Høgskolen i Østfold

Løsningsforslag til

# EKSAMEN

| **Emnekode:** | **Emnenavn:** |
|---|---|
| **ITF20218** | **Datakommunikasjon** |
| **Dato:** | **Eksamenstid:** |
| **30. Nov 2018** | **Kl: 9:00 til kl: 13:00** |
| **Hjelpemidler:**<br>• 4 sider (A4) (2 ark) med egne notater.<br>• Kalkulator.<br>• Gruppebesvarelse, som blir delt ut til de som har levert innen tidsfristen | **Faglærere:**<br>**Erling Strand** |

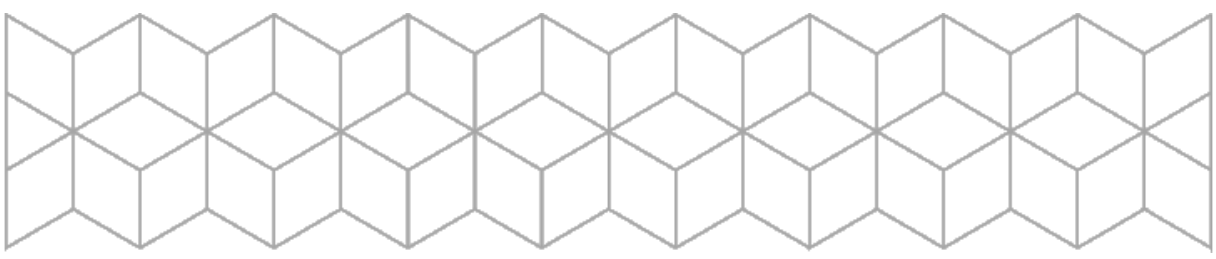
**Om eksamensoppgaven og poengberegning:**

Oppgavesettet består av totalt 7 sider, hvorav 1 førsteside, 4 sider med oppgaver, og 2 sider med vedlegg. Kontroller at oppgaven er komplett før du begynner å besvare spørsmålene.

*Oppgavesettet består av 3 oppgaver. Alle spørsmålene på de forskjellige oppgavene teller likt.* ***Alle svar må begrunnes.***

**Sensurfrist: 21 Desember 2018**

Karakterene er tilgjengelige for studenter i Studentweb www.hiof.no/studentweb



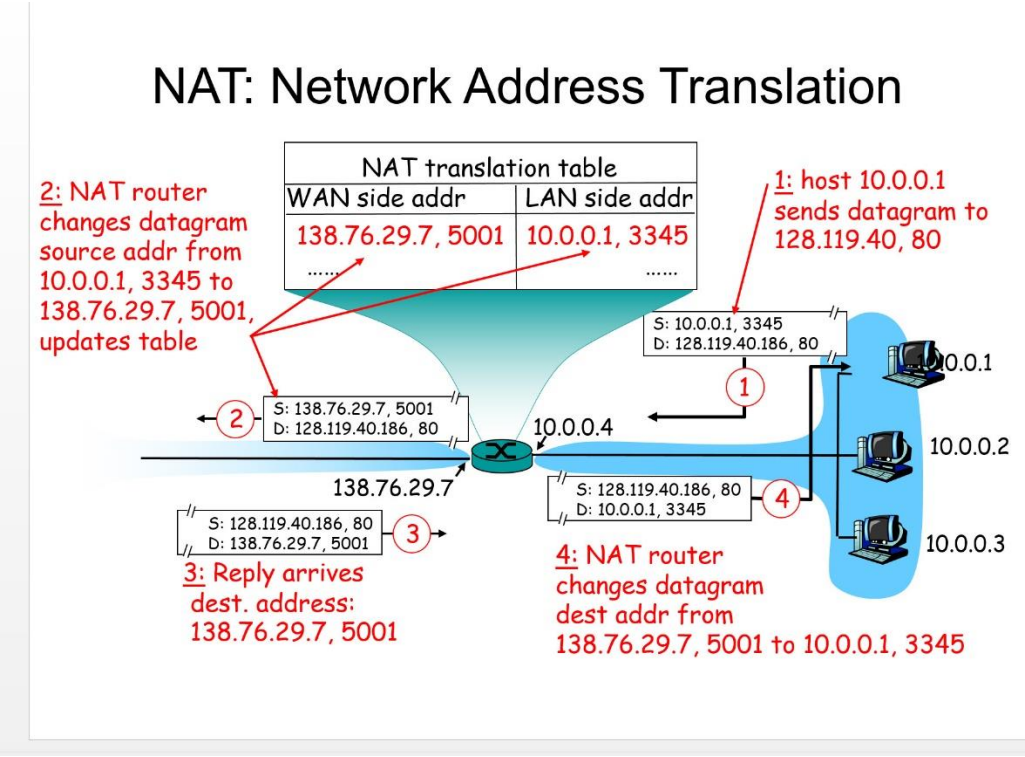
## Oppgave 1

a) *Anta at du har ditt eget LAN (Local Area Network) hjemme, som benytter private IP adresser. Din hjemme-router har både WiFi og mulighet for tilkobling av PC via kabel på LAN siden, og en WAN-tilkobling ut mot internet. Slik de fleste hjemme-routere har. Hvilke funksjoner må din hjemme-router tilby til de som skal koble seg til, for å komme ut på internet? Anta at ingen av disse funksjonene er implementert i noen andre maskiner på ditt LAN. Forklar også litt om hva de funksjonene gjør, og hvorfor de må være tilstede.*

Din hjemme router må tilby:

DHCP: DHCP står for Dynamic Host Configuration Protocol, og den brukes for å dele ut IP-adresse og andre nettverksparametre til en maskin som forespør om det. Enhver PC på et LAN må ha disse nettverksparametrene for å kunne bruke nettverket.

NAT: Network Address Translation oversetter mellom de private IP-adressene du har på ditt LAN til den ene IP-adressen du har ut mot internett. Den du har fått fra ISP, og som er på WAN siden. Når din PC sender en pakke ut på internet, setter den fra-ip adressen i pakka til sin egen private ip adresse. Din PC sier også hvilken portnr. den vil ha svaret tilbake på. NAT oversetter den private IP adressen til den IP adressen som er ut mot internet. Samtidig setter NAT et nytt portnummer den vil ha svaret inn på. Når så svaret kommer fra internet, vil NAT kjenne igjen portnummeret, og da skifte til IP-adressen til den private IP adressen og skifte portnummeret som din PC vil ha svaret inn på.



b) *Anta at din PC (eller annet datautstyr) er satt opp til å hente alle de opplysningen om nettet den trenger, fra din hjemme-router. Hvilke opplysninger er det? Forklar også litt om hvorfor din PC må ha de opplysningene.*

De opplysningene din PC trenger er:

IP-adressen til Gateway: Hvis IP adressen på en pakke, som din PC skal sende, ikke befinner seg på det LAN som din PC er tilknyttet, eller ikke din PC ikke vet hvor den IP-adressen befinner seg, må den sende pakka til gateway. Gateway er veien ut til internet.

IP-adressen til DNS-server: Vanligvis bruker man domenenavnet til den man skal kommunisere med. DNS-serveren oversetter domenenavnet til IP adressen. Din PC må vite hvor den skal finne IP adressen til det domenenavnet du bruker.

Nettmasken på nettet: Nettmasken forteller størrelsen på LAN din PC er tilkoblet. Den info brukes bla. når din PC skal sende ut en broadcast melding.

c) *På ditt LAN hjemme vil du ha en webserver, som er satt opp i en PC. Hva må du programmere/sette opp i din hjemme-router for å få webtrafikk (port 80) fra internet inn på din webserver. Forklar også virkemåten til det du setter opp.*

Port forward i hjemme-routeren må settes opp. Du skriver der inn hvilken privat IP adresse som pakker med portnummer for web (port 80) skal sendes til. En pakke med portnummer 80 som da kommer inn til din hjemme-router, blir sent videre til den PC på ditt LAN, hvor webserveren er.

d) *Du ønsker et eget domenenavn på denne webserveren på ditt LAN hjemme. Du har ikke fast IP adresse fra din internetleverandør (ISP) . Hvilken tjeneste i din hjemmerouter må du da aktivere og sette opp? Forklar litt om virkemåten til denne.*

DynDNS må settes opp. Her skriver du inn hvilket domenenavn du har (host name), og vilken DNS som tilbyr DynDNS. Du må også skrive inn ditt brukernavn og passord til den DNS-serveren som tilbyr DynDNS. Din hjemme-router vil da sende info om hvilken IP adresse den har fått fra ISP til denne DynDNS. Hvergang din hjemme-router får en ny IP adresse fra ISP, vil hjemme-routeren oppdatere info i DynDNS.

*Anta at du ping'er www.dagbladet.no (fra en win10 maskin), og får denne utskriften på din skjerm:*

*Pinging www.dagbladet.no [2a02:c0:ac:3:db::181] with 32 bytes of data:*
*Reply from 2a02:c0:ac:3:db::181: time=2ms*
*Reply from 2a02:c0:ac:3:db::181: time=2ms*
*Reply from 2a02:c0:ac:3:db::181: time=2ms*
*Reply from 2a02:c0:ac:3:db::181: time=2ms*

*Ping statistics for 2a02:c0:ac:3:db::181:*
*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*
*Approximate round trip times in milli-seconds:*
*Minimum = 2ms, Maximum = 2ms, Average = 2ms*

e) *Skriv den fulle IPv6 adressen til dagbladet.no.*

2a02:00c0:00ac:0003:00db:0000:0000:0181

*Anta at du ping'er www.vg.no (fra en linux maskin), og får denne utskriften på din skjerm:*

*PING www.vg.no (195.88.55.16) 56(84) bytes of data.*
*64 bytes from www.vg.no (195.88.55.16): icmp_seq=1 ttl=248 time=2.39 ms*
*64 bytes from www.vg.no (195.88.55.16): icmp_seq=2 ttl=248 time=2.41 ms*
*64 bytes from www.vg.no (195.88.55.16): icmp_seq=3 ttl=249 time=2.82 ms*

*--- www.vg.no ping statistics ---*
*3 packets transmitted, 3 received, 0% packet loss, time 2002ms*
*rtt min/avg/max/mdev = 2.392/2.542/2.824/0.207 ms*

f) *Forklar hva slag info som ligger i «ttl» og «time», og hva du kan bruke disse verdiene til.*

"Ttl" står for time to live. Det er en byte I IPv4 hodet, som minker med 1 for hver router IP-pakka går igjennom. Hvis verdien blir 0, vil ikke pakka bli sendt videre. Routeren, hvor datapakka ble 0, sender info tilbake, at datapakka ble stoppet i den routeren. TTL er en sikkerhet for at ikke en pakke skal kunne gå evig rundt i internet. Ved å lese verdien på TTL kan man finne ut hvor mange routere pakken har gått igjennom, for å komme fram til mottageren.

Time sier hvor lang forsinkelsen er mellom sender og mottager, fram og tilbake. Det er RTT i uttrykket for effektiviteten U. Hvis man også vet datahastigheten (R ) og antall bit i datapakka (L), kan effektiviteten regnes ut.

## Oppgave 2

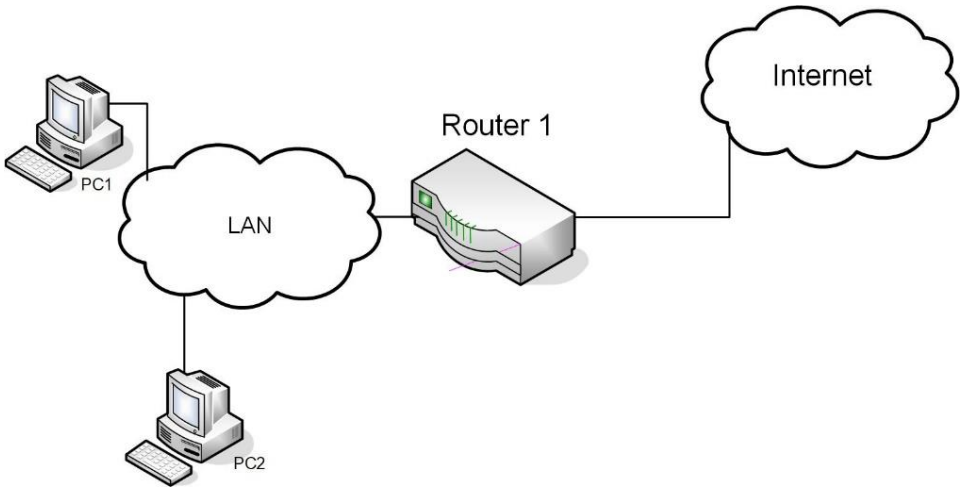
a) *Hva er VLAN? Forklar hva du oppnår ved å sette opp forskjellige VLAN*.

VLAN står for **V**irtual **L**ocal **A**rea **N**etwork. VLAN fungerer på lag 2 i TCP/IP modellen, og kan settes opp i f.eks switcher. Det kan brukes hvis f.eks en PC skal fysisk flyttes til et annet fysisk område, men allikevel tilhøre det samme LAN, som den har hatt tidligere. Det opprettes da et VLAN, hvor alle enheter som skal høre til dette LAN, blir lagt inn i dette VLAN. Det ser da ut som om alle enheter, som er definert inn i dette VLAN, er på samme LAN. VLAN kan i utgangspunktet defineres helt fra begynnelsen av, da LAN blir laget. Da står man fritt til å flytte PC'er (host) rundt omkring, uten å tenke på at de må kobles fysisk til samme switch.

b) *Hva er TRUNK? Trunk settes ofte opp mellom routere. Hva oppnår du ved å sette opp trunk mellom to routere? I hvilke tilfeller er det aktuelt å sette opp trunk mellom routere?*

Hvis man har et VLAN på forskjellige fysiske LAN, og som er forbundet med routere, må det settes opp i routerne. Hvis forbindelsen mellom routerene skal deles av flere VLAN, som er etablert på fysisk forskjellige LAN, kan man sette opp en TRUNK mellom routerne. Uten TRUNK måtte hvert VLAN ha hver sin forbindelse mellom routerne.

c) *Anta at du har fått en IP-adresse og nettmaske fra din ISP: 137.23.32.0/19. I begynnelsen lager du et LAN av dette, slik som på figuren under.*



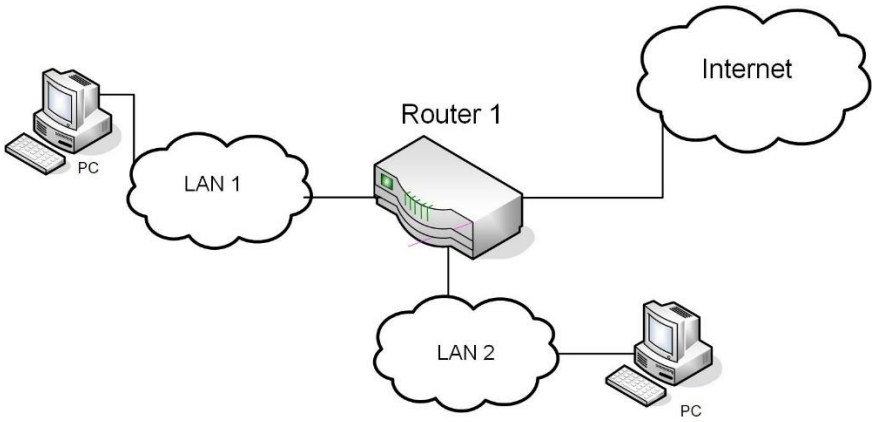
*I) Hvor mange host kan du ha på dette LAN?*

Antall host er gitt av antall bit i hostdelen av adressen. /19 betyr at det er 19 bit i nettdelen av adressen. Det gir 32-19=13bit i hostdel. Det gir $2^{13}$-2=8190 host. -2 fordi ingen host kan få adressen til LAN, hvor alle hostbit er 0. Dessuten kan ingen host få broadcastadressen til LAN, hvor alle hostbit er 1

*II) Hva blir broadcast-adressen på dette LAN?*

I broadcast-adressen er alle hostbit lik 1. Hvis vi ser på de to siste byte i adressen 137.23.32.0 => **001**00000.00000000 Bit med fet skrift hører til nettdelen av adressen. Hvis vi setter alle hostbit til 1, får vi: **001**11111.11111111 => 137.23.63.255 , som er broadcastadressen.

d) *Nå skal du dele dette hovednettet (137.23.32.0/19) i to like store LAN. Se figur under. Disse to LAN bør være så store som mulig, men du må ta hensyn til at du senere skal dele ut flere nett, av mindre størrelse, av dette hovednettet. Hva blir IP adressene til LAN 1 og LAN 2? Velg adresser som ligger mitt i adresseområdet. Angi også nettmasken. Det er nok å angi nettmasken på CIDR form.*



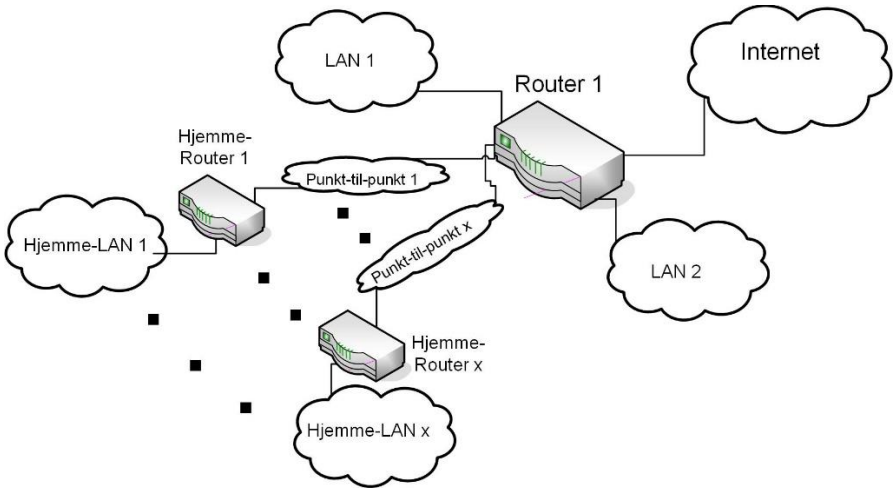

Da vi også skal lage flere nett senere, bruker vi 2 bit til subnettbit. Da grensen mellom nett og hostdel av IP-adressen går i den tredje byte, ser vi på de to siste byte i 137.23.32.00/19. Vi bruker to bit av hostdelen til subnett. Disse subnettbit er markert med **rød** skrift.

**001**00000.00000000

Vi velger adressene i mitten av adresseområdet. Det gir

**001**01000.00000000 -> 137.23.40.00/21
**001**10000.00000000 -> 137.23.48.00/21

e) *De adressene som er igjen fra hovednettet, 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 altså* ***ikke*** *bruke private IP. Alle skal få like store hjemme-LAN. Det skal være plass til 100 host på hvert av disse hjemme-LAN.*




*I) Hvor mange hjemme-LAN kan du ha?*

Når det skal være plass til 100 host på disse hjemme-Lan, må det være 7 bit i hostdelen, fordi $2^7$-2=126 > 100 Vi kan da finne ut hvor mange subnett-bit vi kan ha. De er markert med **rød** skrift:

**001**00000.**0**0000000 ->Subnett-zero kan vi bruke til punkt-til-punkt samband.

På 00-siden går hjemme-LAN fra

**001**00000.**1**0000000 til
**001**00111.**1**0000000.

Det blir $2^4$ – 1 = 1 hjemme-LAN. (-1 fordi subnett-zero skal brukes til punkt-til-punkt.)

På 11-siden går hjemme-LAN fra

**001**11000.**0**0000000 til
**001**11111.**1**0000000. Det blir $2^4$ = 16 hjemme-LAN.

Til sammen kan det bli 15+16=31 hjemme-LAN.

*II) Angi nettadressene til 4 av disse hjemme-LAN, med maske. Velg de som er i hvert sitt ytterområdet av adressene.*

**001**00000.**1**0000000 -> 137.23.32.128/25
**001**00111.**1**0000000 -> 137.23.39.128/25
**001**11000.**0**0000000 -> 137.23.56.00/25
**001**11111.**1**0000000 -> 137.23.63.128/25

III) Angi nettadressene til de punkt-til-punk sambandene som ligger i ytterområde av adressene du velger, med nettmaske.

Vi går ut fra subnett zero. På 00-siden får vi
**00100000.0**00000**00**
**00100000.0**11111**00** som er $2^5$=32 nett, med 2 bit til host, som blir punkt-til-punkt samband
Adressene til punkt-til-punkt samband blir da:
**00100000.0**00000**00** -> 137.23.32.00/30 (subnett zero)
**00100000.0**11111**00** -> 137.23.32.124/30

Dette blir til sammen 32 nett. Nå trenger vi 31 nett, så en av disse kan sløyfes. F.eks kan sub-nett zero sløyfes. Da blir nettadressene til de punkt-til-punkt samband som ligger i ytterområdet:
**00100000.0**00001**00** -> 137.23.32.04/30
**00100000.0**11111**00** -> 137.23.32.124/30

## Oppgave 3

a) *Wireless dataoverføring: Forklar kort bruksområdene for WiFi, WiMax, Bluetooth og ZigBee*.

WiFi skal brukes i LAN. Den skal erstatte kabel i LAN.
WiMax skal koble brukere til internet, som har for lang avstand til å kunne bruke kabel (telefonledninger)
Bluetooth skal koble enheter til din PC/datautstyr. Enheter som naturlig hører til en PC/datautstyr.
ZigBee kobler sammen små enheter, som skal kunne styres, eller som kan gi måledata. Det ble utviklet for å automatisere et hus eller bygning.

b) *En sikker dataoverføring er viktig å bruke når man sender data som ingen andre bør kjenne innholdet av. Forklar hvordan en sikker dataoverføring kan implementeres, og hvilke elementer som gjør den sikker. Ta med en enkel skisse som viser virkemåten Ta gjerne utgangspunkt i ssh eller scp.*

I en sikker dataoverføring krypteres data. Man bruker da to forskjellige nøkler, som er knyttet sammen. En nøkkel er en bitsekvens. Den ene nøkkelen kan være offentlig og den andre må være hemmelig. Den offentlige nøkkelen brukse for å kryptere data som skal sendes til deg. For å kunne dekryptere den meldingen, må den hemmelige nøkkelen brukes, og den har bare du.

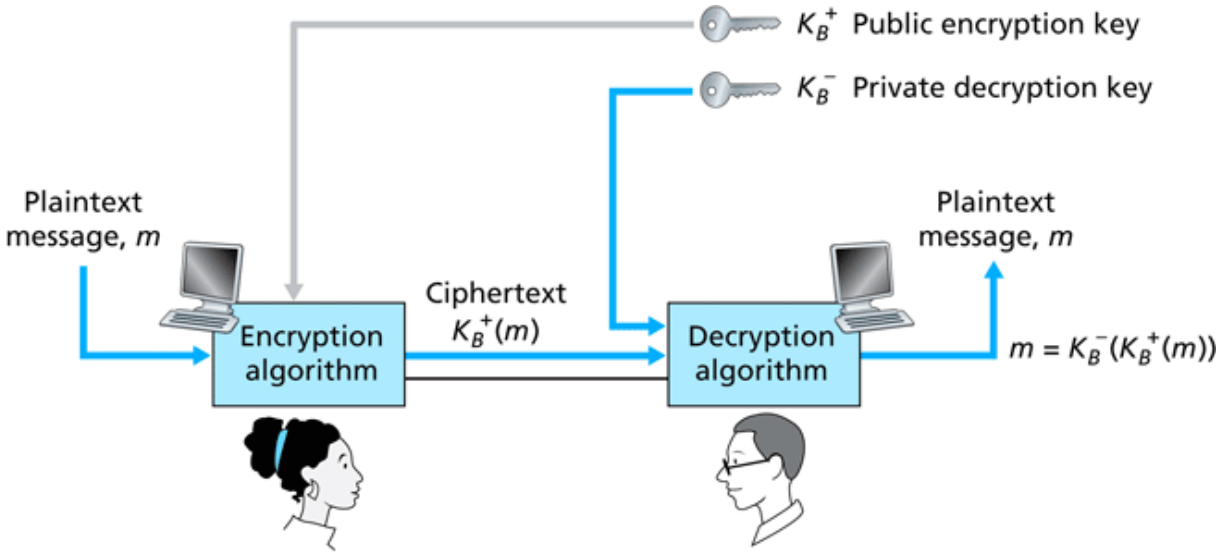



**Figure 8.6** ♦ Public key cryptography

c) *Forklar hvordan TCP oppdager og reagerer på kø på forbindelsen i nettverket.*

Kø kan oppstå i nettverket hvis det er stor trafikk inn på en router.

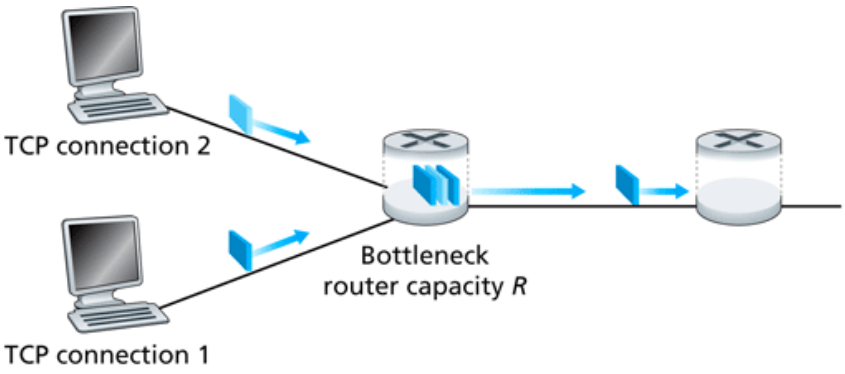



**Figure 3.54** ♦ Two TCP connections sharing a single bottleneck link

Kø oppstår lett hvis det er kontinuerlig dataoverføring, hvor det brukes et stort sendevindu, altså at mange pakker kan sendes før det må komme en ACK. TCP vet i utgangspunktet ikke om, og eventuell hvor stor kø det er i nettverket. TCP begynner derfor pent, for å sjekke hvor stort sendevindu den kan bruke.

Den begynner med et sendevindu på en, som da blir som en idle-RQ protokoll (stopp-og-vent protokoll). Den øker så sendevinduet for hver gang, helt til det blir pakketap. TCP oppdager altså kø ved at det blir tap av pakker. Da minsker den sendevinduet igjen. Slik finner TCP ut hvor stort sendevinduet kan være

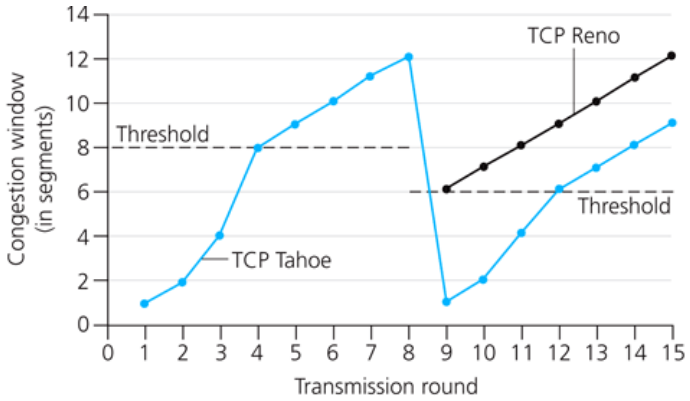



**Figure 3.53** ♦ Evolution of TCP's congestion window (Tahoe and Reno)

d) *I internet finnes det forskjellige AS (Autonomous System). Hva er det, og hvorfor har man delt opp i forskjellige AS?*

**A**utonomous **S**ystem (AS) er en del av internet, som består av flere routere og LAN. Internet er delt opp i mange AS. Hver av disse AS indentifiseres med et nummer; AS<nr>. Routerne innen et AS utveksler info, bla. routinginfo seg i mellom via bestemte protokoller. En stor bedrift, eller institusjon, kan ha sitt eget AS<nr>.

Internet er delt inn i flere AS bla. fordi det er for mange routere i hele internet, til at alle kan utveksle info seg i mellom. Det er derfor hensiktsmessig å la et begrenset antall routere, som  i et AS, utveksle info seg i mellom. Routerne som er "i kanten" på et slik AS, kalles en gateway router. Gateway routere kommuniserer med en tilsvarende gateway router i et annet AS. Den vanlige routing protokollen mellom AS er BGP.

Et AS kan i prinsippet velge hvilken routing algoritme, og dermed routing protokoll som skal brukes i sitt AS. Vanlige routing protokoller innen et AS er RIP eller OSPF

## VEDLEGG

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

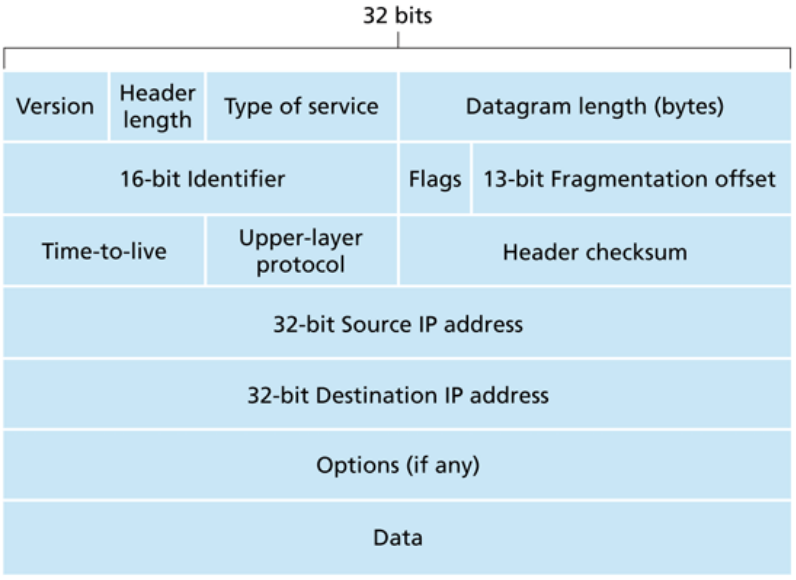



**Figure 4.13** ♦ IPv4 datagram format

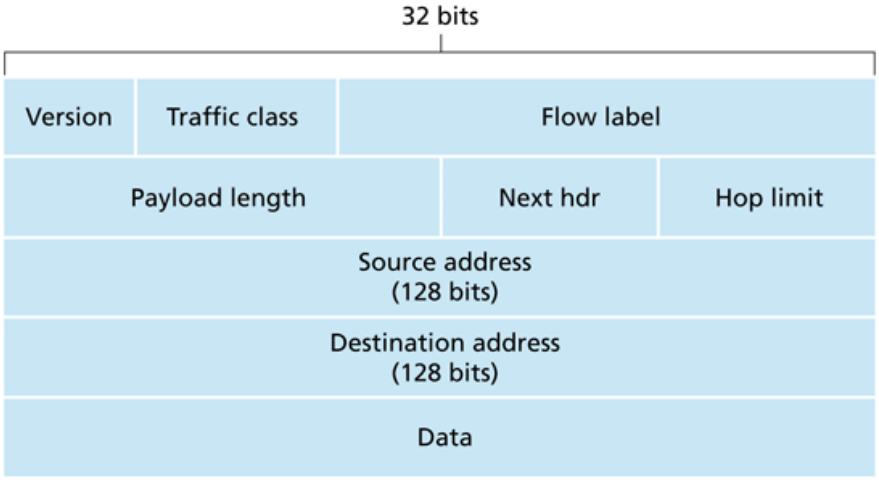



**Figure 4.24** ♦ IPv6 datagram format

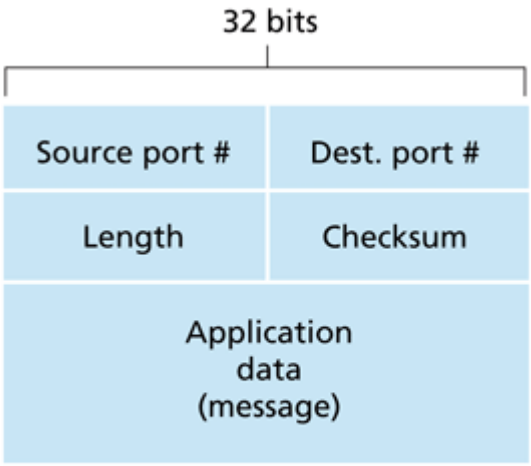



**Figure 3.7** ♦ UDP segment structure

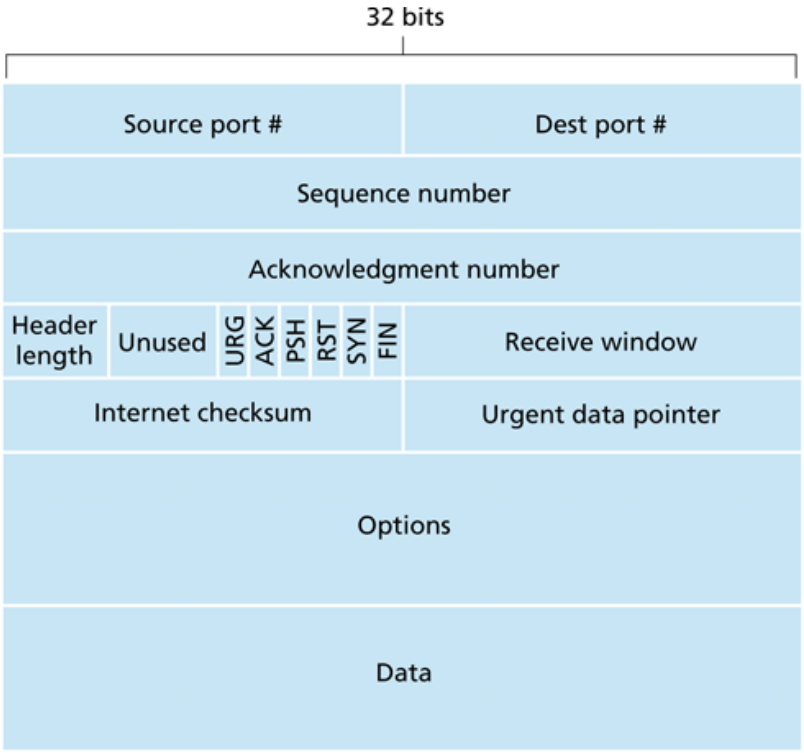



**Figure 3.29** ♦ TCP segment structure