Gruppetime 7

Repetisjon: Transportlaget

- Ansvar for pålitelig overføring av data fra kilden til destinasjonen
  - Uavhengig av de underliggende nettverkstypene
- Benytter seg av protokoller som Transmission Control Protocol (TCP) og User Datagram Protocol (UDP)
  - Sikrer at data overføres effektivt
- Håndterer også oppdeling og reassembling av data i mindre enheter (segmenter eller datagrammer), for å sikre at informasjonen blir overført effektivt over nettverk

- *TCP: Pålitelig overføring, ordnet mottak, raskt*
- *UDP: Upålitelig overføring*

IP-adresser, subnettadresser og nettverksmasker

IP-adresser:

- IPv4 bruker 32 biter til å representere en IP-adresse
- IP-adressen er delt i fire grupper, hver med 8 biter, kalt oktetter (0-255)

Subnettadresse og nettverksmaske:

- En nettverksmaske består av en serie med 1-biter etterfulgt av 0-biter → indikerer hvilke deler av IP-adressen som tilhører nettverket og hvilke som tilhører vertsadressen
- Subnettadressen er den første IP-adressen i hvert subnett og representerer nettverket

Eksempel på subnetting

- La oss ta en IP-adresse og nettverksmaske, og finne subnettadressen
- IP-adresse: 192.168.1.150
- Nettverksmaske: 255.255.255.0 (oftest skrevet som /24, da det er 24 sammenhengende 1-biter)

1. Konverterer nettverksmasken til binær:

   255.255.255.0 = 11111111.11111111.11111111.00000000

2. Anvender nettverksmasken på IP-adressen

IP-adresse: 11000000.10101000.00000001.10010110

Nettverksmaske: 11111111.11111111.11111111.00000000

Subnettadresse: 11000000.10101000.00000001.00000000 (192.168.1.0)

* Subnettadressen i desimalt format er 192.168.1.0, som er den første adressen i dette subnettet

* Benytter AND

Kringkastingsadresse

- IPv4-nettverk med en nettverksmaske på 255.255.255.0 (eller /24 i CIDR-ntasjon), er den kringkastingsadressen satt til alle 1-biter i vertsadressen
- Eksempel:
  - IP-adresse: 192.168.1.0 (subnettet for nettverket)
  - Nettverksmaske: 255.255.255.0
  - Kringkastingsadresse:

    192.168.1.255

- For alle IP-adresser i dette nettverket, vil en kringkastingsadresse på 192.168.1.255 sende data til alle enheter i samme nettverk

Network Address Translation (NAT)

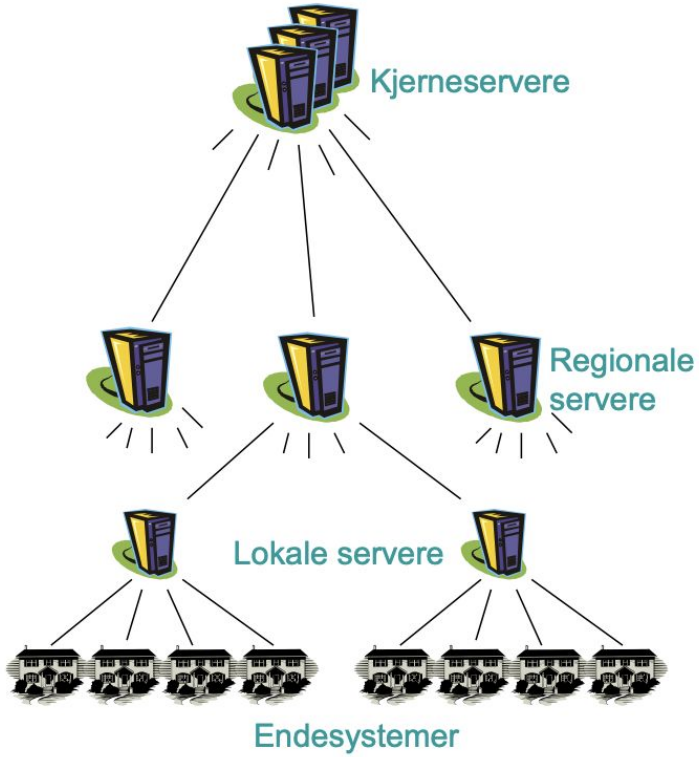
- Network Address Translation
- Brukes i nettverk for å tillate flere enheter i et lokalt nettverk å dele en felles offentlig IP-adresse
  - For tilgang til internett
- Fungerer som en mellommann mellom det private lokale nettverket og det offentlige internett
- Bidrar til sikkerhet ved å skjule interne IP-adresser fra det offentlige internettet → gir bedre bruk av tilgjengelige offentlige IP-adresser

Hvordan bruker man NAT?

- Når flere enheter i et hjem eller kontor deler en enkelt utgående IP-adresse
- Flere enheter? NAT tildeler midlertidig interne IP-adresser til hver enhet
- IP-adressene blir oversatt til den ene offentlige IP-adressen når data skal sendes ut på internett
    - Da kan flere enheter bruke internett med bare én offisiell IP-adresse

Content Delivery Network (CDN)

- Et distribuert nettverk av servere som er plassert geografisk spredt over ulike steder
  - Levere innhold på en rask og effektiv måte til brukere over hele verden
- Formål? nyttig for f.eks. store nettsider for å håndtere stor trafikkbelastning og optimalisere brukeropplevelsen
- Bidrar også ved å beskytte nettsteder mot angrep ved å spre belastningen over flere servere



Peer-to-peer (P2P)

- Desentralisert nettverksstruktur der deltakerne (peers) fungerer som både leverandør og mottaker av ressurser
- Deltakerne deler ressursene direkte med hverandre
  - Uten behov for en sentralisert tjeneste eller server
- Hver deltaker har lik verdi og ansvar:
  - Effektiv deling
  - Effektiv distribusjon av data uten å legge for mye belastning på en enkelt kilde eller server
- Ofte brukt for deling av filer, videostreaming, samt andre destribuerte tjenester

P2P: Fordeler og ulemper

- Fordeler:
  - Inkluderer høy skalerbarhet og robusthet
  - Effektiv utnyttelse av deltakernes ressurser
- Ulemper
  - Kan inkludere utfordringer med sikkerhet og personvern

Domain Name System (DNS)

- Et system som brukes på internett for å oversette let huskbare domenenavn til numeriske IP-adresser som datamaskiner kan forstå
- Avgjørende for internettets funksjon:
  - Gjør det mulig for oss mennesker å bruke enkle og meningsfulle domenenavn istedenfor å måtte huske komplekse IP-adresser
  - Forenkler kommunikasjonen og brukeropplevelsen på nett

DNS: Eksempel

- Du skriver inn en nettsideadresse i nettleseren din
- Datamaskinen sender en forespørsel til en DNS-server
- DNS-serveren søker etter den tilhørende IP-adressen knyttet til det gitte domenenavnet
- Hvis DNS-serveren finner den, returnerer den IP-adressen til datamaskinen din
- Slik kan nettleseren koble til den aktuelle nettsiden

Dynamic Host Configuration Protocol (DHCP)

- En nettverksprotokoll som brukes til å tildele IP-adresser og konfigurasjonsparametere automatisk til enheter i et nettverk når de kobler seg til
- Hovedfunksjon:
  - Forenkle administrasjonen av IP-adresser i et nettverk
  - Når enheten, for eksempel en datamaskin eller mobiltelefon, blir tilkoblet nettverk, sender den en forespørsel til DHCP-serveren for å be om en IP-adresse og andre nettverkskonfigurasjonsdetaljer
  - DHCP-serveren svarer med tildeling av en ledig IP-adresse + andre nødvendige instillinger som subnettmaske, standard gateway og DNS-server

DHCP forts.

- Ved å bruke DHCP automatiseres og koordineres tildelingen av IP-adresser → gjør det enklere å administrere og oppdatere nettverkskonfigurasjoner
- Bidrar til å unngå konflikter med IP-adresser, sikre effektiv bruk av tilgjengelige adresser og forenkle nettverksvedlikehold

Kryptografi og kryptering

- Sikre kommunikasjon og informasjon ved bruk av teknikker for å omforme informasjon til uleselig format ved hjelp av matematiske algoritmer
- Kan bare dekrypteres av de som har riktig nøkkel
- Rolle?
  - Sikker kommunikasjon på internett
  - Beskyttelse av personvern
  - Autentisering av brukere og dataintegritet
- Kryptering er selve prosessen med å bruke en krypteringsalgoritme (nøkkel) for å omforme klar tekst til kryptert tekst
- Dekryptering - kryptert tekst blir gjort om tilbake til kalr tekst ved hjelp ab riktig nøkkel

Symmetrisk vs asymmetrisk

Symmetrisk:

- Både bruker og mottaker bruker samme nøkkel for både kryptering og dekryptering

- Eksempel:
  - Tenk på en nøkkel til et låst skap. Den samme nøkkelen brukes både for å låse (kryptere) og låse opp (dekryptere) skapet

Asymmetrisk:

- Her brukes to forskjellige nøkler (begge matematiske):
  - En offentlig nøkkel for kryptering og
  - en privat for dekryptering

- Eksempel:
  - Forestill deg en postkasse med to nøkkelhull - en offentlig nøkkel kan låse opp postkassen, ens en annen privat nøkkel kan brukes til å låse den opp igjen.
  - Alle kan bruke den offentlige nøkkelen til å legge inn post, men bare eieren kan låse den opp og hente ut innholdet