
Nettverks-oppsummering vår 2024

Innhold

Transmisjonsmedier	2
Kobberkabler	3
Fiberkabler	3
Trådløse medier	3
Standarder, protokoller og modeller	4
Leveringsmetode	4
Referansemodeller	4
Segmentering av data	5
Data Access og adressering	6
Data Link (layer 2)	6
Nettverkskomponenter	7
Duplex	7
Ruting fra klientperspektiv	8
Default Gateway	9
Ruter-trafikkbehandling	9
Gangen i en HTTP-forespørsel til en vanlig nettside	10
Internet Protocol (IP) –adresser og –pakker	12
IPv4	12
Subnet Mask	13
Bit-kalkulasjonen; Network Address	16
Spesielle adresser – ikke så viktig	16
IPv4-Protokoll: Unicast	17
IPv4-Protokoll: Broadcast	17
IPv4-Protokoll: Multicast	17
IPv6	18
IPv6 Protokoll: Unicast	19
IPv6-Protokoll: Anycast	20

IPv6-Protokoll: Multicast.....	20
Subnetting IPv6.....	20
Overgangsordninger mellom IPv4 og IPv6.....	20
Industriell Ethernet.....	22
Funksjon og behov	22
Sammenligning og konsekvens	22
Cyber Security Trends	23
Ransomware Zero-days og Mega Attacks.....	23
Utvidende angrepsoverflate: Den voksende risikoen for kantenheter	23
Statsaffiliet Hacktivisme og Wipers blir den nye normen	23
Tokens Under Angrep: Skyens Akilleshæl	23
PIP Install Malware: Programvarelager Under Angrep.....	24
Linker	25
Løsningsforslag fra tidligere eksamener	26
2020 Vår.....	26
2021 Vår kont.....	28
2022 Høst.....	30
2022 Vår.....	32

Begreper

Overføringsbegreper:

- Båndbredde – maksimal teoretisk overføringshastighet
- Latency – hastighet fra A til B i millisekunder (delay)
- Throughput – hvor mye trafikk kan vi sende
- Goodput – hvor mye av det vi sender er faktisk nytte-data

Kilde: PowerPoint Transmisjonsmedier

Transmisjonsmedier

Kobberkabler

- Billigere en fiber
- Mest vanlige type kabel og mer tilgjengelig
- Treigere overføringshastighet en fiber
- Kan få interferens fra EMI

Fiberkabler

- Immun mot EMI hvis den er hel og ordentlig koblet opp
- Dyrere en kobberkabler
- Raskere hastighet en kobber kabler
- Større rekkevidde en kobber kabler

Trådløse medier

- God mobilitet, tilgjengelighet og fleksibilitet
- Bruker elektromagnetiske radiobølger til å sende binære data
- Har stor mobilitet dvs at nettet er tilgjengelig for alle brukere i ett bygg

Noen begrensinger for trådløse medier

- Dekningsområde
 - Trådløs nett fungerer bra i et åpent område, men i ett bygg med med visse typer byggematerialer så vil det begrense det effektive dekkningsområde
- Trådløs nett blir påvirket i større grad en kobber og fiber i henhold til interferens. Trådløs nett kan bli påvirket av trådløse telefoner, mikrobølgeovner og andre trådløse kommunikasjonsmedier
- Sikkerhet. Siden trådløst nettverk ikke trenger et fysisk medium for å koble seg til nettet så kan brukere og enheter som ikke er autorisert til å være på nettet få tilgang.
- De fleste WLANS opperer i half duplex. Det betyr at bare en enhet kan sende eller motta om gangen. Den trådløse ruten er delt mellom alle enhetene på WLAN-en og mange brukere kan resultere i redusert Bandwidht.

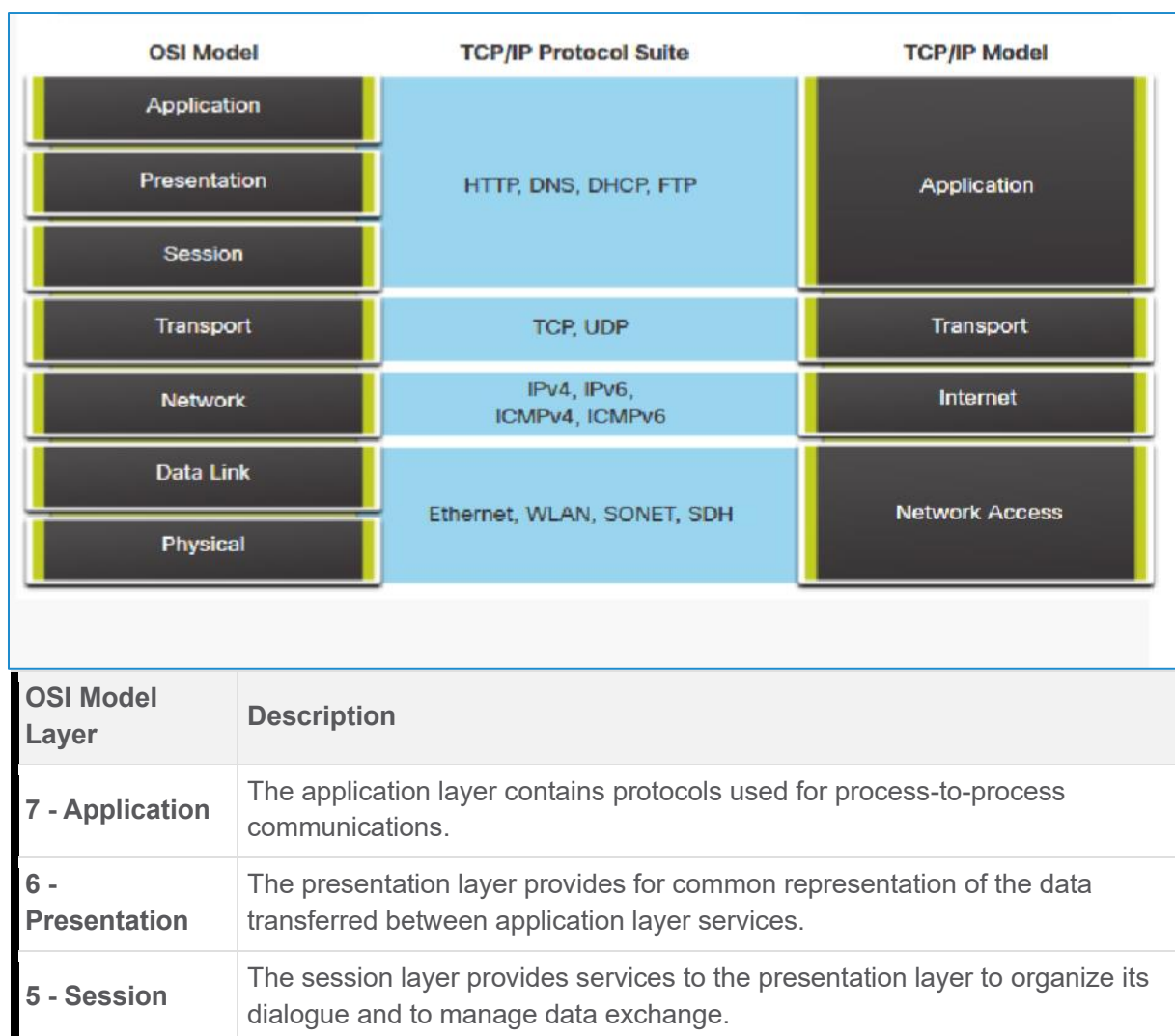
Standarder, protokoller og modeller

Leveringsmetode

- Unicast (en til en kommunikasjon)
- Multicast (en til mange, men vanligvis ikke alle)
- Broadcast (en til alle)

Referansemodeller

OSI, TCI og IP modeller, disse er lagdelt og påvirker lagene på litt forskjellige måter.

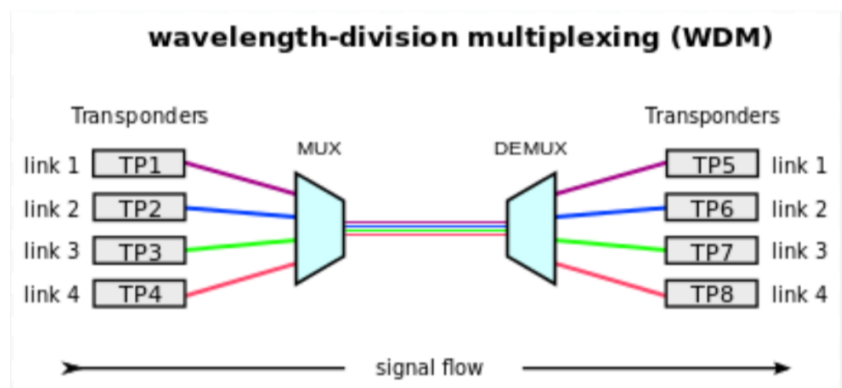


4 - Transport	The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
3 - Network	The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
2 - Data Link	The data link layer protocols describe methods for exchanging data frames between devices over a common media
1 - Physical	The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission to and from a network device.

Hvert lag påvirker spesifikk informasjon og de påvirker ikke de andre lagene. Det vil si at man kan endre på et lag uten å påvirke de andre. Det er et felles språk for å beskrive funksjoner og er tilgjengelig for alle.

Segmentering av data

Deler datastrømmen opp i flere pakker og sender alt igjennom samme datalink.(multiplexing)



Noen

med segmentering av data

fordeler

- økt hastighet: Kan sende store data mengder uten å blokke datalinjen for andre pakker

- økt effektivitet: hvis en pakke blir tapt så slipper man å sende hele datastrømmen på nytt, bare den pakken som blir tapt.

- må nummereres for at mottakeren skal kunne sette sammen pakkene på riktig måte.

Data Access og adressering

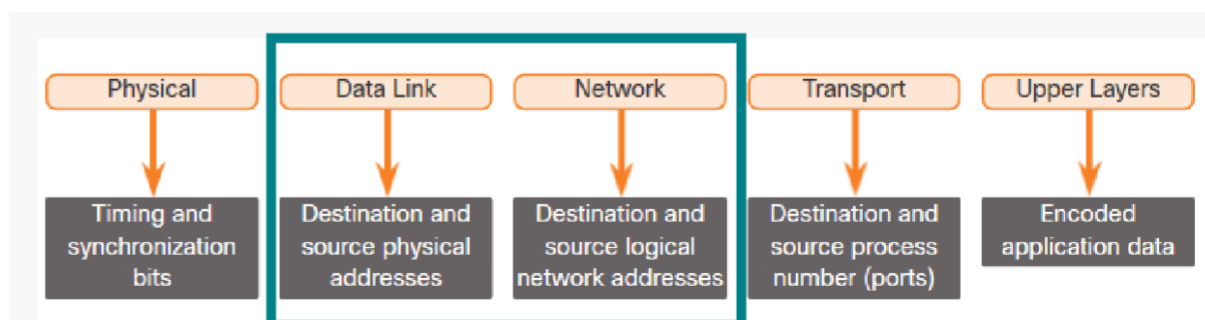
Både DataLink og Network layer brukes til å adressere data. (se OSI/TCI modellen)

Network (lag 3 ip-adresser):

- Kilde (original avsender)
- Mottaker (endelig destinasjon)
- Må brukes for å kommunisere mellom nettverk
- Første del av adressen kalles nettverksdel og er felles for alle devicene på samme nett
- Siste del av adressen kalles for host/klient del. Identifiserer en spesifikk enhet på nettverket.
- For å skille mellom nettverksdelen og host/klient delen så bruker man en submask.

DataLink (lag 2 fysiske adresser):

- hvert nettverkskort har en fast fysisk adresse.
- Mac adressen vil bli endret av alle som mottar og avsender meldingen.
- Source Mac er den som sist sende meldingen videre
- Destinasjon Mac er den neste i rekken som mottar meldingen



Data Link (layer 2)

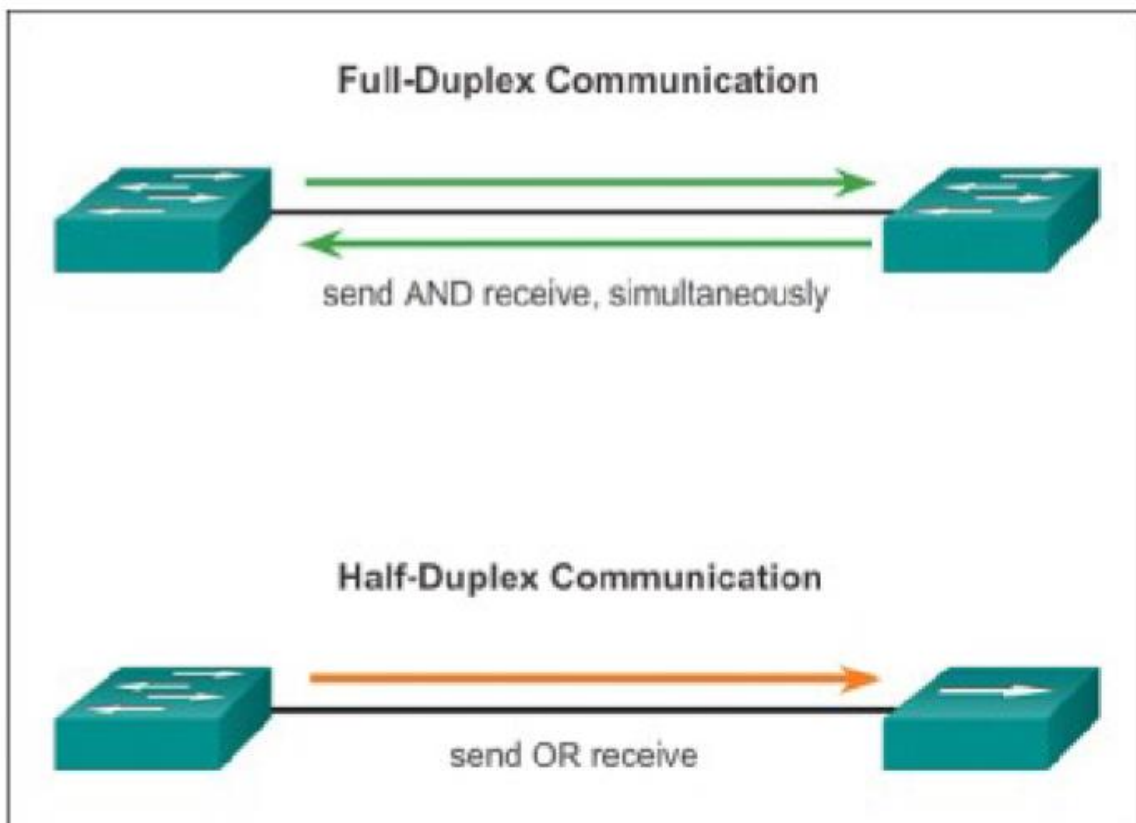
Formålet med data link er at forskjellige typer enheter kan koble seg til uten at det påvirker lagene over og kontrollere hvordan data sendes og mottas på media.

Nettverkskomponenter

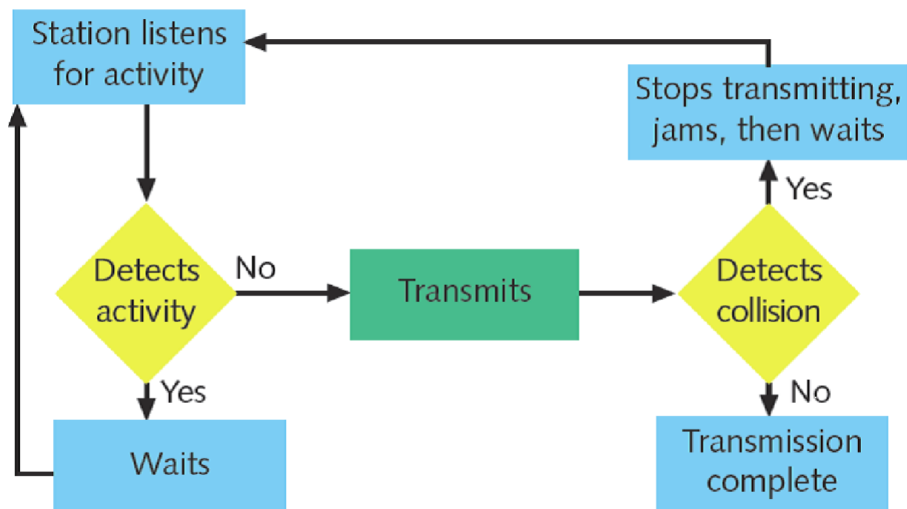
Duplex

Full duplex er to veis kommunikasjon hvor enheter på nettet kan sende og motta meldinger samtidig.

Halv duplex er en-veis kommunikasjon. Det vil si at man kan enten bare sende eller mottat informasjon tenk walkie talkie.



Duplex mismatch



10

Ruting fra klientperspektiv

- Ip-pakken opprettes lokalt hos klienten sin pc altså sourcen
- En klient kan kommunisere med følgende
 - Seg selv
 - Andre enheter på det lokale nettverket (local hosts)
 - Andre enheter på andre nett (remote hosts)
- Når en kilde skal sende en pakke må man først fastslå om destinasjons kilden er på samme nettverk eller et remote nettverk. Med en ipv 4 adresse så sjekker kilden sin egen ip adresse og submask med destinasjons ip adressen. Er nettverksadressene like så er de på samme nett
- Hvis sourcen er på samme lokale nett som destinasjonen så sendes pakken til switchen som sender pakken videre til destinasjonen. Hvis destinasjonen ikke er på samme nett som kilden blir pakken sendt av gårde til default gatewayen som ruter pakken til riktig destinasjon

Default Gateway

Er vanligvis en ruter eller en L3 switch.

- Må ha en ip-adresse i samme nettverk som brukerne
- Kan motta trafikk fra det lokale nettverket og videre sende denne til andre nettverk
- Må ha en rute til andre nettverk

Hvis en enhet eller et lokalt nettverk mangler en default gateway som oppfyller disse kravene over så vil nettverket/enheten ikke klare å kommunisere med enheter utenfor det lokale nettverket. Klienten vet om sin default gateway enten gjennom DHCP protokollen i IPv4 eller statisk (manuelt skrevet inn). Alle enheter på et lokalt nettverk må vite om en default gateway for å klare å kommunisere med nettverk utenfor sitt lokale nett.

Ruter-trafikkbehandling

Statisk ruting

- Må konfigureres manuelt
- Hvis man skal endre noe må man gjøre det manuelt
- Funker greit i små nettverk med lite redundans

Dynamisk ruting

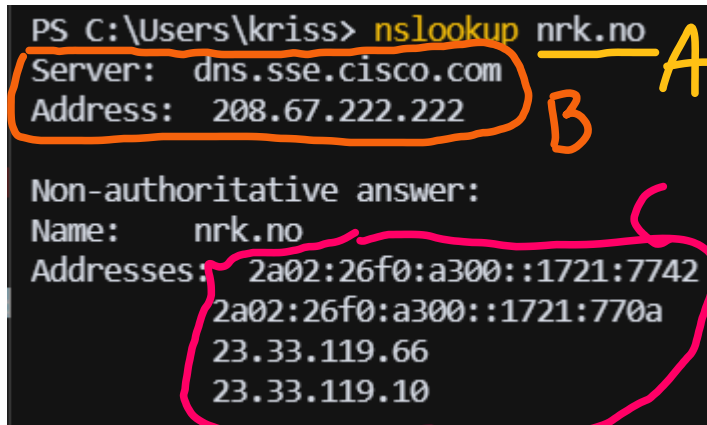
- Oppdager eksterne nettverk
- Vedlikeholder oppdatert informasjon
- Velger beste rute til destinasjonen
- Finner nye ruter når topologien endres

Gangen i en HTTP-forespørsel til en vanlig nettside

1. Navnesøk: Oversette Domene til IP-adresse

```
PS C:\Users\kriss> nslookup nrk.no
Server: dns.sse.cisco.com
Address: 208.67.222.222

Non-authoritative answer:
Name: nrk.no
Addresses: 2a02:26f0:a300::1721:7742
           2a02:26f0:a300::1721:770a
           23.33.119.66
           23.33.119.10
```



Beskrivelse:

- a. Domenet NRK.no
 - b. Sender forespørsel til Domain Name Servers (DNS, eller navnetjener på norsk)
 - i. DNS-protokollen (port 53)
 - ii. DNS-servere tildelt under DHCP
 - iii. I bildet over er DNS-serveren styrt av Cisco. Mest sannsynlig en lokal navnetjener
 - c. Får tilbake NRK sine IP-adresser (to IPv4 og to IPv6)
 - i. Lagrer resultatet lokalt i cache
- ### 2. MAC-søk
- a. IPv4:

Address Resolution Protocol (ARP)

Finne ut hvor pakken skal sendes; oversette IP-adresse til MAC-adresse

 - i. Sjekker først om IP-adressen matcher subnettet maskinen er på (ved hjelp av subnet mask). Er IP-adressen lokalt søker man på ARP-tabellen etter MAC-adressen til den andre lokale maskinen sin NIC. Er den ikke på den lokale tabellen, må man sende en ARP-request (Broadcast til alle på LANet).
 - ii. Hvis IP-adressen er utenfor LAN blir MAC-adressen til Default Gateway valgt. Det er denne som da mottar pakken for videre routing.
 - b. IPv6:

Neighbor Discovery (ND)

 - i. Veldig likt ARP-metoden, men noen distinksjoner (bruker fem ICMPv6-meldinger). Håper vi ikke trenger å kunne dette :)
- ### 3. Maskinen oppretter og sender HTTP-pakker til NRK.no for å spørre etter informasjon

- a. HTTP er layer 7.
 - b. Kapsles inn i TCP (layer 4)
 - c. Kapsles inn i IP (layer 3) hvor man bruker IP-adressen til lokal maskin og NRK.no
 - d. Kapsles inn i ethernet (layer 2) mellom lokal maskin og default gateway, og videre mellom ruter og NRK.no - basert på MAC-adresser.
4. NRK mottar, behandler og svarer. Svar-pakkene pakkes på samme måte og går samme vei tilbake.
5. Ettersom dette er TCP vil det gå mange kontroll-pakker frem og tilbake, for hver pakke med faktisk nyttig informasjon.

Internet Protocol (IP) –adresser og –pakker

I et IPv4-nettverk har alle maskiner en lokal IPv4-adresse (LAN). Default Gateway har den offentlig IP-adressen (WAN). Translasjonen mellom WAN og LAN, i begge retninger, skjer i Network Address Translation (NAT) på Default Gateway/ruteren.

I et fullverdig IPv6-nettverk har alle maskiner to IPv6-adresser: en Global Unicast Address og en Link-Local Address.

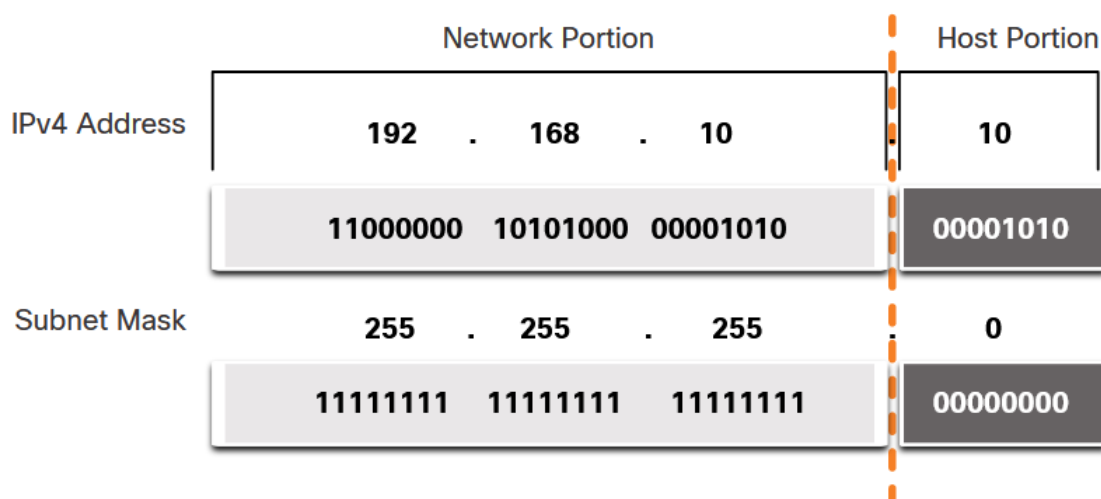
IPv4

$2^8 * (4 \text{ oktetter}) = 32\text{-bit adresser}$ (0.0.0.0 til 255.255.255.255).

Det er designert ulike adresse-områder for ulike formål. Styrt av Internet Assigned Numbers Authority (IANA). Disse er for private nettverk:

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Offentlige IP-adresser fordeles av Regional Internet Registries (RIRs). IP-addressene ble utsolgt rundt 2010.



Subnet Mask

Subnet Masken er en 32-bits “maske” som forteller noe om IPv4-adressen; hvilken del som er network- og host-bits.

1. The ones tell us the network bits of an IP address.
2. The zeros tell us the host bits of an IP address.

CIDR er en måte å notere Subnet Mask. Man noterer antall network bits, feks /24 (vanligste).

Subnetting løser flere problemer:

1. Sikkerhet: Enkel metode for å segmentere et nettverk så grupper med brukere blir atskilt.
Tenk at brukere på et offentlig Wi-Fi ikke skal være på samme segment som servere. Dette kan også løses med Virtuelle LAN (VLANs).
2. Enklere å administrere: Feks at alle IoT-enheter er på 192.168.100.***-nettverket.
3. Trafikkflyt: Mye av trafikken i et IPv4-nettverk er Unicast (fra enhet til enhet), men en del løsninger baserer seg på Broadcast eller Multicast.
Tenk at Chromecast i TVen sender ut meldinger om at “Her er jeg, bruk meg”.
Hvordan skulle andre enheter ellers finne Chromecasten?

Alternativet er at alle enheter sender pakker til alle andre IP-adresser i subnettet på nettverket for å spørre hva de gjør.

Eventuelt må man manuelt skrive IP-adressen til Chromecast.

Subnet eksempel Oblig 4 ↕

Host IP Address	192.168.50.50	
Original Subnet Mask	255.255.255.0	/24 Prefix original
New Subnet Mask	255.255.255.128	/25 prefix new mask
Number of Subnet Bits	1	Antall låste bits i ny maske minus gammel maske = $25-24=1$
Number of Subnets Created	2	2 opphøyd i subnet bits = $2^1 = 2$
Number of Host Bits per Subnet	7	32 minus låste bits i ny maske = $32-25=7$
Number of Hosts per Subnet	126	2 opphøyd i host bits, minus 2 = $2^7 - 2 = 128-2 = 126$
Network Address of this Subnet	192.168.50.0	oppgitt host IP address ganget med new subnet mask, binært AND
IPv4 Address of First Host on this Subnet	192.168.50.1	network address +1 = $0+1=1$
IPv4 Address of Last Host on this Subnet	192.168.50.126	network address + number of hosts per subnet = $0+126=126$
IPv4 Broadcast Address on this Subnet	192.168.50.127	last host +1 = $126+1=127$

Enkel oversikt over de mest brukte subnet masks i bits og tilhørende prefix

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

OBS: ”# of subnets” er antall subnets i forhold til et /24-nettverk, altså 255.255.255.0.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	n n n n n n n n . n n n n n n n n . n h h h h h h h 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 0 0 0 0 0 0 0	2	126
/26	255.255.255.192	n n n n n n n n . n n n n n n n n . n n h h h h h h h 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0	4	62
/27	255.255.255.224	n n n n n n n n . n n n n n n n n . n n n h h h h h h 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0	8	30
/28	255.255.255.240	n n n n n n n n . n n n n n n n n . n n n n h h h h h 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 0 0 0 0	16	14
/29	255.255.255.248	n n n n n n n n . n n n n n n n n . n n n n n h h h h 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 0 0 0	32	6
/30	255.255.255.252	n n n n n n n n . n n n n n n n n . n n n n n n h h h 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 0 0	64	2

Komplett oversikt over ulike Subnet Masks fra /8 til /32. De tre ”# subnets”-kolonnene er av samme type som bildet over.

	10.0.0.0/8					255.*.*	255.255.*	255.255.255.*		
	Prefix/Subbits	Subnet Mask			Subnet Mask in Binary	# subnets	# /16 subnets	# /24 subnets	# addresser	# hosts
10.0.0.0	8	255	0	0	11111111 00000000 00000000 00000000	1	0	0	16 777 216	16 777 214
	9	255	128	0	11111111 10000000 00000000 00000000	2	0	0	8 388 608	8 388 606
	10	255	192	0	11111111 11000000 00000000 00000000	4	0	0	4 194 304	4 194 302
	11	255	224	0	11111111 11100000 00000000 00000000	8	0	0	2 097 152	2 097 150
172.16.0.0	12	255	240	0	11111111 11110000 00000000 00000000	16	0	0	1 048 576	1 048 574
	13	255	248	0	11111111 11111000 00000000 00000000	32	0	0	524 288	524 286
	14	255	252	0	11111111 11111100 00000000 00000000	64	0	0	262 144	262 142
	15	255	254	0	11111111 11111110 00000000 00000000	128	0	0	131 072	131 070
192.168.0.0	16	255	255	0	11111111 11111111 00000000 00000000	256	1	0	65 536	65 534
	17	255	255	128	11111111 11111111 10000000 00000000	512	2	0	32 768	32 766
	18	255	255	192	11111111 11111111 11000000 00000000	1024	4	0	16 384	16 382
	19	255	255	224	11111111 11111111 11100000 00000000	2048	8	0	8 192	8 190
	20	255	255	240	11111111 11111111 11110000 00000000	4096	16	0	4 096	4 094
	21	255	255	248	11111111 11111111 11111000 00000000	8192	32	0	2 048	2 046
	22	255	255	252	11111111 11111111 11111100 00000000	16384	64	0	1 024	1 022
	23	255	255	254	11111111 11111111 11111110 00000000	32768	128	0	512	510
	24	255	255	255	11111111 11111111 11111111 00000000	65536	256	1	256	254
	25	255	255	255	11111111 11111111 11111111 10000000	131072	512	2	128	126
	26	255	255	255	11111111 11111111 11111111 11000000	262144	1024	4	64	62
	27	255	255	255	11111111 11111111 11111111 11100000	524288	2048	8	32	30
	28	255	255	255	11111111 11111111 11111111 11110000	1048576	4096	16	16	14
	29	255	255	255	11111111 11111111 11111111 11111000	2097152	8192	32	8	6
	30	255	255	255	11111111 11111111 11111111 11111100	4194304	16384	64	4	2
ubrukelig	31	255	255	255	11111111 11111111 11111111 11111110	32768	32768	128	2	0
	32	255	255	255	11111111 11111111 11111111 11111111	65536	65536	256	1	-1

Oversikt over ulike nyttige faktaer knyttet til subnetting og IP-adresser

IPv4 Subnet Chart

CIDR	Subnet Mask	Total IPs	Assignable IPs
/1	128.0.0.0	2,147,483,648	2,147,483,646
/2	192.0.0.0	1,073,741,824	1,073,741,822
/3	224.0.0.0	536,870,912	536,870,910
/4	240.0.0.0	268,435,456	268,435,454
/5	248.0.0.0	134,217,728	134,217,726
/6	252.0.0.0	67,108,864	67,108,862
/7	254.0.0.0	33,554,432	33,554,430
/8	255.0.0.0	16,777,216	16,777,214
/9	255.128.0.0	8,388,608	8,388,606
/10	255.192.0.0	4,194,304	4,194,302
/11	255.224.0.0	2,097,152	2,097,150
/12	255.240.0.0	1,048,576	1,048,574
/13	255.248.0.0	524,288	524,286
/14	255.252.0.0	262,144	262,142
/15	255.254.0.0	131,072	131,070
/16	255.255.0.0	65,536	65,534
/17	255.255.128.0	32,768	32,766
/18	255.255.192.0	16,384	16,382
/19	255.255.224.0	8,192	8,190
/20	255.255.240.0	4,096	4,094
/21	255.255.248.0	2,048	2,046
/22	255.255.252.0	1,024	1,022
/23	255.255.254.0	512	510
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.254	2	2 *
/32	255.255.255.255	1	1

* /31 subnets are described in [RFC3021](#), which was primarily motivated by the potential for public address space conservation. There is no need for a broadcast address in a 'IPv4 Point-to-Point Links'.

IPv4 Classfull Ranges [RFC790](#)

Subnet	Range	Class
0.0.0.0/1	0.0.0.0 - 127.255.255.255	A
128.0.0.0/2	128.0.0.0 - 191.255.255.255	B
192.0.0.0/3	192.0.0.0 - 223.255.255.255	C
224.0.0.0/4	224.0.0.0 - 239.255.255.255	D
240.0.0.0/4	240.0.0.0 - 255.255.255.255	E

IPv4 Private IP Ranges [RFC1918](#)

Subnet	Classful description
10.0.0.0/8	a single class A network
172.16.0.0/12	16 contiguous class B networks
192.168.0.0/16	256 contiguous class C networks

IPv4 Special-Purpose Ranges [RFC5736](#), [RFC6890](#) & [RFC81](#)

Subnet	Description
0.0.0.0/8	This network
0.0.0.0/32	This host on this network
100.64.0.0/10	Shared Address Space
127.0.0.0/8	Loopback
169.254.0.0/16	Link local
192.0.0.0/24	IETF Assignments
192.0.0.0/29	IPv4 Service Continuity Prefix
192.0.0.8/32	IPv4 dummy address
192.0.0.9/32	Port Control Protocol Anycast
192.0.0.10/32	Traversal Using Relays around NAT A
192.0.0.170-171/32	NAT64/DNS64 Discovery
192.0.2.0/24	Documentation (TEST-NET-1)
192.31.196.0/24	AS112-v4
192.52.193.0/24	AMT
192.175.48.0/24	Direct Delegation AS112 Service
198.18.0.0/15	Benchmarking
198.51.100.0/24	Documentation (TEST-NET-2)
203.0.113.0/24	Documentation (TEST-NET-3)
240.0.0.0/4	Reserved
255.255.255.255/32	Limited broadcast

The private IP addresses actually also belong to this table, but are omitted here because we have listed them in the separate table above.

Bit-kalkulasjonen; Network Address

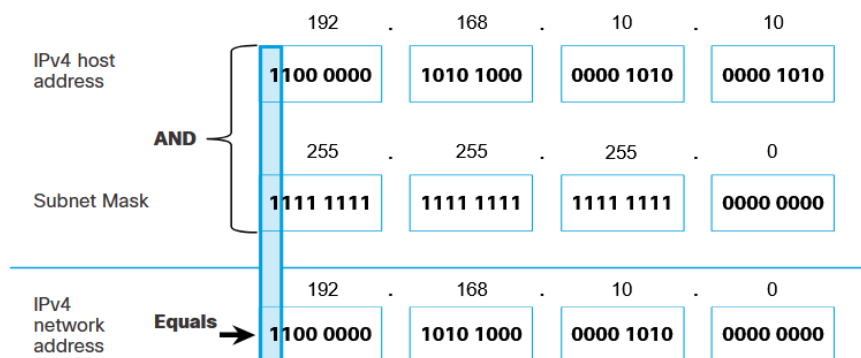
Subnet Binary address is the name for those 32-bit strings of ones and zeros. They map directly to the dotted-decimal notation you know and love like, 192.0.2.11 (which is 11000000000000000000001000001011 in binary).

Bitmask is a binary number you can overlay on another binary number to perform a bitwise operation.

IPv4 address 192.0.2.11	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subnet mask 255.0.0.0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Network address 192.0.0.0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

BITWISE AND OPERATION RULES: 1 AND 1 = 1 | 1 AND 0 = 0 | 0 AND 1 = 0 | 0 AND 0 = 0

- **IPv4 host address (192.168.10.10)** - The IPv4 address of the host in dotted decimal and binary formats.
- **Subnet mask (255.255.255.0)** - The subnet mask of the host in dotted decimal and binary formats.
- **Network address (192.168.10.0)** - The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.



Spesielle addresser – ikke så viktig

There are certain addresses, such as the network address and broadcast address, that cannot be assigned to hosts. There are also special addresses that can be assigned to hosts, but with restrictions on how those hosts can interact within the network.

Loopback addresses

Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254) are more commonly identified as only 127.0.0.1, these are special addresses used by a host to direct traffic to itself.

Link-Local addresses

Link-local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254) are more commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses. They are used by a Windows DHCP client to self-configure in the

event that there are no DHCP servers available. Link-local addresses can be used in a peer-to-peer connection but are not commonly used for this purpose.

IPv4-Protokoll: Unicast

- En til en
- Unicast transmission refers to one device sending a message to one other device in one-to-one communications.
- A unicast packet has a destination IP address that is a unicast address which goes to a single recipient. A source IP address can only be a unicast address, because the packet can only originate from a single source. This is regardless of whether the destination IP address is a unicast, broadcast or multicast.

IPv4-Protokoll: Broadcast

- Sender man en pakke til broadcast-adressen blir pakken sendt til alle på nettverket. Enten regnes ut basert på subnetmask, eller 255.255.255.255 (fungerer på alle nettverk).
- Broadcast går til alle på nettverket, frem til nærmeste ruter.
- Påvirker ytelsen drastisk (over 100 klienter).
- **IP med alle enere er *Broadcast address***
- Broadcast frames har destination MAC-address: FFFF:FFFF:FFFF

IPv4-Protokoll: Multicast

Trafikk går til alle som har meldt seg på.

- Multicast transmission reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group.
- A multicast packet is a packet with a destination IP address that is a multicast address. IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range.
- Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, and packets addressed to its uniquely allocated unicast address.
- Multicast frames har destination MAC-address mellom 0100:5E00:0000 og 0100:5E7F:FFFF.

IPv6

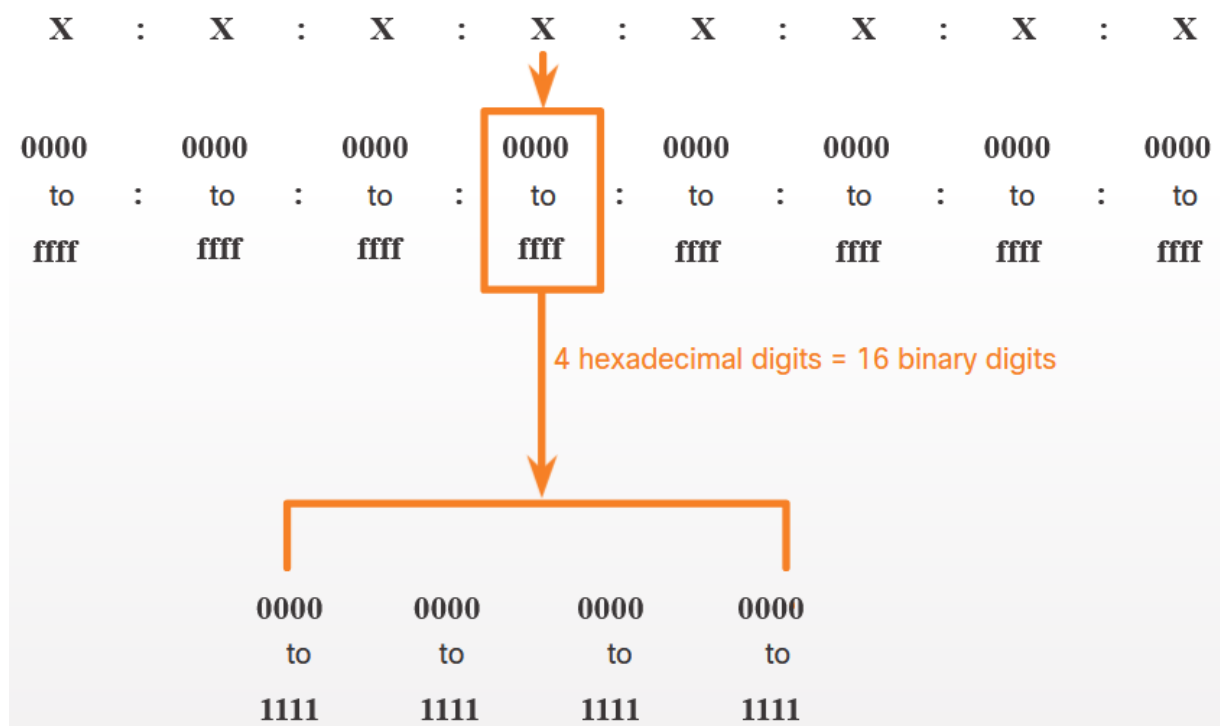
128-bit, HEX

Skriver heksadesimale tall (ikke case-sensitive) adskilt med kolon.

Seg selv: ``::1` (IPv6)

Trenger ikke subnet mask.

- Dropper leading zeros.
- Kan komprimere ETT felt med kun kolon til dobbel-kolon.



Prefix lengde er også i IPv6 representert som for eksempel /64

- › Forskjellen er at vi kan gå fra 0 til 128
- › Anbefalt for lokale nettverk er /64
 - › Diverse protokoller som automatisk tildeler adresser på IPv6 bruker /64
 - › Det å holde seg til denne konvensjonen gjør det lettere å holde styr på



IPv6 Protokoll: Unicast

Har en LLA (?) lokal (nesten som mac) og en GUA global (?).

Unik interface på en enhet som bruker IPv6.

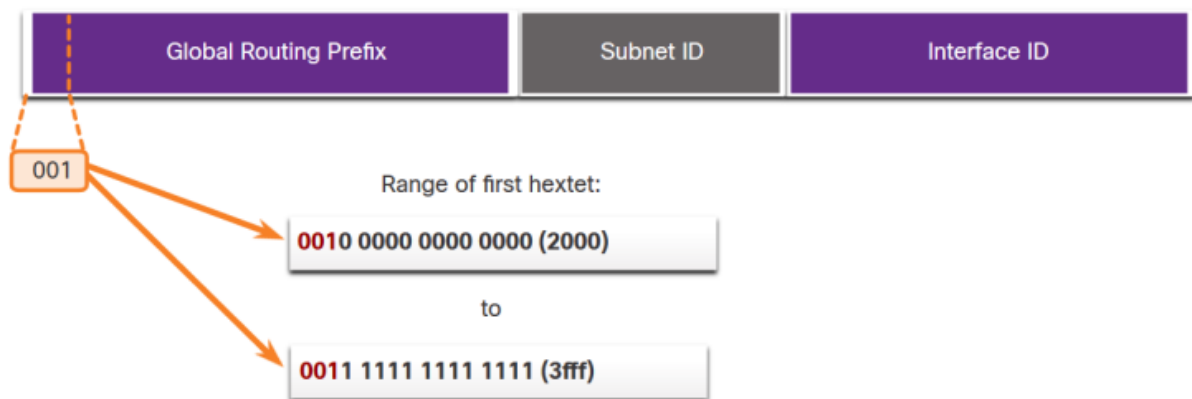
An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device.

Global Unicast Address(GUA)

Globalt unik - fungerer ut mot WAN.

Foreløpig brukes kun globale adresser som har de tre første bits satt til 001 (se figur).

Dette fører til at alle GUA adresser begynner med 2 eller 3 (se figur). Dette er ca. 1/8 av tilgjengelige IPv6 adresser.



- Global Routing Prefix: Prefix eller nettverksdel av adressen som deles ut sentralt.
- Subnet ID: Organisasjon kan dele opp nettverket sitt i subnets.
- Interface ID: IPv6-ekvivalent til IPv4 host-adresse. Identifiserer en spesifikk enhet.

Link-local adresse (LLA)

Kreves på alle IPv6-enheter og brukes for å kommunisere med enheter på samme link.

Kan ikke rutes og kun på aktuell link.

- En IPv6 link-local address lar enheter kommunisere med andre enheter på samme link.
- Pakker med source/destination satt til en LLA kan ikke rutes videre.
- Hvis en LLA ikke konfigureres manuelt på en interface, vil det opprettes en automatisk.
- IPv6 LLAer er i fe80::/10 område

IPv6-Protokoll: Anycast

Byttet broadcast til en smartere modell.

- An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

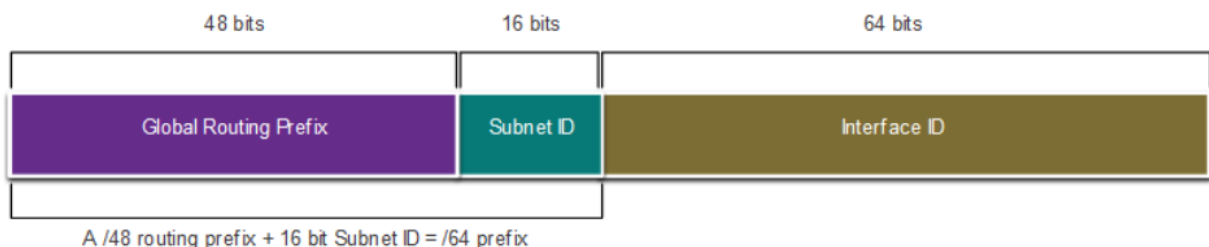
IPv6-Protokoll: Multicast

Trafikk går til alle som har meldt seg på.

- An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
- Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

Subnetting IPv6

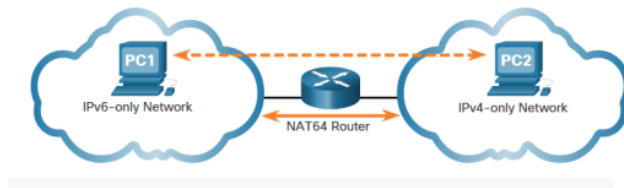
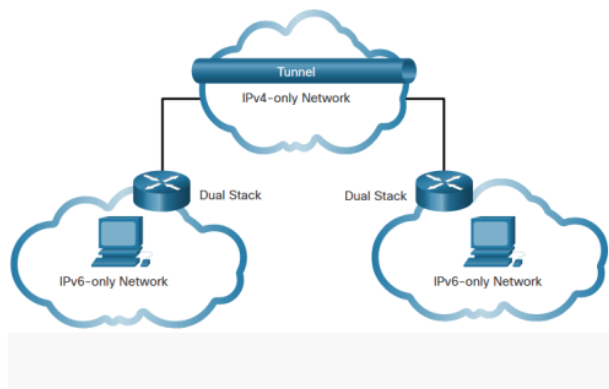
IPv6 er designet med tanke på subnetting fra grunnen av. Et eget subnet felt i IPv6 GUA brukes for å lage subnets.



- Subnetting av 2001:db8:acad::/48 Global Routing Prefix adresse med 16 bit subnet ID.
- Tillater 65.536 /64 subnets.
- Global Routing Prefix (første 48 bit) er felles for alle sammen.
- Bare subnet ID hexteten økes for hvert subnet.

Overgangsordninger mellom IPv4 og IPv6

- Dual stack: Kjører begge samtidig
- Tunneling: Kjører IPv6 innkapslet over et IPv4 nettverk
- Translation (NAT64): Lager en tabell og «oversetter» mellom v6 og v4



Industriell Ethernet

Industriell Ethernet refererer til bruk av Ethernet-teknologi i industrielle applikasjoner som fabrikker, produksjonsanlegg og automatiseringssystemer. Industrielle Ethernet skiller seg mer ut fra standard Ethernet-protokoller og teknologier spesielt ved å være ekstra godt robuste og pålitelige for det industrielle miljøet det er plassert i.



Tidlig på nittitallet var alle protokollene brukt i industrien proprietære på både seriell og Ethernet.

Dette førte til monopolisering når en fabrikk først hadde installert et system, da man ble låst til en spesifikk leverandør som kunne ta seg veldig godt betalt for deler og utvidelser.



Etter hvert som åpne protokoller kom på markedet, ble det mer innovative løsninger og produkter. Dette da små aktører lettere kunne få innpass. Man kunne også lettere kjøpe det beste utstyret på alle områder uten å være låst til en leverandør.

Funksjon og behov

For industrielle applikasjoner er det viktig med deterministiske nettverk der man vet nøyaktig hvor lang tid det går mellom pakkene, for eksempel for å vite hvor lang tid det tar fra man gir stopp-ordre til at maskinen stopper.

Industrielle Ethernet tar i bruk spesialiserte nettverkskomponenter, protokoller og topologier for å sikre stabilitet og ytelse selv i krevende forhold. Slike nettverkskomponenter er f.eks. kabler med “rugged connectors”, switcher som tåler høyere temperaturer, væske/fuktighet og eventuell vibrasjon. Pluggene kan f.eks. være isolerte mot fuktighet og støv, og skrur på kontakten slik at det blir tett og sitter fast. Kablene er ofte av høy kvalitet og robusthet på isolasjonen rundt. Fiber kan også brukes for å redusere EMI.

Full duplex er viktig for å unngå kollisjoner spesielt med tanke på å få kontrollsignaler gjennom på en robust måte. Hastigheten på linkene varierer fra 10 Mbps til 1 Gbps, men er typisk 100 Mbps.

Sammenligning og konsekvens

På et vanlig Ethernet, der man skal laste ned en nettside, hvis noen frames går tapt vil de bli sendt på nytt og det eneste som skjer er at brukeren kun opplever litt delay i lasting av siden.

Hvis på den andre siden noen frames går tapt i en industriell setting, som f.eks. de som inneholder kommandoer, kan dette få store konsekvenser.

Har man et deterministisk nettverk som fungerer optimalt, så skal slike ting enten forhindres eller oppdages og stoppes automatisk.

Cyber Security Trends

Ransomware Zero-days og Mega Attacks

Denne trenden markerer en evolusjon i ransomware-angrep, der angriperne nå benytter seg av zero-day-sårbarheter for å forårsake omfattende forstyrrelser. Ransomware-grupper som CL0P har benyttet slike sårbarheter til å ramme et bredt spekter av organisasjoner globalt. Disse angrepene har blitt mer sofistikerte og skadelige, og inkluderer ofte trusler om å lekke eller selge stjålet data, noe som kan ha alvorlige økonomiske og operasjonelle konsekvenser for de berørte.

Utvidende angrepsoverflate: Den voksende risikoen for kantenheter

Angrep på kantenheter som rutere og svitsjer representerer en økende risiko. Disse enhetene, som ofte er neglisjerte i sikkerhetsstrategier, har blitt et populært mål for både statssponsede og økonomisk motiverte angripere. Slike enheter kan utgjøre innfallsporter til mer omfattende nettverksinntrengninger, noe som understreker behovet for bedre sikkerhetstiltak og oppdateringer for disse kritiske, men sårbare, komponentene i IT-infrastrukturen.

Statsaffilieret Hacktivism og Wipers blir den nye normen

Hacktivism har utviklet seg fra å være en aktivitet drevet av enkeltpersoner og løst organiserte grupper til å bli en metode anvendt av nasjonalstater for å oppnå politiske mål gjennom cybervirksomhet. Dette inkluderer bruk av destruktiv programvare som wipers for å forårsake maksimal skade. Denne trenden har vært fremtredende i konflikter som den russisk-ukrainske krigen og konflikten mellom Israel og Hamas, der slike metoder har blitt normen fremfor unntaket.

Tokens Under Angrep: Skyens Akilleshæl

Sikkerhetstrusler mot autentiseringstokens har økt ettersom angripere målretter disse for å omgå sikkerhetstiltak som flerfaktorautentisering (MFA). Dette kan involvere sofistikerte angrep der angriperne stjeler eller forfalsker tokens for å få uautorisert tilgang til skytjenester og sensitive systemer. Slike angrep har rammet store teknologiselskaper og skyplattformer, og viser hvor sårbar digital infrastruktur kan være når avanserte truselaktører utnytter svakheter i implementeringen av sikkerhetsprotokoller.

PIP Install Malware: Programvarelager Under Angrep

Økningen i skadelig programvare som distribueres gjennom open-source programvarelager, som PyPi og NPM, er en bekymringsfull trend. Angripere utnytter ofte pakkenavn som ligner på populære biblioteker for å spre malware gjennom metoder som typosquatting og merkevarekapring. Disse angrepene kan føre til omfattende forsyningskjedeangrep der selv pålitelig programvare blir et middel for å spre skadelig programvare.

Linker

- [det meste av Netacad-pensumet](#)
- [prøveeksamen](#)

Løsningsforslag fra tidligere eksamener

2020 Vår

Oppgave 3

a. Hva brukes DNS-servere til? Hva skjer dersom du ikke får kontakt med denne?

Oversette domener til IP-adresser. Du vil ikke kunne kontakte domener som du ikke allerede vet adressen på.

b. Hva er en Default gateway? Hvorfor trenger vi denne?

Det er en nettverksenhet, for eksempel en ruter eller L3 switch, som kan rute trafikk til andre nettverk. Den trengs for å sende trafikk ut av det lokale nettverket. Hvis denne ikke finnes eller ikke kan nås, så kan man kun kommunisere internt på samme nettverk/subnett.

c. Hva er fordelene med å bruke en lagdelt modell som OSI-modellen eller TCP/IP-modellen?

Vi kan dele opp nettverksoperasjonene i moduler. Dette gjør at protokoller som opererer på et spesifikt lag har et forhåndsdefinert utvalg av informasjon de kan bruke og påvirke, samt et definert interface for å kommunisere mot lagene over eller under. Denne modulariteten gjør at man kan endre eller forbedre en modul uten å påvirke de andre, og man har muligheten til å bruke enheter fra en hvilken som helst produsent.

d. Forklar forskjellen på full-duplex og half-duplex. På hvilke transmisjonsmedier brukes disse i lokale nettverk?

Full-duplex: begge enhetene på en link kan sende og motta trafikk samtidig. Brukes på kablede nettverk, eksempelvis Ethernet.

Half-duplex: bare en av enhetene kan sende om gangen (eksempel: walkietalkie). Brukes på WiFi, eller eldre kablede nettverk.

e. Gjør rede for behovsforskjellene mellom industrielle og kommersielle/(Internett) nettverk

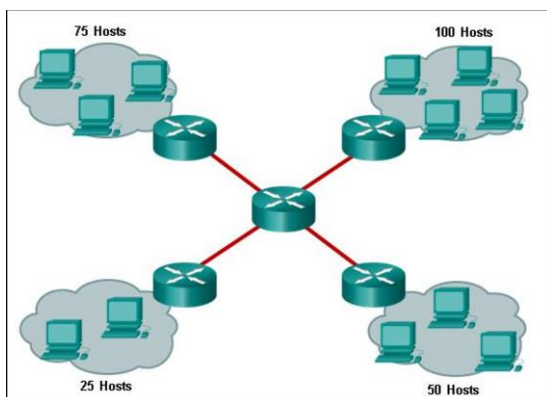
Industrielle nettverk krever ofte kabler, plugger og enheter som tåler mer (fukt, støv, osv). I kommersielle nettverk sendes trafikk som standard etter best effort prinsippet, og kommer frem på litt tilfeldige tidspunkter avhengig av hvor mye trafikk som går på nettverket og andre faktorer. I industrielle nettverk er trafikken mer deterministisk, og enhetene vet når de skal sende og motta trafikk. Man er

avhengig av at trafikk kommer i tide, og at den er pålitelig/intakt. Hvis ikke, kan det oppstå feil i produksjonsprosessen og medføre store problemer.

f. Hva er forskjellen mellom MAC- og IP-adresser? Hvorfor trenger vi begge?

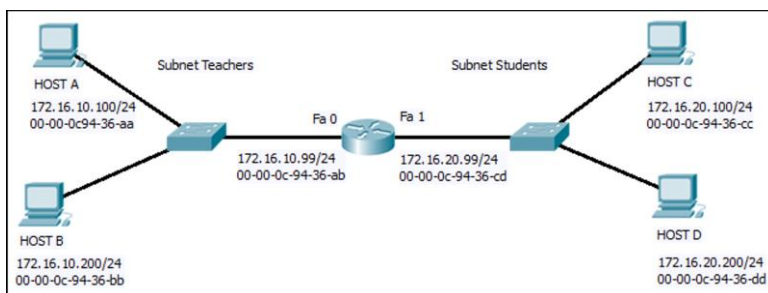
- MAC-adresser er låst til hardware, mens IP-adresser er logisk tildelt.
- MAC-adresser er i hovedsak tilfeldige (med unntak av den første biten, som er avhengig av produsent), IP-adresser kan vi gruppere i subnett
- MAC-adresser er unike, IP-adresser kan brukes om igjen flere steder (på private nettverk)
- Vi trenger begge typene, da de har forskjellige bruksområder. IP-adressene kan rutes globalt eller i private subnett, mens MAC-adresser kun er gyldige på den lokale linken.

g. Et firma bruker adresseblokken 128.107.0.0/16 i sitt nettverk. Det skal deles opp i subnett (se figur nedenfor). Hvilken subnettmasker gir det maksimale antallet subnett samtidig som det dekker behovet for antall hosts?



Det største nettverket trenger 100 hosts. Da bør man velge den masken som gir 100 hosts eller flere, men samtidig gir det maksimale antall subnett. Da ender man på 255.255.255.128, som gir $2^7 - 2 = 128 - 2 = 126$ hosts.

h. Se figur nedenfor. Host B i «Subnet Teachers» sender en pakke til Host D i «Subnet Students». Hvilke lag 2 og lag 3 adresser inneholder PDUen(e) som sendes fra Host B til ruteren?



Siden spørsmålet ber om adressene i PDUen(e) fra Host B til ruteren, er det MAC-adressen til Host B som er kilden og MAC-adressen til ruterens sitt interface Fa0 som er destinasjonen på lag 2. På lag 3 er det IP-adressen til Host B som er kilden, og IP-adressen til Host D som er destinasjonen. Eksplisitt: Lag 2: • Source MAC: 00-00-0c-94-36-bb (Host B) • Destination MAC: 00-00-0c-94-36-ab (Ruterens, Fa 0) Lag 3: • Source IP: 172.16.10.200 (Host B) • Destination IP: 172.16.20.200 (Host D)

2021 Vår kont

Oppgave 3 (bokmål)

a. Forklart kort hva du trenger for å:

i. Kommunisere med en enhet på ditt lokale nettverk

For å kommunisere lokalt må man ha tilgang til et fungerende media som for eksempel en kablet link, eller en trådløs forbindelse. Deretter må man vite MAC-adressen til motparten for å kunne sende trafikk dit. Dersom man har IP-adressen, kan man etterspørre MAC-adressen over nettverket eller omvendt.

ii. Kommunisere med en enhet på et annet nettverk

For å kommunisere eksternt er man avhengig av å vite IP-adressen man skal sende til, samt ha en fungerende default gateway på lag 3 man kan sende trafikk mot. Vet man ikke adressen til mottaker, kan den eventuelt slås opp hos en DNS-server.

b. Forklar forskjellen på båndbredde, throughput og goodput. > Båndbredde er den maksimale teoretiske hastigheten på et gitt medium med en gitt protokoll eller teknologi. Eksempelvis Ethernet med kobberkabel og en Gigabit link, da er båndbredden 1 Gbps.

Throughput er den faktiske overføringsraten, og er vanligvis lavere enn båndbredden. Den påvirkes av mengden trafikk, type trafikk, og antall hopp fra kilde til destinasjon.

Goodput er hvor mye nytte data som er overført over en gitt tid, det vil si throughput minus trafikk overhead (etablere tilkoblinger, metadata, enkapsulering, retransmisjoner, osv.). Goodput er alltid lavere enn throughput.

c. Forklar hvorfor vi har åpne standarder, og hva som er fordelene med dette.

Vi har åpne standarder for å sikre interoperabilitet, konkurranse og innovasjon. Vi unngår også monopoler. Dette gjør at vi kan kjøpe en smarttelefon fra en hvilken som helst produsent, og så lenge de følger standardene, så vil den kunne bruke både mobilnett og WiFi uavhengig av hvem som har produsert WiFi-

ruteren eller radioene til mobilnettet. Små produsenter kan lettere komme seg ut på markedet, da de ikke blir låst ute så lenge de har åpne standarder å følge.

d. Forklar hvorfor vi segmenterer IP-pakker.

Dette er litt det samme som fletting i biltrafikken. Hvis man ikke gjorde dette, kan det bli mye venting for å komme til. Store filer ville tatt opp hele linken i relativt lang tid. Hvis en del av infrastrukturen gikk ned under en stor filoverføring, måtte man ha begynt på nytt. Segmentering forhindrer dette ved å la oss multiplekse trafikken, og alle segmentene trenger ikke å reise samme vei. På denne måten kan vi utnytte flere linker til samme mål. Hvis et segment skulle gå tapt, trenger man bare sende det tapte segmentet på nytt.

e. Hva er det første en switch gjør når den mottar en «frame»? Beskriv prosessen fram til switchen videresender denne.

Den sjekker source MAC adresse opp mot sin egen tabell. Hvis den ikke allerede ligger i tabellen, legges den til sammen med portnummeret den kom inn på. Hvis den eksisterer, oppdateres refresh timeren for den adressen (timer som sletter adressen etter X sekunder, typisk 5 min). Hvis adressen har byttet port, behandles det som en ny adresse og den gamle erstattes.

Deretter sjekkes destinasjonsadressen. Hvis denne eksisterer i tabellen, sendes framen ut på tilhørende port. Hvis ikke, floodes den ut på alle porter med unntak av porten den kom inn på.

f. Hva er et broadcast domene? Forklar hvorfor vi prøver å begrense størrelsen på disse.

Et broadcast domene er hvor langt man kan nå med broadcast trafikk. Da broadcast trafikk ikke videresendes av rutere, er dette typisk begrenset til det lokale nettverket med tilhørende switcher og enheter (PCer, mobiler, andre tilkoblede enheter).

Grunnen til at man vil begrense størrelsen på broadcast domener er at broadcast trafikk må behandles av alle enhetene som mottar den. Dette vil si at hver enhet må åpne og eventuelt videresende broadcast meldingen, samt sjekke om denne er relevant for seg. I mange tilfeller er den ikke det. Dette gjør at jo flere enheter man har i samme broadcast domene, jo mer unødvendig trafikk får man. Dette belaster både nettverket og enhetene. Nettverket går tregere, enhetene må bruke tid og ressurser på å lese meldingene, og enheter på batteri går forttere tom.

g. Dersom Host A sender en IP-pakke til Host B, hva blir destinasjonsadressene (lag 2 og 3) når pakken forlater Host A? Endres disse underveis? Skriv ned og begrunn kort.

Destinasjonsadressene blir på lag 2 MAC-adressen til neste hopp. Dette er ruterens R2 med MAC BB:BB:BB:BB:BB:BB.

På lag 3 blir det endepunktadressen, det vil si Host B sin IP-adresse:
172.168.11.88

Lag 2 adressen endres ved hvert hopp, og vil hele tiden bruke MAC-adressen til neste enhet.

Lag 3 adressen endres ikke underveis.

2022 Høst

- a. **Hva er rollen til "default gateway" (DGW) i et nettverk? Altså, hvordan brukes "default gateway" av enheter i et nettverk?**

Det er en nettverksenhet, for eksempel en ruter eller L3 switch, som kan rute trafikk til andre nettverk. Den trengs for å sende trafikk ut av det lokale nettverket. Hvis denne ikke finnes eller ikke kan nås, så kan man kun kommunisere internt på samme nettverk/subnett.

- b. **Beskriv fordeler og ulemper med trådløs kommunikasjon.**

Trådløs kommunikasjon gir brukerne økt mobilitet og fleksibilitet i og med at man ikke er låst til en bestemt plassering. Man er dog begrenset av rekkevidden på sender og mottaker, og kan bli påvirket av støy/interferens. I verste fall kan kommunikasjonen da bli upålitelig eller i praksis ubrukelig. Samtidig er trådløs kommunikasjon ofte avhengig av at frekvensen man sender på er ledig, ellers kan det oppstå kollisjoner. Da må man sende på nytt. Man må derfor ta hensyn til omgivelsene når man planlegger bruk av trådløs kommunikasjon, samt antall brukere i samme område. Trådløs kommunikasjon er i mange tilfeller half-duplex, slik at jo flere brukere i området, jo tregere blir systemet.

- c. **Rams opp noen spesielle krav som stilles til industrielle nettverk.**

Industrielle nettverk krever ofte kabler, plugger og enheter som tåler mer (fukt, støv, osv). I kommersielle nettverk sendes trafikk som standard etter best effort prinsippet, og kommer frem på litt tilfeldige tidspunkter avhengig av hvor mye

trafikk som går på nettverket og andre faktorer. I industrielle nettverk er trafikken mer deterministisk, og enhetene vet når de skal sende og motta trafikk. Man er avhengig av at trafikk kommer i tide, og at den er pålitelig/intakt. Hvis ikke, kan det oppstå feil i produksjonsprosessen og medføre store problemer.

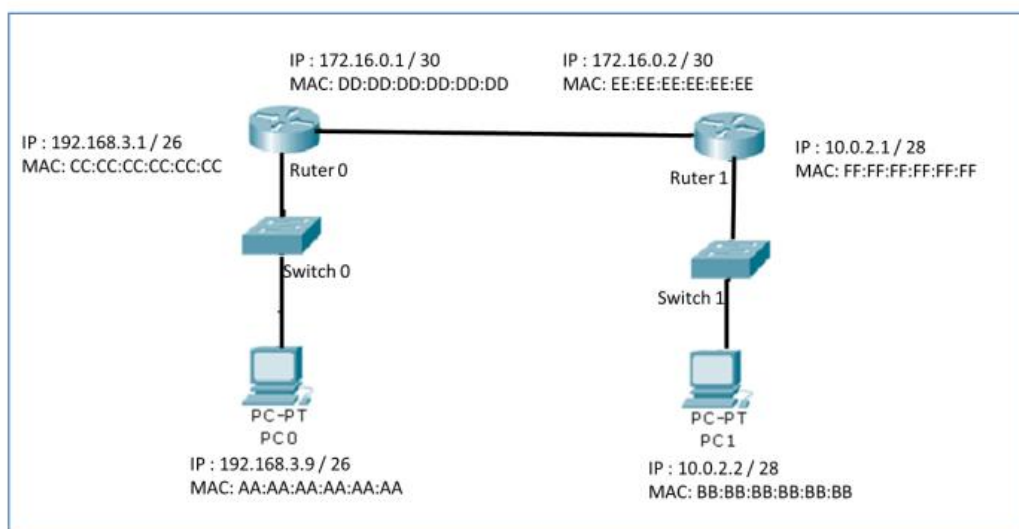
d. **Hva er forskjellen på Broadcast-kommunikasjon, Unicast kommunikasjon og Multicastkommunikasjon?**

Unicast: informasjon overføres til en spesifikk enhet. Eksempler: filoverføring, nedlasting av webside, sende melding.

Multicast: informasjon overføres til en eller flere mottakere. Eksempler: diverse rutingprotokoller, IPTV, andre livestreams som radio eller video.

Broadcast: informasjon overføres til alle enheter på det lokale nettverket. Eksempler: rutingprotokoller, DHCP, ARP

Studer figuren under.



PC0 sender en IP-pakke til PC1.

- e. Lag en tabell som vist under.
Skriv inn avsender- og destinasjonsadresser på meldingen etter hvert som den sendes fra PC0 til Ruter0, fra Ruter0 til Ruter1, og fra Ruter1 til PC1.
Altså: Du skal få frem hvordan MAC og IP adressen endres etter hvert som meldingen traverserer nettverket.

Avsender-enhet (navn)	Mottaker-enhet (navn)	Source MAC	Destination MAC	Source IP	Destination IP
PC0	Ruter0	AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC	192.168.3.9	10.0.2.2
Ruter0	Ruter1	DD:DD:DD:DD:DD:DD	EE:EE:EE:EE:EE:EE	192.168.3.9	10.0.2.2
Ruter1	PC1	FF:FF:FF:FF:FF:FF	BB:BB:BB:BB:BB:BB	192.168.3.9	10.0.2.2

2022 Vår

- a) **(3%) Beskriv fordeler og ulemper med trådløs kommunikasjon.**

Trådløs kommunikasjon gir brukerne økt mobilitet og fleksibilitet i og med at man ikke er låst til en bestemt plassering. I tillegg slipper man å tenke på å ta med seg riktig eller lang nok kabel. Man er dog begrenset av rekkevidden på sender og mottaker, og kan bli påvirket av støy/interferens. I verste fall kan kommunikasjonen da bli upålitelig eller i praksis ubrukelig. Samtidig er trådløs kommunikasjon ofte avhengig av at frekvensen man sender på er ledig, ellers kan det oppstå kollisjoner. Da må man sende på nytt. Man må derfor ta hensyn til omgivelsene når man planlegger bruk av trådløs kommunikasjon, samt antall brukere i samme område. Trådløs kommunikasjon er i mange tilfeller half-duplex, slik at jo flere brukere i området, jo tregere blir systemet.

- b) **(3%) Hvorfor segmenterer vi data når vi eksempelvis skal sende en stor fil over internett? Hva ville skjedd dersom vi ikke segmenterte filen?**

Det er to fordeler med segmentering: økt hastighet og effektivitet. Dette da man kan sende større mengder data uten å binde opp en hel link (ved hjelp av multipleksing), samtidig som man kan unngå å sende hele filen på nytt hvis et segment skulle mangle. Da sender man bare det spesifikke segmentet om igjen.

- c) **(3%) Beskriv formålet med lag 2 i OSI-modellen (data link). Forklar hva som foregår på dette nivået når trafikk skal sendes over et medium.**

Formålet med lag 2 er å innkapsle pakken i riktig format for aktuelt media, eksempelvis Ethernet. Dette lar deg sende trafikk fra lagene over uavhengig av media/link type. I tillegg håndterer dette laget kommunikasjon mellom lag 2 hardware og lag 3 software, oppdeling/struktur internt i aktuell frame, adressering på lag 2 og feildeteksjon. På hvert hopp skjer følgende når det gjelder lag 2:

1. Enheten mottar en frame fra media
2. Fjerner innkapsling fra frame
3. Legger til ny innkapsling før eventuell videresending, tilpasset utgående link
4. Sender frame ut på aktuell link

- d) **(4%) Forklar hva en standard er for noe. Hva er fordelene med åpne standarder?**

En standard er et dokument som angir hvordan noe skal lages eller fungere. Dette kan for eksempel beskrive målene på bildekk, inngangsdører eller hva det skal være. Innenfor nettverk brukes dette gjerne til å beskrive protokoller som benyttes for å få tilgang til tjenester, kommunisere osv. Dette lar deg for eksempel koble til WLAN, laste ned en nettside og lese denne uavhengig av hvem som har produsert enheten din eller hvilket operativsystem/nettleser du bruker. Åpne standarder gir en del fordeler når det gjelder interoperabilitet, konkurranse og innovasjon. Uten åpne standarder ville vi endt opp med en del monopol og utelåsing av mindre aktører, som ville motvirket innovasjon.

- e) **(7%) Forklar hva som skjer når PC1 forsøker å laste ned nettsiden «NRK.no» ut ifra figur 4. Få med hvordan den gjør bruk av lokal DNS og default gateway (DGW).**

1. DNS request til DNS server 192.168.1.254 for NRK.no

2. Mottar DNS reply med 10.0.0.2
3. Sender ARP request for å få tak i MAC-adressen til DGW 192.168.1.1
4. Sender HTTP request til NRK.no på 10.0.0.2, via DGW sin MAC-adresse på L2
5. DGW bruker evt NAT og videresender http request til NRK.no via sin 200.0.0.2 adresse
6. NRK mottar denne og sender svaret til 200.0.0.2
7. «Home» videresender http reply til PC1

2023 Vår

Oppgave 3 (bokmål)

a) Hva trenger du på din enhet for å få tilgang til Internett? Forklar ved hjelp av nettverksbegreper, og få med hvilken funksjon de forskjellige tingene har. (Anta at du har strøm.)

b) Forklar hva interferens er. Få med hvordan dette påvirker Ethernet, fiber og trådløst nett. Hva kan man gjøre for å forhindre interferens på disse forskjellige transmisjonsmediene?

c) Forklar hvordan et broadcast-domene påvirker ytelsen på nettverket, og mulige konsekvenser av dette. Hvordan løses dette i IPv4- og IPv6- nettverk?

d) Se Figur 6. Switchene Øst og Vest sine porter er merket. PC3 sender et ping til hver av de andre PC-ene i rekkefølgen 0-1-2. Hvis man antar at switchene sine adressetabeller er tomme før pingene blir sendt, hvilke MAC-adresser vil Øst ha i sin tabell under port F0/1 i etterkant? Forklar.

Selvfølgelig, her er det fint formulert:

e) Se Figur 7. Her observerer vi to nettverk, Ansatt (blå) og Student (rosa). Ansatt-nettverket krever minst 100 brukere, mens Student-nettverket trenger minst 40. Til tross for at en administrator har konfigurert begge nettverkene korrekt, har vedkommende glemt å dokumentere dem.

Hva er nettverksadressen og prefix til de to nettverkene? Vi antar at tilgjengelig plass ikke blir kastet bort, og hele 192.168.1.0/24-subnettet er tilgjengelig.

Forklar kort hvordan du kommer frem til svaret.

Svar:

a) For å få tilgang til Internett, trenger du følgende:

- Tilgang til nettverket via en eller annen tilkobling, eksempelvis Ethernet/WLAN/5G osv.
- En IP-adresse på din lokale enhet, som kan benyttes på aktiv tilkobling. Dette for å kunne motta svar på meldinger.
- Default gateway for å kunne kommunisere med andre nettverk enn ditt lokale, og eventuelt benytte NAT.
- DNS-server. Kan være samme enhet som default gateway, men er nødvendig for å oversette domener til IP-adresser. Uten denne vil man ikke kunne åpne nettsider eller bruke tjenester uten å ha IP-adressene på forhånd, og lite vil fungere.

b) Interferens er en ytre påvirkning på ditt signal. Dette skaper typisk forstyrrelser, slik at signalet blir svekket, endret eller uleselig.

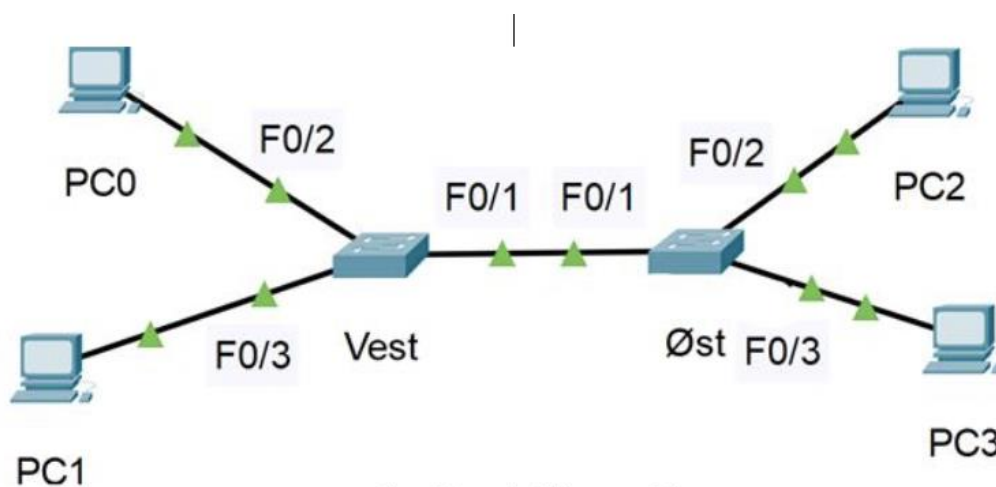
- Ethernet kan bli påvirket av elektromagnetisk interferens i nærheten av kablen. Dette kan føre til feil på signalet, slik at pakker må sendes på nytt. I verste fall kan det bli totalt uleselig, men da skal det ganske kraftig interferens til. I et vanlig hjem er det lite sannsynlig at man opplever alt for mye interferens på Ethernet, men det kan skje i kommersielle/industrielle forhold. For å forhindre dette kan man legge kablene med god avstand fra eventuelle støykilder, eller benytte skjermede kabler.
- Fiber er immun mot elektromagnetisk interferens, da det ikke benytter signalering som lar seg påvirke av dette. Fiberkablene er laget av glassfiber, og overfører lys. Med mindre det er skade på kablen eller utstyret, så blir det ikke interferens.
- Trådløse nettverk er veldig utsatt for interferens fra andre nærliggende nettverk som sender på samme frekvens/kanal, men også fra generell radiostøy. Dette kan føre til alt fra retransmissions/delay til totalt tap av signal, avhengig av styrke og avstand på støysignalet. Også materiale i bygget, vann og speil kan forårsake signaltap. For å forhindre dette bør man undersøke forholdene lokalt, og planlegge hvilke kanaler man skal benytte for å unngå overlapp med nærliggende trådløse nettverk. Ved for dårlig signal/dekning må man kanskje sette opp flere access points.

c) Et broadcast-domene er begrenset til det lokale subnett. Broadcast meldinger vil ikke videresendes ut av subnett, og passerer typisk ikke rutere. Switcher som mottar broadcast meldinger vil videresende disse ut alle porter, med unntak av porten meldingen kom fra. Da broadcast meldinger går til alle, fører det til mye trafikk på

nettverket. Typisk skaper dette mye trafikk som alle må lese, selv om det bare er relevant for noen få. Dette koster både tid, båndbredde og CPU-kraft. Mengden broadcast meldinger øker kraftig jo flere enheter man får på nettverket, og det er derfor hensiktsmessig å begrense antall enheter per subnett. Hvis det blir for mange broadcast meldinger, kan hele nettverket gå ned eller bli ubrukelig.

- IPv4: Løses ved å dele opp i mindre subnett, dvs segmentere nettverket.

- IPv6: Lurespørsmål. IPv6 har ikke broadcast, med mindre man jukser seg til det med all-nodes multicast adressen. IPv6 har dog noe som heter Anycast, hvor man alltid når den nærmeste tilbyderer av en tjeneste. Skulle denne gå ned, så kan man prøve å nå en av de som ligger lenger vekk. Dette gir økt redundans og oppetid. Typisk bruksområde er DNS.



Figur 6 Nettverket i deloppgave 3 d)

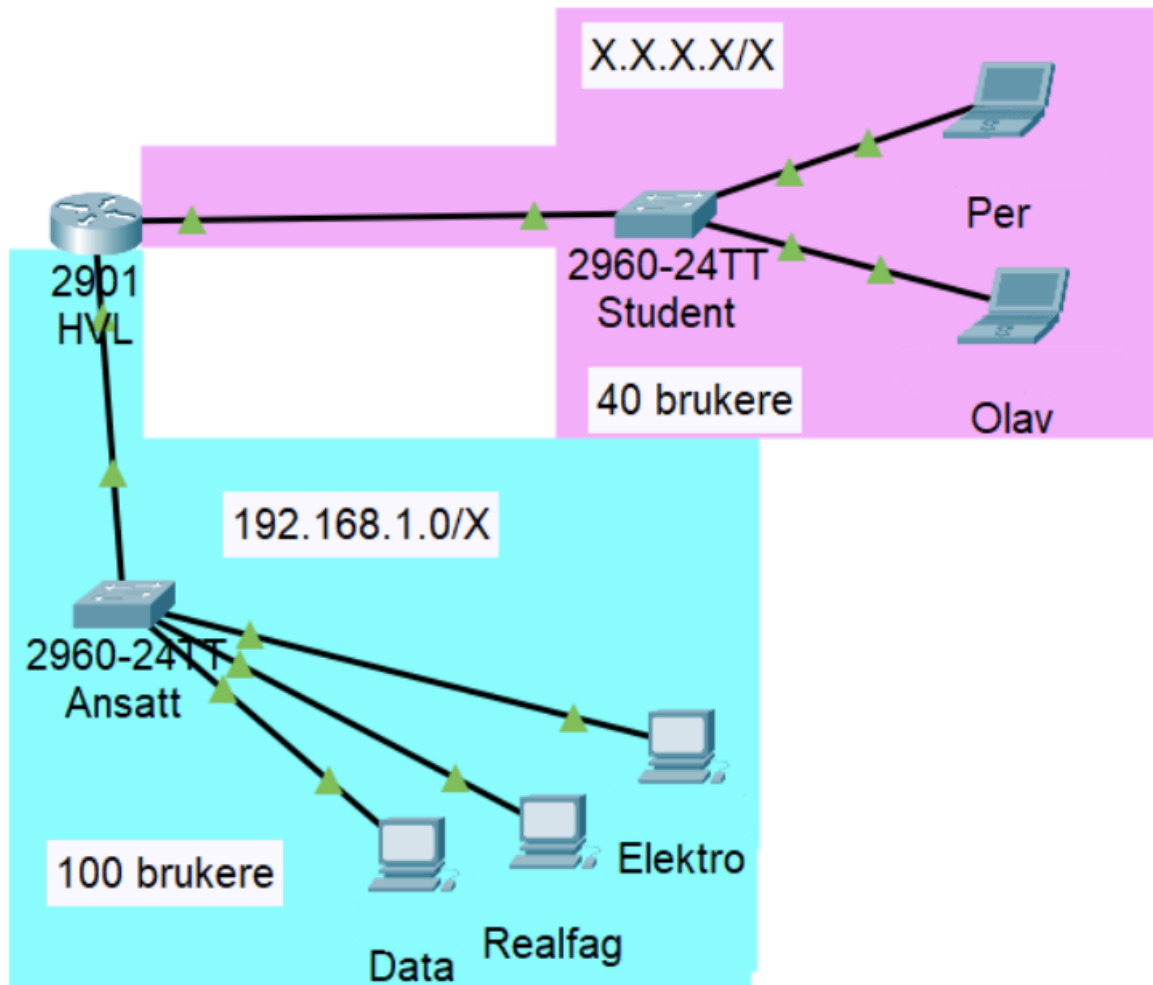
d) Switchene vil notere ned alle MAC-adresser på innkommende meldinger, og merke dem med port.

- Dette vil si at Øst noterer ned MAC-adressen til PC3 på port F0/3 når den sender ut ping.

- Når den får svarene fra PC0 og PC1, kommer disse INN på port F0/1. MAC-adressene på disse PCene blir da notert ned og merket med denne porten (F0/1).

- Når svaret fra PC2 kommer, noteres MAC-adressen ned og merkes med port F0/2.

- Ergo, svaret på oppgaven er at Øst vil ha MAC-adressene til PC0 og PC1 i sin tabell under port F0/1.



Figur 7 Nettverkene i deloppgave 3e)

e) Se Figur 7.

For å unngå å kaste bort plass og optimalt utnytte subnetting, bruker vi Variable Length Subnet Masking (VLSM). Her er svaret til oppgave e) med VLSM:

a) Vi starter med det største nettverket, Ansatt, som trenger 100 brukere. Et /25 subnet gir 126 brukere, så vi bruker dette. Nettverksadressen blir da 192.168.1.0/25, med subnetmasken 255.255.255.128 (fordi bitvis utregning av 1000 0000 gir 128).

b) Student-nettverket trenger bare 40 brukere. Et /26 subnet gir 62 brukere, så vi bruker dette. Vi må ta hensyn til hvor det forrige subnettet slutter. Ved å sette alle host bits i Ansatt-subnettet til 1 (0111 1111), ser vi at det slutter på 192.168.1.127. Vi kan da begynne Student-subnettet på 192.168.1.128 med prefix /26, eller subnetmasken 255.255.255.192 (fordi bitvis utregning av 1100 0000 gir 192).

Dette sikrer at vi ikke kaster bort unødvendig plass og optimalt utnytter tilgjengelige IP-adresser.