1094, 1813, 3010, 3530
- mrežni datotečni sustav - pristupanje i korištenje datoteka preko mreže na jednostavan i transparentan način
- protokoli:
 - v2 - isključivo UDP, bez stanja, zaključavanje nije u protokolu
 - v3 - koristi i TCP (neke implementacije NFSv2 isto), podrška za veće datoteke

Uvod (2)

- v4 - ubrzanja, inspiriran AFS (oko Kerberosa, ćelije, itd.), sigurnost, protokol sa stanjima
- Microsoft ekvivalent - SMB (Server Message Block)
- omogućava rad sa heterogenim mrežama i operacijskim sustavima
- komponente:
 - semantika za udaljeno montiranje (mount)
 - RPC
 - zastarjelo - podrška za XDR, NIS, itd.

Uvod (3)

- prednosti:
 - transparentni pristup, dozvole i sl. vrijede
 - samo jedna centralna kopija
- mane:
 - sporost - neupotrebljiv preko sporih linkova
 - zaključavanje - nužno koristiti loši flock()
 - keširanje - potencijalno dovodi do zastarjelih podataka i desinkronizacije; performanse pate kod vrlo visokog iskorištenja
 - sigurnost!

Uvod (4)

- karakteristike:
 - nema stanja - robusnost, kod ispada klijent ili poslužitelj nema stanja koja treba održavati
 - Unix fs semantika, ali je moguća i jednostavnija
 - ACL i zaštita - prati Unix semantiku: UID i set grupa; provjere se dešavaju na sustavu ispod, a ne na korisniku NFS usluga
 - dizajn protokola - transportno nezavisan (migracija UDP - TCP)

Princip rada

- klijent-server model
- server - klijentima pruža pristup datotekama, ima lokalni dat. sustav i fizički pristup
- klijenti - računala, koriste datotečni sustav kroz mrežu, imaju ga lokalno mountanog
- korisnici - koriste ga na klijentskim računalima
- RPC - protokol za udaljeno izvršavanje funkcija sa drugog računala, u argumentima su podatci a rezultat se vraća kao poruka

NFS komponente

- datoteke:
 - **exports** - udaljene točke za NFS zahtjeve
 - **fstab** - popis datotečnih sustava i particija gdje se nalaze (npr. nfs)
- naredbe:
 - **mount, umount** - montiranje i odmontiranje datotečnog sustava na lokalnom poslužitelju
 - **showmount** - omogućava pregled koji klijenti drže koje datotečne sustave (komunicira sa mountd)

NFS komponente (2)

- naredbe:
 - **sysman nfs** - mijenja zastarjeli nfssetup, interaktivno konfiguriranje klijenta ili poslužitelja i pripadnih servisa
 - **nfsstat** - NFS statistike
 - **rpcinfo** - provjerava RPC poslužitelj
- inicijalno pokretanje:
 - automatski (rc NFS_SERVING)
 - skripta **/sbin/init.d/nfs**

NFS komponente (3)

- servisi:
 - portmap - glavni RPC servis koji RPC brojeve konvertira u IP portove; lokalni RPC servisi mu prijavljuju mu koje brojeve i portove koriste
 - mountd - servis za posluživanje udaljenih NFS mount zahtjeva; čita exports datoteku; vodi računa koji klijent koristi koje sustave
 - nfsd - servis koji odgovara na sve datotečne zahtjeve; može ih biti više aktivnih - automatski se balansiraju
 - nfsiod - asinkroni I/O servis čita unaprijed i vrši zakašnjelo pisanje po blokovima; moguće ih je nekoliko imati aktivnima, automatsko balansiranje

NFS komponente (4)

- server:
 - portmap, mountd, nfs
 - exports datoteka
 - prima zahtjev za udaljenim montiranjem
- klijent:
 - portmap, nfsiod
 - fstab datoteka
 - šalje zahtjev za udaljenim montiranjem

Postavljanje - NFS poslužitelj

- moguće:
 - grafički, konzolski kroz menije - **sysman**
 - ručno - editiranjem **exports** i postavljanjem **rc.config** datoteke kroz **rcmgr**
- 1. postavljanje **/etc/exports**:
 - po jedna linija za svaki datotečni sustav/direktorij koji će se posluživati:
`/lokalni/direktorij klient1`
`/novi/direktorij -ro klient2`

Postavljanje - NFS poslužitelj (2)

- 2. postaviti nužne rc varijable kroz **rcmgr**:
 - omogućiti NFS:
`rcmgr set NFSSERVING 1`
 - broj nfsd servisa:
`rcmgr set NUM_NFSD 8`
 - dozvoliti ne-root korisnicima mountanje sustava:
`rcmgr set NONROOTMOUNTS 0`
 - koristiti li PC-NFS servis (DOS, OS/2, Macintosh):
`rcmgr set PCNFSD 0`
 - koristiti li NFS servis za zaključavanje:
`rcmgr set NFSLOCKING 0`

Postavljanje - NFS poslužitelj (3)

- 3. osigurati se da su DNS imena svih klijenata u DNS bazi ili u **/etc/hosts**:
 - `161.53.2.130 jagor.srce.hr jagor`
- 4. ugasiti ikakve postojeće NFS servise:
 - `/sbin/init.d/nfs stop`
- 5. pokrenuti servis:
 - `/sbin/init.d/nfs start`
- 6. provjeriti ima li NFS procesa
 - `ps xuaw | grep -i nfs`

Postavljanje - NFS klijent

- vrijede opaske kao i za poslužitelj
- 1. postavljanje /etc/fstab:
 - po jedna linija za svaki udaljeni datotečni sustav:
poslužitelj:/dir /lokal/dir nfs
rw,bg,nosuid 0 0
/dir@poslužitelj2 /lokal/dir2 nfs
ro,fg 0 0
- 2. naprave se odgovarajući lokalni direktoriji:
 - `mkdir -p /lokalni/dir ...`

Postavljanje - NFS klijent (2)

- 3. nužni zapisi u **/etc/hosts** ili DNS:
 - 161.53.2.1 server.srce.hr server
- 4. postavke se odgovarajuće rc varijable kroz **rcmgr**:
 - rcmgr set NUM_NFSIOD 7
 - rcmgr set NFSLOCKING 0
- 5. startaju se servisi:
 - /sbin/init.d/nfs stop;
 - /sbin/init.d/nfs start

NFS zaključavanje

- zaključavanje - nužno u radu servisa radi sinkronizacije i izbjegavanja race događaja
- lockf(), fcntl() i flock() će raditi kroz NFS ako postoje NFS servisi za zaključavanje
- moguće zaključati:
 - cijelu datoteku
 - dio datoteke
- standardno NFS zaključavanje nije omogućeno - samo lokalno zaključavanje

NFS zaključavanje (2)

- servisi:
 - rpc.lockd - obrađuje zahtjeve za zaključavanjem, bilo lokalne od jezgre sustava bilo udaljene od drugog istog servisa
 - rpc.statd - nadzor statusa udaljenih zaključanih datoteka
- omogućeno zaključavanje:
 - `rcmgr set NFSLOCKING 1`
- automatski se oslobađaju zaključane datoteke u slučaju pada - svakih 15 sec

Montiranje datotečnog sustava

- **mount** - vrijedi za sve datotečne sustave
- datotečni sustavi na poslužitelju se moraju montirati da bi se mogli koristiti - to se dešava automatski pri podizanju sustava!
- montiranje - asociranje postojećeg datotečnog sustava sa direktorijem; uključivanje sustava u postojeću hijerarhiju
- sintaksa:

```
- mount -t nfs serv:/dir /lokal/dir
```

```
- mount -t nfs dir@serv /lokal/dir
```

Montiranje datotečnog sustava (2)

- parametri:
 - -a - montira sve sustave iz **fstab**
 - -t - tip datotečnog sustava - advfs, nfs, ufs, mfs, cdfs, dvdfs, pcfs, sysv, procfs, dfs, efs, fdfs, ffm
 - -o - opcije pri montiranju sustava, ovisi o tipu
- parametri za NFS montiranje:
 - važniji: rw, ro, suid, nosuid, exec, noexec, dev, nodev, bg, fg
 - sekundarni: intr, nintr, hard, soft, retrans=n, timeo=n, rsize=n, wsize=n, retry=n

Provjera/ispis montiranih sustava

- **mount** - bez argumenata prikazuje sustave
- **df** - zauzeća po blokovima po sustavu
- parametri za **df**:
 - -e - ispis svih mogućih sustava
 - -h - ljudski ispis u MB, GB, KB i sl
 - -i - broj slobodnih inodeova
 - -k - ispis u KB
- primjeri:
 - `mount ; df -k`

Demontiranje datotečnog sustava

- **umount** - demontira jedan ili više sustava
- primjedba: moguće je demontirati sustav samo ako na njemu nema aktivnih datoteka ili procesa - za pronalaženje istih služi **fuser**
- parametri:
 - -a - demontiraj sve moguće sustave
- primjeri:
 - `umount -a`
 - `umount /neki/direktorij`

Dodatne informacije

- **fuser** - prikazuje aktivne procese na datotečnom sustavu
- parametri:
 - -c - tretira datoteku kao da je montirana, traži sve otvorene datoteke u tom sustavu
 - -v - detaljniji ispis sa korisnicima
 - -k - šalje SIGKILL procesima na tom sustavu
- primjer:
 - `fuser -v /neki/direktorij`
 - `fuser -k /neki/direktorij`

Uvoz i izvoz datotečnih sustava

- automatsko montiranje datotečnog sustava pri podizanju sustava - **/etc/fstab**
- pažljivo sa korištenjem! ako NFS poslužitelj ne radi, a u **fstab** je NFS, nema bootanja - uvijek i obavezno koristiti parametar **bg**!
- primjer uvoza:
 - /dev/rz0a / ufs rw 1 1
 - /proc /proc procfs rw 0 0
 - /dev/rz0b swap1 ufs sw 0 2
 - /usr/users@nfsusers /usr/nfsusers nfs
rw,bg,intr 0 0

Uvoz i izvoz datotečnih sustava (2)

- primjer izvoza - **exports**:
 - `/usr/project solder farmer`
 - `/usr/share/man -ro`
 - `/usr/field -r=0 farmer`
- moguće eksportirati:
 - `ufs, cdafs, advfs`
- ne može se eksportirati:
 - `nfs!, mem, proc`
- simbolički linkovi - rade lokalno, ne udaljeno!

Uvoz i izvoz datotečnih sustava (3)

- isplati se izvoziti:
 - /usr/share/man - manje mjesta se troši
 - /usr/src - izvorni kod, centralna nadogradnja
 - /usr/sys - centralno mjesto za kernel
 - /usr/local - centralizirani lokalni alati
- izbjegavati:
 - /etc - nužne su lokalne konfiguracije
 - /sbin - nužni osnovni alati, nikako
 - /dev - udaljeni uređaji, nije podržano
 - /usr/spool, /tmp - privremene lokalne datoteke

Sigurnost

- NFS
 - dizajniran za okoline koje su sigurne
 - inherentno se vjeruje računalima u NFS mreži
- problem:
 - lažni NFS pristup - lako lažirati, UDP promet
 - udaljeni administrator - lokalni administrator prema NFS datotečnom sustavu

Sigurnost - rješenja

- zabrana pristupa administratoru:
 - izbjegavati `-r=0` osim kad je nužno: vjeruje se računalu, postoje root servisi koji moraju pisati
 - aktivirati NFS provjere da li zahtjevi dolaze sa udaljene jezgre, a ne lažnog klijenta
- automatsko provjeravanje:
 - `/etc/nfsportmon on`
- "cum grano salis":
 - minimalni exporti, samo čitanje, precizna kontrola strojeva

Rješavanje NFS problema

- nema pristupa:
 - **exports** na serveru, **fstab** na klijentu
- ne radi poslužitelj:
 - nužni procesi: portmap, mountd, nfsd
- ne radi klijent:
 - nužni procesi: portmap, nfsiod
- pristup spor:
 - povećati broj asinkronih servisa na klijentu:
NUM_NFSIOD 7
 - ili broj servisa na poslužitelju: NUM_NFSD 8

Rješavanje NFS problema (2)

- datotečni sustav montiran sa:
 - hard - datotečni sustav i aplikacije na njemu se smrzavaju dok se poslužitelj ne vrati
 - soft - datotečni sustav se demontira, a aplikacije prekidaju u slučaju pada poslužitelja
- provjeriti ima li RPC servisa/programa, odnosno UDP ili TCP varijanti:
 - `rpcinfo -p poslužitelj`
 - `rpcinfo -u poslužitelj`
 - `rpcinfo -t poslužitelj`

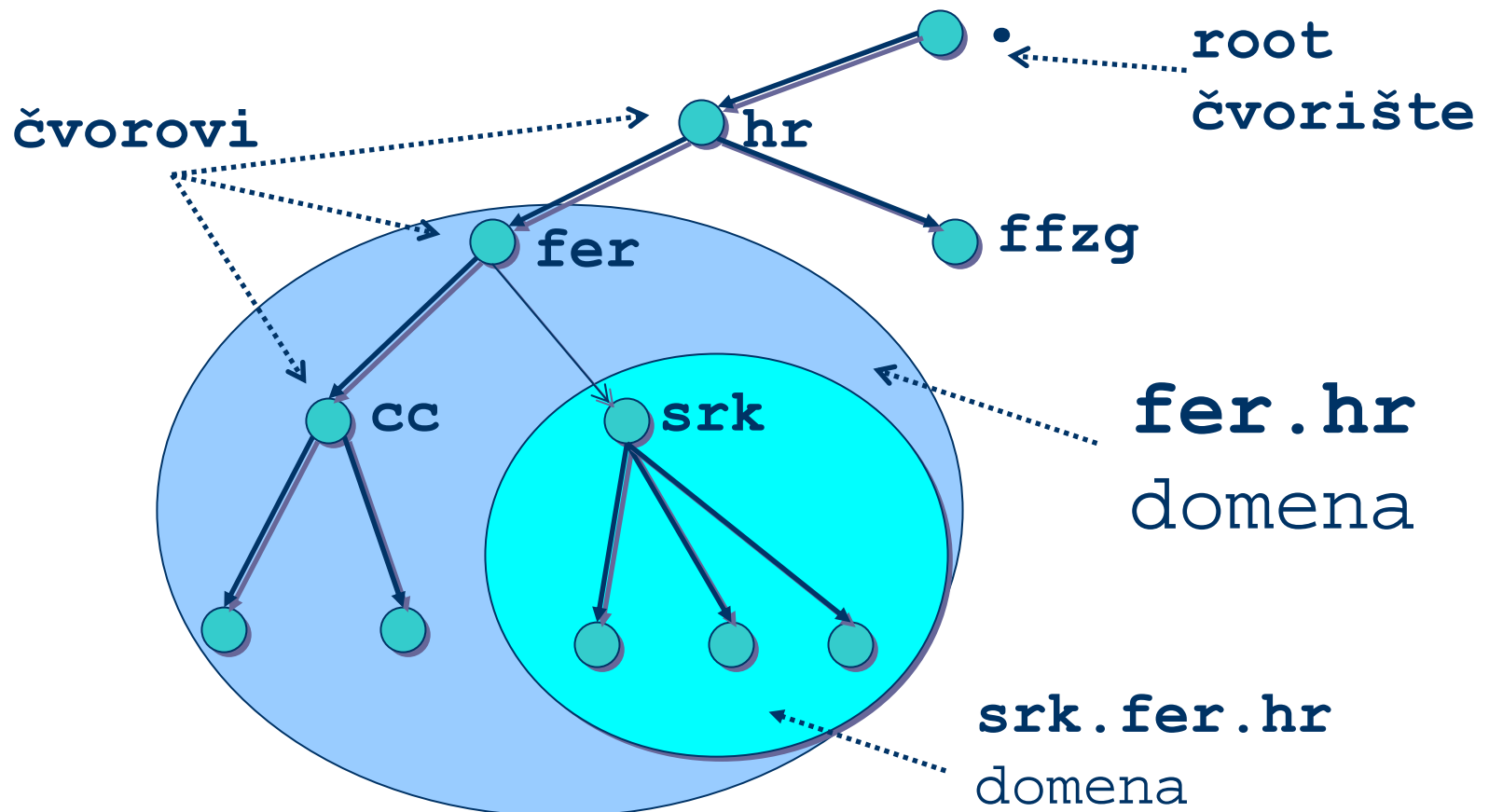
Rješavanje NFS problema (3)

- ima li mnogo Ethernet kolizija?
 - primjer: `netstat -i`
- ima li mnogo izgubljenih UDP paketa?
 - primjer: `netstat -s`
- naredba **nfsstat**:
 - parametri
 - -c - klijentove NFS i RPC statistike
 - -s - poslužiteljeve NFS i RPC statistike
 - -n - statistike i za klijent i za server

Dio VIII: DNS i NTP



Domenski prostor



DNS - opća teorija

- stroga hijerarhija sa glavnim čvorom ("") = .
- **distribuirana** indeksirana (po imenu) baza
- dužina imena (labela) - maks. 63 znaka
- FQDN = kompletno ime sa svim **labelama**, apsolutno prema glavnom čvoru
- u **istom** prostoru **nema dvije iste** labela
- domena = podstablo cjelokupnog stabla, ime domene je ime glavnog (najvišeg = TLD) čvora u toj domeni

DNS - opća teorija (2)

- podaci o domenama - nalaze se u RR
- klase RR: Hesiod, **Internet**, Chaosnet
- TLD: com, edu, gov, mil, net, org, int, arpa + ISO 3166.* domene (2-slovni zapis zemlje)
- delegacija = čvorovi/DNS poslužitelji odgovorni za dotičnu zonu (pružanje informacija) (fer.hr domena → labs3.cc.fer.hr poslužitelj)
- nameserver = autoritativan za domenu (1+)

DNS - opća teorija (3)

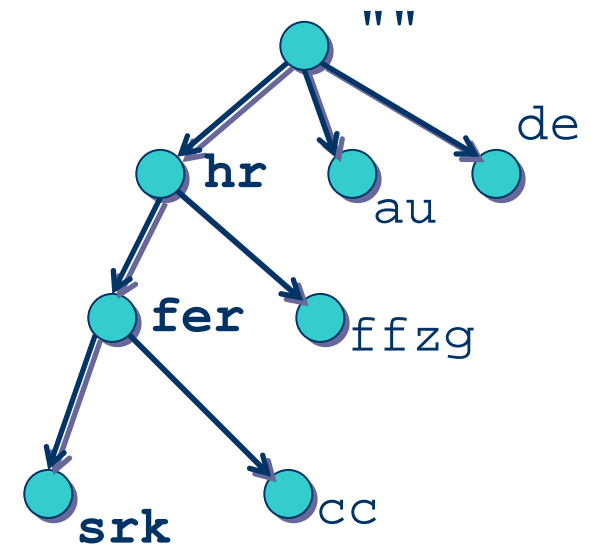
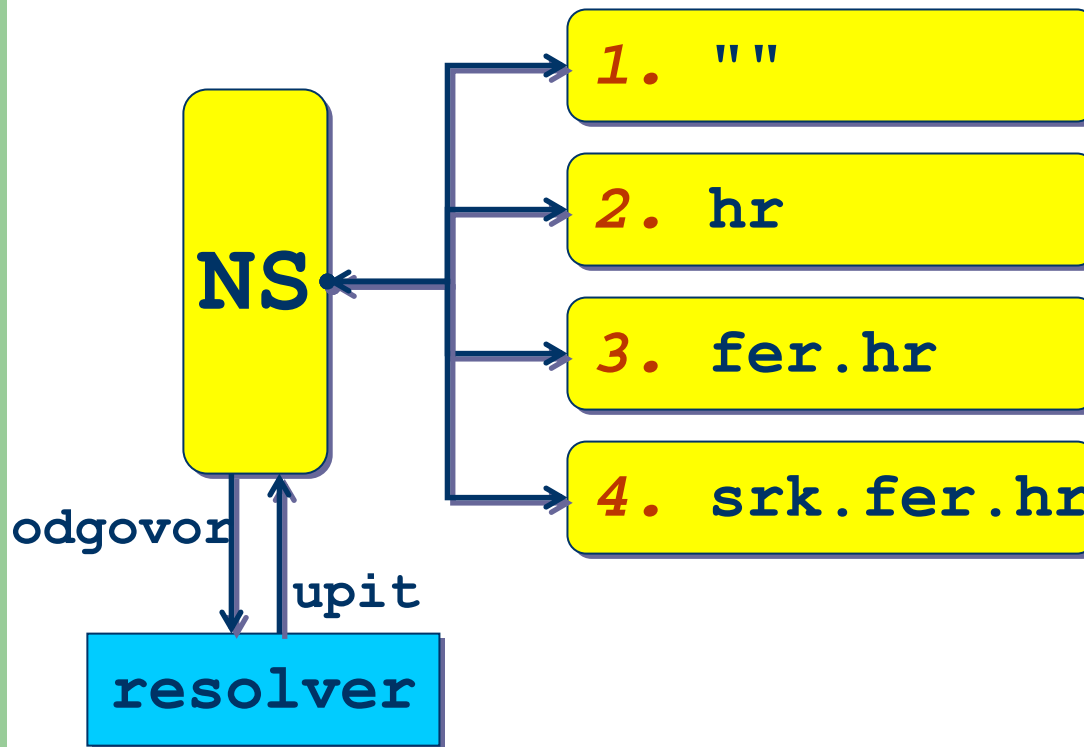
- P: zašto zona umjesto domene?
O: zona = samo relevantne informacije za dotični NS u toj domeni
- tipovi DNS poslužitelja:
 - primarni - zone čita iz lokalnih datoteka
 - sekundarni - kupi zone sa primarnih
 - cache - kupi sve podatke iz autoritativnih NS i drži u memoriji do isteka TTL
 - forwarder - samo prosljeđuje upite dalje
- nužno: **1 primarni i 1 sekundarni po zoni!**^{str. 147}

DNS - opća teorija (4)

- resolver = klijent koji pristupa NS:
 - libc rutine (gethostbyname() ili gethostbyaddr())
 - adns biblioteka
 - dns helper proces (Netscape itd.)
 - /etc/nsswitch.conf i /etc/resolv.conf (*)
 - nscd, /etc/hosts
- name resolution = proces dobivanja podataka od NS
 - ponešto jednostavniji kod cacheiranja podataka!

Proces rezolucije

traži se: fly.srk.fer.hr



DNS - opća teorija (5)

- vrste upita:
 - rekurzivni - rekurzivni upiti, želimo dozvoliti lokalnim klijentima, ali ne i stranim
 - iterativni - NS pogleda i odgovori najbliže što zna
- mapiranje adrese imenima (unazadno):
 - koristi se in-addr.arpa domena
 - 32bitni broj (točkasti zapis) + in-addr.arpa
 - inverzni upiti (inverse query)
 - nema prosljeđivanja

Konfiguriranje poslužitelja

- osnovna konfiguracija DNS procesa:
 - nekada named.boot - danas **named.conf**
 - niz ključnih riječi, počesto vrlo složeno određivanje
 - potrebno navesti **zone** i master/slave opciju
 - kod slave poslužitelja potrebno je navesti tko je master
 - **master** mora imati čitljive navedene zone
 - **slave** ne treba imati pripremljene zone, one će ionako biti obrisane nakon uspješnog prijenosa

Osnovni DNS zapisi

- SOA (start of authority):

```
srk.fer.hr. IN SOA fly.srk.fer.hr.  
  postmaster.fly.srk.fer.hr. (200201071  
  28800 7200 604800 86400 )
```

- serijski broj + vrijeme osvježavanja + vrijeme za ponovni upit + vrijeme trajanja zone + minimalni TTL
- server dokazuje da je autoritativan
- obično su vrijednosti dobro postavljene
- **serijski broj** - važan zbog odluke o retransferu

Osnovni DNS zapisi (2)

- NS (nameserver):

 - poslužitelji za zadanu domenu + SOA!

```
srk.fer.hr. IN NS fly.srk.fer.hr.
```

```
srk.fer.hr. IN NS burek.srk.fer.hr.
```

- A (address):

```
fly.srk.fer.hr. IN A 161.53.70.130
```

```
burek.srk.fer.hr. IN A 161.53.70.132
```

- PTR (pointer):

```
130 IN PTR fly.srk.fer.hr.
```

Osnovni DNS zapisi (3)

- CNAME (canonical name):
 - alias za stvarno ime hosta
 - postoje restrikcije na upotrebu

```
www CNAME fly
```
- MX (mail exchanger):
 - ne smije biti CNAME
 - može biti i za zone i za pojedine hostove
 - pažljivo koristiti!
 - ```
srk.fer.hr. IN MX 5 fly.srk.fer.hr.
```

# Korisne DNS naredbe

- naredbe:
  - **host** - ručno pregledavanje DNS zapisa, korisno i moderno
  - **nslookup** - zastarjelo, na većini Unixoida
  - **dig** - korisno za stvaranje zona, izlazne datoteke u ispravnom formatu
  - **dnswalk** - provjera ispravnosti DNS zapisa za proizvoljnu zonu (radi XFR), detaljni i napredan alat

# NTP servis

- konfiguracijska datoteka - **ntp.conf**
- primjer:
  - peer nesto.negdje
  - server zg1.ntp.carnet.hr
  - server zg2.ntp.carnet.hr
- servis - xntpd
- nadzor - naredbe **ntpq**, **xntpd**
- točno vrijeme u logovima!

**Kraj i diskusija**

