LV 12 Protokoli transportnog sloja (TCP i UDP)

David Rudar i Jan Šotić

PRIPREMA

1. Koje su prednosti i nedostaci protokola TCP?

Prednosti TCP:

Pouzdanost: TCP garantira pouzdanu isporuku podataka. To znači da će svi podaci biti isporučeni bez gubitka i u pravilnom redoslijedu.

Kontrola toka: TCP upravlja tokom podataka kako bi spriječio zagušenja i osigurao optimalan protok.

Višestruke veze: Omogućuje višestruke istovremene poveznice prema jednoj aplikaciji na jednom poslužitelju (npr. web ili e-pošta).

Podrška za popularne aplikacijske protokole: TCP podržava HTTP (web), SMTP (e-pošta), telnet, SSH i druge česte aplikacije na Internetu 1.

Nedostaci TCP:

Overhead: TCP ima veći overhead zbog potrebe za uspostavom veze, potvrdom primitka i upravljanjem tokom podataka.

Sporiji od UDP-a: Zbog pouzdanosti i kontrole toka, TCP može biti sporiji od UDP-a.

Nije pogodan za stvarno vrijeme: Za aplikacije poput VoIP telefonije gdje je brzina važnija od pouzdanosti, UDP je bolji izbor

2. Koje su prednosti i nedostaci protokola UDP?

Prednosti UDP:

Brzina: UDP je brži od TCP-a jer nema uspostavu veze i potvrdu primitka. Idealno za aplikacije gdje je latencija bitna (npr. VoIP).

Jednostavnost: Zaglavlje UDP-a je jednostavnije od TCP-a.

Multicast podrška: Omogućuje slanje iste poruke na više odredišta 2.

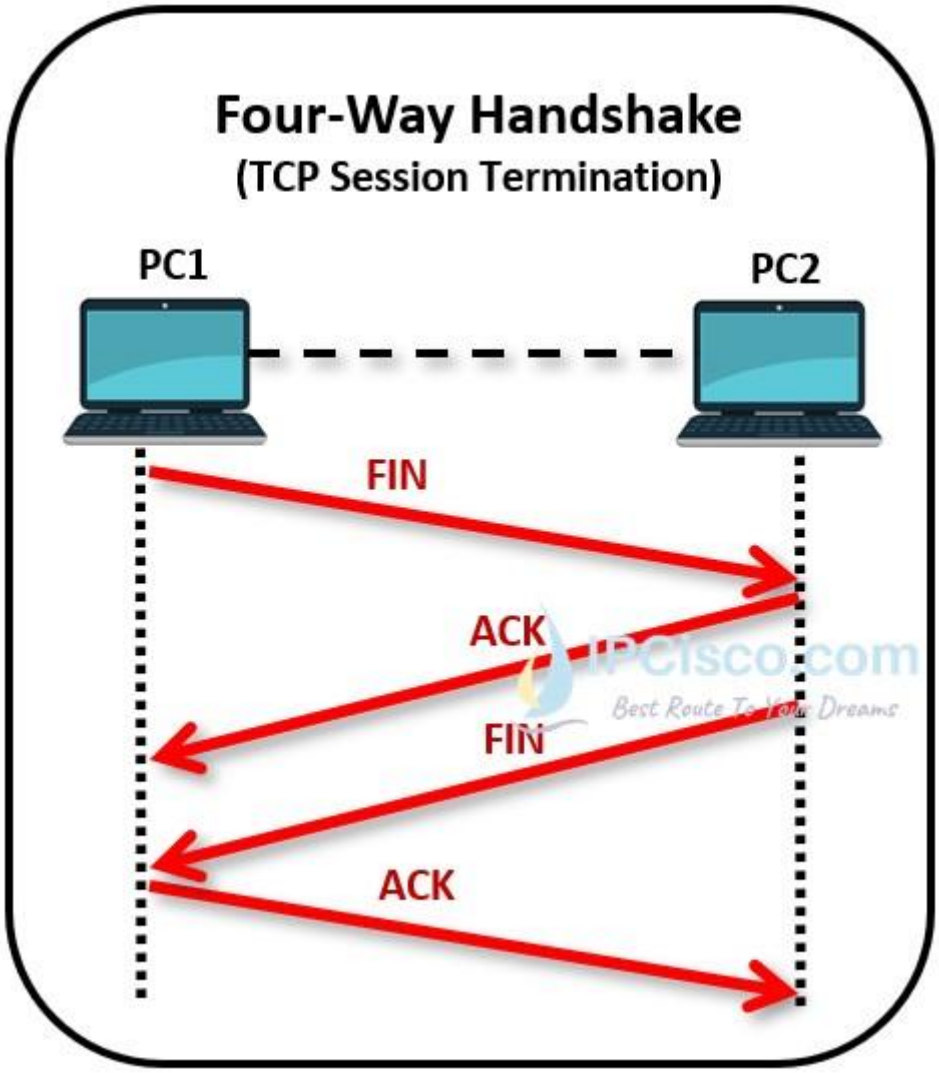
Nedostaci UDP:

Nepouzdanost: UDP ne garantira isporuku podataka. Aplikacije moraju samostalno rješavati gubitak paketa.

Nema kontrole toka: UDP ne upravlja tokom podataka, što može dovesti do zagušenja.

Nema provjere primitka: Radi na principu “pošalji i zaboravi”

3. Skiciraj i objasni postupak uspostave TCP veze između klijenta i poslužitelja.



Inicijacija veze (Three-Way Handshake): Klijent šalje SYN (synchronize) paket poslužitelju kako bi započeo komunikaciju.

Poslužitelj odgovara s SYN-ACK (synchronize-acknowledge) paketom, potvrđujući da je primio zahtjev i spreman za uspostavu veze. Klijent potvrđuje primanje SYN-ACK paketa šaljući ACK (acknowledge) paket poslužitelju. Veza je sada uspostavljena.

Prijenos podataka: Klijent i poslužitelj razmjenjuju podatke koristeći sekvencijski broj kako bi pratili redoslijed i pouzdanost. Svaki paket ima svoj sekvencijski broj i potvrdu primitka (ACK) kako bi se osigurala ispravna isporuka.

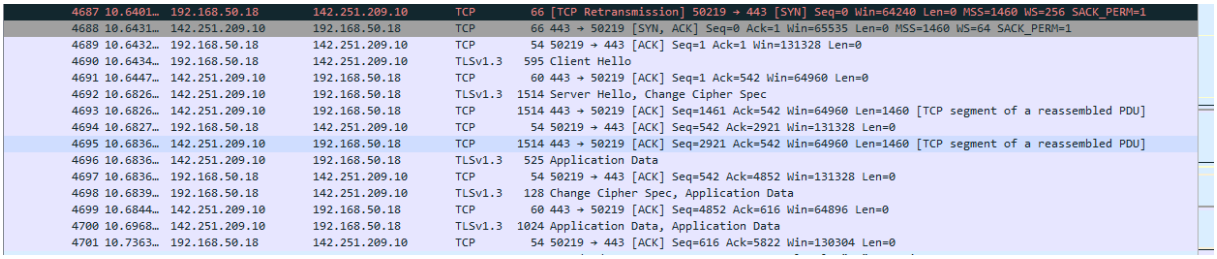
Zatvaranje veze (Four-Way Handshake): Klijent šalje FIN (finish) paket poslužitelju, označavajući da je završio s prijenosom podataka. Poslužitelj potvrđuje FIN paket šaljući ACK. Poslužitelj također šalje FIN paket klijentu. Klijent potvrđuje FIN paket ACK-om. Veza je sada zatvorena.

Ovaj postupak osigurava pouzdanu i sigurnu komunikaciju između klijenta i poslužitelja putem TCP-a.

VJEŽBA

1.

a



4687	10.6401…	192.168.50.18	142.251.209.10	TCP	66 [TCP Retransmission] 50219 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4688	10.6431…	142.251.209.10	192.168.50.18	TCP	66 443 → 50219 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
4689	10.6432…	192.168.50.18	142.251.209.10	TCP	54 50219 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
4690	10.6434…	192.168.50.18	142.251.209.10	TLSv1.3	595 Client Hello
4691	10.6447…	142.251.209.10	192.168.50.18	TCP	60 443 → 50219 [ACK] Seq=1 Ack=542 Win=64960 Len=0
4692	10.6826…	142.251.209.10	192.168.50.18	TLSv1.3	1514 Server Hello, Change Cipher Spec
4693	10.6826…	142.251.209.10	192.168.50.18	TCP	1514 443 → 50219 [ACK] Seq=1461 Ack=542 Win=64960 Len=1460 [TCP segment of a reassembled PDU]
4694	10.6827…	192.168.50.18	142.251.209.10	TCP	54 50219 → 443 [ACK] Seq=542 Ack=2921 Win=131328 Len=0
4695	10.6836…	142.251.209.10	192.168.50.18	TCP	1514 443 → 50219 [ACK] Seq=2921 Ack=542 Win=64960 Len=1460 [TCP segment of a reassembled PDU]
4696	10.6836…	142.251.209.10	192.168.50.18	TLSv1.3	525 Application Data
4697	10.6836…	192.168.50.18	142.251.209.10	TCP	54 50219 → 443 [ACK] Seq=542 Ack=4852 Win=131328 Len=0
4698	10.6839…	192.168.50.18	142.251.209.10	TLSv1.3	128 Change Cipher Spec, Application Data
4699	10.6844…	142.251.209.10	192.168.50.18	TCP	60 443 → 50219 [ACK] Seq=4852 Ack=616 Win=64896 Len=0
4700	10.6968…	142.251.209.10	192.168.50.18	TLSv1.3	1024 Application Data, Application Data
4701	10.7363…	192.168.50.18	142.251.209.10	TCP	54 50219 → 443 [ACK] Seq=616 Ack=5822 Win=130304 Len=0

b. Pronađene segmente usporedite sa skicom iz pripreme, zadatak 3.

Računalo A šalje syn seq=x, Računalo B ga prima te šalje syn seq=y i ACK x+1, Računalo A prima podatke te šalje ACK y+1, na kraju Računalo B prima ACK.

c. Koji je broj ishodišnog priključka (engl.port)?

49971

d. Koji je broj odredišnog priključka (engl.port)?

443

e. Pronađite brojeve koji označavaju redni broj segmenata (SEQ) i komentirajte!

1

Ako redoslijed SEQ brojeva raste bez prekida, to ukazuje na kontinuirani prijenos podataka. Duplikati SEQ brojeva: Ako primijetite duplikate SEQ brojeva, to može ukazivati na ponovno slanje paketa ili probleme u mrežnom prometu. Skočni SEQ brojevi: Skokovi u SEQ brojevima mogu ukazivati na nepravilnosti u prijenosu podataka ili mogu biti rezultat operacija poput ponovnog slanja ili redoslijeda TCP paketa.

f. Čemu služi oznaka Win?

Označava prozor. Prozor u ovom kontekstu odnosi se na količinu podataka koju primatelj može primiti od pošiljatelja prije nego što mora potvrditi primitak.

g. Pronađite brojeve koji označavaju potvrdu primljenog segmenta (ACK) i komentirajte.

Ako primjećujete rastući redoslijed ACK brojeva, to ukazuje na kontinuiranu potvrdu primljenih podataka. ACK bez podataka: Ako primatelj šalje ACK, ali nema novih podataka u segmentu, to može ukazivati na potvrdu prethodno primljenih podataka. Ponovljene potvrde (DupACK): Ako

primijetite ponovljene potvrde s istim ACK brojem, to može ukazivati na moguće gubitke paketa ili probleme u mreži.

h. Koja su ostala polja TCP zaglavlja? Istražite i zapišite čemu služe!

TCP zaglavlje sastoji se od sljedećih polja:

Source Port (Izvorni port): Oznaka izvornog porta šalatelja.

Destination Port (Odredišni port): Oznaka odredišnog porta primatelja.

Sequence Number (Redni broj): Redni broj prvog bajta podataka u segmentu.

Acknowledgment Number (Broj potvrde): Redni broj sljedećeg očekivanog bajta ako je postavljena ACK zastava.

Data Offset (Pomak podataka): Duljina TCP zaglavlja u 32-bitnim riječima.

Flags (Zastave): Različite zastave (SYN, ACK, FIN, RST, PSH, URG) za kontrolu veze i prijenosa podataka.

Window Size (Veličina prozora): Veličina prozora koju primatelj može primiti za kontrolu toka podataka.

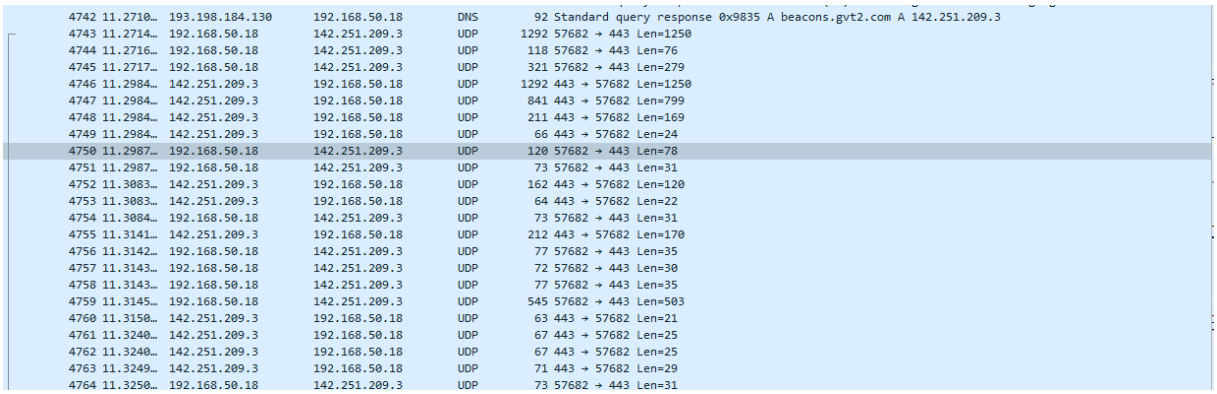
Checksum (Suma kontrola): Provjera integriteta TCP zaglavlja i podataka.

Urgent Pointer (Hitna pokazivač): Označava hitne podatke unutar segmenta.

Options (Opcije): Dodatne opcije i proširenja, kao što su Timestamps, Maximum Segment Size (MSS), i druge opcionalne parametre.

2. Analizirati zaglavlje odlaznih i dolaznih UDP segmenata

a. Pronaći UDP segmente



4742	11.2710…	193.198.184.130	192.168.50.18	DNS	92 Standard query response 0x9835 A beacons.gvt2.com A 142.251.209.3
4743	11.2714…	192.168.50.18	142.251.209.3	UDP	1292 57682 → 443 Len=1250
4744	11.2716…	192.168.50.18	142.251.209.3	UDP	118 57682 → 443 Len=76
4745	11.2717…	192.168.50.18	142.251.209.3	UDP	321 57682 → 443 Len=279
4746	11.2984…	142.251.209.3	192.168.50.18	UDP	1292 443 → 57682 Len=1250
4747	11.2984…	142.251.209.3	192.168.50.18	UDP	841 443 → 57682 Len=799
4748	11.2984…	142.251.209.3	192.168.50.18	UDP	211 443 → 57682 Len=169
4749	11.2984…	142.251.209.3	192.168.50.18	UDP	66 443 → 57682 Len=24
4750	11.2987…	192.168.50.18	142.251.209.3	UDP	120 57682 → 443 Len=78
4751	11.2987…	192.168.50.18	142.251.209.3	UDP	73 57682 → 443 Len=31
4752	11.3083…	142.251.209.3	192.168.50.18	UDP	162 443 → 57682 Len=120
4753	11.3083…	142.251.209.3	192.168.50.18	UDP	64 443 → 57682 Len=22
4754	11.3084…	192.168.50.18	142.251.209.3	UDP	73 57682 → 443 Len=31
4755	11.3141…	142.251.209.3	192.168.50.18	UDP	212 443 → 57682 Len=170
4756	11.3142…	192.168.50.18	142.251.209.3	UDP	77 57682 → 443 Len=35
4757	11.3143…	192.168.50.18	142.251.209.3	UDP	72 57682 → 443 Len=30
4758	11.3143…	192.168.50.18	142.251.209.3	UDP	77 57682 → 443 Len=35
4759	11.3145…	192.168.50.18	142.251.209.3	UDP	545 57682 → 443 Len=503
4760	11.3150…	142.251.209.3	192.168.50.18	UDP	63 443 → 57682 Len=21
4761	11.3240…	142.251.209.3	192.168.50.18	UDP	67 443 → 57682 Len=25
4762	11.3240…	142.251.209.3	192.168.50.18	UDP	67 443 → 57682 Len=25
4763	11.3249…	142.251.209.3	192.168.50.18	UDP	71 443 → 57682 Len=29
4764	11.3250…	192.168.50.18	142.251.209.3	UDP	73 57682 → 443 Len=31

b. Koje protokole enkapsulira UDP?

Protokoli koji se često koriste s UDP uključuju DNS, DHCP, SNMP, TFTP, NTP, Syslog, RIP, BOOTP, i druge.

c. Koji je broj ishodišnog priključka (engl.port)?

2750

d. Koji je broj odredišnog priključka (engl.port)?

443 port 9

e. Koja su ostala polja UDP zaglavlja? Istražite i zapišite čemu služe!

UDP zaglavlje sastoji se od dva polja:

Source Port (Izvorni port): Oznaka izvornog porta pošiljatelja.

Destination Port (Odredišni port): Oznaka odredišnog porta primatelja.

Ova polja identificiraju aplikaciju ili uslugu koja šalje (izvorni port) i kojoj su podaci namijenjeni (odredišni port).

3. Koja je uloga priključka u TCP i UDP segmentima?

U TCP i UDP segmentima, izvorni port označava aplikaciju ili uslugu pošiljatelja, dok odredišni port označava aplikaciju ili uslugu primatelja. Ova polja omogućuju identifikaciju izvora i odredišta podataka te pravilno rutiranje i isporuku na ciljni uređaj i odgovarajuću aplikaciju.

4. Za poznate protokole koje ste „ulovili“ navedite predefinirane brojeve priključaka (za TCP ili UDP)

UDP port 9

TCP- 80 i 443