ISO-OSI medel

Datagr.	ISO-OSI	TCP-IP	prot.
podatki	aplikacijska	,.,,	НТТР,
podatki	predstavitvena	aplikacijska	DNS, POP3,
podatki	sejna		SSH
seg- menti	prenosna	transportna	TCP, UDP
paketi	omrežna	internetna	IP, ICMP
okvirji	povezavna	povezovalna	MAC,
biti	fizična		PPP

Fizična plast

Naloge:

- kodiranje bitov z neko fizikalno veličino (signalom) za prenos po mediju (baker, optika, radijski, IR, ...)
- prenos posameznih bitov v analogni ali digitalni obliki
- prenos celotnega signala (zaporedja bitov po mediju)
- pretvorba signala v obliko, ki je primerna za prenos po mediju

Modulacija

- amplitudna (1: velika amplituda, 0: majhna ampituda)
- frekvenčna (1: visoka frekvenca, 0: nizka frekvenca)
- fazna (1: zakodiramo z fazo 0°, 0: z fazo 180°)
- kvadratna
 - kombinacija amplitudne in fazne modulacije
 - 4 fazni koti 0°, 90°, 180° 270°
 - $-\,\,2$ nivoja amplitude
 - -~8kombinacij faze in amplitude \rightarrow 3 bite
 - lahko imamo tudi več faznih kotov in amplitud in naenkrat zakodiramo do 6 bitov

Povezavna plast

Lahko (ne pa njuno) opravlja naloge: okvirajanje datagramov, zaznavanje in odpravljanje napak, dostop do medija, zagotavljanje zanesljive dostave, kontrola pretoka.

Okvirianie datagramov

Okvir je *enota* na povezavni plasti. Določa začetek in konec prenesenih podatkov.

Zaznavanje in odpravljanje napak

dodamo bite za preverjanje pravilnosti (EDC - Error Detection Code)

- soda/liha pariteta vseh 1 skupaj s pariteto je sodo/liho (omogoča le zaznavanje lihega števila napak)
- dvo dimenzionalna pariteta dodamo praitetni bit za vsako vrstico in vsak stolpec + kumulativni/meta paritetni bit je pariteta paritetnih bitiv (omogoča zaznavanje in odpravljanje enojnih napak in zaznavanje dvojnih napak)
- Hammingova koda

Paritetni biti p imajo indekse 2^i in jih postavimo na mesta, ki jih določajo indeksi. Vmes vstavimo bite podatkov d.

Vsak paritetni bit p_i pokriva i bitov od svoje pozicije naprej, nato preskoči i bitiov in tako naprej. Število 1, ki jih paritetni bit pokriva mora biti sodo.

	1.	2.	3.	4.	5.	6.	7.
	p_1	p_2	d_1	p_4	d_2	d_3	d_4
p_1	✓		✓		✓		✓
p_2		✓	✓			✓	✓
p_A				✓	✓	✓	✓

Ko prejmomo sporočio, preverimo paritetne bite in definiramo:

$$p_i' = \begin{cases} 1 & \text{paritetni bit } p_i \text{ napačen} \\ 0 & \text{sicer} \end{cases}$$

Nato izračunamo sindrom:

 $[\dots p_4' \ p_2' \ p_1']_{(2)} = \#$ bita, ki ga je treba obrniti

- Cyclic Redundancy Check CRC z r paritetnimi biti lahko popravi do r + 1 napak
- Internet checksum uporablja se na transportni
 nlasti

Dostop do skupinskega medija

Imamo dve vrsti povezav: **dvotočkovna** (le en pošiljatel in prejemnik - PPP, DHLC) in **oddajna** (več vozlišč komunicira naenkrat - Ethernet, Wireless LAN).

Kanal lahko delimo na več načinov:

Delitev kanala

Time Division Multiple Access TDMA, Frequency Devision Multiple Access FDMA Ni kolizij

Sočasni/naključni dostop (kolizijski)

- ALOHA Če pride do kolizije, se paket po naključnem času ponovno pošlje.
- razsekana ALOHA Čas je razsekan na časovne intervale. V vsakem intervalu se lahko pošlje en paket. Če pride do kolizije, se v nasldnjem intervalu pošlje ponovno z verjetnostjo p.
- Carier Sense Multiple Access CSMA Poslušaj ali že kdo oddaja preden začeneš oddajati sam.
- Carier Sense Multiple Accerss Collision
 Detection CSMA/CD Če zaznaš kolizijo nehaj
 oddajati in pošlji motilni siganal.

Izmenični dostop

- Rezervacija s centralnim vozliščim (pooling): centralno vozlišče zaporedno dodeluje medij posameznim vozliščem (zakasnitev, ena točka odnovedi)
- Rezervacija z žetonom, ki kroži (token)
 (zakasnitev, ena točka odpovedi žeton)

Dostop do brezžičnega medija

Protokol 802.11 (WiFi) za dostop do medija uporablja Carier Sense Multiple Accerss Collision Avoidance - CSMA-CA.

Uporablja signala:

- Request To Send RTS
- Clear To Send CTS

Terminal, ki želi pošiljati najprej pošlje RTS in čaka na CTS. Ko terminal prejme CTS, ne bo oddajal toliko časa kot traja, da se prenese en paket.

Protokoli na povezavni plasti

Ethernet

Okvir ethernet:

pream- bula	ponorni nalosv	izvorni naslov	tip	podatki	CRC
8B	6B	6B	2B	1500B	4B

Ethernet ponuja:

- nepovezavna storitev
- nezanesljiva storitev (kontrola pravilnosti se izvaja s CRC a brez popravljanja, potrjevanje in ponovno pošiljanje se ne uporabljata)
- uporablja CSMA/CD (pri vsaki koliziji se čakanje eksponentno poveča 0 1, 0 3, 0 7, 0 15, . . .)

Point to Point Protocol - PPP

Povezavni protokol; imamo le enega pošiljatelja in prejemnika.

Okvir PPP:

zastavica za začetek	address	control	protokol	podatki	CRC	zastavica za konec
1B	1B	1B	1B/2B	≤1500B	2B/4B	1B

Poja "address" in "control" se ne uporabljata.

Pred niz 01111110 (zastavica) urivamo ubežno kodo 01111101.

Naslavljanje naprav na povezavni plasti

Vsaka naprava ima fizični naslov (Media Access Control - MAC) iz 48 bitov.

Naslov FF-FF-FF-FF-FF je brodcast (prejemniki so vsi).

Address Resolution Protocol - ARP

Vsaka naprava ima ARP tabelo [IP | MAC | TTL]

Če naprava želi ugotoviti MAC druge naprave, pošlje \mathbf{ARP} poizvedbo $(Moj\ max\ je\ y,\ kdo\ ima\ IP\ x^g)$ na brodcast naslov. Naparava, ki ima ta IP odgovori z \mathbf{ARP} odgovorom $(Jaz\ imam\ IP\ x\ in\ oj\ MAC\ je\ z.)$. Nato si obe napravi shranita MAC naslove v \mathbf{ARP} tabelo.

Stikalo

Stikalo uporablja **stikalno tabelo** [MAC | vrata | TTL], da se odloči, na katera vrata poslati okvir. Ko prejme kak okvir, si zapomni lokacijo pošiljatelja in okvir:

- poplavi na vsa vrata razen na tista iz katerih je prišel okvir (če ne ve, na katerih vratih je prejemnik)
- posreduje na izbrana vrata (če ve, na katerih vratih je prejemnik)
- filtriria / zavrže okvir (če je namenjen istim vratom iz katerih je prišel)

Omrežna plast

Lahko omogoča:

- 1. zagotovljena dostava paketov
- 2. dostava v zagotovljenem času
- 3. dostava v pravem vrstnem redu
- 4. zagotovljena spodnja meja pasovne širine
- 5. največja dovoljena varianca zakasnitve (jitter)
- varno komunikacijo (zaupnost integriteto podatkov, avtentikacijo)

Storitve interneta

		zagotovljene storitve				
Omrežje	Model	pas. širina	brez izgub	vr. red	čas	obv. o zamaš.
Internet	best effort	×	×	×	×	\times_{izguba}
ATM	CBR constant bit rate	const	✓	✓	✓	ni zamaš.
ATM	ABR available bit rate	min	×	✓	×	√

Usmerievalnik

Naprava, ki deluje na omrežni plasti in skrbi za transport datagrama po jedru omrežja. Povezuje ralične medije in portokole.

Funkcije usmerjevalnika:

- Posredovanje paketov/forwarding: prenos na pravi izhodni vmesnik glede na destinacijo paketa in posredovalno tabelo.
- Usmerjanje/routing: določanje poti paketov od izvora do cilja. Usmerjevalniki s poočjo usmerjevalnih protokolov najdejo najcenejšo pot.

Povezavna omrežia / navidiezni vodi

Faze pri vzpostavitvi navideznega voda: vzpostavitev, tok podatkov, rušenje

Usmerjevalniki usmerjajo pakete glede na *št. voda* v paketu in posredovalno tabelo [vhodni vmesnik | vhodna *št. voda* | izhodni vmesnik | izhodna *št. voda*].

Nepovezavna / datagramska omrežja

Ni faze vspostavljanja povezave. Paket lahko do cilja pride po različnih poteh.

Usmerjevalniki usmerjajo glede na ciljni (IP) naslov in usmerjevalno tabelo [predpona naslova | vmesnik].

Internet Protocol - IP

Paket IPv4

Dolžina glave brez "možnosti" je 20B.

4b	4b	4b	4b	4b	4b	4b	4b	
Verzija	Dolžina glave	Tip st	coritve	Skupna dolžina				
	Identifikacija Zastav.					av. Zamik fragmenta		
T	ΓL	Prot	okol	Kontrolna vsota				
	Izvorni IP naslov 32b							
Ponorni IP naslov 32b								
$Mo\check{z}nosti$				Zpolnjevanje			evanje	
Podatki								

Fragmentacija

IP datagram se mora enkapsulirati v omejene okvirje (MTU) povezavne plasti. Zato se IP paket razbije na več manjših. Da fragmente lahko sestavimo nazaj se uporabljajo polja v glavi:

- ID: pri vseh fragmentih enak
- Zastavica MF: 0, če je to zadnji fragment; 1, sicer

Podomrežia

• Offset: enota za odmik je 8 Byte

Razred	Začetek naslova	Maska
A	0 xxxxxxx	255.0.0.0
В	10 xxxxxx	255.255.0.0
C	110 xxxxx	255.255.255.0
D	1110 xxxx	-
E	11110 xxx	-

Posebni naslovi

- Privatni (24 bitni) 10.0.0.0/8
- Privatni (20 bitni) 172.16.0.0/12
- Privatni (16 bitni) 192.168.0.0/16
- Povratna zanka (localhost) 127.0.0.0/8
- Link-local 169.254.0.0/16

Posebni naslovi v lokalnem omrežju

- Naslov omrežja: 1. naslov v omrežju (same ničle)
- Hosts: vsi naslovi vmes
- Brodcast: zadnji naslov v omrežju (same enke)

Dinaminčno dodeljevanje naslovov - DHCP

Ko se naprava priključi v omrežje, pošlje **DHCP discover**, DHCP strežnik(i) odgovori(jo) z **DHCP offer**, naprava izbere IP iz ponudbe in pošlje **DHCP request**, končno strežnik potrdi z **DHCP ACK**.

Internet Control Message Protocol - ICMP

Sporočilo je enkapsulirano v paketu IP. Uporablja se za sporočanje napake, nedosegljivosti, protokola, vrat, \dots

Traceroute pošlje vrsto paketov z TTL=1,2,3,... vsakič ko paketu poteče TTL router pošlje nazaj ICMP sporočilo.

Network Address Translation - NAT

Lokalne naslove slika v globalne in obratno.

To doseže z NAT preslikovalno tabelo [globalni naslov, port \mid zasebni naslov, port].

Vsak zahtevek ima izvorni in ponorni port/vrata.

IPv6

Naslovi so razdeljeni (:) na 8 blokov po 16 bitov. Zaporedje blokov samih ničel lahko krajšamo z "::",

Dolžina glave je vedno 40B.

4b	4b	4b	4b	4b	4b	4b	4b
Verzija	Traffic class			Flow label			
	Payload len			Next header Hop limit			limit
	Izvorni IP naslov 128b						
Ponorni IP naslov 128b							
Podatki							

Novo polje "flow label" (vrsta toka) za zagotavljanje kakovosti storitev za posebne tokove podatkov.

Prehodni mehanizmi

- Dvojni slkad: Vse naprave imajo IPv4 in IPv6. Če je na poti kakšno IPv4 vozlišče, se bo proromet vmes pretvarjal v IPv4.
- Tuneliranje: Če je na poti kakpno IPv4 vozlišče se IPv6 paket enkapsulira v IPv4.

Usmerjanje

Usmerjevalni algoritmi so lahko:

- centralizirani (imajo podatke o celem omrežju) ali decentralizirani (imajo podatke le o sosednjih vozliščih)
- prilagodljivi (lahko prilagajajo cene povezav glede na zasičenost) ali naprilagodljivi

Decentralizirano usmerjanje

Vsako vozlišče pozna ceno povezave do svojih sosedov. Hrani **vektor razdalj, vektorje razdalj svojih sosedov** in **posredovalno tabelo** [cilj | cena | via sosed].

Ko vozlišče prejme vkektor razdalj svojega soseda, izračuna nov vektor razdalj če lahko do nekega vozlišča pride ceneje prek nekega soseda, posodobi posredovalno tabelo.

Usmerjevalniki so povezani v **avtonomne sisteme - AS** v katerih uporabljajo isti $\mathbf{INTRA-AS}$ usmerjevalni protokol.

- Routing Information Protocol RIP usmerjanje z vekotrjem razdalj (na 30s, 180s+ → prekinjena povezava), cena je število skokov, max cena je 15M
- Open Shortest Path First OSPF obvestila se s poplavljanjem posredujejo po celem sistemu, vsak potem preračuna najkrajše poti
- Interior Gateway Routing Protocol IGRP Cisco-va izboljšava RIP; cena je odvisna od pasovne širine, zakasnitve, obremenitve, MTU in zanesliivosti.

Za povezovanje AS mad seboj se uporablja INTER-AS usmerjevalni protokol, ki pa morabiti enak v celem omrežju.

 Border Gateway Protocol - BGP omogoča, da omrežja oglašujejo svojo prisotnost drugim omrežjem

/1	128.0.0.0
/2	192.0.0.0
/3	224.0.0.0
/4	240.0.0.0
/5	248.0.0.0
/6	252.0.0.0
/7	254.0.0.0
/8	255.0.0.0
/9	255.128.0.0
/10	255.192.0.0
/11	255.224.0.0
/12	255.240.0.0
/13	255.248.0.0
/14	255.252.0.0
/15	255.254.0.0
/16	255.255.0.0
/17	255.255.128.0
/18	255.255.192.0
/19	255.255.224.0
/20	255.255.240.0
/21	255.255.248.0
/22	255.255.252.0
/23	255.255.254.0
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252
/31	255.255.255.254
/32	255.255.255.255

Transportna plast

Naloge transportne plasti so:

- $\bullet\,$ povezovanje dveh oddaljenih procesov
- multipleksiranje/demultipleksiranje komunikacije med procesi
- zanesljiv prenos podatkov
- kontrola pretoka in zasičenja

Vrata - port

FTP-data: 20, FTP-cmd: 21, SSH: 22, Telnet: 23, SMTP: 25, DNS: 53, HTTP: 80, POP3: 110, IMAP: 143, IRC: 194, HTTPS: 443

User Datagram Protocol: UDP

Nepovezavna storitev, nudi le best-effort: ni zagotavljanja vrstnega reda, ni nadzora zamašitev, ...

Dolžina glave je le 8B.

16b	16b		
Izvorna vrata	Ponorna vrata		
Dolžina (skupaj z glavo) v B	Internetna kontrolna vsota		

Internetna kontrolna vsota

Pošiljatelj: pošiljatelj sešteje 16 bitne besede in shrani eniški komplement = kontrolna vsota Prejemnik: sešteje 16 bitne besede skupaj s kontrolno vsoto → dobiti mora same enice

Potrjevanje

sprotno potrjevanje: po vsakem pošiljanju počakaj na potrditev

tekoče pošiljanje: večji razpon za številčenje paketov, shranjevanje paketov na obeh straneh

- ponavljanje N potrjenih (go-back-N)
 - pošiljatelj hrani okno največ dovoljenih nepotrjenih paketov
 - ACK(n) potrdi vse pakete do vključno n
 - časovna kontrola za najstarejši paket, ko poteče pošlji vse nepotrjene pakete na novo
- ponavljanje izbranih (selective repeat)
 - prejemnik shranjuje sporočila in jih sortira pred dostavo
 - pošiljatel ponovno pošlje le tiste pakete za katere ni prejel potrdila
 - vsak paket ima svojo časovno kontrolo

neposredno: uporaba ACK in NCK posredno: samo ACK, namesto NCK se ponovi ACK zadnjega segmenta

Transfer Control Protocol: TCP

Povezavna storitev, full duplex, zanesljiv, kontrola pretoka, kontrola zasičenja, tekoče pošiljanje in neposredno potrjevanje

10	6b		16b
Izvorna vrata			Ponorna vrata
Dolžina (skupe	ıj :	z glavo) v B	Internetna kontrolna vsota
		zaporedno	ı št. (B)
		št. potrdi	tve (B)
Dolzina glave	0	zastavice	sprejemno okno
Internetna kontrolna vsota			karalec urg. data
opcije (spremenljiva dolžina)			

Dolžina glave (4b) je podana v številu 32-bitnih besede

Sprejemno okno (16b) št. bajtov, ki jih sprejemnik lahko sprej
me

Zastavice (9b):

- URG*: urgentni podatki
- ACK: potrditev povezave
- PSH: takoj predaj aplikaciji
- RST, SYN, FIN: vzpostavljanje in rušenje povezave

Vzpostavitev povezave - trojno rokovanje

- Odjemalec pošlje segment z zastavico SYN (sporoči začetno številko segmenta, ni podatkov)
- Strežnik vrne segment SYN ACK (rezervira medpomnilnik, odgovori z začetno številko svojega segmenta)
- Odjemalec vrne ACK, lahko že s podatki ("štuporama")

Rušenje povezave

- $1.\,$ odjemalec pošlje segment TCP FIN strežniku
- 2. strežnik potrdi z ACK, zapre povezavo, pošlje FIN
- odjemalec prejme strežnikov FIN, potrdi ga z ACK (počaka časovni interval, da po potrebi ponovno pošlje ACK, če se ta izgubi)
- 4. strežnik sprejme ACK, končano

Nastavitev časovne kontrole

Na potrditev moramo čakati vsaj RTT (Round Trip Time).

Način potrjevanja

TCP uporablja podobno strategijo kot ponavljanje N nepotrjenih. Pošiljatelj ima časovno kontrolo le za najstarejši nepotrjen segment, vendar ob poteku časovne kontrole ne pošlje vseh segmentov v oknu, temveč le najstarejči nepotrjen segment.

RFC2018 vpeljuje potrjevanje le izbranih paketov.

Dogodek pri prejemniku	Odziv prejemnika
	Počakaj na naslednji segment max 500 ms. Če ta pride v tem intervalu, izvedi zakasnjeno potrditev obeh (delayed ACK). Če ne pride v tem intervalu, potrdi samo prejetega.
	Takoj pošlji <i>kumulativno</i> potrditev za oba segmenta brez izvajanja zakasnjene potrditve.
	Takoj potrdi zadnji še sprejeti segment ($pošlji duplikat ACK$).
Sprejem segmenta z najnižjo številko iz vrzeli (polnjenje vrzeli)	Takoj potrdi segment.

Hitro ponovno pošiljanje (fast retransmit)

Ponovno pošiljanje se običajno izvede po preteku časovne kontrole. Če pa pošiljatel prejme 3 potrditve za že potrjen paket, takoj izvede ponovno pošiljanje.

Kontrola pretoka

Usklajevanje hitrosti pošiljanja med pošiljateljem in prejemnikom.

Prejemnik sporoča razpolžljiv prostor v pomnilniku v polju 'sprejemno okno':

rwnd = velikost - [lastByteRcvd - lastByteRead]

Nadzor zasičenja

Določimo congestion window (cwnd).

 $\min(\mathtt{rwnd},\mathtt{cwnd})$ določa št. največ nepotrjenih paketov preden moramo čakati.

```
\begin{aligned} & \texttt{OcenjenRTT}[i] = (1-\alpha) \texttt{OcenjenRTT}[i-1] + \alpha \texttt{IzmerjeniRTT}[i] \\ & \texttt{DevRTT}[i] = (1-\beta) \texttt{DevRTT}[i-1] + \beta \big| \texttt{IzmerjeniRTT}[i] - \texttt{OcenjenRTT}[i] \big| \\ & \texttt{CakalniInterval}[i] = \texttt{OcenjenRTT}[i] + 4 \texttt{DevRTT}[i] \end{aligned}
```