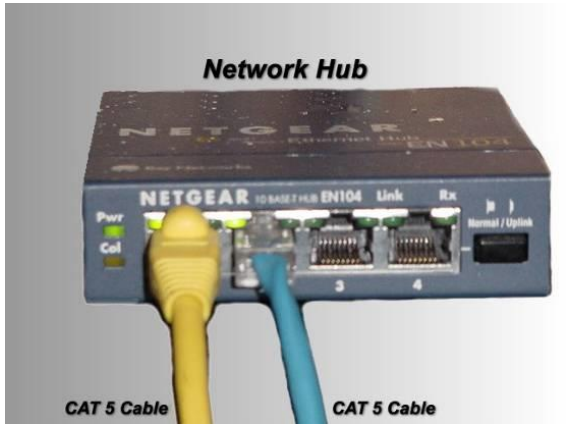


6105 Windows Server og datanett

Leksjon 10 Nettverkskomponenter

- HUB'er, svitsjer og rutere (noe repetisjon)
- ICMP-protokollen
- Adresseoversetting – NAT (noe repetisjon)
- Portforwarding
- Brannmur / pakkefilter
- Windows Firewall

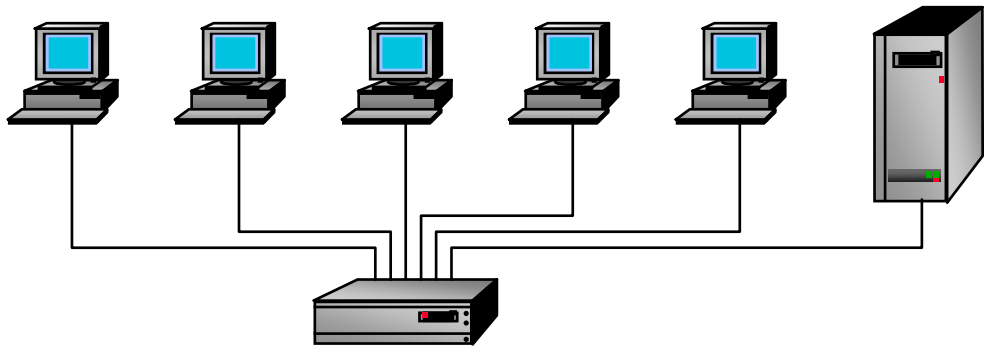
Pensum:

- Kvisli: *Datakommunikasjon og maskinvare*, kapittel 3 TCP/IP protokollene
- Kvisli: *Datakommunikasjon og maskinvare*, kapittel 4 Nettverkskomponenter
- Kvisli: Windows Server og nettverk, kapittel 13 Windows brannmur

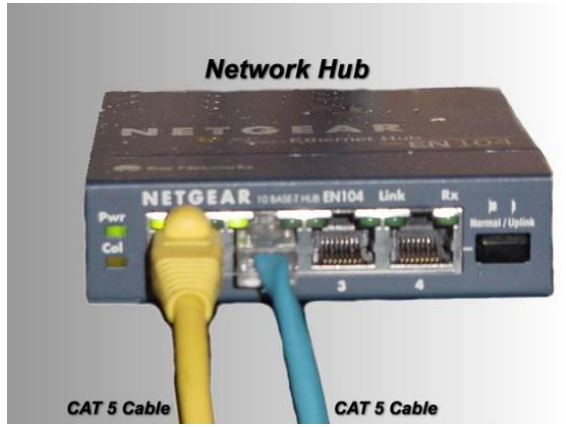
Linker:

- Det finnes mye stoff om dette på Wikipedia: Søk på begrepene

HUB = multiport repeater



HUB



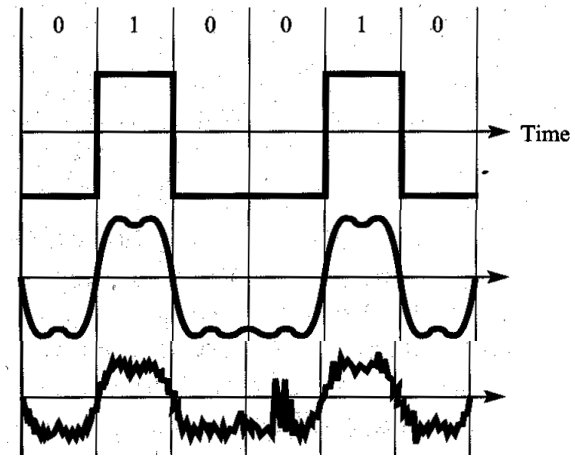
Nettverks HUB (engelsk: hub = nav)

- En "portreplikator" (multiport repeater) for trådparkabel (TP)
- Knytter sammen flere ”kabelgrener” til ett fysisk nett
- HUB'en har flere RJ-45 utganger (og evt. én inngang)
  - » vanligvis 4 – 24 utganger (porter)
- En datamaskin kan kobles til hver port

I moderne lokalnett bruker man svitsjer istedet for HUB’er.
Se neste foil.

Obs! En HUB repeterer (gjentar) fysisk signal på alle porter!

- Alle enheter deler på nettets / HUBens totale kapasitet
- Alle porter må benytte samme hastighet/bitrate



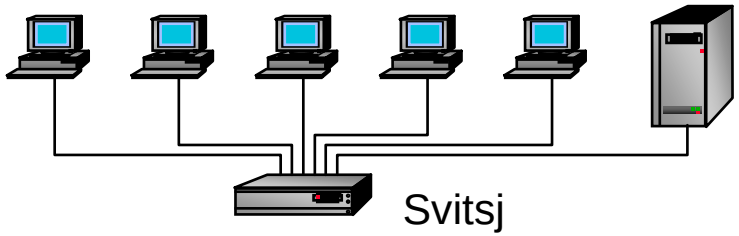
En HUB jobber på lag 1 (fysisk) i OSI modellen

- behandler kun signaler og bits

Svitsj

Svitsj

- Fungerer nesten som en HUB men:
- Behandler pakker (rammer) på **lag 2 (lenkelaget)**
- Leser fysiske MAC-adresser i lenkehodet på hver pakke (ramme)
- Videresender pakker (rammer) bare til riktig "gren" i nettet



Fordeler

- Unngår unødvendig trafikk på nettet
- Hver PC disponerer all båndbredde fram til svitsjen
- Vanskeligere å tappe
- Kan ha ulik bitrate på hver port
  - » Eks: 2 stk 1 Gbit/s porter og 24 stk 100 Mbit/s porter

Typisk konfigurasjon

- 100 eller 1000 Mbit/s til hver arbeidsstasjon
- 1, 10 eller 100 Gbit/s til tjenere og rutere

"Rack-svitsj"

- Svitsjer som kan monteres i "rack-skap"

Rutere (repetisjon)

Datamaskin med:

- Minst to nettverkskort (interface) - koblet til hvert sitt IP-nett
- IP-protokoll installert, men ikke høyere lags protokoller

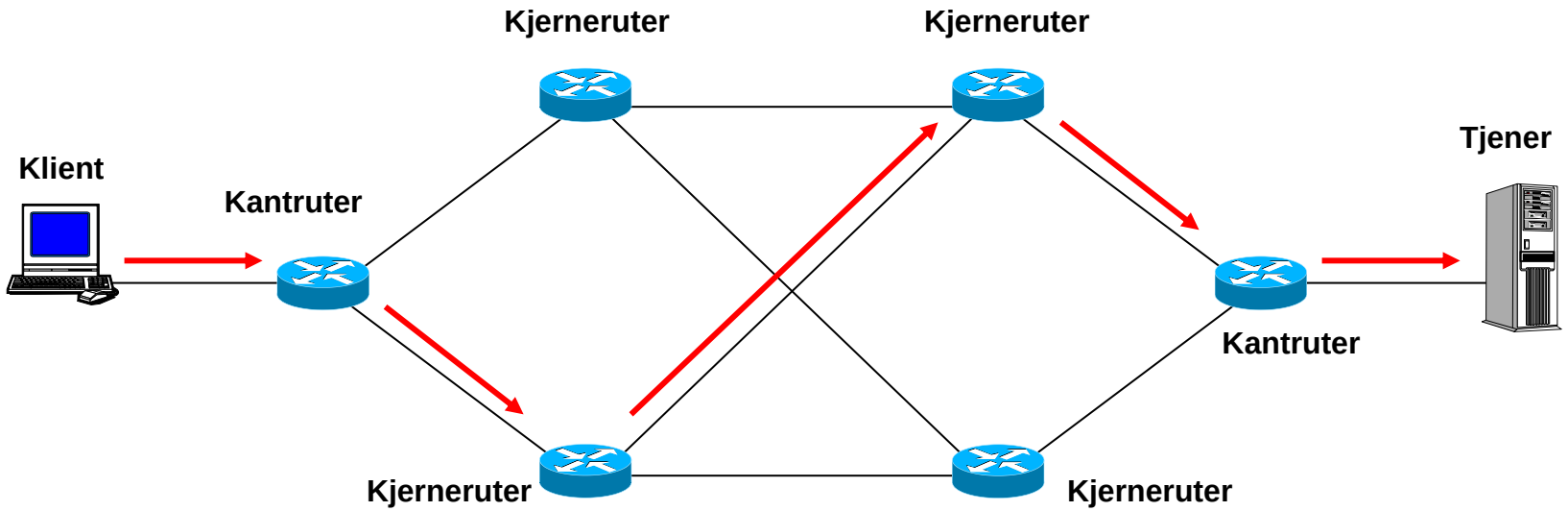
Ruterens oppgaver

- Behandler pakker på lag 3 (nettverkslaget)
- Mottar IP-pakker og leser IP-adresser i IP-hodet
- Bestemmer hvilket nett pakken skal sendes ut på
- Videresender pakken til neste ruter, eller endelig mottaker

Flere typer rutere

- Små ”hjemmerutere”
- Store kjernenettrutere i Internett
- ”Kantrutere” – kobler lokalnett til internett
- ”Vanlige” PCer kan konfigureres som rutere

Ruting (repetisjon)



Figuren er hentet fra Frode Sørensen: *Innføring i nettverk*, IDG Books Norge

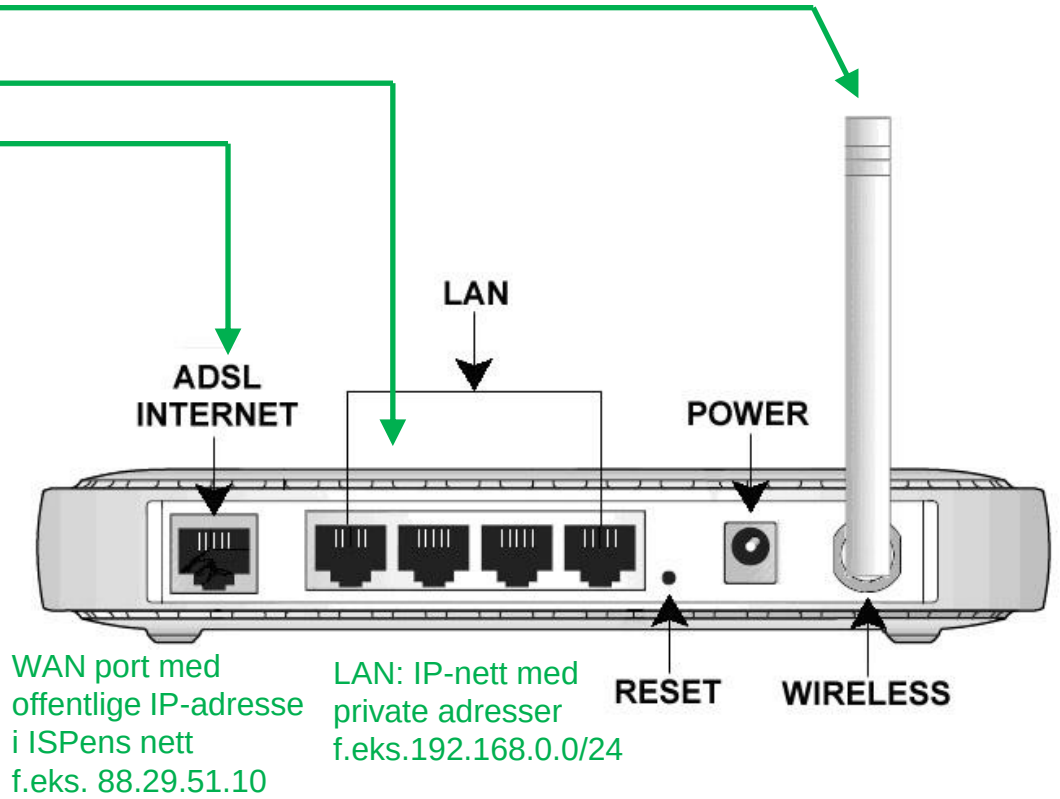
Rutere finnes beste vei gjennom nettet fram til mottaker

- Beste = raskeste, billigste, sikreste .....
- Beste vei kan endre seg over tid – linjer kan endres eller gå ned
- Rutere må kunne takle slike endringer

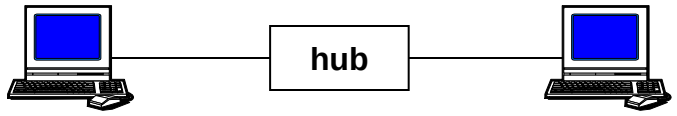
Trådløs ”hjemmeruter”

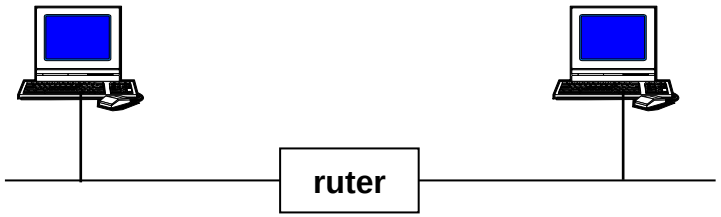
En trådløs ruter til hjemmebruk har flere funksjoner i én boks:

- **Aksesspunkt for WiFi (IEEE 802.11)**
- **Svitsj for ethernet LAN (IEEE 802.3)**
- **Ekstern WAN port**
  - Ethernet- eller fiberport for tilkobling til Internett
    - » Eventuelt ADSL port i eldre ADSL-rutere
  - Portens IP-adresse tilhører nettleverandørens IP-nett
- **Ruter mellom internt nett (LAN) og WAN**
  - Med adresseoversetting (NAT)
- **Brannmurfunksjoner**
  - Filtrering av innkommende trafikk
- **DHCP-tjener**
  - Tildeler (private) IP adresser i LANet
- **Webtjener**
  - For administrasjon av ruteren via en webside



Oppsummering: hub, svitsj og ruter





Hub

OSI-lag: 1 - Fysisk lag

Oppgave: Kopiere (repetere) signaler til nytt fysisk medium

Leser: fysisk signal og bitmønster

Videresender: til alle fysiske porter

Svitsj

OSI-lag: 2 - Lenkelaget

Oppgave: Videresender *rammer* (lag 2 pakker) til riktig "gren i nettet"

Leser: MAC adresser i rammene

Videresender: til fysiske port der mottaker finnes

Ruter

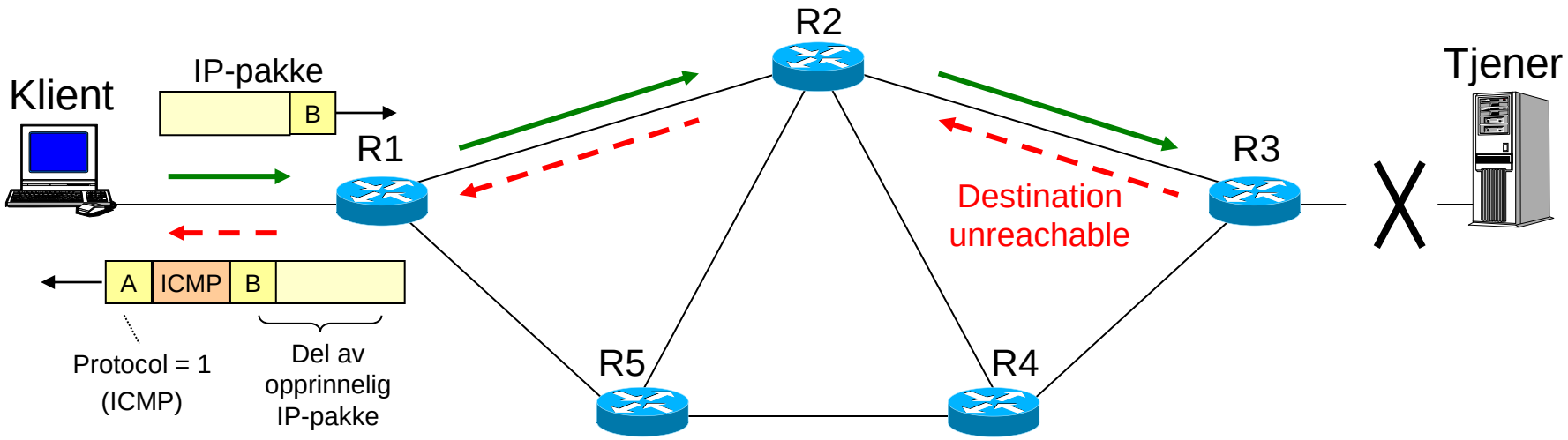
OSI-lag: 3 - Nettverkslaget

Oppgave: Videresende pakker (IP-pakker) mellom IP-nett

Leser: IP-adresse i IP-pakkene

Videresender: til neste ruter eller endelig mottaker

ICMP protokollen



Figuren er hentet fra Frode Sørensen: *Innføring i nettverk*, IDG Books Norge

ICMP brukes for å sende *kontrollmeldinger* i IP-nett

ICMP pakker pakkes inn med IP-hode og transporteres av IP

Likevel regnes vanligvis ICMP som en lag 3 protokoll (ikke lag 4)

ICMP protokollen

ICMP = Internet Control Message Protocol

- Transportprotokoll for feilmeldinger og annen kontrollinformasjon i nettet
- Brukes primært av rutere og andre nettkomponenter
- Brukes også for å sende ”testmeldinger” i nettet, f.eks. av ping
- Definerer et stort antall meldingstyper

Mye brukte meldingstyper:

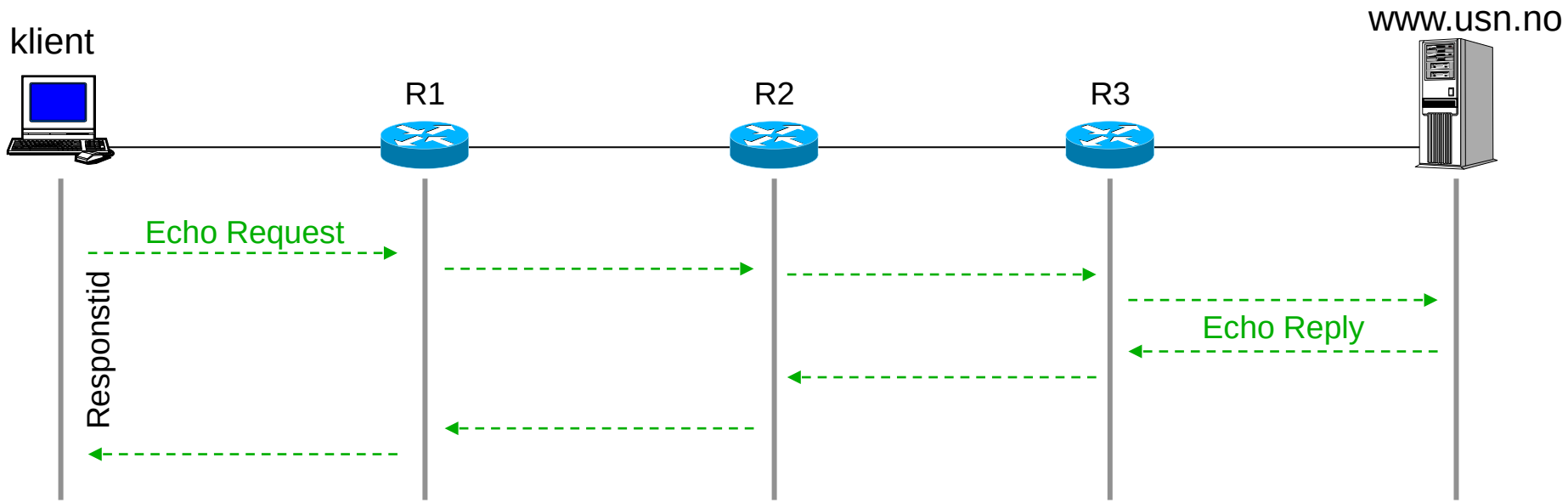
Echo Request	Ber om svar fra en maskin (brukes av ping)
Echo Reply	Svarer på Echo Request
Timestamp Request	Måler tiden ICMP pakken bruker
Timestamp Reply	Svarer på Timestamp Request
Router Advertisement	Routere informerer om sin eksistens og adresse
Destination Unreachable	Mottakers IP-adresse kan ikke nås
Time Exceeded	Telleren *Time-to-live* i en IP pakke har nådd 0
Source Quench	Flaskehals har oppstått i ruter eller mottaker

ICMP og ping

Kommandoen ping bruker ICMP meldinger

- Sender en *Echo Request* melding
- Mottar en *Echo Reply* melding

Eksempel: `ping www.usn.no`



Responstiden er den tiden det tar å få svar på en ping

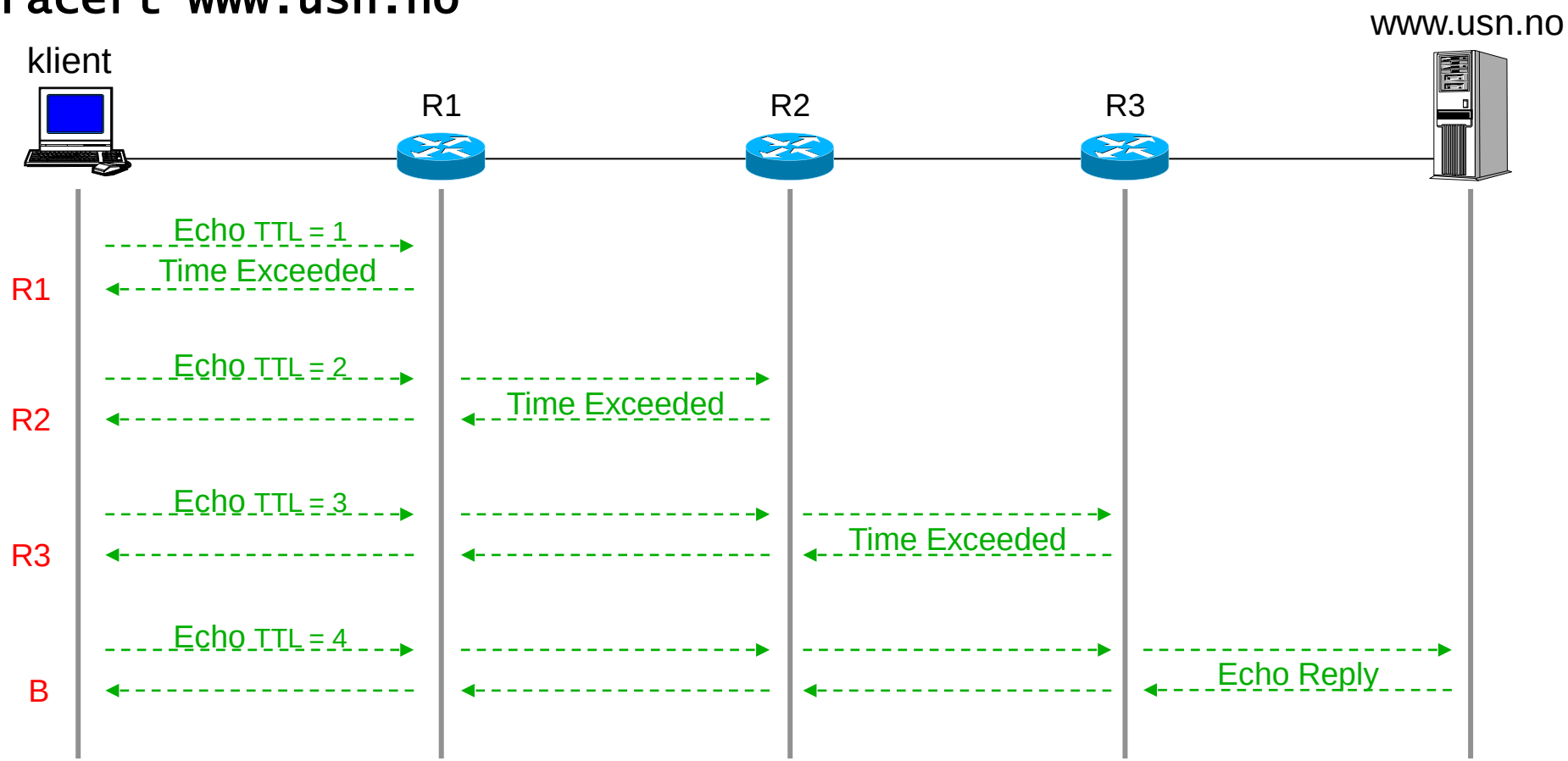
- Måles i millisekunder (ms)
- Skyldes hovedsaklig *forsinkelser* (*latency*) i hver av ruterne på vegen

ICMP og traceroute

Traceroute bruker flere ICMP meldinger etter hverandre

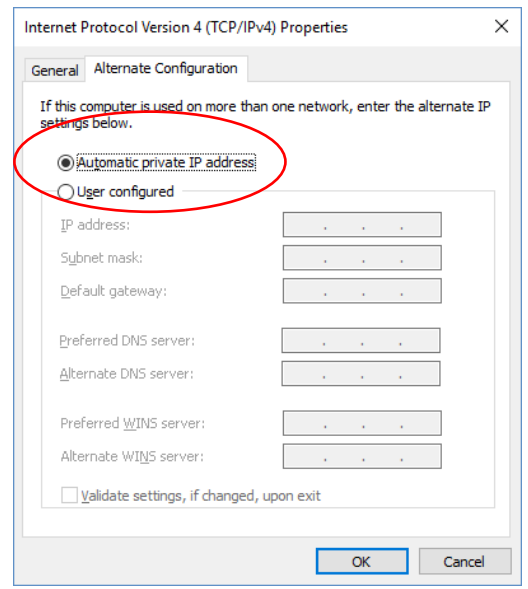
- øker begrensning i antall hopp (*Time-To-Live*) for hver melding
- måler dermed responstiden til hver av ruterne på vegen til mottaker

Eksempel: `tracert www.usn.no`



Private IP-adresser (repetisjon)

Reserverte adresseområder			Nettverk	Kommentar
10.0.0.0	-	10.255.255.255	10.0.0.0/8	2^{24} adresser
172.16.0.0	-	172.31.255.255	172.16.0.0/12	2^{20} adresser
192.168.0.0	-	192.168.255.255	192.168.0.0/16	2^{16} adresser
169.254.0.0	-	169.254.255.255	169.254.0.0/16	(Automatisk privat IP-adr.)



Private IP-adresser skal ikke brukes på Internett

- Dvs. ikke på maskiner/nettkort som er knyttet direkte til Internett
- Private IP-adresser videresendes ikke av rutere i Internett !

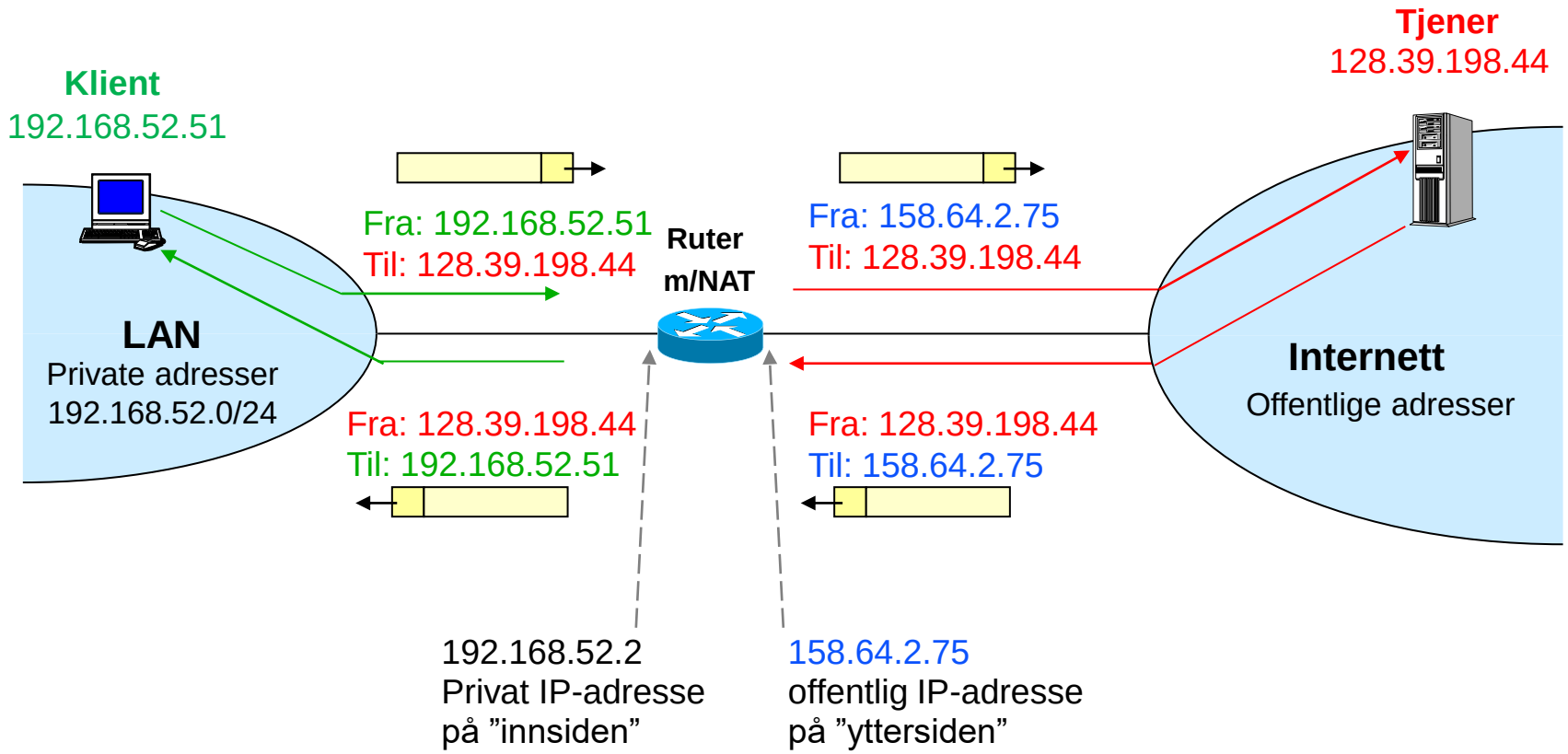
Beregnet for bruk i "lukkede" IP-nett

- IP-nett som er ”gjemt” bak en ruter, og ”usynlige” for Internett.
- Ruteren gjør adresseoversetting (NAT) for pakkene rutes ut på Internett.
- Private IP-nett er ”usynlige” for hverandre – unngår adressekonflikt med like private adresser
- Private IP-adresser kan brukes "fritt" av alle.

Hvorfor?

- "Sparer" offentlige (offisielle) adresser på maskiner som ikke har behov for det.
- Har begrenset problemet med for få adresser i IP versjon 4

Adresseoversetting – NAT (repetisjon)



Figuren er modifisert fra Frode Sørensen: *Innføring i nettverk*, IDG Books Norge

Adresseoversetting – NAT (repetisjon)

Problemstilling:

- Ruter mellom internt nett og åpent Internett med offentlige (offisielle) adresser
- Ønsker å bruke private IP-adresser i internt nett
- Private IP-adresser må ikke slippe ut på Internett!

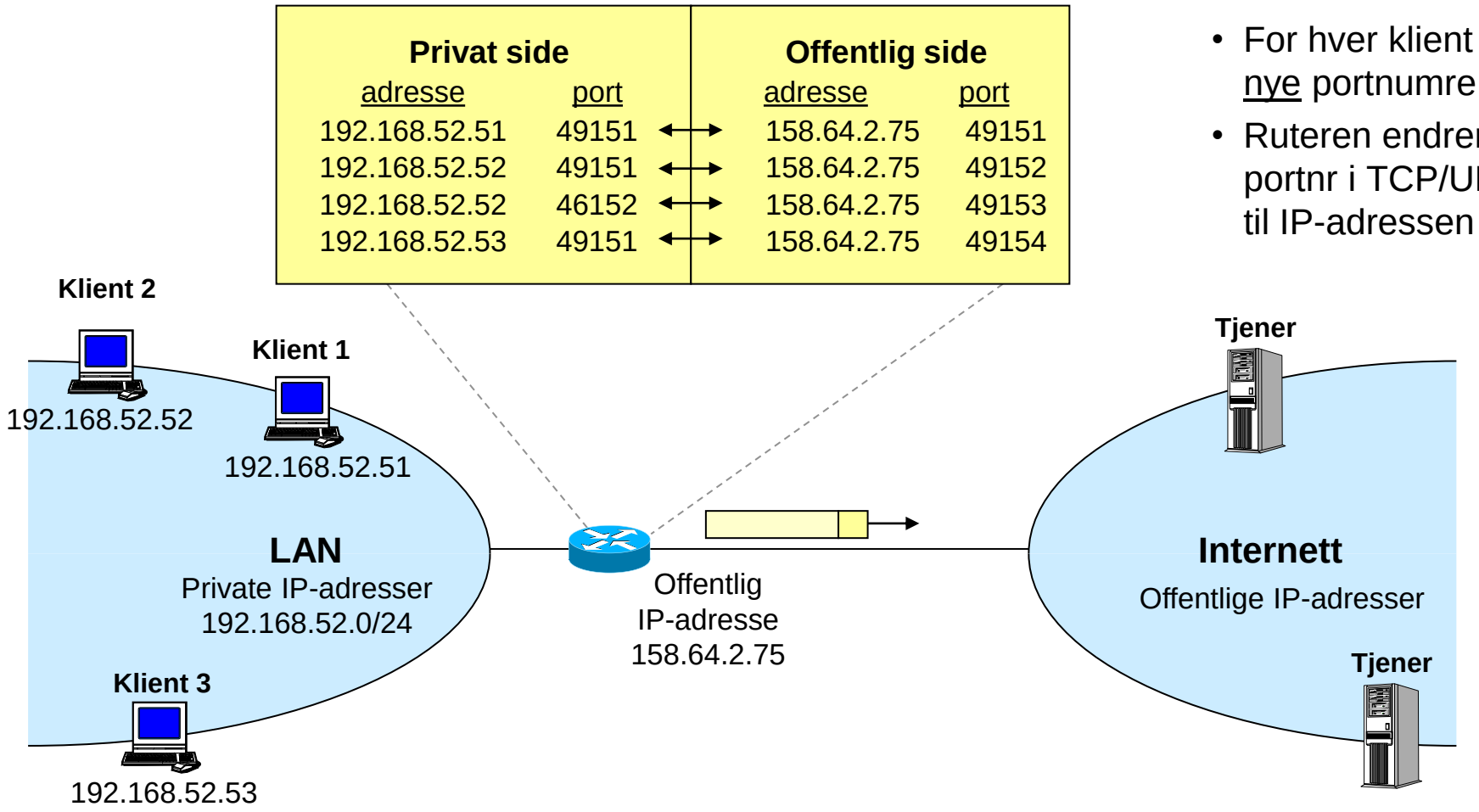
Løsning: NAT – Network Address Translation

- Ruter har én offentlig (offisiell) IP-adresse på ”yttersiden”
- Ruter oversetter private IP-adresser til sin offentlige (offisielle) IP-adresse
- Kun ruterens offentlige (offisielle) adresse er ”synlig” på Internett

Detaljer:

- Ruter endrer avsenderadresse på alle utgående IP pakker, til sin egen offentlige IP-adresse.
  - » Fra ”ytre nett” (Internet) ser det ut som om alle IP-pakker kommer fra ruteren!
- Alle innkommene IP-pakker vil ha ruterens offentlige IP-adresse som mottakeradresse
- Ruteren endrer mottakeradresse til riktig privat IP-adresse, før pakken sendes inn i LAN’et
- NAT kan også benyttes med flere offentlige IP-adresser på yttersiden

NAT bruker portoversetting



- For hver klient tildeler ruteren nye portnumre på yttersiden
- Ruteren endrer avsenders portnr i TCP/UDP-hodet i tillegg til IP-adressen i IP-hodet

Figuren er modifisert fra Frode Sørensen: *Innføring i nettverk*, IDG Books Norge

NAT bruker portoversetting

PAT – Port Address Translation

- Ruteren lagrer en tilstandstabell med alle portnummer og tilhørende private IP-adresse/portnr på innsiden
- Må brukes når NAT-ruteren kun har én offentlig (offisiell) IP-adresse på utsiden.
- Alle private socketadresser over-settes til en entydig offentlig socket-adresse.
- Hvert portnr på yttersiden tilsvarer én socketadresse på innsiden.

Fordeler/hensikter med PAT

- Flere maskiner kan dele én felles offentlig (offisiell) IP-adresse
  - » Reduserer behovet for offentlige IP-adresser
- Skjuler interne IP-adresser for tilgang fra ytre nett
  - » gir en viss form for sikkerhet, hindrer etablering av forbindelser fra utsiden

NAT'ing er også en sikkerhetsmekanisme

Ulemper med PAT

- Kommunikasjonen må initieres fra innsiden
  - » Klienter i ytre nett kan ikke kontakte tjenere i LAN'et (ingen info i tilstandstabellen)
  - » Dette kan løses med port forwardning (se neste foil)
- Forbindelsesfrie protokoller som UDP krever spesiell behandling
  - » Ruteren må reservere portnummeret i PAT-tabellen en viss tid for det kan gjenbrukes.
- Enkelte protokoller/applikasjoner vil fungere dårlig
  - » De som benytter varierende portnummer (f.eks. FTP, Oracle Net)
  - » IP-tunnellering (VPN / IPsec)

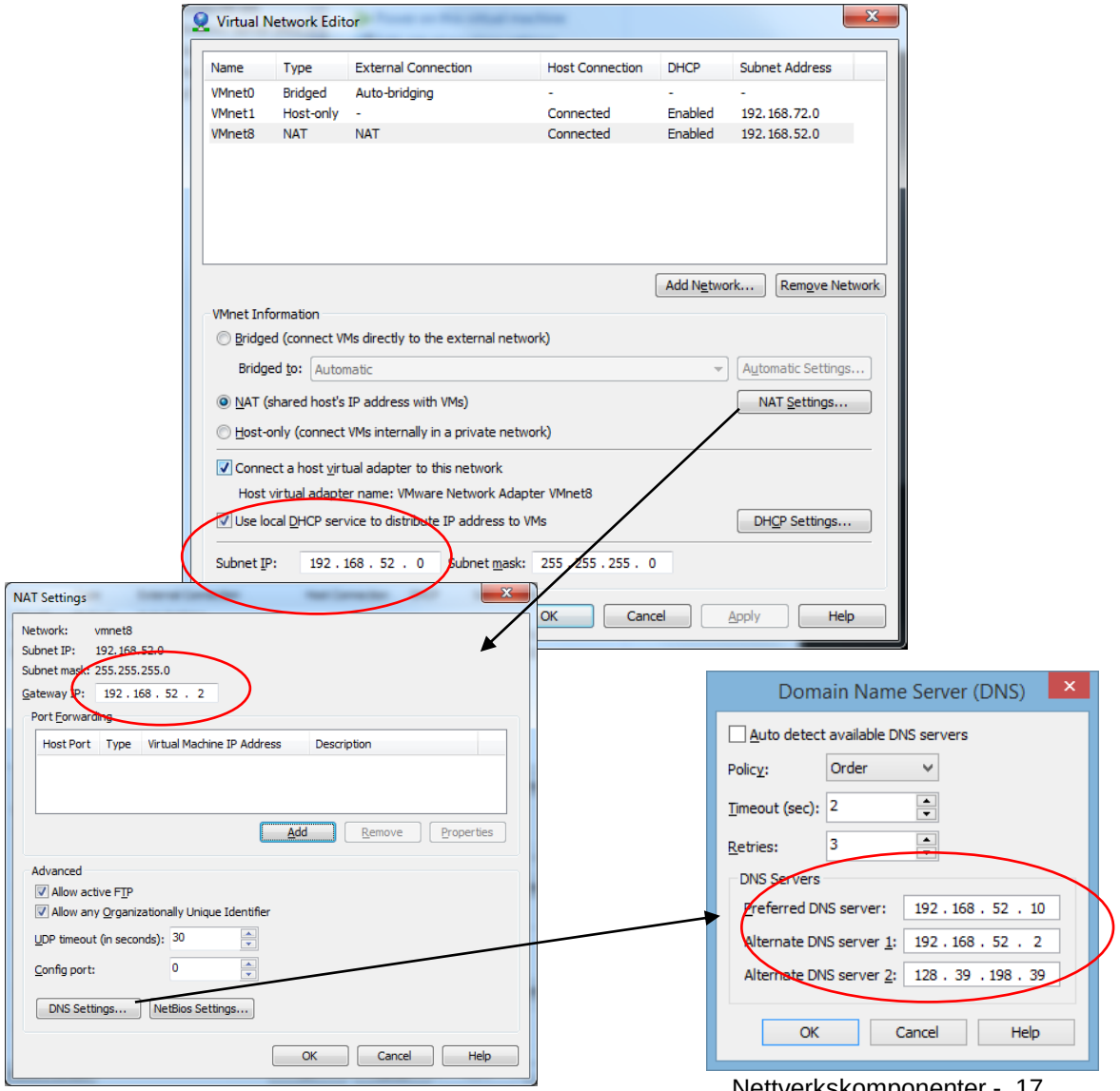
NAT i VMWare Virtual Network Editor

VMWare fungerer som ruter med adresseoversetting (NAT)

- Defineres under **VMNet8** som er NAT-nettet
  - » IP-nett/maske (Subnet IP og mask)
    - definerer adresseområde for NAT-nettet

Under NAT Settings kan du velge

- IP-adresse for default ruter (Gateway IP)
  - » Bestemmer VMWares adresse i NAT-nettet
- DNS Settings
  - » IP-adresse til DNS-tjenere
  - » Disse blir delt ut av DHCP til klienter i NAT-nettet



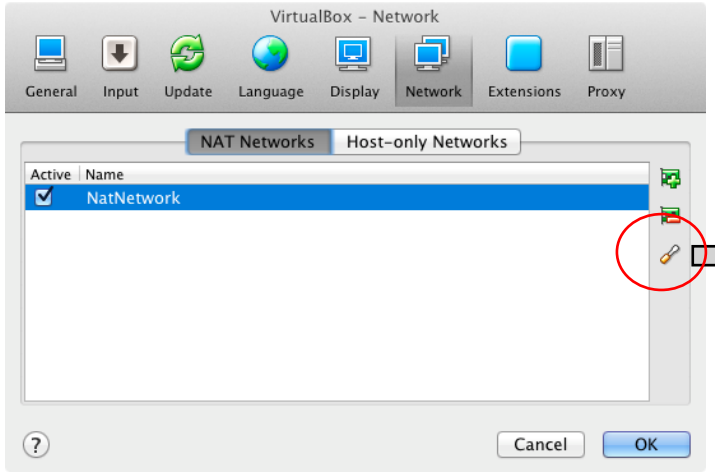
NAT i VirtualBox

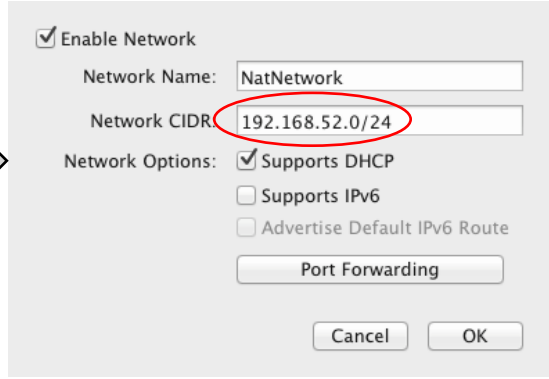
VirtualBox fungerer som ruter med adresseoversetting (NAT)

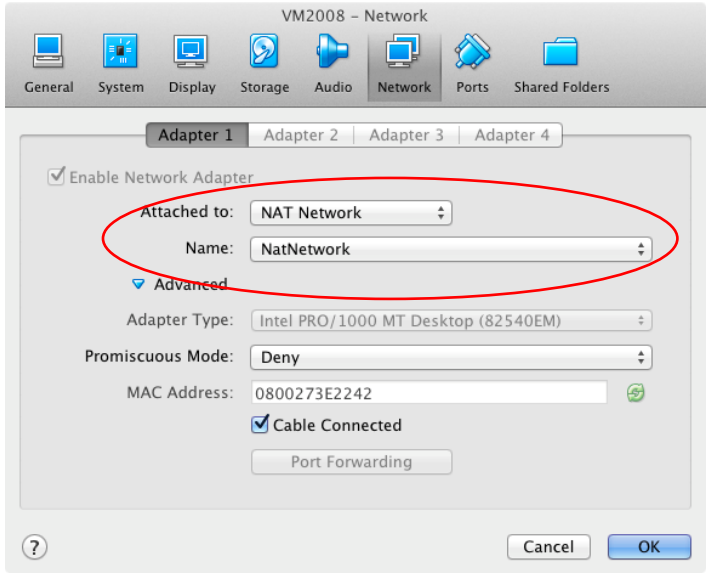
- Defineres under *Preferences – Network*
- DHCP-tjener i VB kan aktiveres/deaktiveres
- Adresser velges automatisk basert på det IP-nettet du oppgir for NAT-nettet.
  - .1 er adresse til ruteren i VB (som er default gateway i NAT-nettet)
  - .2 er adresse til DNS tjeneren i VB

Machine → Settings → Network

- Du må plassere VM'ene i NAT-nettet
- VM'ene kan få IP-adresse manuelt (statisk) eller fra DHCP-tjener i VirtualBox

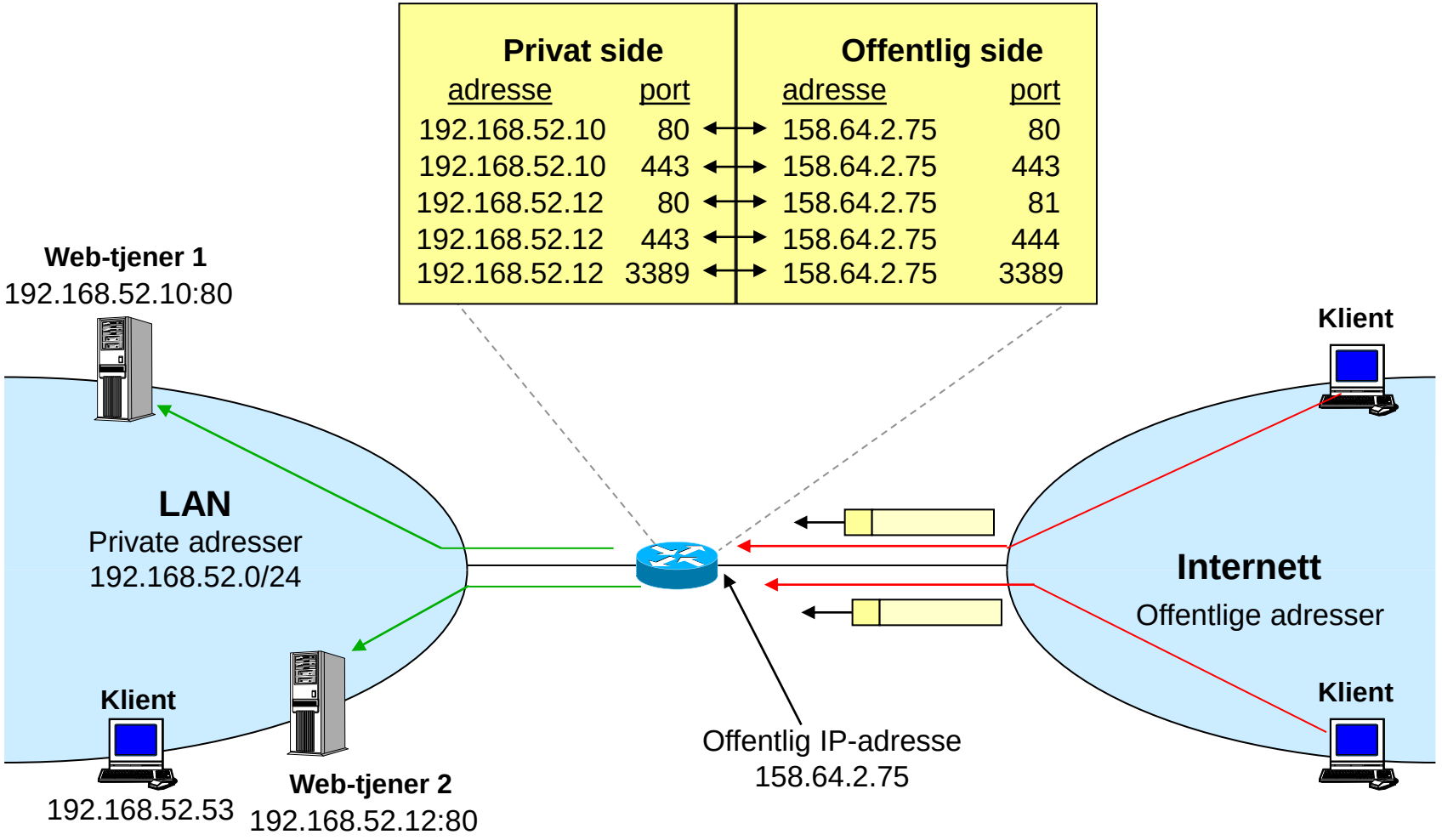






Skjermbilder fra Mac

Portforwarding gir tilgang fra utsiden



Figuren er modifisert fra Frode Sørensen: *Innføring i nettverk*, IDG Books Norge

Portforwarding gir tilgang fra utsiden

Problem:

- Hva om vi ønsker å nå en tjener i indre nett, fra en klient utenfor?
- Vanlig NAT tillater ikke TCP/UDP trafikk som initieres utenfra
  - » Fordi de private IP-adressene er skjult for maskiner i ytre nett
  - » Fordi ruteren ikke kan vite hvilken indre adresse man ønsker å nå

Løsning: Port forwarding

- Ruteren kan lagre en tabell over hvilke IP-adresser+portnr som skal nås utenfra
  - » Tabellen må konfigureres manuellt i ruteren!
- Klienter i ytre nett kontakter ruterens IP-adresse, som om den var tjeneren
- Ruter videresender pakker til riktig privat IP-adresse i LANet.

Eksempel: Webtjener i indre nett skal kunne nås utenfra

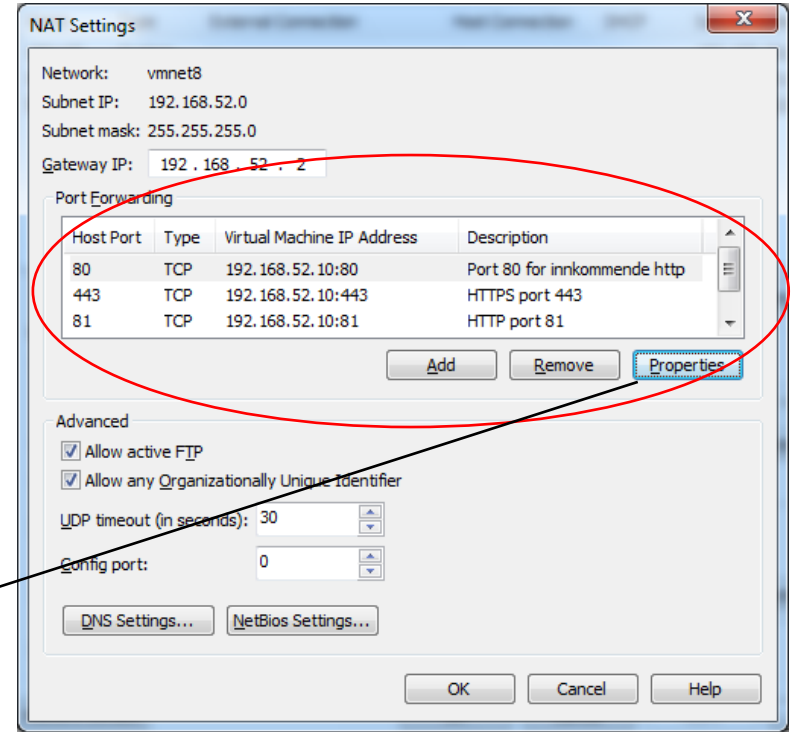
- Webtjeners private socketadresse: 192.168.52.10:80
- Ruters offentlige (offisielle) IP-adresse på utsiden: 158.64.2.75
- Ruter lagrer følgende videresendingsinformasjon: 158.64.2.75:80 →192.168.52.10:80
- Klienter i ytre nett kontakter 158.64.2.75:80
- Ruter videresender pakkene til 192.168.52.10:80

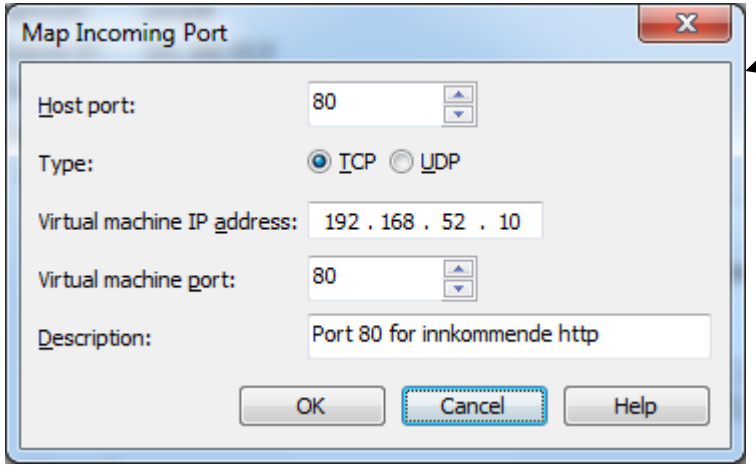
Portforwarding i VMWare

Videresendingsregler defineres i NAT Settings

For hver regel definerer du:

- Portnummer (*Host port*) og transportprotokoll (*Type*) i ytre nett
- IP-adresse det skal videresendes til i indre nett (*Virtual machine IP address*)
- Portnummer det skal videresendes til i indre nett (*Virtual machine port*)
- Navn på regelen (Description)





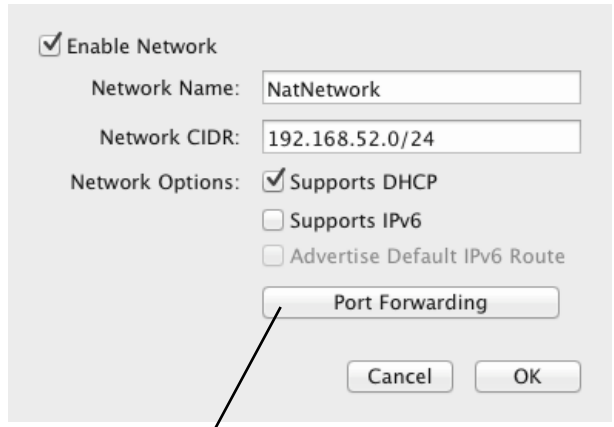
Portforwarding i VirtualBox

Videresendingsregler defineres under Port Forwarding

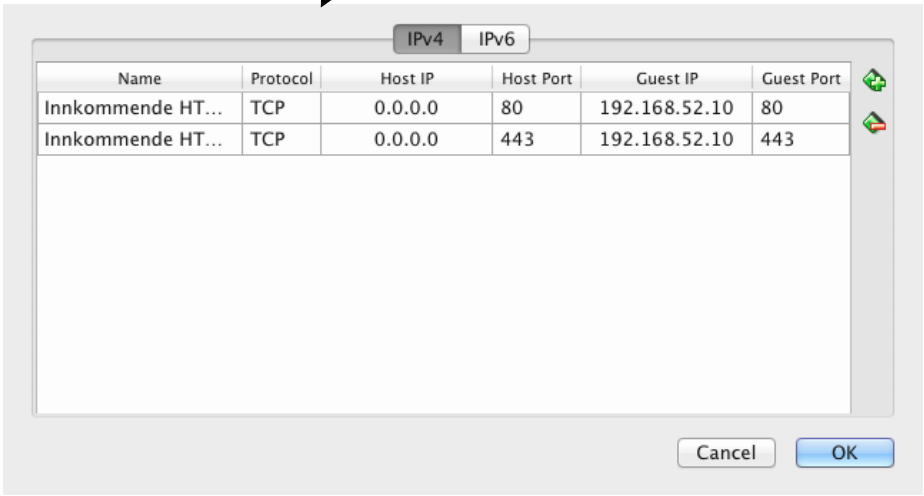
- I vinduet for NAT-nettet

For hver regel:

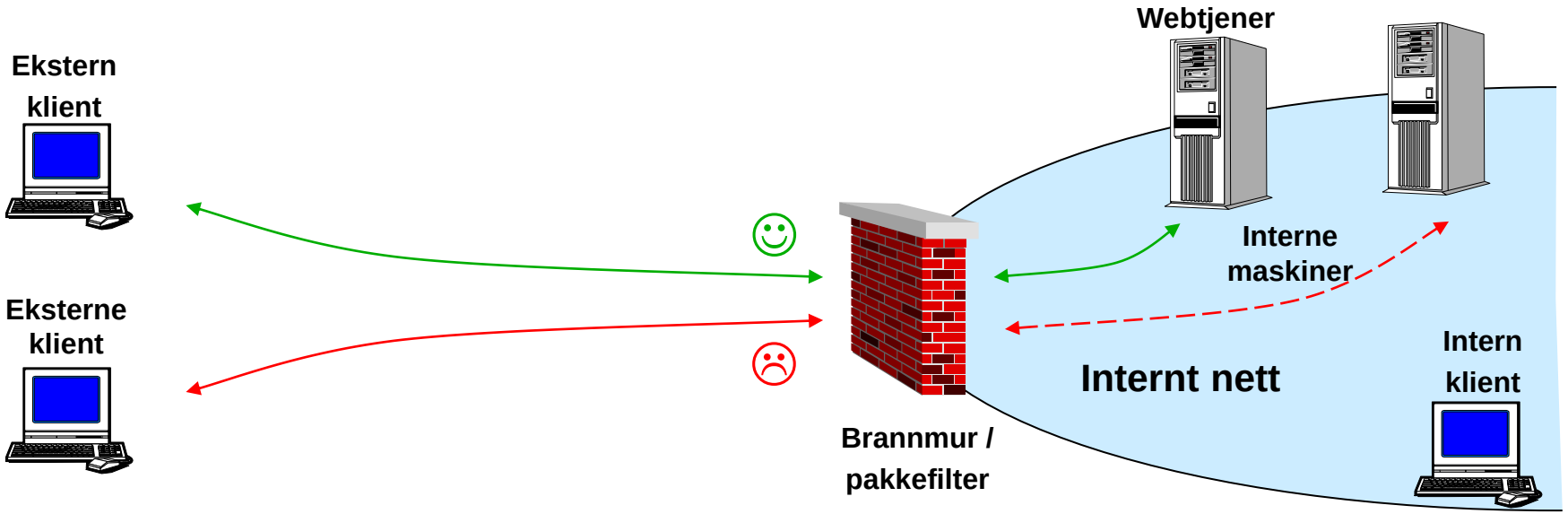
- *Navn* på regelen
- *Transportprotokoll*, *IP-adresse* og *portnummer* (i ytre nett)
  - » 0.0.0.0 betyr alle maskinens IP-adresser i ytre nett
- IP-adresse for videresending i indre nett (*Guest IP*)
- Portnummer for videresending i indre nett (*Guest Port*)



Skjermbilder fra Mac



Brannmur / pakkefilter



Formål

- Stoppe uønsket trafikk inn/ut av lokalnett
- Slippe gjennom ”lovlig” trafikk

Brannmur / pakkefilter

En brannmur filtrerer bort "uønsket" trafikk

- Bare pakker som samsvarer med gitte kriterier slippes gjennom
- Alle andre pakker stoppes i ruteren

Filtreringskriterier

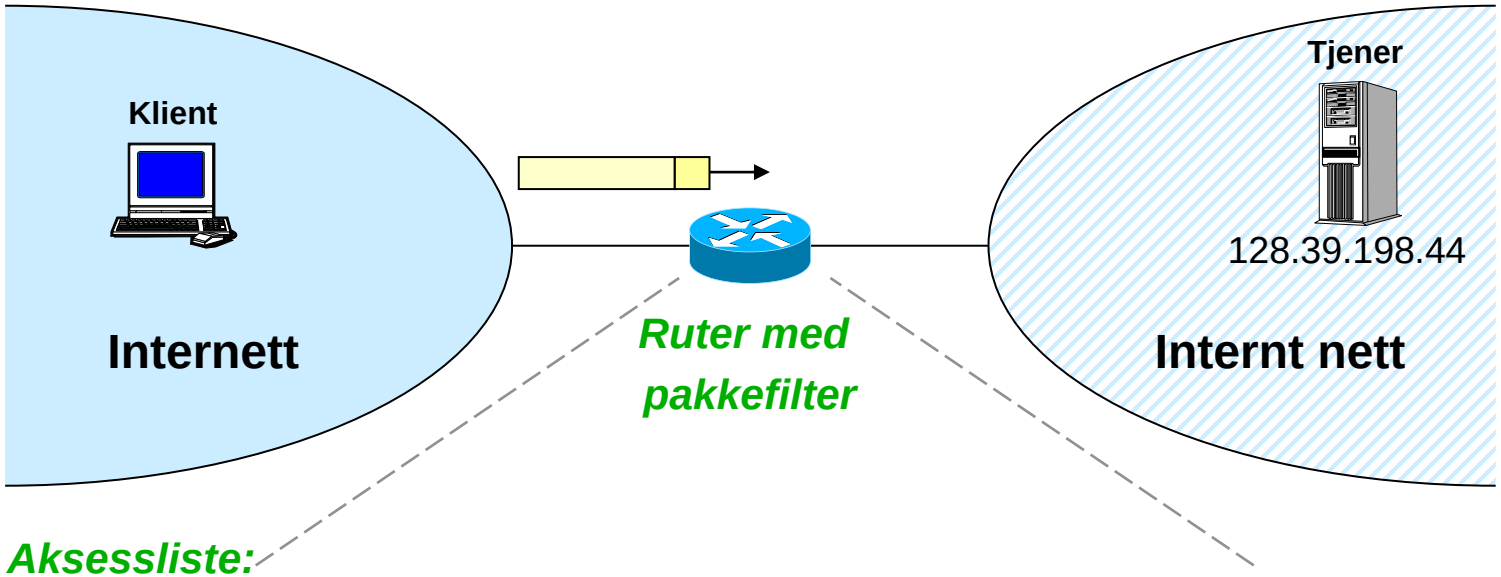
- IP-adresse / portnummer til avsender og mottaker
- Protokolltype / -nummer
- Kommunikasjonsretning (inn/ut)
- Initieringsretning – hvilken side av brannmuren startet kommunikasjonen

En brannmur jobber på flere OSI-lag fordi den kan bruke info i pakkehodene fra flere lag

Aksessliste (ACL-Access Control List)

- Tabell som viser hvilke pakker som skal slippe gjennom (filtreringsregler)
- Konfigureres manuellt i brannmuren
- Eksempel:
  - » slipp gjennom innkommende http trafikk til webtjeneren i det interne nettet
  - » slipp gjennom all utgående http trafikk fra det interne nettet

Brannmur / pakkefilter



Aksessliste:

Pakke-retning	Mottaker adresse	Mottaker port	Avsender adresse	Avsender port	Protokoll
Inn	128.39.198.44	80	alle eksterne	>49150	TCP
Ut	alle eksterne	>49150	128.39.198.44	80	TCP
Inn	alle interne	>49150	alle eksterne	80	TCP
Ut	alle eksterne	80	alle interne	>49150	TCP

Innkommende HTTP-trafikk

Utgående HTTP-trafikk

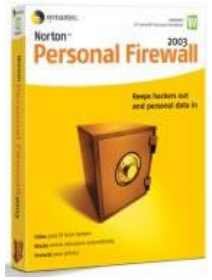
Brannmurer

Nettverksbrannmur / ruterbrannmur

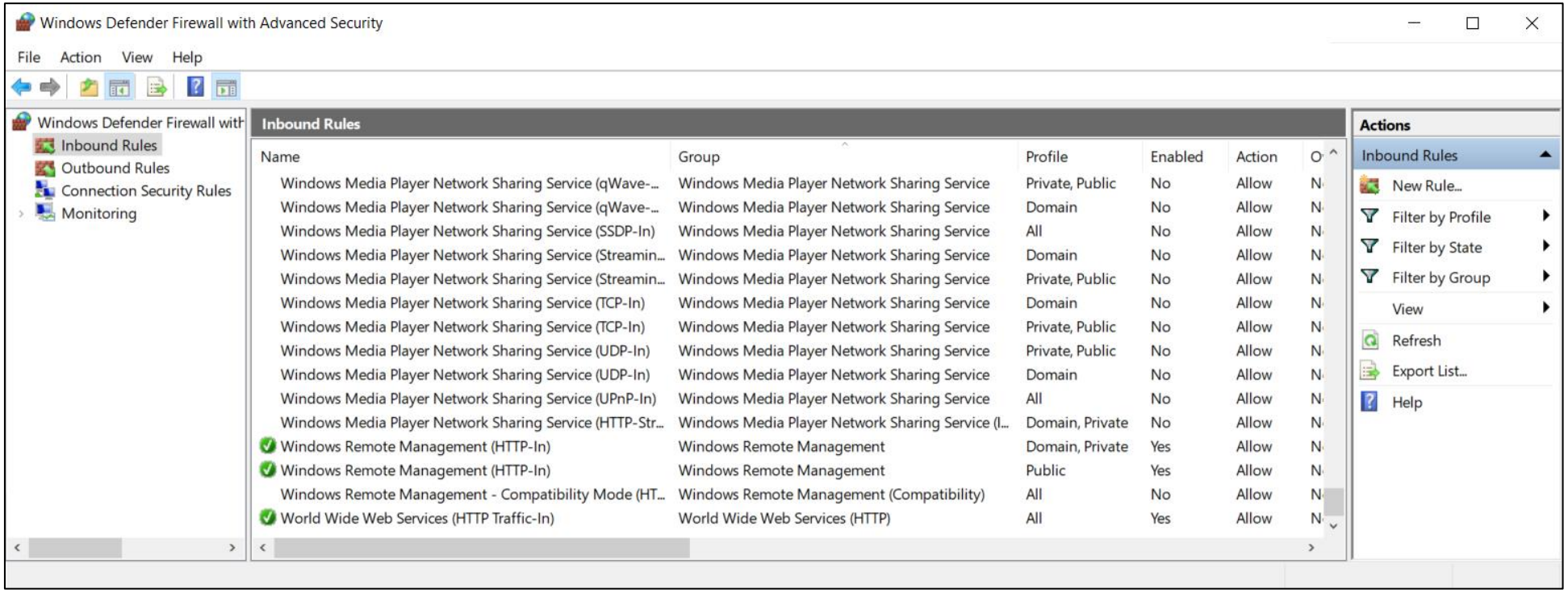
- Spesielle "hardwarebokser", eller programvare på en dedikert maskin / ruter
  - » Plasseres mellom LAN og WAN
  - » Inneholder ofte ruter, pakkefilter og evt. NAT
- Beskytter hele nettverket på innsiden av brannmuren
- Pris: 5000 – 100.000 kr.
- Utfordring: Stor trafikkmengde krever svært hurtig prosessering av pakker dersom brannmuren ikke skal bli en flaskehals med forsinkelse!

Vertsmaskinbasert brannmur (lokal brannmur)

- Programvare som installeres på én maskin og beskytter kun denne
  - » Inneholder kun pakkefilter for trafikk til / fra denne maskinen (ikke ruter eller NAT)
- Eksempler:
  - » Windows Firewall
  - » Norton Personal Firewall
  - » F-Secure Firewall
- Pris: Noen hundrelapper



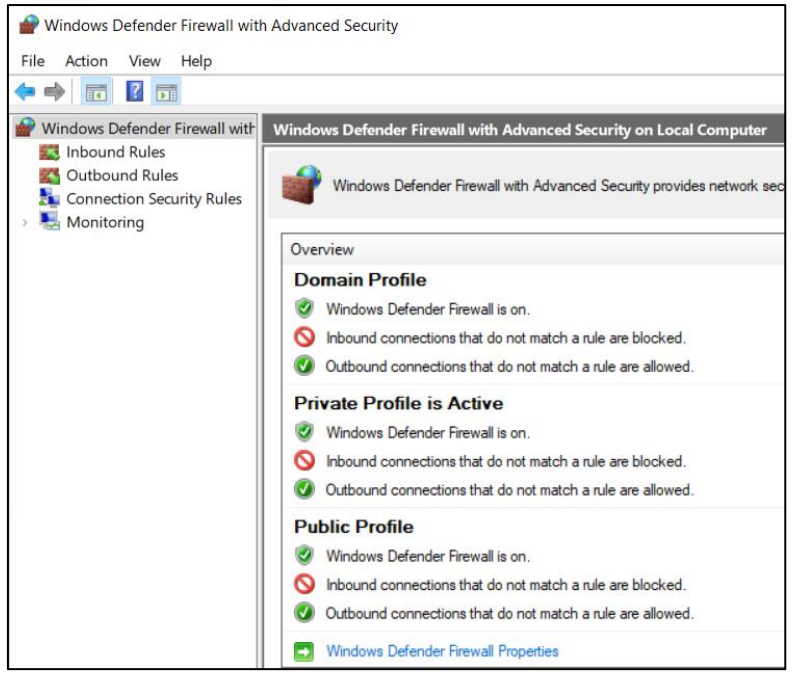
Brannmur i Windows Server

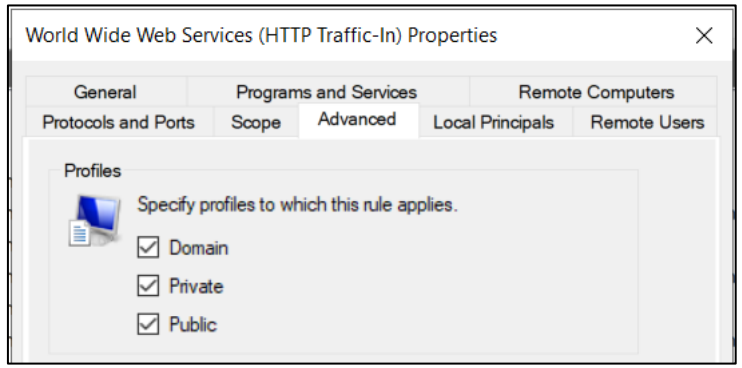


Demo:

- Profiler
- Inngående og utgående brannmurregler
- Brannmurregler / filtere
- Gyldighetsområde (scope)
- Logging i brannmuren

Brannmurprofiler





Domain Profile

– Gjelder når maskinen brukes i et AD domene og har tilgang til domenekontrolleren i domenet.

Private Profile

– Gjelder i private nettverk. I utgangspunktet er ingen nettverk private, men brukeren kan definere en nettverksplassering som privat, f.eks. et hjemmenettverk

Public Profile

– Gjelder når maskinen brukes i alle andre nett utenfor eget domene. For eksempel hvis en bærbar maskin brukes i et offentlig trådløst nett på reise.

Brannmurinnstillinger kan settes for hver profil

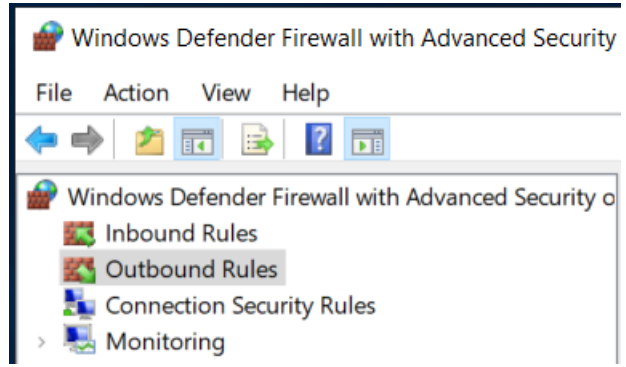
Innkommende og utgående brannmurregler

Innkommende regler

- Gjelder kommunikasjon som er **initiert fra** ”utsiden” av brannmuren
  - » Dvs. klientprogrammet er på andre maskiner i nettverket

Utgående regler

- Gjelder kommunikasjon som er **initiert fra** fra ”innsiden” av brannmuren
  - » Dvs. klientprogrammet er på maskinen som kjører brannmuren

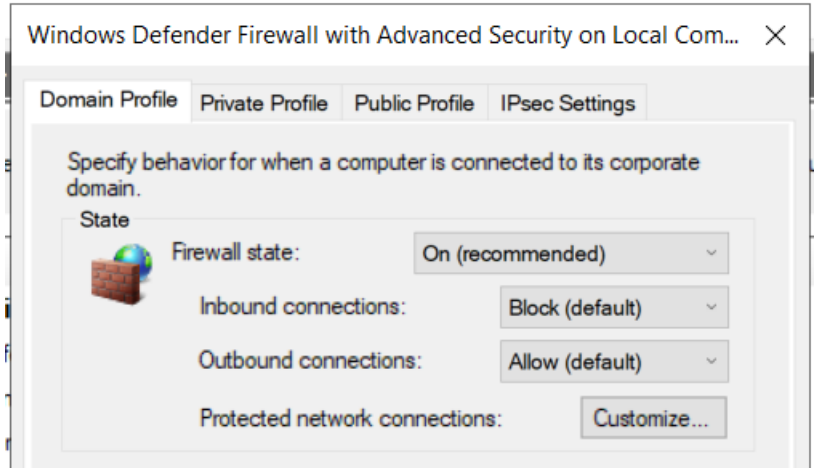


Obs! Reglene gjelder pakker som går "begge veger"

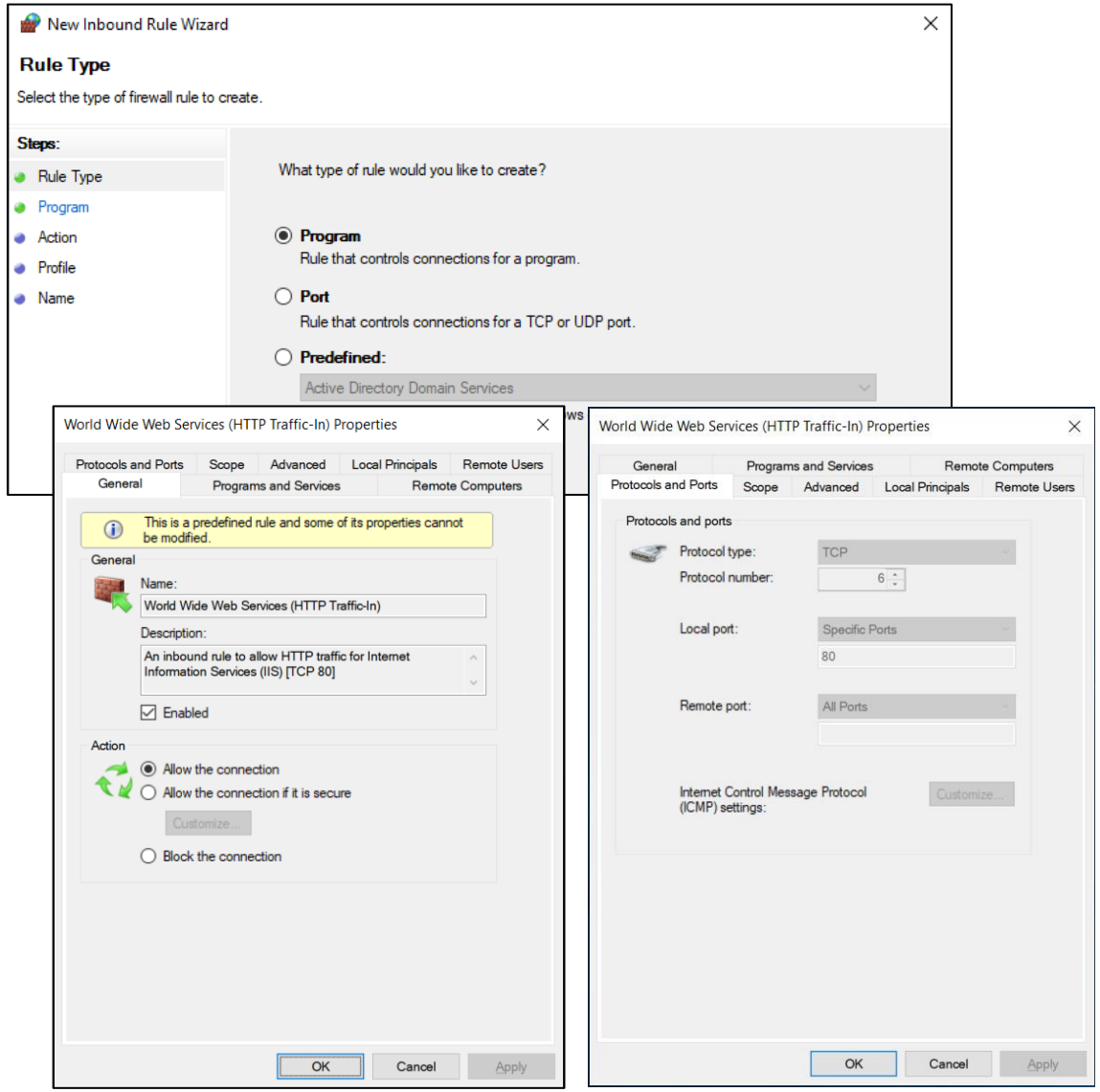
- Dvs. både til og fra klient-/tjenerprogram

Standardinnstillinger i Windows Firewall:

- Alle utgående forbindelser tillates
- Alle innkommende forbindelser blokkeres
  - » Regler må åpnes manuelt
  - » Windows åpner mange regler "automatisk" ved installasjon av tjenerroller/-funksjoner



Brannmurregler



Fire regeltyper:

Program

- Gjelder all trafikk til/fra en bestemt *programfil*

Port

- Gjelder for trafikk til/fra én bestemt TCP eller UDP port.

Predefined

- Ferdigdefinerte brannmurregler i Windows tilpasset bestemte Windows-komponenter.

Custom

- Defineres manuelt med en kombinasjon av program og portnummer.

Brannmurregler

Gyldighetsområde (scope)

Avgjør hvilke avsendere / mottakere brannmurregelen skal gjelde for.

- Alle maskiner i nettet
- Enkelte IP-adresser
- Et helt IP-nett (subnett)
  - » eks: 192.168.52.0/24
- Et adresseområde (range)