UVOD

DOSTOP DO OMREŽJA

- Modemski/klicni – telefon zaseden
- DSL – individualen dostop
- Kabelski – TV infrastruktura

OMREŽJE

- Povezan način – eno povezava za vsak prenos
- Nepovezan način – po paketih

PLASTI (ISO/OSI)

- Aplikacijska – podatki
- Predstavitvena – podatki
- Sejna – podatki
- Transportna – segment
- Omrežna – paket
- Povezavna – okvir
- Fizična – bit/signal

FIZIČNA PLAST

NALOGE

- **Kodiranje bitov**
- **Prenos posameznih bitov**
- **Prenos celotnega signala**
- **Pretvorba signala**

MODULACIJA

- Amplitudna
- Frekvenčna
- Fazna
- Kvadratna (Amplitudna in fazna)

POVEZAVNA PLAST

header	data	tail

PROTOKOLI

- Ethernet
- WiFi
- Token ring
- PPP

EDC

2D

Liha → liho št. 1

Soda → sodo št. 1

10101 | 0
11110 | 1
01110 | 0
11010 | **1** – komulativni bit

HAMMINGOVA KODA

- 7 bit code, check bit positions 1, 2, 4
- Check 1 covers position 1, 3, 5, 7
- Check 2 covers position 2, 3, 6, 7
- Check 4 covers position 4, 5, 6, 7

0 1 0 0 1 1 1
P1 = 0+0+1+1 = 0
P2 = 1+0+1+1 = 1
P4 = 0+1+1+1 = 1
Syndrome = 110 → flip position 6

NALOGE

- okvirjanje datagramov
- zaznavanje in odpravljanje napak
- dostop do medija
- zagotavljanje zanesljive dostave
- kontrola pretoka

KOLIZIJE

Delitev kanala (TDMA, FDMA)

Naključni dostop

- Aloha – paket se pošlje enkrat po naključju (18%)
- Razs. Aloha – enaki časovni intervali (37%)
- CSMA – poslušaj ali že kdo oddaja
- CSMA/CD (ethernet) – prekini (jam signal)
- CSMA/CA (WiFi) – RTS, CTS
  - Skriti terminal (A – B – C)
  - Izpostavljeni terminal (B – A – C – D)

Izmenični dostop

- Centralno vozlišče
- Žeton (token ring)

ETHERNET

Topologija

- Vodilo – ista kolizijska domena
- Zvezda – ločena kolizijska domena

Preamble	Dest. Addr.	Source Addr.	Type	Data	CRC
7x 10101010 1x 10101011	6B	6B	2B IP/ARP...	46 – 1500B MTU = 1500B	4B

- Nepovezana storitev – ni rokovanja
- CRC (Cyclic redundancy check)
- Potrjevanja in ponovnega pošiljanja **NI**
- CSMA/CD → jam signal (oznanitev kolizije)

PPP (POINT TO POINT)

Start	Address	Control	Protocol	Info	Check	End
1B	1B	1B	1B/2B	~	2B/4B	1B

- Povezava med dvema točkama
- En pošiljatelj in en prejemnik

Stuffing

- Escape sequence 0111101, da vemo, da ni začetek/konec

NASLAVLJANJE NAPRAV

MAC ADDRESS

- Strojni naslov – fizični in stalni
- 48 bitov = 6B → 12HEX znakov
  - A – 10 (1010)
  - B – 11 (1011)
  - C – 12 (1100)
  - D – 13 (1101)
  - E – 14 (1110)
  - F – 15 (1111)

ARP

IP naslov	MAC naslov	TTL (min 20)

ARP query – polnjenje tabele

- Naprava z IP poizve po MAC

NAPRAVE

Repeater – ojačevalec signala
Hub – razdelilec, ista kolezijska domena
Switch – forwarding, flooding, filtering (tabela)

VLAN

- Deluje kot stikala, ampak virtualno

OMREŽNA PLAST

STORITVE

- **zagotovljena dostava** paketov
- dostava paketov v **zagotovljenem času**
- dostava paketov v **pravem zaporedju**
- zagotovljena spodnja **meja pasovne širine**
- največja dovoljena **varianca zakasnitve** (jitter):
- **varno komunikacijo** (zaupnost, integriteto podatkov, avtentikacijo)

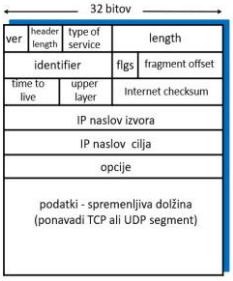
USMERJEVALNIK

- Usmerjanje – določitev poti od izvora do cilja
- Posredovanje – iz vhodnega na izhodni vmesnik

VRSTA OMREŽJA

- Povezavna – vodi (povezava med prej. in poš.) → posredovalne tabele (longest prefix)
- Nepovezava – paketna (posredovanje paketov)

IPV4



- **VER** (4b): verzija IP protokola
- **HEADER LENGTH** (4b): dolžina glave (v 32-bitnih besedah), poda, kje se začnejo podatki
- **TYPE OF SERVICE** (8b): za razlikovanje datagramov, ki potrebujejo "posebno" obravnavo
- **LENGTH** (16b): skupna dolžina celega datagrama v Byte-ih (običajno dolžina 1500B)
- **ID, FLAGS, OFFSET** (32b): potrebno za IP fragmentacijo
- **TTL** (8b): za preprečitev ciklanja datagramov po omrežju, vsak usmerjevalnik zmanjša vrednost za 1
- **UPPER LAYER** (PROTOCOL) (8b): številka enkapsuliranega protokola v podatkih (6-TCP, 17-UDP)
- **CHECKSUM** (16b): kontrolna vsota (samo) glave datagrama, preračuna jo vsak usmerjevalnik
- **IPv4 naslovi** (32b): naslovi izvora in cilja (začetnega in končnega sistema)
- **OPCIJE** (32b): za možne razširitve glave datagrama (slabosti: večji čas procesiranja, neznana lokacija začetka podatkov; običajno jih ni, glava dolga 20B)
- **PODATKI** (spremenljiva dolžina)

FRAGMANTACIJA

- **MTU** – maximum transmission unit
- **MF/DF** – more fragments/don't fragment
- **OFFSET** – odmik 8B → $offset = \frac{data-header}{8}\ (if\ \%\ 8\ !=0,$ zaokrožiš navzdol)

RAČUNANJE IPV4

163.146.71.40/9
10100011.10010010.01000111.00101000

Omrežje:	163.128.0.0
Prva naprava:	163.128.0.1
Zadnja naprava:	163.255.255.254
Broadcast:	163.255.255.255
Št. naprav:	$2^{32-maska=23} - 2 = 8388606$

DHCP

- Discover
- Offer
- Request
- ACK

→Dobiš svoj IP

NAT

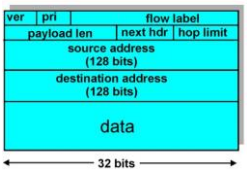
Uporaba ponovljivih lokalnih IPjev

Globalni IP, Port	Zasebni IP, Port

IPV6

Fiksna glava, ni opcij, ni checksuma

- **IPv6 naslovi** – 128b (8 x 16b (Hex))



- **VER** (4b): verzija IP protokola (6)
- **PRI ali TRAFFIC CLASS** (8b): podobno kot Type Of Service pri IPv4, oznaka prioritete za posebne pakete/aplikacije
- **FLOW LABEL** (20b): oznaka "toka" podatkov, ki omogoči posebno zagotavljanje kakovosti storitve (npr. audio/video)
- **PAYLOAD LENGTH** (16b): velikost podatkov, ki sledijo glavi
- **NEXT HDR** (8b): tip enkapsuliranega protokola
- **HOP LIMIT** (8b): enako kot TTL

PREHOD

Dual stack (Dvojni sklad)

- promet se pretvarja da je IPv4

Tunneling (Tuneliranje)

- IPv6 zapakiramo v IPv4

USMERJEVALNI PROTOKOLI

Centralizirani

- Centralno vozlišče koordinira usmerjanje (link-state)
- Tabela najkrajših poti

Decentralizirani

- Vsako vozlišče ima svojo posredovalno tabelo na osnovi podatkov podanih od sosedov
- Usmerjanje je iterativno

PORAZDELJENO USMERJANJE

Good news travel fast

- Podatek o znižanju cene povezav se hitro širi

Bad news travel slow

- Podatek o zvišanju cene se širi počasi

INTRA-AS USMERJANJE

RIP

- Vektorji razdalj → cena povezave (1 hop) je 1, max cena poti = 15

OSPF

- Usmerjanje glede stanje povezav → preračuna najkrajšo pot

IGRP

- Izboljšava RIP, vektorji razdalj glede MTU, zakasnitve…

INTER-AS USMERJANJE

BGP

- Omrežja oglašujejo prisotnost drugim

TRANSPORTNA PLAST

STORITVE

- Povezovanje dveh procesov
- Multipleksiranje/demultipleksiranje komunikacije
- Zanesljiv prenos podatkov
- Kontrola pretoka, zasičenosti

SOCKET

- Vsak proces ima svoj socket (<IP naprave | port procesa>)

PORT SCAN

- Napad, kjer napadalec preveri na katera vrata se strežnik odzove

PROTOKOLI

UDP

- Best-effort, nezanesljiv, hiter in preprost

Kontrolna vsota

- 2x16bitov sešteješ (Carry se prišteje na začetek)
- Eniški komplement (obrat bitov) → Kontrolna vsota
- Sešteješ podatek (2x16bitov) in kontrolno vsoto, če so same enice je OK

TCP

Napake

- Izguba paketov
- Izguba potrditve
- Prekratek časovni interval → podvojeni paketi (zato se števiči pakete)

Potrjevanje

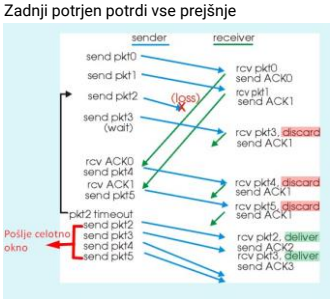
- Neposredno – ACK in NACK
- Posredno – samo ACK

Pošiljanje

- Sprotno – vsak paket posebej
- Tekoče – več paketov z drsečim oknom (GBN, SR)

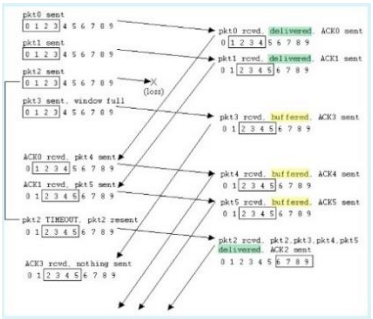
Go-Back-N (GBN)

- Štoparica za najstarejši paket
- Zavrže paket če ni po vrsti (ACK za najstarejšega)
- Zadnji potrjen potrdi vse prejšnje

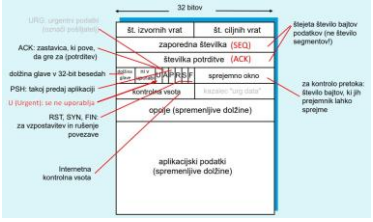


Selective repeat (SR)

- Vsak paket potrjuje posamezno
- Pošlje le paket za nepotrjenega
- Štoparica za vsak nepotrjen paket
- Prejemnik hrani pakete tudi, če kaj od prej manjka



TCP segment



- SEQ = prejšnji ACK
- ACK = prejšnji SEQ + data

Three-way Handshake – Vzpostavljanje povezave

- → syn seq=x →
- ← syn ack=x+1 seq =y ←
- → ack=y+1 seq=x+1 →
- → data(+ lahko že pošlje podatke) →

Rušenje povezave

- → FIN → (odjemalec pošlje request za zaprtje)
- ← ACK ← (strežnik potrdi)
- |čas interval začne| ← FIN ← (strežnik zapre povezavo)
- → ACK → (zveza zaprta)
- |čas interval konča| (v primeru da ni ACK pošlje še enkrat)

Napada SYN FLOOD

- Napadalec pošlje več zahtev za odprtje povezave SYN in zapolni strežnik

RTT

- $OcenjeniRTT[i] = (1-\alpha) * OcenjeniRTT[i-1] + \alpha * IzmerjeniRTT[i]$
- $DevRTT[i] = (1-\beta) * DevRTT[i-1] + \beta * |IzmerjeniRTT[i] - OcenjeniRTT[i]|$
- $CakalniInterval[i] = OcenjeniRTT[i] + 4 * DevRTT[i]$

Potrjevanje pri TCP

- Štoparica na 500ms po prejetem paketu – po tem času →ACK
- Če prejme takoj novega, oba takoj potrdi z ACK za zadnjega
- Če se paket izgubi takoj pošlje ACK zadnjega prejetega
- Če čaka izgubljene jih potrdi takoj ko jih dobi – ni čas. intervala

Hitro ponovno pošiljanje (fast retransmit)

- Ko dobi tri kopije (4. zaporedni) ACK za isti paket ga takoj ponovno pošlje – ne čaka časovnega intervala

Kontrola pretoka

- $rwnd = velikost - [LastByteRcvd - LastByteRead]$
- Prejemnik sporoča pošiljatelju svoj preostali prostor $rwnd$

Kontrola zasičenosti

- $cwnd$ – congestion window
- Eksponentno (2x, slow start, do **praga**) → povečuje eksponentno
- Linearno (+1, izogib zasičenju, od **praga**) → povečuje po ena
- Potek čas. intervala (Timeout) → zmanjša $cwnd$ na 1 → $prag = \frac{cwnd}{2}$
- Fast recovery (3x podvojeni ACK) → $prag = \frac{cwnd}{2}$, $cwnd = \frac{cwnd}{2} + 3$

Razvoj nadzora zasičenosti

- Tahoe – izguba vedno na $cwnd = 1$
- Reno – 3x ACK → $cwnd = \frac{cwnd}{2} + 3$
- Vegas – linearno zmanjšanje ob zasičenju

APLIKACIJSKA PLAST

Aplikacija	protokol aplikacijskih protokolov	dovoljena izguba	potrebna minimalna časovna širina	časovno občutljivost	obstajajo transportni protokoli
prenos datotek	FTP	ne	ne (elastična)	ne	TCP
e-pošta	SMTP, POP3, IMAP	ne	ne (elastična)	ne	TCP
splet	HTTP	ne	ne (elastična)	ne	TCP
oddaljeni dostop	telnet	da	~10 kb/s	da	TCP
multimedija (realni čas)	RTP, HTTP	da	10 kb/s – 5 Mb/s	da	TCP/UDP
multimedija (shranjena)	RTP, HTTP	da	10 kb/s – 5 Mb/s	da	TCP/UDP
interaktivne igre	HTTP, lastniki	da / ne (?)	~10 kb/s	da	TCP/UDP
IP telefonija	SIP, RTP, lastniki	da	100 kb/s – 3 Mb/s	da	TCP/UDP

PORTI

- DNS - 53, UDP
- DHCP - 67/68, UDP
- FTP - 20/21, TCP
- SSH - 22
- TELNET – 23
- SMTP - 25, TCP
- POP3 - 110, TCP
- IMAP - 143, TCP
- HTTP - 80, 8080, TCP
- HTTPS – 443

HTTP

Statusi v HTTP odgovorih

- 1xx – informativne kode
- 2xx – uspešno
- 3xx – preusmeritev
- 4xx – napaka pri odjemalcu
- 5xx – napaka na strežniku

Vrste povezav

- **Nevztrajne** – za vsak prenesen objekt se vzpostavi nova TCP povezava
- **Vztrajne** – strežnik uporabi isto povezavo za prenos več objektov
- **Vztrajne s cevovodom** – tekoče pošiljanje več zahtev naenkrat

Medstrežnik (Proxy)

- Hrani kopje strani
- Pogojna zahteva – `If-modified-since: Mon, 31 may 2021 09:32:22`

FTP

- Port 20 – prenos podatkov
- Port 21 – kontrola (login, ukazi…)
- Aktivni način – strežnik odpre
- Pasivni način – odjemalec odpre

Ukazi

- USER ime
- PASS geslo
- LIST
- RETR ime_datoteke
- STOR ime_datoteke

ELEKTRONSKA POŠTA (MAIL)

- Poštni strežniki
- Odjemalski programi
- Protokol za prenos sporočil (SMTP)

SMTP

- TCP Port 25
- 7-bitni ASCII
- PUSH princip
- Dostava pošte do prejemnikovega strežnika

POP

- TCP Port 110
- Prejem pošte s poštnega strežnika

IMAP

- Kompleksen, več funkcionalnosti
- Večja obremenitev strežnika

DNS

- UDP Port 53
- Type:
  - A – address (AAAA = IPv6)
  - NS – name server
  - CNAME – canonical name
  - MX – mail exchange

Name	Value	Type	TTL

Korenski strežnik

- 13 korenskih strežnikov

TLD strežniki

- Generične domene – com, org, edu…
- Domene držav – si, uk, it…

Avtoritetivni strežniki

- amazon, yahoo…

POTEK:

Uporabnik potrebuje IP od www.amazon.com

- povpraša korenski strežnik po TLD strežniku za domeno .com
- povpraša .com TLD strežnik po naslovu avtoritativnega strežnika amazon.com
- povpraša strežnik podjetja amazon.com po IP naslovu za www.amazon.com

Lokalni DNS strežnik

- posrednik do DNS hierarhije (zgoraj navedeni strežniki)
- rekurzivna poizvedba

P2P

- ni strežnika, ki bi bil nenehno prižgan
- izmenjava podatkov med poljubnima končnima sistemoma
- skalabilnost – krajši čas prenosa (več seed-erjev namesto enega strežnika)

BitTorrent

- skupina odjemalcev, ki si delijo kose (chunks)
- **tracker** – admin strežnik
- **podmnožica sosedov** – z njimi izvaja izmenjavo
- rearest first
- vzpodbuda k sodelovanju
- zainteresiran in zamašen (kontrolna bita)

Skype

- supernodes – hranijo upr. ime in IP
- relay – zaradi NAT
- A in B vzpostavita prvo povezavo preko relay-a (dobita IP), nato lahko direktno vzpostavita povezavo

PODPORNE STORITVE

Predstavitvena plast

- Predstavitev podatkov – v nevtralen jezik
- Predstavitev alfa numeričnih znakov – ASCII
- Stiskanje podatkov
- Zaščita podatkov – kriptografija

Sejna plast

- Vzpostavljanje, rušenje, vzdrževanje sej med aplikacijama
- Protokoli – H.245, RTCP, SCP

KRIPTOGRAFIJA

SUBSTITUCIJA

Cezar

- Zamik za k črk

Vinegarjev

- Vsaka črka ima svojo abecedo glede na ključ

Porterjev kriptogram

- Kriptiranje s simboli (2D tabela)

TRANSPOZICIJA

- Ključ (neka beseda)
- Katera po abecedi je črka ključa
- Polnimo za dolžino ključa dolge vrstice

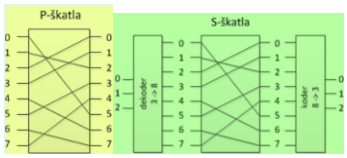
BLOČNA KRIPTOGRAFIJA

P – škatla

- Premeče bite
- Ima svoj ključ (primer: 2315746)

S – škatla

- Dekoder → P-škatla → Koder



DES

- Trans.→16 preslikav→SWAP→~Trans.

3DES

- K1(enkr)→K2(dekr)→K3(enkr) ponoviš←

Verižno kriptiranje blokov

- Pošiljatelj $c(i) = K\big(m(i)\ xor\ c(i-1)\big)$
- Prejemnik $m(i) = K^{-1}\big(c(i)\big)\ xor\ c(i-1)$

RSA

- $n = p * q$
- $z = (p-1) * (q-1)$
- ENCR. $m \rightarrow c = m^e\ mod\ n$
- DECR. $c \rightarrow m = c^d\ mod\ n$
- **Javni ključ** → $E(n, e)$
- **Zasebni ključ** → $D(n, d)$
- e nima skupnih deliteljev z z
- d je tak, da $e * d\ mod\ z = 1$

OPERATIVNA VARNOST

FIREWALL

Vrste filtriranj:

- **Izolirano filtriranje** – glede na vsebino paketa (IP, Port…)
- **Filtriranje paketov v kontekstu** – response je dovoljen če je bil prej izveden request
- **Dostopni seznam**:

izvorni naslov	ciljni naslov	protokol	izvorna vrata	ciljna vrata	zastavica	akcija
222.22/16	izven 222.22/16	TCP	> 1023	80	any	dovoli
izven 222.22/16	222.22/16	TCP	80	> 1023	ACK	dovoli
222.22/16	izven 222.22/16	UDP	> 1023	53	---	dovoli
izven 222.22/16	222.22/16	UDP	53	> 1023	-----	dovoli
all	all	all	all	all	all	zavrzi

- **Aplikacijski prehodi** – glede na uporabnika

SISTEMI ZA ZAZNAVANJE VDOROV

- IDS – zazna in sporoči o napadu
- IPS – zazna napad in ukrepa

Primerjava s shranjenimi vzorci

- Izvorni IP, zaporedje bitov…

Opazovanje netipičnega prometa

- Sistem reagira na statistično neobičajen promet

NAPADI

1. prisluškovanje in ponarejanje sporočil
2. matematični napadi – kripto. algoritmi/ključi
3. ugibanje gesel (brute force, slovar…)
4. virusi, črvi, trojanci
5. izkoriščanje šibkosti v programski opremi
6. socialni inženiring
7. pregled vrat (port scan)
8. brskanje po smeteh (dumpster diving)
9. rojstnodnevni napad – napad na zgoščevalne funkcije
10. zadnja vrata (back door)
11. ponarejanje IP naslovov (IP spoofing)
12. prestreganje komunikacije (MITM)
13. ponovitev komunikacije (replay)
14. ugrabitev TCP sej (TCP hijacking)
15. napadi s fragmentacijo
16. odpoved delovanja sistema (DOS/DDOS)

DOS – Denial of Service

1. Prekoračitev medpomnilnika – pošljemo preveč podatkov
2. SYN napad – ne končamo z rokovanjem
3. Teardrop – spremeni št. fragmentov
4. Smurf – broadcast za preobremenitev
5. Bots