OSI modellen
TCP/IP protokol arkitekturen
IP adresser
DHCP
DNS
Fysiske netværks enheder

Operativsystemer og netværk

Lektion 4

OSI modellen

Vi ser på modellen endnu en gang og vender den på hovedet

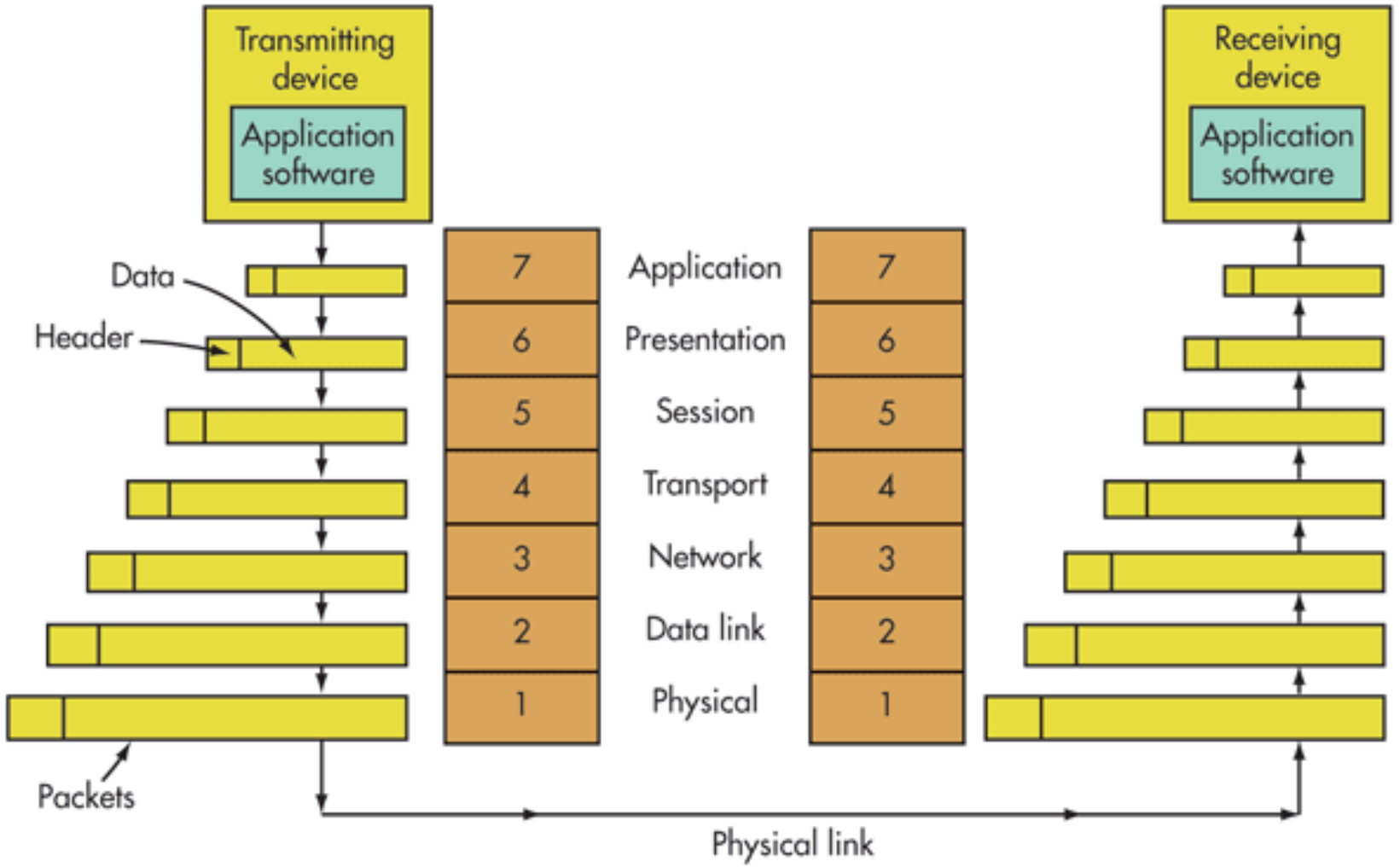
OSI modellen

- OSI, Open Systems Interconnect Reference Model.
  - Man kan læse den fra begge retninger, derfor også ISO.
- En **protokol** er det regelsæt, der afslutter punkter i et netværk, når de kommunikerer. Protokoller specificerer interaktioner mellem de kommunikerende enheder.
- Protokoller findes på flere niveauer i en forbindelse.
  - For eksempel er der protokoller for dataudveksling på enhedens hardware niveau og protokoller for dataudveksling på programniveau.
- I OSI modellen er der en eller flere protokoller på hvert lag i netværks udvekslingen som begge ender af udvekslingen skal anerkende og observere.

OSI modellen

- Alle de nødvendige og ønskede operationer, som kræves, er grupperet sammen i en logisk rækkefølge på hvert af lagene.
- Hvert lag er ansvarlig for specifikke funktioner.
- Hvert lag i OSI moddellen kan kun benytte det underliggende lags funktioner og kun tilbyder funktioner til laget over.
  - Det vil sige at lag 5 ikke bare benytter lag 2 men hele stakken nedad.
- Et system, der implementerer en sådan protokolopførsel bestående af en serie af disse lag, kaldes en **'protokolstak'** eller bare **'stak'**

OSI modellen



OSI modellen

OSI modellen – Lag 1: Det fysiske lag

- Det fysiske lag definerer alle elektriske og fysiske rammer for netværks-elementerne
- Dette lag dækker stik-type, spændinger og kabel-specificationerne. Netværks-hubs, repeatere, netværks-kort og Host Bus Adaptere (HBA'er brugt i Storage Area Networks) er fysisk-lags enheder
- De mest fremtrædende funktioner af laget er:
  - Oprettelse og afslutning af elektrisk forbindelse til overførsels-mediet
  - Deltager i effektivisering af kommunikation mellem flere brugere.
    F.eks. contention ("vente på stilhed, før man blander sig") og flow-styring
- Modulering eller oversættelse mellem repræsentationen af digitale data til tilsluttet udstyr og tilsvarende signaler sendt via kommunikations kanalen. Det betyder at de skal omdannes så de kan sendes v.h.a. enten kabel (som kobber eller fiber) eller radio
- I dette lag findes SCSI "busser" og diverse fysisk definerede Ethernet standarder; Ethernet indeholder både dette lag og "data link laget" (lag 2). Det samme gælder andre lokale netværks typer, som Token ring, FDDI og Wireless LAN

OSI modellen

OSI modellen – Lag 2: Data Link-laget

- Layer 2 operationer pakke og udpakke data i frames.
- Data Link-laget giver mulighed for at overføre data mellem netværks-moduler og finde, muligvis rette, fejl der måtte optræde i det fysiske lag
- Adresserings-metoden er fysisk, dvs. MAC-adressen, der i de fleste tilfælde er "hard-coded" inde i netkortet
  - Nogle netværks-kort understøtter at administratoren specificerer en anden MAC-adresse, men som regel er det ikke muligt at ændre den.
- Adresseringen er ikke hierakisk opdelt. Det bedst kendte eksempel på dette lag er Ethernet.
- I dette lag arbejder Netværksbroer og Switche.

OSI modellen

OSI modellen – Lag 3: Netværkslaget

- Netværkslaget tilbyder de rutiner der skal til, for at sende en variabel størrelse datablok, fra kilde til slut, via et eller flere netværk.
- Dette lag holder også styr på QoS som "Transportlaget" bygger på.
- Netværkslaget udfører routing-funktioner (sender pakkerne til deres rette modtager), kan udføre ind- og udpakning og rapportere om leveringsfejl.
- Routere arbejder i dette lag og sender data gennem det udvidede netværk og gør internettet muligt.
- Dette er et logisk adresseringssystem, hvor værdier er valgt af netværksadministratoren.
- Adressesystemet er struktureret hierakisk. Det bedste eksempel på en layer 3 protokol er IP.

OSI modellen

OSI modellen – Lag 4: Transportlaget

- Dette lag giver kvalitet of Service (QoS) funktioner og sikrer fuldstændig levering af data.
- Integriteten af data er sikret på dette lag via fejlkorrektion og lignende funktioner via flowkontrol, "indpakning" / "ud-pakning" og fejlkontrol.
- Nogle protokoller er "state-" og "connection-" orienterede. Dette betyder at transportlaget holder styr på pakkerne og gensender dem der aldrig kom frem.
- Det bedst kendte eksempel på en transportlagsprotokol, er Transmission Control Protocol (TCP). Transportlaget er det lag der omdanner data til TCP pakker eller User Datagram Protocol (UDP), Stream Control Transmission Protocol (SCTP), osv. til pakker.

OSI modellen

Lag 5: Sessionslaget

- Lag 5 software håndterer godkendelse (authentication) og godkendelses funktioner.
- Det styrer også forbindelsen mellem de to kommunikerende enheder, etablerer en forbindelse, opretholder forbindelsen og afslutter den til sidst.
- Dette lag kontrollerer også at dataene leveres.

OSI modellen

Lag 6: Præsentationslaget

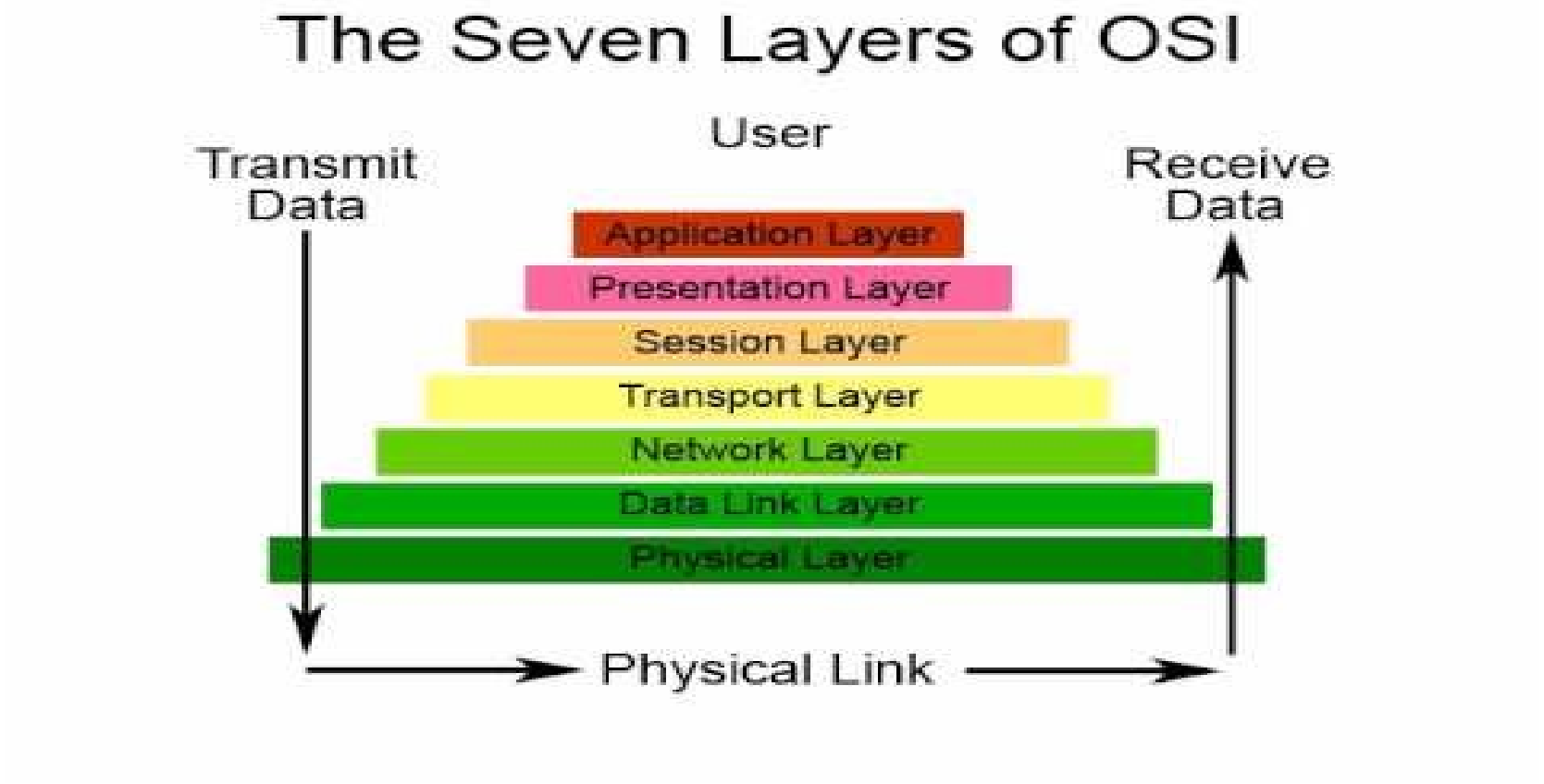
- Dette lag kontrollerer data, for at sikre, at den er kompatibelt medkommunikations-ressourcerne.
- Det sikrer kompatibilitet mellem dataformater på applikations niveau og de lavere niveauer.
- Det håndterer også ethvert behovfor dataformatering eller kodekonvertering, samt data kompression og kryptering.

OSI modellen

Lag 7: Applikationslaget

- Dette lag arbejder med software til at give kommunikationsfunktioner efter behov.
- Det kontrollerer tilgængeligheden af en kommunikations partner og ressourcerne til at støtte enhver dataoverførsel.
- Det virker også med end applikationer såsom domænenavn (DNS), filoverførselsprotokol (FTP), Hypertext Transfer Protocol (HTTP), Internet Message Access Protocol (IMAP), posthus protokollen (POP), Simple Mail Transfer Protocol (SMTP), Telenet, og terminal emulering.

OSI modellen



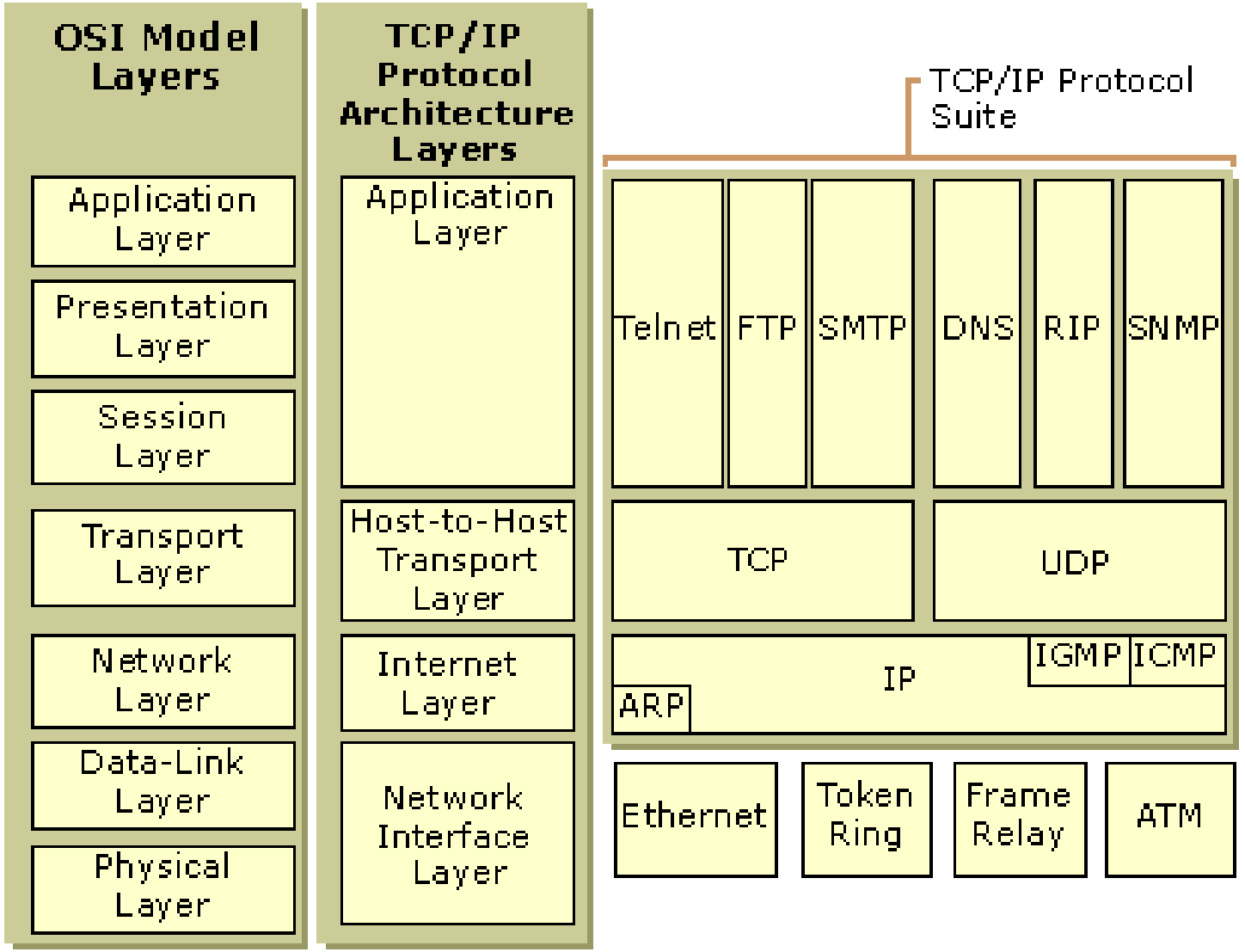
TCP/IP protokol arkitektur

DARPA modellen

TCP/IP

- TCP / IP-protokoller følger en fire-lags konceptuel model kendt som DARPA modellen, opkaldt efter det amerikanske regerings agentur, der oprindeligt udviklede TCP / IP.
- De fire lag i DARPA modellen er: Applikation, Transport, Internet og Netværkskort.
- Hvert lag i DARPA modellen svarer til et eller flere lag i syv lags Open Systems Interconnection (OSI) modellen.

TCP/IP


OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IP
IGMP
ICMP
ARP
Ethernet
Token Ring
Frame Relay
ATM

TCP/IP

- TCP / IP-protokoller følger en fire-lags konceptuel model kendt som DARPA modellen, opkaldt efter det amerikanske regerings agentur, der oprindeligt udviklede TCP / IP.
- De fire lag i DARPA modellen er: Applikation, Transport, Internet og Netværkskort.
- Hvert lag i DARPA modellen svarer til et eller flere lag i syv lags Open Systems Interconnection (OSI) modellen.

TCP/IP

Netværkskort laget

- Network Interface Layer (også kaldet Network Access layer) er ansvarlig for at placere TCP / IP-pakker på netværks mediet og modtage TCP / IP-pakker fra netværks mediet.
- TCP/IP er designet til at være uafhængigt af netadgangs metoden, frame format og medie. På denne måde kan TCP / IP anvendes til at forbinde forskellige netværkstyper.
  - Disse omfatter LAN teknologier som Ethernet og Token Ring og WAN teknologier som X.25 og Frame Relay.
- Uafhængighed fra specifikke netværksteknologi giver TCP / IP evnen til at tilpasses nye teknologier.

TCP/IP

Netværkskort laget

- Network Interface laget omfatter både Data Link og det Fysiske lag af OSI-modellen.
- Bemærk, at Internet laget ikke benytter de sekventerings og kvitterings tjenester, der kan være til stede i data-link laget.
  - En upålideligt Network Interface lag antages, og pålidelig kommunikation gennem sessions etablering og sekventering og anerkendelse af pakker er transport lagets ansvar.

TCP/IP

Internet laget

- Internet Layer er ansvarligt for adressering, paknings og routing funktioner.
- De centrale protokoller for internet laget er IP, ARP, ICMP, og IGMP.
  - Internet Protocol (IP) er en routable protokol ansvarlig for IP-adressering, routing og fragmentering og samling af pakker.
  - Address Resolution Protocol (ARP) er ansvarlig for binding af internet lags adressen til Network Interface lag-adressen som en hardware-adresse.
  - Internet Control Message Protocol (ICMP) er ansvarlig for at levere diagnostiske funktioner og rapporterer fejl på grund af den tabt levering af IP-pakker.
  - Internet Group Management Protocol (IGMP) er ansvarlig for forvaltningen af IP multicast grupper.
- Internet layer svarer til Network layer I OSI modellen.

TCP/IP

Transport laget

- Transport Layer (også kendt som host-to-host Transport Layer) er ansvarlig for at levere session og datagram kommunikationstjenester til applikationslaget.
- De centrale protokollerne for transport laget er Transmission Control Protocol (TCP) og User Datagram Protocol (UDP).
  - TCP er en en-til-en, forbindelsesorienteret, pålidelig kommunikationstjeneste. TCP er ansvarlig for etableringen af en TCP-forbindelse, sekventering og anerkendelse af pakker sendt og inddrivelse af pakker tabt under transmissionen.

TCP/IP

Transport laget

- UDP er en-til-en eller en-til-mange, forbindelsesløs, upålidelig kommunikationstjeneste. UDP bruges, når mængden af data, der skal overføres, er lille (såsom data, som ville passe ind i en enkelt pakke), når overhead til at etablere en TCP-forbindelse ikke er ønsket eller når programmerne eller øvre lags protokoller sørger for pålidelig levering.

- Transportlaget omfatter ansvaret fra OSI Transport laget og nogle af ansvarsområderne fra OSI sessions laget.

TCP/IP

Applikations laget

- Application Layer giver applikationer mulighed for at få adgang til tjenester fra de andre lag og definerer de protokoller som applikationer bruger til at udveksle data. Der er mange applikationslags protokoller og nye protokoller er altid under udvikling.
- De mest kendte applikationslagsprotokoller er dem, der anvendes til udveksling af brugerinformation:
  - Hypertext Transfer Protocol (HTTP) bruges til at overføre filer, der udgør websider på World Wide Web.
  - File Transfer Protocol (FTP) bruges til interaktiv filoverførsel.
  - Den Simple Mail Transfer Protocol (SMTP) bruges til overførsel af mails og vedhæftede filer.
  - Telnet, en terminal emulering protokol, der bruges til at logge på eksternt til netværks værter.

TCP/IP

Applikations laget

- Derudover bidrager følgende protokoller til at lette applikationslagets anvendelse og forvaltning af TCP/IP-netværk
  - Domain Name System (DNS) bruges til at binde et værtsnavn til en IP-adresse.
  - Routing Information Protocol (RIP) er en routing-protokol, som routere bruger til at udveksle routing oplysninger om et IP internetværk.
  - Simple Network Management Protocol (SNMP) bruges mellem en netværk managements konsol og netværksenheder (routere, broer, intelligente hubs) at indsamle og udveksle netværks management information.

TCP/IP

Applikations laget

- Eksempler på applikationslaget grænseflader til TCP/IP-applikationer er Windows Sockets og NetBIOS.
  - Windows Sockets tilbyder et standard application programming interface (API) under Windows.
  - NetBIOS er et industristandard-interface til at få adgang til protokol tjenester såsom sessioner, datagrammer og name resolution.

TCP/IP

IP adresser

En enheds netværks-telefonnummer

IP adresser

Ved opsætning af netværk på de fleste computere kræves en en IP-adresse, undernetmaske (subnet mask) og som regel en standardgateway som del af TCP / IP konfigurationsindstillingerne.

TCP/IPs succes som netværksprotokol for Internettet er især på grund af dens evne til at forbinde netværk af forskellige størrelser og systemer af forskellige typer.

Disse netværk er arbitrært defineret i tre hovedklasser (sammen med et par andre), der har foruddefinerede størrelser, som hver især kan inddeles i mindre undernet af systemadministratorer.

En undernetmaske bruges til at opdele en IP-adresse i to dele. Den ene del identificerer værten (computer), den anden del identificerer netværk, som det tilhører.

IP adresser

Opgave

- Jeg antager at I alle kører Windows.
- Find jeres computeres IP adresse
  - Start f.eks. Kommando prompten (windows-tast + R og skriv CMD) og skriv ipconfig og tryk enter.
  - Hvert netkort eller virtualiserings software har en IPv4 adresse.

IP adresser

IP adresser: Netværk og værter

- En IP-adresse er et 32-bit tal, der entydigt identificerer en vært (computer eller anden enhed, såsom en printer eller en router) på et TCP/IP-netværk.
- IP-adresser er normalt udtrykt i punkt-decimalformat, med fire tal adskilt af punktummer, f.eks 192.168.123.132. For at forstå, hvordan undernetmasker bruges til at skelne mellem værter, netværk og undernetværk vil vi undersøge en IP-adresse i binær notation.
  - Punkt-decimal IP-adressen 192.168.123.132 er (i binær notation) 32 bit tallet 11000000010100011110111000100. Dette nummer kan være svært at overskue, så man opdeler det i fire dele af otte binære cifre.

IP adresser

IP adresser: Netværk og værter

- Disse otte bit sektioner er kaldes **oktetter**. Eksempel IP-adressen bliver således 11000000.10101000.01111011.10000100. Dette tal giver kun lidt mere mening, så til de fleste anvendelser konverteres den binære adresse til punktdecimalformat (192.168.123.132). Decimaltallene adskilt af punktummer er oktetterne konverteret fra binær til decimal.

- For at et TCP/IP wide area network (WAN) kan arbejde effektivt som en samling af netværk, skal de routere, der sender pakker af data mellem netværk, ikke kende den nøjagtige placering af en vært, til hvilken en pakke af information er bestemt. Routere skal kun vide hvilket netværk værten er medlem af og bruge oplysningerne gemt i deres rute tabel til at bestemme, hvordan de får pakken til destinations værtens netværk. Efter pakken er leveret til destinations netværket bliver pakken leveret til den korrekte vært.

IP adresser

IP adresser: Netværk og værter

- For at dette kan fungere består en IP-adresse af to dele.
- Den første del af en IP-adresse bruges som en netværks adresse, den sidste del som værts adresse.
  - Hvis du tager eksemplet 192.168.123.132 og opdeler det i disse to dele får du følgende:
    - 192.168.123. Netværk
132 Vært

      eller
    - 192.168.123. Netværk
0 . 0 . 0 .132 Vært

IP adresser

Undernet / Subnet maske

- Det andet element, som er nødvendig for at TCP/IP fungerer er undernetmasken.
- Undernetmasken bruges af TCP/IP-protokollen til at afgøre, om en vært er på det lokale undernet eller på et eksternt netværk.
- I TCP/IP, er de dele af IP-adressen, der anvendes som netværks og værtsadresser ikke fast, så netværket og værtsadresserne kan ikke bestemmes, medmindre du har flere oplysninger.
- Disse oplysninger leveres i et andet 32-bit tal kaldet en undernetmaske. Den typiske undernetmaske er 255.255.255.0, så lad os gå ud fra den.

IP adresser

Undernet / Subnet maske

- Det er ikke klart, hvad dette tal betyder, medmindre man ved at 255 i binær notation er 11111111, så undernetmasken er:

  11111111.11111111.11111111.0000000

- Hvis vi sætter IP-adressen og undernet masken sammen kan netværk og værtsdelen af netværket adskilles:

  11000000.10101000.01111011.10000100 - IP addresse (192.168.123.132)
  11111111.11111111.11111111.00000000 - Subnet maske (255.255.255.0)

- De første 24 bit (antallet af dem i undernetmasken) identificeres som netværks adressen og de sidste 8 bit (antallet af resterende nuller i undernetmasken) identificeres som værts adresse.

IP adresser

Undernet / Subnet maske

- Dette giver:
  11000000.10101000.01111011.00000000 - Netværks adresse (192.168.123.0)
  00000000.00000000.00000000.10000100 - Værts adresse (000.000.000.132)
- I dette eksempel ved vi ved hjælp af en 255.255.255.0 undernetmaske at netværks-id er 192.168.123.0 og værtens adresse er 0.0.0.132.
- Når en pakke ankommer på 192.168.123.0 subnettet (fra det lokale undernet eller et eksternt netværk), og det har en destinations adresse 192.168.123.132, vil computeren modtage den fra netværket og behandle den.

IP adresser

IPv6

- Hidtil har alle de adresser vi har talt om været IPv4 adresser, men der er en version 6 af IP der erstatter IPv4.
- Der er indført mange forbedringer i IPv6, men den største forskel er størrelsen af adressefeltet, som er på 128 bit mod kun 32 bit i IPv4.
- Udvidelsen af adressefeltet giver teoretisk mulighed for op til $3{,}4 \times 10^{38}$ (340 sekstillioner) adresser, som kan sammenlignes med, at der i IPv4 kun var mulighed for omkring 4 milliarder adresser – et maksimum vi reelt har nået, men ikke alle enheder er på samme netværk hele tiden så det går endnu.

DHCP

Automatisk tildeling af IP på et lokalnetværk

DHCP

Dynamic Host Configuration Protocol (DHCP) er en klient / server-protokol, der automatisk udstyrer en Internet Protocol (IP) vært med dens IP-adresse og andre relaterede konfigurations oplysninger såsom under-net-masken (subnet mask) og standard-gateway.

- Hver enhed på et TCP / IP-baseret netværk skal have en unik unicast IP-adresse for at få adgang til netværket og dets ressourcer.
- Uden DHCP, skal IP-adresser til nye computere eller computere, der flyttes fra et subnet til et andet konfigureres manuelt; IP-adresser til computere, der fjernes fra netværket, skal manuelt regenereres.
- DHCP tillader værter at opnå ønskede TCP / IP-konfiguration fra en DHCP-server.

DHCP

- DHCP automatiserer denne proces og styrer den centralt.
- DHCP-serveren opretholder en pulje af IP-adresser og leaser en adresse til en DHCP-aktiveret klient, når den starter op på netværket.
  - Fordi IP-adresserne er dynamiske (lejede) snarere end statiske (fast tilknyttede), bliver adresser der ikke længere er i brug automatisk returneret til puljen til omfordeling.
- Netværksadministratoren etablerer DHCP-serveren (kan være en Windows PC, kan være netværksudstyr som en router), der opretholder TCP / IP-konfigurations informationerne og giver adresse konfiguration til DHCP-aktiverede klienter i form af et lease offer.

DHCP

- DHCP-serveren gemmer konfigurations oplysningerne i en database, der indeholder:
  - Gyldige TCP/IP-konfigurationsparametre til alle klienter på netværket.
  - Gyldige IP-adresser, holdes i en pulje for tildeling til klienter samt udeladte adresser.
  - Reserverede IP-adresser forbundet med bestemte DHCP-klienter. Dette giver mulighed for konsekvent tildeling af en enkelt IP-adresse til en enkelt DHCP klient.
  - Lease varighed eller det tidsrum, som IP-adressen kan bruges før en lease fornyelse er påkrævet.
- En DHCP-aktiveret klient modtager efter at acceptere et lease:
  - En gyldig IP-adresse til det undernet, som den er tilsluttet.
  - Anmodede DHCP-indstillinger, der er yderligere parametre, som en DHCP-server er konfigureret til at tildele sine klienter. Nogle eksempler på DHCP-indstillinger er Router (standardgateway), DNS-servere og DNS domænenavn.

DHCP

DHCP bruges som standard på stort set alle netværk i dag. Der er en række grunde til dette:

- Pålidelig IP-adresse konfiguration.
  - DHCP minimerer konfigurations fejl forårsaget af manuel IP-adresse konfiguration, såsom trykfejl eller adresse konflikter forårsaget af tildelingen af en IP-adresse til mere end én computer på samme tid.
- Reduceret netværksadministration.
  - DHCP indeholder følgende funktioner til at reducere netværksadministration:

DNS

Hvordan man finder sider på internettet

DNS

DNS er en forkortelse for **Domain Name System** (Domain Name Server, Domain Name Service). En DNS-server eller **navneserver** er en server placeret på et IP-baseret datanet, der tager sig af oversættelsen af de navne man normalt arbejder med på Internettet.

- DNS binder menneske-læsbare værtsnavne som www.eal.dk til maskinlæsbare IP-adresser som 185.19.134.177.
- DNS indeholder også andre oplysninger om domænenavne som mail-tjenester.
- En computer følger en række trin for at omdanne den læsbare web-adresse i en maskinlæsbar IP-adresse.
- Dette sker hver gang du bruger et domænenavn, uanset om du læser hjemmesider, sender e-mail eller ser Netflix.
- Kommunikation over et IP-baseret datanet kan kun foregå ved hjælp af disse IP-adresser – ligesom telefonnumre. En DNS-server kan sammenlignes med en telefonbog med et alfabetisk register.

DNS

Trin 1: Anmod om information

- Processen begynder, når man beder ens computer om at resolve et værtsnavn, såsom besøger http://eal.dk.
- Det første sted computeren tjekker, er dens lokale DNS cache, som lagrer oplysninger, som din computer for nylig har hentet.
- Hvis din computer ikke allerede kender svaret er det nødvendigt at udføre en DNS forespørgsel.

DNS

Trin 2: Spørg rekursive DNS servere

- Hvis oplysningerne ikke er gemt lokalt spørger ens computer (kontakter) ens internetudbyders rekursive DNS-servere.
- Disse specialiserede computere udfører arbejdet ved en DNS forespørgsel på dine vegne.
- Rekursive servere har deres egne cacher, så processen ender som regel her og oplysningerne returneres til brugeren.

DNS

Trin 3: Spørg rod navneservere

- Hvis rekursive serverne ikke har svaret spørger de rod navne-serverne.
- En navneserver er en computer, der besvarer spørgsmål om domænenavne, såsom IP-adresser.
- De tretten rod navneservere fungerer som en slags telefoncentral for DNS. De kender ikke svaret, men de kan dirigere vores forespørgsel til en person, der ved hvor man kan finde det.

DNS

Trin 4: Spørg TLD navneservere

- Rod navneserverne vil se på den første del af vores anmodning, læst fra højre mod venstre – www.eal.dk – og dirigere vores forespørgsel til Top-Level Domain (TLD) navneserverne for .dk.
- Hvert TLD, såsom .com, .org og .dk har deres eget sæt af navneservere, der fungerer som en receptionist for hver TLD.
- Disse servere har ikke de oplysninger, vi har brug for, men de kan henvise os direkte til de servere, der har de oplysninger.

DNS

Trin 5: Spørg de autoritative DNS-servere

- TLD navneserverne gennemgår den næste del af vores anmodning – www.eal.dk – og dirigerer vores forespørgsel til navneserverne ansvarlige for dette specifikke domæne.
- Disse autoritative navneservere er ansvarlig for at kende alle oplysninger om et bestemt domæne, som er gemt i DNS records.
- Der er mange typer af optegnelser, der hver indeholder en anden form for information.
- I dette eksempel, vi ønsker at kende IP-adressen for www.eal.dk, så vi beder den autoritative navneserver om Adress Record (A).

DNS

Trin 6: Hent optegnelsen

- Den rekursive server henter en optegnelse for eal.dk fra den autoritative navneservere og gemmer optegnelsen i sin lokale cache.
- Hvis nogen ellers anmoder om host records for eal.dk vil de rekursive servere allerede har svaret, og behøver ikke at gå gennem opslags processen igen.
- Alle optegnelser har en time-to-live værdi, der er som en udløbsdato. Efter et stykke tid, vil den rekursive server blive nødt til at bede om en ny kopi af optegnelsen for at sikre at oplysningerne ikke bliver forældede.

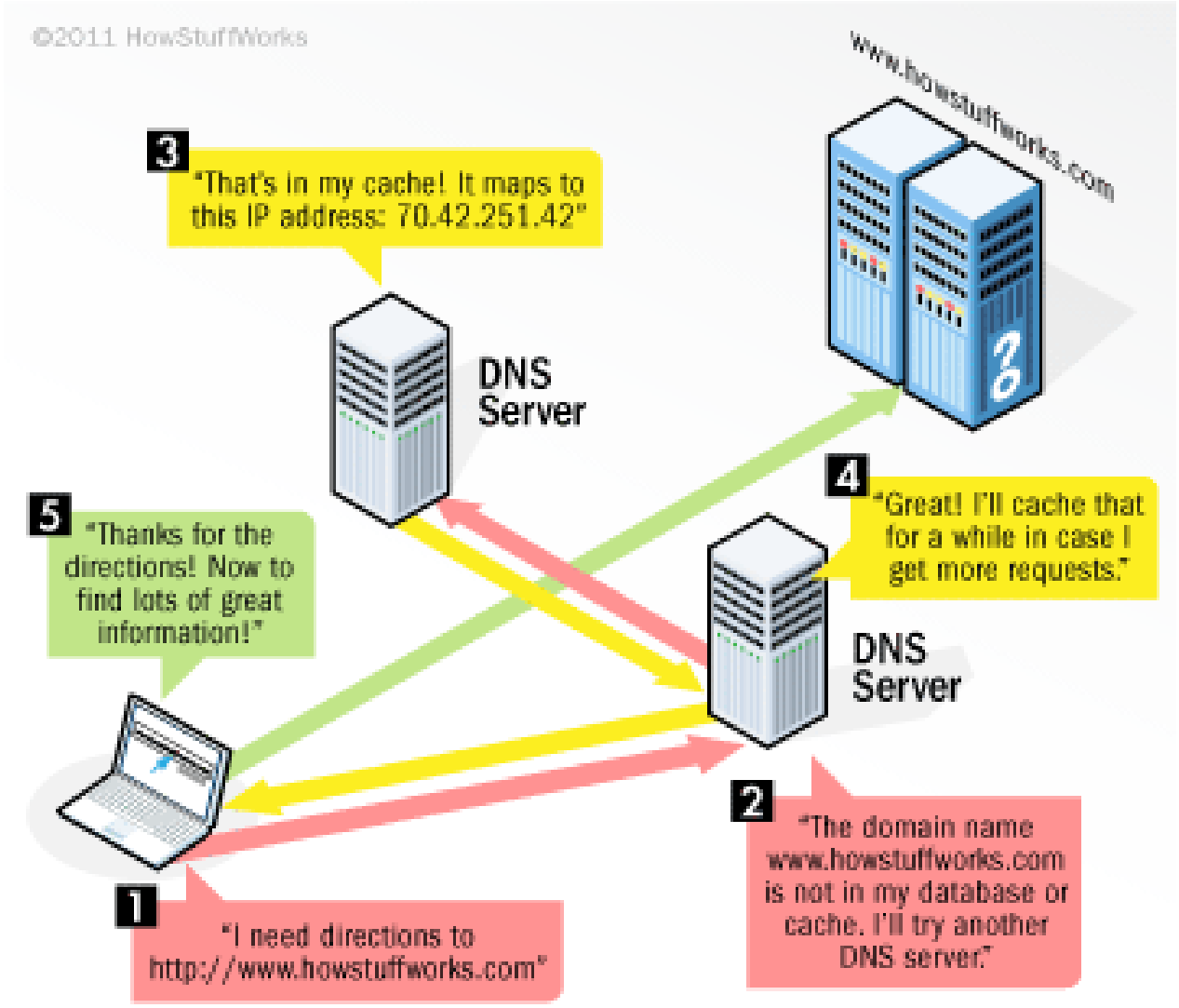
DNS

Trin 7: Hent svaret

- Bevæbnet med svaret returnerer den rekursive server A record tilbage til computeren.
- Ens computer gemmer optegnelsen i sin cache, læser IP-adressen fra optegnelsen og sender disse oplysninger til ens browser. Browseren åbner så en forbindelse til webserveren og modtager hjemmesiden.

Hele denne proces, fra start til slut, tager kun millisekunder at fuldføre.

DNS


©2011 HowStuffWorks
www.howstuffworks.com
3
"That's in my cache! It maps to this IP address: 70.42.251.42"
DNS Server
4
"Great! I'll cache that for a while in case I get more requests."
5
"Thanks for the directions! Now to find lots of great information!"
DNS Server
2
"The domain name www.howstuffworks.com is not in my database or cache. I'll try another DNS server."
1
"I need directions to http://www.howstuffworks.com"

Fysiske netværks enheder

Disse konkrete ting består et netværk af

Fysiske netværks enheder

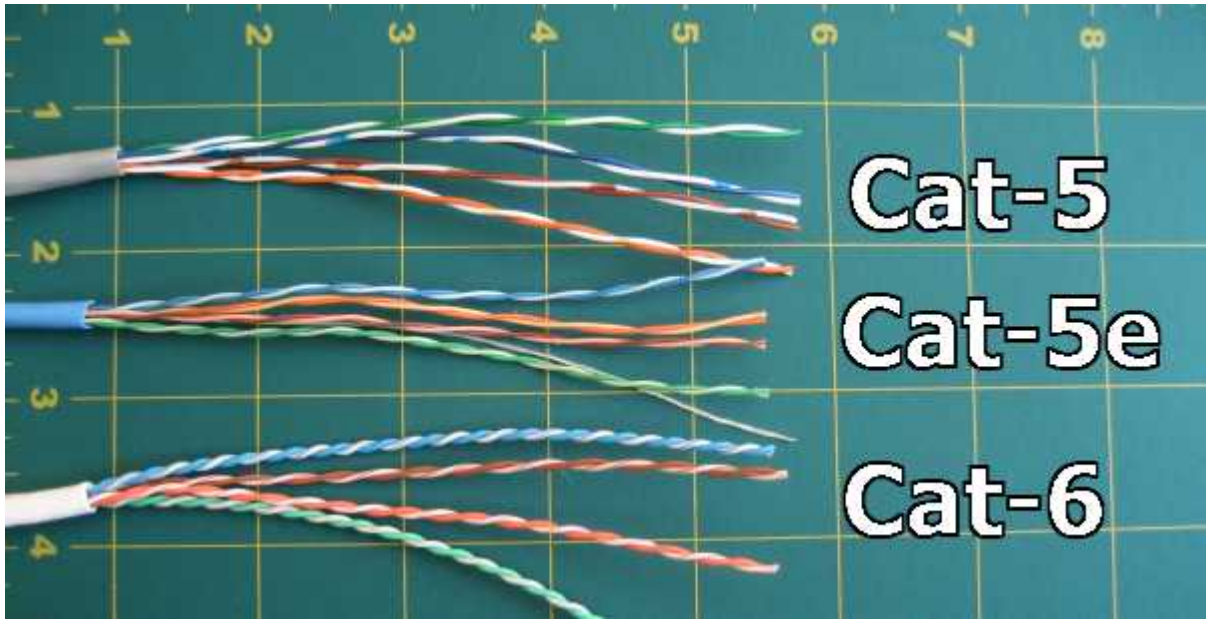
Kabler

- Den rekursive server henter en optegnelse for eal.dk fra den autoritative navneservere og gemmer optegnelsen i sin lokale cache.

Fysiske netværks enheder

Kabler

- Normalt bruger man kobber-kabler bestående af otte snoede ledninger.
- I dag ser vi typisk de tre nedenstående "kvaliteter", der bestemmes af hvor ofte kablerne er snoet.
  - Cat 5 = 100Mbit, Cat-5e = Gbit, Cat-6 10Gbit



Fysiske netværks enheder

Opgave

- Saml et netværks-kabel

Fysiske netværks enheder

Netværks repeater

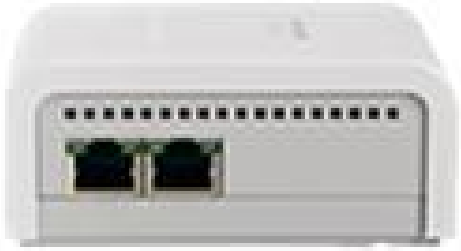
- En repeater forbinder to segmenter af det netværkskabel.
- Det retimer og regenererer signalerne til ordentlige amplituder (styrker) og sender dem til de øvrige segmenter.
- Når vi taler om, ethernet topologi vil man sandsynligvis om an bruge en hub som en repeater.
- Repeatere kræver en lille mængde tid til at regenerere signalet. Dette kan medføre et propagation delay, som kan påvirke netværkd kommunikation, når der er flere repeatere i træk. Mange netarkitekturer begrænser antallet af repeatere, som kan anvendes i en række.
- Repeatere fungerer kun på det fysiske lag i OSI netværksmodellen.

Fysiske netværks enheder

Hub

- Hubs bruges normalt til at forbinde segmenter af et netværk.
- En hub indeholder flere porte.
- Når en pakke ankommer til en port kopieres den til de andre porte, således at alle segmenter af netværket kan se alle pakker.
- En 10/100Mbps hub må dele sin båndbredde med hver af dens porte.
  - Når kun en PC sender vil det have adgang til den maksimale tilgængelige båndbredde. Men hvis flere pc'er udsender så skal båndbredden fordeles mellem alle disse systemer, hvilket vil forringe ydeevnen.

Fysiske netværks enheder



Repeater

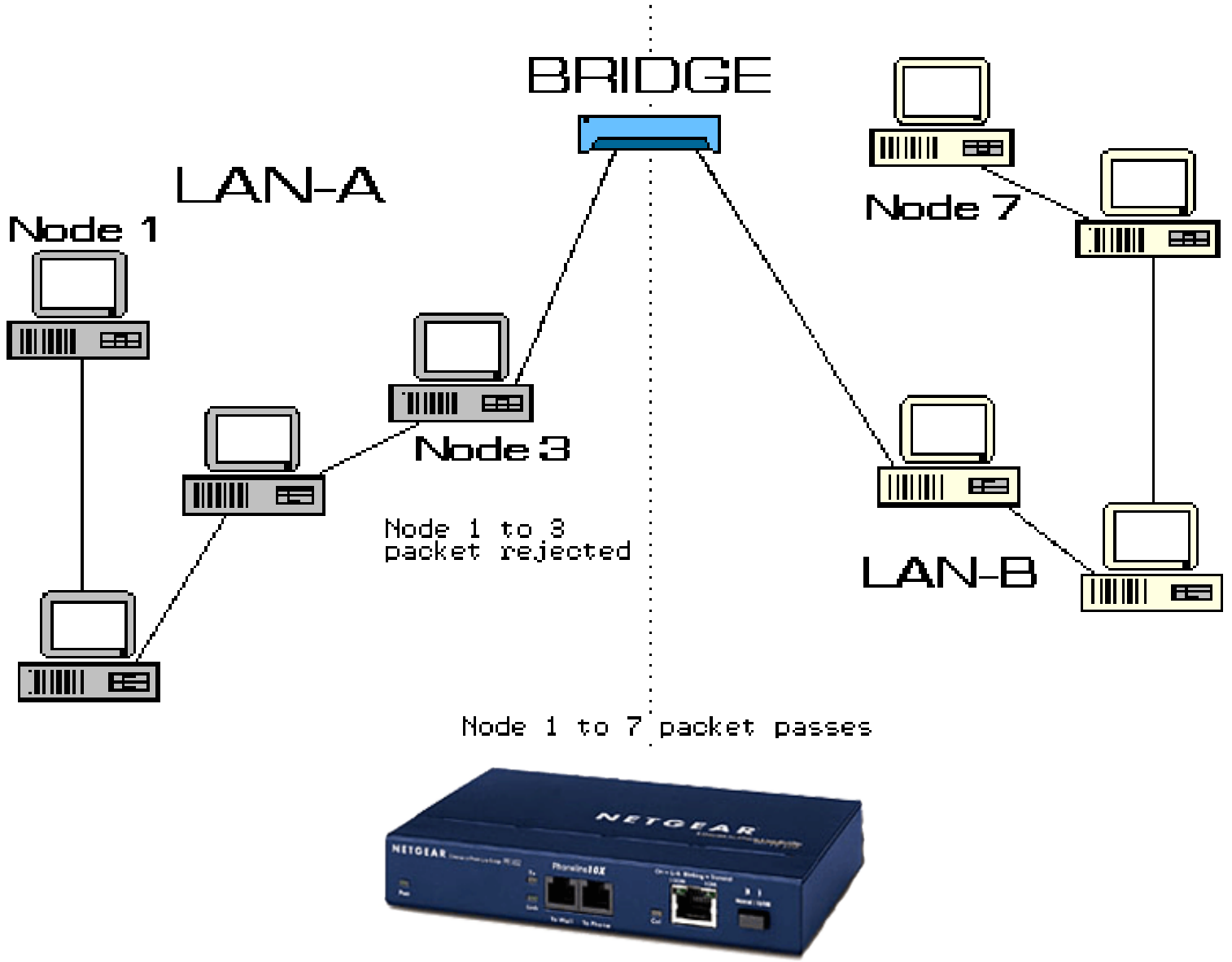
Hub

Fysiske netværks enheder

Bro

- En bro læser yderste del af data om datapakken, for at bedømme, hvor budskabet skal hen. Det reducerer trafik på andre netværkd segmenter, eftersom det ikke sender alle pakker.
- Broer kan programmeres til at afvise pakker fra bestemte netværk.
- Bridging forekommer på datalink laget af OSI-modellen, hvilket betyder at broen kan ikke læse IP-adresser, men kun den yderste hardwareadresse af pakken. Broen kan læse ethernet data, som giver den hardware adressen på destinations adressen, ikke IP-adressen.
- Broer forwarder alle broadcast beskeder.

Fysiske netværks enheder



Fysiske netværks enheder

Switch

- En switch registrerer MAC-adresserne på alle de enheder tilsluttet til den.
  - Med denne information kan en switch identificere hvilket system sidder på hvilken port.
- Når en pakke er modtaget ved switchen præcis hvilken port at sende den til, uden væsentlig forøgelse af netværkets svartider.
- I modsætning til en hub, vil en 10/100Mbps switch tildele fulde 10/100Mbps til hver af sine porte.
  - Uanset antallet af pc'er transmitterende, vil brugerne altid har adgang til den maksimale båndbredde.

Fysiske netværks enheder

Switche

Fysiske netværks enheder

Netværks router

- En router bruges til at route datapakker mellem to netværk.
- Det læser informationen i hver pakke for at fortælle, hvor den skal hen.
  - Hvis det er bestemt til det direkte netværk den har adgang til, vil det fjerne den ydre pakke, readressere pakken til den rigtige ethernet-adresse og sende den på dette net.
  - Hvis det er bestemt til et andet netværk, og skal sendes til en anden router, vil det igen pakke den ydre pakke, der skal modtages af den næste router og sende den til den næste router.
- Der benyttes routing tabeller til at hjælpe med at bestemme pakke destinationer.
- Routing sker på netværks laget af OSI-modellen.
- Selv om de kan omdanne information på datalink niveau kan routere ikke omdanne oplysninger fra et dataformat såsom TCP/IP til et andet såsom IPX/SPX.
- Routere ikke sende broadcast pakker eller beskadigede pakker.
- Hvis routingtabellen ikke angiver den korrekte adresse af en pakke, kasseres pakken.

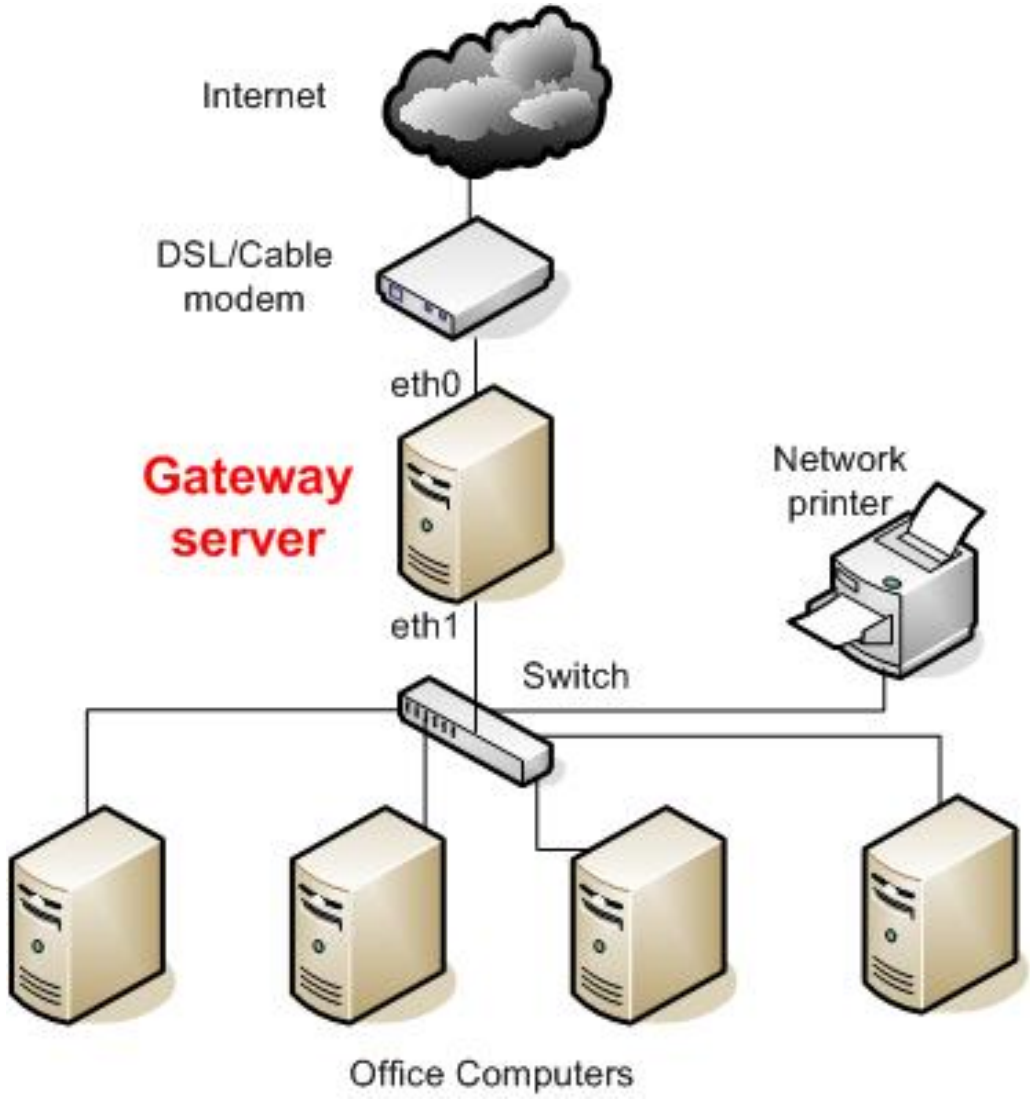
Fysiske netværks enheder

Fysiske netværks enheder

Gateway

- En gateway kan oversætte informationer mellem forskellige netværk dataformater eller netværksarkitekturer.
- De fleste gateways opererer på applikationslaget, men kan operere på nettet eller sessions laget af OSI-modellen.
- Gateways vil starte på det lavere niveau og fjerne oplysninger, indtil de når til det ønskede niveau og ompakke oplysninger og arbejde sig tilbage mod hardware laget af OSI-modellen.
- Det kan forvirre at ordet gateway ofte bruges når man snakker om en router. Det betyder ikke routeren er en gateway som defineret her, selv om den kan være.

Fysiske netværks enheder



Fysiske netværks enheder

Gateway

Fysiske netværks enheder

NAT (Network Address Translator)

- NAT er en forkortelse for Network Address Translation.
- NAT er en Internet standard, der gør det muligt for et lokalt-netværk (LAN) til at bruge et sæt IP-adresser til intern trafik og et andet sæt adresser til ekstern trafik.
- En NAT-boks placeret hvor LAN møder internettet sørger for alle nødvendige IP-adresse oversættelser.
- NAT tjener tre hovedformål:
  - En slags firewall der skjuler interne IP-adresser.
  - Lader en virksomhed bruge flere interne IP-adresser.
    - Da de kun bruges internt er der ingen mulighed for konflikt med IP-adresser, der bruges af andre virksomheder og organisationer.

Fysiske netværks enheder

NAT og NAPT

- NAPT (Network Address og Port Translation) er en udvidelse af NAT, der lader mange IP-adresser forbindes til en enkelt IP-adresse.
- Dette gøres ved hjælp af TCP og UDP port information i den udgående trafik.
- NAPT (Network Address og Port Translation) bruges til at forbinde et sæt private IP-adresser ved hjælp af en enkelt offentlig IP-adresse eller en lille gruppe af offentlige IP-adresser. NAPT er også omtalt som PAT (Port Address Translation), IP masquerading, NAT Overload og mange-til-en NAT.
- I NAPT, er mange IP-adresser knyttet til en enkelt IP-adresse. Dette vil medføre en tvetydighed i forhold til de returnerede pakker. For at undgå dette problem gør NAPT brug af TCP/UDP port information i den udgående trafik og opretholder en oversættelses tabel. Dette vil tillade routing af de returnerede pakker korrekt til modtageren.

Kilder

Materiale benyttet i denne lektion
Noget af det er udover pensum-listen!

Kilder

OSI modellen

- http://electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip
- http://searchnetworking.techtarget.com/definition/protocol
- https://youtu.be/sVDwG2RdJho

TCP/IP protokol arkitekturen

- https://technet.microsoft.com/en-us/library/cc958821.aspx
- https://youtu.be/-v64FHQxE7E

IP adresser

- http://www.tutorialspoint.com/ipv4/
- https://support.microsoft.com/en-us/kb/164015
- https://da.wikipedia.org/wiki/IPv6

Kilder

DHCP

- https://technet.microsoft.com/en-us/library/dd145320(v=ws.10).aspx

DNS

- https://da.wikipedia.org/wiki/Domain_Name_System
- http://dyn.com/blog/dns-why-its-important-how-it-works/
- http://computer.howstuffworks.com/dns.htm
- https://technet.microsoft.com/en-us/library/cc730921(v=ws.11).aspx

Fysiske netværks enheder

- http://www.howtogeek.com/70494/what-kind-of-ethernet-cat-5e6a-cable-should-i-use/
- https://www.trangosys.com/cat-5-ethernet-cable-standards-pin-out-assignments/

Kilder

Fysiske netværks enheder

- http://www.comptechdoc.org/independent/networking/guide/netdevices.html
- http://www.differencebetween.com/difference-between-nat-and-vs-napt/