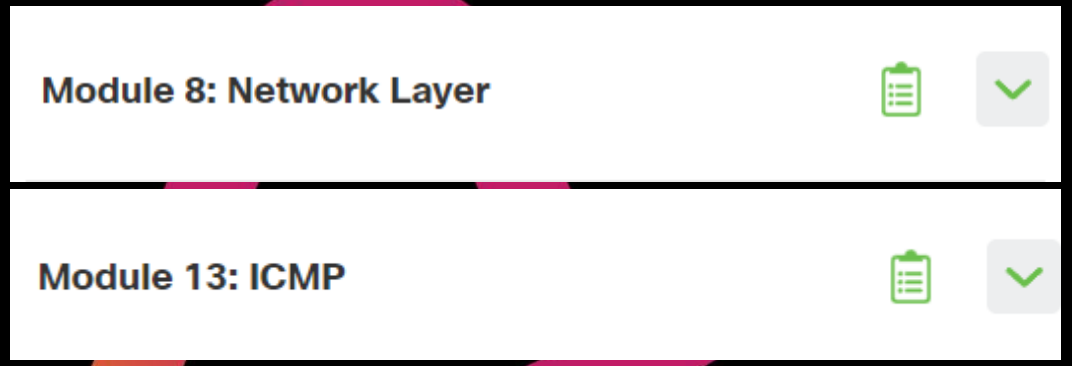
L3-Network Layer

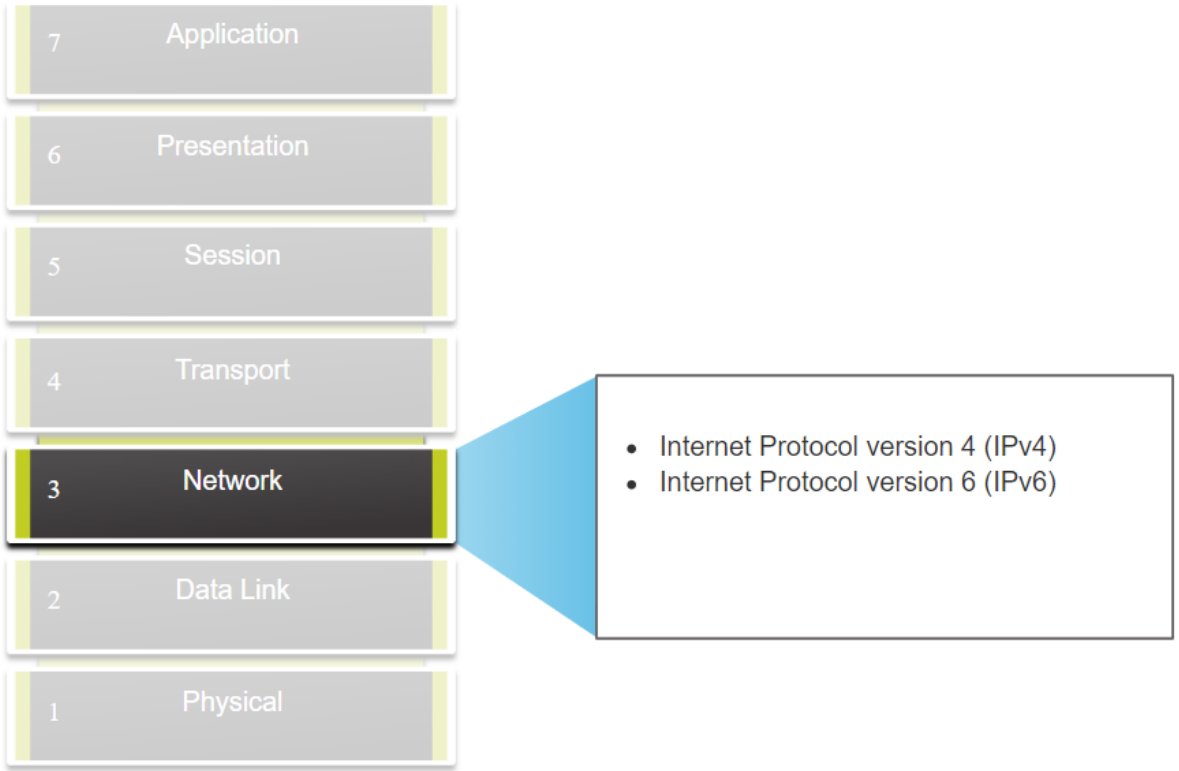
https://www.netacad.com/



- Internet Protocol (IP)
  ICMP

Mrežni sloj

- Mrežni sloj (OSI model) pruža usluge/funkcionalnosti koje krajnjim uređajima omogućuju razmjenu podataka između udaljenih računalnih mreža.
- IPv4 i IPv6 su glavni komunikacijski protokoli mrežnog sloja.
- Ostali protokoli mrežnog sloja uključuju protokole usmjeravanja kao što je Open Shortest Path First (OSPF) i protokole za razmjenu poruka kao što je Internet Control Message Protocol (ICMP).



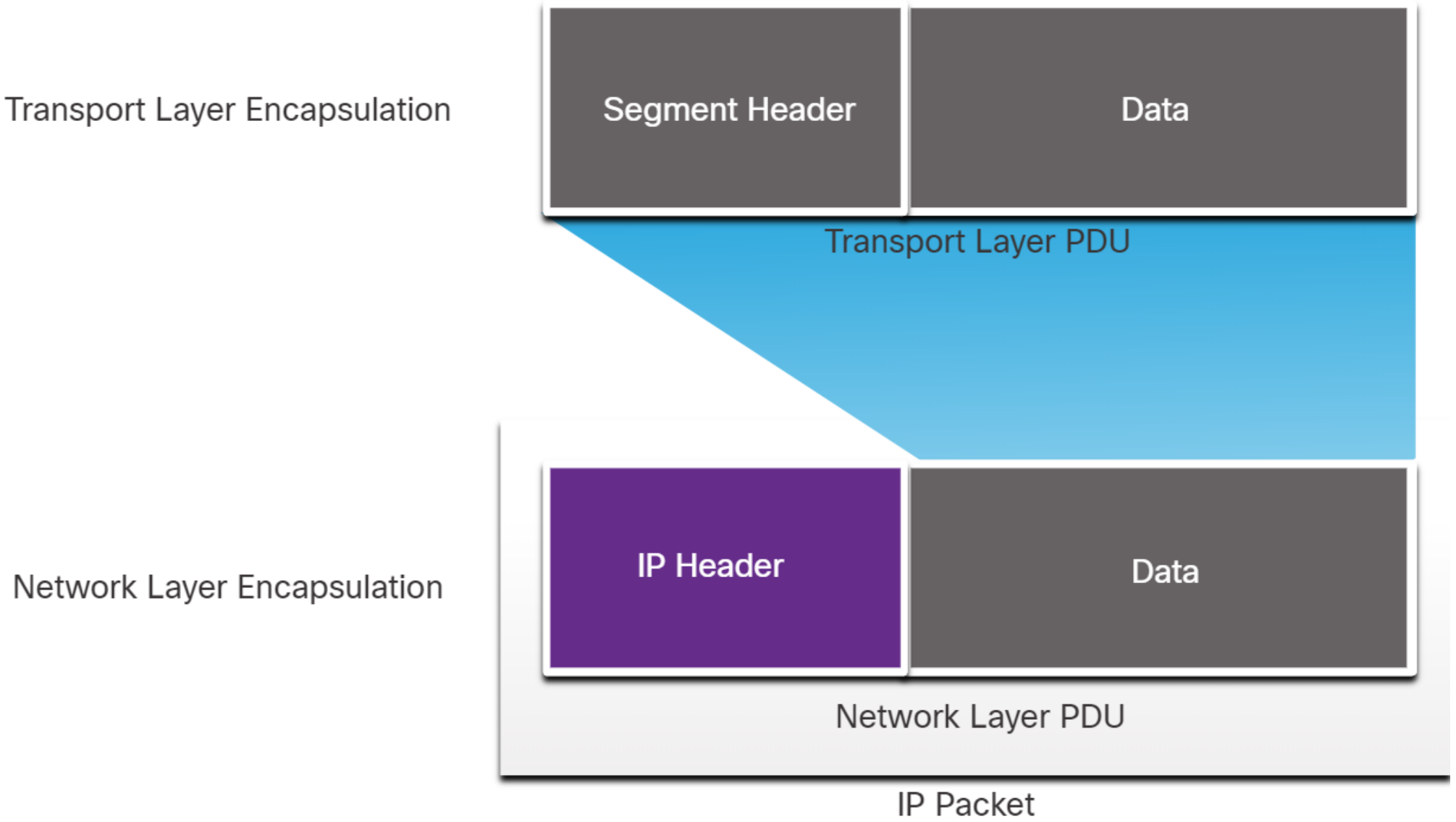
Mrežni sloj

Exam question

Kako bi se postigla komunikacija između mreže izvora i mreže odredišta komunikacije, protokoli mrežnog sloja izvode četiri osnovne operacije:

- Adresiranje krajnjih uređaja - krajnji uređaji moraju biti konfigurirani s jedinstvenom IP adresom za identifikaciju na mreži.
- Enkapsulacija - Mrežni sloj enkapsulira PDU transportnog sloja (segment/datagram) u paket. Proces enkapsulacije dodaje informacije o IP zaglavlju, kao što je IP adresa izvorišnog (šalje) i odredišnog (primajućeg) računala.
- Usmjeravanje - mrežni sloj pruža usluge za usmjeravanje paketa na odredišno računalo na drugoj mreži. Za putovanje u druge mreže, paket mora obraditi usmjernik. Uloga usmjernika je odabrati najbolji put i usmjeriti pakete prema odredišnom računalu u procesu poznatom kao usmjeravanje. Svaki usmjernik koji paket prijeđe da bi stigao do odredišnog računala naziva se skok.
- Dekapsulacija - kada paket stigne na mrežni sloj odredišnog računala, računalo provjerava IP zaglavlje paketa. Ako odredišna IP adresa unutar zaglavlja odgovara vlastitoj IP adresi, IP zaglavlje se uklanja iz paketa. Nakon što mrežni sloj dekapsulira paket, rezultirajući PDU transportnog sloja prosljeđuje se odgovarajućoj usluzi na transportnom sloju. Proces dekapsulacije izvodi odredišni uređaj.

Mrežni sloj-enkapsulacija



Glavne karakteristike IPv4

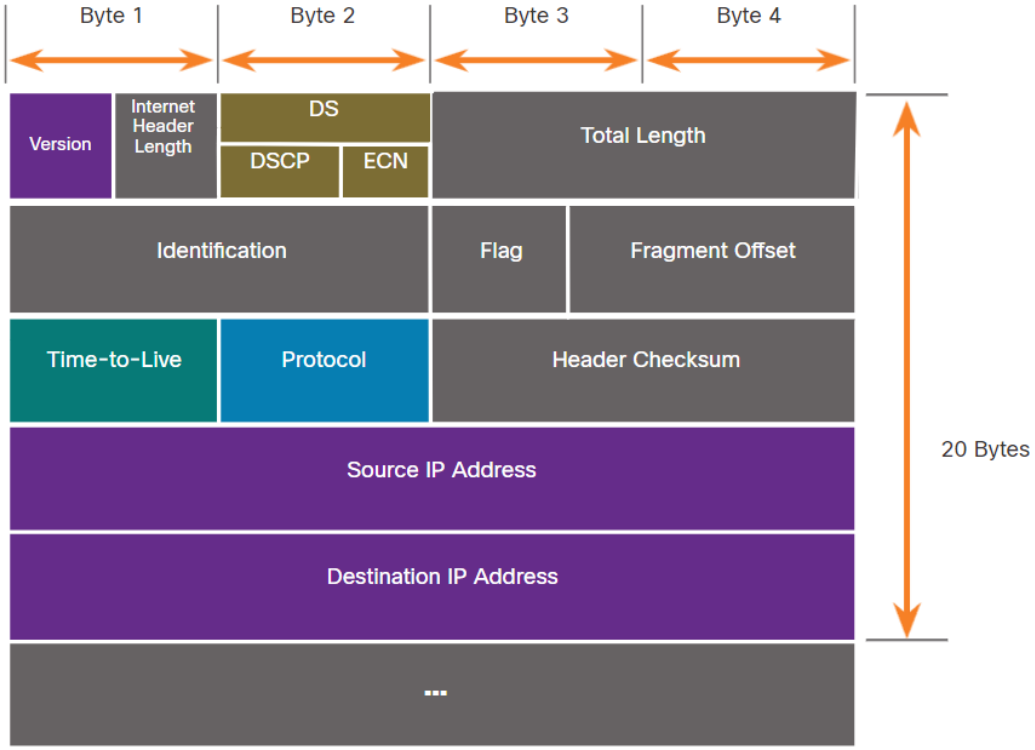
Exam question

- IP je dizajniran kao protokol s „niskim opterećenjem” (eng. Low overhead) same komunikacije.
- Omogućuje samo funkcije koje su potrebne za isporuku paketa od izvora do odredišta preko međusobno povezanog sustava mreža.
- Protokol nije dizajniran za praćenje i upravljanje protokom paketa. Ove funkcije, ako je potrebno, obavljaju drugi protokoli na drugim razinama, prvenstveno TCP na razini 4.

Ovo su osnovne karakteristike IP-a (analogija poštanskog ureda):

1. Ne uspostavlja vezu- Nije uspostavljena veza s odredištem prije slanja podatkovnih paketa.
2. Best Effort - IP je sam po sebi nepouzdan jer isporuka paketa nije zajamčena.
3. Neovisan o mediju - Rad je neovisan o mediju (tj. bakrenom, optičkom ili bežičnom) koji prenosi podatke.

Polja zaglavlja IPv4 paketa



- **Version (4)** – Uvijek je IPv4 protokol (binarno 0100)
- **IHL – Internet Header Length (4)** – 32-bit, veličina 20 bajta/160 bita, ako nema dodatnih opcija (inače do 60 bajta)
- **DS (Differentiated Services)**
  - **DSCP – Differentiated Services Code Point (6)** – QoS mehanizam (originalno ToS – Type of Service)
  - **ECN – Explicit Congestion Notification (2)** – detekcija zagušenja ako obje strane koriste ovu opciju (ne koristi se)
- **Total Length (16)** – ukupna veličina IP datagrama. Minimalno 20 bajta (samo zaglavlje), max. 65535 bajta (iako često je 1500 bajta)

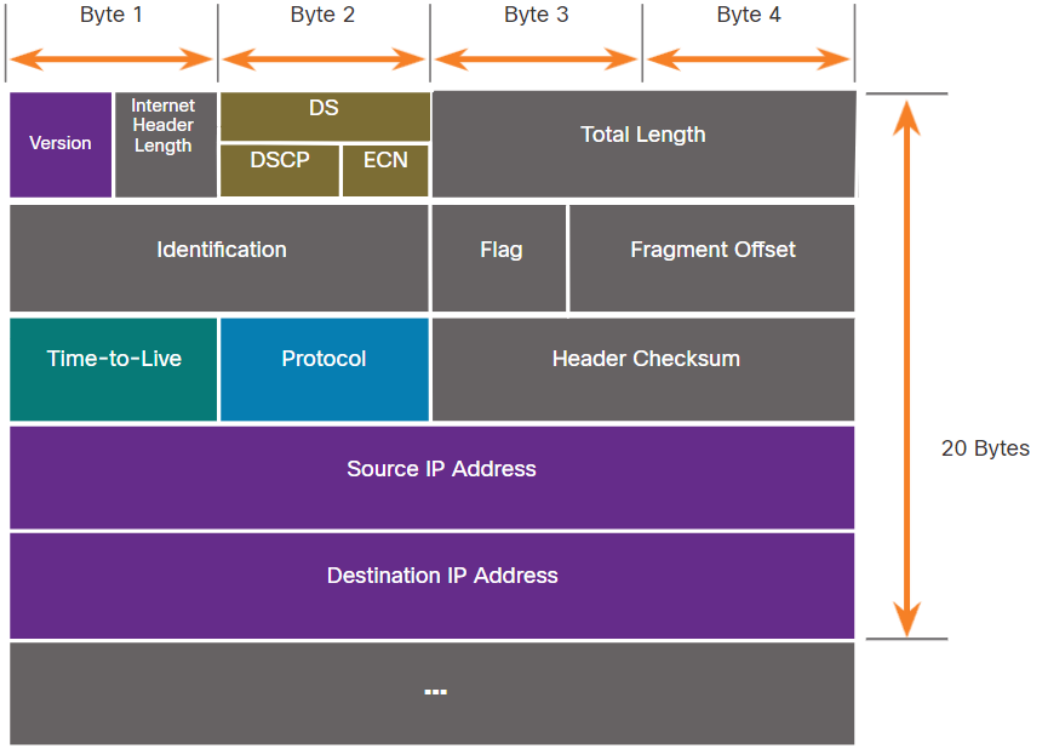
- **TTL – Time To Live (8)** – Mehanizam za sprječavanje petlji koji pokazuje sve usmjernike kroz koje naš paket prolazi na putu do odredišta
- **Protocol (8)** – protokol koji se nosu u IP paketu (6 = TCP, 17 = UDP, 89 = OSPF)
- **Header Checksum (16)** – detekcija grešaka u slanju paketa
- **Source IP address (32)**
- **Destination IP address (32)**
- **Options (nx32…0-40 bytes)** – razne opcije ovisno o IHL polju

Exam question

Polja zaglavlja IPv4 paketa

Tri polja koja se koriste za upravljanje fragmentacijom
Identification (16) – koristi se za fragmentiranje i sastavljanje fragmentiranih paketa

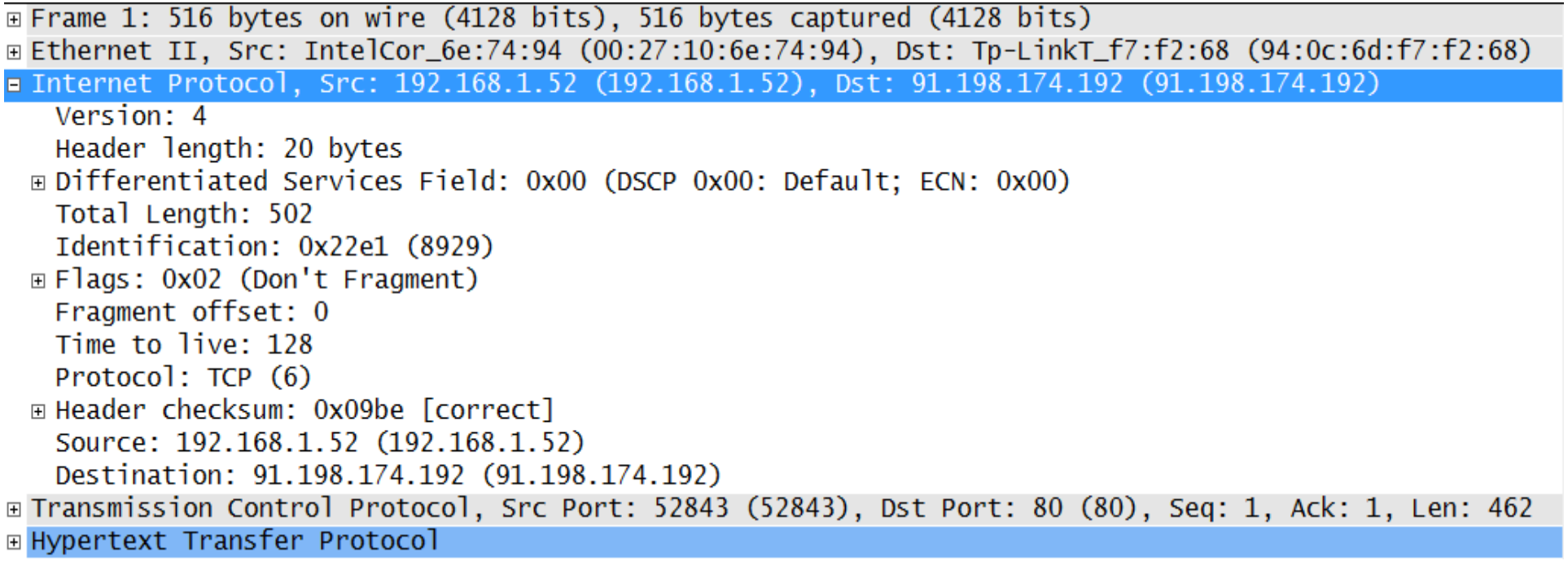
- **Flags (3)** – obično se koriste dvije – DF (Don't Fragment) i MF (More fragments)
- **Fragment Offset (13)** – relativni položaj fragmenta u odnosu na cijeli IP datagram
- Fragmentacija omogućuje fragmentiranje i ponovno sastavljanje paketa
- Danas se fragmentacija praktički ne koristi (osim ako nešto nije pogrešno konfigurirano)



IPv4 zaglavlje u Wiresharku

Exam question

- Ovako izgleda IPv4 paket u Wiresharku - dakle vidimo sva polja iz zaglavlja (ovaj nema Options i zaglavlje je 20 okteta).
- Ukupni paket je 502 okteta (bajta), njegov TTL je 128, a protokol unutar je TCP (Protokol = 6)



IP adresiranje i Osnove IP adresiranja

Exam question

4 okteta

- IP adresa je 32-bitni broj (4 okteta) – znači broj od 0 do 4.294.967.296 (oko 4 milijarde adresa)
- Radi jednostavnosti prikazujemo je kao 4 dekadska broja (za svaki oktet po jedan) razdvojena točkama radi „lakšeg" pamćenja i tumačenja:
- Primjeri IP adresa: 0.0.0.0, 88.80.13.160, 213.251.145.96, 255.255.255.255, 127.0.0.1

➢ www.index.hr 198.41.176.5
➢ www.racunarstvo.hr 178.79.149.215
➢ www.imenik.hr 193.200.203.100

Osnove IP adresiranja

Exam question

4 bytes

198. **41.** **176.** **5**

llOOOllO.OOlOlOOl.lOllOOOO.OOOOOlOl

178. **79.** **149.** **215**

lOllOOlO.OlOOllll.lOOlOlOO.llOlOlll

193. **200.** **203.** **100**

llOOOOOl.llOOlOOO.llOOlOll.OllOOlOO

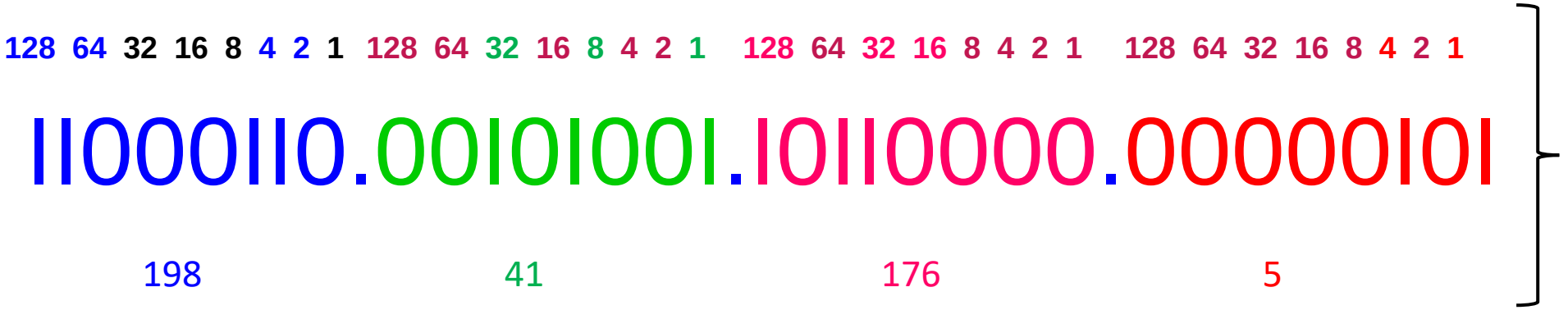
Pretvaranje binarno u decimalno i obratno

Exam question

4 bytes

- Value of “used” bit depends on the position of the bit inside the octet (byte)

Values are: 128 64 32 16 8 4 2 1



Binary to decimal Conversion

Pretvaranje binarno u decimalno i obratno

Exam question

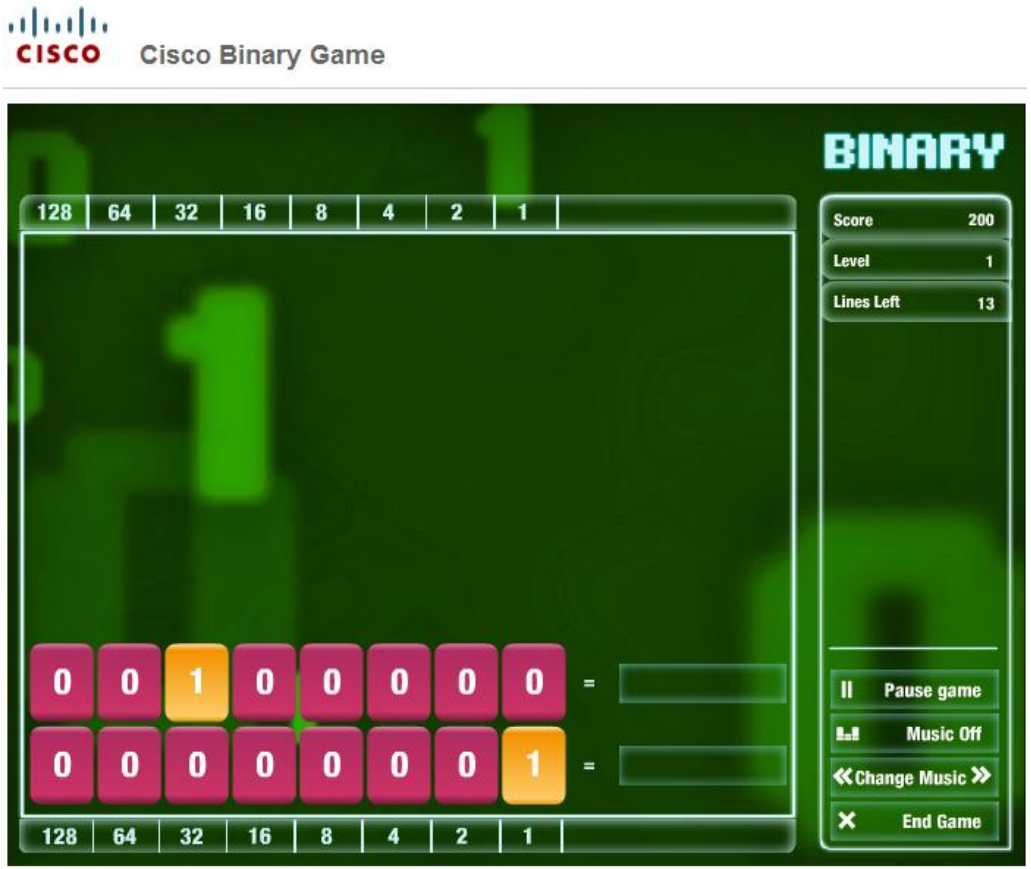
4 bytes

128	64	32	16	8	4	2	1	
1	1	0	0	0	1	1	0	=198
0	0	1	0	1	0	0	1	=41
1	0	1	1	0	0	0	0	=176
0	0	0	0	0	1	0	1	=5

198=128+64+4+2 41=32+8+1 176=128+32+16 5=4+1

Cisco Binary Game za vježbu

4 bytes



https://learningnetwork.cisco.com/docs/DOC-1803

https://2048game.com

Kako host (računalo) usmjerava

Exam question

Računalo koje je izvor prometa mora moći usmjeriti paket na odredišni host (računalo). Kako bi to učinili, krajnji uređaji koriste vlastitu tablicu usmjeravanja.

Izvorišno računalo može poslati paket na slijedeći način:

1. Samo sebi – Računalo može samo sebe pingati slanjem paketa na posebnu IPv4 adresu 127.0.0.1 ili IPv6 adresu ::1, što se naziva sučelje povratne petlje (eng. Loopback). Pinganjem loopback sučelja testira se TCP/IP stack na glavnom računalu.
2. Računalima u lokalnoj mreži - Ovo je odredišno računalo kojie je u istoj lokalnoj mreži kao i računalo koje šalje promet. Oba računala dijele isti mrežni dio IP adrese (**10.10.41**.50 i **10.10.41**.61)
3. Udaljeno računalo - Ovo je odredišno računalo na udaljenoj mreži. Izvorišno i odredišno računalo ne dijele istu mrežnu adresu.

Je li paket namijenjen lokalnom ili udaljenom računalu određuje računalo koje šalje promet.
U IPv4 - Izvorišni uređaj koristi vlastitu mrežnu masku zajedno sa svojom vlastitom IPv4 adresom i odredišnom IPv4 adresom za ovu odluku.

Default Gateway

Exam question

Zadani pristupnik (eng. Default Gateway) mrežni je uređaj (tj. Usmjernik ili preklopnik…može biti i vatrozid) koji može usmjeravati promet prema drugim mrežama. Ako upotrijebite analogiju da je mreža poput sobe, tada je Gateway poput vrata. Ako želite doći do druge sobe ili mreže, morate pronaći ta vrata i proći kroz njih.

Na mreži je Gateway obično usmjernik s ovim značajkama:

- Ima lokalnu IP adresu u istom rasponu adresa kao i druga računala na lokalnoj mreži.
- Može prihvatiti podatke u lokalnu mrežu i proslijediti podatke izvan lokalne mreže.
- Usmjerava promet na druge mreže.

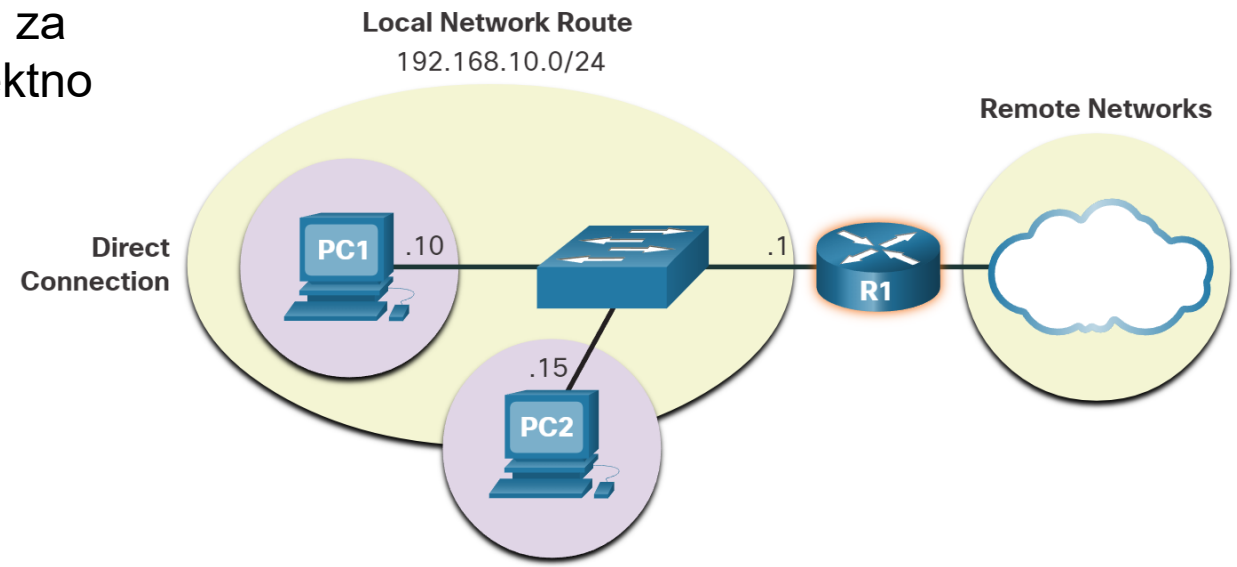
Za slanje prometa izvan lokalne mreže potreban je Gateway.
Promet se ne može proslijediti izvan lokalne mreže ako ne postoji Gateway, ako GW nema IP adresu ili ako nije uključen i spojen na mrežu.

Računala šalju promet prema Gatewayu

Exam question

Tablica usmjeravanja računala obično uključuje i IP adresu GW. Računalo može IP postavke dobiti od GW putem DHCP-a ili može biti ručno konfigurirano

- Konfiguriranje računala IP adresom GW-a u usmjerničkoj tablici računala stvara predefiniranu putanju
- Zadana putanja je putanja koju će računalo koristiti za sav promet koji treba poslati u mreže koje nisu direktno povezane s računalom (LAN)



Računala šalju promet prema Gatewayu

Exam question

- Na Windows računalu, naredba route print ili netstat -r može se koristiti za prikaz usmjerničke tablice računala.
- Dijagram prikazuje topologiju mreže koja se sastoji od računala, spojenog na preklopnik na mreži 192.168.10.0/24. Preklopnik je spojen na usmjernik R1, koji je zatim spojen na oblak.
- PC1 ima adresu .10, a sučelje rutera na koje je preklopnik spojen ima adresu .1.


```
C:\Users\PC1> netstat -r
(output omitted)
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
      192.168.10.0    255.255.255.0         On-link     192.168.10.10     281
    192.168.10.10  255.255.255.255         On-link     192.168.10.10     281
   192.168.10.255  255.255.255.255         On-link     192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link     192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link     192.168.10.10     281
(output omitted)
```

?

ICMP- Internet Control Message Protocol

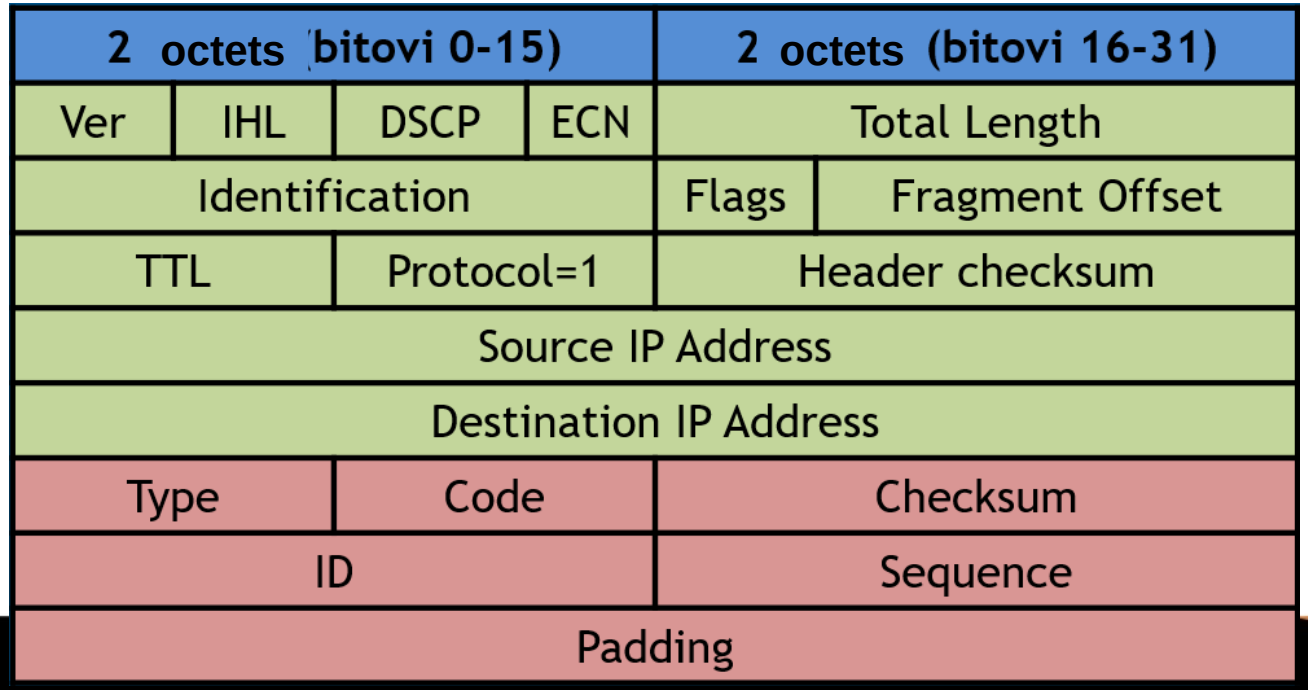
- IP protokol nema ugrađeni mehanizam za provjeru isporuke. Radi po principu Best-effort
- Ne postoji mehanizam kontrolnih poruka unutar samog IP protokola
- Ovaj posao obavlja ICMP - Internet Control Message Protocol -> Gotovo svi uređaji na mreži razumiju ICMP poruke

- Type i Code polja definiraju tip (8-zahtjev, 0-odgovor, 3-odredište nedostupno, 11-TTL premašen) i podtip (npr. Za tip 3 podtipovi su odredišna mreža nedostupna, odredišni host nedostupan, paket administrativno filtriran) poruka
- Kontrolni zbroj (checksum) za otkrivanje pogreške
- ID i sekvenca identificiraju poruku (ping)
- Padding – za velike pakete…ping –l 65000 10.10.10.10.

2 okteta (bitovi 0-15)		2 okteta (bitovi 16-31)
Type	Code	Checksum
ID		Sequence
Padding		

ICMP- zajedno s IP zaglavljem

- Prenosi se izravno preko IP-a (bez TCP-a ili UDP-a)
- U slučaju nekih vrsta grešaka ili događaja mrežni uređaji šalju informacije definirane vrstom i podvrstom (kodom) greške.
- Različite vrste i kodovi za različite pogreške pomažu u prepoznavanju i rješavanju problema
- Osnovni alati za testiranje također koriste ICMP za ping ili traceroute.



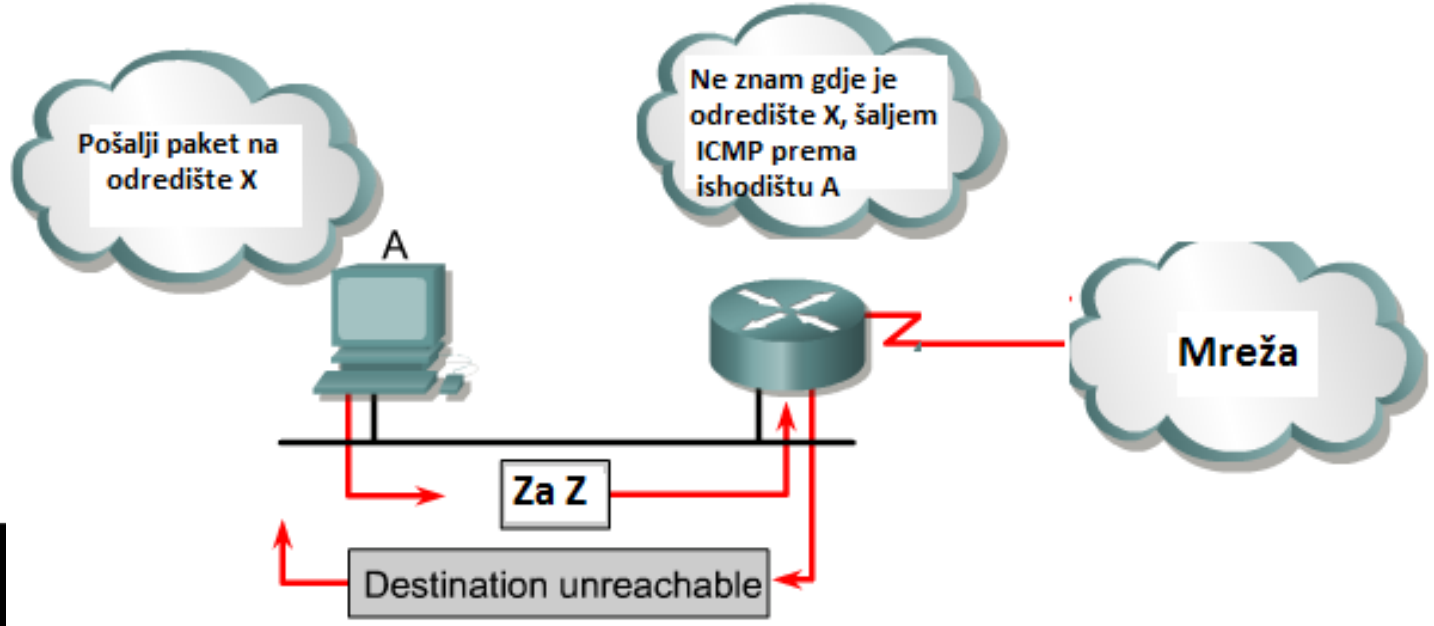
ICMP- echo (tip 8/0) request (8) i reply (0)

Exam question

- ICMP Echo request (type=8) i reply (type=0)
- Pošaljemo paket (s nekom veličinom paddinga da vidimo koliko veliki paket može proći) prema nekom odredištu (s ICMP type=8, na to kao odgovor dobijemo reply s ICMP type=0
- Osnova za ping alat, pošaljemo poruku, dobijemo odziv (kao kod sonara, zato se alat zove ping)
- Računalo s druge strane može biti „nepristojno” te ne uzvratiti na naš Echo request, tada dobijemo „Request Time Out” poruku kao i kada druga strana nije dostupna.
- Pomoću pinga dobijemo RTT (Round-Trip-Time) – znači koliko paketu treba od nas do odredišta i nazad

ICMP- Destination Unreachabe (3)

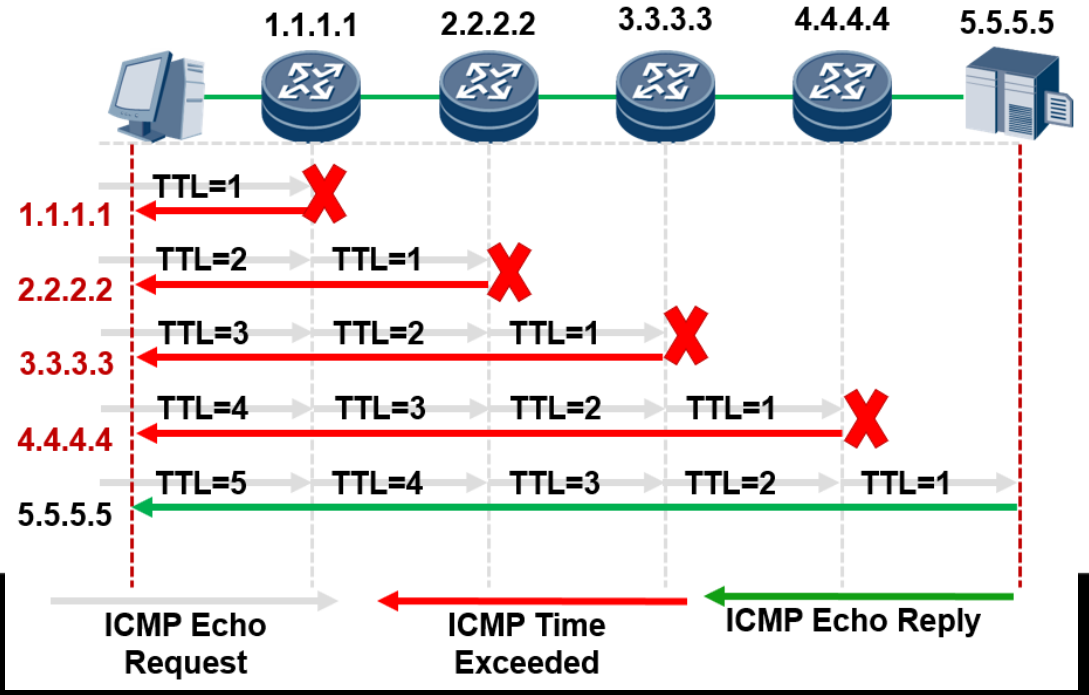
- Šaljemo paket od A prema Z, no već na B usmjernik nema u tablici nikakvu rutu prema Z te vraća poruku pošiljatelju (A) da je odredište nedostupno (ICMP type=3)
- U podtipu (code) javlja detaljniju informaciju:
  - Code= 0 network unreachable, 1 host unreachable, 4 fragmentation needed and DF set, 6 destination network unknown, 7 destination host unknown i tako dalje...
- Ovo često otkrivamo također pomoću ping alata koji ili timeouta ili dobije ICMP odgovor ovog tipa
  - Routeru može biti zabranjeno odnosno ugašeno odgovaranja i propuštanje dalje ICMP poruka, tako da je moguće dobiti ovakove poruke u tracerouteu ili pingu.



ICMP- Time exceeded (type 11)

Exam question

- Sjetimo se TTL parametra u zaglavlju IP paketa
- U slučaju ping-ponga paketom između dva usmjeritalja, TTL će otići na nulu te onaj tko odbaci paket šalje pošiljatelju ICMP paket type=11 sa SVOJOM IP adresom – saznamo IP adresu routera u nizu.
- Alat traceroute koristi ovaj mehanizam, pošalje ICMP Echo request (tip 8) ICMP paket s TTL=1 i čeka Time Exceeded odgovor, pa TTL=2, TTL=3 i tako dalje dok ne dođe do destinacije
- Tracerotue se zaustavi kada na ICMP Echo request dobije ICMP Echo reply (odnosno kada stigne do tražene destinacije).



ICMP- Time exceeded (type 11)

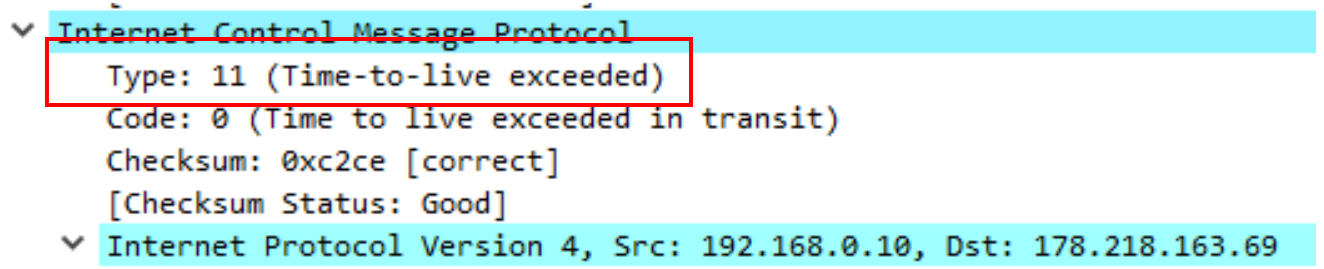
Exam question

C:\Users\sharkoon>tracert www.algebra.hr

Tracing route to www.algebra.hr [178.218.163.69]
over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.0.1
2	7 ms	7 ms	5 ms	10.219.160.1
3	6 ms	6 ms	6 ms	100.64.1.18
4	7 ms	6 ms	6 ms	100.64.0.17
5	8 ms	7 ms	7 ms	100.64.0.2
6	6 ms	9 ms	7 ms	dh120-77.xnet.hr [83.139.120.77]
7	7 ms	7 ms	8 ms	sedmiodjel.cix.hr [185.1.87.107]
8	7 ms	7 ms	8 ms	185.46.32.196
9	6 ms	12 ms	7 ms	algebra2.plusvps.com [178.218.163.69]

Trace complete.



96 28.850689	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=209/53504, ttl=6 (no response found!)
97 28.858385	83.139.120.77	192.168.0.10	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
98 28.860546	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=210/53760, ttl=6 (no response found!)
99 28.867900	83.139.120.77	192.168.0.10	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
100 28.870104	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=211/54016, ttl=6 (no response found!)
101 28.882970	83.139.120.77	192.168.0.10	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
102 29.876652	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=212/54272, ttl=7 (no response found!)
103 29.882931	185.1.87.107	192.168.0.10	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
104 29.884146	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=213/54528, ttl=7 (no response found!)
105 29.890802	185.1.87.107	192.168.0.10	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
106 29.891878	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=214/54784, ttl=7 (no response found!)
107 29.898919	185.1.87.107	192.168.0.10	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
108 30.898088	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=215/55040, ttl=8 (no response found!)
109 30.908255	185.46.32.196	192.168.0.10	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
110 30.910445	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=216/55296, ttl=8 (no response found!)
111 30.918416	185.46.32.196	192.168.0.10	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
112 30.920570	192.168.0.10	178.218.163.69	ICMP	106 Echo (ping) request id=0x0001, seq=217/55552, ttl=8 (no response found!)
113 30.928093	185.46.32.196	192.168.0.10	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

?