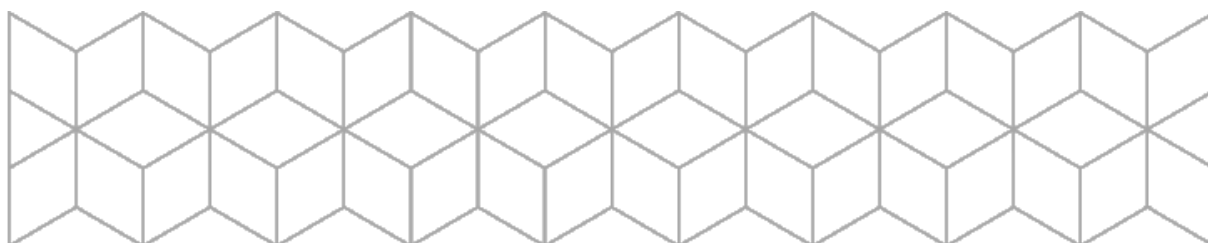


Løsningsforslag

EKSAMEN

Emnekode: ITF20219	Emnenavn: Datanettverk
Dato: 28. Nov 2019	Eksamenstid: Kl: 9:00 til kl: 13:00
Hjelpemidler: <ul style="list-style-type: none">• 4 sider (A4) (2 ark) med egne notater.• Kalkulator.• Gruppebesvarelse, som blir delt ut til de som har levert innen tidsfristen	Faglærere: Erling Strand
Om eksamensoppgaven og poengberegning: <p>Oppgavesettet består av totalt 8 sider, hvorav 1 førsteside, 4 sider med oppgaver, og 3 sider med vedlegg. Kontroller at oppgaven er komplett før du begynner å besvare spørsmålene.</p> <p><i>Oppgavesettet består av 7 oppgaver. Alle spørsmålene på de forskjellige oppgavene teller likt. Alle svar må begrunnes.</i></p>	
Sensurfrist: 19 Desember 2019	
Karakterene er tilgjengelige for studenter i Studentweb www.hiof.no/studentweb	



Oppgave 1

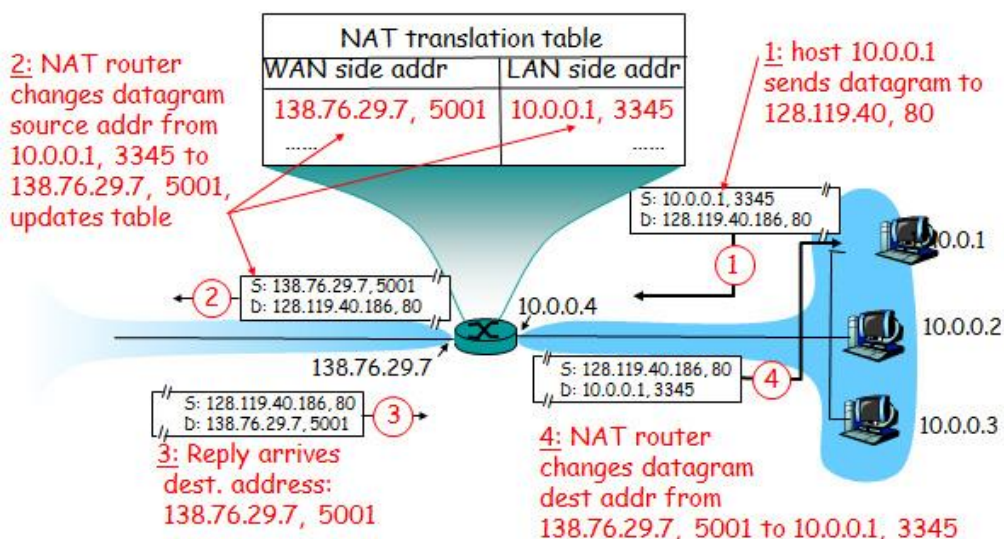
Anta at du har en hjemme-router som er koblet til en ISP (Internet Service Provider) og et privat LAN (Local Area Network), som benytter private IP adresser.

- a) Din hjemme-router inneholder NAT. Forklar hva du oppnår ved å ha NAT, og gi en kort beskrivelse av virkemåten.

NAT brukes for å oversette IP-adresser mellom forskjellige nettverk. Den kan være implementert i en hjemme-router, som gjør det mulig å ha mange PC'er med hver sin «private» IP-adresse på den ene siden, og kun en IP-adresse på den siden som er ut mot Internet. På den måten kan man ha mange host på et LAN, med hver sin «private» IP adresse. Alle PC'ene på dette LAN kan være på Internet samtidig, mens Internet ser bare en IP adresse fra alle sammen. Det er NAT som oversetter adressene fra hjemme nettverket (LAN) til Internet.

Når en pakke kommer fra en host på det private LAN, vil den i NAT i routeren få en ny fra-IP adresse. Den får også en ny fra-portnummer. Når svaret kommer fra internet, vil NAT kjenne igjen port-nummeret, og sende pakken til den riktige host, med det riktige portnummeret. Se figur

NAT: Network Address Translation



- b) Du har en PC på ditt private LAN. Den skal du bruke som WEB-server, og alle på internet skal kunne lese web-sidene dine. Hva må du da programmere/sette opp i din hjemme-router? Forklar også virkemåten til det du setter opp. Anta at din PC skal ha IPv4: 192.168.1.2, og den har MAC: 18-28-61-9a-22-2f

Det er to ting som da må programmeres i hjemmerouteren:

- 1) Portforward. Den må settes slik at en pakke som kommer fra internet, med port nr.80 skal sendes videre på det private LAN, til IP 192.168.1.2, som er WEB-serveren.
- 2) DHCP. Den må settes opp slik at en host med MAC 18-28-61-9a-22-2f, alltid skal få IP 192.168.1.2

Oppgave 2

Anta at du ping'er www.princeton.edu, og får denne utskriften på din skjerm:

```
Pinging www.princeton.edu [140.180.223.42] with 32 bytes of data:  
Reply from 140.180.223.42: bytes=32 time=130ms TTL=240  
Reply from 140.180.223.42: bytes=32 time=130ms TTL=240  
Reply from 140.180.223.42: bytes=32 time=134ms TTL=240  
Reply from 140.180.223.42: bytes=32 time=129ms TTL=240
```

Ping statistics for 140.180.223.42:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 129ms, Maximum = 134ms, Average = 130ms

- a) Forklar hva slags info som ligger i «TTL», og hva du kan bruke disse verdiene til.

TTL står for Time To Live. Det er en byte i hodet på en IPv4 pakke, som minsker med en for hver router pakka går igjennom. Når TTL blir 0, vil ikke pakka bli sendt videre. Dette er en sikkerhet i Internet, slik at ikke en pakke skal kunne gå evig i nettet.

Den routeren som pakka var i, da TTL fikk verdien 0, vil sende en ICMP pakke tilbake til senderen, om at pakka er stoppet. I denne pakka ligger også info om hvilken router som stoppet pakka.

Da et ping returnerer verdien på TTL, kan man også finne ut hvor mange routere pakken har vært innom, på vei til mottageren.

- b) Anta at du bruker stopp-og-vent (idle-RQ) overføring og pakkestørrelsen er på 1500 byte. Datahastigheten er på 10 Mbit/s. Hva blir effektiviteten på forbindelsen?

For å finne effektiviteten U, kan vi bruke formelen:

$$U = \frac{L/R}{RTT + L/R}$$

RTT i denne formelen er tiden en pakke bruker fram til, og tilbake fra den host pakken skal til. Det er «time» i ping forespørselen.

L er antall bit i pakka, og R er bithastigheten i bit/s. L/R vil da si hvor stor pakken er i tid.

I denne forbindelsen til www.princeton.edu er:

$$L/R = \frac{1500 [\text{byte}] \cdot 8 \left[\frac{\text{bit}}{\text{byte}} \right]}{10 \cdot 10^6 \left[\frac{\text{bit}}{\text{s}} \right]} = \frac{12000 [\text{bit}]}{10 \cdot 10^6 \left[\frac{\text{bit}}{\text{s}} \right]} = 1,2 \cdot 10^{-3} [\text{s}]$$

Innsatt i formelen for U, og med en «time» (RTT) på 130 ms, gir det:

$$U = \frac{1,2 \cdot 10^{-3} [\text{s}]}{(130 \cdot 10^{-3} + 1,3 \cdot 10^{-3}) [\text{s}]} = 0,0091$$

Effektiviteten U=0,0091.

Dvs 0,9% av tiden brukes til å sende data.

- c) Hva blir den effektive datahastigheten på denne forbindelsen til Princeton?

Den effektive datahastigheten er (den fysiske) datahastigheten multiplisert med effektiviteten. Det blir:

$$10 \cdot 10^6 \cdot 0,0091 [\text{bit/s}] = 91 \cdot 10^3 [\text{bit/s}] = 91 [\text{kbit/s}]$$

Oppgave 3

- a) Hva er forskjellene på en IPv4 adresse og en MAC adresse. Forklar også hvorfor begge to må brukes.

En IPv4 adresse virker på lag 3 i TCP/IP modellen. Det er et system på disse adressene slik at det er mulig å finne ut hvor en IPv4 adressen befinner seg på internet.

En IPv4 adresse består av totalt 4 byte. IPv4-adressen består av en nettdel og en hostdel. En host vil få en ny IPv4 adresse når den blir koblet til et annet nett (LAN). Alle host på et LAN har samme nettdel av adressen.

En MAC adresse består av 6 byte. De 3 første byte forteller hvilken fabrikant det er og de 3 siste bestemmer fabrikanten selv.

En MAC adresse virker på lag 2 i TCP/IP modellen. Det er ikke mulig å finne ut hvor en host med en bestemt MAC adresse befinner seg på internett, før datapakken er på det samme lokalnettet hvor denne MAC adressen befinner seg.

En host tar imot pakker basert på MAC adressen. IPv4 adressen brukes for å få pakke fram til riktig LAN, og der finner pakken riktig MAC adressen, basert på IPv4 adressen. Det finnes i ARP-tabeller. Hvis ikke MAC adressen til en host med en bestemt IPv4 adresse er kjent, sendes det ut en ARP-melding på dette LAN. En ARP-melding sendes som en broadcast til alle på LAN. Den host som har den IPv4 adressen som er i ARP-meldingen, svarer med info om sin MAC adresse.

b) Både PC'er, routere og annet må vite IP adressen til gateway-router. Hvorfor det?

Gateway router er veien ut på internett. Hvis en host ikke vet hvor en IP adresse befinner seg, som den skal sende til, vil pakken bli sent via gateway-routeren ut på internett.

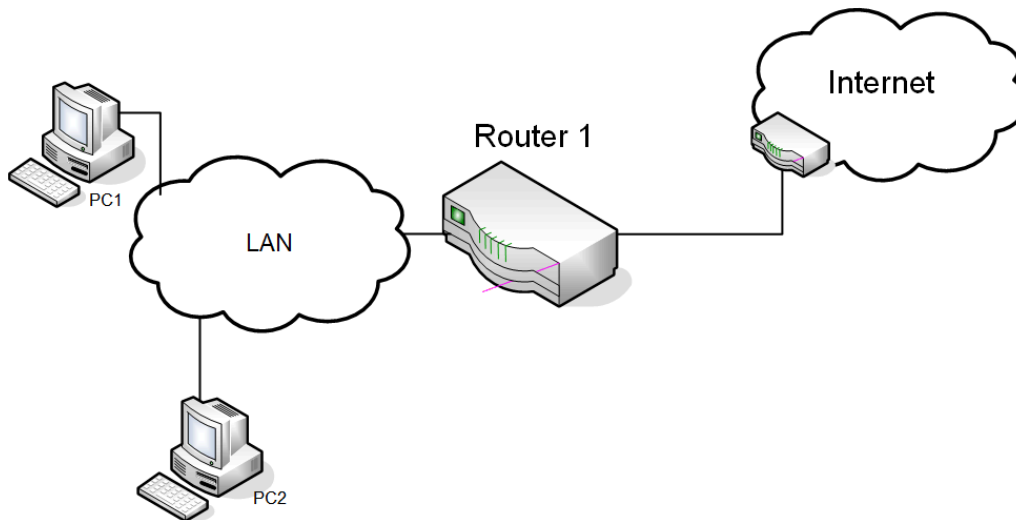
c) Skriv denne IPv6 adressen på en kortere form:

2001:067c:0000:003d: 0000:0000:0000:0016

2001:67c:0:3d::16

Oppgave 4

Anta at du har fått en IPv4-adresse og nettmask fra din ISP: 108.45.32.0/22. I begynnelsen lager du et LAN av dette, slik som på figuren under. Det skal **ikke** brukes private IP adresser.



a) Hvor mange host kan du ha på dette LAN?

/22 betyr at det er $32-22=10$ bit i hostdelen av IP adressen. Maks antall host blir da $2^{10}-2=$ **1022 host**.

-2 fordi nett-adressen og broadcast adressen kan ikke gis til en host.

b) Hva blir broadcast-adressen på dette LAN?

Broadcast adressen har bare 1'ere i hostdelen av adressen
Grensen mellom nettdel og hostdel av adressen går i den 3. byte. Vi ser da på byte 3 og 4:

32.0 -> **00100000**.00000000

Fet skrift indikerer bit i nettdelen av IP-adressen. Bare 1'ere i hostdelen gir:

00100011.11111111 -> 35.255

Broadcast adressen blir da 108.45.35.255

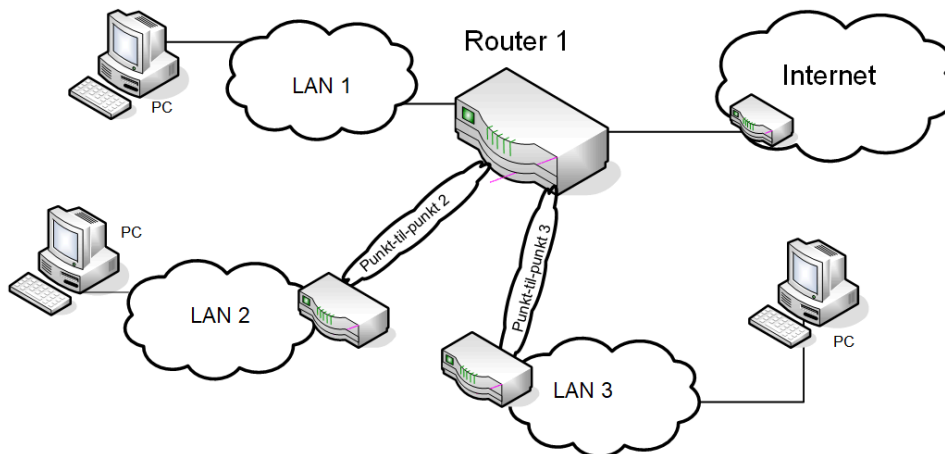
c) Hvilken IP adresse vil du gi Router 1, på LAN siden?

Vanligvis gir man routeren den første adressen etter nettadressen.
Det blir 108.45.32.01

Det gjør man bla. fordi det skal være enkelt å finne ut, uten å måtte spørre nettansvarlig.

Oppgave 5

Nå skal du dele dette hovednett (108.45.32.0/22) i tre like store LAN. To av disse LAN skal plasseres langt vekk, slik at det må være en punkt-til-punkt forbindelse til disse to LAN. Alle tre LAN skal være så store som mulig. Hva blir IP adressene til disse tre LAN, og på de to punkt-til-punkt forbindelsene? Angi også nettmasken. Det er nok å angi nettmasken på CIDR form. Det skal **ikke** brukes private IP adresser.



Hvis vi skal lage 3 LAN må vi bruke 2 bit fra hostdel til subnettbit. Med 2 bit kan vi få totalt 4 LAN, av like stor størrelse. Det ene av disse LAN brukes til punkt-til-punktforbindelser. Velger LAN 00 til det. **Rød farge** angir subnettbit. Da får vi:

00100000. 00000000 -> 108.45.32.0 / 22 - LAN vi går ut fra

00100011. 00000000 -> 108.45.35.0 / 24 → LAN 1

00100010. 00000000 -> 108.45.34.0 / 24 → LAN 2

00100001. 00000000 -> 108.45.33.0 / 24 → LAN 3

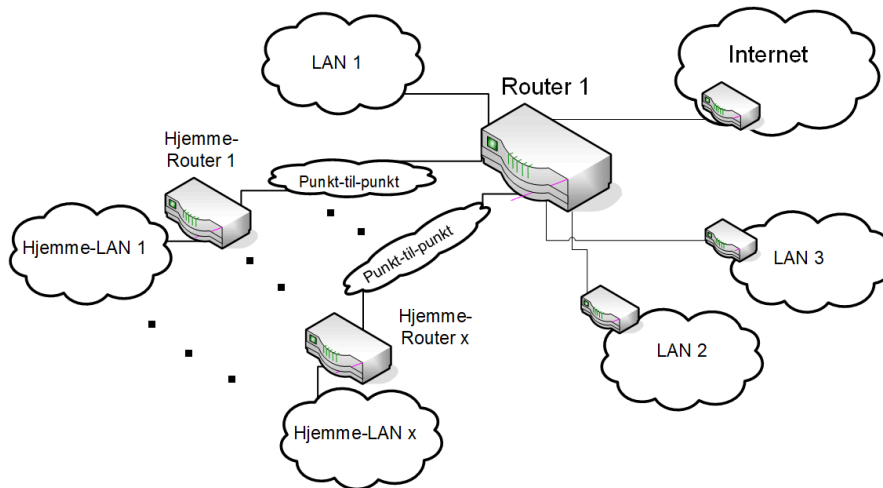
00100000. **00000100** -> 108.45.32.04 / 30 Punkt-til-punkt 2

00100000. **00001000** -> 108.45.32.08 / 30 Punkt-til-punkt 3

På en punkt-til-punkt-forbindelse er det kun 2 host. En i hver ende. Da er det nok med 2 host-bit. $2^2-2=2$

Oppgave 6

De adressene som er igjen fra hovednett, skal du dele ut til ansatte som ønsker å lage sine egne nett hjemme. De får da et hjemme LAN og et punkt-til-punkt samband til disse hjemme-LAN. Disse hjemme-LAN skal heller **ikke** bruke private IP. Alle skal få like store hjemme-LAN. Det skal være plass til 30 host på hvert av disse hjemme-LAN.



a) *Hvor mange slike hjemme-LAN kan du ha?*

Et nett med plass til 30 host har 5 hostbit, fordi $2^5 - 2 = 30$.

Da får vi 6 hjemme-LAN

00100000.00000000 -- Dette er brukt til punkt-til-punkt forbindelser.

00100000.00100000 -> «Hjemme-LAN 0»- må også brukes til punkt-til-punkt

00100000.01000000 -> Hjemme-LAN 1

00100000.01100000 -> Hjemme-LAN 2

00100000.10000000 -> Hjemme-LAN 3

00100000.10100000 -> Hjemme-LAN 4

00100000.11000000 -> Hjemme-LAN 5

00100000.11100000 -> Hjemme-LAN 6

Vi sjekker om det er adresser nok til punkt-til-punkt forbindelsene:

00100000.00001100

00100000.00010000

00100000.00010100

00100000.00011000

00100000.00011100

00100000.00100000

b) Angi nettdressene til disse hjemme-LAN, med maske.

00100000. 01000000 -> 108.45.32.64 / 27 Hjemme-LAN 1

00100000. 01100000 -> 108.45.32.96 / 27 Hjemme-LAN 2

00100000. 10000000 -> 108.45.32.128 / 27 Hjemme-LAN 3

00100000. 10100000 -> 108.45.32.160 / 27 Hjemme-LAN 4

00100000. 11000000 -> 108.45.32.192 / 27 Hjemme-LAN 5

00100000. 11100000 -> 108.45.32.224 / 27 Hjemme-LAN 6

Oppgave 7

a) Forklar TCP/IP stack'en. Nevn navnene på lagene, litt om hva hovedoppgavene til hvert lag er og hvorfor man har laget denne?

Lag 1 kalles det fysiske laget og forteller hva som skal beskrives i det fysiske laget. Det fysiske laget har som oppgave å få overført en bit feilfri mellom to punkter. Det er på dette laget at en beskrivelse av en bit finnes.

Lag 2 kalles datalink laget og forteller hva som skal beskrives for å få datapakker over til neste node i et nettverk.

Lag 3 kalles nettverkslaget og forteller hva som skal beskrives for at datapakker skal finne veien gjennom et nettverk.

Lag 4 kalles transportlaget og forteller hva som skal beskrives for at datapakker skal komme over til endepunktet i forbindelsen.

Lag 5 kalles applikasjonslaget, og sørger for at data fra applikasjonene på hver side får de data som er nødvendig.

En protokoll dekker et, eller flere lag i denne modellen (Internet Protokoll Stack).. Grensesnittet mellom lagene er veldefinert. En protokoll kan bruke «tjenester» levert av laget under, og den tilbyr tjenester til laget over. Den samme protokollen kan da brukes på forskjellige protokoller på lagene under. F.eks vil den samme web-browseren brukes uavhengig av hva slags linje som går ut.

- b) WiFi har flere IEEE 802.11 standarder. De forskjellige har sin egen bokstav etter 11-tallet. F.eks 802.11a, 802.11b, 802.11g, 802.11n osv. Forklar hva hovedforskjellene mellom disse forskjellige standardene er.

Hovedforskjellene mellom de forskjellige 802.11 standardene er hvilken modulasjon som brukes, og datahastigheten som er mulig å oppnå. Dessuten hvilket frekvensområde carrier-frekvenser er i, båndbredden på hver kanal, og antall MIMO strømmer.

- c) I WiFi er det to forskjellige konfigurasjoner som kan brukes. Begge disse skal kunne virke innen det samme fysiske området. Forklar hovedforskjellene på disse.

WiFi kan settes opp i ad-hoc mode og i infrastruktur mode. I ad-hoc mode kan en host ta initiativ til å sende til en annen host. I infrastruktur mode er det et AP (aksess-punkt) som styrer all kommunikasjon. Den forespør hver host om den har noe å sende.

- d) Forklar hvordan TCP justerer dataflyten i en forbindelse.

I TCP-hodet er det et felt som heter Receive Window. I ACK-pakke fra mottageren, legger mottageren info om hvor stor plass det er igjen i mottagerbufferet. Hvis Receive Window er lite, vil senderen justere flyten, slik at den ikke blir så stor.

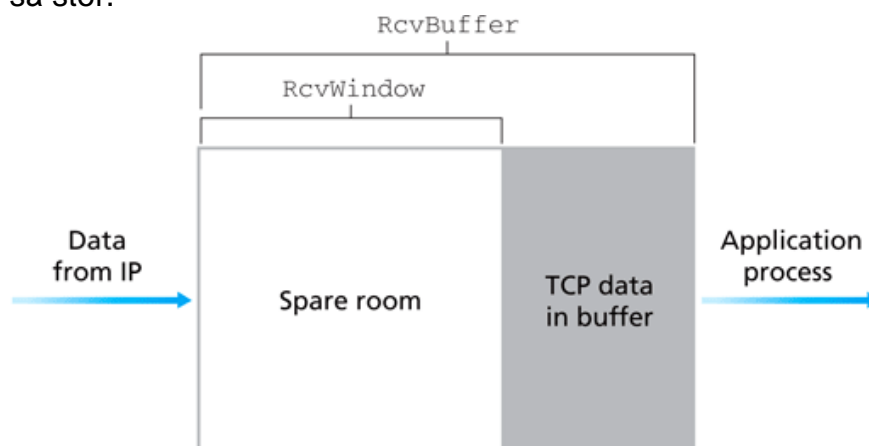


Figure 3.38 ♦ The receive window (RcvWindow) and the receive buffer (RcvBuffer)

VEDLEGG

Noen kjente portnummer:

www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
ftp-data	20/tcp	File Transfer [Default Data]
ftp-data	20/udp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
telnet	23/tcp	Telnet
telnet	23/udp	Telnet

$$U = \frac{L/R}{RTT + L/R}$$

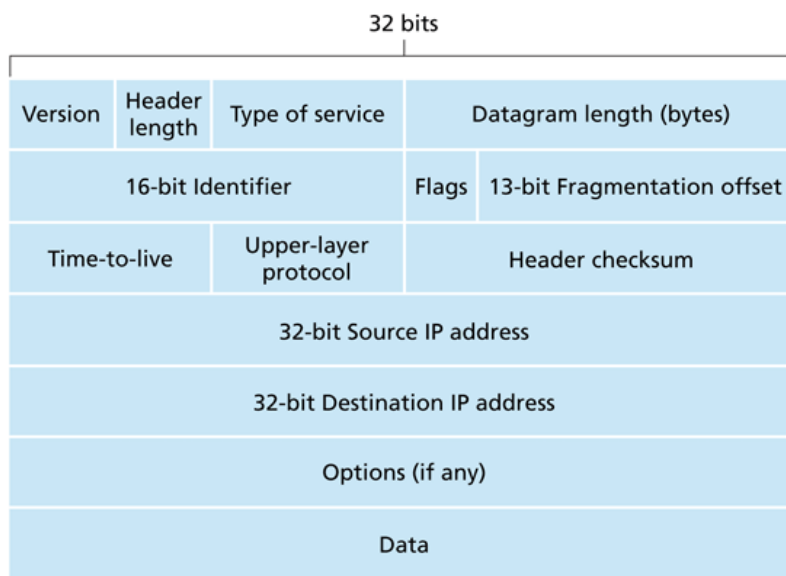


Figure 4.13 ♦ IPv4 datagram format

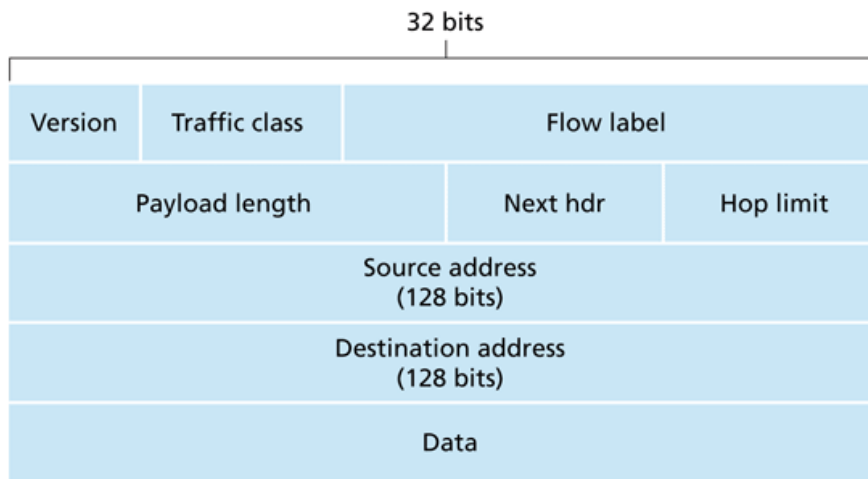


Figure 4.24 ♦ IPv6 datagram format

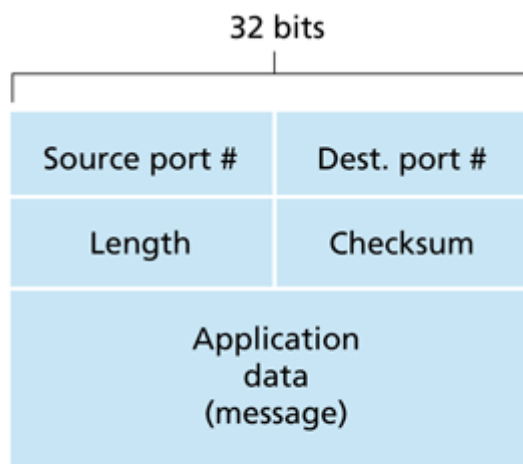


Figure 3.7 ♦ UDP segment structure

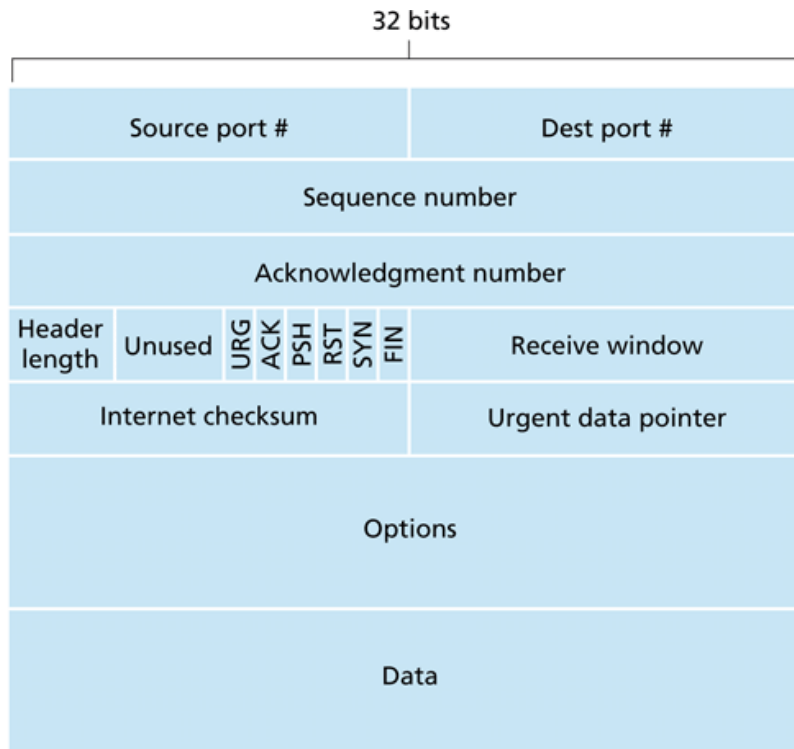


Figure 3.29 ♦ TCP segment structure