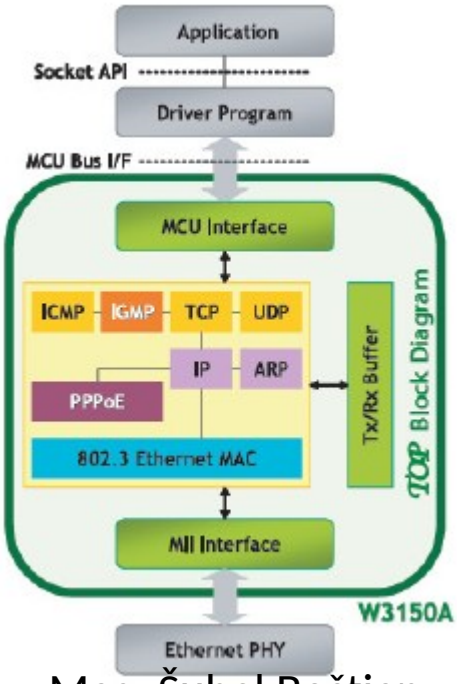
Srednja šola

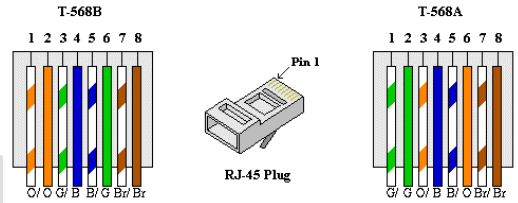
Izobraževalni program:

SSI TEHNIK MEHATRONIKE

Predmet:

INO Industrijska omrežja





Laško 2025

Mag. Šuhel Boštjan

Kazalo

Kazalo vsebine

RAČUNALNIŠKE KOMUNIKACIJE IN OMREŽJA I 10

ZGODOVINA 10

Naprava z napravo *10*

Vzporedna komunikacija 10

Zaporedna komunikacija 10

RS-232 10

RS-485 11

Oddaljene naprave med seboj *11*

Dolga linija 11

Kratka linija , lebdeč potencial in dvojne zvite linije 12

Predožičeni Ethernet moduli 12

UVOD V OMREŽNO POVEZOVANJE 13

Osnovni pojmi pri komunikacijah *13*

Vrste omrežij *13*

Po velikosti lahko razdelimo omrežja na : 13

Glede na organizacijo omrežja razdelimo na: 13

Glede na dolžino sumacijske točke omrežja razdelimo na: 14

Javna in privatna omrežja *14*

REFERENČNA MODELA ISO OSI IN TCP/IP 14

De facto in de iure pristop standardizaciji *14*

Povezovalni in nepovezovalni protokoli *15*

ISO OSI model *15*

TCP/IP model in razlike glede na ISO OSI *19*

Primerjava 19

Nabor protokolov 20

TEHNOLOŠKE OSNOVE KOMUNIKACIJE 21

Prenosni sistem, ki omogoča fizičen prenos podatkov po različnih prenosnih medijih *21*
Različne vrste prenosnih medijev *21*
Sukana parica 21
Optika 21
Radiofrekvenčno 21
Fizikalne lastnosti in omejitve fizičnega omrežja *21*
Sukana parica 21
Optika 22
Radiofrekvenčno 22
Električna instalacija 22
Razlika med digitalnim in analognim prenosom podatkov *22*
LOKALNA RAČUNALNIŠKA OMREŽJA 22
Lokalna računalniška omrežja *22*
Ojačevalniki 23
Preklopniki 23
Delovanje lokalnih računalniških omrežij *23*
Hrbtenica računalniškega omrežja *23*
Različne topologije omrežij, njihove lastnosti in področja uporabe *23*
Lastnosti aktivnih elementov in pasivnih elementov hrbtenice *23*
Izbra ustreznega elementa glede na zahteve *24*
Praktična izvedba lokalnega računalniškega omrežja *24*
Značilnosti Etherneta *24*
Napake, ki se pojavljajo v omrežju *25*
OMREŽNA IN TRANSPORTNA PLAST 26
Lastnosti omrežne in transportne plasti *26*
Ethernet telegram 26
Wireless telegram 26
FDDI telegram 27
Različne vrste usmerjanja in usmerjevalni algoritmi *28*
Principi 28
Usmerjanje po najkrajši poti 28
Usmerjanje po več poteh 28

Centralizirano usmerjanje ... 28
Izolirano usmerjanje ... 28
Usmerjanje v Internetu RIP ... 28
Usmerjanje v Internetu OSPF ... 29
Usmerjanje v Internetu BGP ... 29
Vzroki za zasičenje in mehanizmi za preprečevanje zasičenja ... 30
IP protokol in naslavljanje ... 30
Pomen podomrežij ... 30
Protokoli ... 31
TCP ... 31
UDP ... 31
ICMP ... 31
IGMP ... 31
ARHITEKTURA ODJEMALEC-STREŽNIK ... 31
Arhitektura odjemalec -strežnik ... 31
Povezovalna komunikacija s pomočjo TCP protokola ... 31
Nepovezovalna komunikacija s pomočjo UDP protokola ... 31
VARNOST UPORABNIŠKIH STORITEV ... 32
Pomen varnosti uporabniških storitev ... 32
Tehnike kodiranja podatkov ... 32
Pomen digitalnih potrdil ... 33
Elektronski podpis ... 33
Preverjanje pristnosti dokumenta ... 35
Postopek pošiljanja elektronsko podpisanega šifriranega dokumenta ... 36
OSNOVNE INFORMACIJSKE STORITVE ... 37
Standardne informacijske storitve ... 37
Spletna pošta ... 37
Spletne strani ... 37
Razpršeni strežniki ... 37
Imenski sistem in njegove značilnosti ... 38
FAT ... 39
NTFS ... 39

Vloga programske opreme pri uporabi računalniških omrežij 40
STORITVE INTERNETA 40
Zgodovino interneta in standardne storitve, ki jih internet ponuja svojim uporabnikom 40
Različni načine dostopi do internet 42
Pasovna prepustnost 42
Plačevanje storitev 42
Tehnologijo priklopa 42
Pomena interneta za sedanjo družbo 43
Socialni 43
Ekonomski 43
Izobraževalni 43
Zabava 43
Denarni 44
Delo 44
Racionalizacija 44
Partnerstvo 44
RAČUNALNIŠKE KOMUNIKACIJE IN OMREŽJA II 45
DELOVANJE INTERNETA 45
IP usmerjanje in IP usmerjevalni algoritmi 45
Privatni IP naslovi 45
ICMP protokol in njegove osnovne aplikacije 46
Echo Request And Reply Message Format 46
Reports Of Unreachable Destinations 46
Source Quench Format 47
Route Change Request From Routers 47
Detecting Circular Or Excessively Long Routes 47
Reporting Other Problems 47
Clock Synchronization And Transit Time Estimation 48
Obtaining A Subnet Mask 48
IGMP(Internet Multicasting) protokol in njegove osnovne aplikacije 49
Delovanje ARP in RARP protokola 50
ARP 50

Delovanje protokolov TCP in UDP.....50
UDP(User Datagram Protocol).....50
TCP(Transmission Control Protokol).....52
Sodobno zagotavljanje kvalitete storitve (QoS).....58
Protokol NAT.....58
BOOTP protocol.....59
Delovanje DHCP protokola.....60
Vloga, pomen in delovanje DNS protokola.....61
Delovanje standardnih protokolov aplikacijske plasti (http, ftp, smtp, ...).....61
POŽARNI ZID IN NAVIDEZNA PRIVATNA OMREŽJA (VPN).....61
Tipi vdorov in povzročena škoda.....61
Računalniški virusi.....61
Črvi.....61
Trojanski konji.....62
Programske bombe.....62
Hrošči.....62
Naloge požarnega zidu.....63
Princip navideznih privatnih omrežij in načini njihove izvedbe.....63
Arhitektura IPSec.....64
Načini zviševanja stopnje varnosti prenosov podatkov (IKE, SSL, ...).....65
USKLAJEVANJE FIZIČNE URE.....67
Potreba po usklajevanju ure na računalnikih.....67
Zakaj usklajevanje časa?2.....67
NTP protocol.....67
Kako deluje.....67
Hierarhija NTP strežnikov.....68
Format NTP paketov.....68
Načini usklajevanja8.....69
NAMEŠČANJE IN KONFIGURIRANJE STREŽNIŠKE PROGRAMSKE OPREME.....70
Glavni servisi komunikacijskih strežnikov.....70
Načini konfiguracij in parametri.....70
Spletnega strežnika.....70

FTP strežnika,..... 70
INDUSTRIJSKE MREŽE ZA PRENOS PODATKOV..... 70
Posebnosti, ki so značilne za industrijska omrežja,..... 70
Topologije industrijskih omrežij za prenos podatkov,..... 71
Seznanitev z značilnostmi industrijskega Etherneta..... 72
Prednost..... 72
Slabosti..... 72
Primerjava IPv4 - IPv6..... 74
Naslovi..... 74
Ipv4..... 74
Ipv6..... 74
Skupni naslovi..... 75
Unicast..... 75
Multicast..... 75
Anycast..... 75
Čelo..... 75
Razširitvena čela..... 75
Čelo opcij etap(Hop-by-Hop options header)..... 76
Čelo usmerjanja(Routing header)..... 77
Fragmentacijsko čelo(Fragmentation header)..... 79
Ugotavljanje avtentičnosti(Authentication header)..... 80
Enkripcijsko čelo(Encryption security payload header)..... 80
Čelo z opcijami cilja(Destination options)..... 82
Realno časovni mikrosekundni protocol z vgrajenim ethernetom..... 83
Problem..... 83
Rešitev problema..... 83
µ sekundni realnočasovni protokol z vgrajeni ethernetom..... 84
10Gbaud asinhroni prenos..... 84
100Gbaud asinhroni prenos..... 84
Osnovni 1µS cikel..... 84
RTM/ETH podatkovno področje..... 84
Lokalna RTM10(100)/ETH10(100) mreža..... 85

Meritev linijske zakasnitve *87*
Meritev neaktivnosti oddajne linije *87*
Porazdeljena sinhronizacija *88*
Oblike telegramov *88*
RTM10 telegram 89
RTM100 telegram 90
ETH10 telegram 90
ETH100 telegram 91
DTM telegram 92
RTM/ETH - ON telegram 93
RTM/ETH - OFF telegram 93
Protokol *94*
Meritev linijske zakasnitve 94
Določitev številke postaje N 95
Vklop kraka mreže na sublimacijsko točko 95
µ sekunda *96*
AD podatkovni tok 96
RTMADT 96
DMAADRTM 96
DMARTMAD 97
RTMPS 97
Povzetek *97*
O delu 97
Ugotovitve 98
Raspberry OS 99
Ifconfig *99*
Traceroute *100*
Arp *100*
Route *101*
Ping *102*
Sftp *102*
Wireshark 103

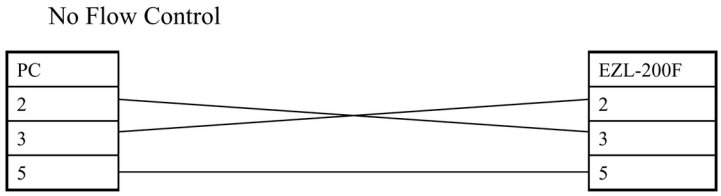
Izbira mrežne naprave *103*
Zajemanje telegramov *104*
Filtriranje *105*
Sestavljeni filtri *106*
LITERATURA 108

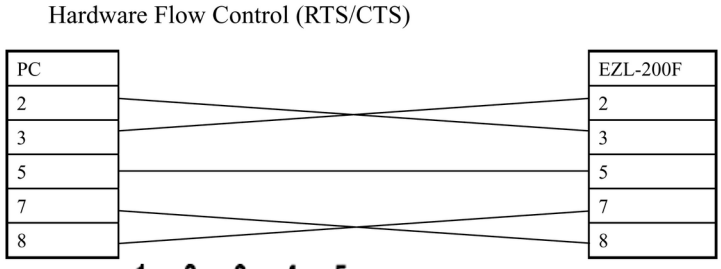
RAČUNALNIŠKE KOMUNIKACIJE IN OMREŽJA I

ZGODOVINA

Naprava z napravo

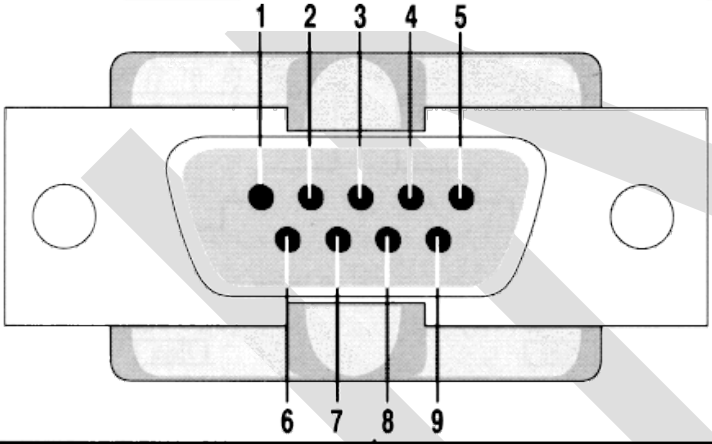
Po začetnem navdušenju nad prvimi računalniki se je hitro pojavila potreba po izmenjavi podatkov med računalniki.





Vzporedna komunikacija

V prvih računalnikih je bila širina podatkovnega vodila 8 bitov. 1 byte je še danes osnovna enota za podatek. Prvi poskusi komuniciranja so bili vzporedni. Vzporedna komunikacija rabi toliko vzporednih linij, kolikor je širina prenašane beside. Ker je bil to byte so poskusi tekli v smeri vzporedne komunikacije z 8 linijami. Kmalu se je pokazalo, da je veliko lažje peljati eno podatkovno linijo in podatke v oddajniku in sprejemniku predelati v zaporedni tok podatkov.



Pin	Signal	Pin	Signal
1	Data Carrier Detect	6	Data Set Ready
2	Received Data	7	Request to Send
3	Transmitted Data	8	Clear to Send
4	Data Terminal Ready	9	Ring Indicator
5	Signal Ground		

Zaporedna komunikacija

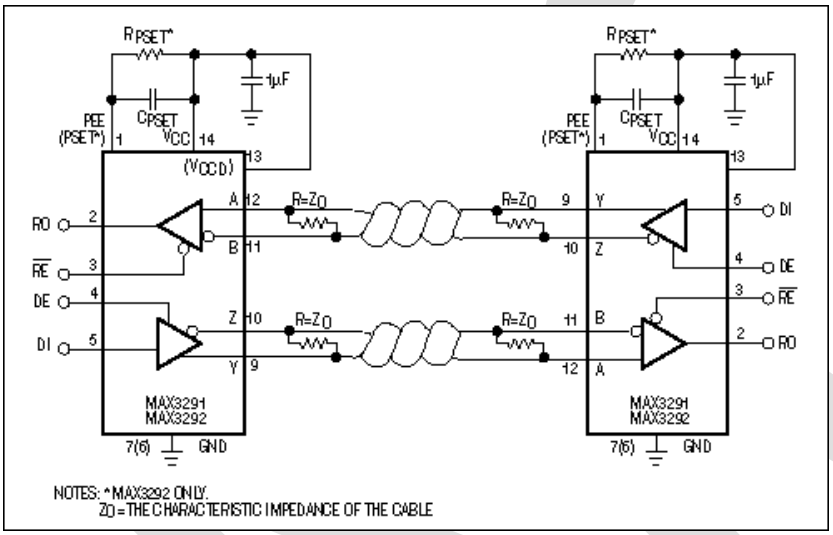
Zaporedna komunikacija rabi samo eno podatkovno linijo, ker se podatki ene besede(byta) pretvorijo v zaporedni tok bitov. Na oddajni strain imamo vzporedno v serijsko pretvornik. Na sprejemni strain imamo serijsko v vzporedno pretvornik. Vsaka naprava ima en oddajnik in en sprejemnik serijskih podatkov.

RS-232

Standard RS-232 je bil razvit za povezavo dveh naprav. Standardna prenosna hitrost je bila 9600baud(9600 bitov na sekundo). Pred ukinitvijo uporabe so hitrosti že dosegale 1Mbaud. Glavna pomankljivost standard je bila standardna komunikacijska napetost +-10V. Komuniciranje preko enosmernega napetostnega nivoja vezanega na zemljo je bil recept za

motnje. Ker so bili različni računalniki preko komunikacije povezani na isto maso, so različne motnje hitro zmotile predviden tok komuniciranja. Signalne linije so namreč tanke in imajo realno in imaginarno upornost. Še večji problem je nastal, ko smo hoteli medsebojno povezati več računalnikov. Tipične razdalje za RS-232 komunikacije so bile do 15m. RS-232 je oddajal byte po byte. Ko je npr. Računalnik oddajal en byte je imel računalnik, pri hitrosti 9600baud, cca 1ms časa, da je med oddajanjem byta pripravil naslednji byte. Če mu to ni uspelo se je oddajanje prekinilo, dokler ni računalnik poslal naslednega byta.

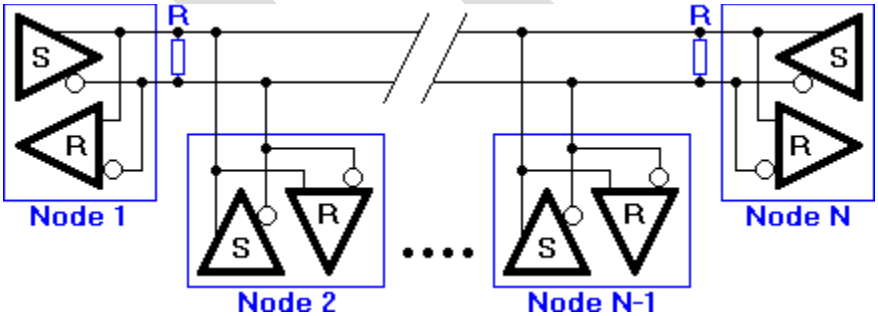
RS-485



Uvedba lebdečega potenciala in zvite žice je bistveno zmanjšala občutljivost na motnje , povečala prenosno hitrost in razdaljo komuniciranja. Za povezavo dveh naprav rabimo dve dvojni liniji. V standardnem struktoriranem ožičenju RJ-45 imamo na voljo 4 dvojne zvite linije.

Oddaljene naprave med seboj

Dolga linija



RS-485 standard omogoča vezavo, kjer povežemo vse oddajnike in sprejemnike na eno linijo. Pri dolgih linijah naletimo na omejitev svetlobne hitrosti, ki je samo 300m na 1µs. Temu pojavu rečemo tudi valovodni pojav. Vsi protokoli, ki poskušajo komunicirati preko dolgih linij, morajo predvidet pavzo med telegrami vsaj tolikokrat po 1µs, kolikokrat po 300m imamo dolgo linijo. Ta problem ni opazen pri nizkih hitrostih komunikacije. Pri velikih hitrostih pa je teoretična omejitev, ki je nikakor ne moremo odpraviti. Prve računalniške mreže temelječe na opletenem kablu so trčile ravno na to oviro.

Kratka linija , lebdeč potencial in dvojne zvite linije

Današnje hitre komunikacije temeljijo na lebdečem potencialu in dvojni zviti liniji. Ideja pa je da vse naprave povežemo skupaj v napravi, kjer vse priključke povežemo med seboj na kratki liniji znotraj naprave.

Tako delujejo vse mreže danes. Vedno imamo serijski RX-sprejem in serijsko TX-oddajo. Za serijsko oddajanje in sprejemanje signala uporabljamo danes tudi optiko, radiofrekvenčno tehnologijo in razne modeme.

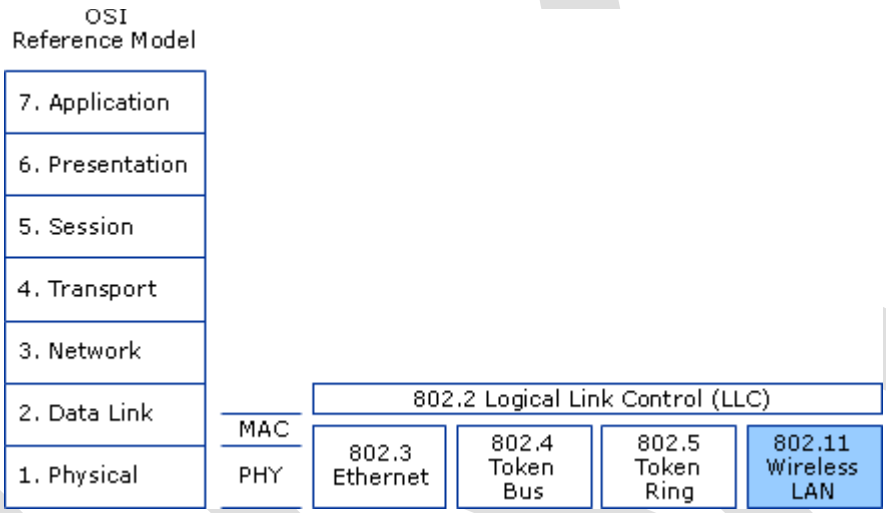
Predožičeni Ethernet moduli

Pri komuniciranju se je pojavila še težava hitrega obdelovanja prenašanih podatkov. Hitro je postalo jasno, da so procesorji prepočasni za obdelavo podatkob byte po byte, kakor so to še zmogli pri počasnih RS-232 povezavah. Pri hitrostih komuniciranja npr 100Mbaud, bi računalnik moral obdelati podatek prej kakor v 0.1µS. Težavo smo rešili z uporabon Ethernet integriranih vezij, ki samodejno oddajajo in sprejmejo njim namenjen telegram dolžine do 1500bytov. Pri danes standardni hitrosti 1Gbaud mora računalnik obdelati telegram na cca 2µs, kar ni lahko tudi za moderne zelo hitre procesorje.

UVOD V OMREŽNO POVEZOVANJE

Osnovni pojmi pri komunikacijah

Informacijska omrežja delimo glede na komunikacijski medij na povezana(Connection oriented) in nepovezana(Packet Switched - Connectionless). Tipičen predstavnik povezanega komunikacijskega medija so bile stare analogne telefonske central, ki so vspostavile nepostedno žično povezavo med telefonoma.
Nepovezana omrežja komunicirajo paketno. Komunikacijska omrežja so danes vsa serijska, kjer se podatki prenašajo serijsko, bit po bit in tvorijo oktete(ali byte).
Danes uporabljane tehnologije za izvedbo lokalnih računalniških mrež opisuje skupina standardov IEEE802.



Vrste omrežij

Po velikosti lahko razdelimo omrežja na :

lokalno omrežje - Local Area Network (LAN)
svetovno omrežje - Wide area network (WAN)
globalno omrežje - Global area network (GAN)

Glede na organizacijo omrežja razdelimo na:

omrežje enak z enakim (slika) - peer to peer (P2P)
omrežje klient/strežnik (client/server, kjer imamo lahko
datotečni strežnik (file server)

tiskalniški strežnik (print server)
aplikacijski strežnik (aplication server)
poštni strežnik (email server)

Glede na dolžino sumacijske točke omrežja razdelimo na:

Preklopna(switch) – Sumacijska točka je kratka znotraj naprave. Vsaka naprava ima do preklopnika svoj oddajno/sprejemni čip. Značilne so male zakasnitve omrežja(pod 1ms). Naprave komunicirajo brez omejitve. Oddaja lahko več naprav naenkrat. Vse več medijev uporablja preklopni način komuniciranja(5G mobilno omrežje je zadnja tehnologija, ki je začela uporabljati preklopnik.
Ojačevalna(hab) – Sumacijska točka je dolga(lahko več kilometrov). Vsaka naprava ima svoj oddajno/sprejemni čip, vendar lahko oddaja naenkrat samo ena. Značilne so velike zakasnitve telegramov (tipično več kot 10mS). Tipični mediji WiFi, kabelski internet.

Javna in privatna omrežja

Javno omrežje povezuje globalno z unique naslovi(Vsaka naprava ima svoj naslov, ki se ne ponovi nikjer drugje) Primer je telefonsko ali internetno omrežje.

Privatno omrežje povezuje naprave znotraj omejenega teritorija. Vsaka naprava znotraj privatnega omrežja ima unique naslov. Privatna omrežja se lahko gradijo z uporabo javnega omrežja ali neodvisno od javnega omrežja.

REFERENČNA MODELA ISO OSI IN TCP/IP

De facto in de iure pristop standardizaciji

Glede na to, da govorimo o obdelavi podatkov, potrebujemo bolj natančen odgovor. Skoraj vsi računalniški programi na nek način obdelujejo podatke. To pomeni, da programi sprejemajo podatke kot vhod, jih obdelajo in tvorijo izhodne podatke. Pomislimo na orodja za pisarniško poslovanje: Oblikovalnik besedil, preglednica, priprava predstavitev, oblikovanje hipertekstnih gradiv. Prav v vseh teh in podobnih primerih najbrž želimo, da to, kar smo ustvarili, shranimo na disk za kasnejšo obdelavo. Morda pa jih posredujemo komu drugemu. Ta jih bo moral s svojim programom prebrati in morda spet obdelati.

Ali morata imeti oba uporabnika povsem enak program? Kaj pa, če imata različen operacijski sistem?

Odgovor leži v dogovorjenih oziroma ustaljenih formatih zapisov datotek. Tako lahko dokumente, ki smo jih napisali s programom »Writer« in shranili kot datoteke tipa *.doc, razume tudi popularani Word. (ni pa to vedno nujno).

Podobni »de facto« standardi veljajo tudi za druge programe, in ne le na področju pisarniškega poslovanja, pač pa tudi računalniškega načrtovanja, programiranja ipd. Poglejmo kakšen program in hitro lahko ugotovimo, da ima verjetno pri shranjevanju podatkov možnost »shrani kot:«, kjer lahko izberemo primeren format.

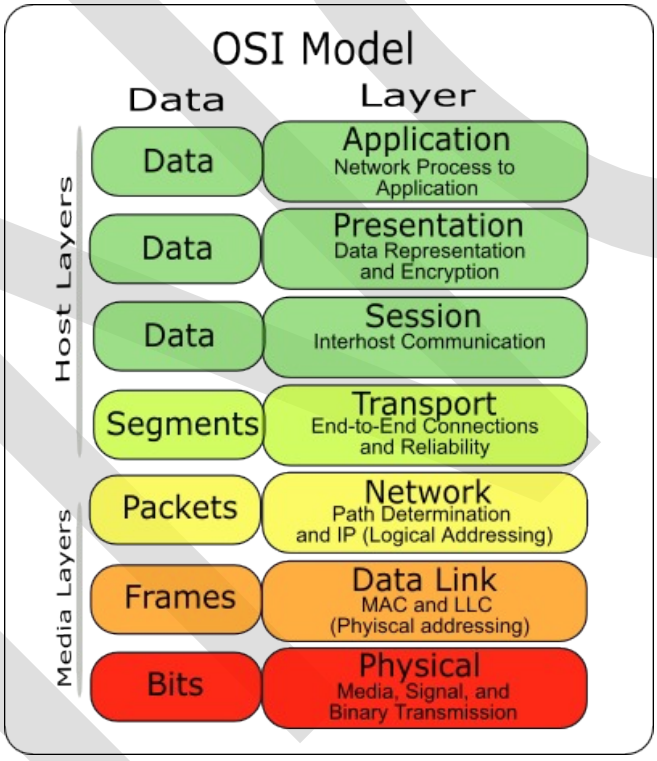
Povezovalni in nepovezovalni protokoli

Povezovalni protokoli vzpostavijo povezavo med dvema točkama. Mehanizmi povezave zagotavljajo pravilni prenoos podatkov med točkama. Povezovalni protocol najprej zahteva povezavo. Druga točka nam odgovori in vspostavi povezavo. Uporabniški program uporablja preverjene podatke, protocol pa poskrbi za pravilni prenos podatkov. Tipičen primer je TCP telegram

Nepovezovalni protokoli samo pošljejo podatek k drugi točki. Kaj se zgodi s tem podatkom je potem stvar programa. Tipičen primer je UDP telegram

ISO OSI model

Referenčni model ISO/OSI je sestavljen iz sedmih plasti. Na vsaki plasti so določene posamezne omrežne funkcije. Model je bil razvit leta 1984 in velja za osnovni arhitekturni model za komunikacijo med računalniki. Model OSI je sistematičen in konceptualno zasnovan, vendar je le referenčni model, ki v celoti ni nikoli zaživel



Aplikacijska plast:
Vmesnik med uporabnikom in OSI modelom. Tu so definirani protokoli za elektronsko pošto, svetovnega spleta, prenašanje datotek, časovni protokol. Odgovoren je za prepoznavo sogovornika in sinhronizacije komunikacije.

Aplikacijska plast je vmesnik med uporabnikom in komunikacijskim omrežjem. Določa protokole, ki omočajo elektronsko pošto, izdelavo predstavitvenih strani, prenašanje datotek in podobno. Skladno z razvojem OSI modela so se razvijale tudi aplikacije OSI, ki pa se niso širše uveljavile. Primeri: File Transfer, Access and Management (FTAM), Virtual Terminal Protocol (VTP).

Predstavitvena plast:

Zagotavlja različne načine kodiranja in sisteme pretvorb za aplikacijsko plast. Pretvarja podatke, poslane po omrežju, iz ene v drugo obliko, določa sintakso, transformacijo in formiranje podatkov.
Predstavitvena plast skrbi za uskladitev različnih načinov predstavitve podatkov:
kompresijo in dekompresijo podatkov (kodiranje ali zamenjava pogostih funkcij ali besed z zelo kratko kodo, z namenom povečanja učinkovitosti prenosa);
nabor znakov in kod (ASCII, EBCDIC),
šifriranje podatkov za potrebe zaščite podatkov, ki so v ta namen ob prenosu kodirani, da jih lahko razume le uporabnik, kateremu je sporočilo namenjeno,
podatkovne formate, ki omogočajo uporabo standardnih predstavitvenih, zvočnih in video formatov za potrebe uporabe aplikacij na različnih računalniških sistemih.

Sejna plast:

Nadzira komunikacijo med računalniki. Vzpostavlja ter prekinja komunikacijo med lokalnim in oddaljenim računalnikom. Določa vrsto komunikacij (enosmerno, dvosmerno).
Sejna plast določa:
vzpostavitev, vzdrževanje in prekinitev seje, to je komunikacije med končnimi računalniki;
vrste komunikacije:
enosmerna (simplex): na eni strani je postaja, ki oddaja sporočilo, na drugi strani pa ena ali več postaj, ki sporočilo sprejemajo;
izmenično dvosmerno (half duplex): postaja lahko sprejema in oddaja podatke, vendar jih lahko istočasno samo oddaja ali samo sprejema
dvosmerno (full duplex): postaja lahko istočasno sprejema in oddaja podatke.

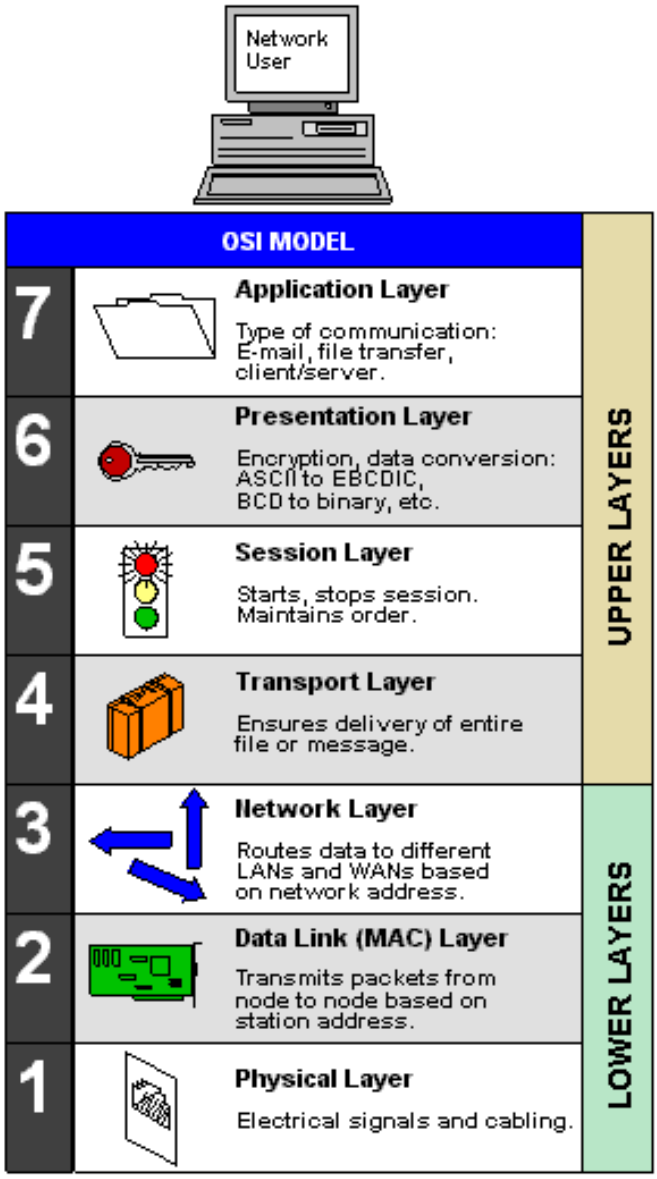
Transportna plast:

Plast definira način prenosa, dolga sporočila razbije na manjše dele. Odkriva in odpravlja napake, multipleksira.
Transportna plast zagotavlja višje ležečim plastem povezavo med končnima računalnikoma. Na prenosni poti poskrbi za pravilen in zanesljiv prenos podatkov. Med drugim določa:
razstavljanje dolgih sporočil na pakete (fragmentacija) ob oddajanju in sestavljanje sporočil iz paketov (defragmentacija) ob sprejemanju. Pri tem je pomembna urejenost zaporedja paketov, saj lahko paketi prispejo v drugačnem vrstnem redu, kot so bili poslani;
odkrivanje in odpravljanje napak: transportna plast odkriva napake in o tem obvesti plast, na kateri je do napake prišlo

Omrežna plast:
Vzpostavlja, prekinja in vzdržuje povezavo med uporabniki. Izbira pot in skrbi za preklapljanje paketov, zavez ter sporočil.
Omrežna plast skrbi za pravilno potovanje paketov različnih dolžin in po različnih poteh. Zagotavlja pravilno fragmentacijo in defragmentacijo, pravilen vrstni red pošiljanja in prejemanja paketov. Zgotavljanje kvalitete servisa je prav tako naloga te plasti.
Protokoli: IP, IPX, DecNet

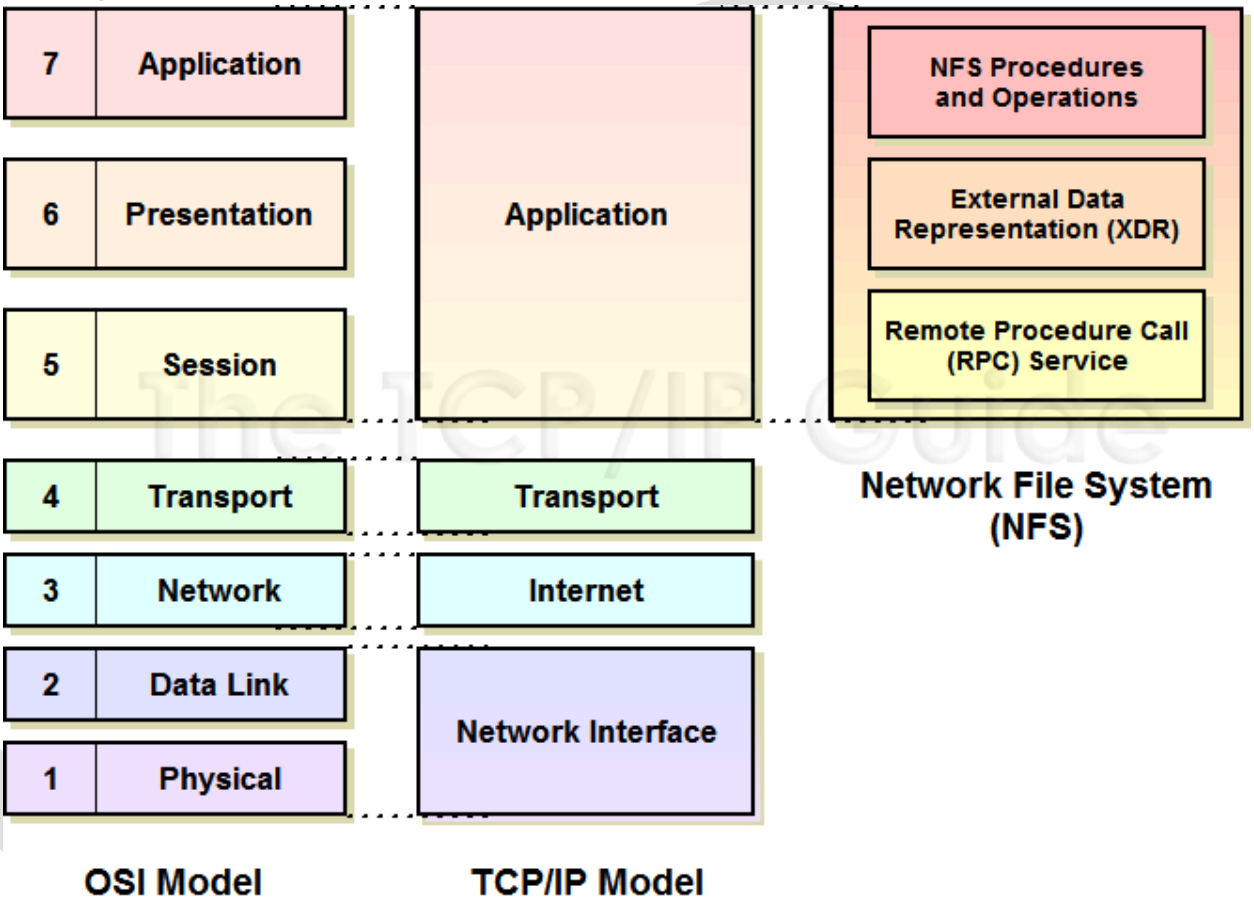
Povezovalna plast:
Določa enote sporočila, način ugotavljanja napak, kontrolo pretoka, MAC podnivo.
Povezovalna plast skrbi za:
določanje enote sporočil (znake, bloke, pakete),
način ugotavljanja napak med dvema sosednjima vozliščema,
odpravo napak,
omrežno topologijo,
mehanizme dostopa do prenosnega medija.
kontrolo pretoka
Protokoli: Ethernet, FDDI, PP; MAC, LLC

Fizična plast:
Predpisuje prenosni medij preko katerega se prenašajo podatki. Definira nivo signala, hitrost prenosa, način zapisa podatkov.
Fizična plast definira električne in mehanske lastnosti vodnikov in konektorjev. Definirane so prenosne frekvence in napetostni nivoji, načini kako se se zapisujejo podatki v obliko, ki je primernaza prenos po izbranem mediju.
Mediji: bakreni vodniki (koaks, utp, optika...)
Konektorji: BNC, RJ45 ...



TCP/IP model in razlike glede na ISO OSI

Primerjava



TSP/IP model je nastal kot odziv na hiter razvoj interneta. Njegova odlika je predvsem uporabnost. Sestavljen je iz štiri plasti. Spodaj vidimo njegovo zgradbo primerjalno s ISO/OSI modelom. Ugotovimo lahko, da prva plast pokriva dve plasti iz ISO/OSI modela. Naslednje dve plasti se pokrivata. Četrta plast pa pokriva kar tri plasti ISO/OSI modela (plast seje, predstavitveno in aplikacijsko sejo). Za razliko od dejure OSI modela je TCP/IP defacto model komunikacij

7.	Aplikacijska plast	Aplikacijska plast
6.	Predstavitvena plast	
5.	Plast seje	

4.	Prenosna plast	Prenosna plast
3.	Mrežna plast	Omrežna plast
2.	Povezavna plast	Dostopovna plast
1.	Fizična plast	

Nabor protokolov

Spodaj vidimo vse najvažnejše protokole za povezovanje računalnikov. Postavljeni so v pripadajoči nabor. Vidimo lahko, da so v naboru ISO/OSI protokoli. ki so manj poznani. Nam najbolj poznane internetne protokole najdemo v naboru TCP/IP. V mešanem naboru so protokoli, ki spadajo v en in drugi nabor. Predvsem je tu zanimiva fizična plast. ki jo upotablajta tako eden kot drugi. Povedati pa je treba da se TCP/IP model z njimi ne ukvarja in jih posebej definira ampak jih zgol uporablja.

plast		mešano	TCP/IP nabor	OSI nabor
#	ime			
7	aplikacijska	HL7, Modbus, SIP, SSI	HTTP, SMTP, SMPP, SNMP, FTP, Telnet, NFS, NTP, RTP MIME, XDR, SSL, TLS Sockets. Session establishment in TCP. SIP. TCP, UDP, SCTP	FTAM, X.400, X.500, DAP
6	predstavitvena	TDI, ASCII, EBCDIC, MIDI, MPEG		ISO 8823, X.226
5	seje	Named Pipes, NetBIOS, SAP, SDP		ISO 8327, X.225
4	transportna	NetBEUI, nanoTCP, nanoUDP		TP0, TP1, TP2, TP3, TP4
3	mrežna	NetBEUI, Q.931	IP, ICMP, IPsec, ARP, RIP, OSPF	X.25 (PLP), CLNP
2	povezovalna	Ethernet, 802.11 (WiFi), token ring, FDDI, PPP, HDLC, Q.921, Frame Relay, ATM, Fibre Channel	PPP, SLIP	X.25 (LAPB), Token Bus
1	fizična	RS-232, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, DSL, 802.11b, 802.11g		X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703)

TEHNOLOŠKE OSNOVE KOMUNIKACIJE

Prenosni sistem, ki omogoča fizičen prenos podatkov po različnih prenosnih medijih

Za zagotovitev prenosa podatkov po različnih medijih mora komunikacijski protocol izpolnjevati nekaj zahtev.

- Prenos je vzpostavljen serijsko, z osnovno enoto bit in sestavljeno enoto octet(byte)
- Poslani telegram lahko prispe na cilj ali pa ne.
- Vrstni red sprejema telegramov ni nujno enak vrstnemu redu oddaje telegramov

Različne vrste prenosnih medijev

Sukana parica

Najstarejši medij, ki se še vedno uporablja. Gre za zvito žico, ki je zvita zaradi preprečevanja občutlivosti na elektromagnetne motnje. Ethernet opisuje skupina standardov IEEE802.3. Uporabljana je metoda random send/carrier detect. Kar pomeni takojšnje časovno naključno pošiljanje telegramov, z mehanizmi detekcije kolizije.

Optika

Najmodernejši medij, ki nadomešča ostala dva(radiofrekvenčnega, kjer je to mogoče).

Radiofrekvenčno

Za mobilne naprave in kjer ni dostopa do drugih internetnih povezav. Najcenejši način širjenja internetnega omrežja. Dosega se visoke stopnje zaneslivosti povezave in relativno visoke prenosne hitrosti 10Mbaud in 54Mbaud. Radiofrekvenčno mrežno komunikacijo opisuje družina standardov IEEE802.11.

Fizikalne lastnosti in omejitve fizičnega omrežja

Sukana parica

Ethernet omrežje po standard IEEE802.03. Dovoljena razdalja med priključkoma 120m in prenosne hitrosti 10Mbaud, 100Mbaud, 1Gbaud(tu so razdalje manjše okoli 30m).

Optika

Najvišje prenosne hitrosti 2.5Gbaud, 10Gbaud, 40Gbaud. Optika je idealni medij za prenos. Uporabljajo se prenosne tehnike po standard IEEE802.3(Ethernet), IEEE802.1 bridget network, kot druge manj poznane tehnike prenosa.

Radiofrekvenčno

Imamo nekaj standardov

1.IEEE802.11abg obratuje na malih močeh pod 100mW in izkorišča zakonodajo, večine držav, ki dovoljuje delo z malimi močmi brez licenc. Tipičen doseg na prostem je 100m in znotraj prostora v stavbah(Tudi skozi zidove, do cca 20m).

2.IEEE802.16 obratuje na močeh nekaj 100W in je potrebna licenca za obratovanje. Prenosne hitrosti so do 10Mbaud do uporabnika, do oddaljenosti okoli 10km(vidna razdalja)

Električna instalacija

V zadnjem času se pojavlja prenos podatkov po elektro instalaciji. Gre za hubano omrežje s prenosnimi hitrostmi 200 do 500Mbaud.

Razlika med digitalnim in analognim prenosom podatkov

Digitalni prenos mora zagotavljati zaznavo samo dveh stanj 1 ali 0. Z raznimi pristopi zagotovimo, da prisotnost motenj ne vpliva na zaznavo. Pri analognem prenosu podatkov moramo skrbeti za primerno nepopačenost signala na celotni prenosni poti signala. Za koliko lahko popačimo analogni signal je odvisno od zahtev sprejemnika signala. Digitalne prenosne poti so veliko enostavnejše in veliko hitreje zadostijo zaznavno kvaliteto za samo dva stanja. Do neke mere lahko napake digitalnih prenosov popravimo programsko, česar ne moremo trditi za analogni prenos.

LOKALNA RAČUNALNIŠKA OMREŽJA

Lokalna računalniška omrežja

Lokalna omrežja (LAN, Local Area Networks) povezujejo računalnike in računalniško opremo (tiskalnike, deljene pomnilniške naprave...) na geografsko omejenem območju. Tipično je to stavba ali skupina stavb. Povezave med računalniki so zelo hitre, zato taka omrežja omogočajo visoko stopnjo integracije in komunikacijsko intenzivne porazdeljene aplikacijeAktivni in pasivni elementi lokalnega računalniškega omrežja

Ojačevalniki

Vsi vhodi so obravnavani enakopravno. Telegram, ki ga pošlje naprava, se pošlje vsem napravam (tudi napravi ki je telegram poslala), ki so priključene na ojačevalnik. Če je omrežje sestavljeno zgolj iz ojačevalnikov moramo paziti, na največje dovoljeno število prehodov skozi ojačevalnike. Za eternet je ta številka 5.

Preklopniki

Preklopnik sprejme na določenem vhodu telegram. Če je naslovni MAC telegram v preklopnikovi tabeli, telegram pošlje samo v vejo, ki je v MAC tebeli, drugače pošlje telegram v vse veje. Če MAC telegram še ni v MAC tabeli preklopnika se le-ta doda na seznam prisotnih MAC naslovov.

Zaradi te lastnosti preklopniki ločijo promet glede na vejo mreže in nujnopotrebno komunikacijo. Preklopniki so učinkovit element izkoriščanja prehodne kapacitete mrež. Za razliko od ojačevalnikov, preklopnik filtrira promet glede na MAC naslov in pošlje telegram le v tisto vejo za katero ve, da je na njo priklopljena naprava z zahtevanim MAC naslovom.

Delovanje lokalnih računalniških omrežij

Lokalne računalniške mreže povezujejo lokalno in so grajene na omejenem področju. Z uporabo aktivnih in pasivnih mrežnih elementov širimo omrežje po potrebi. Pri načrtovanju je treba upoštevati potrebno prepustnost v določeni točki. Pravilno načrtovanje preprečuje zamašitve omrežja in optimalno koriščenje prenosnih poti.

Hrbtenica računalniškega omrežja

Hrbtenica je ime za del omrežja kjer se pričakuje največji promet in je ponavadi priključena na glavni priklop v prostrano omrežje(ruter). The ruterjev je lahko več in točke med ruterji so po definiciji hrbtenica omrežja. Na hrbtenico potem lepimo krake omrežja, ki signal pripeljejo do uporabnikov. Za izgradnjo hrbtenic se danes uporablja optika s hitrostjo 1Gbaud, 2,5Gbaud, 10Gbaud ali 40Gbaud.

Različne topologije omrežij, njihove lastnosti in področja uporabe

Poznamo topologijo zvezde, obroča, dvojnega obroča in linije.

Lastnosti aktivnih elementov in pasivnih elementov hrbtenice

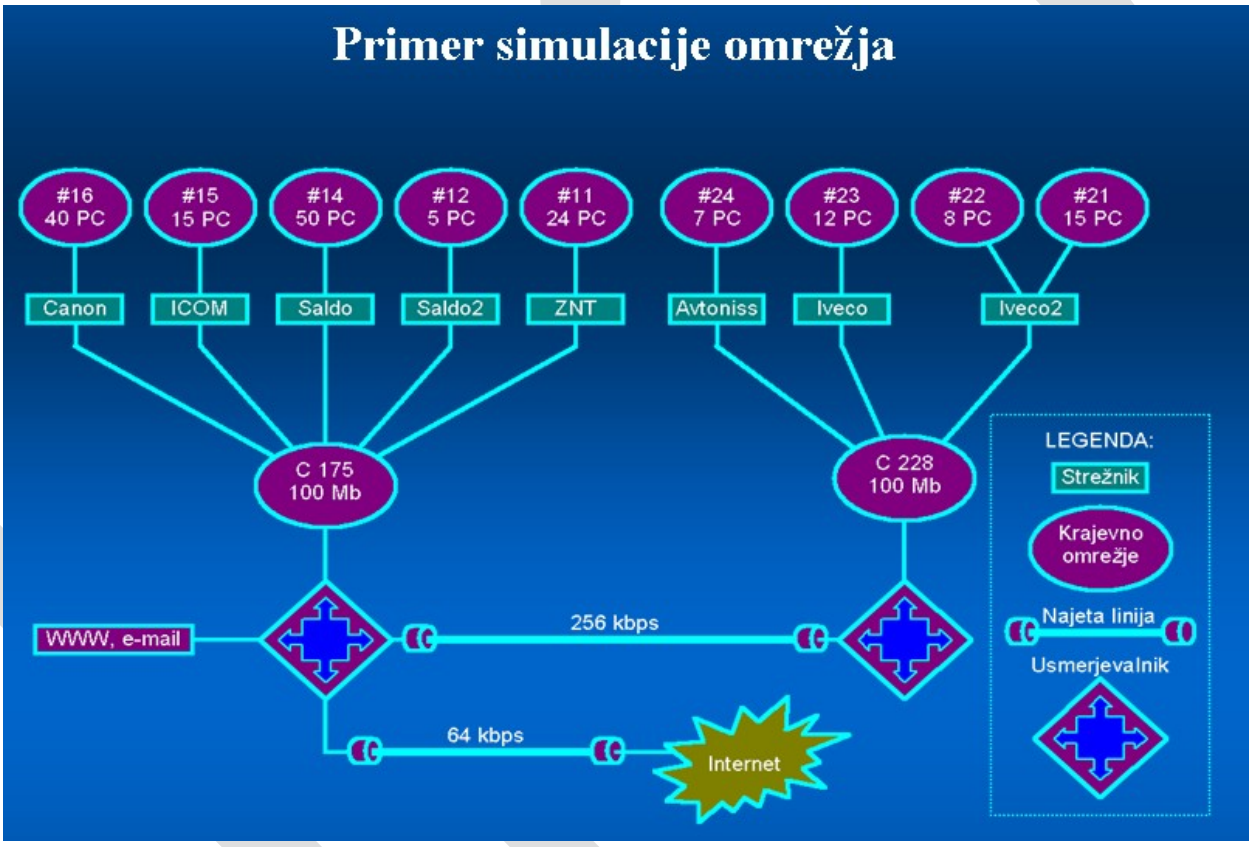
Aktivni elementi si samodejno zgradijo tabelo preslikave s katero usmerjajo promet po omrežju. Pasivni elementi ponavadi samo ojačujejo signal, so pa zato hitrejši.

Izbra ustreznega elementa glede na zahteve

Ustrezen element se izbira glede na predvideno hitrost prenosa v posameznem delu omrežja. Hitrost se meri v bitih na sekundo(Baud). Bolj praktična enota je kBaud(kilo(1000) bitov na sekundo), Mbaud(Mega(1000000) bitov na sekundo.

Poleg hitrosti moramo pri realnem obretovanju upoštevati še pogoje delovanja(industrijski, temperature, zahtevana zanesljivost). Zaradi zagotavljanja zahtevanih parametrov, so sestavni elementi omrežja podvrženi testom, zato so elementi za zahtevnejše obratovanje ponavadi dražji.

Praktična izvedba lokalnega računalniškega omrežja



Značilnosti Etherneta

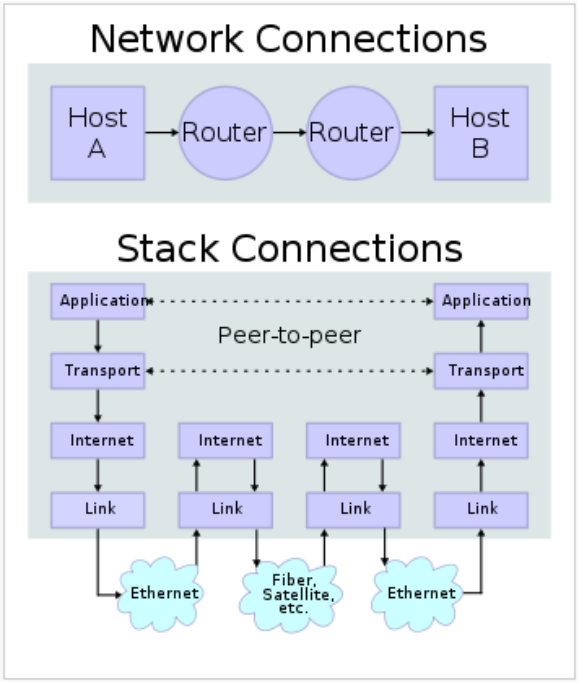
Ethernet je zvezdno omrežje enakopravnih sprejemnikov in oddajnikov. Oddajniki oddajo v omrežje po naključnem algoritmu, sprejemniki so pa sposobni zaznat kolizijo podatkov. V primeru kolizije se podatek enostavno pošlje še enkrat.

Napake, ki se pojavljajo v omrežju

Napake so strojne in sistemske. Strojne napake so posledica slabega ožičenja, slabih sprejemnih pogojev, odpovedi posameznih mrežnih delov. Sistemske napake so posledica slabega načrtovanja in napačnega nadgrajevanja omrežja.

OMREŽNA IN TRANSPORTNA PLAST

Lastnosti omrežne in transportne plasti



Ethernet telegram

Spremenljive dolžine z dolžinami 64 do 1518 oktetov(bytov). Ethernet je ena od danes uporabljanih tehnologij za izvedbo računalniških mrež.

Preambula(8)	Ciljni MAC(6)	Izvorni MAC(6)	Type(2)	Frame Data(64-1500)	CRC(4)

MAC(Media Access Control) je edinstvena(unique) 6 oktetna koda, ki se pojavlja samo enkrat v omrežju.

Zgoraj je predstavljen Ethernet okvir opisan v standard IEEE811.3.

Wireless telegram

Spremenljive dolžine z dolžinami 0 do 2312 oktetov(bytov).

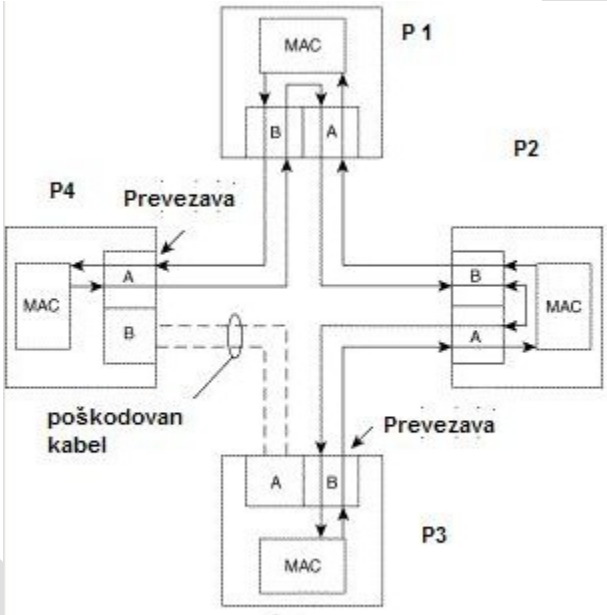
Frame control 2	Duration ID 2	Address 1 6	Address 2 6	Address 3 6	Sequence Control 6	Address 4	Frame Data 0-2312	FCS 4

Frame control(16 bit)

Verzija protokola 2	Type 2	Sub type 4	To DS 1	From DS 1	More Fragments 1	Retray 1	Power Mgt 1	More data 1	WEP 1	Order 1

Zgoraj je predstavljen Wireles okvir opisan v standard IEEE811.11. Podrobneje sta razčlenjena prva dva byta telegram t.i. Frame control.

FDDI telegram



Fiber Distributed Data Interface

1	1	1	2-6	2-6	0-4500	4	1	1
Začetek okvirja	Nadzor dostopa (Access Control)	Vrsta okvirja (Frames Control)	Naslov cilja (Destination Address)	Izvorni MAC (Source Address)	Podatki (Data)	CRC	Konec okvirja (End Delimitter)	Stanje okvirja (Frame status)

Minimalni okvir(žeton)

1	1	1
Začetek okvirja	Nadzor dostopa	Konec okvirja

	(Access Control)	(End Delimitter)

Različne vrste usmerjanja in usmerjevalni algoritmi

Principi

1. Statično ali dinamično (ali upošteva trenutne razmere v omrežju in jim prilagaja usmerjanje prometa?)
2. Po eni poti ali po več poteh (ali gredo v nekem trenutku vsi paketi z istim ciljem po isti poti?)

Možne s vse štiri kombinacije.
OPTIMALNO usmerjanje: enakomerno obremenjene povezave.

Usmerjanje po najkrajši poti

Glede na čas, ceno, število skokov...

Usmerjanje po več poteh

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

Centralizirano usmerjanje

Glavno vozlišče (*master*, *koordinator*)
Zbira podatke o razmerah v omrežju
Izračuna tabele in jih razpošlje
TEŽAVA: velika omrežja s hitrimi spremembami

1. dinamično
2. lahko po eni ali po več poteh

Izolirano usmerjanje

NE UPOŠTEVA razmer v omrežju
Hot potato: vozlišče se hoče čimprej znebiti paketa, zato ga vrže

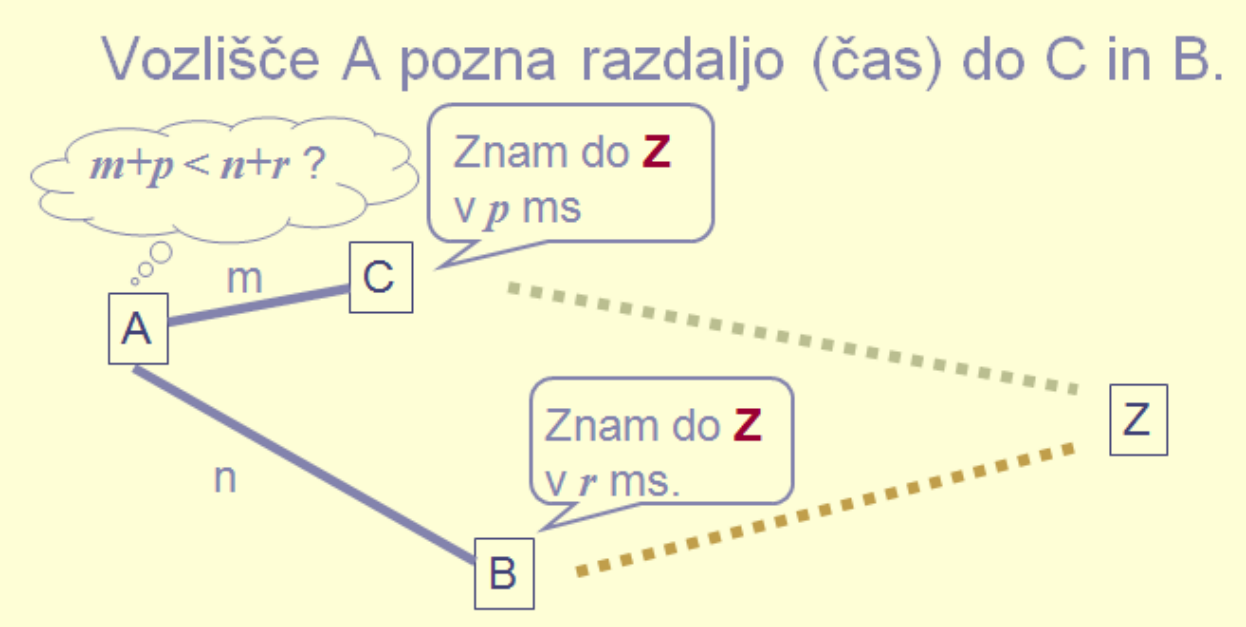
1. V najkrajšo izhodno vrsto
2. Dolžina vrste × utež

Poplavljanje – v vse izhodne vrste
Selektivno poplavljanje – tiste, ki so približno v pravi smeri

Usmerjanje v Internetu RIP

RIP - Routing Information Protocol Porazdeljeno usmerjanje (znotraj hrbtenice)

- Vsako vozlišče pozna razdaljo do vseh svojih sosedov.
- Vsakih T časovnih enot si izmenjajo usmerjevalne tabele.
- Potem pregledajo in po potrebi prilagodijo svoje tabele.
- Vozlišče A pozna razdaljo (čas) do C in B.



Usmerjanje v Internetu OSPF

OSPF – Open Shortest Path First Usmerjanje po najkrajši poti (znotraj hrbtenice)

- Usmerjanje znotraj avtonomnih sistemov (“link state”).
- Usmerjevalniki si pošiljajo sporočila
  - link state update / request/ ack – cena, čas
  - Database description – vsi usmerjevalni pod.
- Vsak si izračuna najkrajše poti v svoji okolici.
- Dinamično usmerjanje po več poteh, hierarhija, varnost.

Usmerjanje v Internetu BGP

BGP – Border Gateway Protocol skrbi za usmerjanje med različnimi hrbtenicami

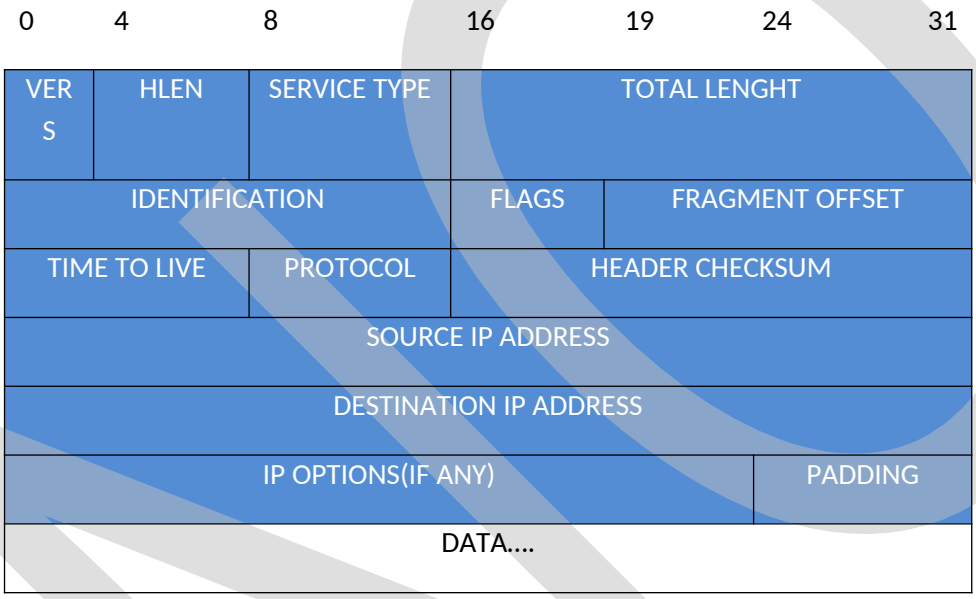
- IGRP želi čim učinkoviteje prenesti promet od izvora do ponora.
- BGP mora upoštevati še politiko, kini odvisna od tehnologije.
  - Promet z izvorom ali ponorom v IBM ne sme prek Microsoftove infrastrukture.
  - Čez Albanijo pošiljamo le, če ne gre drugod.

Vzroki za zasičenje in mehanizmi za preprečevanje zasičenja

Zasičenje se pojavlja pri prenosnih poteh s premalo bitno prepustnostjo in prevelikim navalom zahtevkov za prenos. Raševanje zasičenj je večplastno z boljšimi algoritmi rutanja, s stiskanjem podatkov in s povečevanjem prepustnih hitrosti prenosnih poti .

IP protokol in naslavljanje

Glava IP protokola vsebuje podatek o izvornem in ciljnem IP naslovu.



HLEN pomeni dolžino IP glave pomnoženo z 32. TOTAL LANGHT je dolžina IP telegrama vključno z glavo in podatki. SERVICE TYPE je sestavljen iz treh bitov za prioriteto(prioriteta 0-7), in Bitov D(low delay), T(high troughput) in R(high reliability). TTL je edino polje telegram, ki se spreminja ob vsakem prehodu preko usmerjevalnika. To polje se vsakič kogre telegram preko usmerjevalnika zmanjša za 1. Če se polje zmanjša na ena se pot telegram predčasno konča. S tem preprečimo krožne neskončne poti telegramov.

Pomen podomrežij

Podomrežja so imela svoj velik pomen v IPv4 kot drobljenje razredov na podrazrede, kar nam je omogočilo večje število vendar manjših omrežij. V bistvu je to ena od treh metod umetnega povečevanja razpoložljivih naslovov v starem IPv4, ki je umru predvsem zaradi premalega števila naslovov.

Ostale dve metodi sta še NAT storitev s sistemom lokalnih omrežij(192.168.x.x) in proxy standard(Tu niso mišljeni proxy strežniki, kot podpora medpomnenju, zaradi v preteklosti premale prepustne kapacitete priklopov na internet.

Protokoli

UDP in TCP protokola sta osnovna za komunikacijo med aplikacijami. Programsko so dodana vrata , ki omogočajo komunikacijo med različnimi aplikacijami večopravilnih operacijskih sistemov. ICMP protokol je namenjen sporočanju in se razen redkih izjem ne uporablja v aplikacijah. IGMP protocol je namenjen pošiljanju podatkov vsem (broadcast) v omrežju.

TCP

TCP je povezan protocol, namenjen programskemu zagotavljanju zanesljivosti povezave. Izgubljeni telegram se ugotavljajo in pošljejo ponovno. .TCP protokoli predvideva 65536 programskih vrat.

UDP

UDP je nepovezan protocol namenjen pošiljanju podatkov med aplikacijami. Aplikacija mora poskrbeti za izgubljene telegrame. . UDP protokol predvideva 65536 programskih vrat.

ICMP

ICMP je sporočilni protocol, ki ga razen v redkih izjemah, uporablja le TCP/IP protocol za avtomatsko javljanje določenih podatkov in napak na izvor telegram.

IGMP

IGMP je telegram, ki pošilja podatke vsem na mreži.

ARHITEKTURA ODJEMALEC-STREŽNIK

Arhitektura odjemalec -strežnik

Povezovalna komunikacija s pomočjo TCP protokola

TCP protokol IP standard omogoča vspostavitev podatkovnega toka med dvema aplikacijama. Komunikacija je dvosmerna in zanesljiva na programskem nivoju. Sam protokol poskrbi za odkrivanje izgubljenih telegramov in njihovo ponovno pošiljanje.

Nepovezovalna komunikacija s pomočjo UDP protokola

UDP protokol IP standarda omogoča pošiljanje in sprejemanje telegramov. Aplikacija ki sprejema UDP telegrame mora preverjat sprejem telegram na določenem portu. Če se določen telegram na komunikacijski poti izgubi je stvar aplikacije, da odloči kaj narediti v takem primeru.

VARNOST UPORABNIŠKIH STORITEV

Pomen varnosti uporabniških storitev

Informacijska varnost pomeni tudi stalno dostopnost vseh ključnih podatkov in storitev vsem upravičenim uporabnikom v vsakršnih okoliščinah. Zato načrtovanje neprekinjenega poslovanja. Učinkovitega sistema informacijske varnosti pa si ni mogoče zamisliti, če se ta ne začne že pri razvijanju, naročanju, prevzemanju in vzdrževanju programske opreme. Skrb za informacijsko varnost mora biti namreč prisotna že pri načrtovanju uporabniških rešitev. Pomembno je tudi, da so ustrezno varovani razvojni postopki in okolje ter hkrati povsem ločeni od okolja in postopkov za redno delo. Na informacijsko varnost pa se ne sme pozabiti tudi pri kasnejšem vzdrževanju uporabniških rešitev. Med bistvene sestavine varovanja podatkov sodi tudi obvladovanje dostopa, ki mora vedno izhajati iz poslovnih zahtev ter hkrati zagotavljati jasno porazdeljeno odgovornost uporabnikov in omogočati jasno upravljanje dostopa do operacijskih sistemov in uporabniških rešitev tako pri delu v poslovnih prostorih, mobilnem poslovanju in delu na daljavo. Obvladovanje dostopa pa pomeni tudi nadzor nad dostopom do sistemov in podatkov ter njihovo uporabo. Upravljanje z informacijskimi sistemi sodi med zahtevnejše naloge informacijske varnosti. Zagotoviti mora namreč ustrezna pravila in navodila za vse izmenjave podatkov (komunikacije) z različnih vidikov: znotraj organa in z zunanjim svetom, med ljudmi zaposlenimi oziroma delujočimi pri/v organu in drugimi ljudmi, informacijskimi sistemi z drugimi sistemi in informacijskimi sistemi z ljudmi, osebno ali s pomočjo papirja ali tehnoloških sredstev in v elektronski, papirnati ali drugi obliki. Enako pomembni so jasno določeni postopki ter vključitev elementov informacijske varnosti v vse postopke v organu javne uprave. Najbolj zahtevno področje informacijske varnosti so človeški viri. Zato je ključen pregled tveganj in ustreznih ukrepov za njihovo zmanjševanje, ki se začne pri ustreznih določbah notranjih aktov in sistemizacije delovnih mest v organu javne uprave ter nadaljuje preko pridobivanja novih sodelavcev, njihovega uvajanja in usposabljanja do prenehanja zaposlitve iz tega ali onega razloga. Posebej so obdelani postopki za ravnanje v primeru različnih varnostnih dogodkov in odzivanje nanje.

Tehnike kodiranja podatkov

Kodiranje je predstavitev informacije z dogovorjenimi znaki. Ker je možnosti za kodiranje znakov neskončno, se je potrebno dogovoriti, kako bomo znake kodirali. Uvesti je potrebno standard. Če bi znaki bili na vsakem računalniku drugače kodirani, bi nam to onemogočilo prenos podatkov iz enega na drug računalnik. Sredi šestdesetih let so v ZDA programerski strokovnjaki za najpogosteje uporabljene znake določili stalne kode, kar naj bi omogočalo izmenjavo informacij med poljubnimi računalniki. Ta dogovor so poimenovali »American Standard Code for Information Interchange«, kar pomeni ameriška standardna koda za izmenjavo informacij. Standard na kratko označimo ASCII in izgovorimo "aski". Standard ASCII ne predpisuje vseh 256 kod, ki jih omogoča zapis z osmimi biti, ampak le 128, od kode 0 do kode 127. V njej ne najdemo šumnikov, ki jih seveda nujno potrebujemo. Standard ASCII je

neposredno uporaben samo v angleško govorečih deželah. Pisave drugih dežel povečini vsebujejo dodatne lastne znake, ki jih ASCII ne pozna. Omenjeni problem rešujemo z uvajanjem dodatnih kodnih standardov, ki jih imenujemo kodne tabele.

Pomen digitalnih potrdil

Digitalna potrdila so digitalni identifikacijski dokumenti. Primerjamo jih lahko z osebno izkaznico, le da so prirejeni za uporabo v digitalnem svetu. Uporabniki potrebujejo kvalificirano digitalno potrdilo tako za uporabo spletne rešitve kot tudi za poročanje z izmenjavo elektronskih sporočil. Brez digitalnega potrdila podobnih spletne rešitve, kjer se zahteva identifikacija in kodiranje ni mogoče uporabljati.

Uporabnik zahtevek za digitalno potrdilo vloži pri(npr.) vladnem overitelju SIGEN-CA. Nato po ustreznem postopku pridobi avtorizacijsko kodo in geslo za prevzem digitalnega potrdila. Prevzem (spletnega) digitalnega potrdila opravi s pomočjo navodil. Za zagotavljanje visoke stopnje varnosti je treba z digitalnim potrdilom ravnati skrbno kot npr. s ključi od blagajne ali z žigom. Pri tem velja dosledno upoštevati napotke za varno ravnanje s (spletnimi) digitalnimi potrdili.

Elektronski podpis

Elektronski dokumenti nimajo fizične oblike, zato lastnoročni podpis za njihovo podpisovanje ne pride v poštev. Elektronski podpis je zato zamišljen kot elektronska identiteta osebe, ki se odloča za elektronsko poslovanje. V elektronskem okolju veljajo drugačna pravila kot v uveljavljenem svetu papirja, pisalnih peres, žigov in arhivskih omar. Dokumenti, shranjeni na elektronske medije so osvobojeni fizičnih omejitev, ki narekujejo pravila klasičnega poslovanja. Lahko so neštetokrat reproducirani, shranjeni na mnogo manjšem prostoru ali poslani na drug konec sveta v delcu sekunde, celoten delovni proces pa je lahko poleg tega skoraj v celoti avtomatiziran Elektronski dokumenti seveda nimajo fizične oblike, zato lastnoročni podpis za njihovo podpisovanje težko pride v poštev. Edinstvena oblika lastnoročnega podpisa in povezanost s fizičnim dokumentom sta lastnosti, ki ju v elektronskem okolju ni mogoče podvojiti. Temeljne naloge lastnoročnega podpisa – zagotavljanje avtentičnosti in pravne veljavnosti dokumenta, povezanosti dokumenta s podpisnikom in dokaz o njegovi izjavi volje so pri elektronskem poslovanju težko izpolnjene na enostaven način. V elektronskem svetu si ljudje pri sporazumevanju ne gledajo iz oči v oči. Komunikacija in sklepanje poslov lahko potekata brez fizičnega stika med strankami, kar s seboj prinaša dobršno mero negotovosti. Tako kot lastnoročni podpis na papirnatem dokumentu povezuje podpisnika s samim dokumentom, fizične lastnosti papirja in črnila pa zagotavljajo njegovo nespremenljivost, se lahko tudi v elektronskih komunikacijah, odvisno od izbire tehnološke rešitve, bolj ali manj približamo varnosti in pravni gotovosti, ki jo ponuja lastnoročni podpis. Elektronski podpis je torej neke vrste elektronska identiteta osebe, ki se odloča za elektronsko poslovanje. Poglejmo si, na kakšen način elektronski podpis deluje in kako zagotavlja lastnoročnemu podpisu enakovredno varnost

in zanesljivost. Obstaja velika izbira tehnoloških postopkov za elektronsko podpisovanje, vendar vsi ne nudijo enake varnosti in zanesljivosti. Med najbolj razširjene oblike elektronskega podpisovanja in hkrati tudi najbolj varne, spada uporaba kriptografskih metod, ki temeljijo na infrastrukturi javnih ključev. Takšna oblika elektronskega podpisa je znana tudi pod imenom »digitalni podpis«. Temelj digitalnega podpisovanja je kriptografija, veja uporabne matematike, s katero lahko sporočilo spremenimo iz prvotne oblike v neko drugo, neprepoznavno obliko, iz nje pa lahko kasneje zopet izračunamo prvotno obliko sporočila. Novejša vrsta kriptografije, imenovana tudi asimetrična kriptografija, se je razvila šele v zadnjih desetletjih in temelji na uporabi različnih ključev. Pri asimetrični kriptografiji se z uporabo posebnega algoritma ustvarita dva različna ključa (zasebni in javni ključ), ki sta med seboj matematično povezana. Sporočilo, šifrirano z enim ključem, se lahko dešifrira le z drugim ključem iz istega para, in obratno. Zaradi takšnih lastnosti je ta vrsta kriptografije primerna tudi za uporabo med več različnimi subjekti.

Elektronski podpis ni skeniran lastnoročni podpis, temveč posebna metoda podpisovanja, ki temelji na asimetričnem šifriranju (uporaba javnega in zasebnega ključa).

Svoj zasebni ključ mora poznati samo podpisnik in ga skrbno varovati.

Za varnost poslovanja je poskrbljeno s pomočjo t.i. infrastrukture javnih ključev, katere najpomembnejši člen so overitelji.

Z uporabo para ključev se lahko učinkovito zagotavlja zaupnost komunikacije. Za lažjo predstavo si zamislimo dve osebi, Janka in Metko, ki si želita izmenjavati zaupna sporočila ter imata vsak svoj par ključev:

1. Janko objavi ali pošlje Metki svoj javni ključ, prav tako Metka objavi ali pošlje Janku svojega;
2. Janko napiše svoje sporočilo, ga šifrira z Metkinim javnim ključem in ji šifrirano sporočilo pošlje;
3. Zaradi matematičnih lastnosti para ključev, lahko Jankovo sporočilo z uporabo svojega zasebnega ključa dešifrira le Metka;
4. Metka napiše odgovor in ga šifrira z Jankovim javnim ključem, zato ga lahko dešifrira le Janko s svojim zasebnim ključem.

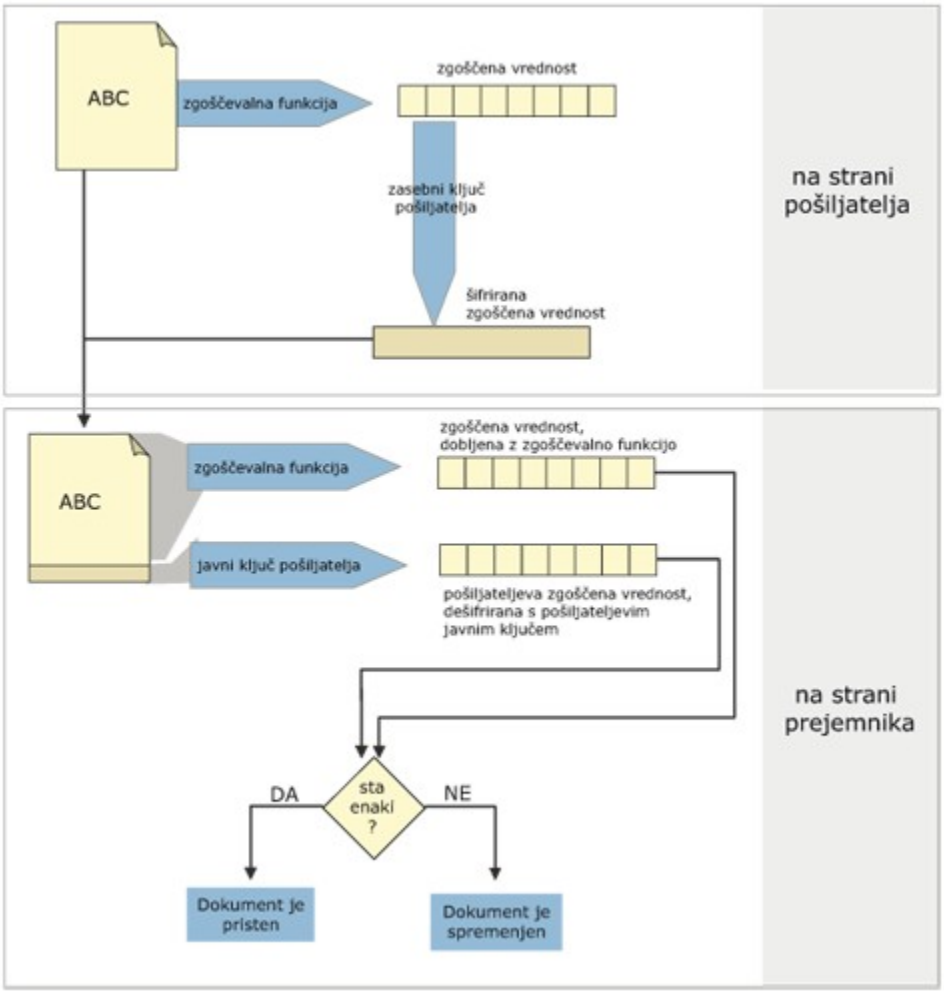
Vendar le zaupnost še zdaleč ni dovolj za učinkovito in varno elektronsko poslovanje, saj je potrebno zagotoviti še druge pogoje: avtentičnost podpisnika, pristnost in neprekliclјivost podpisanega dokumenta. Izpolnjevanje teh pogojev je možno zelo učinkovito zagotoviti z uporabo digitalnega podpisa, ki poleg šifriranja vsebuje še dodaten tehničen postopek, zgostitveno funkcijo. Poglejmo si, kako poteka postopek digitalnega podpisovanja:

1. Janko ima par ključev - enega (zasebni ključ) obdrži zase, drugega (javni ključ) pa objavi v posebnem imeniku ali ga na drug način napravi javno dostopnega;
2. Janko nato natančno določi obseg podatkov, ki jih želi podpisati - ti podatki predstavljajo sporočilo. Z uporabo posebne programske opreme nato izračuna zgostitveno vrednost sporočila.

Izračun zgostitvene vrednosti sporočila je postopek, pri katerem se z uporabo matematičnega algoritma (zgostitvene funkcije) napravi edinstven »povzetek« sporočila, ki predstavlja vsebino sporočila.

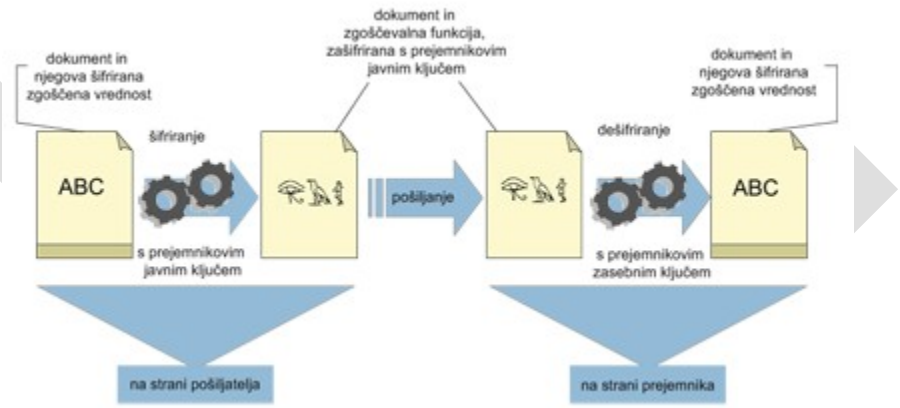
3. Z uporabo zasebnega ključa Janko šifrira ustvarjeno zgostitveno vrednost sporočila – tako šifrirani vrednosti rečemo digitalni podpis.
4. Janko digitalni podpis pripne k sporočilu in oba skupaj pošlje Metki.
5. Metka od Janka sprejme sporočilo s pripetim digitalnim podpisom.
6. Z uporabo Jankovega javnega ključa dešifrira pripeti digitalni podpis in dobi zgostitveno vrednost sporočila.
7. Metka še sama ustvari zgostiveno vrednost sporočila ter jo primerja z dešifrirano zgostitveno vrednostjo iz jankovega podpisa. Če se ujemata, je to zagotovilo, da je sporočilo prišlo od Janka ter da ni bilo spremenjeno.

Preverjanje pristnosti dokumenta



Digitalni podpis torej zaradi uporabe posebnih matematičnih funkcij in algoritmov zagotavlja pristnost sporočila in avtentičnost podpisnika. Nespremenljivost je zagotovljena z uporabo zgostitvene funkcije, ki zaradi matematičnih principov, na katerih deluje, za vsako možno sporočilo vedno ustvari edinstveno zgostitveno vrednost. Varnost takšnega postopka temelji na matematično dokazani predpostavki, da se ne more zgoditi, da bi imeli dve različni sporočili isto zgostitveno vrednost, če se za njun izračun uporabi ista zgostitvena funkcija. Uporaba para ključev pa zagotavlja avtentičnost podpisnika – matematične lastnosti asimetrične kriptografije so zagotovilo, da je bilo sporočilo podpisano z zasebnim ključem podpisnika, saj v nasprotnem primeru nikakor ne bi moglo biti dešifrirano z javnim ključem iz istega para. Le z uporabo varnih matematičnih postopkov pa še nismo v celoti zadostili vseh pogojev, ki so potrebni za popolno zanesljivost elektronskega podpisa. Uporaba para ključev zagotavlja, da je bilo neko sporočilo resnično podpisano s točno določenim zasebnim ključem, ker pa so ključi in zgostitvene vrednosti le zaporedja številk, ki ne vsebujejo nobenih osebnih podatkov, nam to še ne jamči, da nek par ključev resnično pripada točno določeni osebi.
To zadrego je mogoče rešiti na dva načina. Prvi način je uporaben pri poslovanju med strankami, ki se med seboj že poznajo in si zaupajo ali imajo sklenjeno pogodbeno razmerje. Takrat si stranke enostavno sporočijo svoja javna ključa. Vendar pri modernem elektronskem poslovanju, kjer v poslovna razmerja stopa več različnih strank, ki se ne poznajo in nimajo sklenjenih nobenih dogovorov, takšna rešitev ne zadošča. V teh primerih je rešitev infrastruktura javnih ključev.

Postopek pošiljanja elektronsko podpisanega šifriranega dokumenta



Osnovna ideja infrastrukture javnih ključev je v obstoju neke zanesljive tretje osebe. Zanesljive tretje osebe so overitelji digitalnih podpisov, ki jamčijo za povezavo med parom ključev in identiteto določene osebe. V ta namen overitelji izdajajo digitalna potrdila, v katerih je vsebovan javni ključ nosilca potrdila in nek razlikovalen podatek o njegovi identiteti. Avtentičnost identitete nosilca overitelji zagotovijo s preverjanjem identitete oseb, katerim potrdila izdajajo in tako zagotavljajo povezanost med javnim

ključem in točno določeno osebo. Zaradi te povezave na overiteljih in njihovih storitvah temelji tudi varnost in zanesljivost uporabe elektronskih podpisov.

OSNOVNE INFORMACIJSKE STORITVE

Standardne informacijske storitve

Spletna pošta

Je najstarejša spletna storitev. Opisuje jo TCP standard POP3 in je klasična Strežnik/uporabnik struktura. V zadnjem času storitev prevhema http storitev, ker se čedalje več poštnega internetnega prometa opravi v specializiranih web portalih. Način s poštnimi uporabniki(outlook) se uporablja kjer je naše delavno mesto vezano na en kraj, kar pomeni ponavadi na službeno mesto. Spletna pošta in še posebej zaščitena spletna pošta postaja z novimi spletnimi bankami temelj denarnega prometa, kar daje pošti povsem novo dimenzijo spletnega orodja za delo z denarjem. Preko pošte si lahko izmenjujemo mnenja, spletne vsebine(pripete vsebine), omogoča pa pošiljanje v vednost, posredovanje, odgovor, masovno pošiljanje, skrito pošiljanje in podobne stvari znane tudi iz klasične pošte. Klasična in elektronska pošte se bosta v prihodnosti dopolnjevale.

Spletne strani

So storitve po standard http1.1. Gre za klasično Strežnik/uporabnik arhihekturo. Spletne tehnologije so danes najbolj propulzirajoče in jih delimo na železne tehnologije(Html, css, javascript, xml), tehnologije podatkovnih baz in strežnikov(asp, aspx, vbscript, php) in tehnologije navdiha(java, flash). Ker spletne tehnologije prevzemajo druge tehnologije, je tudi tu ogromno inovacij, spreminjanja, izboljševanja. Pojavljajo se vedno nove funkcionalnosti. Spletno okno kot terminal je danes prevladujoča tehnologija IT industrije(kot vmesnik človek stroj). Celotne klasične veje državne uprave se selijo na internetne portale.

Razpršeni strežniki

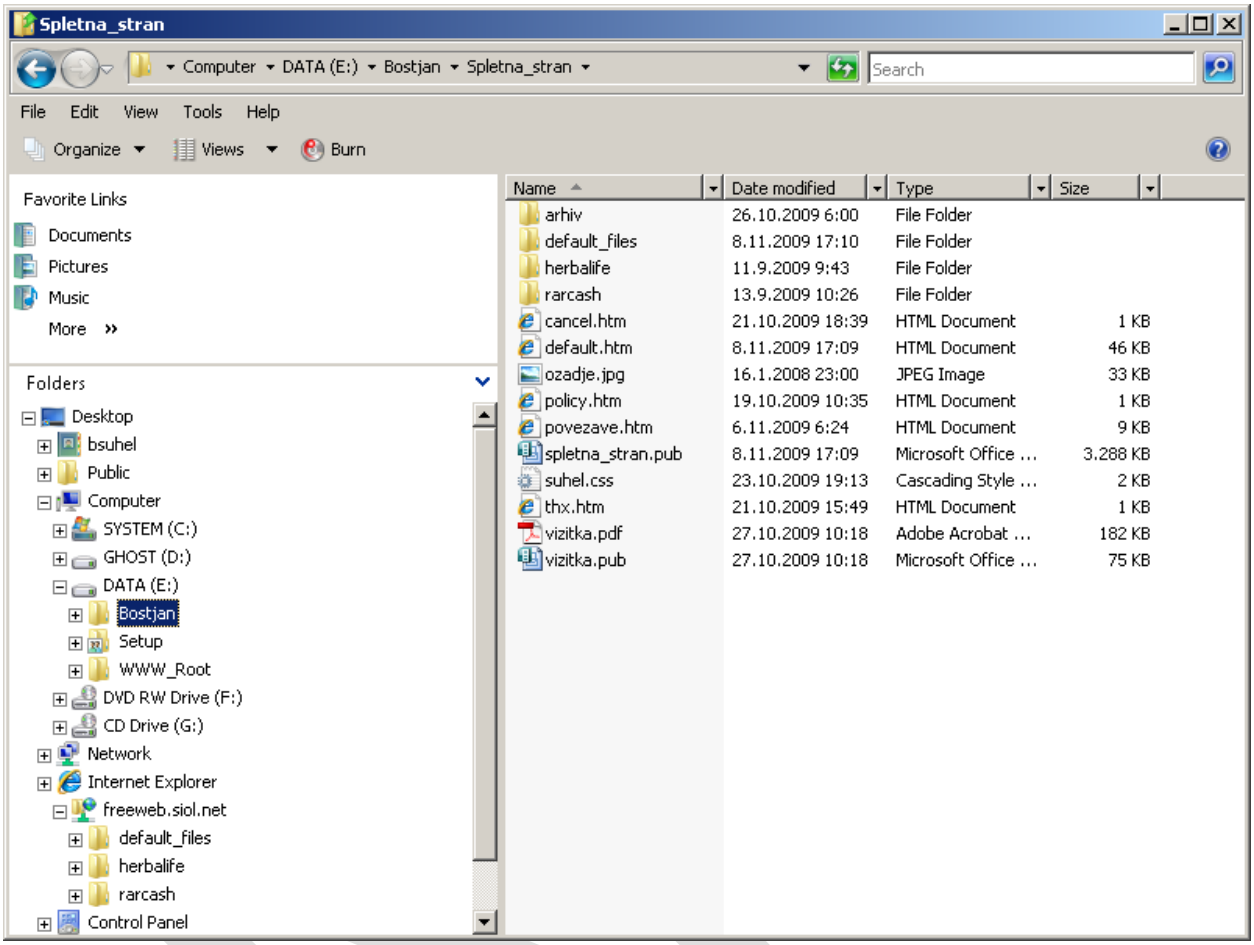
V zadnjem času se pojavlja termin razpršenih podatkov. Gre za razprševanje in avtomatsko selitev podatkov v dele omrežja, kit e podatke več uporabljajo. Še najbolj znani so program za razširjanje velikih količin podatkov tipa torrent. Gre za sistem prenosa celih velikih map na različne lokacije. Vloga Strežnika in uporabnika se prepleta, če sem uporabnik, postanem za že prenešene segmente podatkov nemudoma tudi strežnik. To so bili začetki nove veje razpršenih strežnikov, ki so reševali problem avtentičnosti(Na starih verzijah je lahko kdorkoli zamenjal že prenešene dele datotek ali cele datoteke s čimerkoli in distribuiral spremenjeno vsebino) in identifikacije.

Razpršeni stražniki naredijo samo še korak naprej strategijo prenosa po potrebi, iskanje, prenos, zaščita identifikacije in avtentičnosti pa je podobno. Največja multinacionalka, ki dela z razpršenimi strežniki je google. Oni dejansko postavijo strežnike in pozabijo nanje, ker je dražje vzdrževanje, kakor je zaupati

statističnim podatkom in računati na povprečen čas delovanja do odpovedi. Tako nam na povsem brezplačni pošti lahko ponujajo neverjetnih cca 8Gbytov prostora za skladiščenje pošte in priponk.

Imenski sistem in njegove značilnosti

Imenski sistem je naraven in ob enem edini možen način organiziranosti podatkov. Od nekdaj ljudje urejamo podatke po omarah, predalih mapah. Ena mapa ne more biti v dveh omarah naenkrat, to bi bilo nelogično in nenaravno. Taka organizacija nas vedno pripelje v drevesno organiziranost od debla do vej, vejic in listov. In kot je v naravi normalna rast, odmiranje, odebeltev obremenjene veje, odpadanje litsov, porajanje novih listov in spreminjanje barve listov, se nekaj podobnega dogaja z drevesom podatkov. Za delovanje učinkovitga podatkovnega sistema moramo zagotoviti rast novih vej(kreiranje map), odmiranje vej(brisanje map), označevanje vej(preimenovanje map), porajanje novih listov(kreiranje datotek), odmiranje listov(brisanje datotek), spreminjanje barve listov(preimenovanje datotek). In vse to mora operacijski sistem znati opraviti hitro in brez tempiranih časovnih bomb. Časovna bomba je dejstvo, da neka operacija z večanjem podatkov začne delovati počasi. Če je ta odvisnost npr eksponencialna, je to sigutno časovna bomba, ker bo stvar v neki točki zanesljivo postal neuporabna, ker bodo odzivni praktično neuporabni.



Moderni grafični vmesniki v ničemer ne omejujejo veljavnost zgoraj napisanih dejstev. V zgodovini sta več ali manj znana dva tipa imenskih organizacij.

FAT

Za fat organizacijo(File allocation Table) je značilna imenska tabela, ki pa vsebuje samo začetni in končni segment datoteke. Poleg drugih pomankljivosti, ki so jih odpravljali sproti(FAT12, FAT16, FAT32) je imela omenjena organizacija usodno skrito tempirano bombo in sicer pozicioniranje izredno dolgih datotek, ki so se začele z dolgimi podatkovnimi bazami in filmi dolgimi preko 1Gbyte. Zaradi sekvenčne navezave datoteke je bila Edina metoda poiskati sredino take datoteke iskanje od začetka in preskakovanje iz segmenta na segment, dokler nismo našlipravega segmenta.

NTFS

Pomankljivost skrite časovne bombe za pozicioniranje zelo dolgih datotek odpravlja NTFS(New Tehnology File Sistem) organiziranost z matriko začetkov za vse segmente diska. Taka organiziranost je skoraj enako hitra kot FAT pri osnovnih operacijah nad datotekami, ko pa datoteke narastejo se ohranja

odziv pri pozicioniranju. Tak zapis je tudi bolj odporen na napake, ker imamo vedno na voljo okostje datoteke in lahko izgubimo samo kak segment.

Vloga programske opreme pri uporabi računalniških omrežij

Programska oprema so seveda standardi v praksi. In kot velja za ostale dele računalnika, so omrežja in omrežni program ena najbolj potrebnih aplikacij in hkrati tudi najbolj skrbno načrtovani in preizkušani deli programske opreme.

STORITVE INTERNETA

Zgodovino interneta in standardne storitve, ki jih internet ponuja svojim uporabnikom

Internet je bil v svojih zametkih projekt, ki ga je vodila agencija ARPA (Advanced Research Projects Agency) pri ameriškem obrambnem ministrstvu.

Že **v 60-tih letih** je bilo jasno, da bodo morebitni vojaški spopadi v prihodnosti potekali z računalniško podporo. V tem času so bili računalniki veliki, energetsko potratni, odvisni od kontroliranih pogojev okolja in zato zelo ranljivi v vojaškem smislu. Osnovna zamisel, ki je rodila Internet je bila povezana z varstvom podatkov in dostopa do njih. Če bi bili računalniki povezani, bi bili lahko pomembni podatki nameščeni na več računalnikih, pa kljub temu dostopni z neke kontrolne točke. Če bi bile povezave med računalniki pomnožene, bi bil, tudi v primeru prekinitve nekaterih med njimi, dostop do podatkov še vedno možen.

Že tedaj so se zavedali problematike naslavljanja podatkov in varnosti prenosa. Omrežje, ki naj poskrbi, da bodo podatki prišli na računalnik, kamor so bili poslani, se mora zavedati lokacije računalnikov, v podatkih pa mora biti ciljni naslov tudi jasno zapisan. Omrežje tudi ne sme dovoliti, da bi prišli podatki na cilj pokvarjeni. Rešitve teh osnovnih problemov so temeljile na raziskavah o *paketno-preklopnih mrežah*, objavljenih že leta 1962. Prva shema načrtovanega omrežja je bila javno predstavljena leta 1967.

Leta 1969 je ARPA zgradila prvo eksperimentalno omrežje, imenovano ARPANET. Na začetku so v njem sodelovali samo štirje veliki računalniki na ameriških univerzah: UCLA, Stanford University, UCSD in Utah University. Omrežje je že omogočalo prenos sporočil in deljenje datotek. Na tem omrežju so nastale in se razvijale vse velike ideje, ki so privedle do nastanka Interneta, kot ga poznamo danes.

V 70-tih letih se je ARPANET hitro širil. Leta 1972 je povezoval že 37 velikih računalnikov. Zanimivo je, da je bil, kljub vojaškemu pokroviteljstvu, ves čas omogočen dostop civilnim raziskovalnim organizacijam, večina najodmevnejših raziskav pa je bila objavljena. Tako je prvi program za elektronsko pošto nastal že leta 1972. Leta 1973 so bile opravljene prve *transatlantske povezave* v ARPANET iz Anglije in Norveške.

ARPANET se je počasi preoblikoval iz mreže navzkrižno povezanih računalnikov v *hrbtenico*. K temu je največ pripomoglo *priključevanje prvih manjših omrežij*, ki so nastala po ARPANETovem vzoru (npr. ALOHAnet v l. 1972).

Širjenje omrežja je pospešilo razvoj omrežnih orodij. Nekatera med tedanjimi, sicer posodobljena, uporabljamo še danes. Leta 1972 je National Center for Supercomputing Applications (NCSA) razvil program *Telnet*, namenjen priključevanju in delu na oddaljenem računalniku. *FTP* (File Transfer Protocol) in ustrezni podporni programi, uvedeni naslednje leto, so močno poenostavili prenos datotek med računalniki.

Preoblikovanje v hrbtenico je pospešilo tudi razvoj protokolov. Leta 1974 je nastala prva verzija družine protokolov, imenovana TCP/IP (Transmission Control Protocol / Internet Protocol), namenjena standardizaciji postopkov v omrežju. TCP/IP je bil na voljo zastonj, kar je dodatno pripomoglo pri njegovi širitvi. Pojavi se prvi javni ponudnik omrežnih storitev s čemer se začne tudi komercializacija ARPANETa.

80-ta leta so prinesla odločilne spremembe, tako v tehničnem, kot v organizacijskem smislu. V letih 1982 in 1983 se pojavijo prvi namizni računalniki in s tem se začne množiti število raziskovalcev, ki žele dostop v omrežje. **TCP/IP sprejmejo leta 1983 kot standard**, ki velja za celo hrbtenico ARPANETa. Večina novih namiznih računalnikov dela z operacijskim sistemom UNIX in TCP/IP postane kmalu sestavni del tega operacijskega sistema. Samostojna omrežja pospešeno nastajajo in se priključujejo ARPANETu.

V tem času ARPANET postane preobsežen in preveč pester, da bi ga še lahko obvladovala ena organizacija. Leta 1983 se razcepi v dve hrbtenici: ARPANET, ki ostane raziskovalno in razvojno omrežje ter MILNET, ki prevzame vojaški del nalog.

Zasnova ARPANETa se ni veliko spremenila od začetkov in z eksponentno rastjo omrežja postane to kmalu prepočasno. Leta 1986 začne delovati veliko hitrejša hrbtenica **NSFNET**. Vodi jo NSF - National Science Foundation. NSFNET temelji na mreži superračunalnikov, nameščenih na ameriških univerzah. NSF podpira razvoj in priključevanje novih omrežij tako, da financira ustrezni razvoj na ameriških univerzah. Uveljavitev enotnih pravil dela, ki jih uvedel TCP/IP in vloga NSF sta verjetno najpomembnejša faktorja v razvoju iz relativno omejenega ARPANETa v Internet, kot ga poznamo danes. Po svetu nastajajo številne javne in privatne hrbtenice, ki se zlivajo z NSFNET.

V 90-tih letih je tehnična zasnova Interneta ustaljena. Nove rešitve prinašajo predvsem hitrejši prenos podatkov, kar posledično prinaša tudi eksponentno rast količine informacij, ki so na Internetu na voljo javnosti. Vedno očitnejša postaja potreba po učinkovitejših orodjih za iskanje informacij in dostop do njih. V letih 1991 in 1993 se pojavita orodji **Gopher** in **World Wide Web**. Gopher omogoča hierarhično menujsko ureditev informacijskih virov, World Wide Web pa uvede v globalno omrežje idejo hipertekstnega povezovanja dokumentov. Leta 1994 se pojavita pregledovalnika Mosaic in Netscape, ki omogočita vključevanje nebesedilnih podatkov v dokumente na WWW.

Različni načine dostopi do internet

Dostop do internet je za končnega uporabnika možen preko internetnih provajderjev. Internetni provajderji so podjetja, ki zagotavljajo internetni dostop po eni ali več danes tehnologij. Ključni podatek je pasovna prepustnost za dolvlačenje in gorvlačenje podatkov. Internetne dostope lahko ovrednotimo glede na naslednje parameter.

Pasovna prepustnost

Pasovna prepustnost je ključni podatek hitrosti pretakanja podatkov. Osnovna enota je Baud, kar pomeni pretok enega bita na sekundo. Pri simetričnem priklopu gre za enako hitrost dolvlačenja in gorvlačenja podatkov, pri asimetričnem priklopu gre za različni hitrosti. Hitrosti pretakanja informacij se merijo v kBaud-ih, Mbaud-ih in pri pogovarjanju o t.i. hrbteničnih omrežjih je govora o Gbaudih. Tipična priklopna hitrost je recimo 1/1,5Mbaud U/D.

Plačevanje storitev

Poznamo plačevanje po količini prenesenih podatkov, pavšalno plačevanje na časovno enoto(ponavadi mesec), plačevanje po času uporabe povezave in mešano kombinacijo pravkar naštetih načinov plačila. Danes internetni provajderji večinoma zagotavljajo povezavo s plačilom pavšalnega mesečnega računa.

Tehnologijo priklopa

Danes so internetnim provajderjem na voljo ADSLX, optika, kabelska, brezžična, mobilna in satelitska tehnologija za prenos podatko do končne stranke.

ADSLX tehnologija izkorišča telefonsko parico, ki je še ostanek starih analognih telefonskih omrežij. Prednost je že obstoj omrežja in posledično začetna manjša investicija. Dosegajo se hitrosti do nekaj Mbaud.

Kabelska omrežja izkoriščajo stara analogna televizijska omrežja, ki so temeljila na koaksialnem kablu. Kabelska omrežja so lahko razprostranjena na nivoju celotnega mesta. Prednost je že obstoj omrežja in posledično začetna manjša investicija. Tudi tu se dosegajo hitrosti nekaj Mbaud.

Brezžična omrežja po standard IEEE802.16 omogočajo prenos internetnega signala do nekako 10 km in dosega prenosne hitrosti do 10Mbaud.

Mobilna omrežja, ki so bila prvotno namenjena predvsem prenosu digitalnega signala za prenos zvoka, se čedalje bolj uporabljajo za prostrano dostopnost internetnega signala. Zadnje generacije mobilnih omrežij že zagotavljajo prenosne hitrosti nekaj Mbaud, kar zadostuje za video pogovore, brskanje po internet in ostale storitve povezane z ip omrežji. Mobilna omrežja so zelo prostrana, saj pokrivajo medsebojno povezana večino svetovnega poseljenega področja. Provajderji priklop še vedno računajo po prometu.

Satelitska tehnologija omogoča dostope tam , kjerne moremo z nobeno drugo tehnologijo to so oceani. Še vedno je več kot 60% zemeljske oble pokrito z interenetom samo preko satelita. Za satellite je značilno plačevanje zelo dragega prometa , asimetrični priklopi, relativno velike antene na strain sprejema, zahteva outdoor delovanje in direkten pogled do satelita. Hitrosti , posebno pri infrastrukturnih povezavah so lahko zelo velike, nekaj 10 GBaud. Problem je tudi geostacionarna zakasnitev(0,4 sekunde) ali pa občasno nepokritje določenih predelov pri satelitih v nizki orbiti.

Pomena interneta za sedanjo družbo

Socialni

Socialni v smislu racionaliziranega sporazumevanja. Komuniciranje iz domačega naslonjala z raznimi socialnimi grupami, partnerji, družino. Nakupovanje preko iterneta, opravlanje vseh poslov preko internet, davčna uprava preko internet vse to nas dela učinkovite. Socialna plat internet a postaja po nekaterih raziskavah zelo pomembna v času velike mobilnosti in površnih realnih socialnih stikov.

Ekonomski

Internet kot univerzalni medij omogoča prenos informacij. Če sledimo modernim parolam o ceni informacije je očitno, da internetna industtrija neposredna ali posredno daje kruh velikemu procentu celotne populacije. Nenazadnje se to vidi pri % položnic, ki jih plačujemo vsak mesec. Če seštejemo najeme mobitelov, priklop na internet(Siol trio npr), ceno RTV naročnine pridemo do 30% in več od skupnih stroškov.

Izobraževalni

Izobraževanje na daljavo, iskalniki informacij, javni strežniki, moderne marketinške metode nam olajšajo življenje. Ogromno podatkov, za katere smo morali nekoč potovat nekam, dobimo s klikom na gumb, izobraževanje in vaje so dosegljive v virtualnih laboratorijih, elektronski pisemski nabiralnik nadomešča klasično pošto, elektronska pošta prevzema nove vsebine. Mladi in stari si vse najdemo in naučimo iz internet, vspostavlja se svetovna internetna knjižnica in še bi lahko naštevali

Zabava

Internetne igra, vizualizacije, virtualni svetovi, računalniško vodeni turnirji raznoraznih kategorij iger nadomeščajo klasično druženje ob kavici. Povezani smo tako virtualno, glasovno kot preko pogovora s stipkovnico. Specialni uporabni vmesniki, pisani za večino dobro znanih iger(šah tarok, dama) in pa razne strategije ki temeljijo na udeležbi junakov, ki jih vodijo igralci, so neizmeren vir zabave. In človek ki se zabava je zadovoljen, racionalen, troši malo energije.

Denarni

Internetne banke, portal, ki ponujajo zaslužek, portal ki ponujajo stave, portal ki prodajajo storitve, internetne trgovine, za vse to je potreben denar. V udobju naslonjača vlagamo na borzi, stavimo na ruletah, opravljamo določena opravila in služimo denar, in ta denar je pravi, ko ga dvignemo na bankomatu. Pravzaprav je največja svetovna banka s 480 komitenti že nekaj časa internetna banka PayPall, pa morda še druga na svetu s 110 miljoni komitenti AlertPay, to so multinacionalke prihodnosti, ki ponujajo neverjetno varnost, preglednost, statistično zagotovljeno spoštovanje. Mednarodni bančni system SWIFT zagotavlja prepoznavnost banke in njeno transparentnost, zagotavlja pa tudi univerzalno bančništvo. Stvar je tu, se je ne da ustaviti, rešeni so principi obdavčevanja.

Delo

Delo preko internet od doma je oblika, ki se čedalje bolj širi. Združuje in racionalizira mnoge stroške. Pravzaprav se vse kar ni povezano s fizičnim premikanjem stvari seli za računalnik, za specialne portale. Pogoj za delno ali kompletno delo od doma je opravljanje vseh opravil od doma. Opravila, ki jih ne moremo opraviti od doma pač opravimo fizično. Iskanje ravnovesja je ključno. Ljudje smo veliko bolj zadovoljni in iskoriščeni, ker nismo podvrženi uveljavljenim rutinskim urnikom, ki večini ne ustreza v smislu učinovitosti. Nekdo je neverjetno učinkovit od polnoči do 4 zjutraj, drugi je sposoben delati 56 ur skupaj potem pa naslednjih 56 ur spat in tako naprej

Racionalizacija

Internetna(ali računalniška) industrija je tudi požiralec ostalih vej industrije. TV se seli na internet, radio se seli na internet, oglaševanje se seli na internet, DVD –ji se ukinjajo stvari se naravno racionalizirajo in urejajo. Okno ki ga lahko živimo je omejeno navzdol z racionalnostjo življenja. Ravno racionalnost v primerjavi s ostalimi uporabniki je tisti vzvod, kin as sili k uporabi tehnologij, ki tako racionalnost omogočajo. Kaj hitro se lahko neracionalnemu lahko zgodi, da kljub pridnosti in hitrosti ne dohaja tistega, ki prvih dveh lastnosti ne obvlada najbolje, vendar mu racionalnost(učinkovitost) omogoča kvaliteto življenja.

Partnerstvo

Čedalje več na novo sklenjenih partnerskiz zvez temelji na spoznavanju preko internet. Ko se bomo otresli čustvenih blokad(tabujev), bomo pač primorani v tako obliko druženja. In ker zaenkrat otroka še ne moremo narediti z izmenjavo osbnih identifikacijskih ključev, nas tisti najlepši del na koncu še vedno čaka. Obstajajo statistike, ki kažejo na trajnejši odnos, na v povprečju večjo zaupljivost, so pa seveda ti portal polni pasti, ampak tudi klasičen način jih ima in to dokazano več.

RAČUNALNIŠKE KOMUNIKACIJE IN OMREŽJA II

DELOVANJE INTERNETA

IP usmerjanje in IP usmerjevalni algoritmi

Vsak mrežni segment ima en ali več prehodov(router). Ko naprava(računalnik) zahteva pošiljanje na naslov ki ni omrežni naslov lokalnega segmenta, se telegram pošlje na prehod(ruter). Tu se izgubi informacija o MAC naslovu in od tu dalje telegram potuje med ruterji z informacijo ciljnega IP naslova. Ko telegram pripšotuje do prehoda(ruterja), ki je na mrežnem naslovi cline naprave, se iz ARP tabele ruterja poišče MAC naslov ciljne naprave(računalnika) in se telegram pošlje na cilj.

Usmerjevalni protokoli vključujejo naslednje protokole:
- IGRP (Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System to Intermediate System)
- RIP (Routing Information Protocol).

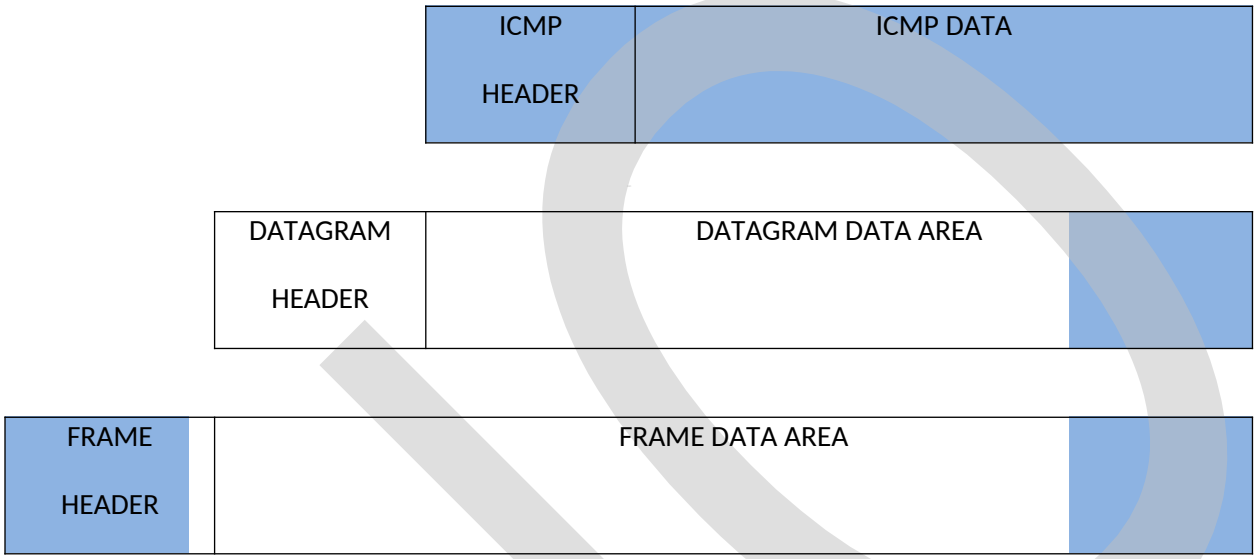
RIP: RIP je vektor razdalje, ki je bil prvotno izdelan za PUP (Xerox PARC Universal Protocol, leta 1980) in je bil uporabljen za XNS (leta 1981). RIP je bil širše osvojen šele s strani računalniško omrežnih prodajnih avtomatov. RIP je bil izdelan za razmeroma homogeno manjša oziroma skromnejša omrežja. V tem merilu je RIP kar precej uporaben oziroma koristen, v velikih omrezjih pa ima RIP kar nekaj slabih strani oziroma lastnosti. Zaradi teh svojih slabosti je bil RIP v mnogih primerih zamenjan z bolj modernimi usmerjevalnimi protokoli.
IGRP: IGRP je usmerjevalni protokol, ki je bil razvit v sredini 80-ih let s strani organizacije CISCO. IGRP je izdelan za uporabo v vecjih, zahtevnejših IP in OSI omrezjih. Da si zagotovi fleksibilnost IGRP dovoljuje več usmerjevalnih poti.
OSPF: OSPF je hierarhicni usmerjevalni protokol, razvit za IP omrezja s strani IETF (Internet Engineering Task Force). OSPF izhaja iz zgodnjejše verzije OSI's IS-IS usmerjevalnega protokola. OSPF usmerjevalniki so zmožni izračunati najkrajšo pot do sporozila.

Privatni IP naslovi

Privatni naslov IPv4 192.168.x.x nam omogočajo tvorjenje izoliranih omrežij. Lokalna omrežje se da omejeno povezovati na prostrana omrežja. Prehod med privatnim omrežjem in prostranim omrežjem je NAT in se mu v komercialnem jeziku tudi reče prehod ali ruter. Prednost privatega omrežja je priključitev cele Bklase (65000 naprav) na samo eno prostrano IP številko. Seveda so pri takem priključevanju določene omejitve.

ICMP protokol in njegove osnovne aplikacije

ICMP(Error And Control Messages)



Echo Request And Reply Message Format

Preverjanje prisotnosti (Pinganje) naprave uporablja paket ICMP ECHO (TYPE 8) v upanju da nam naprava vrne ICMP ECHO_REPLY(TYPE 0).

0	8	16	24	31
TYPE(8 or0)	CODE(0)	CHECKSUM		
IDENTIFIER		SEQUENCE NUMBER		
OPTIONAL DAT.				

Reports Of Unreachable Destinations

0	8	16	24	31
TYPE(3)	CODE(0-12)	CHECKSUM		
UNUSED(MUST BE ZERO)				
INTERNET HEADER+FIRST 64 BITS OF DATAGRAM				

Source Quench Format

0	8	16	24	31
TYPE(4)	CODE(0-12)	CHECKSUM		
UNUSED(MUST BE ZERO)				
INTERNET HEADER+FIRST 64 BITS OF DATAGRAM				

Route Change Request From Routers

0	8	16	24	31
TYPE(5)	CODE(0-3)	CHECKSUM		
ROUTER INTERNET ADDRESS				
INTERNET HEADER+FIRST 64 BITS OF DATAGRAM				

Detecting Circular Or Excessively Long Routes

0	8	16	24	31
TYPE(11)	CODE(0 or 1)	CHECKSUM		
UNUSED(MUST BE ZERO)				
INTERNET HEADER+FIRST 64 BITS OF DATAGRAM				

Reporting Other Problems

0	8	16	24	31
TYPE(12)	CODE(0 or 1)	CHECKSUM		
POINTER	UNUSED(MUST BE ZERO)			
INTERNET HEADER+FIRST 64 BITS OF DATAGRAM				

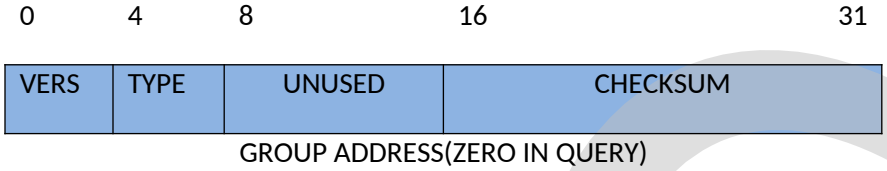
Clock Synchronization And Transit Time Estimation

0	8	16	24	31
TYPE(13 or 14)	CODE(0)	CHECKSUM		
IDENTIFIER		SEQUENCE NUMBER		
ORIGINATE TIMEST AMP				
RECEIVE TIMEST AMP				
TRANSMIT TIMES AMP				

Obtaining A Subnet Mask

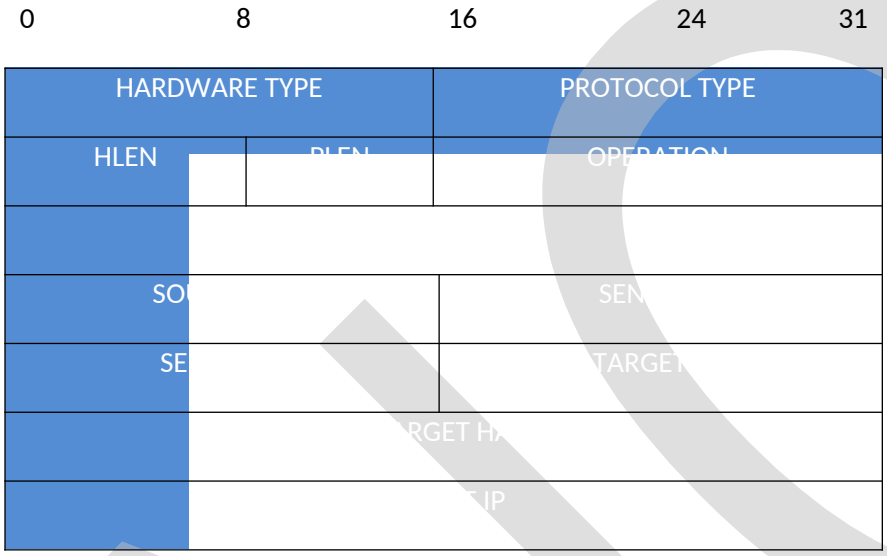
0	8	16	24	31
TYPE(17 or 18)	CODE(0)	CHECKSUM		
IDENTIFIER		SEQUENCE NUMBER		
ADDRESS MASK				

IGMP(Internet Multicasting) protokol in njegove osnovne aplikacije



Delovanje ARP in RARP protokola

ARP



ARP(Address resolution protocol) Je namenjen pridobivanju parov IP:HA(MAC). Naprava, ki želi zgraditi ARP tabelo IP:HA pošlje ARP telegram na Broadcast naslov(Host same 1). Vse naprave(računalniki) vrnejo ARP datagram z zahtevanimi podatki. Arp tabela se zgradi ob zagonu naprave, kasneje se dopolnjuje dinamčno, če naprava zazna na lokalni mreži še kakšno drugo dvojico IP:HA. Dolžina ARP telegram se spreminja glede na tip omrežja. Predstavljeni telegram velja za Ethernet omrežje, kjer je HA(MAC) dolg 6 oktetov.

Delovanje protokolov TCP in UDP

UDP(User Datagram Protocol)

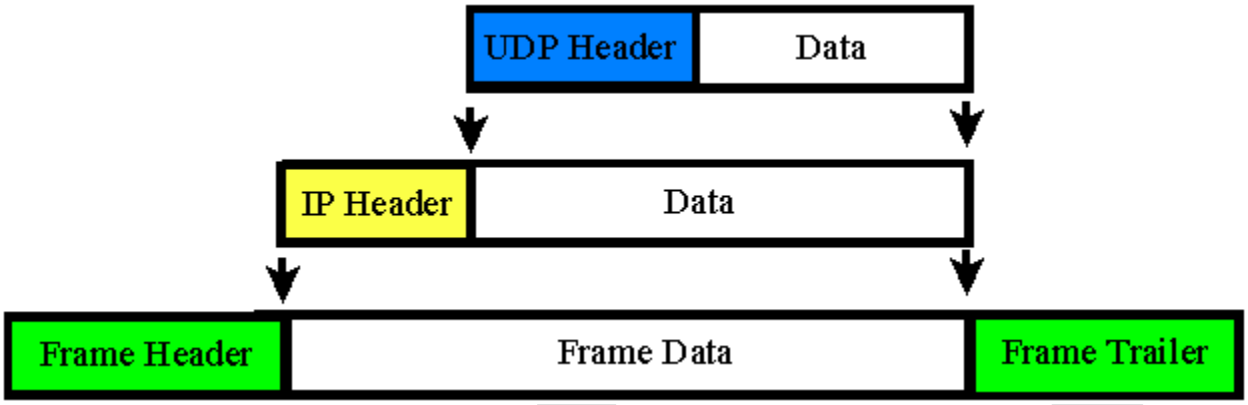
UDP provides an unreliable, connectionless delivery

Application programs using UDP are responsible for message loss, duplication, delay, out-of-order delivery, and loss of connectivity

Examples of applications that use UDP transport include Network Time Protocol (NTP), Sun's Network File System (NFS), and the Simple Network Management Protocol (SNMP)

Each UDP message is called a **user datagram**

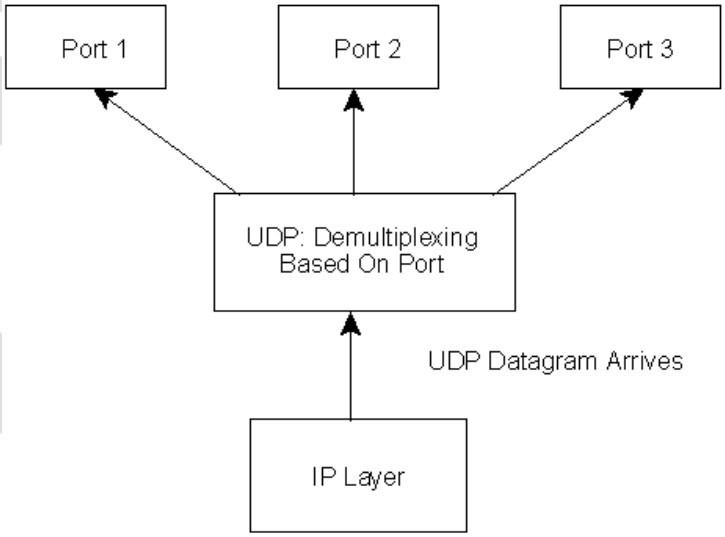
UDP Message Encapsulation



UDP Message Format

0	16	31
UDP SOURCE PORT	UDP DESTINATION PORT	
UDP MESSAGE LENGHT	UDP CHECKSUM	
DATA....		

UDP messages are stored in queues on destination host, one queue per destination port



TCP(Transmission Control Protokol)

TCP provides reliable, end-to-end data transmission with flow control

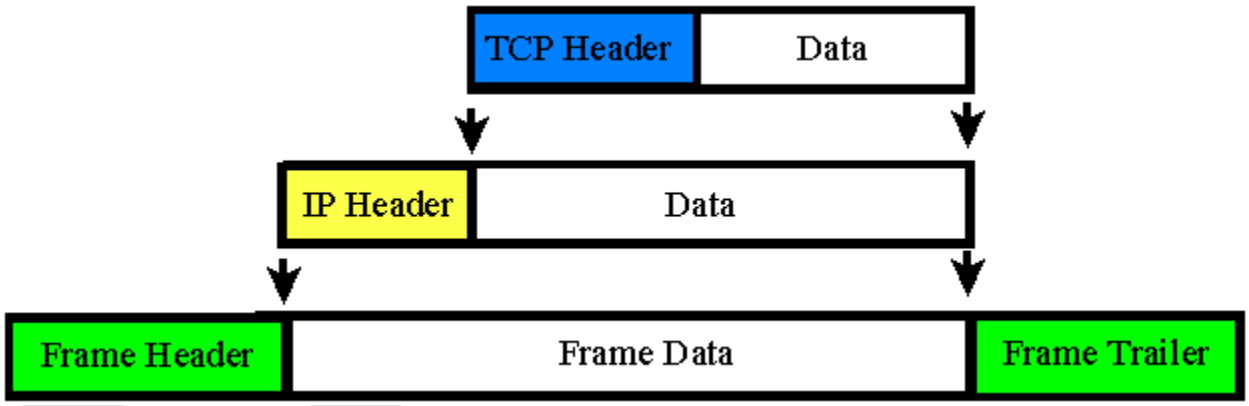
Examples of TCP applications include Telnet, FTP, WWW, POP, IMAP, etc.

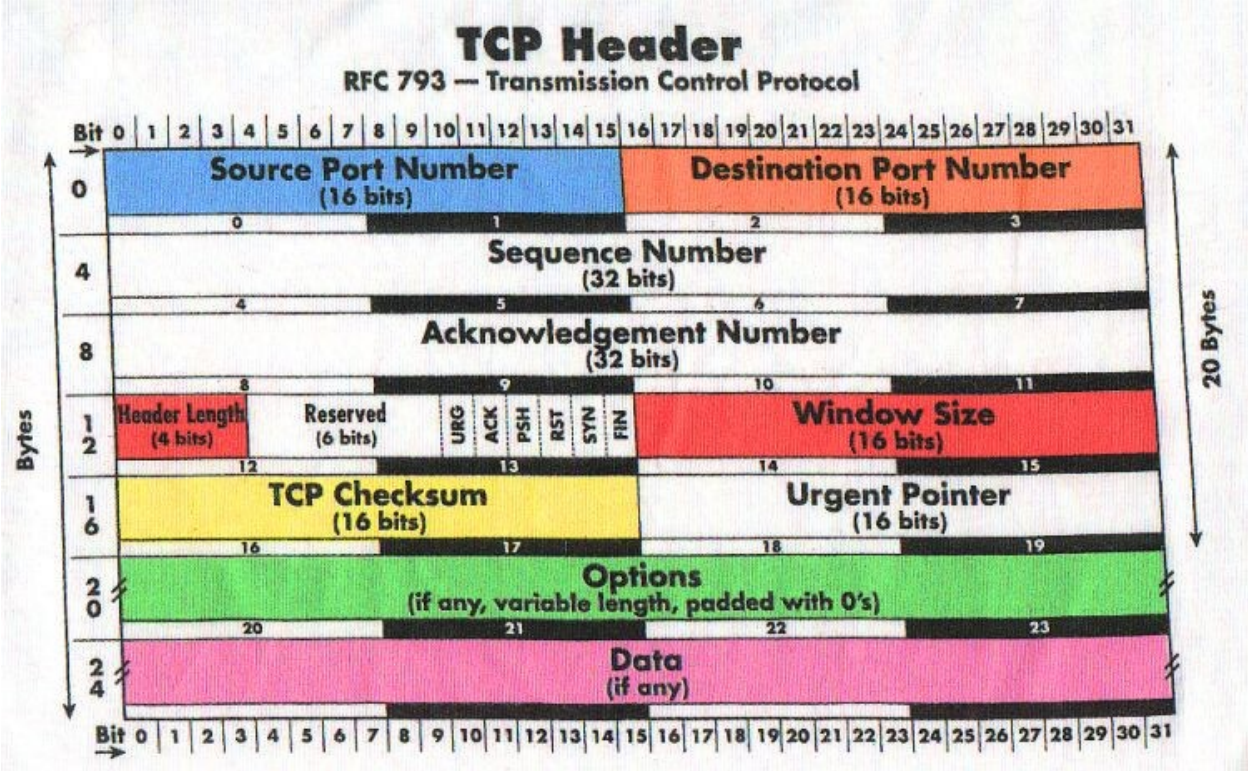
Basic features of TCP transmission:

- **Streamed Data** - Data from sender to receiver organized as a *stream* of bits divided into 8-bit bytes (data streams have no TCP imposed structure)
- **Buffered Transfer** - Applications send bytes to TCP software that delivers the stream of bytes in exactly the order sent (not necessarily grouped the same way)
- **Full-duplex Transmission** - Both hosts can send and receive data and control information independently

The unit of transfer in TCP is called a segment

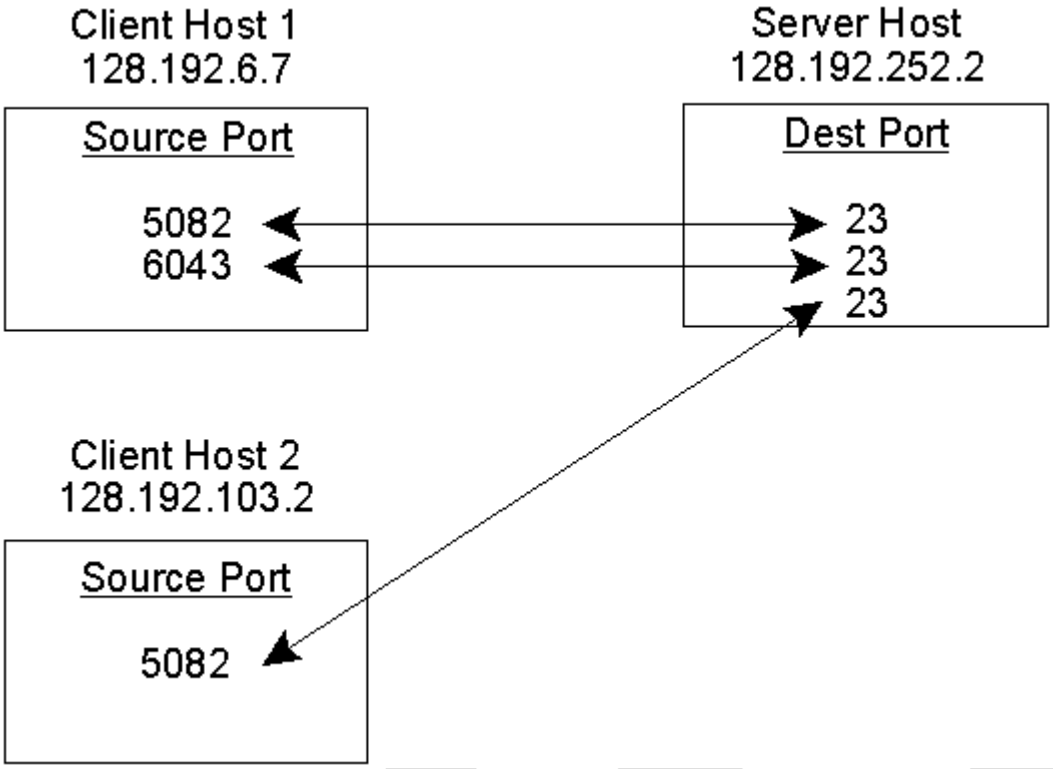
TCP Segment Encapsulation



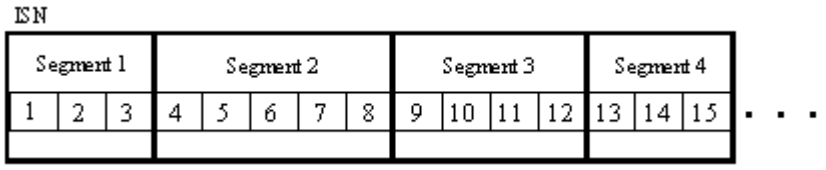


Connection defined by the pair of numbers (source IP, source port) and (dest IP, dest port)

Different connections can use the same destination port on server host as long as the source ports or source IPs are different


Client Host 1
128.192.6.7
Source Port
5082
6043
Server Host
128.192.252.2
Dest Port
23
23
23
Client Host 2
128.192.103.2
Source Port
5082

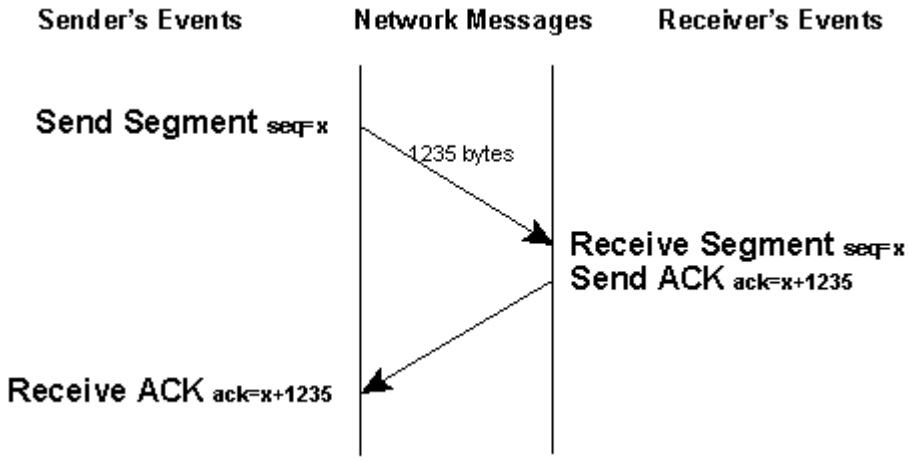
TCP breaks data stream into segments



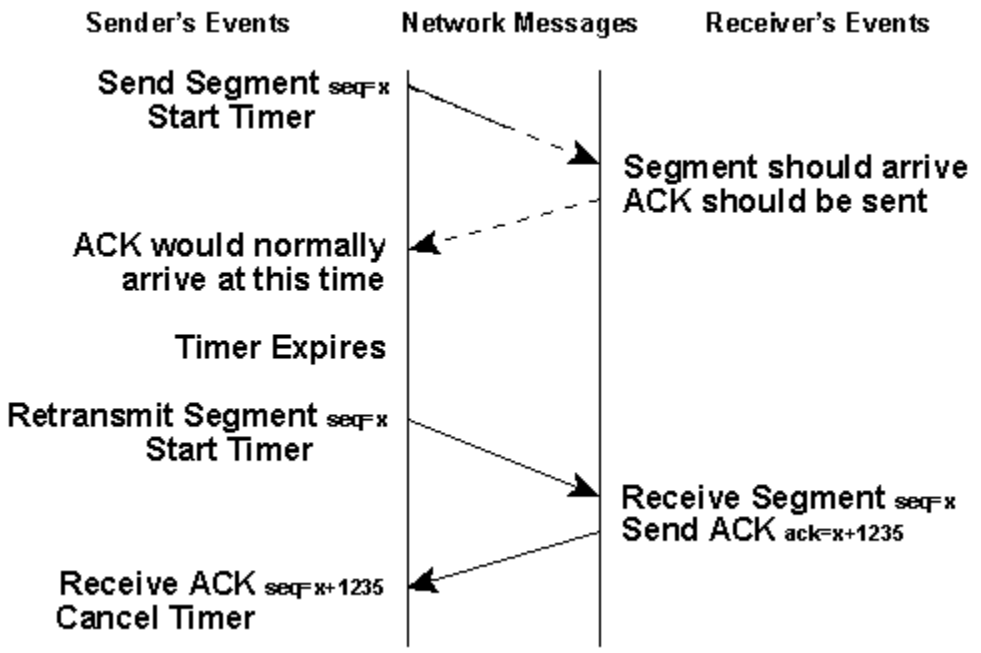
Sequence numbers used to place received segment data in the correct order

- Initial sequence number (ISN) marks the beginning of data stream
- ISN is random and negotiated when connection is established

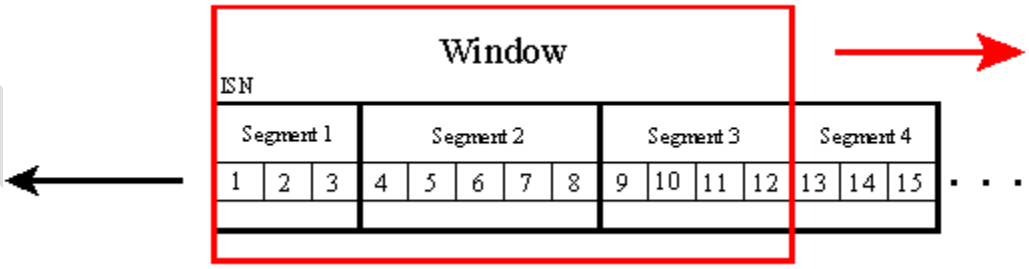
Acknowledgement numbers tell sender that receiver expects *next* segment



When a segment is sent, a timer is started; if an ACK has not been received when the timer expires, the segment is resent



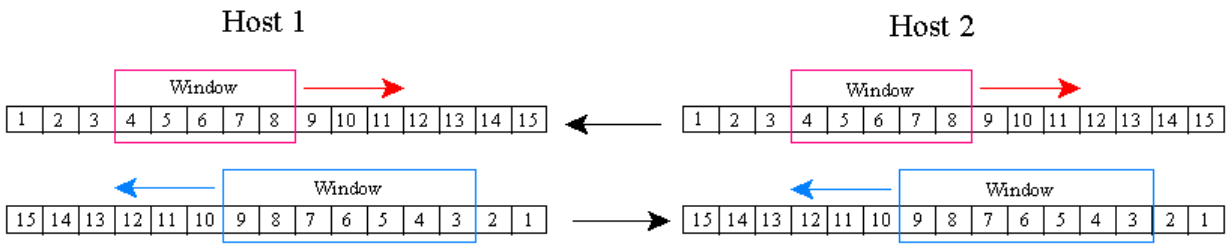
Sliding windows are used to transmit data stream efficiently and for flow control



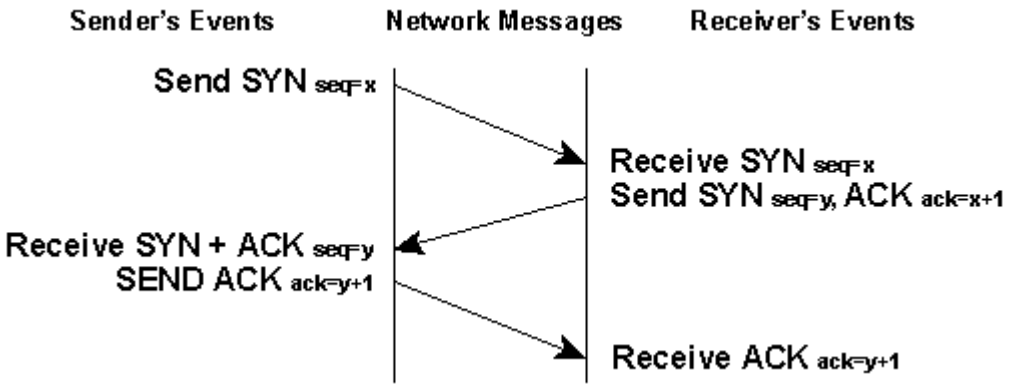
Receiver sends acceptable window size to sender during each segment transmission (flow control)

- if too much data being sent, acceptable window size is reduced
- if more data can be handled, acceptable window size is increased

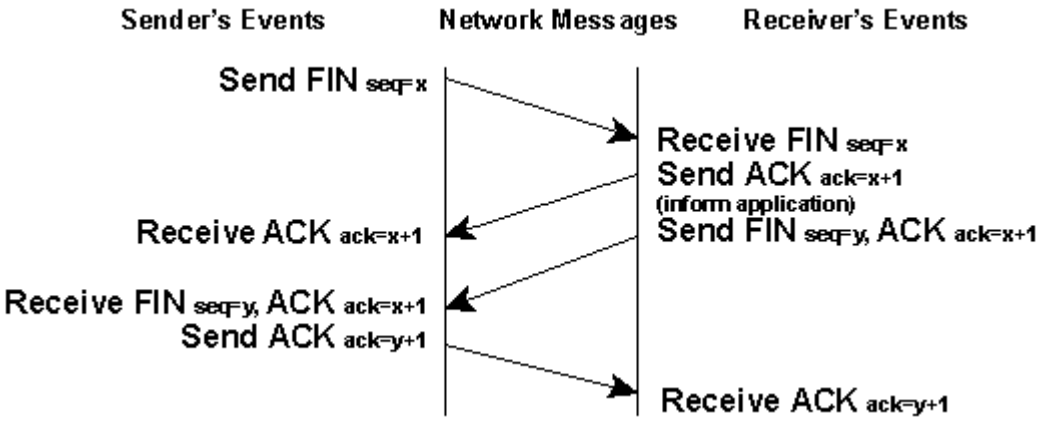
Actually four windows used, i.e., send and receive windows in both directions (full-duplex)



A TCP connection is established using a "three-way handshake"



A TCP connection is closed using a "modified three-way handshake"

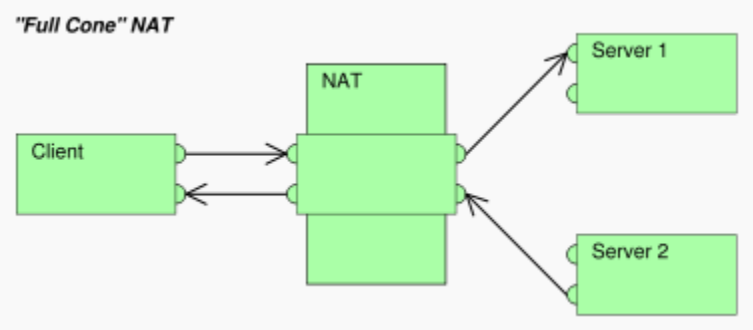


A TCP connection is aborted via a connection reset (RST bit set in the CODE field)

Sodobno zagotavljanje kvalitete storitve (QoS)

Protokol NAT

IPv4 ima premalo naslovnega prostora. NAT(Network address translation) je internetna storitev ki omogoča priključitev lokalne mreže Ipv4 preko ene zunanje IP številke v prostrano internetno omrežje.



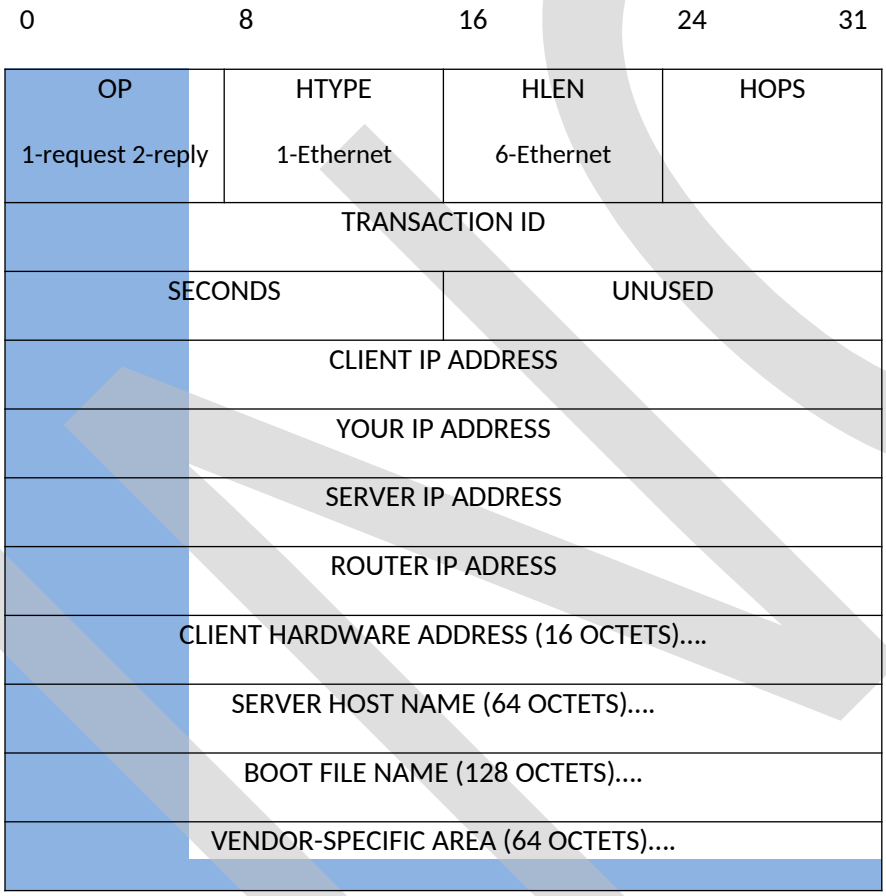
Za tvorjenje lokalnih mrež imama IPv4 rezervirano B klaso 192.168.x.x. NAT storitev zahteva mapiranje portov zunanje IP številke na notranje porte in IP številke.

Pri mapiranju ločimo med preusmerjanjem UDP in TCP telegramov.

BOOTP protocol

BOOTstrap Protocol(in DHCP) jealternatina RARP , uporabna za diskless računalnike, kjer je v mrežo povezanih veliko računalnikov brez diska in imajo boot program zapisan v ROM-u komunikacijske kartice. Ker so ti ROM-I enaki, koda ne more vsebovati IP nasalova.

BOOTP uporablja UDP telegram IP 255.255.255.255 za zahtevo vsem v segment mreže(limited broadcast). Klient ali server pošlje toliko informacij, kot jih ve, neznane naslove pusti na 0.0.0.0.



Ko Klient ve za svoje IP podatke, ime serverja in ime boot datoteke, lahko s pomočjo katerekoli storitve za prenos podatkov(npr TFTP) prenese boot datoteko in se zažene.

Delovanje DHCP protokola

Dinamic Host Configuration Protocol Message Format

0	8	16	24	31
OP	HTYPE	HLEN	HOPS	
TRANSACTION ID				
SECONDS		FLAGS		
CLIENT IP ADDRESS				
YOUR IP ADDRESS				
SERVER IP ADDRESS				
ROUTER IP ADRESS				
CLIENT HARDWARE ADDRESS (16 OCTETS)				
SERVER HOST NAME (64 OCTETS)				
BOOT FILE NAME (128 OCTETS)				
OPTIONS (VARIABLE)				

DHCP protocol omogoša avtomatično konfiguracijo računalnikov, ki nimajo statičnega IP naslova. DHCP zahteva je IGMP telegram, ki je namenjen vsem v lokalni mreži. To se dogaja v velikih lokalnih omrežjih, kjer ni potrebe po statičnem naslovu in nam ne dodeljevanje IP naslovov omogoča lažje vzdrževanje programske opreme. DHCP strežnik je lahko samo eden v segment. Ko prejme DHCP telegram, vrne odgovor pošiljatelju in v ta odgovor doda manjkajoče podatke za konfiguracijo omrežja. Podatki, ki manjkajo računalniku z dinamično IP konfiguracijo so predvsem IP naslov, IP podmaska in IP prehoda. Dodatno se ponavadi prenaša še podatek o DNS strežniku, ki naj ga računalnik obišče, ko zahteva pretvorbo domenskega zahtevka v IP naslov.

Vloga, pomen in delovanje DNS protokola

DNS(Domain name server) so strežniki za pretvorbo domenske zahteve v IP naslov strežnika. Organizirani so hierarhično z močno krovno kontrolo.

Delovanje standardnih protokolov aplikacijske plasti (http, ftp, smtp, ...)

POŽARNI ZID IN NAVIDEZNA PRIVATNA OMREŽJA (VPN)

Tipi vdorov in povzročena škoda

Tipi vdorov so tako raznovrstni, da je spodaj opisana klasifikacija le približna. V system vdre programmer, ki za svoje orodje uporabi program, pomankljivost sistema, neprevidnost uporabnika. Načinov vdora je toliko kot je idej pri zloveščih programerjih. Zato je borba proti vdorom stalna, tako kot je stalno pisanje in izmišljevanje novih načinov vdora.

Računalniški virusi

Računalniški virus je program, ki okuži druge računalniške programe in datoteke tako, da vanje shranjuje kopije svoje programske kode. Ko takšen okužen program ali datoteko uporabimo, se hkrati aktivira tudi virus. Kopije so pogosto namenoma nekoliko drugačne, da jih protivirusni programi težje odkrivajo, zato moramo protivirusne programe vedno sproti nadgrajevati z informacijami o novih virusih.

Črvi

Črv (angl. worm) je programček, ki se z razpošiljanjem samega sebe razmnožuje običajno preko omrežja (interneta), pri čemer uporablja poštne naslove iz poštnih programov (npr. Outlook Express). Črv lahko zaganja druge programe, se razpošilja na druge računalnike ter hkrati razpošilja tudi dokumente iz okuženega računalnika, sam po sebi pa ne spreminja datotek ali sektorjev na diskih. Hkrati lahko vsebuje kakšen drug virus (npr. trojanskega konja), ki ob okužbi omogoči oddaljen dostop do okuženega računalnika preko interneta. Črvi so nevarni predvsem zato, ker ne potrebujejo gostitelja, ampak se razširjajo samostojno in precej nenadzorovano, zato lahko močno obremenijo internet omrežje, lahko pa razpošiljajo tudi kakšne zaupne informacije

(dokumente) iz okuženega računalnika.

Trojanski konji

Trojanski konj je samostojen izvršljiv program, ki vsebuje uničevalno kodo. Tako kot pri mitološkem trojanskem konju tudi pri računalniških trojanskih konjih od zunaj ne opazimo, da v sebi skrivajo škodljivo jedro. Običajno se sami ne razmnožujejo, poškodujejo ali uničujejo pa podatke na spominskih medijih (diskih). Poleg tega omogočajo nadzor okuženega računalnika na daljavo (preko interneta), najbolj znana Trojanska konja pa sta Back Orifice in NetBus, ki omogočata napadalcu brisanje, kopiranje, upravljanje s programi, skratka popolni oddaljeni nadzor nad okuženim računalnikom.

Programske bombe

Programske bombe so samostojni programi, sicer namenjeni opravljanju nekega koristnega dela, ki pa imajo nekje v svojem jedru skrito škodljivo kodo, ki se aktivira, ko so izpolnjeni neki pogoji. Glede na tip teh pogojev jih delimo na časovne in logične.
Programske bombe so lahko napisane zaradi izsiljevanja ali maščevanja, lahko pa jih avtor napiše le za zabavo.
Bombe se ob izpolnitvi določenega pogoja (logične bombe) ali ob določenem času (časovne bombe) sprožijo in povzročijo podatkovno škodo ali pa je njihov namen le moteje uporabnika.

Hrošči

Hrošč (angl. bug) je napaka v izvornem besedilu programa, ki jo je programer pustil nenamerno in sama po sebi ni virus, vendar vseeno predstavlja nevarnost za sistem. Takšne »luknje« v programu namreč predstavljajo šibke točke sistema, ki jih lahko zlonamerneži preprosto in hitro izkoristijo za vdor v sistem in povzročanje škode. Pred kratkim je takšen hrošč v Microsoft Internet Information Services omogočil internetnemu črvu »Code Red« povzročitev ogromne škode po celem svetu, saj se Code Red brez omenjene napake v IIS sploh ne bi mogel širiti.

Naloge požarnega zidu

Večina organizacij priključuje svoje računalnike v internet z uporabo požarnega zidu. Požarni zid je računalnik, katerega glavna naloga je, da služi kot vratar med računalniki znotraj in zunaj organizacije (poizkuša preprečiti vdor v računalnike v organizaciji). S stališča strežnika, ki želi npr. računalniku v organizaciji dostaviti pošto, to lahko pomeni, da se ne pogovarja direktno s tem računalnikom, temveč s požarnim zidom.
Požarni zidovi so neke vrste usmerjevalniki. To je nek sistem ali skupina sistemov, ki uresničujejo organizacijsko varnostno strategijo med zasebnim omrežjem organizacije - Intranet in zunanjim omrežjem Internet. Varnostna strategija opredeljuje dovoljene storitve in dovoljene vstope, ter druga varnostna merila. Vloga požarnega zidu je v nadzorovanju: katere notranje storitve so lahko dostopne od zunaj, kateri zunanji porabniki imajo dovoljen dostop do dovoljenih notranjih storitev in do katerih zunanjih storitev (elektronska pošta, WWW, ...) imajo dostop notranji uporabniki. Da je požarni zid učinkovit, mora ves promet v in iz Interneta potekati preko požarnga zidu, kjer se nadzoruje. Požarni zid opravlja naslednje naloge

1. FILTRIRANJE (IP filtering): omejevanje strežniških dostopov na določene naslove IP, ali izključitev določenih naslovov IP iz strežniških dostopov.
2. KRIPTOGRAFIJA (Cryptography): veda, ki vsebuje načela sredstva in metode za transformacijo podatkov z namenom, skriti njihovo vsebino, dokazati njihovo avtentičnost, preprečiti njihovo modifikacijo, zagotoviti njihovo celovitost in preprečiti njihovo nepooblaščeno uporabo. Je eno od tehnoloških sredstev za zagotavljanje varnosti podatkov na informacijskih in komunikacijskih sistemih. Poznamo simetrične kriptosisteme (sinonim za kriptografijo skritega ključa) in asimetrične kriptosisteme (sinonnim za kriptografijo javnega ključa).
3. PAKETNO FILTRIRANJE(Packet filtering): 1) Tip požarnega zidu, ki prepušča, blokira, promet na podlagi filtriranja paketov IP. Paketno filtriranje je navadno prva obrambna črta. 2) Usmerjevalnik paketnega filtriranja prepušča/blokira promet na podlagi informacij v paketu
4. POŽARNI ZID APLIKACIJSKEGA PREHODA (Application gateway firewall): tip požarnega sistema, na katerem tečejo aplikacije proksi, ki imajo vlogo strežnika za odjemalce na Internetu. Strežnik proksi sprejme vse zahteve od odjemalca in (če so te dovoljene) jih pošlje strežniku v Intranetu. Aplikacijske prehode uporabljamo za zagotovilo, da odjemalec iz Interneta in strežnik v Intranetu komunicirata po ustreznem aplikacijskem protokolu.
5. PREHOD (Gateway): računalnik, ki povezuje dve omrežji, usmerja pakete IP in pretvarja protokole ali sporočila iz enega v drugo omrežje. V Intranetu ima strežnik proksi vlogo prehoda med zasebnim omrežjem in Internetom. "Prehod" je pogosto sinonim za usmerjevalnik.

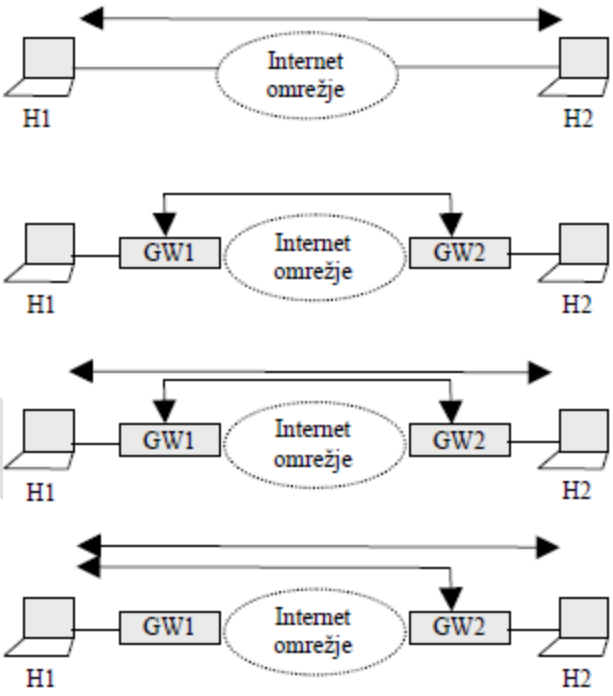
Princip navideznih privatnih omrežij in načini njihove izvedbe

Internet se je razvil v pomembno poslovno orodje, ki omogoča izmenjavo velike količine podatkov. Sem spadajo tudi podatki kritičnih aplikacij poslovnega procesa kot so proizvodna veriga, dobava, prodaja, poslovne in finančne transakcije. Zaradi potrebe po zaščiti podatkov, ki se prenašajo po javnem mediju,

je prišlo do razvoja navideznih zasebnih omrežij(VPN – Virtual Private Network). V primeru, da je prenosni medij IP omrežje, govorimo o navideznih zasebnih omrežjih na IP nivoju(IP VPN). Varno IP VPN omrežje je kombinacija tuneliranja(tunneling), šifriranja(encryption), avtentikacije(authentication), upravljanja in nadzora do virov. Pojem VPN obsega množico komunikacijskih standardov, ki omogočajo tuneliranje, enkripcijo in avtentikacijo podatkov. Med slednje spade tehnologija IPsec(IP security), ki definira različne vrste zvez med dvema ali več sistemi.

Arhitektura IPSec

IPsec temelji na ovijanju(encapsulation) in šifriranju prometa za namen prenosa preko IP omrežja. Povezava več lokacij se vrši s polno mrežo tunelovmed lokacijama ali z zvezdasto povezavo oddaljenih lokacij s centralno lokacijo. Infrastruktura je javni Internet, zato je treba dati poudarek tudi kvaliteti kvaliteti storitve prenosa preko javnega medija.

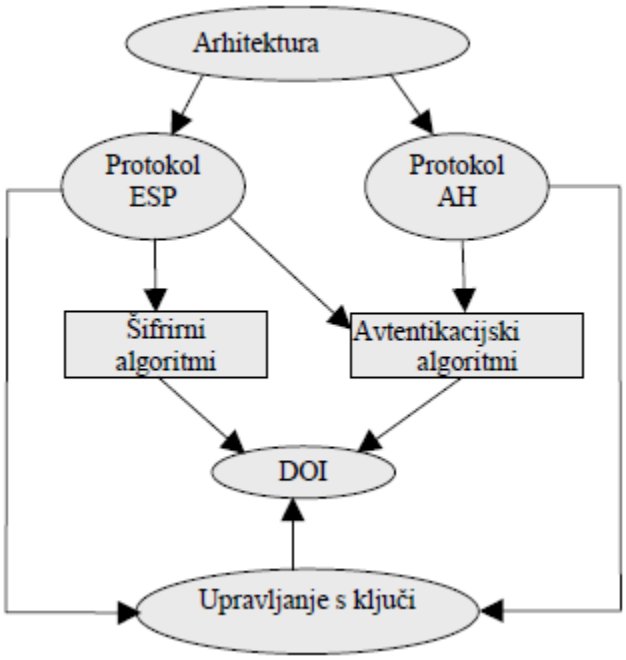


Za varnost je poskrbljeno saj so uporabljeni mehanizmi šifriranja(npr 3DES). Poleg koristne vsebine se lahko šifrira tudi glava IP paketa, celotni ip paket se nato ovije v drugi IP paket. Obstajata dva načina transportni in tunelski. Transportni se uporablja za zaščito protokolov višjih nivojev oziroma aplikacij. Pri komunikaciji dveh IPsec komunikacijskih naprav oziroma varnostnih prehodov(security getaway) se uporablja tunelski način. Pojem varnostni prehod označuje napravo, ki izvaja IPsec funkcije v korist tretjega sistema. Ob vzpostavitvi tunela med dvema točkama se na začetku izvrši še avtentikacija. Slika prikazuje različne vrste IPsec zvez med računalniškimi sistemi ali varnostnimi prehodi. V prvem primeru

dva računalniška sistema preko Interneta vzpostavita varno IPsec zvezo. V drugem primeru gre za komunikacijo med dvema varnostnima prehodoma, na katera sta priključena LAN segmenta. Komunikacija med prehodoma je zaščitena, ne pa tudi komunikacija med prehodom in končnim sistemom. Pomankljivost je odpravljena v tretjem primeru, kjer je dodatno zaščitena tudi zveza med končnima segmentoma. Tug re za gnezdo enega tunela v drugem. Zadnji primer predstavlja razmere, ko se računalniški system H1 najprej poveže s ponudnikom internetnih storitev H2, pridobi IP naslov, vspostavi IPsec tunel s ciljnim prehodom GW2, nato pa še tunel ali komunikacijo v transportnem načinu s končnim računalniškim sistemom H2. Značilnost IPsec tehnologije je varnost prenosa, ki je zagotovljena z močnim šifriranjem in avtentikacijo. IPsec naprava lahko vsebuje tudi požarni zid, s čimer zvezo še dodatno zaščitimo.

Načini zviševanja stopnje varnosti prenosov podatkov (IKE, SSL, ...)

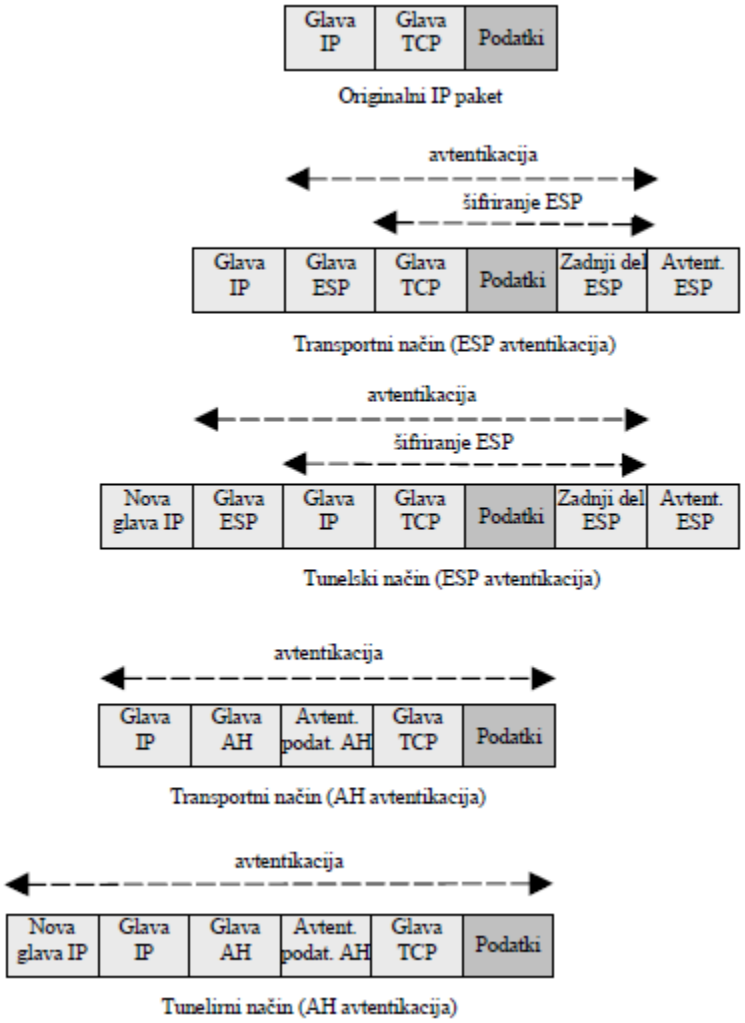
Tehnologije oziroma protokolni sklad IPsec opisujejo mnogi RFC dokumenti, ki so logično združeni v skupine.



Gradniki protokolnega sklada IPsec so.

- Arhihektura
- Protokol avtentikacijskega čela(AH – Authentication Header)
- Protokol šifriranja koristne vsebine(ESP – Encaptulation Security Payload)

- Šifrirni algoritmi
- Avtentikacijski algoritmi
- Domena interpretacije (DOI – Domain of Interpretation)
- Upravljanje s ključi



USKLAJEVANJE FIZIČNE URE

Potreba po usklajevanju ure na računalnikih

Praktično vsak računalnik ima v svojem drobovju fizično uro, kvarčni kristal, ki v primeru vzbujanja oscilira s točno določeno frekvenco. Sekundo določa točno določeno število nihajev kristala. V centraliziranem sistemu, kjer je ura ena sama, težav z usklajevenjem ure nimamo. Čim pa imamo sistem več računalnikov, vznikne vprašanje medsebojne usklajenosti posameznih ur. Če mora vsak računalnik poznati absoluten čas, govorimo o usklajevanju »pravih«, fizičnih ur (npr. Z radijskim signalom, ki ga oddaja dobro znani časovni strežnik). Včasih pa je dovolj že, da se računalniki dogovorijo med seboj, pri čemer ni tako pomembno, da dogovorjena vrednost (čas) res ustreza dejanskemu času. Tedaj govorimo o logičnih urah. Časovni strežnik lahko oddaja točen čas z radijskim signalom (pri tem so zakasnitve manjše in bolj predvidljive) ali pa po komunikacijsem omrežju. Znana radijska signala sta na primer angleški signal MSF iz Rugbyja in nemški signal DCF iz Frankfurta. V internetu najdemo tudi nekaj spletišč, ki ponujajo koordiniran univerzalni čas (UTC) ali mednarodni atomski čas (TAI); pogosto so to strežniki državnih inštitutov, oddelkov ali laboratorijev za meteorologijo.«[1]

Zakaj usklajevanje časa?[2]

1. Varnost: nujno je, da imajo računaliki, povezani v internet, točen čas, saj se v primeru vdora v sistem lahko na sodišču kot dokaz predložijo le dnevniki s točnimi časovnimi žigi.
2. Pregledi finančnega poslovanja in računovodstvo: vedeti moramo kdo in kdaj je spreminjal datoteke.
3. Avtentikacija: enkripcijski in avtentikacijski protokoli (npr. Kerberos) zahtevajo točen čas tako na strežniku kot na odjemalcu.
4. Porazdeljene datoteke: pomembno je, da se strežnik in odjemalci strinjajo glede časa, da so datoteke lahko sinhronizirane.

NTP protocol

Network Time Potocol (NTP) je protokol za sinhronizcijo časa preko omrežja. NTP je tudi program (ntp daemon with utilities), ki ta protokol izvaja in nadzira računalnikovo uro. Tako protokol kot program je razvil profesor David L Mills z univerze University of Delaware (ZDA) in ga še vedno vzdržuj. Zaradi visoke zanesljivosti in stroge skrbi pri ravnanju s časom, zaradi odprtokodne narave in zaradi enostavnosti uporabe, je veliko ljudi priravljenih prispevati k projektu in imeti korist od njega. To je zagotovilo, da bo NTP še nekaj časa ostal najboljši način za sinhroniziranje računalniških ur preko omrežja.

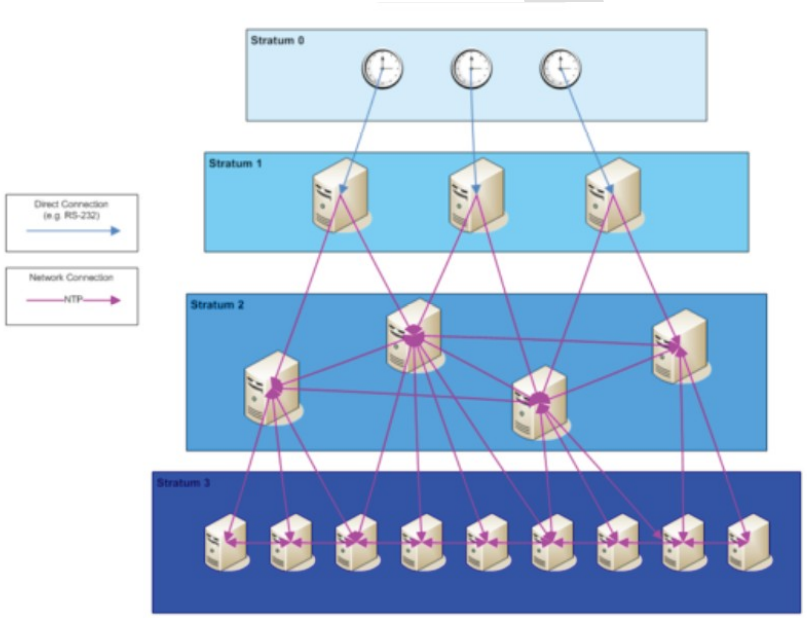
Kako deluje

NTP uporablja za sinhronizacijo računalnikove ure posebne algoritme, ki skrbijo (za razliko od preprostejših protokolov) za zveznost in monotonost računalnikovega časa - skokovite spremembe časa ali preskok časa nazaj imajo lahko neprijetne posledice na delovanje programov. Uravnavanje časa je izvedeno z izmenjavo kratkih občasnih paketov z NTP strežniki. NTP omogoča časovno sinhronizacijo

prek interneta s točnostjo okrog 10 milisekund in prek krajevnih omrežij s točnostjo okrog 200 mikrosekund in pri tem le zanemarljivo dodatno obremenjuje omrežje in računalnik.

Hierarhija NTP strežnikov.

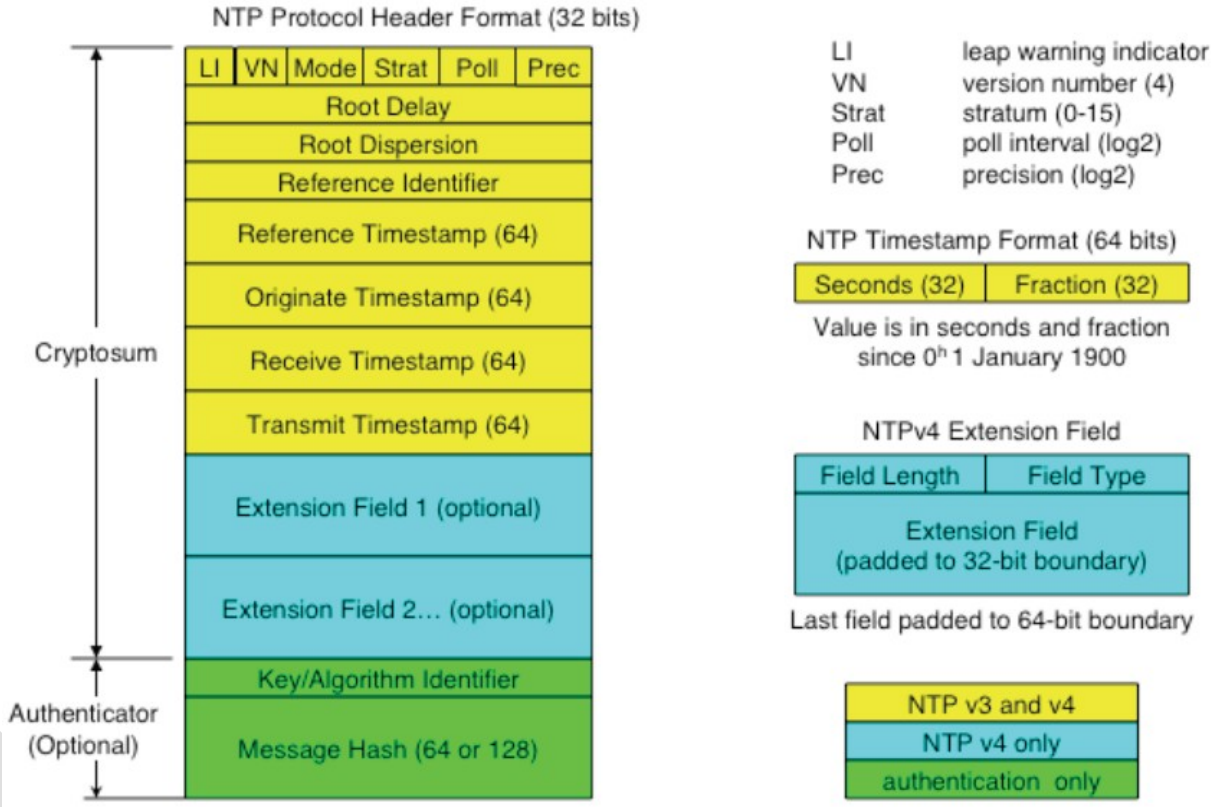
Strežniki na prvem nivoju (Stratum 1) so sinhronizirani z napravami, ki imajo karseda točen čas (koordinirani univerzalni čas UTC), npr. atomske ure, GPS ure ali ure, ki točen čas sprejemajo preko radijskih signalov. Strežniki na drugem nivoju (Stratum 2) so posredno ali neposredno sinhronizirani s primarnimi strežniki. Na najnižjem nivoju, v listih drevesa, so procesi, ki se izvajajo na uporabniških računalnikih. »Ure strežnikov niže v hierarhiji so verjetno manj točne kot ure strežnikov, ki so više v drevesu. Če kateri od strežnikov izpade ali postane nedosegljiv, se drevo preoblikuje. Če izgine izvor signalov UTC, se primarni strežnik prelevi v sekundarnega in se uskladi s katerim drugim sekundarnim strežnikom.«



Format NTP paketov

NTP paket je setavljen iz zaporedja 32-bitnih besed, sestavljen je iz treh komponent: glave (rumena), enega ali več razširitvenih polj (turkizna) in dela za avtentikacijo (message authentication code, MAC, zelena), ki ni obvezen. Leap Indicator (LI): 2-bitni indikator, ki opozarja, da se bo zadnji minuti dneva odvzela ali dodala sekunda. Version Number (VN): 3-bitna celoštevilska vrednost, ki podaja NTP/SNTP številko verzije. Mode: 3-bitno celo število predstavlja način usklajevanja, ki je lahko simetrično aktivni, simetrično pasivni, odjeamlec, strežnik, oddaja. Vrednosti 0, 6 in 7 so rezervirane. Stratum: 8-bitno nepredznačeno celo število, ki pove stopnjo strežnika (Stratum). Stopnje so od 0 do 15, ostale vrednosti so rezervirane. Poll Interval: 8-bitno predznačeno celo število, ki predstavlja dolžino interval med dvema uspešnima sporočiloma v sekundah. Možne vrednosti so med 4 (16 s) in 14 (16284 s). Navadno se uporabljajo vrednosti med 6 (64 s) in 10 (1024 s). Precision: 8-bitno predznačeno celo število, ki

predstavlja natančnost lokalne ure. Root Delay: tudi round-trip delay, 32-bitno predznačeno število s fiksno vejico, predstavlja zakasnitev zaradi prenosa po omrežju. Od nekaj milisekund, do nekaj sto milisekund. Root Dispersion: 32-bitno nepredznačeno število s fiksno vejico. Skupaj z root delay se uporablja za računanje sinhronizacijske razdalje med vrstniki (peer synchronisation distance). Reference Identifier: 32-bitno število, ki identificira zunanji referenčni vir.



Načini usklajevanja[8]

1. Večtočkovno oddajanje se uporablja v hitrih krajevnih omrežjih. En ali več strežnikovperiodično odda večtočkovno sporočilo (ki vsebuje trenutni čas) preostalim računalnikom. Ti ustrezno uskladijo svoje ure in pri tem upoštevajo tudi predvideno komunikacijsko zakasnitev sprejetega sporočila. Pričakovana točnost pri tem ni ravno visoka, vendar za mnoge namene popolnoma zadošča.

2. Proceduralni način se uporablja, kadar želimo doseči večjo točnost kot pri večtočkovenem oddajanju, pa tudi kaddar večtočkovno oddajanje ni izvedljivo. Delovanje je podobno kot pri Christianovemu načinu: strežnik sprejme zahtevo in odpošlje odčitek svoje ure.

3. Simetrični načni se uporablja, kadar želimo doseči čim višjo točnost, na primer na višjih nivojih drevesa. Pri vsaki sinhronizaciji namreč lahko pričakujemo uvedbo majhne napake, ki se kopičijo niže v drevesu. Zato je toliko pomembneje, da so išjenivojski strežniki čim bolj točni.

NAMEŠČANJE IN KONFIGURIRANJE STREŽNIŠKE PROGRAMSKE OPREME

Glavni servisi komunikacijskih strežnikov

Http strežnik, ftp strežnik, smtp strežnik, VPN strežnik, remote access strežnik, dhcp strežnik, mail strežnik, telnet strežnik

Načini konfiguracij in parametri

Spletnega strežnika

Spletni strežniku se določi korensko mapo. Za vsako podmapo je potrebno določiti predpostavljeno datoteko. Predpostavljena(default) datoteka je tista datoteka , ki se zažena ko zahtevamo to mapo. V primeru, da dahtevamo neobstoječo datoteko, nam strežnik, če mi tako želimo izpiše vsebino mape. Seveda izpis imenika dovolimo izjemoma, ker je to podatek, ki ga želimo ponavadi skrivat. Pri spletnem strežniku lahko določimo odziv strežnika na raznorazne napake.

FTP strežnika,

Ftp strežniku najprej določimo korenski imenik. Korenski imeniki in pravice dostopa se lahko vežejo na uporabnike. Tako ima vsak uporabnik svojo mapo, kamor lahko odlaga svoje datoteke. Ponavadi se FTP storitev nastavlja skupaj s storitvijo Http.

INDUSTRIJSKE MREŽE ZA PRENOS PODATKOV

Posebnosti, ki so značilne za industrijska omrežja,

Že samo ime **industrijski ethernet** nakazuje na to da gre načeloma za ethernet fizični nivo po OSI modelu, pridevnik industrijski pa nazornejše prikazuje, da gre za omrežje, ki povezuje naprave za industrijsko oz. produkcijsko rabo v industrijskem okolju.

Industrijski Ethernet je tehnologija osredotočena na proizvodnjo, obdelavo in nadzor za razliko od standardne informacijske tehnologije, ki je osredotočen uporabnika. Industrijski Ethernet (IE) se osredotoča na proizvodnjo dobrin, z tehnološko dovršenimi procesi, kjer izmenjava informacij na relaciji stroj-stroj, človek-stroj ali stroj-človek igra bistveno vlogo in dodaja proizvodnemu procesu in končno tudi izdelku bistveno dodano vrednost, glede na proizvodne tehnologije brez komunikacij.

Industrijski Ethernet je zasnovan tako, da omogoča nadzor in prosti pretok informacij nad proizvodnim procesom. Preko medsebojno povezanih podsistemov (elementov kot npr. PLC krmilnik, Periferna enota, ...) omogoča prenos in spremljanje številnih proizvodnih parametrov, ki tradicionalno izvirajo iz analognega sveta. To so npr. temperatura, vlažnost, pH, tlak, pretok, viskoznost, gostota, teža, vibracije, navor , RPM, napetost, tok, sevanje, itd.

IE (Industrijski Ethernet) kompatibilne naprave, se po svojem delovanju veliki meri ne razlikujejo veliko od naprav iz klasičnega IT sveta. Ker so te naprave običajno izpostavljene neprijaznim industrijskim okoljem (vlaga, temperature, vibracije, elektro-magnetni vplivi) so le te izdelane z upoštevanjem višjih standardov. Gre predvsem za robustnejše dizajne ohišij in napajalnih vezij ter izbiro zaneslivejših elektronskih komponent, ki omogočajo strožje MTBF (Mean Time Between Failure) in EMI (Electro Magnetic Interference) zahteve.

Topologije industrijskih omrežij za prenos podatkov,

Topologija je zelo podobna topologiji klasičnih IT mrež.

Razlika med pisarniškim in industrijskim Ethernetom

LASTNOST	PISARNIŠKI ETHERNET	INDUSTRIJSKI ETHERNET
IP zaščita	IP20	IP65/IP67
napajanje	230VAC	24VUC
montaža	namizna	na nosilne letve v zaščitnih omarah
oblika	ležeča namizna	miniaturna za nosilne letve
temperatura delovanja	0°C do 40°C	0°C do + 55°C oz v klima ohišjih -40°C do +70°C
občutljivost na tresljaje	-	2g
občutljivost na udarce	-	15g
izvedba hlajenja	ventilator	pasivno preko ALU hladinih teles
odpornost na umazanijo	prah	prah, olje, čistila
kemična odpormost	ni odporen na agesivno atmosfero	odporen na agresivno atmosfero
preiskusi za varnost	standard EN 60 950	standard EN 60 950
preiskusi za odpornost na EMC	standard EN 50 081-1 pisarniški	standard EN 50 081-2 industija
	standard EN 50 082-1 pisarniški	standard EN 50 082-2 industrija
		standard EN 50 155 za železnice
reakcijski čas	večji od 100 mili sekund	manjši od 20 mili sekund - realni čas
življenska doba	večja kot 3 leta	večja kot 3 leta
rezervni deli	4 leta	10 let
topologije mrež	zvezdasta, drevesna	linijska-BUS, zančna-RING, drevesna-TREE, zvezdasta-STAR
prenos podatkov	veliki paketi (tudi slike, itd)	mali paketi (merilni, krmilni) podatki
tip prenosa	neperiodičen	periodičen
čas prenosa	sekundni	mikrosekundni

Seznanitev z značilnostmi industrijskega Etherneta.

V preteklosti, so lahko računalniški sistemi za avtomatizacijo npr. PLC krmilnik komunicirali z drugimi napravami le preko sebi lastnih ali redkih odprtih protokolov, kot so Modbus, Sinec H1, Profibus, CANopen, DeviceNet ali FOUNDATION Fieldbus.

Danes je stvar enostavnejša in komunikacija med napravami v industrijskem okolju je mogoča po enotnem industrijskem ethernet omrežju, vsaj kar se tiče fizičnega nivoja (Glej OSI model). Na višjih nivojih proizvajalci še vedno uporabljajo sebi lastne protokole, ki ki omogočajo povezavo naprav istega proizvajalca ali zgolj istega tipa. Obstajajo pa tudi odprti standardi za komunikacijo preko industrijskega etherneta, kot je naprimer Modbus over TCP, ki je že podprt s strani večjih svetovnih proizvajalcev krmilne opreme.

Prednost

Povečana hitrost prenosa, na do 1Gbit/s s IEEE 802 z Cat6 kabli ali preko optičnih povezav

Povečala splošna storilnost
Povečana razdalja
Zmožnost uporabe standardne ethernet aktivne mrežne opreme: dostopne točke, usmerjevalniki, stikala. Kabli in optična vlakna, so mnogo cenejši kot pri namenskih kablih za serijske komunikacije vključno z napravami za zaključitev linije (terminatorji)
Zmožnost povezave več vozlišč (omejitev na 2 vozlišči pri RS232 povezavah)
Stare Master-Slave arhitekture nadomeščajo Peer-to-peer arhitekture, ki jih poznamo iz sveta interneta
Boljša interoperabilnost

Slabosti

Obstoječe komunikacije je načeloma težko seliti na IE arhitekturo, to ponavadi zahteva kar selitev celotnega sistema vodenja na novejšo arhitekturo kjer je IE podprt (čeprav obstajajo vmesniki za “tuneliranje” serijskih komunikacij preko IE)

Uporaba za relalnočasne aplikacije lahko trpi zaradi TCP protokola, ki po svoji naravi ni deterministične (za realnočasne aplikacije že obstajajo nadgradnje IE npr. Siemensov ProfiNET)

Upravljanje celotnega TCP / IP sklada je bolj zapleteno kot zgolj pošiljanje in prejemanje podatkov. Kot naprimer pri serijski komunikaciji.

Minimalni Fast Ethernet podatkovni okvir obsega 80 bytov, medtem ko so tipične industrijske komunikacije podatkovnih velikosti okoli 1-8 bajtov. To pri uporabi v industrijskih komunikacijah pripelje do učinkovitosti, ki je le okoli 5%. To znižuje prednosti višje hitrosti prenosa napram serijskim komunikacijam z nižjo hitrostjo.

Na Gigabit Ethernet je minimalna velikost podatkovnega okvirja 512 bytov, kar še dodatno zmanjšanje učinkovitosti tipično na manj kot 1%.

Nekateri industrijski ethernet protokoli že uveljavljajo spremembe, ki zmanjšujejo efekt te slabosti.

Primerjava IPv4 - IPv6

Naslovi

Ipv4

Ipv4 ima samo 4 byte naslovnega prostora(4.294.967.296), kar je glavna pomankljivost.

1	7	24	Razred A	Od 0.0.0.0
0	mrežni del(127)	Uporabnik(16.777.216)		Do 127.255.255.255
2	14	16	Razred B	Od 128.0.0.0
10	mrežni del(16.384)	Uporabnik(65536)		Do 191.255.255.255
3	21	8	Razred C	Od 192.0.0.0
110	mrežni del(2.097.152)	Uporabnik(256)		Do 223.255.255.255
4	28		Razred D	Od 224.0.0.0
1110	skupni naslov(268.435.456)			Do 246.255.255.255
5	27		Razred E	Od 247.0.0.0
11110	Rezervirano(134.217.728)			Do 255.255.255.255

Ipv6

Ipv6 ima 16 bytov naslovnega prostora(3,402823669209384634633746074317e+38)

Vrsta dodelitve	Oznaka(binarna)	Delež naslovnega prostora
rezerviran	0000 0000	1/256
nedodeljen	0000 0001	1/256
rezerviran za dodelitev NSAP	0000 001	1/128
rezerviran za dodelitev IPX	0000 010	1/128
nedodeljen	0000 011	1/128
nedodeljen	0000 1	1/32
nedodeljen	0001	1/16
nedodeljen	001	1/8
individualni naslovi za ponudnike	010	1/8
nedodeljen	011	1/8
geografsko razporejeni individualni naslovi	100	1/8
nedodeljen	101	1/8
nedodeljen	110	1/8
nedodeljen	1110	1/16
nedodeljen	1111 0	1/32
nedodeljen	1111 10	1/64
nedodeljen	1111 110	1/128

nedodeljen	1111 1110 0	1/512
lokalno naslavljanje(link local)	1111 1110 11	1/1024
lokalno naslavljanje(site-local)	1111 1110 10	1/1024
skupni naslovi	1111 1111	1/256

Skupni naslovi

Anycast je nov način pošiljanja preko skupnih naslovov v IPv6. Uporablja se v IP Multicast, Internet Relay Chat, Network News Transfer Protocl, Protocol for SYnchronous Conferencing, Web onferencing (WWCP). Omogoča enkraten prenos podatka, dokler je to mogoče. To je bistvena izboljšava v primerjavi z IPv4.

Unicast

Pošlji temu naslovu

Multicast

Pošlji vsem članom skupine

Anycast

Pošlji kateremu koli članu skupine

Čelo

Čelo datagrama IPv6 je v primerjavi z datagramom IPv4: preprostejše zgradbe, fiksne dolžine (40 zlogov), manj polj v čelu (Ipv4 - 14, ipv6 - 8).

Razširitvena čela

V IPv6 so za razne opcije predvideni razširitvena čela, ki vprimeru uporabe sledijo čelu IP v zapisanem vrstnem redu:

		Dolžina v oktetih	status
	Naslednje čelo Čelo datagrama Ipv6 (IP v6 header)	40	obvezen
Naslednje čelo	Opcije etap (Hop-by-hop option header)	spremenljiva	opcija
Naslednje čelo	Usmerjanje	spremenljiva	opcija

(Routing header)			
Naslednje čelo		spremenljiva	opcija
	Nadzor drobljenja datagrama (Fragment header)		
Naslednje čelo		spremenljiva	opcija
	Preverjanje avtentičnosti (Authentication header)		
		spremenljiva	opcija
	Javni enkripcijski ključ (Encapsulating security payload header)		
Naslednje čelo		spremenljiva	opcija
	Čelo z opcijami cilja (destination option)		
	Čelo TCP	20	obvezen
	Do 64k oktetov podatkov s preveritvenim kodom na koncu		

Čelo opcij etap(Hop-by-Hop options header)

Čelo z etapnimi opcijami Vsebuje informacije, ki jih mora, če je čelo prisotno, preveriti vsak usmerjevalnik na poti datagrama.

0	8	16	31
Naslednje čelo	Dolžina		
	Opcije		

Sestavljajo ga tri polja:

Naslednje čelo (8 bitov) Pove tip naslednjega čela

Dolžina čela (8 bitov) Dolžina čela je podana v 64 bitnih enotah

Opcije Polje nastavljive dolžine vsebuje eno ali več opcijskih določil. Vsako določilo ima tri podpolja:

1. tip opcije (8 bitov)
2. dolžina podatkov opcije (8 bitov)
3. podatki

Tip opcije je razdeljen v tri dele:

1. spodnjih 5 bitov določa opcijo,

2. Zgornja 2 bita določata akcijo, če naprava ne prepozna opcije:
00 preskoči to opcijo in nadaljuje z obdelavo ostalih opcij
01 zavrži paket
10 zavrži paket in z ICMP pošlji na naslov pošiljatelja sporočilo problem s parametri_ (koda 2) z označbo neznan tip opcije
11 zavrži paket in z ICMP pošlji na naslov prejemnika, če ta ni skupinski, sporočilo problem s parametri (koda 2) z označbo neznan tip opcije
3. tretji bit določa, ali se na poti med pošiljateljem in prejemnikom datagrama lahko spremenijo podatki opcij.
Do leta 1997 je bila definirana le ena opcija: jumbo payload
orjaški paket, daljši od 65 536 oktetov.

V primeru te opcije:

1. podatek v opciji določa dolžino podatkov v datagramu
2. najdaljši orjaški datagram je dolg okoli 4 milijarde, oktetov podatkov, kar zadošča za prenos zelo velike video datoteke,
3. v dolžino podatkov v čelu IP so zapisane ničle
4. prepovedana je uporaba fragmentacijskega čela.

Čelo usmerjanja(Routing header)

Čelo za usmerjanje. Vsebuje navodila za usmerjanje datagrama skozi medomrežje. Čelo usmerjanja omogoča pošiljatelju datagrama določitev poti preko točno določenih naprav v medomrežju. Zato se za to čelo v angleški literaturi uporablja tudi ime Source Routing.

Generična oblika čela ima določena naslednja polja

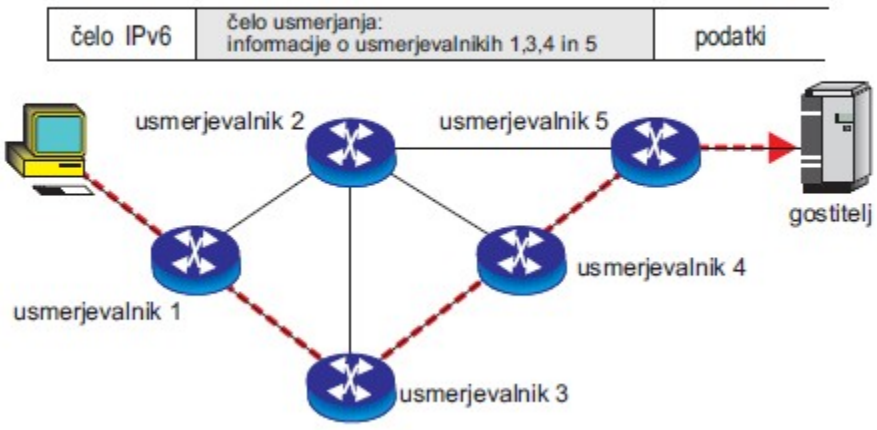
0	8	16	31
Naslednje čelo	Tip usmerjanja	Dolžina čela	
Opcije			

naslednje čelo (8 bitov), pove tip naslednjega čela
tip usmerjanja (8 bitov), določa tip usmerjanja
dolžina čela (8 bitov), določa število naslovov v čelu
preostale etape (8 bitov), vsebuje število etap, ki jih mora datagram še prehodoti do končnega cilja
rezervacija (32 bitov), za bodočo uporabo podatki usmerjanja (dolžina odvisna od tipa usmerjanja),specifični za tip usmerjanja
Če usmerjevalnik ne prepozna tip usmerjanja, paket zavrže. Do sedaj je bil definiran le tip usmerjanja 0
določa naslednja polja

0	8	16	31
Naslednje čelo	0	Število naslovov	Naslednji naslov
rezervirano			
Naslov1			

Naslov2
.....
Naslov n

Splošna zgradba čela usmerjevanja pri usmerjanju skozi n usmerjevalnikov.
Število naslovov (8 bitov), dolžino čela izrazi s številom zapisanih naslovov. V enem čelu jih je lahko največ 23.
naslednji naslov (8 bitov) vsebuje indeks naslednjega naslova,pošiljatelj ga postavi na nič.
rezervacija (8 bitov), ni definirano
maska striktnosti (24 bitov), bitov maske od leve proti desni označujejo zaporedne naslove usmerjevalnikov. Lega bitov od leve proti desni označuje zaporedne naslove usmerjevalnikov in predpisuje,ali je naslov naslednje destinacije datagrama sosed predhodnemu naslovu (1: mora biti, 0: ni nujno)
naslov (128 bitov) vsebuje naslov usmerjevalnika, ki ga mora datagram preiti.



Primer uporabe čela usmerjanja
Striktno usmerjanje
V maski so z 1 označeni vsi naslovi usmerjevalnikov na poti datagrama
Če se na poti vrine nov usmerjevalnik, ki ni naveden v čelu usmerjanja, datagram ne pride na cilj
Ohlapno usmerjanje
V maski striktnosti je z 0 označenih (vsaj nekaj) naslovov usmerjevalnikov na planirani poti datagrama datagram zato lahko preide vse navedene usmerjevalnike, lahko pa potuje tudi preko nenapovedanih

Na primer, da sta striktno navedena na poti le usmerjevalnik 1, 4 in 5, usmerjevalnik 3 pa je ohlapno naveden . V tem primeru bo v normalnih okoliščinah datagram potoval po označeni poti 1-3-4-5, v primeru izpada usmerjevalnika 3, pa bo ubral pot 1-2-4-5

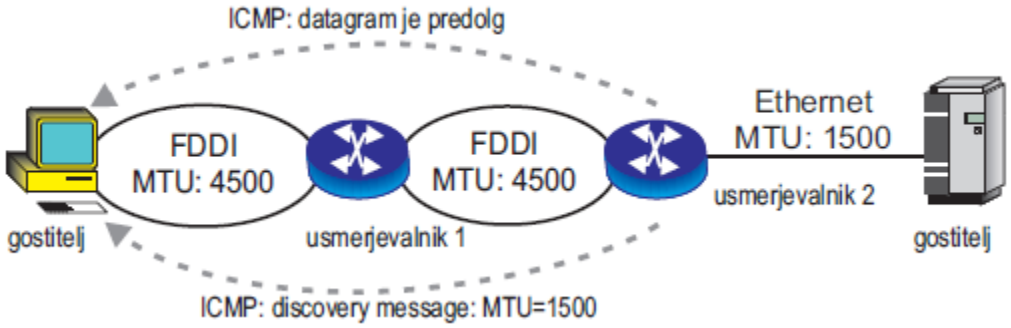
Fragmentacijsko čelo(Fragmentation header)

fragmentarno čelo. Vsebuje informacije, kako je pošiljatelj razdrobil originalni datagram v fragmente. Pri IPv6 vir datagrama, pri izvedenem drobljenju datagrama, s fragmentacijskim čelom prejemnika obvesti, da okviri, ki jih pošilja, vsebujejo fragmente datagrama. Ker fragmentacijo datagramov vrši pošiljatelj paketov, so usmerjevalniki razbremenjeni tega opravila. Zato se znatno poveča njihova prepustnost (hitrost usmerjevanja).

0	8	16	29	31
Naslednje čelo	Rezervirano	Odmik fragmenta	Rez	M
Oznaka originalnega datagrama				

Naslednje čelo (8 bitov), pove tip naslednjega čela
Rezervirano (8 bitov), polje je rezervirano za bodočo uporabo
Odmik fragmenta označuje, kje se podatki v fragmentu začenjajo v originalnem datagramu. Odmik merimo v 64 bitnihenotah, zato so podatki _ z izjemo zadnjega fragmenta lahko dolžine enaki mnogokratniku 64bitov.
Rez (2 bita), rezervirana bita za bodočo uporabo
Zastavica M (1 bit): 1: sledi še en fragment, 0: zadnji fragment
Oznaka enoumno označi identificira originalni datagram. Oznaka mora biti v času, ko je/bo paket v (med)omrežju edinstvena za naslov pošiljatelja in prejemnika.

Primer droblenja datagrama



Drobljenje datagrama se izvrši glede na najmanjšo vrednost Maximum Transmission Unit (MTU) podomrežja, ki je na poti datagrama.
Pošiljatelj pošlje prvi paket dolg 4500 oktetov (omejitev omrežja FDDI, na katerega je priključen).
Ta paket usmerjevalnik 1 lahko posreduje preko podomrežja FDDI usmerjevalniku 2. Usmerjevalnik 2 ve, da ima omrežje Ethernet omejitev MTU =1500 oktetov, zato zavrže datagram Pošiljatelju pošlje ukaz ICMP:Datagram too Big in sporočilo ICMP:discovery message: MTU = 1500. Naslednji paket pošiljatelja ne bo daljši od

1500 oktetov, dodano mu bo fragmentacijsko čelo s podatki, kako je datagram drobljen. Če bi na poti paketa bilo omrežje s še manjšim MTU, bi se opisani postopek ponovil.

Ugotavljanje avtentičnosti(Authentication header)

Čelo za avtentikacijo. Vsebuje informacije o avtentičnosti pošiljatelja

Velika pomanjkljivost protokola IPv4 je, da ne omogoča ugotavljanje avtentičnosti sprejetega okvira in ne pozna kriptografskega prekodiranja. Zato je možno na komunikacijski poti proti volji pošiljatelja prestrezati, preusmerjati in spreminjati okvire. Zlorabe, ki se lahko pri tem zgodijo, zelo omejujejo uporabo IPv4 v mnogih dejavnostih, kjer je avtentičnost in tajnost ključnega pomena, na primer v bančništvu. Problem avtentičnosti in varnosti se pri omrežjih IPv4 v splošnem skuša reševati v višjih plasteh. Ta problem protokol IPv6 rešuje s posebnim čelom s katerim zagotavlja, da je bil sprejeti paket res poslan od avtentičnega izvora ter da med potovanjem ni bil spremenjen.

0	8	16	31
Naslednje čelo	Dolžina podatkov		
	Security Parameter Ind.	(SPI)	
	Sekvenčni števec	(Za preprečevanje pon.)	
	Avtentikacijski podatki		

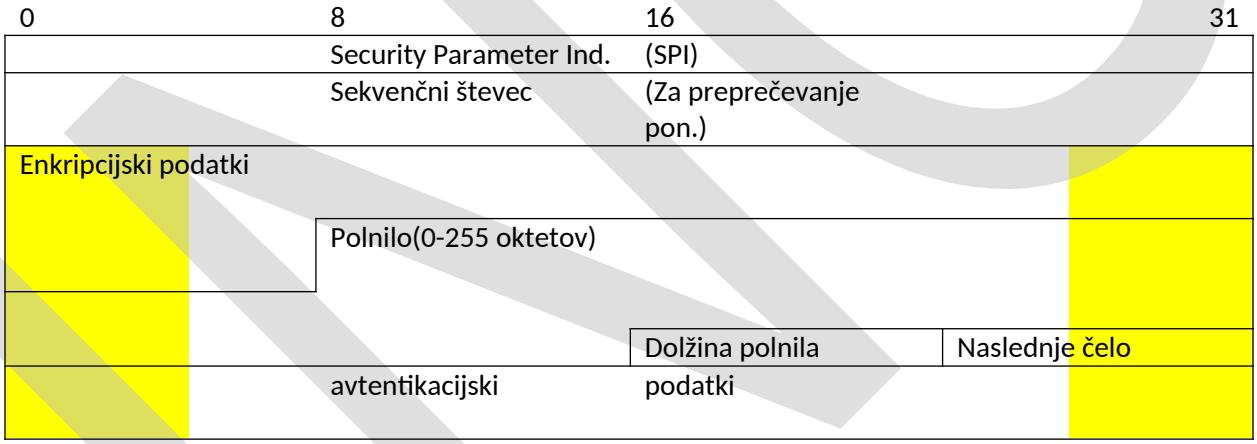
Polja

dolžina (8 bitov), dolžina podatkov o avtentičnostiv 32-bitnih besedah
SPI (32 bitov), indeks algoritma, ki izračuna podatke avtentičnosti
števec (32 bitov) služi za štetje ponavljanja
Podatki avtenti£nosti (spremenljiva dolžina), vsebina je odvisna od uporabljenega algoritma ugotavljanja istovetnosti
Podatki avtenti£nosti se ra£unajo z razli£nimi algoritmi.
Najpogosteje se uporabljata DES in MD5
Avtentičnost se ne glede na uporabljen algoritem računa za ves datagram z izjemo polj, ki se med prenosom spreminjajo (za ta polja se pri računanju avtentičnosti upoštevajo ničle)
Računanje avtentičnosti se izvede pred fragmentacijo datagrama
S števcem ponavljanja preprečimo, da bi se pri ponovnem pošiljanju paketa (zaradi ugotovljene napake med prenosom) ponovil varnostni algoritem za zagotavljanje avtentičnosti

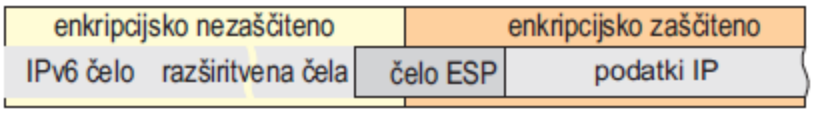
Enkripcijsko čelo(Encryption security payload header)

Čelo za kriptografsko zaščito. Vsebuje javni ključ zaščito podatkov

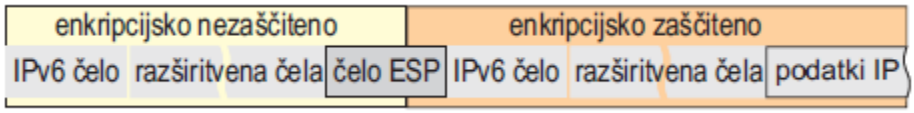
Zagotovitev avtentičnosti sicer reši problem preverjanja pravega izvora podatkov, ne zaščiti pa poslanih (zaupnih) podatkov pred nepooblaščenim pregledom.
Tajnost podatkov zagotovimo z enkripcijo podatkov.
Za zagotovitev tajnosti poslanih podatkov so bili (šele) leta 1995 predlagani predlogi standardov za to področje:
I RFC 1825: Pregled varnostne arhitekture
I RFC 1826: Opis razširitve IP z avtentikacijo paketov
I RFC 1828: Posebnosti avtentikacijskih mehanizmov
I RFC 1827: Opis razširitve IP z enkripcijo
I RFC 1829: Posebnosti kriptografskih mehanizmov
IPv4 pogojno podpira tudi te mehanizme, pri IPv6 pa so sestavni del protokola.
Z enkripcijskim čelom kriptogram, ki zagotovi visok nivo tajnosti podatkov.
Enkripcijsko čelo lahko vsebuje tudi podatke avtentičnosti vira.



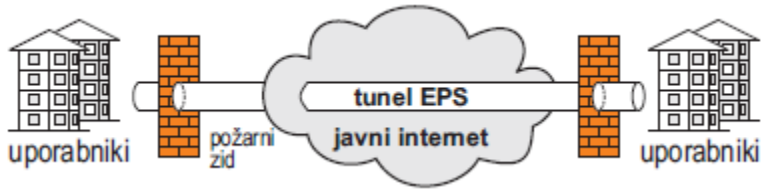
Kriptogram lahko vsebuje enkapsuliran datagram od zaporedne številke paketa v enkripcijskem čelu nadalje ali pa ves datagram.



Kadar je enkapsuliran ves datagram, prenos zahteva tako imenovano tuneliranje



Šfriranje celotnega okvira onemogoči delovanje analizatorjev prometa, saj sta naslova izvora in ponora skrita.
V osnovi je bil ta način enkripcije razvit za zaščito s požarnimi zidovi. Ta izvede enkripcijo poslanega paketa, doda pa mu svoje čelo z naslovom sprejemnega požarnega zidu.
Sprejemni požarni zid odstrani enkripcijo in paket v originalni obliki pošlje naslovljeni napravi v originalni obliki.
Za pošiljatelja in prejemnika sta požarna zidova in/ali enkripcija transparentna



Čelo z opcijami cilja(Destination options)

Čelo z opcijami za vmesne cilje Vsebuje opcije, ki se obdelajo v prvem cilju datagrama, ki je zapisan v naslovu prejemnika in nato zaporedoma v vseh destinacijah naštetih v čelu usmerjanja.

Realno časovni mikrosekundni protocol z vgrajenim ethernetom

Problem

Ethernet s svojim naključnim dostopom in zaznavo kolizije dobro rešuje zahteve lokalnih mrež, popolnoma odpove pri realno časovnih sinhronizacijah podatkov na µ sekundnem časovnem nivoju. Poleg ETH(Ethernet) naslovnega prostora bi si želeli RTM(Real Time Memory) naslovno področje, kjer bi imeli sinhronizirane podatke ostalih naprav priključenih v lokalno omrežje v času boljšem od 1 µ sekunde, to je čas v katerem naredi signal po svetlobnem vodniku 240m in 100-120m po bakreni parici. Mikro sekundni realno časovni protokol RTP zagotavlja prenos izmerjenih podatkov na katerokoli točko znotraj krogle premera L1m v 1 µS ali bolje. Zato je potrebno definirati prekinitveno rutino (DMAADRTM), ki prestavi aktivne podatke(Active Data - AD) na RTM področje. Čas prejemanja in preverjanja kontrolne vsote (RT) je potreben pri sprejemu telegrama. Direktni dostop do pomnilnika (DMARTMAD) poskrbi , da prejeti podatki pridejo iz RTM področja na aktivne podatke (AD).µ sekundni realno časovni protokol prestavi AD oddajnika v AD prejemnika v času 1µS ali hitreje.Direktni dostop do pomnilnika (DMARDTM) poskrbi za prenos aktivnih podatkov(AD) na realno časovno področje (RTM).

Problem masovnega priklopa rešuje časovno deljenje realno časovnih segmentov(RTMPS), ki za ceno hitrosti sinhronizacije RTM področja, omogoči hkratni priklop do 160 RTM/ETH naprav in seveda neomejeno ETH naprav.

Rešitev problema

Nakazana je rešitev problema, nekoč morda opisana v doktoratu in inplementirana v prakso. To zadnje bo zagotovo, morda ne ravno v tej obliki na predlagan način, vendar je realnočasovnost na nivoju 1 µ sekunde tako splošna potreba, da bo trg slej ko prej deležen preizkusa velikega števila standardov, ki bodo reševali sinhronizacijo podatkov v realnem času. Da bo zagotovo rešitev, ki bo preživela ta test, najboljša, najcenejša in za uporabnika nevidna je jasno. Vse komunikacije bodo potekale v isti arhihekturi kot danes, z enakimi standardnimi storitvami, le da bo v ozadju odprta možnost izredno hitrega sinhroniziranja podatkov na dvoportnih RAM področjih, ki jih bodo izkoriščali na novo uvedene realnočasovne storitve. In to ne izpostavljene ethernetnemu naključju in ne omejene s hitrostmi, ki jih omejuje 20 let star komunikacijski fizični standard. Opisan postopek se ustavlja ob samih naravnih omejitvah hitrosti svetlobe in je tako absoluten, neprekosljiv, vsaj v danes znanem fizikalnem svetu. Realno časovne komunikacije bodočnosti bodo imele še en dodan nivo enkapsulacije(vstavljanja) in bodo pokrivale tako realnočasovne zahteve, kakor množičen priklop velikega števila naprav, kar je navidez nezdružljivo.

µ sekundni realnočasovni protokol z vgrajeni ethernetom

10Gbaud asinhroni prenos

Pri hitrosti 10Gbaud pomeni 1nS 1 byte prenosa. Vsak byte ima poleg 8 bitov podatkov še liho pariteto in sinhronizacijsko pavzo(logična 0) skupaj 10 prenesenih bitov v 1nS. Take hitrosti v praksi dosegamo z (I1)bakreno parico , steklenimi vlakni ali telemetrijo.

100Gbaud asinhroni prenos

Pri hitrosti 100Gbaud pomeni 0.1nS 1 byte prenosa. Tehnologija je v razvoju omogoča pa prenos ETH telegrama v enem kosu brez fragmentiranja. Pri hitrosti 100Gbaud imamo tudi 19 x večji RTM prostor na napravo.

Slika 1 Prenos podatkov znotraj telegrama

Osnovni 1µS cikel

Osnova je časovno prožen protokol (K1)(TTP – Time trigered protocol) s periodo 1 µS. Znotraj mikrosekunde si sledi 16 telegramov dolžine 32 nS in 1 telegram dolžine 182 nS pri komunikacijski hitrosti 10Gbaud ali 100Gbaud. Pavza med telegrami je 18 nS. Vsak telegram ima 5 nS dolgo sinhronizacijo(pre ambula) in 3 nS dolg iztek (post ambula). Način sinhronizacije predstavljen v tem delu ne omogoča točne periode, ker je le-ta odvisna od sinhronizacijskega pogreška, ki bo opisan kasneje.

RTM/ETH podatkovno področje

Slika 2 Sledenje telegramov znotraj 1 µS cikla

16 x 22(308) bytov, dostopnih sistemu preko naslovnega prostora. Za RTM/ETH podatke skrbi mrežna kartica in so dostopni preko dual port pomnilnika. Ker lahko ETH področje postavimo na dobro znane naslove, se ETH/RTM mrežna kartica, obnaša kot navadna ETH mrežna kartica, dokler operacijski system ne nadgradimo z RTM funkcijami.

Slika 3 RTM/ETH podatkovno področje

Vsaki postaji v RTM/ETH mreži pripada polje 20(308)bytov na RTM podatkovnem prostoru. Tu hranimo podatke o zakasnitvi kraka postaje iz katere prihaja telegram, 16 RTM podatkov in T0, ki pomeni število µ sekundnih ciklov od zadnjega osveževanja RTM podatkov.

Lokalna RTM10(100)/ETH10(100) mreža

Realno časovna mikro sekundna RTM10(100)/ETH10(100) lokalna mreža ima obliko zvezde s centralnim ojačevalnikom (repeater – hub) in kraki za RTM10(100)/ETH10(100) (Naprave ki potrebujejo RTM10(100) področje in Ethernet funkcionalnost) in ETH10(100)(Naprave, ki potrebujejo samo Ethernet funkcionalnost) naprave. Kraki za RTM10(100)/ETH10(100) naprave so dolgi do L1m, kraki za ETH10(100) naprave so dolgi do L2m. RTM10(100)/ETH10(100) naprav je lahko do 160, ETH10(100) naprav je lahko poljubno število. Protokol ne predvideva povezovanja lokalnih odsekov omrežja, zato govorimo o realno časovnem 1µS prenosu podatkov znotraj krogle s premerom L1m, oziroma L2m za ETH10(100) naprave. L1 ima svoje meje v hitrosti procesiranja in prenosa podatkov skozi medij, L2 ima svoje meje v dušenju medija.

Gre za simetrično zvezda postavitev s standardnimi povezavami(sukana parica, optično vlakno, RF prenos), kjerkoli v kraku ali ojačevalniku lahko naredimo most na IEEE811.3 Ethernet ali katero koli drugo danes uporabljano omrežje. Tu opisana RTM10(100)/ETH10(100) rešitev celo omogoča prehod RTM10(100) in ETH10(100) podatkov preko mostička. RTM10(100) podatke prenašamo preko mostičev v poljubno število lokalnih odsekov RTM10(100)/ETH10(100) mrež z zakasnitvami reda 1µS ali manj na

Slika 4 Zvezda postavitev RTM/ETH naprav

Slika 5 Segmentacija RTM/ETH in ETH naprav

Meritev linijske zakasnitve

Svetloba naredi v 1 µS približno 300m v vakumu, 240m po svetlobnih vodnikih in 100-120m po bakreni parici. Protokolna sublimacijska točka je v ojačevalniku. Za pravilno sinhronizacijo telegramov rabimo podatek o zakasitvi linije od naprave do ojačevalnika. V ta namen izmerimo zakasnitev linije(DTM – delay time measure).

Meritev linijske zakasnitve se opravi z merilnim vezjem za vsako ETH10(100)/RTM10(100) ali ETH10(100) linijo pred sinhronizacijo v omrežje. Za te namene se uporabi poseben merilni telegram. Za odklop ali priklop ETH10(100)/RTM10(100) ali ETH10(100) linije na sublimacijsko točko ojačevalnika se uporabi poseben telegram. Sublimacijska točka se odklopi tudi po mrtvem času linije(Time dead line - Tdl), ko se predpostavlja izpad linije. Meritev se opravlja na nS natančno , v tem času naredi svetloba v vakuumu 30cm, svetloba po svetlobnem vodniku 24cm in signal po bakreni parici 10 do 12 cm. Meritev predpostavlja enako dolžino sprejemne Rx in oddajne Tx linije. Ker merimo čas potovanja merilnega telegrama od naprave do ojačevalnika in nazaj lahko dolžino dejansko izmerimo še za polovico bolj natančno. Nadaljnje izvajanje bo pokazalo, da nas zanima samo zakasnitev linije in ne medij, zato je protokol neodvisen od medija.

Meritev neaktivnosti oddajne linije

Slika 6 Meritev linijske zakasnitve - DTM

Naprava priključena v RTM10(100)/ETH10(100) omrežje mora oddati telegram (RTM10(100) ali ETH10(100)) vsaj vsake Ti. Če je naprava neaktivna dalj kakor Ti v mS se jo odklopi iz sublimacijske točke. Za ponovni priklop naprave rabimo RTM10(100)/ETH10(100) – ON telegram iz odklopljene naprave. Ti predlagam okoli 10 mS. Kritične so naprave s samo ETH10(100) funkcijo, ker nimamo stalnih RTM10(100) telegramov in moramo programsko zagotoviti prazne ETH telegrame, ki resetirajo Ti števec. Ojačevalnik ima torej v vsaki liniji logiko za prepoznavanje RTM/ETH – ON in RTM/ETH – OFF telegramov in števec neaktivnosti linije Ti.

Slika 7 Meritev neaktivnosti oddajne linije

Porazdeljena sinhronizacija

Pravilno pošiljanje telegramov ob pravem času je predpogoj za tvorjenje protokola v sublimacijski točki ojačevalnika. Naprava ima podatke o zakasnitvi linije LTDx in sprejema telegrame po liniji RX. Ključen je čas oddaje telegrama po oddajni liniji TX in to ob pravem času, da ravno prispe do sublimacijske točke ko je po protokolu to potrebno.

Označimo fronte telegramov RTM kot sinhronizacijske značke Sx protokola. V sublimacijski točki ojačevalnika velja , da si sinhronizacijske točke S_0 do S_{15} sledijo na 50 nS, nakar sledi 200nS pavza za ETH telegrame. Ker vsaka RTM/ETH naprava pošilja telegrame ciklično na 1µS je potrebno izvršit popravke v primeru razglasitve. Pri prejemanju naprava n prejema skupni signal z LTD_n zakasnitvijo. Pri oddajanju moramo poslati telegram LTD_n pred potrebnim časom glede na sublimacijsko točko. Ta predpostavka velja v primeru enakih dolžin in materiala Rx in Tx linije.

Slika 8 Časovni okvir porazdeljene sinhronizacije

$$Sn_r = n * 50nS$$
$$Rx_n : S_n = n * 50nS + LTD_n$$
$$Rx_m : S_m = m * 50nS + LTD_m$$
$$Tx_n : S_n = n * 50nS - LTD_n$$
$$Tx_m : S_m = m * 50nS - LTD_m$$
$$\Delta Tn = S_m(Rx) - S_n(Tx) - Tc$$
$$\Delta Tn = f(m,n) * 50nS - 2 * LTD_n - Tc$$

Oblike telegramov

Vsi telegrami imajo na začetku 5 bytov namenjenih sinhronizaciji(pre ambula) 1 byte je rezerviran za tip(type) telegram in 1 byte za stevilko postaje. Na koncu imamo 4 byte ciklične redundantne kode(CRC) in 3 byte izteka(post ambula). RTM in ETH telegram sta definirana za hitrost mreže 10Gbaud in 100Gbaud. Merilni in nadzorni telegram potekajo vedno pri hitrosti 10Gbaud. Pri obeh hitrostih ohranjamo podobno sledenje telegramov (Slika 1).

RTM10	11H	32	Realno časovni podatki postaj

RTM100	66H	32	Realno časovni podatki postaj
ETH10	22H	182	Ethernet podatki postaj
ETH100	77H	182	Ethernet podatki postaj
DTM	33H	32	Telegram za merjenje zakasnitve linije
RTM/ETH - ON	44H	32	Priključitev na sublimacijsko točko
RTM/ETH - OFF	55H	32	Odklop iz sublimacijske točke

RTM10 telegram

5	FFH	Preambula
1	11H	Type
1		N(0-15)
2		LDTn(nS)
16		RTM
4		CRC
3	FFH	Postambula

RTM10 telegram je dolg 32 bytov ali 32 nS. Sinhronizacijski glavi(preambula) sledi tip(11H) ki definira telegram. Sledi številka postaje N. Naslednje integer polje je podatek o zaksnitvi linije postaje, ki je telegram poslala. Koristnih RTM podatkov je 16 bytov. Le-ti se zbirajo v distribuiranih RTM tabelah postaj. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula).

RTM100 telegram

5	FFH	Preambula
1	12H	Type
1		N(0-15)
2		LDTn(nS)
304		RTM
4		CRC
3	FFH	Postambula

RTM100 telegram je dolg 320 bytov ali 32 nS. Sinhronizacijski glavi(preambula) sledi tip(66H) ki definira telegram. Sledi številka postaje N. Naslednje integer polje je podatek o zaksnitvi linije postaje, ki je telegram poslala. Koristnih RTM podatkov je 304 bytov. Le-ti se zbirajo v distribuiranih RTM tabelah postaj. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula).

ETH10 telegram

št bytov		Op
5	FFH	Preambula
1	22H	Type
1		N(0-255)
1		C(0-9)
2		LDTn(nS)
1		Nv(1-165)

165		ETH
4		CRC
3	FFH	Postambula

ETH telegram je dolg 182 bytov ali 182 nS. Sinhronizacijski glavi(preambula) sledi tip(22H) ki definira telegram. Sledi številka postaje N in števec ETH telegramov C. Naslednje integer polje je podatek o zaksnitvi linije postaje, ki je telegram poslala. Nv je število veljavnih ETH bytov. Koristnih ETH podatkov je 165 bytov. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula).

ETH telegrami sledijo RTM telegramu številka 15. Rezervirani čas 200nS je izkoriščen za naključni dostop vseh(do 254) naprav v segmentu RTM/ETH mreže. Za prenos Ethernet telegrama dolžine 1554 rabimo 10 zaporednih pošiljanj ETH telegrama. Novo pošiljanje telegrama je po načelu naključnega dostopa z zaznavo kolizije in uporabo Ethenet metod za razrešitev nastale kolizijske situacije.

ETH100 telegram

5	FFH	Preambula
1	77H	Type
1		N(0-255)
2		LDTn(nS)
2		Nv(1-1802)
1802		ETH
4		CRC
3	FFH	Postambula

ETH telegram je dolg 1820 bytov ali 182 nS. Sinhronizacijski glavi(preambula) sledi tip(2H) ki definira telegram. Sledi številka postaje N. Pri tej hitrosti lahko standardno dolžino telegrama pošljemo v enem kosu in ne rabimo fragmentiranja. Naslednje integer polje je podatek o zaksnitvi linije postaje, ki je

telegram poslala. Nv je število veljavnih ETH bytov. Koristnih ETH podatkov je 165 bytov. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula).

ETH telegrami sledijo RTM telegramu številka 15. Rezervirani čas 200nS je izkoriščen za naključni dostop vseh(do 254) naprav v segmentu RTM/ETH mreže. Za prenos Ethernet telegrama dolžine 1554 rabimo rabimo pri 100Gbaud mreži samo eno pošiljanje, kar je velika prednost proti 10Gbaud mrežam, kjer moramo ETH telegram fragmentirat. Novo pošiljanje telegrama je po načelu naključnega dostopa z zaznavo kolizije in uporabo Ethenet metod za razrešitev nastale kolizijske situacije.

DTM telegram

DTM telegram je dolg 32 bytov ali 32 nS. Sinhronizacijski glavi(preambula) sledi tip(33H) ki definira telegram. Sledi številka postaje N in 18 bytov polnila. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula).

5	FFH	Preambula
1	33H	Type
1		N(0-15)
18	F0H	Polnilo
4		CRC
3	FFH	Postambula

RTM/ETH - ON telegram

DTM telegram je dolg 32 bytov ali 32 nS. Sinhronizacijski glavi(preambula) sledi tip(44H) ki definira telegram. Sledi številka postaje N. Naslednje integer polje je podatek o zaksnitvi linije postaje, ki je telegram poslala, sledi čas Ti(mS), to je čas po katerem se v primeru neaktivnosti postaje linija prekine in 14 bytov polnila. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula). Ta telegram aktivira sprejemno in oddajno linijo sublimacijske točke.

5	FFH	Preambula
1	44H	Type
1		N(0-15)
2		LDTn(nS)
2		Ti(mS)
14	F0H	Polnilo
4		CRC
3	FFH	Postambula

RTM/ETH - OFF telegram

DTM telegram je dolg 32 bytov ali 32 nS. Sinhronizacijski glavi(preambula) sledi tip(55H) ki definira telegram. Sledi številka postaje N. Naslednje integer polje je podatek o zaksnitvi linije postaje, ki je telegram poslala. in 16 bytov polnila. Na koncu imamo še 4 bytno CRC kodo in 3 byte izteka(postambula). Ta telegram deaktivira sprejemno in oddajno linijo sublimacijske točke.

5	FFH	Preambula
1	55H	Type
1		N(0-15)
2		LDTn(nS)
16	F0H	Polnilo
4		CRC
3	FFH	Postambula

Protokol

Meritev linijske zakasnitve

RTM/ETH naprava najprej pošlje DTM(Type 33H) telegram in izmeri čas, ki ga le ta potrebje, da se vrne po mreži na nS natančno. Meritev zahteva časovno bazo 1GHz in ustrezne hitre števce, ki izmerijo čas potovanja telegrama. V času meritve je sublimacijska točka ojačevalnika ločena od merjenega kraka mreže. Sama meritev je stvar merilnega programa, ki lahko DTM telegram pošlje poljubnokrat in s pomočjo povprečenja dobljenih rezultatov izračuna časovno zakasnitev linije TDLn. Merilni program izloči očitno napačne rezultate in končni rezultat deli z dve. Pri meritvi predpostavimo enako dolžino sprejemne in oddajne linije, kar je pri sukani bakreni parici enostavno izvedljivo, pri optičnem vodniku pa zahteva pozornost monterja.

Zelo pomembna je ugotovitev, da medij ne vpliva na meritev, ker nas ne zanima dejanska dolžina temveč samo zakasnitev linije. Če predpostavimo da imamo za prenos telegrama med dvema RTM/ETH100 napravama 892 nS(446 nS od ojačevalnika do RTM postaje) si lahko izračunamo polmer krogle L1(Slika 3), ki ga dosežemo z različnimi tehnologijami prenosa. Za RTM/ETH10 naprave je čas prenosa 936 nS, zato je ustrezno daljša razdalja L1.

Wireles	30	133,8	140,4
Optični vodnik	24	107,0	112,3
Sukana parica	10-12	44,6-53,5	46,8-56,1

Dejansko je ime protokola upravičeno, do izračunanega polmera RTM mreže. Prav nič nas pa ne omejuje, da v primeru potrebe krak enostavno podaljšamo, le , da v tem primeru skupna zakasnitev RTM podatkov presega 1µS.

Določitev številke postaje N

RTM/ETH protokol zahteva določitev številke postaje za RTM in MAC naslova ETH. DTM telegram ima lahko poljubno številko postaje N(predvideno 0), ker ne oddaja na sublimacijsko točko. Tudi RTM/ETH – ON telegram ima lahko poljubno številko postaje N(predvideno 0), ker se priklop sublimacijske točke izvrši po pošiljanju telegrama. Sedaj sledi prisluškovanje mreži in ugotavljanje prve proste RTM številke(0-15). Tu je možen scenarij, kolizije v primeru dveh naprav, ki bi sočasno ugotavljale prosto številko postaje. Prednastavljene številke postaj niso možne. Kolizijo se ugotavlja in odpravlja po principu ETH mrež. ETH telegram dobi MAC naslov po principu dodajanja MAC naslovov. Če zmanjka RTM številk se lahko naprava vedno priklopi kot ETH. Sistemski administrator bo moral samo paziti, da v enem segmentu RTM/ETH mreže ne bo predvidel več kakor 160 RTM naprav.

Vklop kraka mreže na sublimacijsko točko

Z RTM/ETH ON telegramom(Type 44H) vklopimo krak na sublimacijsko točko. To se zgodi po koncu telegrama. Od tega trenutka dalje lahko oddajamo telegrame preko Tx linije in sprejemamo telegrame preko Rx linije. Sublimacijska točka se avtomatično odklopi od kraka če je Tx nedejaven Ti sekund. ETH napravam se lahko zgodi, da jih ojačevalnik odklopi od sublimacijske točke, če naprava ne pošlje nobenega ETH telegrama več kakor Ti mS. ETH telegrame naprav ki izkoriščajo samo ETH povezavo moramo zagotoviti programsko na čas , ki je krajši od Ti(predvidoma 10 mS).
Zaznava RTM/ETH ON telegramov je v DTMSn sekciji kraka ojačevalnika.

µ sekunda

AD podatkovni tok

AD – activ data, so aktivni podatki sistema. µ sekundni protokol vzpostavi 1Mbs podatkovni tok med aktivnimi podatkovnimi naslovi naprav segmenta RTM/ETH mreže in to z zakasnitvijo 1µS ali bolje.

DMAADRTM10	2	Direkten prenos AD področja na RTM področje
DMAADRTM100	38	Direkten prenos AD področja na RTM področje
2xLTD	800	2 x zakasnitev najdaljšega kraka
RT	32	Sprejem in obdelava RTM telegrama
DMARTMAD10	2	Direkten prenos RTM področja na AD področje
DMARTMAD100	38	Direkten prenos RTM področja na AD področje
Skupaj RTM/ETH10	864	Skupaj prenos aktivnih podatkov
Skupaj RTM/ETH100	908	Skupaj prenos aktivnih podatkov

RTMADT

RTMADT je tabela kazalcev na aktivne podatke sistema. Uporablja se za hitre direktne dostope do aktivnih podatkov v DMAADRTM in DMARTMAD prekinitvah. Vsaka skupina po 8 bytov(64 bitov) RTM področja ima svoj absolutni kazalec na odgovarjajočo lokacijo aktivnih podatkov (AD). Ker imamo do 16 RTM/ETH naprav moramo imeti 2 x 16 polnih naslovov do aktivnih podatkov.
Ob upoštevanju današnje hitrosti delavnega pomnilnika (1GHz) je za prenos 16 bytov RTM pomnilnika na ustrezno AD področje ali obratno potrebno 16nS. V najslabšem primeru bi porabili za prenos 16 RTM podatkov na AD področje 32nS v 1µS okviru, kar je približno 3,2% razpoložljivega časa podatkovnega vodila.
Pri 100 Gbaud mrežah imamo RTM področje veliko 16 x 304 bytov, kar je 16 x 38 skupin podatkov po 64 bitov. Pri upoštevanju prepustne hitrosti vodila delavnega pomnilnika (1GHz) bi v najslabšem primeru porabili 16 x 38 = 608nS v 1 µS, kar je 60,8% razpoložljive hitrosti podatkovnega vodila.

	RTMAD	emenitev
RTM/ETH10	2 x 16	3,2%
RTM/ETH100	38 x 16	60,8%

DMAADRTM

DMAADRTM je direktni dostop do aktivnih podatkov(AD) sinhronizirana s pošiljanjem RTM podatkov postaje. DMAADRTM se proži 40nS pred predvidenim pošiljanjem RTM telegrama in

prenese 16 AD podatkov na RTM področje. DMAADRTM prekinitve imajo svoje registre , kar minimizira delo s skladom. Čas od prožitve DMAADRTM do pošoljanja RTM telegrama se prišteje LTD podatku RTM telegrama, tako dobimo v sublimacijski točki RTM telegram z neodvisnimi naslovnimi podatki in pravilno zakasnitvijo. V realnih napravah(PC npr) imamo še DMA(Direct Memory Access) prekinitve, ki so navadnim prekinitvam nadrejene s strani napravi nadrejene naprave. Naprava z RTM/ETH mrežno kartico bo morala imeti dovolj realnega časa, da bo lahko servisirala DMAADRTM prekinitve(DMA ki servisira RTM/ETH kartice ima najvišjo prioriteto). DMAADRTM je lahko prožen tudi na 50 nS, zato je nujna uporaba tabele kazalcev na aktivne podatke (RTMADT).
Tu je še en problem, namreč periferija(npr AD pretvornik) ponavadi nima funkcije zakasnjenega proženja AD pretvorbe, ki bi se zgodila pretvorbeni čas pred proženjem DMAADRTM prekinitve. Proizvajalci senzorske in druge periferije, bodo morali predvideti zakasnjeno proženje A/D pretvorbe, ki bo gotova ravno pred proženjem DMAADRTM. Pomembna je tudi hitrost AD in DA pretvorbe(oziroma katere koli obdelave podatkov), ker le-ta pravzaprav enakopravno vstopa v zakasnitveno verigo RTM/ETH mrež.

DMARTMAD

DMARTMAD je direktni prenos RTM področja do aktivni podatkov(AD), neposredno po prejemu sveže kopije RTM podatkov za vsako postajo. DMARTM proži mrežna avtomatika neposredno po prejemu svežih RTM podatkov za vsako RTM/ETH postajo posebej. DMARTMAD je lahko tudi na 50nS, zato je nujna uporaba tabele kazalcev na aktivne podatke (RTMADT). Pri današnji hitrosti delavnega pomnilnika, je poraba časa pri RTM/ETH100 mrežah zelo velika. Stanje se bo izboljšalo, ko bodo tercialna podatkovna vodila pridobila na hitrosti.

RTMPS

RTMPS(Real Time Memory Place Share), je možnost opisanega protokola, da posamezen realno časovni segment deli z do 10 RTM/ETH postajami. Seveda so potem sinhronzacijski časi 10 x dalši, vendar nam mehanizem omogoči večje število priklopljenih RTM/ETH postaj na mrežni segment. Za identifikacijo pošiljajoče postaje se uporabi N pomnožen z 10 x številko postaje na RTM segment. Tako imamo lahko npr 0-ti RTM segment deljen med 10 RTM/ETH naprav, ki imajo RTM področje sinhronizirano vsake 10µS, kar je za večino RTM procesov več kot dovolj hitro. Seveda imamo lahko še vedno na istem mrežnem segmentu 15 RTM/ETH naprav sinhroniziranih na 1µS in poljubno število ETH naprav.
RTM prostor postane dolg 78848 x 10 bytov = 788480 bytov = 0.78 Mbyte, kar je pri današnji tehnologiji zanemarljivo.

Povzetek

O delu

Tretje individualno delo je priprava na doktorat. Obravnavana tema je široka in temeljno posega na obstoječe področje lokalnih mrež. Delo upošteva stanje tehnologije in teoretično obdela

zmogljivosti realnočasovnih mikrosekundnih lokalnih mrež z vsebovanim ethernetom. Vse uporabljane tehnologije obstajajo ali v komercialni uporabi ali na razvojnih policah laboratorijev. Z uporabo meritve zakasnitve linije, uporabo topologije zvezde in vsebovanim ethernetom opisani protokol in strojna topologija združuje realnočasovne zahteve in masovni priklop na lokalno mrežo.
Mreža zgrajena po idejah opisanih v tem delu bo(bi) izgledala podobno kot danes uporabljana topologija, le da dodaja odzivnost, ki se približuje naravnim omejitvam zaradi hitrosti svetlobe. V doktoratu bom opisano temo nadgrajeval , objavil širši strokovni javnosti , izpopolnil simulacije in pokazal izvedbeno pot.

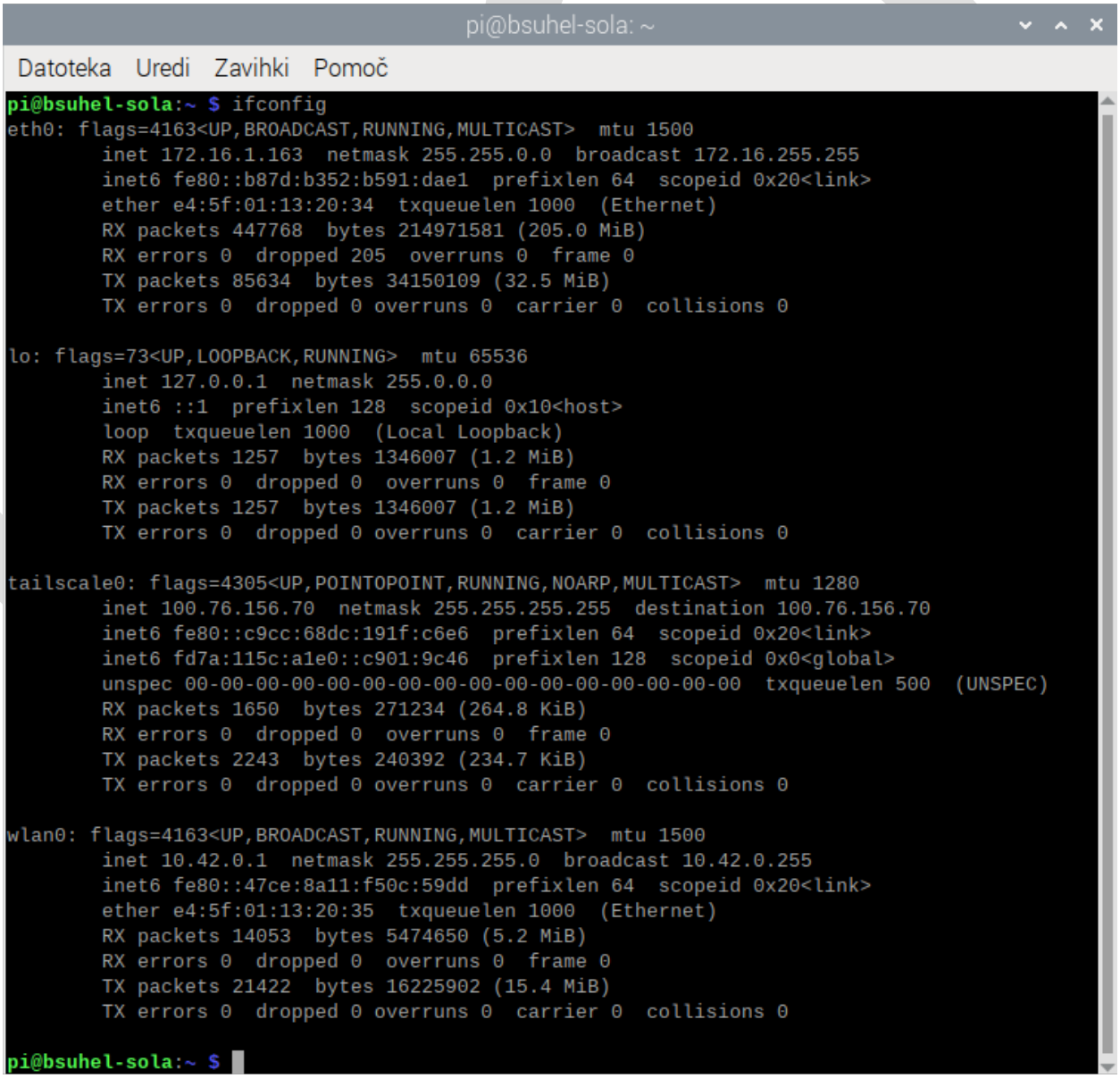
Ugotovitve

RTM/ETH mreže narejene po tu predstavljenem principu bodo zadovoljevale potrebo po sinhronizaciji realnočasovnega RTM področja med napravami in masovnega ETH priklopa naprav za izmenjavo podatkov. Pri hitrostih, ki so povsem na mejah naravnih omejitev svetlobne hitrosti moramo na novo definirati prioritete podatkovnih tokov in spremeniti zasnovo DMA in skladovnih(stack) prekinitev. Prepustnos 100Gbaud mreže je teoretično 1000000 ETH telegramov na sekundo(1802Mbyte/sek/mrežo) in zmožnost ustvariti podatkovni tok 38 x 64bit AD(activ data) to AD na postajo(do 16(160) RTM postaj) na 1(10)µsekundo v krogli s premerom 107 m, če uporabimo kot medij svetlobno vlakno.
Še veliko bolj uporabne so zagotovljene prepustnosti zaradi RTM področja. To delo sicer ne posega v široko uporabnost in nove standardne funkcionalnosti , ki jih moramo še odkriti in zapisati. Zamislimo si standarden FTP, ki lahko pri prenosu ugotovi , da sta obe napravi RTM/ETH in izkorist prosti del RTM kanala, ki ima zagotovljeno prepustnost 1000000 RTM100 telegramov po 304 byte, kar je 304Mbyte/sek/napravo. Tu lahko hkrati prenašamo podatke na vseh 16 RTM/ETH.
RTM/ETH mreža ohranja vso funkcionalnost obstoječih ETH mrež in doda RTM funkcionalnost. Pokazal sem tudi, povezljvost obstoječih in RTM/ETH mrež in celo RTM/ETH mrež med sabo. Z deljenjem posameznega RTM segmenta med 10 naprav protokol omogoči časovno/zmogljivostne optimizacije.
RTM/ETH mreže zaradi izrednih zahtev po procesorski moči , postavljajo omejitve glede DMA dostopov ostalih procesorju nadrejenih sklopov(Diski, video). Zaradi osnovnega 50µS cikla, je edina DMA nadrejena naprava lahko RTM/ETH mreža.

Raspberry OS

Opis nekaj standardnih programov, ki jih predpisuje TCP/IP standard. OS ima standardne ukaze in omogoča njihovo izvajanje v Terminalnem oknu.

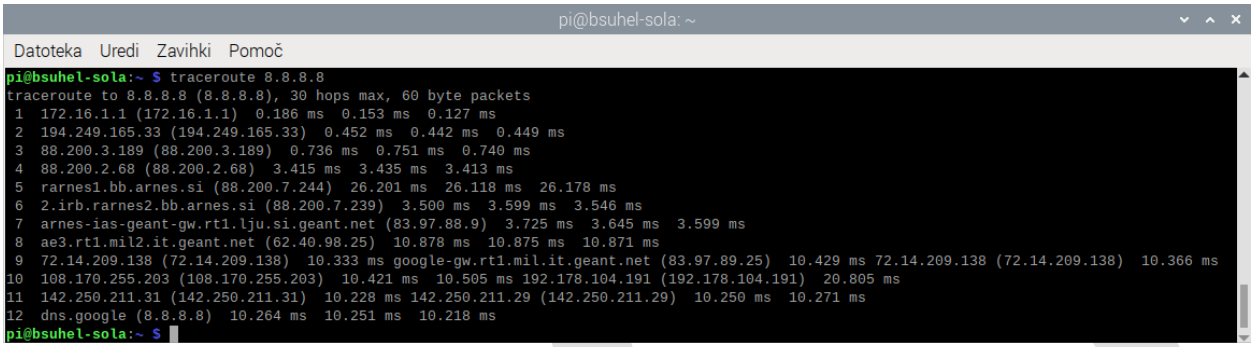
Ifconfig



suhel.raspberryip.com

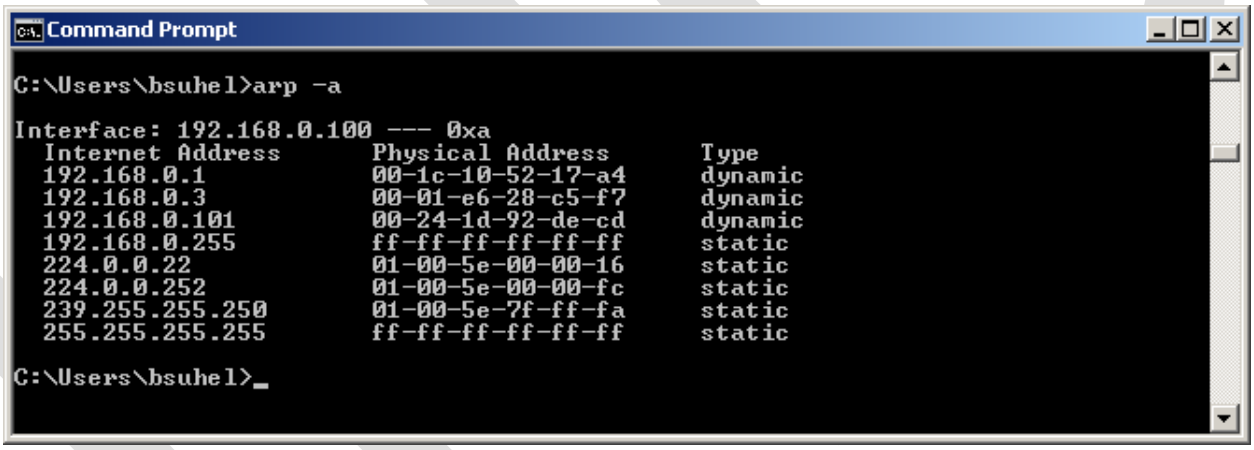
If config izpiše nastavitve lokalnih mrež.

Traceroute



Tracert nam pokaže najverjetnejšo pot potovanja telegram , če komuniciramo z neko domeno.

Arp

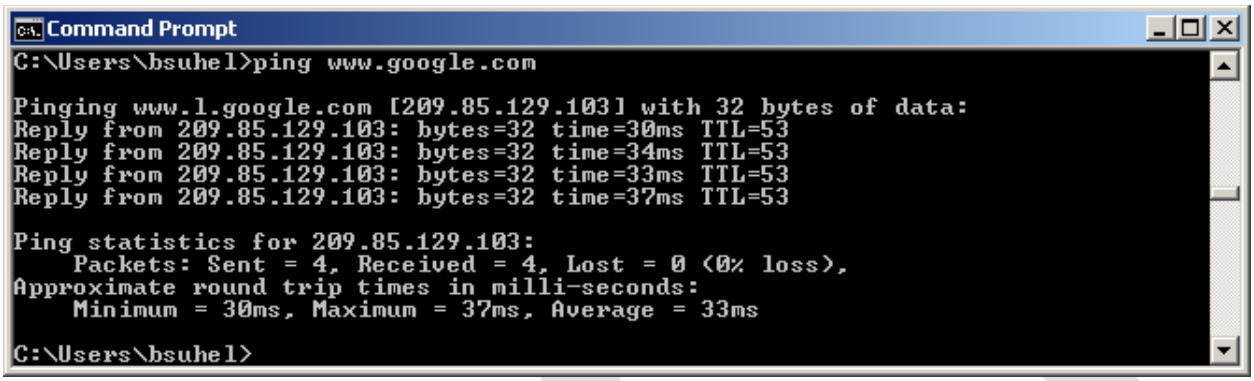


Arp nam pokaže relacijsko tabelo IP<-->MAC, ki jo tvori IP opravilo arp. Dinamične povezave trajajo omejen čas in se v primeru neobnovitve po določenem času izbrišejo. Statične povezave ostanejo v tabeli do izklopa računalnika.

Route

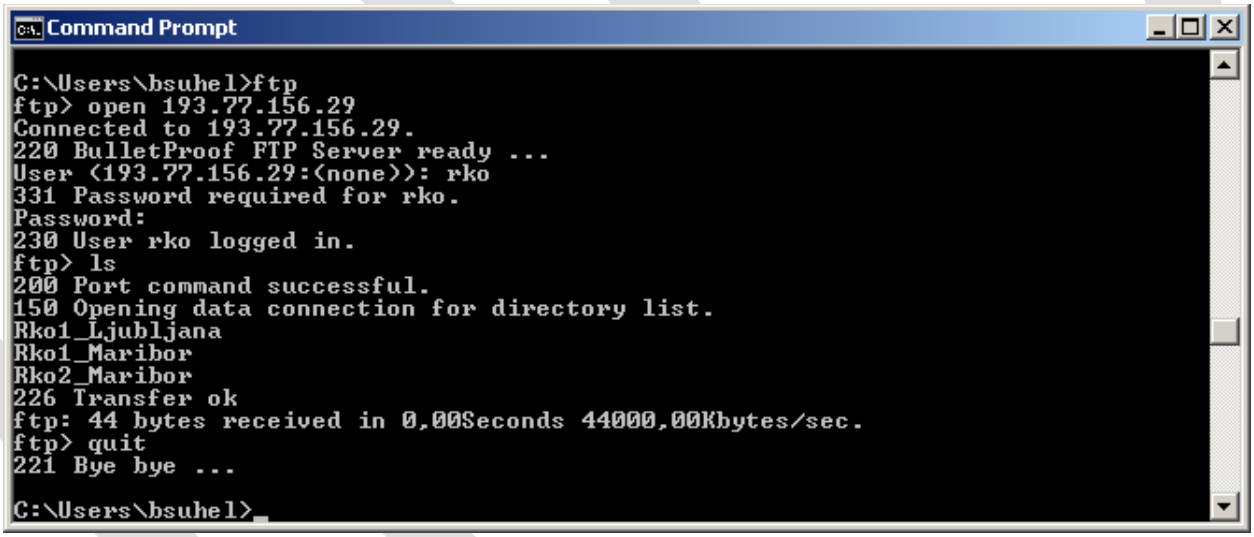
Ukaz route nam pokaže preusmerjanja zaupana hostu(napravi). To so tista preusmerjanja , ki jih računalnik izvede , da pride do prehodov(ruterjev). Lokalna preusmerjanja morajo biti definirana za vse protokole.

Ping



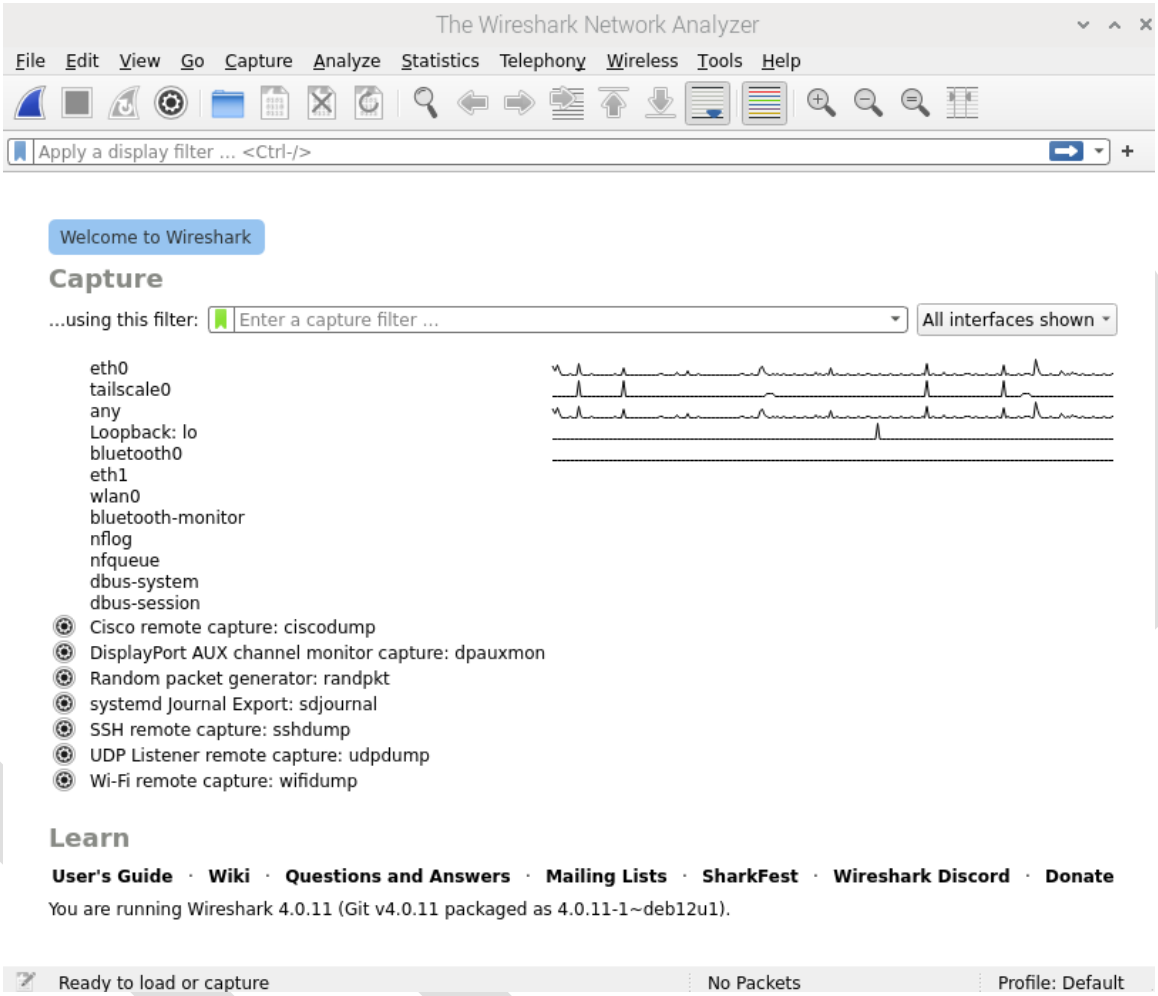
Ping je namenjen preverjanju prisotnosti naprave. Za ping se uporablja ICMP IP telegram

Sftp



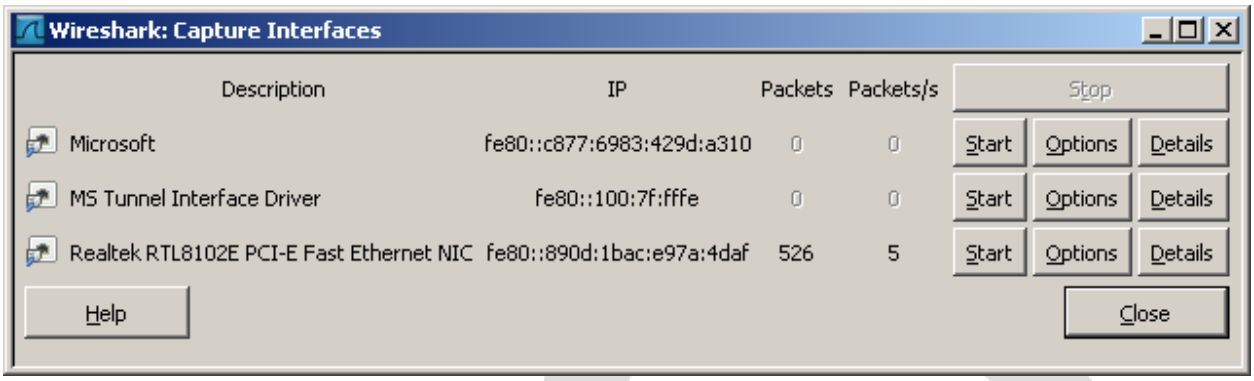
Vgrajena storitev ftp, primerna za prikaz osnovnih ukazov, ki jih uporabljajo tudi drugi preogrami, vključno z windows explorerjem. Primer prikazuje aktivacijo ftp, priklop in identifikacijo. Nato izpišemo vsebino mape(ls) in zapustimo program.

Wireshark

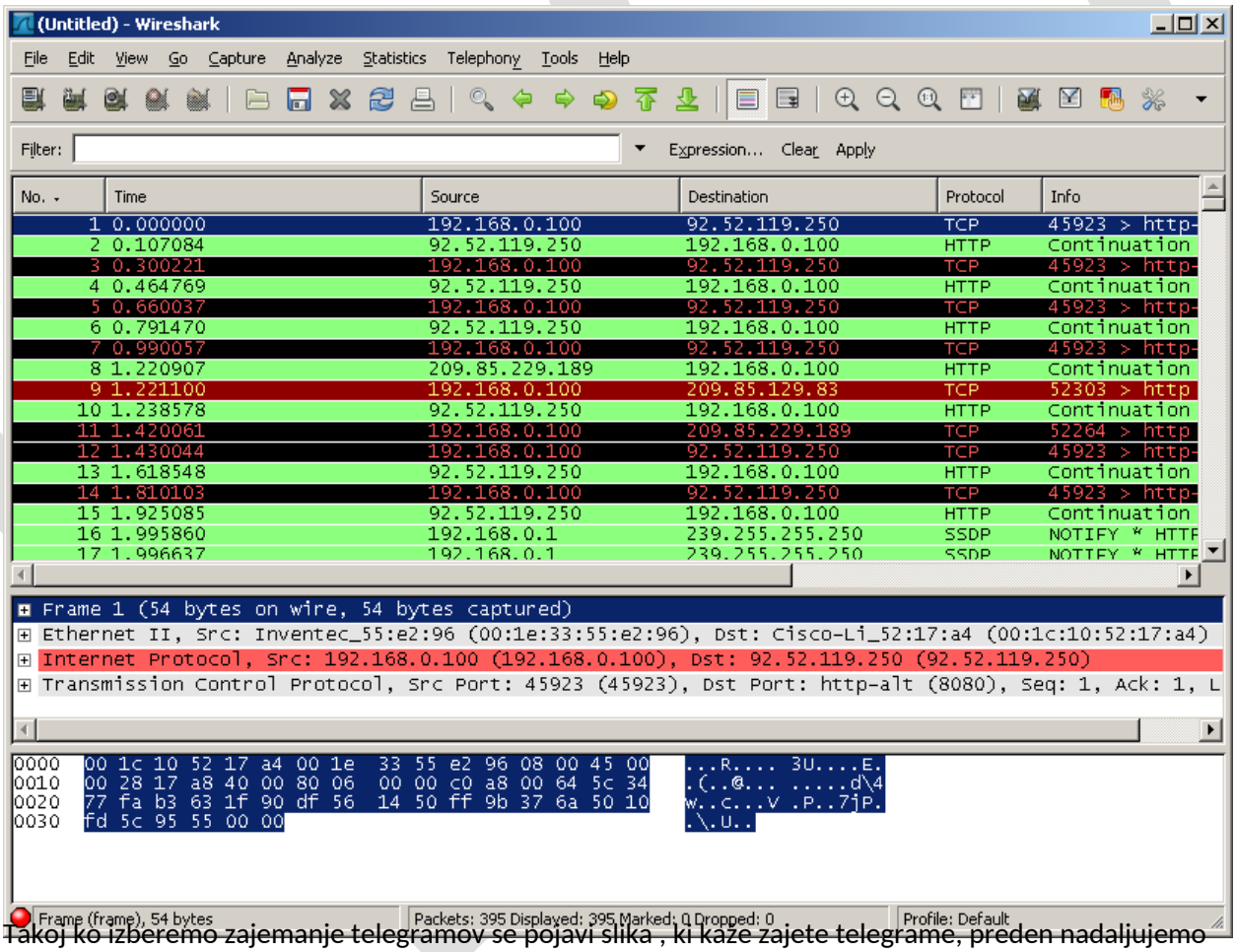


Izbira mrežne naprave

Internet→Wireshark.Po namestitvi je program pripravljen za spremljanje IP prometa na vašem računalniku. WireShark je popularen program za analizo protokolov. Z uporabo menuja Capture->Interfacess... dobimo spodnje oknjo, v katerem izberemo omrežno napravo, na kateri bomo spremljali promet. Za dogajanje na lokalni mreži je bolj primerna izbira wireless naprave, ker nimamo omejevanja prometa, kot na Ethernet ožičeni napravi, ki ima ponavadi na drugi strani preklopnik, ki omejuje promet znotraj lokalnega segmenta. Če rabimo komunikacijo proti wan omrežju, je ponavadi boljša izbira Ethernet naprave, ker nam omeji promet na lokalnem omrežju. Vsekakor je dobro vedeti kaj počnemo.



Zajemanje telegramov



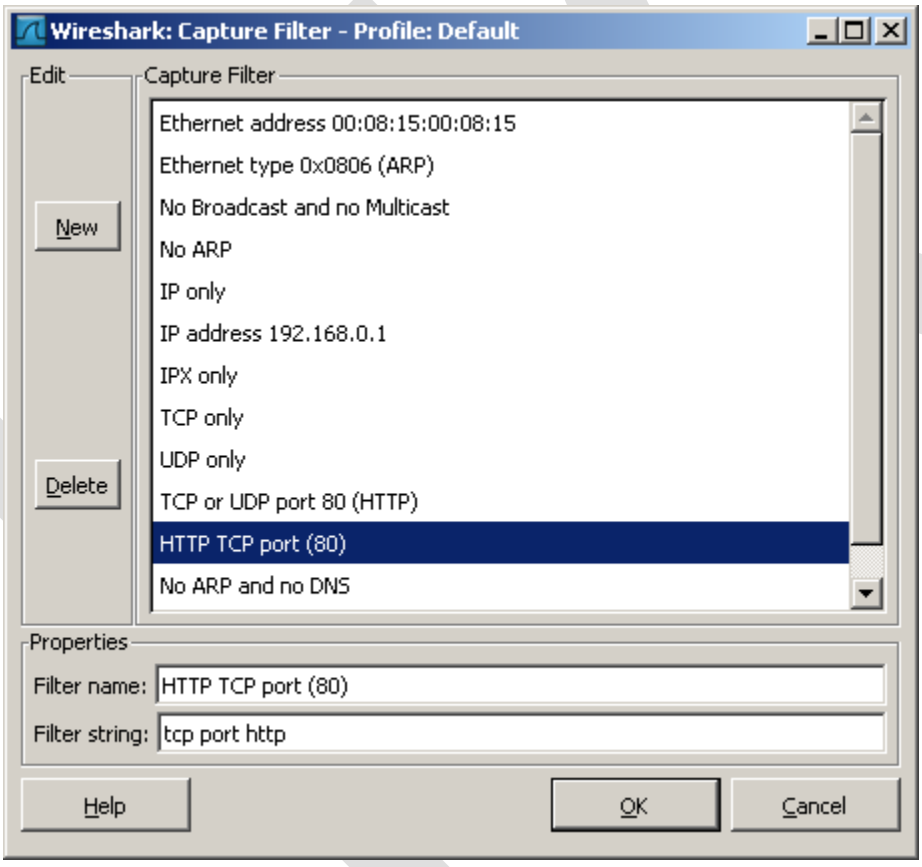
Takoj ko izberemo zajemanje telegramov se pojavi slika , ki kaže zajete telegrame, preden nadaljujemo moramo v menuju Capture>>Stop ustaviti skeniranje, kern am lahko preobilje prometa povzroča težave. Sedaj fokusiramo prvi TCP telegram , malo uredimo prikazna polja po višini in že lahko razberemo

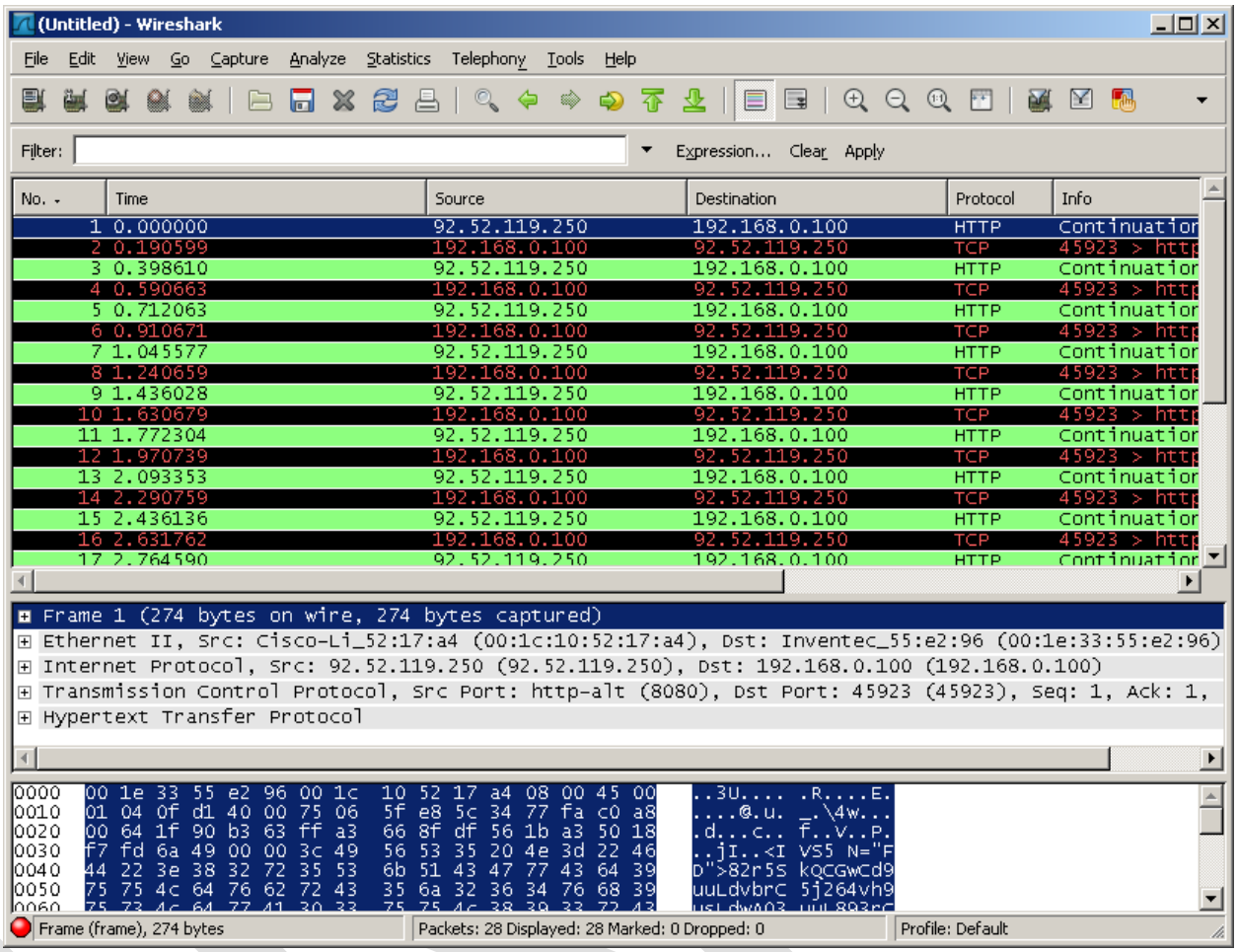
nekatere osnovne nam do sedaj znane podatke. Ne pozabimo, da imamo pred sabo v svtu najbolj popularno orodje za spremljanje prometa tako, da lahko z njim počnemo marsikaj. Taki in podobni program osnovno orodje raznih hekerjev, zato ni slabo , da se zavemo njegove moči, v izogib preveliki lahkomiselnosti pri varovanju omrežja.

V našem primeru gre za TCP/IP protocol IPv4 standarda. Odčitate si lahko Src in Dst IP naslov in pa Src in Dst port, preberete si lahko pa tudi podatke telegram.

Filtriranje

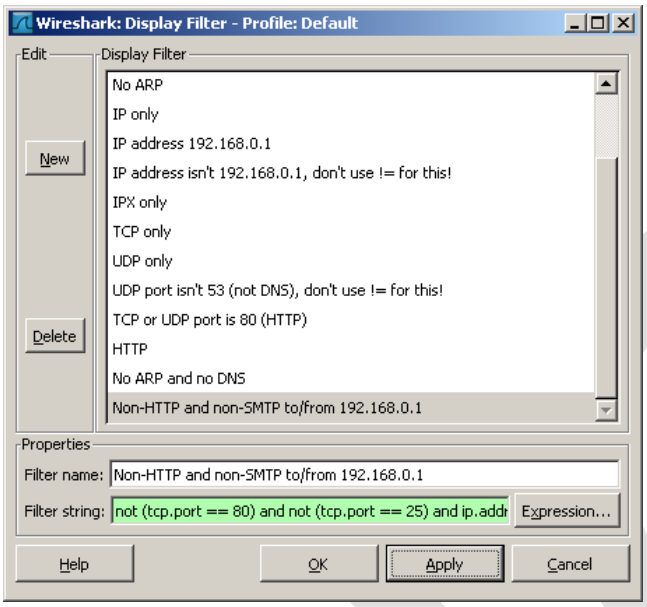
Sedaj se nam zastavi logična potreba, kaj če mene zanimajo samo TCP telegram in še to telegram, ki komunicirajo s portom 80(Http dobro znan(whell known) port)? Nastavimo filter v meniju Capture>>Capture_Filters.





Sestavljeni filtri

Vidimo, da smo zelo omejili prikaz zajetih telegramov. Na ta način lahko gradimo filter z uporabo boolovih operatorjev. Z nastavljenim filtrom lažje spremljamo dogajanje na mreži, ki zna biti zelo pestro. Stvar povratnega inžinirstva je potem rekonstruirati promet med parom strežnik/uporabnik. S tem orodjem lahko zlahka odkrijemo neželjen promet, ki ga lahko povzroča več vzrokov, še najverjetnejši so razni spy programi in virusi. Promet si lahko shranemo, za kasnejšo analizo.


Wireshark: Display Filter - Profile: Default
Edit
Display Filter
New
Delete
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
TCP or UDP port is 80 (HTTP)
HTTP
No ARP and no DNS
Non-HTTP and non-SMTP to/from 192.168.0.1
Properties
Filter name: Non-HTTP and non-SMTP to/from 192.168.0.1
Filter string: not (tcp.port == 80) and not (tcp.port == 25) and ip.addr
Expression...
Help
OK
Apply
Cancel

LITERATURA

1. ISBN 0-13-216987-8 Douglas E. Comer, Internetworking with TCP/IP, VOLUME I, Principles, Protocols, and Architecture
2. http://www.uga.edu/~ucns/lans/tcpipsem/
3. Žarko .Čučej, Moderni telekomunikacijski sistemi, Internetni protokol ,Maribor 23. avgust 2005, univerza v Mariboru, fakulteta za elektrotehniko
4. W. Richard Stevens, TCP/IP Illustrated, Volume 1, The Protocols, ISBN 0201633469
5. Gary R. Wright W. Richard Stevens, TCP/IP Illustrated, Volume 2, The Implementation, ISBN 020163354X
6. http://www.w3.org// - World Wide Web Consortium
7. http://www.w3schools.com/// - W3 Schools
8. http://en.wikipedia.org/// - Wiki pedija
9. http://www.wireshark.org/download.html
10. http://www.cryptool.org/index.php/en/download-topmenu-63.html