TCP

Razdelki: vrata, SEQ in ACK (prvi naključen, štejeta št. bajtov podatkov!), dolžina glave, zastavice RST, SYN, FIN, okno za kontrolo pretoka, kontrolna vsota.

Trojno rokovanje – SYN (x seg=x), nazaj SYN, ACK(x+1, seg=y), nazaj ACK(y+1, seg=x+1) – tu so lahko zraven že podatki, tj. piggybacking.

Rušenje povezave – enako kot handshake, namesto SYN je FIN. FIN →; ACK ←; FIN ←; ACK →; wait → CLOSED

Način potrjevanja – Delayed ACK če v 500ms prideta dva paketa. Če zaznamo luknjo še enkrat pošljemo zadnji ACK. Ko dobiš ta segment takoj pošlješ ACK.

Fast retransmit – če dobiš nazaj tri ponovljene ACK, takoj pošlješ še enkrat tistega za tem ACK.

Kontrola pretoka – rwnd poslan v vsaki glavi segmenta. Rwnd je velikost prostega prostora v medpomnilniku.

Congestion control – Slow start: cwnd = 1, za vsak ACK ga zvečaš za 1, ob izgubi nastaviš prag = cwnd/2, cwnd = 1, ko pride do praga gre v congestion avoidance

Congestion avoidance: cwnd linearno povečuješ za 1, če dobi 3 duplikate gre v fast recovery.

Fast recovery: cwnd = cwnd/2 + 3 prag = $\frac{cwnd}{2}$

Če uporabljaš UDP in TCP v istem omrežju UDP pobere veliko večino bandwidtha. TCP pošilja s hitrostjo min(rwnd, cwnd)

Ocenjevanje RTT

OcenjeniRTT[i] = (1−α) * OcenjeniRTT[i−1] + α * IzmerjeniRTT[i]

DevRTT[i] = (1+β) * DevRTT[i−1] + β * |IzmerjeniRTT[i] − OcenjeniRTT[i]|

Čakalni interval[i] = OcenjeniRTT[i] + 4*DevRTT[i]

Aplikacijska plast

Aplikacijsko sporočilo je osnovna enota. Poznamo 3 različne arhitekture: odjemalec–strežnik, P2P, mešana

HTTP

Dostop na zahtevo, stateless. Na vratih 80. Deluje v smislu request – response. Za potrditve, ponovitve skrbi TCP.

Request

Kode v odgovorih: 1xx – informative, 2xx – uspešno, 3xx – preusmeritev, 4xx – napaka na odjemalcu, 5xx – napaka na strežniku.

Vrste povezav:

Nevztrajne: za vsak objekt nova TCP povezava (2 RTT/objekt).

Vztrajne: ista povezava za več objektov (1 RTT/objekt)

Vztrajne s cevovodom: več zahtev naenkrat brez čakanja na prejem prejšnih. Pri vztrajnem se povečuje še cwnd, tako, da je še hitrejše.

Piškotki

Imamo jih ker je HTTP stateless in ne razlikuje med odjemalci. Shranjeni so pri odjemalcu. Server hrani evidenco izdanih piškotkov. ID piškotka se pošilja v glavi requesta/responsa.

Medstrežnik – Proxy

Odgovarja na zahteve namesto strežnika. Ima kopije spletnih strani. Če nima, pošlje req. na server. Odjemalec mora biti ustrezno konfiguriran. Hitrejši odgovor, manj prometa.

Pogojna zahteva if-modified-since: datetime. Odgovor če se ni spremenila: HTTP/1.1. 304 Not Modified.

FTP

Vzpostavi dve ločeni povezavi, kontrolno (vrata 21) in podatkovna (vrata 20). Sporočila: USER ime, PASS geslo, LIST, RETR file, STOR file.

Odgovori strežnika: 331 Username OK, pass required, 125 Data connection open, transfer starting, 452 Error writing file, 425 can't open data connection.

Elektronska pošta

Arhitektura: Poštni strežniki hranijo poštne predale, imajo izhodno vrsto sporočil. Odjemalski programi imajo protokol za prenos sporočil.

SMTP

Vse v 7-bitnem ASCII. Tudi binarne priponke potrebno prekodirati v ASCII. Lahko v command liniji.

HELO/EHLO, MAIL FROM, RCPT TO, DATA, QUIT.

Lahko več objektov v enem sporočilu.

Dostop do predala

SMTP: dostava pošte do prejemnikovega strežnika.

POP3, IMAP, HTTP: prejem pošte s poštnega strežnika

Primerjava protokolov

POP: preprost, vrata 110. 3 faze: avtorizacija, prenos, pasodabljanje (QUIT)

IMAP: kompleksen, več funkcionalnosti. Uporabnik lahko določi mape. Možen prenos le delov sporočil. Hrani sejo.

HTTP: brskalnik, dostop od kjerkoli. Mape.

HTTP strežnik komunicira s poštnim strežnikom.

DNS

Hierarhično porazdeljena organizacija za preslikovanje imen v IP naslove. Korenski, TLD in avtoritativni strežniki.

Iterativna poizvedba: strežnik vrne naziv strežnika za naslednje poizvedovanje.

Rekurzivna poizvedba: poizvedba na lokalnem strežniku.

DNS poisoning: med cached zapise vstaviš zapis, ki preusmeri na neko drugo stran.

P2P storitve

Problem je v NATu, ker pride dohodni promet brez da bi ga zahteval.

Skalabilnost je performančna lastnost sistema, da še vedno dobro dela tudi, ko se poveča št. uporabnikov. P2P ima veliko skalabilnost.

Bit Torrent

Nek server – tracker, ki sledi kdo ima katere koščke. Odjemalec izbere sosede in izvaja izmenjavo le z njimi. Zahteva najprej najbolj redke koščke. Pravičnost: kdor hitro pošilja, tudi hitro prejema

zastavica choked v aplikacijskem sporočilu pove da naj vsi nehajo pošiljati.

Skype

Komunikacija med poljubnimi uporabniki.

Lastniški aplikacijski protokol, podrobnosti neznane.

Strežnik za prijavo preverja podatke o uporabnikih.

Odjemalec se po avtentikaciji poveže do najbližjega nadzornega vozlišča (supernode), ta ima 2 bistveni nalogi: • hrani preslikave up.ime → IP naslov
• skrbi za povezovanje med uporabniki.

Predstavitvena plast

skrbi za usklajevanje predstavitve podatkov.

Storitve: Predstavitev podatkov (ASN.1.).

Predstavitev: alfanumeričnih znakov (kodne tabele)

Stiskanje podatkov.

Zaščita podatkov (kriptiranje)

Sejna plast

Vzpostavljanje, rušenje sej. Odgovornost za obnovitvene točke, obnove sej, sinhronizacijo podatkov.

Možni odnosi: • sejna povezava – transportna povezava
• več sejnih povezav – transportna povezava
• sejna povezava – več transportnih povezav

Kriptografija

Zgoščevalna funkcija text zahasha v nekaj iz česar se ne da dobiti nazaj original texta. Malo možnosti da različni štvari data isti hash.

Vigenerjev kriptogram je Cezarjev v 2D.

Porterjev kriptogram kriptira po 2 znaka hkrati v neksimbol

Kodiranje pomeni, da celo besedo nadomestimo z drugo.

Transpozicija pomeni, da spremenimo zaporedje.

Bločna kriptografija pomeni da delamo z bloki in ne s posameznimi biti. Permutacijska škatla, substitucijska škatla (dekoder, p. škatla, kodor). Poznamo DES, 3DES, AES.

Verižno kriptiranje: čez bločno kriptografijo damo (trenutni blok xor prejšni kriptogram) namesto le trenutni blok. Imamo začetni vektor. $C(i) = K_s(m(i) \oplus c(i-1))$

Asimetrična kriptografija pomeni, da imamo enkripcijski E in dekripcijski D ključ, ki nista enaka. $D(E(m)) = m$

RSA

$m(i) = K_s^{-}(c(i)) \oplus c(i-1)$

p in q sta praštevili

$n = p*q$ $z = (p-1)*(q-1)$

e izberemo da nima skupnih deliteljev z z,

d tako da $e*d \bmod z = 1$, $d = (k*z+1)/e$

kriptiranje: $c = m^e \bmod n$

dekriptiranje: $m = c^d \bmod n$

Avtentikacija

Z RSA: pošiljatelja tako, da zakriptira s svojim privatnim ključem.

Prejemnika tako, da zakriptiramo z njegovim javnim ključem. Integriteto preverjamo s hashi.

Pošljemo ga zraven sporočila in potem primerjamo.

Digitalni podpis

Ker je počasno pošiljatelj zakriptira le zgoščeno vrednost. Certifikacijska agencija: Preverja povezavo med javnimi ključi in identitetami oseb – shrani v certifikat, ki ga zakriptira s svojim zasebnim ključem.

Hierarhično preverjanje: uporabnik – organizacijska CA – korenska avtoriteta.

Požarni zid

Filtrira promet od zunaj.

Izolirano filtriranje: na 3. in 4. plasti ISO, glede na podatke v glavi. Tabela naslovi – akcija, od zgoraj navzdol.

V kontekstu: Pregleduje TCP povezave, blokira nezahtevane pakete. Aplikacijski prehod omogoča filtriranje na podlagi podatkov na aplikacijskem nivoju. Samo za avtorizirane uporabnike vzpostavi povezavo do strežnika.

IDS in IPS

IDS zaznava vdore v sistem, IPS pa ukrepa. Izvaja se poglobljena analiza prometa. Zaznavanje z vzorci napadov: primerja promet z bazo že poznanih podatkov.

Zaznavanje netipičnega prometa: statistika, lahko zazna še nepoznane tipe napadov a je več false positivov.

Napadi

• Tiny Fragment Attack: pošiljaš tako majhne pakete, da se glava enkapsuliranega protokola razdeli.
• Overlapping fragment Attack: napačni offset, paketi se pokrivajo, sistem ne ve kaj z njimi
• Portscan: Išče katera procesi tečejo (delovini porti se odzovejo)
• SYN flood: Strežniku pošljеš veliko TCP SYN, on napol odpre veliko povezav zato postane neodziven (DOS). Solution: Timeout ali IPS
• Smurf: napadalec zlorabi omrežje, ki dovoli broadcast na zunaj. Pošlje ICMP paket z
• Birthday attack: sporočilo prestrežemo in zamenjamo z novim hash.

OSI Model

- Aplikacijska - HTTP, POP3, FTP, SMTP, DNS, P2P
- Predstavitvena
- Sejna
- Transportna - UDP, TCP
- Omrežna - IPv4, IPv6, DHCP, NAT, ICMP
- Povezavna - ARP, PPP
- Fizična

Fizična plast

Lastnosti prenosnega kanala so smer (enosmerno, dvosmerno - sočasno, izmenično), zaporednost (serijski ali paralelni), št. točk (dvotočkovni, skupinski).

Naloge fiz. plasti: 1.) Kodiranje bitov 2,3.) Prenos posameznih bitov in celotnega signala 4.) Pretvorba signala za prenos po mediju

Modulacija: Poznamo amplitudno, frekvenčno in fazno. Kvadratna je kombinacija amplitudne in fazne.

Povezavna plast

Enota na tej plasti je okvir. Naloga plasti je prenesti okvir med sosednjima vozliščema upoštevajoč tip medija

Povezavna plast lahko izvaja:

1.) Okvirjanje datagramov
2.) Zaznavanje, odpravljanje napak
3.) Dostop do medija (MAC (media access control) protokol)
4.) Zanesljiva dostava (potrjevanje, ponovno pošiljanje)
5.) Kontrola pretoka

Zaznavanje in odpravljanje napak

EDC - error detection code. Dodatni biti za zaznavanje napak. Izračuna se iz podatkov, primerjamo EDC iz sporočila z izračunanim iz prejetega sporočila.

Parnost - liha (skupaj s paritetnim bitom liho enic) in soda paritetna shema. Lahko jo delamo v 2 dimenzijah, lahko odpravimo 1 ali 2 napaki.

Hammingova koda - uporablja sodo paritetno shemo. Prvi bit preverja 1,3,5,7, drugi bit preverja 2,3,6,7, četrti bit pa 4,5,6,7. Sindrom: $p_4 p_2 p_1$

CRC - uporablja polinome in lahko popravi r+1 napak, če je r št. dodatnih bitov. Ponavadi CRC32. PPP ga uporablja, Ethernet tudi ampak ne odpravlja napak, za to skrbi transportna plast.

Dostop do skupinskega medija

Ciljamo na izkoristek, pravičnost in kolektivnost (decentraliziran protokol)

Izogibanje in razreševanje kolizij

Delitev kanala - ni dober izkoristek

TDMA - kanal razdeljen na časovne intervale, vsak lahko govori le v svojem intervalu.

FDMA - vsak svoj fiksen frekvenčni pas.

Naključni dostop:

ALOHA - ob koliziji pošlje paket do konca in potem pošlje še enkrat. Pri razsekani uporabi moramo biti sinhronizirani, z veliko verjetnostjo pošljemo v naslednjem intervalu. 18% / 37% effective.

CSMA - Poslušaj preden pošlje. Problem je zakasnitev signala. Kote dodamo CD (collision detection)

CSMA/CD - Uporabo jam signala, če zazna kolizijo pokvari še vse ostale podatke. Hitrejša sprostitev kanala preko/after kolizije ob koliziji.

Izmenični dostop

Dva pristopa: rezervacija s centralnim vozliščem (polling) in z žetonom (token).

CSMA/CA (collision avoidance) - Izogibanje trkov z uskljajevanjem časov pošiljanj, uporaba RTS in CTS.

Skriti terminali - terminala se ne vidita a lahko ustvarita kolizijo v sredini med njima. Izpostavljeni terminali - štirje, soseda lahko povzročata kolizije, a lahko navzven že vedno komunicirata.

Ethernet - danes topologija zvezde s stikalom v centru.

Ethernet

Okvir je sestavljen iz preambule (za sinhr. ur in hitrosti), naslova prejemnika in pošiljatelja, Type - kateri protokol je enkapsuliran, Data - MTU ali manj, CRC. oznaka: hitrost + BASE + medij

preambula 8B	dest. 6B	Source 6B	Type 2B	DATA 46-1500B	CRC 4B

Protokol PPP (Point to point protocol)

Povezava med dvema točkama. Escape sequence vrinemo pred naravnimi bajti, je dolžine 1B.

start	address	control	protocol	info	CRC	end
1B	1B	1B	1/2 B	≤1500B	2/4B	1B

MAC naslov

Dolg je 48 bitov, zapišemo kot 6*2 šestnajstiških znakov. FF-FF-FF-FF-FF-FF je MAC broadcast naslov

ARP

Pretvarja med IP in MAC naslovi v lokalnem omrežju. Deluje tako da A pošlje MAC broadcast z IP naslovom B. B odgovori z ARP responsom, zapiše se v tabelo. <IP | MAC | TTL>

Aktivna oprema

Repeater - ojačevalec signala

Hub - razdelilec, signal pošlje naprej vsem

Switch - stikalo, preklaplja med priključenimi napravami

Opravlja posredovanje, poplavljanje, filtriranje.

Tabela CAM/FIB - MAC - vrata <MAC | vrata | TTL>

Omrežna plast

Datagrame na tej plasti imenujemo paketi. Cilj je paket prenesti od pošiljatelja do končnega prejemnika.

Internet deluje v načinu best-effort, kar v praksi pomeni, da ne zagotavlja ničesar.

Usmerjevalnik

Usmerja (routing) in posreduje (forwarding) pakete. Ima posredovalno tabelo, na podlagi katere se odloči kam poslati paket.

Povezavna omrežja

Vzpostavimo povezavo preko omrežja, imamo navidezne vode, paketi vsebujejo podatke za posredovanje.

Nepovezavna omrežja (datagramska)

Usmerjevalniki hranijo posredovalne tabele in stanje o povezavah. Za usmerjanje paketov/posodabljanje tabel skrbijo usmerjevalni algoritmi. Za shranjevanje naslovov v tabelah imamo dva načina: združimo dele naslovov v območja in vsakemu dodelimo vmesnik, Shranimo le predpone in pošljemo na vmesnik, kjer je najdaljša ujemajoča predpona.

IPv4

Razdelki: Ver (4b), Header length (4b), TOS (8b, za razlikovanje posebnih datagramov), Length (16b), ID + Flags + Offset (32b, za fragmentacijo), TTL (8b), Upper layer (8b, kateri je enkapsuliran protokol), Checksum (16b), IP naslova (2*32b), opcije (32b)

Fragmentacija

ID: št. paketa, pri vseh kosčkih enak

FLAGS: DF - dont fragment, MF - more fragments

OFFSET: pozicija fragmenta v prvotnem datagramu

DHCP (Dynamic host configuration protocol)

Naprava pošlje DISCOVER, dobi OFFER, odgovori z REQUEST in dobi ACK. Dejansko deluje na 7. plasti, vrata 67, 68.

NAT (Network address translation)

Uporablja vrata, da lahko celo lokalno omrežje z enim javnim IP naslovom dostopa do interneta.

NAT tabela lokalni naslov (+vrata) in to preslika v javni naslov + vrata.

ICMP (Internet Control Message protocol)

Se pošilja v IP paketu. Uporablja se za obvestila napak v omrežju. Ping uporablja ICMP paketa tipa 0 (reply) in 8 (request). Traceroute uporablja TTL, ki ga za vsak naslednji paket zveča. Nazaj dobi TTL expired z naslovom usmerjevalnika.

IPv6

Razdelki: Ver (4b), PRI (ority) (8b, Tos v v4), Flow Label (20b), Payload len (16b), Next hdr (8b, enkapsuliran protokol), Hop limit (8b, TTL). Za hitrejše usmerjanje glava fiksno 40B, ne vsebuje kontrolne vsote, fragmentacija ni dovoljena. Če je paket prevelik dobi nazaj odgovor Packet Too Big. Flow label za zagotavljanje QoS.

Prehod med verzijama

Dvojni sklad (dual stack) - usmerjevalniki znajo pretvarjati med verzijama, uporabljajo v6 razen če to ni možno. Nekatera polja se izgubijo (Flow label)

Tuneliranje - zapakiramo IPv6 paket v IPv4. Lahko pride do fragmentacije.

Usmerjevalni protokoli

Skrbijo za posodabljanje usmerjevalnih tabel.

Lahko so centralizirani ali decentralizirani, prilagodljivi ali neprilagodljivi.

Z vektorjem razdalj - je iterativna, glede na podatke o povezavah s sosedi in podatki, ki jih dobi od sosedov. Ob spremembi pošlje tabelo sosedom.

Principa good news travels fast in bad news travels slow.

Omrežje razdelimo na avtonomne sisteme. Med temi sistemi se uporablja BGP, znotraj AS pa:

RIP - Routing Information Protocol. Z vektorjem razdalj, cena na podlagi hopov.

OSPF - open shortest path first. Link-state. S poplavljanjem obvestila celemu omrežju.

IGRP - Interior Gateway routing protocol. Ciscov RIP. Cena je utežena vsota stvari.

Transportna plast

Osnovna enota je segment. Naloga je sporočilo razbiti na segmente, jih pošiljati med procesi.

Ports:
80 - HTTP
25 - SMTP
53 - DNS
23 - telnet
194 - IRC
443 - HTTPS

UDP

Uporabljan ko je hitrost pomembnejša od zanesljivosti. Best-effort. Kontrolna vsota je eniški komplement vsote 16b besed.

Ponavljanje nepotrjenih (go back-N)

Pošiljatelj ima okno, prejemnik pošilja ACK zadnjega dobljenega. Ob napaki mora poslati vse od zadnjega potrjenega naprej še enkrat, prejemnik vse tiste za napako zavrže. Timer za najstarejši nepotrjen paket v oknu.

Ponavljanje izbranih (selective-repeat)

Prejemnik ima buffer. Ponovno pošlje le pakete, za katere ni dobil ACK. Timer za vsak posamezni nepotrjen paket.