TCP/IP

25. Juli 1996

Indholdsfortegnelse

1. Indledning

TCP/IP er en netværks-uafhængig transport protokol, der tilbyder følgende:

Remote Login	At logge på en anden host
Remote execution	at udføre processer på en anden computer end den man er logget ind på.
File transfer	at overføre filer fra host til host
Remote Boot	Boot af diskløse enheder over nettet

Man kan desuden indhente oplysninger om hvilke hosts, der er tilgængelige og hvilke brugere, der er logget ind på dem.

I 1969 udviklede Det amerikanske forsvarsdepartement, DoD, et netværk kaldet ARPANET. Dette blev i 70'erne videreudviklet til TCP som er en netværksuafhængig implementation af ARPA protokollen, der leverer højniveau protokol services og applikationer.

I 1980 opstod "Internettet", et verdensomspændende net af netværk, fortrinsvis bestående af forsknings- og uddannelsesinstitutioner og firmaer, der bidrager til det amerikanske forsvar.

Internettet voksede hurtigt til over 2.000 netværk i 1989 med over 100.000 hosts, og det antal er mangedoblet til adskillige millioner i dag.

Ethvert netværk i Internettet får tildelt en entydig internetadresse fra centralt hold, således at enhver host i dette net får en internetadresse, der begynder med de samme tal.

En Internet adresse består af 4 tal i intervallet mellem 0 og 255:

Der findes forskellige kategorier af net i internettet:

Klasse A: Starter med fra 1 - 127
Første tal til netadr. og de tre sidste til hostadr.
Subnetmaske: 255.0.0.0
Eksempel: 89.1.5.9, hvor 89.0.0.0 er netadressen

Klasse B: Starter med fra 128 - 191
De to første tal til netadr. og de to sidste til hostadr.
Subnetmaske: 255.255.0.0
Eksempel: 152.95.64.200, hvor 152.95.0.0 er netadressen

Klasse C: Starter med fra 192 - 223
De tre første tal til netadr. og det sidste til hostadr.
Subnetmaske: 255.255.255.0
Eksempel: 205.54.98.64, hvor 205.54.98.0 er netadressen

Klasse D: Starter med tal større end 224
28 bit til gruppeadr.

Klasse E: Reserveret til eksperimentel brug.

Antallet af netværk i hver klasse og antallet af hosts i hvert af disse netværk er altså begrænset:

Der kan højst findes 127 net af Klasse A, og hvert af disse kan have over 16 mio. hosts.

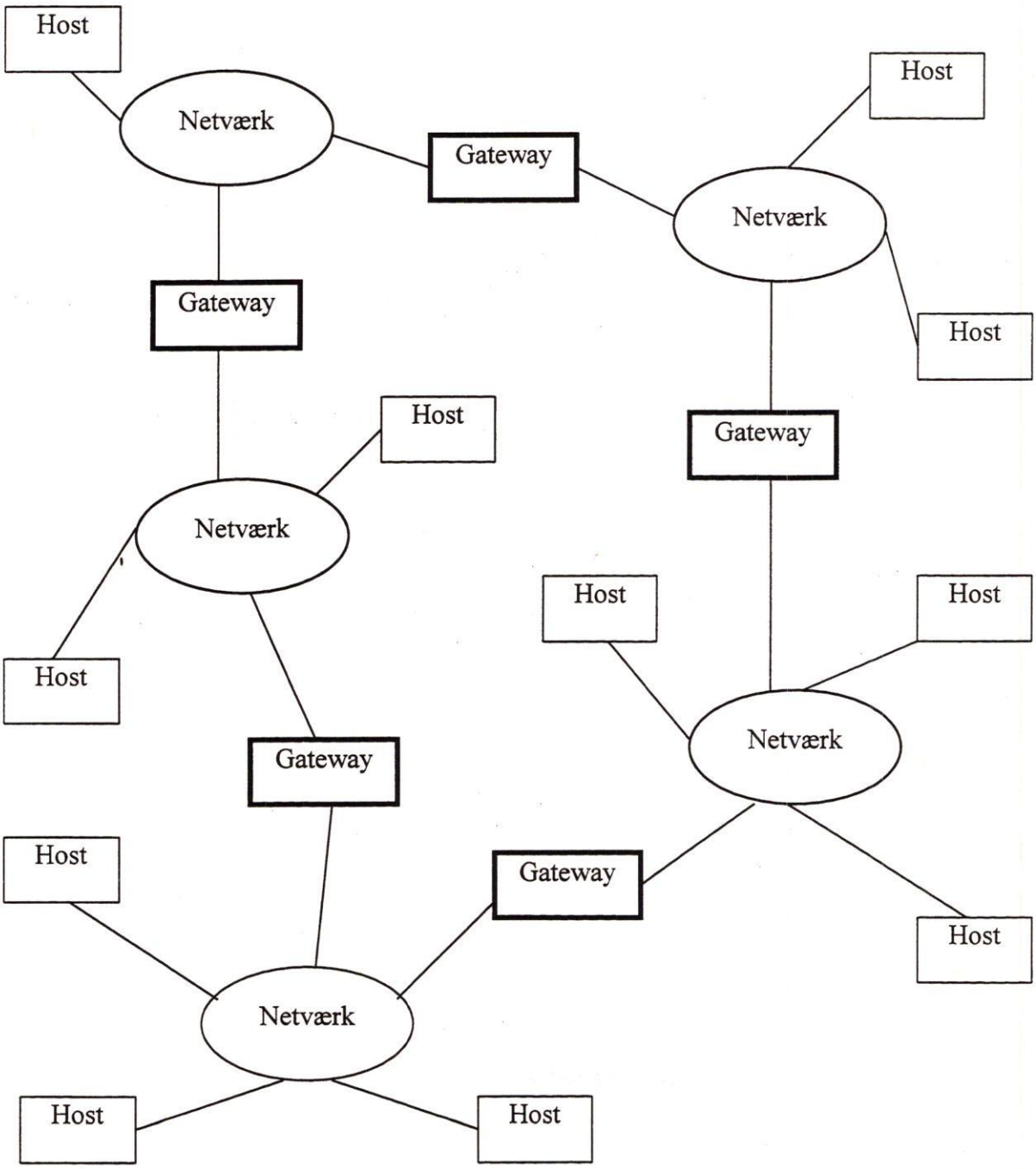
For klasse B netværk er tallene 16.384 net med maximalt 65.536 hosts, og for klasse C, 2 mio. net med maximalt 256 hosts.

Et eksempel på en internet adresse på en host i et klasse A netværk kunne være: 89.1.0.1, mens en host i et klasse B netværk kunne hedde 129.1.2.3 og én i et klasse C netværk kunne hedde 199.142.3.1.

Internet adresser, der ender med 255 eller med 0 er **broadcast adresser**. F.eks. vil 152.95.255.255 være en broadcast til hele nettet 152.95.0.0, og 152.95.64.255 vil være en broadcast til subnettet 152.95.64.0. (Mere om subnet senere).

2. Internettet

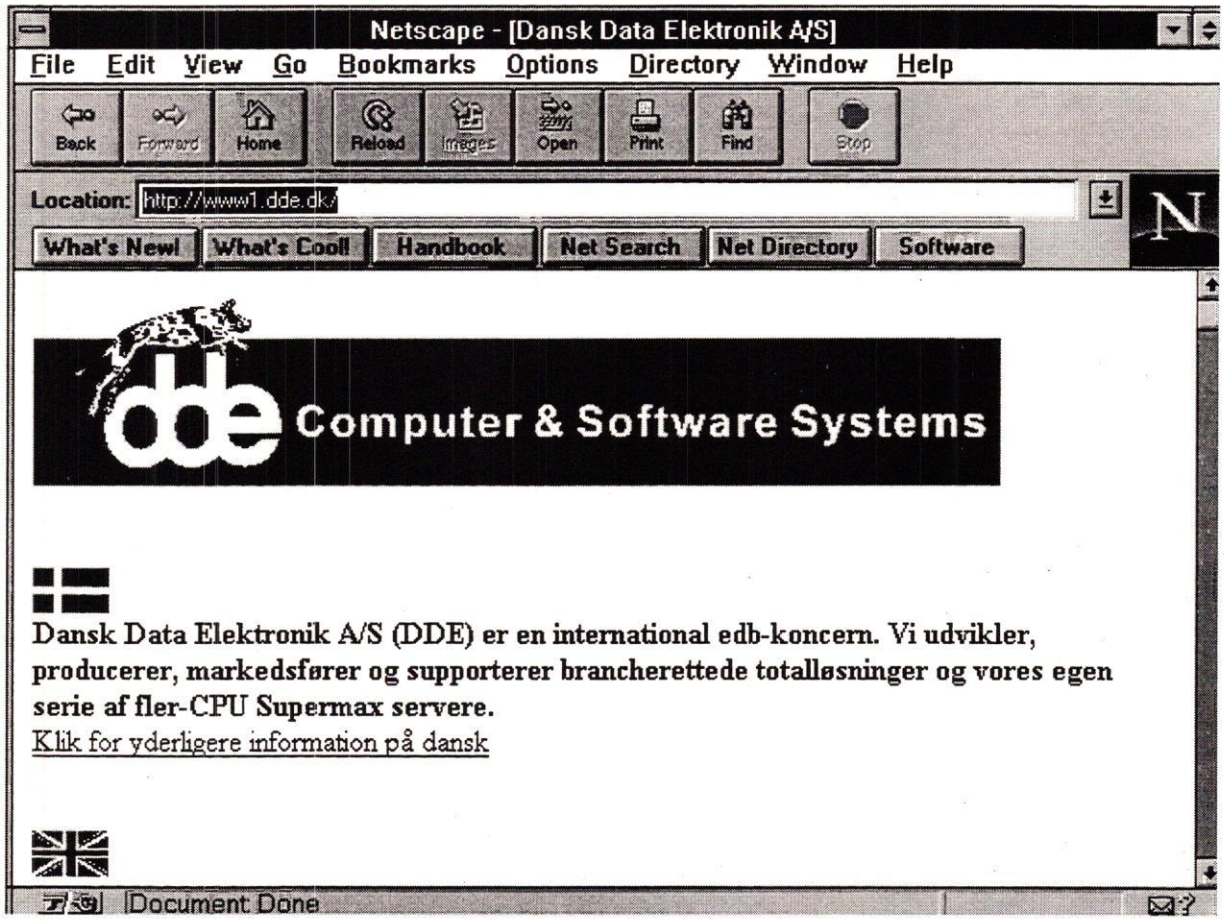
Internettet er som nævnt et verdensomspændende netværk af TCP/IP netværk forbundet ved hjælp af gateways.



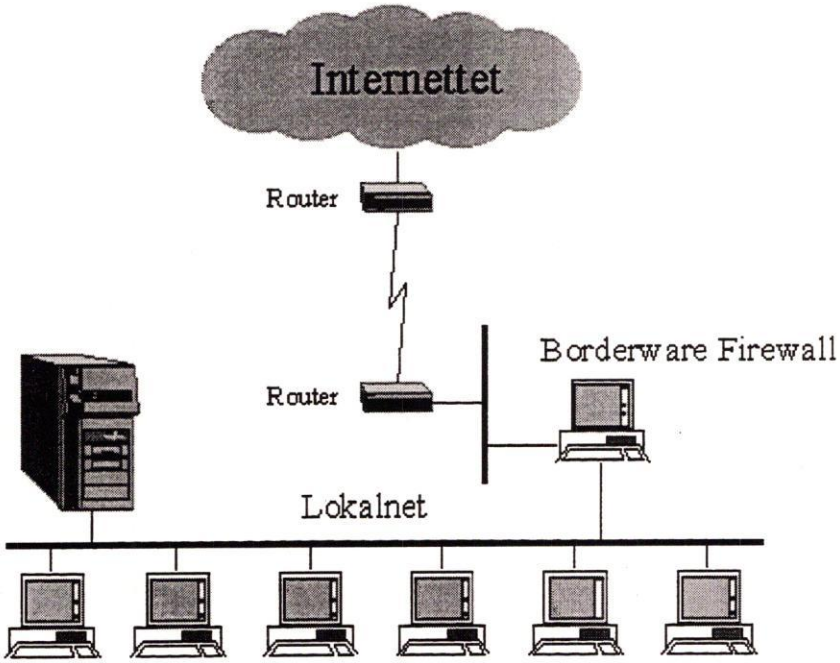
I starten benyttede man hovedsageligt tegnbaseret kommunikation til at søge informationer, hente filer, logge på etc. ved hjælp af Internettet.

Nu benytter man som oftest en sk. **Browser**, som er et program, der giver en grafisk grænseflade til søgning på forskellige **WEB servere** etc. på Internettet. (WWW ~ World Wide Web ~ Verdensomspændende spindelvæv).

De mest benyttede browsere er Netscape, Mosaic eller Microsoft Internet Explorer.



Når man sætter sin server op på internettet åbner man også op for sikkerheden, således at andre nu kan få adgang til denne. For at sikre at ingen kommer uautoriseret ind på serveren, opsætter man typisk en **Firewall**.



På denne figur er firewall'en en ekstra server, der er opsat, men en firewall kan være en softwarepakke, som man installerer på sin gateway, eller man kan benytte filtre i routerne.

3. Ordliste

Når man snakker transport protokoller, er der et væld af forkortelser og gloser, der benyttes. Her er en hjælp til at forstå alle disse.

ARP **Address Resolution Protocol, RFC 826**. En broadcast protokol brugt til at opløse Internet adresser til fysiske net adresser (f.eks. Ethernetadresser).

ARPA **Advanced Reaserch Projects Agency** under det amerikanske forsvar.

BOOTP En protokol, der benyttes til at bestemme IP adresse på hosten selv og en boot server og navnet på en passende bootfil.

Browser En browser er et program, som kan benyttes til at "surfe" på internettet ved hjælp af en grafisk brugerflade. Af kendte browsere kan nævnes: Netscape, Mosaic, Microsoft Internet Explorer.

DDN **Defence Data Network**. Det vidt forgrenede net for det amerikanske Department of Defence.

Domain **Domain Name Protocol, RFC 1034, RFC 1035.** Definerer mapningen mellem hostnames og Internet adresser på en central location.

Ethernet **Ethernet** eller **IEEE 802.3** er et net baseret på en access metode kaldt **CSMA/CD**. Ethernet blev oprindeligt udviklet af Xerox Corporation i 1972. En specifikation blev udgivet i 1980 . Denne specifikation, kaldet "Den blå bog", var basis for **CSMA/CD LAN**, der blev udgivet i 1983.

Ethernet adresse En 48 bit identifikation af en enhed. Hver enhed i et net skal have en entydig adresse. De højeste bit kendetegner som regel producenten. Visse reserverede adresser har specielle betydninger. En adresse bestående af kun 1-taller (FF-FF-FF-FF-FF-FF), er en broadcast adresse, der sender til samtlige enheder

Firewall Maskinel/programmel, der forhindret uautoriseret adgang til eget netværk fra resten af Internettet.

Gateway En enhed, der forbinder to net. Kan være en host, der kan snakke med begge net, og således har 2 IP adresser.

HTML **Hyper Text Markup Language**. Et dokumentformat, der benyttes til at skrive dokumenter, der skal ligge på WEB servere.

ICMP **Internet Control Message Protocol, RFC 792**, brugt af Gateways.

IEN **Implementation for Engineering Note**, svarende til en RFC. Et forslag til en Internet Standard.

Internet adresse (eller **IP adresse**) En 32 bit adresse, der identificerer enheder på net, der benytter Internet Protokollen.

IP **Internet Protocol, RFC 791**. Det laveste niveau af **ARPA** protokollen.

Java Et programmeringssprog, der vinder hurtigt frem, til at skrive programmer, der kan vises ved hjælp af en browser.

LAN **Local Area Network**. Et net, hvor flere enheder er forbundet fysisk med kabler, typisk Ethernet coaxial kabler.

Pakker Enheder af information, der indeholder en "header", med adresser og information om behandling, og en besked.

Port Bestemmelses sted for kommunikationen.

POP Post Office Protocol. En af Internet mail standarderne. For at en bruger skal kunne modtage E-mail, skal denne have en såkaldt E-mail konto på en E-mail server. Det program, som brugeren benytter til at læse og behandle E-mail, afvikles i mange tilfælde på en anden computer. POP specificerer, hvordan E-mail clienten identificerer sig over for serveren, og hvordan E-mail'en overføres fra serveren til clienten.

Protokol Et sæt regler, data formater og konventioner, der bestemmer overførslen af data.

Proxy Server
En server, der udfører en opgave "på vegne af" et clientprogram eller en anden server. Typisk fungerer en firewall som proxy server, idet den kan hente information på Internettet på vegne af computere på lokalnettet.

RFC **Request for Comment.** En standard fra DDN.

Router Et stykke hardware, der opdeler en lokalnet i flere subnet eller forbinder ét netværk med et andet. Man kan f.eks. opdele sin trafik ved hjælp af routere, således at man nægter adgang for visse protokoller/brugere til et subnet.

RWHO/RUPTIME Berkeley protokol brugt til at sende **UPTIME** over **UDP.**

TCP **Transmission Control Protocol, RFC 793.** Benyttes til at tildele transport service i **ARPA** protokol familien.

TELNET **ARPA** applikations niveau protokol, **RFC 854, RFC 855**. En to-vejs, byte orienteret kommunikations protokol.

TFTP **Trivial File Transfer Protocol, IEN 133**. Denne protokol overfører filer uden at kontrollere rettigheder.

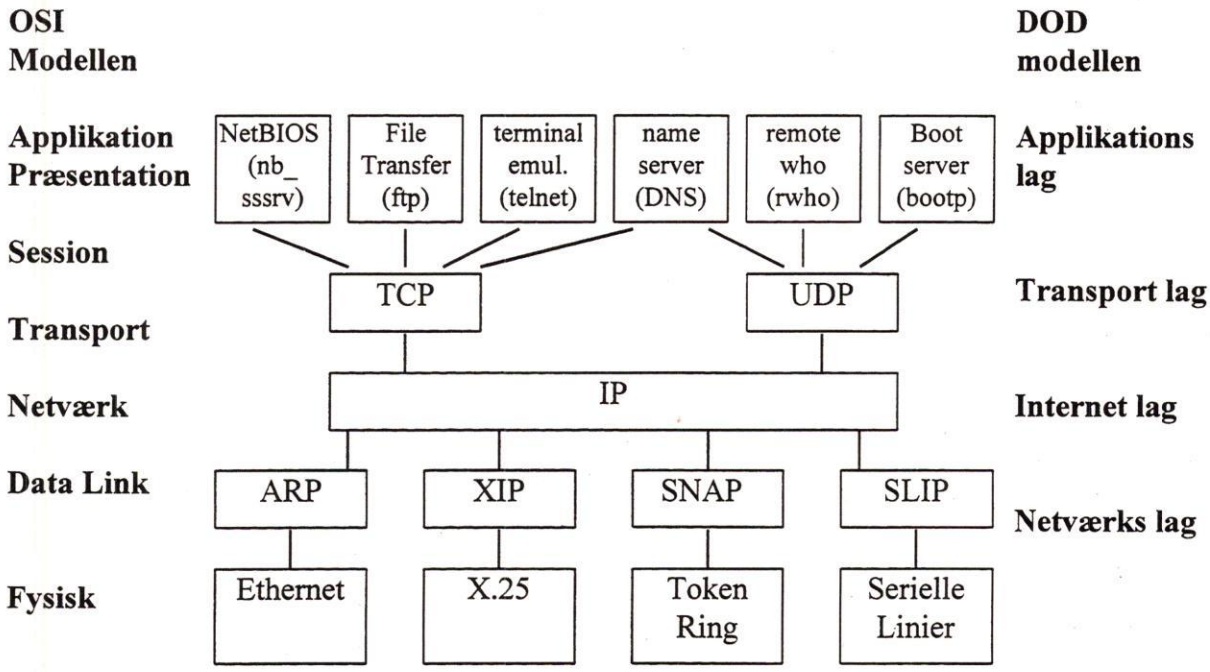
Transceiver En elektronisk kobling mellem et coaxial kabel og et dropkabel.

UDP **User Datagram Protocol, RFC 768.** Denne protokol tilbyder datagram service over Internet protokollen.

WAN **Wide Area Network**. Computers, der er placeret langt fra hinanden, men er forbundet med f.eks. telefonlinier.

WWW En **World Wide Web** Server viser HTML dokumenter i en grafisk brugerflade ved hjælp af en Browser.

DOD og OSI Modellen



4. Adresser

Data, der sendes rundt i nettet, sendes i pakker. Disse pakker er mærkede med kontrol information, så som adressen på afsenderen.

4.1 Ethernet adresser

Hver host i nettet har en entydig fysisk adresse. F.eks. på et Ethernet har hver host en entydig **Ethernet adresse** på 12 hexadecimale tal:

02608C406C8C

Ethernet adressen er for PCer og printere med netkort bestemt af netkortet, for Supermax'er er den bestemt af MIOC'en eller NIOC'en og for NTC'er er den bestemt af NTC'ens netkort.

4.2 Internet adresser

Internettet er et net bestående af en lang række sammenhængende TCP/IP net.

Hver host har en **Internet adresse** (eller en **IP adresse**), der består af 4 heltal (32 bit) adskilt af punktummer:

89.11.1.33

Hvert af disse heltal kan være mellem 0 og 255.

De første felter (1, 2 eller 3) bestemmer nettets adresse, og skal være det samme for alle hosts på samme net. Ved net tilsluttet Internettet, tildeles netadressen centralt, så man sikrer, at to forskellige net ikke får samme netadresse.

Det sidste felt/felter af IP adressen udpeger hosten i det pågældende net.

Internet adressen er uafhængig af typen af net (Ethernet, X25, ...), men de Gateways, der forbinder de enkelte net, skal være i stand til at håndtere de forskellige typer net, og deres forskellige adresseformater.

4.3 Sammenhængen mellem ethernetadr. og IP adr.

IP adresse vil for enhver host være defineret i en fil afhængig af hosttype, og for PCers vedkommende også af, hvilken type TCP der anvendes.

Supermax Her defineres sammenhængen mellem MIOCens ethernetadr. og IP adr. i /etc/netconf, hvis der er flere MIOCer på maskinen vil filnavnet indeholde MIOCens unitnummer f.eks. /etc/netconf.5 eller /etc/netconf_5.

NTC Sammenhængen bliver defineret, når NTCen konfigureres gennem POM. Konfigurationen for NTCen vil ligge i kataloget /usr/pomsys/lib/objects i filen for denne NTC type (f.eks. ntc8). Afhængig af NTCens prom kan sammenhængen også defineres i /etc/bootptab.

PC Afhængig af hvilken TCP der anvendes, benyttes følgende filer:

MS TCP-32 til WFW	c:\windows\system.ini
MS TCP (16-bit) til WFW	c:\windows\protocol.ini
MS TCP (16 bit) til LM 2.2	c:\lanman.dos\protocol.ini
Windows 95	i registry
Windows NT	i registry

For diskløse PC'er defineres sammenhængen i filen /etc/bootptab. (Se herom senere).

PRINTER Printere med netkort defineres i filen /etc/bootptab eller i printerens setup. Printere uden netkort er ikke defineret som hosts, de kobles op via en NTC.

TCP kommandoen **arp** kan give oplysning om, hvordan Ethernet adresser og Internet adresser hænger sammen på net:

arp -g

Internet Address	*Ethernet Address*	*Type*	*Life*
89.11.1.33	*02-60-8C-40-6C-8C*	*temp*	*5 mins*
89.11.0.1	*08-00-75-A1-00-27*	*temp*	*8 mins*
89.11.0.10	*08-00-75-A1-00-74*	*temp*	*2 mins*
89.11.0.12	*08-00-75-A1-00-38*	*temp*	*4 mins*
89.11.0.13	*08-00-75-A1-00-40*	*temp*	*3 mins*

Brugerne behøver ikke være klar over hverken Internet adresser eller Ethernet adresser på nettet. De kan i stedet benytte **hostnames**.

4.4 Hostnames

Et hostname er et symbolsk navn, som knyttes til hver host. Hostnames er lokale for nettet, og de tildeles af netadministratoren.

F.eks. kan hosten med Internet adressen 89.11.0.10 have hostname unv2, mens hosten med Internet adressen 89.11.1.33 hedder JST.PC.

Der gælder følgende regler for hostnames:

- **Et hostname kan bestå af op til 32 alfanumeriske tegn**
- **Det første tegn skal være et bogstav**
- **Alle hostnames på nettet, skal være forskellige på de første 9 pladser, da utility programmerne kun benytter de første 9 tegn**
- **Der skelnes mellem store og små bogstaver**

4.5 Opløsning af hostnames til IP adresser

Opløsningen af hostnames til IP adresser kan ske på to forskellige måder:

- ved hjælp af en hostsfil
- ved hjælp af DNS (Domain Name Service)

4.5.1 Domain name server

Hvis man ønsker at anvende DNS, skal man opsætte en eller flere servere som **Nameserver**, og alle clienter skal sættes op til at anvende denne nameserver.

Hver gang en client benytter et hostname, vil den først forespørge nameserveren om IP adressen, og derefter vil den kunne benytte denne til den videre kommunikation.

En UNIX host sættes op til at bruge nameserver ved at redigere filen /etc/resolv.conf. Her skal der ligge mindst to linier.

- Én, der angiver domain navnet
- Én eller flere linier, der angiver IP adresse på nameserveren(e)

F.eks.

```
domain dde.dk
nameserver 152.95.16.1
nameserver 152.95.24.1
```

Når man kører med DNS skal man have et domain navn.

Domain navne fås fra den nationale myndighed, hvis man er tilsluttet Internettet.

F.eks. har DDE domain navnet: **dde.dk**, mens kursusafdelingen har domain navnet **kursus.dde.dk**, som er en underinddeling af dde.dk.

Sidste del af domain navnet er typisk to tegn, der angiver landekode, og i USA har man endelser på 3 tegn:

xxx.edu	Education - Uddannelsesinstitutioner
xxx.com	Commercial - Kommercielle virksomheder
xxx.net	
xxx.gov	Governement - Statslige institutioner

Hver host i et domain har et "fully quallified domain name", FQDN, således at hosten JST-PC i DDE's domain har FQDN JST-PC.dde.dk, og brugernes E-mail adresser angives også ved hjælp af domain navnet. F.eks.: jst@dde.dk

I Windows for Workgroups, Windows 95 og NT skal man også angive domain name og Nameserver. For Windows for Workgroups gøres det vha **Netværksinstallation**, og for de to sidstnævnte gøres det fra **Kontrolpanel**, **Netværk**.

Opsætning af selve nameserveren kan vi desværre ikke komme ind på på dette kursus.

4.5.2 Hostfil

Beliggenheden for hostfilen afhænger af hvilken platform, man benytter:

UNIX	/etc/hosts
Windows for Workgroups	C:\WINDOWS\HOSTS
Windows 95	C:\WINDOWS\HOSTS
NT	C:\WINNT\SYSTEM32\DRIVERS\ETC\HOSTS

I denne fil skal der findes en linie for hver host i nettet, der angiver hostnavn og IP-adresse:

```
# Host Database
#
127.0.0.1    loopback
89.18.0.1    kaka localhost
89.11.0.10    unv2
89.11.0.11    unv4
89.11.0.1    mother m
```

Der skal være en linie med IP adressen **127.0.0.1** og host navnet **loopback**. Denne linie giver adgang til hosten selv.

Den lokale host skal have et alias (skrives i 3. ord på linien) **localhost**.

Enhver host kan angives med ét eller flere alias

Hvis ikke en host er defineret i hostfilen, kan man ikke benytte **hostnavnet**, men er tvunget til at benytte **IP adressen** i stedet.

Opgave

formål: *- at kigge på adresser*

1. **Find IP-adresse og ethernet adresse på din PC ved at benytte kommandoen IPCONFIG /ALL fra en DOS prompt.**

2. **Hvilken klasse netværk er der tale om?**

3. **Find IP-adressen på serveren ved at pinge den på hostnavnet. (Benyt kommandoen ping <server>).**

4. **Hvilke hostsnames er kendt af serveren? Kan du finde din egen PC? Hvorfor tror du ikke det er nødvendigt, at alle PC'erne er i serverens hostfil.**

5. UNIX Systemfiler

5.1 Konfiguration af nettet på en Supermax multiserver

På enhver UNIX maskine vil man have en konfigurationsfil for TCP/IPen. På en Supermax Multiserver kan man fra indgangen **sysadm config** komme ind til menuen for netværks konfiguration.

Under punktet **kernelconfig**, defineres ethernet konfigurationen, det vil sige, hvor mange ethernet moduler og deres placering på MIOCen/MIOCerne. Desuden defineres eventuelle SLIP (Serial Line Internet Protocol) linier og interfaces til X.25 linier (XIP).

Hvis der installeres f.eks. et nyt ethernetmodul skal punktet **setup** under **network configuration** anvendes. Dermed ændres der i ethernet konfigurationen, og man skal altså ikke selv ind og rette i **kernelconfig**.

Hvis der er tilføjet nye netværks-interfaces, skal dette tilføjes under punktet **ipconfig** i menuen **netconfig**. Her skrives i filen /etc/netconf.

Efterfølgende skal indgangen **netcreate** under **netconfig** menuen udføres, for at effektuere ændringer foretaget i kernekonfigurationen og netkonfigurationen, og nettet skal stoppes og startes. Netcreate genererer en ny /etc/netconf fil.

5.1.1 /etc/netconf

Filen benyttes til at definere internet adressen på hosten og konfigurationen af hosten, og benyttes af netdæmonen **/etc/netd**. Ved start af nettet læser netdæmonen /etc/netconf og downloader moduler og drivere i MIOCen.

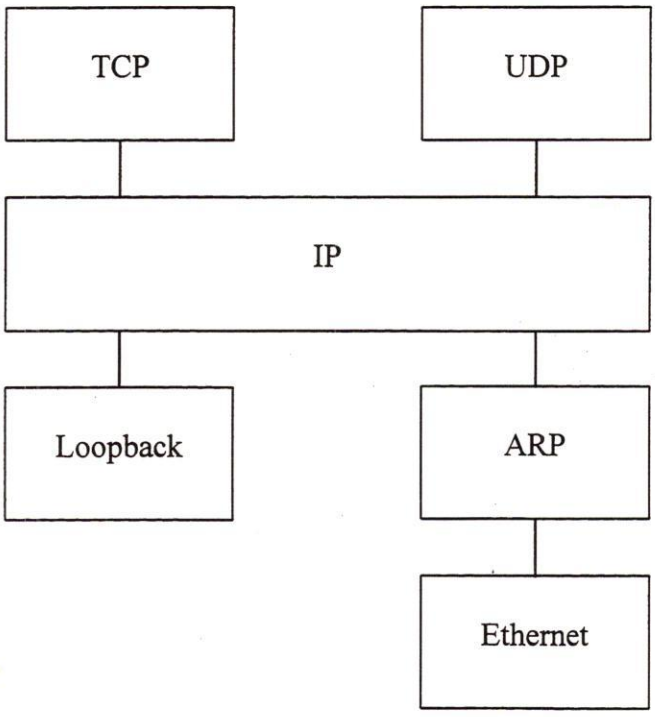
Den standard **netconf** fil, der skrives ved installationen, vil normalt være passende, så lav ingen ændringer, uden at det er nødvendigt.

Der oprettes en netconf fil for hver MIOC. F.eks. /etc/netconf.6 og /etc/netconf.8 for MIOCer med unitnumrene 6 og 8.

Hvis man skal ændre i filen, skal man **altid** benytte **sysadm, packagemgmt, stcpmgmt, config**.

Filen indeholder følgende:

- **Navne og sammenhæng mellem moduler og drivere i streams.**
  Standard er TCP og UDP over IP, IP over Loopback og ARP, ARP over Ethernet.



Dette skal kun ændres, ved tilføjelse af flere net interfaces, så som en seriel linie, der vil kræve en SLIP driver for hvert interface til hosten, eller TCP/IP via X.25, der vil kræve en XIP driver.

- **Internet adressen skal specificeres**

- **Subnet masken**
  Standardværdien er 0. Denne behøver man kun angive, hvis nettet er et subnet.

- **Broadcast forwarding support**
  Kun nødvendig, hvis hosten skal være gateway mellem flere net. Standard værdien er **n**.

- **Keepalive support**
  Standardværdien er **y**. Denne skal være **y**, hvis man ønsker, at keepalive pakker skal sendes over etablerede TCP forbindelser, der ikke har været sendt data over i et stykke tid. Dette kunne f.eks. være en PC, der slukkes, mens den kører terminalemulering til en host via telnet.

- **Pakkestørrelse**
  Den maksimale størrelse på pakker, som hardware må sende. Denne kan sættes til standardværdien 0, som betyder at den maksimale pakkestørrelse, vil blive som defineret af hardware.

  Man kan ændre denne størrelse, hvis der opstår problemer med den størrelse, der er bestemt udfra hardware.

- **Trailer encapsulation**
  Standardværdien er off.

  Trailer pakker er konstrueret til at lade systemet minimere lager til lager kopiering, hvor det er muligt.
  Trailer encapsulation protokol klarer dette ved at skrive en "header" information efter selve datablokkene.

  Trailerne slås til ved at skrive følgende:

  arp eth0 APR_TYPE=trailers

  Hosten vil genkende trailer-pakker, der fremsendes, uanset om trailer transmission er enablet for nettet.

Eksempel på **netconf** fil:

```
#ident " (#)SupermaxTCP netconfig 3.5 5/21/91"
# netd configuration file

tcp     d       /dev/tcp
udp     d       /dev/udp
ip      dc      /dev/ip
arp     m       arp
eth0    dc      /dev/eth
loop    d       /dev/loop

slip0   d       /dev/slip0
xip0    d        /dev/xip

%%

tcp     ip
udp     ip
ip      loop    IP_NET{127,0,0,1,,}

ip      arp     IP NET={89.18.0.1,0,0,0,0,forwb=n,kalive=y,0 }
arp     eth     ARP_TYPE
```

Filen i dette eksempel er fra en maskine med én MIOC. Hvis en maskine har mere end en MIOC, vil MIOCens unitnummer afspejles i drivernes navne.

Ethernetdriver: eth0 dc /dev/eth.8
driver til ethernetmodul 0 på MIOC 8.

eth1 dc /dev/eth1.8
driver til ethernetmodul 1 på MIOC 8.

Hvis der kun er én MIOC, vil der ikke være nummerangivelse på /dev/eth eller /dev/eth1.

De samme regler vil være gældende for følgende drivere tcp, ip, udp.

F.eks.	tcp	dc	/dev/tcp.8
	ip	dc	/dev/ip.8
	udp	dc	/dev/udp.8

Drivere til eventuelle SLIP og XIP linier vil ligeledes være angivet med nummer på driverfilen, hvis der er mere end en MIOC.

Ved installation af TCP/IP på en Supermax med flere MIOCer promptes man for at sætte en default MIOC. Herved linkes /dev/tcp.8 til /dev/tcp, /dev/udp.8 til /dev/udp og /dev/eth.8 til /dev/eth.

Skal der anvendes en anden MIOC end default MIOCen, sættes indholdet af shell-variablen TCPIOC til nummeret på den ønskede MIOC

```
TCPIOC=6; export TCPIOC
```

Dette har betydning for kommandoen netstat og i øvrigt for hvilket netværk man arbejder på.

5.2 Konfiguration af nettet på en UNIX 4.2 maskine

På en UNIX rel. 4.2 maskine kan man aflæse net opsætningen med kommandoen:

```
ifconfig -a

lo0: flags=49<UP,LOOPBACK,RUNNING>
        inet 127.0.0.1 netmask ff000000
eth0: flags=23<UP,BROADCAST,NOTRAILERS>
        inet 152.95.64.104 netmask ffffff00 broadcast
              152.95.64.255
```

Her ses at loopback benytter IP adresse 127.0.0.1, og netmask er sat til ff000000, hvilket betyder, at subnetmaske er 255.0.0.0, da ff er 255 skrevet hexadecimalt. Hvert tal i en IP adresse modsvarer to hexadecimale cifre.

eth0 er ethernet interface, her beskrives at ip adressen er 152.95.64.104, netmasken er seks f'er og to nuller, svarende til subnetmaske 255.255.255.0, og broadcast adressen er 152.95.64.255.

Disse oplysninger ligger i filen **/etc/confnet.d/inet/interface** i de sidste linier:

```
lo:0:localhost:/dev/loop::add_loop:
eth:0::/dev/eth_0:netmask 0xffffff00
   broadcast 152.95.64.255 -trailers::
```

Skal man ændre disse, skal det ske ved hjælp af kommandoen **/etc/confnet.d/configure -i**, der nok kræver en tekniker ved hånden.

5.3 Netværks database filerne

Disse filer indeholder information om hosts, netværks protokoller, services og boot af diskløse PCer og evt. printere med netkort. De kan ændres på en Supermax Multiserver fra **sysadm tables** eller med **vi**.

DATABASE TABLES sysadm indgange		FILER
1 bootptab	update bootp database	/etc/bootptab
2 hosts	update internet host database	/etc/hosts
3 networks	update network database	/etc/networks
4 peruser	update per-user rhost database	.rhosts
5 protocols	update protocol database	/etc/protocols
6 services	update service database	/etc/services
7 system	update system equiv database	/etc/hosts.equiv
8 x25mapping	update IP/X25 address database	/etc/x25mapping

5.3.1 /etc/bootptab

Hvis man kører med diskløse PC'er, der skal boote over nettet ved at hente opstartsfilerne fra en server, skal PC'erne være forsynet med en Boot Prom i tilknytning til netkortet.

En Boot Prom er en Programmerbar ROM (Read Only Memory), der kan broadcaste PC'ens ethernetadresse ud over nettet, hvorefter serveren ved hjælp af bootp dæmonen svarer ved at sende IP-adressen på PC'en og hvilket bootimage (opstartsfil), der svarer til netop den PC.

Herefter anmoder PC'en om at få sendt bootimage, og Serveren sender denne ved hjælp af tftp.

Et bootimage for en PC er en "kopi" af en systemdiskette med helt ordinære opstartsfiler, **AUTOEXEC.BAT, CONFIG.SYS** og **COMMAND.COM** lavet ved hjælp af et program **CRTDSK**, og lagret på serveren.

På serveren skal der i filen **/etc/bootptab** ligge en række oplysninger om de PC'er, der kan boote herfra. Filen benyttes af bootp dæmonen.

Printere med netkort skal være indskrevet i denne fil, hvis de skal bootes via nettet. Bootimage til printeren leveres fra printerleverandøren, hvis den er nødvendig.

Desuden skal x-terminaler bootes over nettet fra /etc/bootptab.

NTCer bootes normalt som netserver, det vil sige med de definitioner NTCen er oprettet med i POM, men kan også bootes med bootp, hvilket vil sige, at NTCen bootes fra /etc/bootptab. Bootmetoden er afhængig af NTC'ens prom.

Filen /etc/bootptab er opdelt i to sektioner adskilt af et **%**. Linier, der starter med #, er kommentarlinier.

I den første del findes to linier:

- **det katalog, hvor bootfilerne ligger**
- **den bootfil, der benyttes som standard.**

I den anden del af filen ligger en linie i filen for hver PC. En sådan linie indeholder følgende oplysninger:

<hostnavn> <hw-type> <hw-adr> <ip-adr> <bootfil>

hvor:

- **hostnavn** hostnavnet på den client, der er beskrevet
- **hw-type** er typen på nettet, sædvanligvis 1 for 10 Mb Ethernet
- **hw-adr** er ethernet adressen i 6 hexadecimale bytes, f.eks. 08-00-39-73-68-2D
- **ip-adr** er IP-adressen på clienten
- **bootfil** er en parameter, der kan bruges til at angive navnet på den bootfil, der skal bruges af clienten. Er den ikke angivet, benyttes den standardværdi, der er angivet i den første del af filen.

Eksempel på en **/etc/bootptab** fil:

```
##########################################################################
#
# SupermaxTCP - Network utility
#
# Copyright 1989  Spider Systems Limited
# Copyright 1991  Dansk Data Elektronik A/S
#
# BOOTPTAB
#
# Example bootp table file, database for bootp daemon.
#
##########################################################################
#               (#)bootptab             3.5
# Blank lines and lines beginning with '#' are ignored.

# home directory
/usr/lib/stcp/bootfiles

# default bootfile
default

%%

# The remainder of this file contains one line per client interface
# with the information shown by the table headings below. First
# search is on internet address if specified in incoming request. If # not specified, hardware
address is used.
# The 'host' name is tried as a suffix for the 'bootfile' when
# searching the home directory (e.g., bootfile.host).

# host      htype   haddr               iaddr       bootfile
router1     1       08-00-39-00-60-0E   89.0.5.9     router.1_0
router2     1       08-00-39-00-60-0F   89.0.5.10   router.1_0
bf          1       00-00-C0-05-57-23   89.6.1.0    scope0
lcc         1       00-00-C0-20-26-08   89.6.1.1    scope0
lea         1       00-00-C0-78-6D-23   89.6.1.2    scope0
hp4prt      1       00-00-C0-3B-34-2D   89.6.1.3
```

5.3.2 protocols filen

Denne fil indeholder information om protokollerne i internettet,
og skal normalt ikke ændres.

For hver protokol findes en enkelt linie med følgende information:

<Officielt protokolnavn> <protokolnummer> <aliases>

De enkelte felter i filen skal stå adskilt af tabs og/eller blanktegn.

Eksempel på **protocols** fil:

```
#ident "      (#)SupermaxTCP protocols 3.5 seq 2.1 2/14/91"
#
# Intern      et (IP) protocols
#
#
ip            0        IP          # internet protocol, pseudo protocol number
icmp          1        ICMP        # internet control message protocol
tcp           6        TCP         # transmission control protocol
udp           17       UDP         # user datagram protocol
```

5.3.3 services fil

Denne fil indeholder information om de services, der er kendt af Internettet, og skal normalt ikke ændres.

Den indeholder én linie for hver service med følgende format:

<officielt servicenavn><port nummer>/<protokolnavn><aliases>

Således at enhver service bliver knyttet sammen med et sk. portnummer.

Af services kan f.eks. nævnes:

telnet
ftp
tftp
smtp

Hvis man ønsker at "snakke FTP" med en server, kalder man således op på den port, der er defineret for FTP på serveren. Disse numre er standard, og bør absolut ikke ændres.

Eksempel på del af **/etc/services**:

```
#ident " (#)SupermaxTCP services 5.1 seq 1.1 25/10/91"
#
# Network services, Internet style
#
echo            7/udp           ping
echo            7/tcp           ping
discard         9/udp           sink null
discard         9/tcp           sink null
systat          11/udp          users
systat          11/tcp          users
daytime         13/udp
daytime         13/tcp
netstat         15/tcp
quote           17/udp          text
quote           17/tcp          text
chargen         19/udp          ttytst
chargen         19/tcp          ttytst
ftp             21/tcp          ftpd
telnet          23/tcp          telnetd
smtp            25/tcp          mail
time            37/tcp          timserver
name            42/tcp          nameserver
httpd           80/tcp                          #www-server
#
# UNIX specific services
#
portmap         111/tcp         portmapper      # nfs
portmap         111/udp         portmapper      # nfs
exec            512/tcp         rexec rexecd
login           513/tcp         rlogin rlogind
who             513/udp         rwho rwhod whod
shell           514/tcp         rsh rshd cmd
printer         515/tcp         spooler         # experimental
talk            517/udp
route           520/udp         router routed   # 521 also
uucp            540/tcp         uucp uucpd
orasrv          1525/tcp        oracle
nfs             2049/udp        nfsd
xwindow         6000/tcp
```

Opgave

Formål: - at se på konfigurationen af hosten

1. **List hosts-filen og se hvilken IP-adresse hosten mes-pc har.**

   Hvad hedder hosten med IP adresse 152.95.64.205?

2. **Hvilken IP adresse har kursusmaskinen?**
   I hvilke filer kan IP adressen aflæses?

3. **Hvilket nummer har servicen telnet? tftp? nfs?**

4. **Hvilken service har nummer 21? 6000?**

Herfra løses opgaven samlet!

5. **Tilføj hosten unv1 med IP adresse 152.95.64.101 til hosts-filen.**

   Ping unv1 og se om der "er bid".

6. TCP/IP kommandoer

Der findes flere forskellige TCP/IP kommandoer til at overvåge de forskellige hosts.

6.1 arp

Kommandoen **arp** kan bruges, til at liste hvordan Ethernetadresser og IP adresser er mappet til hinanden. Arp kommandoen er en generel TCP/IP kommando, men de options man kan benytte afhænger af TCP/IP versionen:

arp -g

Internet Address	*Ethernet Address*	*Type*	*Life*
89.7.0.1	*08-00-75-A1-00-11*	*temp*	*3 mins*
89.11.1.33	*02-60-8C-40-6C-8C*	*temp*	*9 mins*
89.5.0.1	*08-00-75-A1-00-02*	*temp*	*10 mins*
89.7.1.4	*08-00-75-A1-00-99*	*temp*	*9 mins*
89.11.0.1	*08-00-75-A1-00-27*	*temp*	*9 mins*
89.10.0.1	*08-00-75-A1-00-31*	*temp*	*7 mins*
89.10.0.2	*08-00-46-00-3D-FF*	*temp*	*3 mins*
89.1.0.218	*00-00-C0-95-3A-25*	*temp*	*7 mins*
89.18.0.1	*08-00-75-A1-00-E0*	*temp*	*9 mins*
89.11.0.22	*08-00-75-A1-00-1F*	*temp*	*9 mins*
89.1.0.1	*08-00-75-A1-00-01*	*temp*	*5 mins*
89.8.0.1	*08-00-75-A1-00-1A*	*temp*	*10 mins*

Når IP modulet vil sende en besked til en IP adresse, checkes arp tabellen for at finde den tilsvarende ethernetadresse. Findes informationen ikke, broadcastes IP adressen på nettet. Hosten med den pågældende IP adresse svarer ved at sende en pakke med IP adresse og ethernetadresse. ARP kender nu ethernetadressen og gemmer oplysningerne i sin cache til fremtidig brug.

Er der ingen trafik til/fra adressen, slettes adressen fra arptabellen, når minutterne i **Life** er talt ned.

6.2 netstat

Kommandoen benyttes til at vise status for nettet. Brugt uden parametre vil uddata komme til at se således ud:

Active connections

Proto	*Recv-Q*	*Send-Q*	*Local Address*	*Foreign Address*	*(state)*
tcp	*0*	*0*	*unv10:nb_sssrv*	*89.18.1.23:14616*	*ESTABLISHED*
tcp	*0*	*0*	*unv10:nb_sssrv*	*89.18.1.11:2592*	*ESTABLISHED*
tcp	*0*	*0*	*unv10:login*	*slv:1023*	*ESTABLISHED*
tcp	*0*	*0*	*unv10:nb_sssrv*	*89.18.1.27:18708*	*ESTABLISHED*
udp	*0*	*0*	*unv10:who*	**:**	
udp	*0*	*0*	*unv10:nb_nmsrv*	**:**	
udp	*0*	*0*	*unv10:nb_dgsrv*	**:**	
(a)	(b)	(c)	(d):(e)	(f):(g)	(h)

Her har felterne følgende betydning:

(a) Navnet på den protokol, der benyttes af forbindelsen.

(b) Den mængde bytes, der er modtaget, men ikke behandlet.

(c) Den mængde bytes, der venter på at blive sendt.

(d) Hostnavnet eller IP adressen på den lokale host.

(e) Portnummeret eller navnet på den forbindelse, der benyttes.

(f) den anden host

(g) port for den anden host

(h) Status for TCP forbindelsen.

Hvis man angiver et tidsinterval i sekunder efter kommandoen, vil kommandoen vise informationerne med det angivne antal sekunder imellem.

6.3 NetBIOS status

TCP/IP kan også benyttes på PC'ere. Dette bruges f.eks. i forbindelse med brug af LAN Manager eller Windows for Workgroups, Windows 95 eller Windows 95 og terminalemulering ved hjælp af DDE-Term.

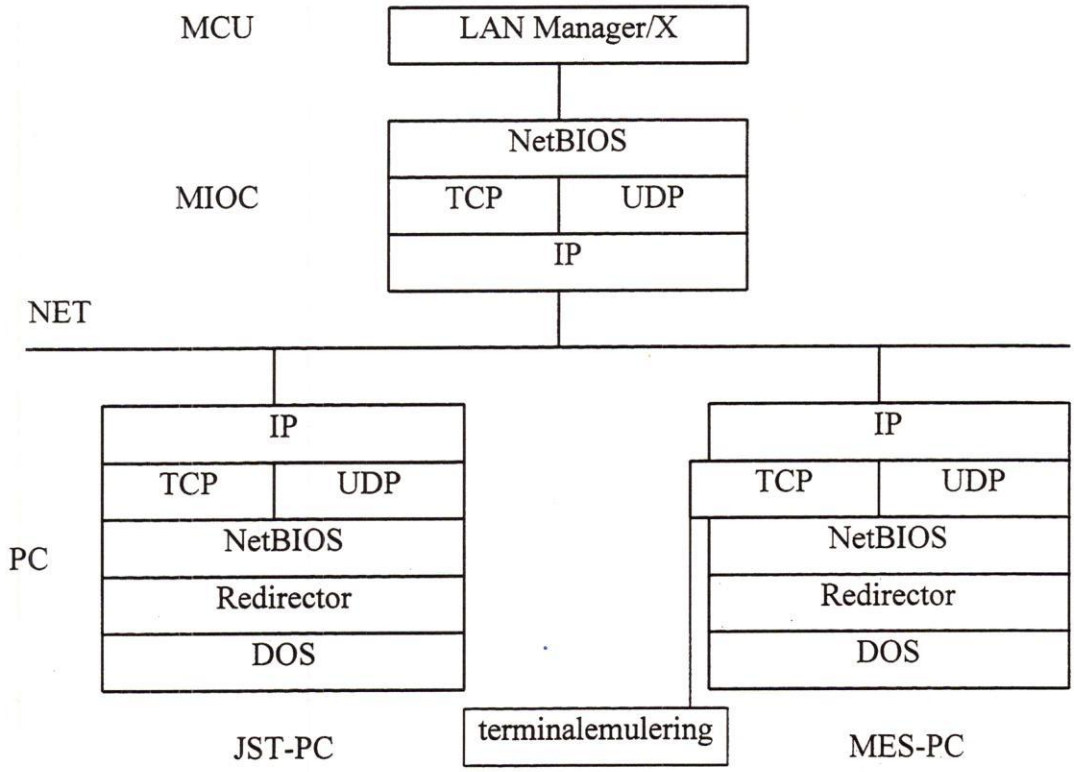
Lan Manager/X (LM/X eller ASU) er et såkaldt netværks-operativsystem. Ved hjælp af LM/X kan man benytte en Supermax som server for PC'er, således at PC'erne kan udskrive via Supermax'ens spoolersystem og gemme filer i filsystemet på Supermax'en.

LAN Manager og Windows for Workgroups/Windows 95/NT kræver et NetBIOS lag for at kunne køre oven på TCP/IP.

For at PC'erne og Supermax'en skal kunne kommunikere, skal de "snakke samme sprog". Det vil i dette tilfælde være **TCP/IP, NetBEUI** eller **IPX**.

DDE-Term er et terminal-emuleringsprogram, der gør det muligt at benytte PC'en som terminal.

DDE-Term kan konfigureres til at benytte NetBIOS eller telnet til at køre oven på TCP/IP protokolstakken.



Som kommunikationsprotokol benyttes NetBIOS over TCP/IP.

På det højeste niveau på Supermaxen ligger selve LM/X serverprogrammet. Herunder ligger NetBIOS og TCP/IP lagene.

På PC'erene er det højeste niveau DOS, med en såkaldt redirector (Lan Manager eller , Windows 95, NT eller Windows for Workgroups) under, og herefter ligger NetBIOS og TCP/IP.

Med programmet **nbtstat** kan man se status for **NetBIOS**:

NetBIOS endpoint status
Node name: <kaka> Scope Id: <>

Type[dev]	Input	Output	Local Name	Foreign Name	(state)
ssenp[6]	22	8044	kaka.login	P00000c0410f6c	DATAXFER
ssenp[5]	432K	1987K	kaka	JST-PC	DATAXFER
ssenp[8]	205K	373K	kaka	OVI-PC	DATAXFER
ssenp[11]	766K	9077K	kaka	ULF-PC	DATAXFER
ssenp[14]	20M	2066K	kaka	PET-PC	DATAXFER
ssenp[15]	23	8801	kaka.login	P000aa0066a2b6	DATAXFER
ssenp[7]	668	28498	kaka.login	P0985f11d80000	DATAXFER
ssenp[9]	2043	20545	kaka	EGU-PC	DATAXFER

Her ses 5 PCer der kører LAN Manager og 3 PCer der kører NetBIOS login. Når PCerne kører LAN Manager, vil deres computername blive brugt som NetBIOS navn.

6.4 ping

Dette program gør det muligt at teste, om en anden host svarer på nettet.

```
ping unv8
```

vil sende 4 pakker til hosten **unv8**, og vise om der blev modtaget svar for disse:

```
Pinging host unv8 : 89.11.0.13
ICMP Echo Reply:TTL 60
ICMP Echo Reply:TTL 60
ICMP Echo Reply:TTL 60
ICMP Echo Reply:TTL 60
Host unv8 replied to all 4 of the 4 pings
```

Hvis en host ikke svarer på en **ping**, kan hosten eller gateway'en til hosten være nede, eller **TCP/IP**'en på hosten kan være stoppet.

6.5 /etc/net

Kommandoen benyttes til at starte og stoppe TCP/IP'en på en Supermax Multiserver, og til at se status.

TCP/IP'en startes ved at afgive kommandoen:

```
/etc/net start
```

Dette gøres ved boot ved udførsel af filen **/etc/rc.d/starttcp.**

Hvis man ønsker at aflæse status af TCP/IP'en, gøres dette ved kommandoen:

```
/etc/net status
```

Her får man en udskrift, der dels fortæller om TCP/IP'en kører, dels fortæller hvilke dæmoner, der kører:

```
/etc/net status
SupermaxTCP network is up
netd is running
inetd is running
telnetd is running
ftpd is running
tftpd is running
pftpd is running
rlogind is running
rshd is running
rwhod is running
bootpd is running
nbtd is running
nbtlogin is running
snmpd is running
named is running
smtpd is running
orasrv is running
uucpd is running
```

I dette eksempel kan man se, at TCP/IP'en kører, og bl.a. net-, telnet-, ftp-, rlogin-, rsh-, rwho-, NetBIOS-, sendmail-, route- og simple network management- dæmonerne kører.

Inet dæmonen er en dæmon, der kan konfigureres til at have flere funktioner. I filen /etc/inetd.conf konfigureres hvilke funktioner den skal udfylde.

```
#       @(#)inetd.conf  5.3
#
#       INETD.CONF :: Inetd configuration file
#
#
pop3    stream  tcp     nowait  root    /etc/pop3post   pop3post
imap    stream  tcp     nowait  root    /etc/imapd      imapd
finger  stream  tcp     nowait  root    /etc/fingerd    fingerd
ntalk   dgram   udp     wait    root    /etc/talkd      talkd
#exec   stream  tcp     nowait  root    /etc/rexecd     rexecd
echo    stream  tcp     nowait  root    internal        internal
echo    dgram   udp     wait    root    internal        internal
discard stream  tcp     nowait  root    internal        internal
discard dgram   udp     wait    root    internal        internal
daytime stream  tcp     nowait  root    internal        internal
daytime dgram   udp     wait    root    internal        internal
chargen stream  tcp     nowait  root    internal        internal
chargen dgram   udp     wait    root    internal        internal
time    stream  tcp     nowait  root    internal        internal
time    dgram   udp     wait    root    internal        internal
```

TCP/IP'en stoppes ved kommandoen:

```
/etc/net stop
```

Dette gøres sædvanligvis fra en fil i kataloget **/etc/shutdown.d**.

Når man afgiver kommandoen skal man være opmærksom på, at der også findes en LAN Manager/X kommando ved navn **net** med den tilsvarende syntax. Den ligger i kataloget **/usr/bin**, så hvis man har en path, hvor **/usr/bin** står inden **/etc** kataloget, så får man fat i den gale kommando, hvis ikke man angiver fuld path.

LAN Manager kommandoen **net** kan også kaldes ved at skrive **NET** med store bogstaver, så det kan man gøre, hvis man ønsker at bruge denne kommando.

6.6 ruptime

Kommandoen fortæller hvilke hosts, der er tilgængelige på nettet:

```
ruptime
dde       down    14+02:04
demo5     down    26+00:15
desony    up      13+06:20,  0 users    load 0.01, 0.00, 0.00
ecad5     up      2+01:12,   8 users
ella      up      9+02:07,   0 users
kaka      up      11+01:13,  10 users
unv10     up      2:23,      0 users
unv8      up      2+03:38,   0 users
usa       down    2:13
vert      up      2:33,      1 user
willy     down    9+06:02
wp        down    22+03:18
(a)       (b)     (c)        (d)          (e)
```

(a) Hostnavnet

(b) Oppe eller nede

(c) Antal dage + timer:minutter maskinen har været oppe/nede

(d) Antal brugere, der er logget på

(e) Load information, der viser hvor belastet den pågældende host har været for hhv. 5, 10 og 15 minutter siden. Vises dog ikke for Supermax'er.

Man kan benytte en række options til **ruptime:**

-l Listen udskrives sorteret efter load information

-t Listen sorteres efter oppetid

-u Listen sorteres efter antallet af brugere.

6.7 rwho

Med rwho kan man få listet information om alle de brugere, der er logget ind på nettet.

```
rwho
info     DDE:tty12              Feb  6 11:01 :01
pt3      DDE:tty10              Feb  6 11:01
dhh      kaka:tty22             Feb  6 10:07
hdb      kaka:tty24             Feb  6 10:40
jst      kaka:tty07B            Feb  6 07:57
mil      kaka:RtyFA09           Feb  6 11:03
mil      kaka:tty13             Feb  6 10:54 :02
mof      unv10:NBTFA1ABmof      Feb  6 10:56 :06
pckursus unv10:NBTFA18          Feb  6 10:45 :10
root     vert:console           Feb  6 03:32 :04
```

Rwho lister alle de brugere, der har været aktive inden for den sidste time. Hvis man ønsker al få listet samtlige brugere, skal man benytte option **-a**.

Option **-u** kan bruges til at få listen sorteret efter logins.

6.7.1 Start af nettet uden rwho-dæmonen

Med TCP-kommandoerne **ruptime** og **rwho** kan man fra en host se hvilke andre hosts, der er på nettet, samt hvilke brugere der er logget ind på de enkelte hosts.

```
rwho
```

Uddata-eksempel:

```
jsc       unv10:petntc08jsc    Dec  3 10:30
max0      unv4:tty69           Dec  3 09:00 :03
max1      unv4:tty68           Dec  3 09:00
max2      unv4:tty22           Dec  3 09:00
max3      unv4:tty24           Dec  3 10:20
max4      unv4:tty23           Dec  3 08:59
max5      unv4:tty25           Dec  3 10:27
adm1      unv6:U511006         Dec  3 10:23 :01
adm2      unv6:U511001         Dec  3 09:41
adm3      unv6:U520FF8         Dec  3 09:42 :01
adm4      unv6:U511000         Dec  3 09:41
root      unv6:console         Dec  3 09:00 :01
```

Set ud fra et sikkerhedsmæssigt synspunkt er dette ikke altid ønskeligt, og det koster mange ressourcer både for hosten og i nettet.

Netadministratoren kan vælge at slå denne mulighed fra individuelt for en host: Hosten vil dermed ikke melde sig ud på nettet og kan heller ikke selv præsentere statusoplysningerne om indloggede brugere på andre maskiner.

Da ruptime og rwho baserer sig på informationer, som rwho-dæmonen, rwhod, registrerer, skal denne dæmon ikke startes op. Samtlige TCP/IP-services fastlægges og opstartes fra filen

```
/etc/net
```

her kan man udkommentere rwhod-kaldet, således:

```
# Commands to start the network:
# inserted by setup

# START:
START="
[ ! -f $NET/routed.run ] || routed.run
sleep 2 #wait for routed to initialize
[ ! -f $NET/named.run ] || named.run
sleep 2 #wait for named to initialize
[ ! -f $NET/ftpd ] || ftpd
[ ! -f $NET/telnetd ] || telnetd
[ ! -f $NET/tftpd ] || tftpd
[ ! -f $NET/pftpd ] || pftpd
[ ! -f $NET/rlogind ] || rlogind
[ ! -f $NET/rshd ] || rshd
#[ ! -f $NET/rwhod ] || rwhod
[! -f $NET/snmpd ] || snmpd
```

Som svar på en hosts forespørgsel om oppe-hosts

```
ruptime
```

vil der nu efter en tid meldes "down ages", som udfor unv8 herunder:

```
unv1          up  7+01:58,     0 users
unv10         up  8+01:10,     1 user
unv3        down 76+19:47
unv4          up  9+22:37,     6 users
unv6          up     2:49,     9 users
unv8        down     ages
```

Opgave

Formål: - at afprøve TCP/IP kommandoerne rwho, arp, netstat, og ping.

1. **Hvad viser kommandoen finger jst@kaka.kursus.dde.dk?**
   Hvad er det, der starter finger kommandoen op?

2. **På hvilken/hvilke host(s) arbejder brugeren hmj? fla? jst?**

3. **Hvilken ethernet adresse har hosten med IP adresse 152.95.64.205**

4. **Hvor mange TCP/IP forbindelser har kursusmaskinen?**

5. **Hvor mange NetBIOS forbindelser har kursusmaskinen?**

6. **Kører TCP/IP'en på host'ene unv3 og skrot (ja, det hedder den)?**

7. **Check hvilke dæmoner der kører.**

8. **Hvad laver talk kommandoen?**

Løses samlet:

9. **Stop rwho dæmonen og afprøv rwho kommandoen.**

10. **Konfigurér finger kommandoen til at starte op på kursusmaskinen, således at man fra unv3 kan kalde "finger tcp0@unv7", uden at få "connection refused".**

7. Routere og gateways

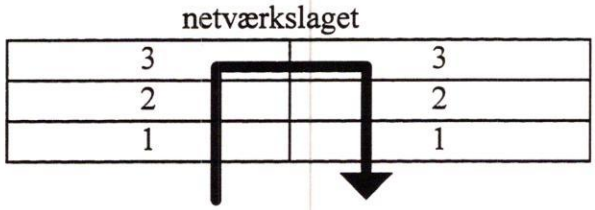
En router benyttes til at opdele et netværk på det, der efter OSI Modellen hedder netværks laget (se side 14).

Routere har typisk routing tabeller, som fortæller, hvilken vej pakker skal køre til forskellige netværk, og som skal konfigureres manuelt.

Mange routere har evnen til at justere routing tabellerne til belastningen og den aktuelle konfiguration af nettet gennem interaktion med network management systemer eller router-to-router kommunikation.

Routere er protokol-afhængige. Hvis en særlig router kun er sat op til DECnet, vil den ikke kunne route IP datagrammer.

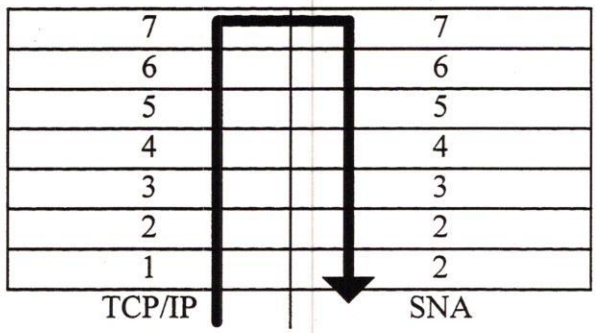
Router



Mange computersystemer kan benyttes som routere, men flere leverandører leverer stand-alone routere, som kan administrere mange protokoller og transmissions teknologier i en enkelt enhed.

En TCP/IP **router** opdeler, eller om man vil, forbinder på IP laget, hvor en **gateway** f.eks. kan være gateway mellem et TCP/IP netværk og et SNA net, således at man kan køre f.eks. 3270 terminalemulering efter konverteringen:

Gateway



Når man benytter en router eller en gateway, skal man konfigurere nettet til at benytte denne.

På en Supermax Multiserver kan det gøres i filen **/etc/net**, hvor man erstatter linien **routed** med en linie:

```
/usr/bin/route -s add 152.95.64.251
```

På en UNIX rel. 4.2 maskine skal man redigere i filen **/etc/inet/rc.inet**. Her skal man udkommentere linien:

```
#/usr/sbin/in.routed -q
```

og til gengæld tilføje linien:

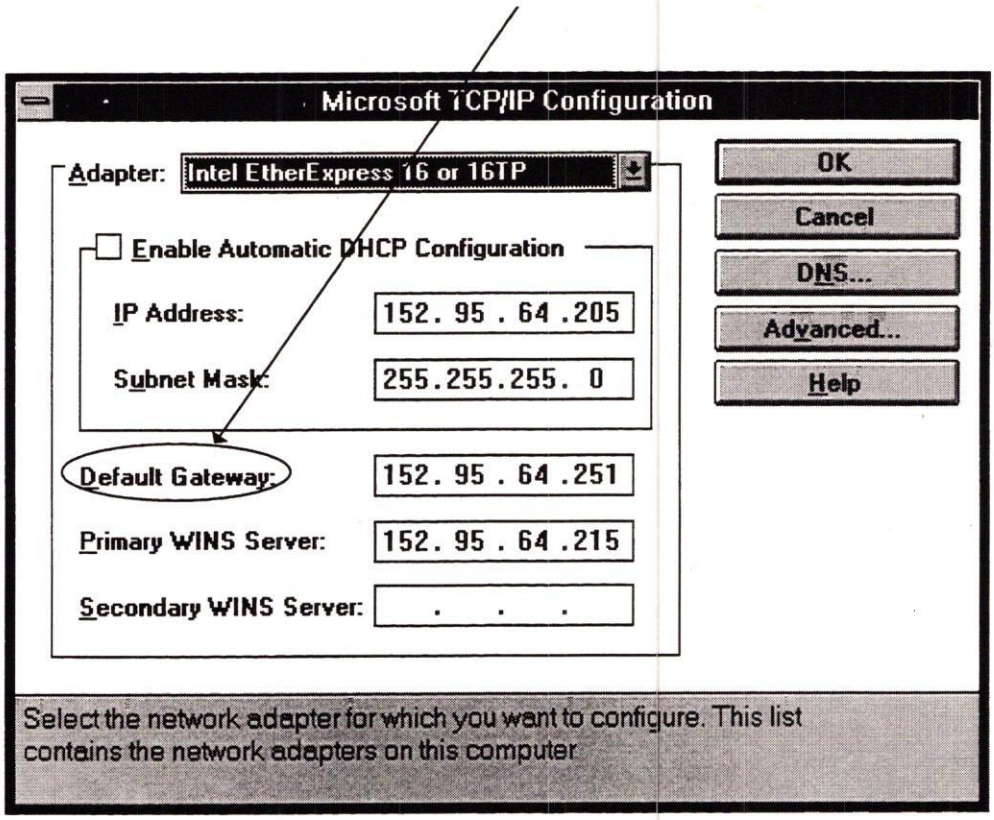
```
/usr/sbin/route default 152.95.64.251 1
```

dér hvor der står en tilsvarende kommentar.

Routed giver dynamisk routning, hvor route kommandoen giver en statisk routning.

På en PC skal man angive gateway. Hvor dette skal gøres afhænger af den TCP/IP, man har installeret, men en angivelse af "gateway" i denne forstand kan være en router.

Her et eksempel fra Windows for Workgroups, Netværksinstallation:



7.1 Route kommandoen

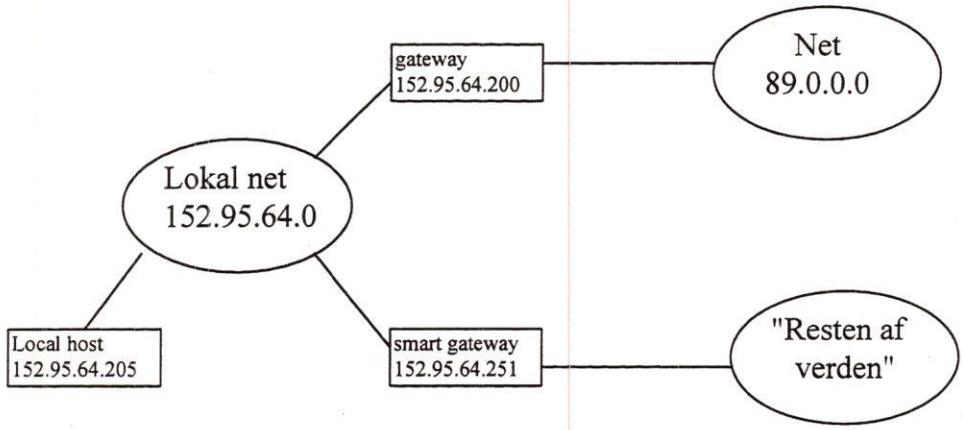
Med route kommandoen kan man tilføje gateways, såkaldte smart gateways, eller udskrive en routing tabel.

En gateway tilføjes ved at angive gateway IP-adresse, samt net-adresse:

```
route add <gateway> <netværk>
```

En **smart gateway** er en gateway, der benyttes, hvis ikke der er tale om en lokal host, eller en host, der ligger på et net, der har en veldefineret gateway. En smart gateway tilføjes ved at angive option -s og adressen:

```
route -s <gateway>
```



route print

Network Address	Netmask	Gateway Address	Interface	Metric
89.0.0.0	89.0.0.0	152.95.64.200	152.95.64.205	1
0.0.0.0	0.0.0.0	152.95.64.251	152.95.64.205	1
152.95.64.205	255.255.255.255	127.0.0.1	127.0.0.1	1
152.95.255.255	255.255.255.255	152.95.64.205	152.95.64.205	1
152.95.64.0	255.255.255.0	152.95.64.205	152.95.64.205	1
255.255.255.255	255.255.255.255	152.95.64.205	152.95.64.205	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1

Opgave

formål: *- at se på routing information*

1. **Gå ud i en DOS prompt**

2. **Find ud af, om der er defineret en gateway for din PC.**
   Du kan evt. benytte `IPCONFIG` kommandoen med option `/ALL`.

3. **Udskriv routing informationen for din PC.**

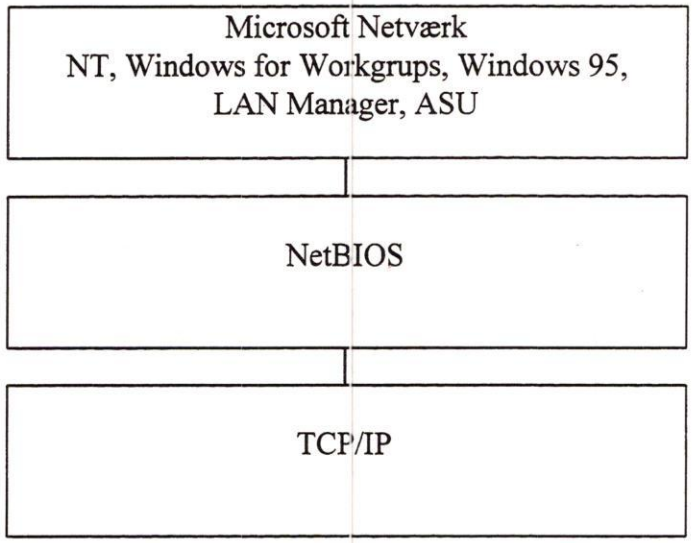
8. Microsoft TCP/IP

Microsoft TCP/IP findes i flere udgaver: Windows 95, Windows for Workgroups 16 bit og 32 bit og Windows NT 3.51.

Konfigurationen ændres på forskellig vis:

På **Windows 95** gøres det fra Kontrolpanel, Netværk, på **Windows for Workgroups** fra Netværksgruppen, Netværksinstallation og fra **Windows NT 3.51** gøres det fra Control Panel, Network.

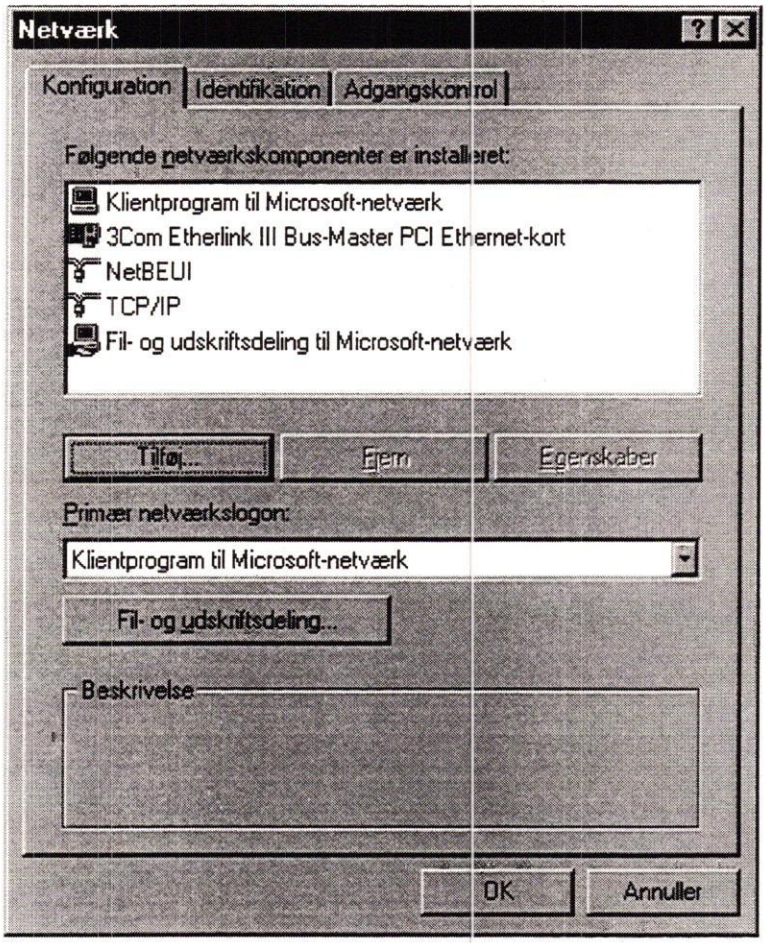
Microsoft TCP/IP benyttes sædvanligvis med Microsoft Netværk, men man kan også benytte andre applikationer som f.eks. ftp, telnet.



I det følgende vises konfigurationen på en Windows 95 client, men de begreber, der gennemgås, er tilsvarende på de øvrige versioner af Microsoft TCP/IP, selvom skærmbilledet måske ser lidt anderledes ud.

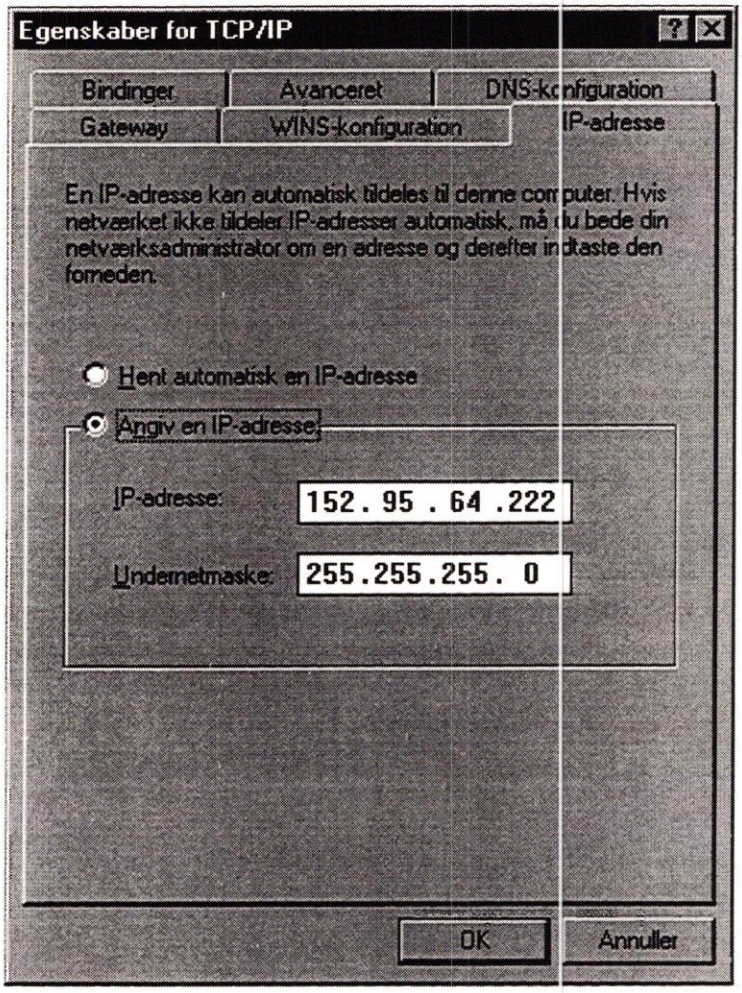
8.1 TCP/IP på Windows 95

For at redigere i TCP/IP opsætningen på en Windows 95 client, skal man som sagt vælge kontrolpanel, netværk:



Herfra skal man udpege TCP/IP ved at dobbeltklikke på den eller ved at klikke den ud og vælge egenskaber trykknappen:

Her får man følgende billede, hvor man kan vælge mellem 6 faneblade: IP-adresse, WINS-konfiguration, Gateway, DNS-konfiguration, Avanceret eller Bindinger:



Først skal man tage stilling til hvilken IP-adresse, denne host skal benytte. Her har man mulighed for at vælge en **automatisk IP-adresse**, hvilket betyder at clienten ved opstart af Windows broadcaster et ønske om en IP-adresse, og dette ønske kan så høres af en såkaldt DHCP server (DHCP = Dynamic Host Configuration Protocol).

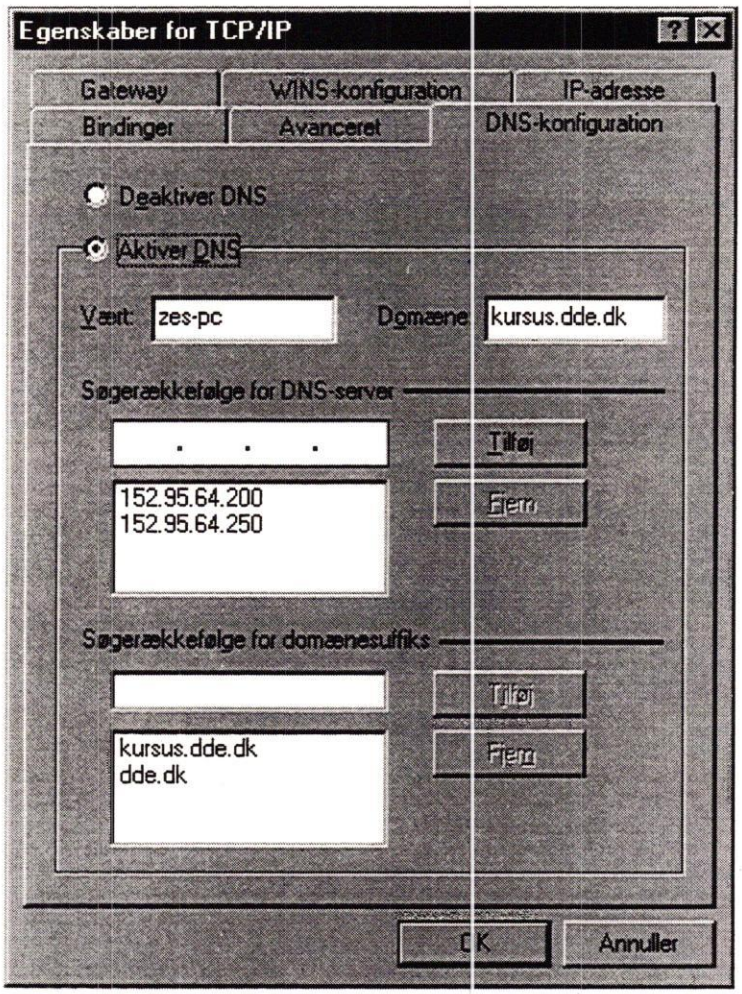
En DHCP server er en NT server, der har fået konfigureret en pulje af IP-adresser, som den stiller til rådighed for de clienter, der ønsker at benytte automatisk IP-adresse (DHCP).

Dette betyder, at en DHCP client kan skifte IP-adresse fra boot til boot, men i reglen benyttes den samme IP adresse i et antal dage af gangen. Dette kan konfigureres på DHCP serveren.

Hvis man benytter DHCP, skal man være opmærksom på, at clienten sammen med IP-adressen kan modtage andre TCP/IP konfigurationer, der overskriver de konfigurationer, man indsætter manuelt, sædvanligvis WINS server, men muligvis også DNS server, DNS domain, Gateway, ...

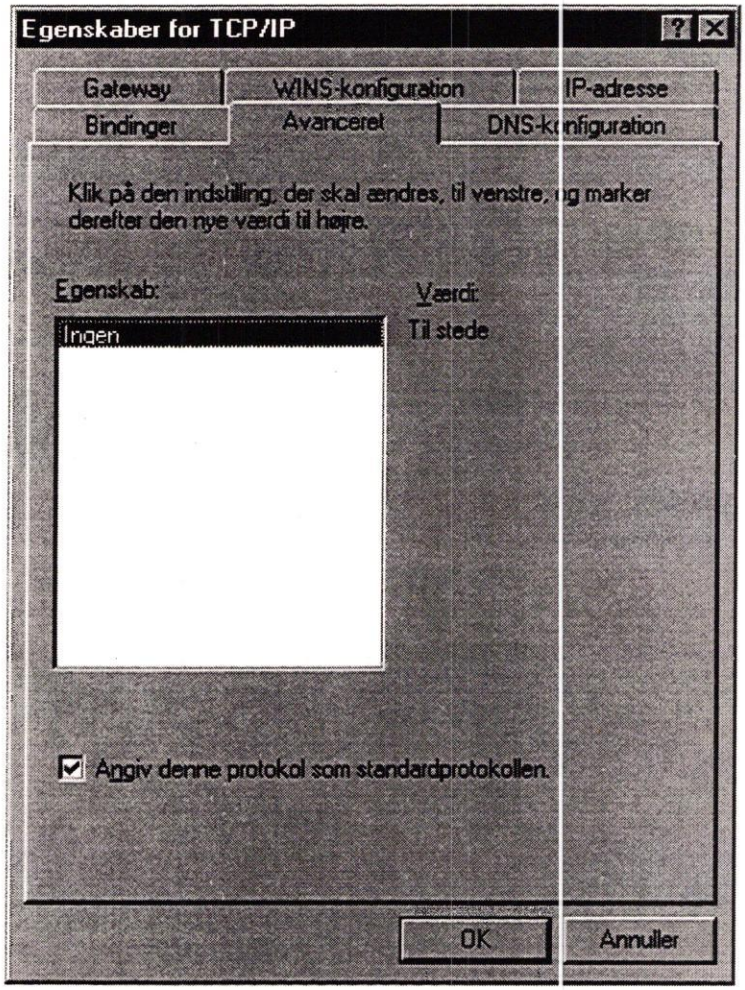
Hvis man ønsker at benytte fast IP-adresse, skal man indskrive den her og angive subnetmaske for nettet.

Hvis man har en Name server, skal man vælge **DNS-konfiguration** fanen.



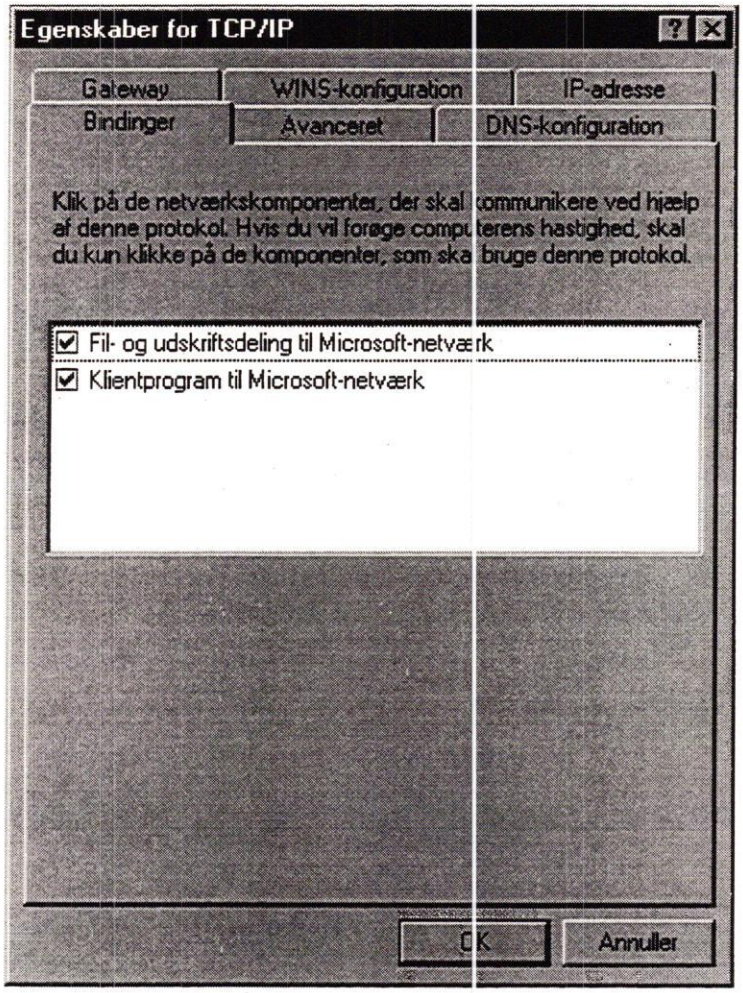
Her skal man angive hostname (værtsnavn) og domain name, og derefter opremse de nameservere man har adgang, således at den nærmeste nameserver, angives først, og således benyttes oftest. Når man benytter DNS, skal man som tidligere nævnt også angive et domain. Her kan man angive en søgerækkefølge for domain names, således at hvis man søger en host, vil den nævnte domains gennemsøges i nævnte rækkefølge.

I **avanceret** skal man blot være opmærksom på at man kan vælge TCP/IP som standardprotokol, hvilket betyder at den får **LANA nummer** 0, og forbindelser vil først forsøgt blive etableret ved hjælp af TCP/IP. Hvis dette fejler, forsøges en eventuel sekundær protokol.



I fanen **Bindinger** skal man udpege de komponenter, der skal benytte TCP/IP protokollen.

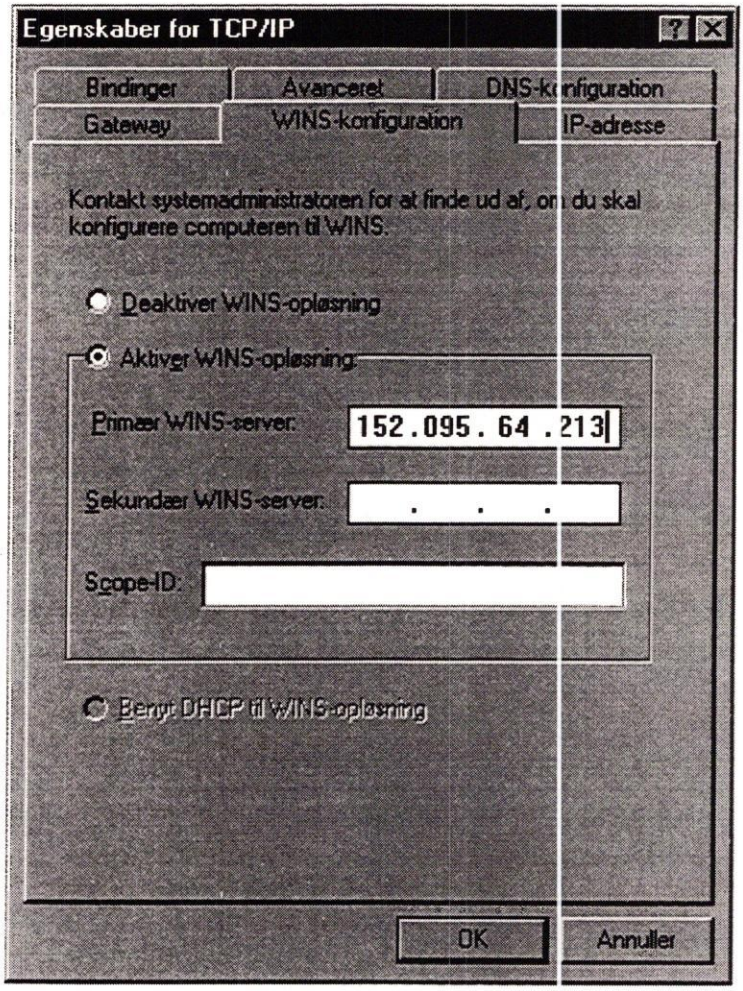
Som standard drejer det sig om Fil- og printerdeling, hvor PC'en kan dele sine kataloger og printere med de øvrige PC'er på nettet, og Microsoft Netværk, som er det clientprogram, der benyttes ved brug af ressourcer fra NT, LAN Manager, Windows 95 og Windows for Workgroups servere.



Fanen WINS konfiguration benyttes, hvis man har en NT server, der fungerer som WINS server. En WINS server, er en server, der benyttes i forbindelse med navneopløsning på NetBIOS niveauet.

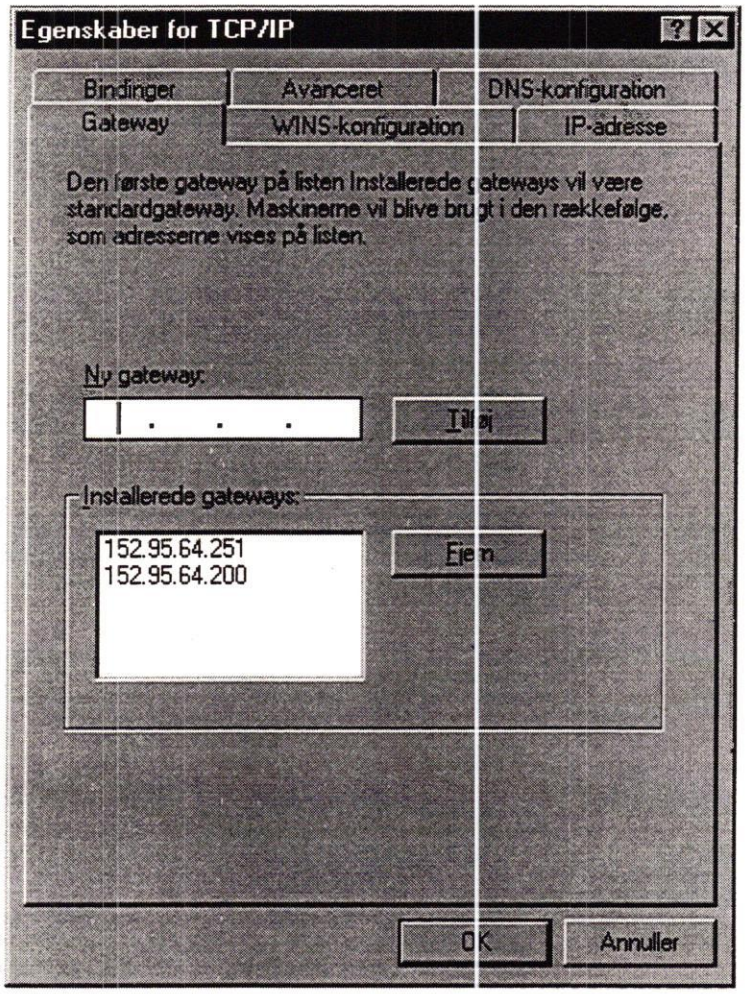
Normalt opløses disse navne ved hjælp af broadcasts, men man kan spare en del net-trafik ved at opsætte en WINS server. De clienter, der konfigures til at benytte WINS eller DHCP, tilføjes automatisk til WINS databasen, og andre clienter, kan manuelt tilføjes til denne på serveren af systemadministratoren.

Hvis man benytter DHCP er WINS en fremragende måde at holde rede på hvilke clienter, (udfra computernames=NetBIOS adresser) der benytter hvilke IP-adresser.



I fanen **Gateway** skal man angive hvilke routere/gateways, der er til rådighed for nettet.

Her skal man angive deres IP-adresser.



8.2 LMHOSTS

LMHOSTS er en fil, der benyttes til at angive IP adresser på servere, der ligger på den anden side af eventuelle routere.

Da NetBIOS opløsningen som standard foregår ved hjælp af broadcasts, og disse sædvanligvis ikke videresendes over routere, er man nødt til at benytte LMHOSTS filen for de hosts, man skal nå med NetBIOS over routeren.

NetBIOS benyttes som tidligere nævnt til forbindelser i Microsoft netværk og til visse terminalemulerings-programmer (nblogin).

Windows 95 benytter automatisk LMHOSTS filen i C:\WINDOWS kataloget, på alle de øvrige clienttyper skal man eksplicit markere, at man ønsker at benytte LMHOSTS.

8.3 Kommandoer

Man kan benytte mange af de sædvanlige TCP/IP kommandoer til Microsoft TCP/IP. Men der findes også nye kommandoer:

ipconfig

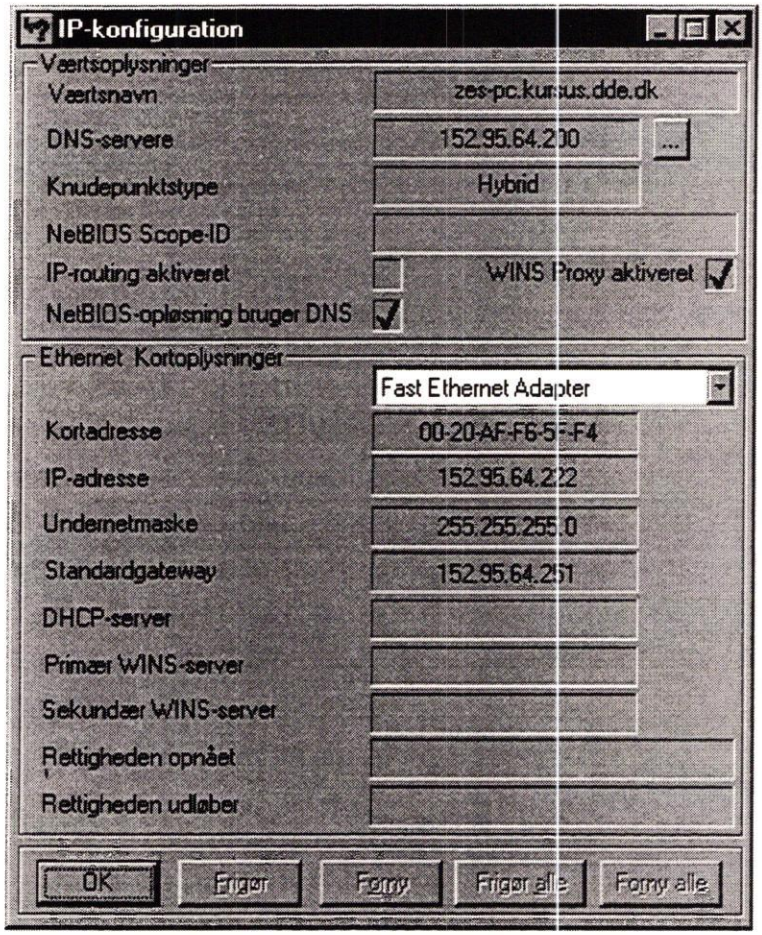
er en meget nyttig kommando, der viser opsætningen af TCP/IP'en på clienten:

```
Windows IP Configuration Version 1.0

Ethernet adapter Intel EtherExpress 16:

   IP Address. . . . . . . : 152.95.64.205
   Subnet Mask . . . . . . : 255.255.255.0
   Default Gateway . . . . : 152.95.64.251
```

Man kan få yderligere information om TCP/IP konfigurationen ved at benytte kommandoen med option /all:

```
ipconfig /all

Windows IP Configuration Version 1.0

        Host Name . . . . . . . . : jst-
        pc.kursus.dde.dk
        DNS Servers . . . . . . . : 152.95.64.200
                                    152.95.64.250
        Node Type . . . . . . . . : Hybrid
        NetBIOS Scope ID. . . . . :
        IP Routing Enabled. . . . : No
        WINS Proxy Enabled. . . . : No
        DNS Resolution For Windows Networking
        Applications Enabled : No

Ethernet adapter Intel EtherExpress 16:

        Physical Address. . . . . : 00-AA-00-66-AC-
        10
        DHCP Enabled. . . . . . . : No
        IP Address. . . . . . . . : 152.95.64.205
        Subnet Mask . . . . . . . : 255.255.255.0
        Default Gateway . . . . . : 152.95.64.251
        Primary WINS Server . . . : 152.95.64.215
        Secondary WINS Server . . : 152.95.17.215
```

På en Windows 95 client hedder den tilsvarende kommando dog **winipcfg**, og giver følgende uddata:



Denne kommando kan bl. a. give information om, hvilken IP adresse man har fået ved hjælp af DHCP, og kan fortælle hvilken DHCP server, man har fået den fra.

Har man fået en IP adresse ved hjælp af DHCP kan denne frigøres ved brug af **/RELEASE** optionen eller **Frigør** trykknappen, og man kan anmode om en ny ved brug af **/RENEW** optionen eller **Forny** trykknappen.

Opgave

formål: *at se på konfiguration af TCP/IP på clienten*

1. **Alt afhængigt af, om du sidder ved en Windows 95 eller en Windows for Workgroups client, skal du benytte kommandoen IPCONFIG eller WINIPCFG til at se på konfigurationen af TCP/IP på clienten.**

2. **Skriv denne ud på en printer, så du har den til senere.**

3. **Fjern nu TCP/IP'en fra PC'en.**

4. **Installér den igen, men denne gang skal du vælge DHCP.**

5. **Efter boot, skal du se efter den ny TCP/IP konfiguration, og sammenligne med den gamle. Har du fået en IP adresse?**

6. **Frigiv IP adressen med option /RELEASE til IPCONFIG, og anmod om en ny med IPCONFIG /RENEW.**

7. **Se efter om det lykkedes, eller om du fik den gamle igen.**

9. Remote login

Ved hjælp af TCP/IP kan man logge sig ind på andre maskiner på 2 forskellige måder:

- **telnet**
- **rlogin**

og man kan desuden udføre enkelt kommandoer på en anden host, ved hjælp af kommandoen:

- **remsh**

Rlogin og remsh bliver behandlet senere i afsnittet Remote Utilities side 93ff.

9.1 telnet

Uanset operativsystem, kan man logge på en anden host ved hjælp af **telnet**:

```
telnet unv8

Trying...
Connected to unv8
Escape character is '^]'
login:
```

Hvis man ikke angiver et hostnavn eller en IP adresse, vil man få telnet prompten:

```
telnet>
```

og man skal derefter benytte kommandoen **open** til at forbinde sig til den anden host:

```
telnet> open unv8
Trying...
Connected to unv8
Escape character is '^]'
login:
```

Hvis man i stedet ønsker at afslutte telnet fra prompten, skriver man:

```
telnet> quit
```

og kommer tilbage til den lokale host.

Hvis man er logget på den anden host, kan man komme tilbage til telnet prompten ved at taste den angivne escape sekvens, eller helt tilbage til den lokale host ved at logge ud på sædvanlig måde.

Escape karakteren kan ændres til f.eks. **^X** ved at skrive:

```
esc ^X
```

fra telnet prompten.

Hvis man kalder op til en UNIX host forskellig fra en Supermax, skal man på denne host sætte variablen **$TERMTYPE** til T3-24-C80.

Hvis man kalder op til en Supermax fra en anden type host, skal man fra telnet prompten give kommandoen:

```
termtype DDE-VTI
```

hvilket medfører, at Supermax'ens VTI (brug af terminology tabeller) sættes i funktion.

På den host, som man kalder op fra, kan man enten i sit hjemmekatalog eller i **/usr/bin** have en fil liggende, med en række telnet kommandoer. Hvis den har navnet **.telnetrc** vil den automatisk blive udført, hver gang man kalder **telnet**.

Filen kan bruges til at initialisere telnet variable. Kommandoerne skal afgives præcis som fra telnet prompten.

Et eksempel på en **.telnetrc** fil kunne være:

```
esc ^X
termtype DDE-VTI
options
```

9.1.1 Konfiguration af en telnetforbindelse på en Supermax Multiserver

Når man etablerer en telnetforbindelse fra en anden host, vil kataloget **/etc/stcpports** blive gennemsøgt for at finde en fil, der har den anden hosts navn.

Hvis man f.eks. kalder op til kaka fra NTC'en NTC1, vil filen **/etc/stcpports/NTC1** på kaka blive benyttet.

Dette er en fil, der for hver af portene fortæller, hvordan telnet-forbindelser skal konfigureres.

En linie i denne fil kan se ud på følgende måde:

```
<port> [restricted] [d /dev/wmux.<unitnr>] [m vti] * <UNIX kommandoer>
```

Her betyder:

<port>	TCP/IP Portnummer. Port 1 hedder 2010, port 2 2020 og så fremdeles. Hvis det skal være fælles for alle porte, kan man benytte **all**.
restricted	TTY-nummeret afledes af hostnavnet på den host der kaldes op fra, efterfulgt af 4 hexadecimale tal.
d /dev/wmux.<unitnr>	Brugerne kan køre med vinduer. (ds, ts, qs). **<unitnr>** er unitnummeret for MIOC'en.
m vti	Der benyttes vti (terminology-tabeller)

Hvis man kører "restricted", vil man på tty-numrene kunne se fra hvilken host, der er kaldt op.

F.eks. vil **/dev/mes0816** være tty-nummeret for en terminal, der kalder op fra en NTC med navn **mes**. Hvis porten også er defineret som restricted fra POM, vil man yderligere kunne se fra hvilken port på NTC'en der er kaldt op, ved hjælp af kommandoen **bc**:

```
bc
base=16 #Input-tallet er hexadecimalt
0816    #Det hex-tal, der skal konverteres til
        #decimaltal
2070    #Tallet konverteret til 10-
   talssystemet
<ctrl+d>
```

I dette tilfælde er der altså kaldt op fra port nummer 7 fra NTC'en.

Hvis der ikke er oprettet en konfigurationsfil for en host, benyttes en default stcpportsfil, der ligger indbygget i telnet. Denne default konfigurationsfil indeholder følgende:

m vti * /etc/terminology $TERMTYPE

9.1.2 Eksempler på /etc/stcpports filer

Forbindelser fra PC:

```
all restricted d /dev/wmux.<unitnr> m vti *
       /etc/terminology int/sgd-pc.t; cat /etc/issue
```

Forbindelser fra NTC2:

```
2010 restricted d /dev/wmux.<unitnr> m vti *
       /etc/terminology $TERMTYPE; cat /etc/issue; echo
       "Godmorgen Viggo"
2020-2059 restricted m vti * /etc/terminology $TERMTYPE;
       cat /etc/issue.sp
all restricted d /dev/wmux.<unitnr> m vti *
       /etc/terminology $TERMTYPE; cat /etc/issue
```

Forbindelser fra Supermax:

```
all restricted m vti * /etc/terminology $TERMTYPE; cat
       /etc/issue
```

I disse eksempler benyttes flere gange variablen **$TERMTYPE**:

$TERMTYPE Terminology på terminalen fra telnet parameteren, fra **.telnetrc** filen eller fra terminaltypen på NTC porten.

Opgave

Formål: *- at afprøve de forskellige former for remote login*

- at sætte op til at kunne køre rlogin og telnet

1. **Sørg for at du har password på unv3.**
2. **Prøv at logge dig på unv3 med telnet fra unv7 med samme login, som du er logget på med nu.**
3. **Se med kommandoen tty, hvilken tty du er logget på.**
4. **Prøv nu om du kan logge dig på unv3 fra telnet ikonet i Microsoft TCP/IP programgruppen på din PC.**
5. **Hvordan går det med brug af funktionstaster? Prøv med de forskellige emulationer (Termtype).**

10. Kopiering af filer

TCP/IP giver flere muligheder for at kopiere filer mellem forskellige hosts: **rcp, ftp** og **tftp**. Rcp behandles separat i afsnittet Remote Utilities side 93 ff.

10.1 FTP

Kommandoen ftp tillader en bruger at kopiere filer fra en host til en anden.

Man kan kopiere en fil fra en host til en anden ved at starte med at connecte sig til den anden host:

```
ftp unv8

Connected to unv8.
220 unv8 ftp server (SupermaxTCP ftpd 3.5)
   ready
User (unv8.jst): <Retur>
331 Password required for jst.
Password: <Password>
User jst logged in.
ftp>
```

Først startes **FTP** op, og man spørges så hvilket username, man ønsker at bruge. I eksemplet vælges default, som er det login, man er logget ind med på den lokale host, ved at taste retur.

Herefter promptes man for password for brugeren på den anden host, og når dette er afgivet, får man **FTP** prompten.

Hvis man ikke angiver en host i kaldet, får man direkte adgang til **FTP** prompten, og man kan da logge på en host ved at benytte kommandoen **open** efterfulgt af navnet på host'en.

Hvis man kommer til at taste galt ved valg af username eller password, kan man benytte **FTP**-kommandoen **user** evt. efterfulgt af brugernavnet, hvis forbindelsen til serveren er etableret:

```
ftp> user jst
331 password required for jst.
Password: <Password>
230 User jst logged in.
ftp>
```

Når man er logget på en remote host, og ønsker at se hvilket katalog, der er arbejdskatalog på denne host, kan man benytte **FTP** kommandoen **pwd**:

```
ftp> pwd
251 "/usr/lanman/users/jst" is current
   directory.
```

Hvis man kobler sig op på FTP servere på internettet kan man naturligvis ikke være oprettet som bruger. Her benytter man et anonymt login ved at logge på som "**anonymous**".

Herefter vil man blive bedt om at sende sin E-mail identitet til serveren:

```
ftp ka-srv
Connected to ka-srv.kursus.dde.dk.
220 ka-srv Windows NT FTP Server (Version
   3.51).
User (ka-srv.kursus.dde.dk:jst): anonymous
331 Anonymous access allowed, send identity
   (e-mail name) as password.
Password:abc@dde.dk
230 Anonymous user logged in as guest.
```

10.1.1 Kopiering med ftp

Når man har logget sig ind på en remote host, kan man kopiere en fil fra denne ved at benytte kommandoen **get** eller **recv**:

```
ftp> get
(remote-file)   scr
(local-file)    unv8.script
200 PORT command is okay.
150 Opening data connection for scr
    (89.18.0.1, 2395) ( 14 bytes). 226 Transfer
    complete.
15 bytes received in 0.02 seconds (0.75
    Kbytes/sec)
ftp>
```

Her kopieres filen **scr** fra den remote host til en fil på den lokale host med navnet **unv8.script**.

Man kan også angive kommandoen:

```
ftp> get  scr unv8.script
200 PORT command is okay.
150 Opening data connection for scr
    (89.18.0.1, 2396) ( 14 bytes). 226 Transfer
    complete.
15 bytes received in 0.02 seconds (0.75
    Kbytes/sec)
ftp>
```

Hvis man ønsker at kopiere flere filer fra den anden host på én gang skal man benytte kommandoen **mget**, der fungerer tilsvarende **get**.

Hvis man ønsker at kopiere en fil fra den lokale host til den remote, kan man benytte kommandoen **put:**

```
ftp> put
(local-name) .profile
(remote-name) kaka.prof
200 PORT command is okay.
150 Opening data connection for kaka.prof
   (89.18.0.1, 2399).
226 Transfer complete.
739 bytes send in 0.04 seconds (18.48
   Kbytes/sec)
ftp>
```

Igen kunne man have angivet kommandoen på én linie:

```
ftp> put .profile kaka.prof
```

Kommandoen **put** er i øvrigt helt ækvivalent med kommandoen **send.**

Hvis man ønsker at kopiere flere filer fra den lokale host til den anden host, kan man benytte kommandoen **mput.**

10.1.2 Øvrige FTP kommandoer

append f1 f2
Tilføj en lokal fil til en fil på den anden host.

bye Log af den anden host og afslut FTP.

cd dir Skift arbejdskatalog på den anden host.

close Log af den anden host, men bliv i FTP.

delete fil Slet en fil på den anden host.

dir [dir] List indholdet af (arbejds-) kataloget på den anden host, svarende til UNIX kommandoen ls -g

help [kommando]
Print en hjælpemeddelelse om den evt. angivne kommando.

lcd dir Skift arbejdskatalog på den lokale host.

ls [dir] List indholdet af (arbejds-) kataloget på den anden host, svarende til UNIX kommandoen ls.

mdelete filer
Slet de angivne filer fra den anden host.

mdir [filer] lokalfil
Lister de angivne filer fra den anden host, og anbringer resultatet i lokalfil på den lokale host. Hvis man ønsker resultatet listet på skærmen, kan man angive en "-".

mkdir [dir] Opret et nyt katalog på den anden host.

quit Synonym for **bye**

rename fra til
Omdøber filen "fra" til "til" på den anden host.

rmdir [dir]
Sletter det angivne katalog fra den anden host.

status Viser den aktuelle status for FTP.

? Synonym for **help.**

10.2 TFTP

Tftp kommandoen muliggør kopiering til og fra en anden host. En afgørende forskel på FTP og TFTP er, at man skal være oprettet som bruger på begge hosts for at kunne benytte FTP. Med TFTP kræves det i stedet, at der skal være læserettighed for alle til en fil på den remote host, for at man kan tage en kopi af den, og der skal være skriverettighed for alle, for at man kan kopiere en fil til et katalog på den remote host.

Hvis man ønsker at kopiere filen **script** fra host'en **unv8** til den lokale host, kan man gøre det på følgende måde:

```
tftp unv8 get script unv8.script
```

Kopien vil her få navnet **unv8.script** på den lokale host. Hvis man havde udeladt et lokalt navn, ville kopien få samme navn på den lokale host.

Hvis man ønsker at kopiere fra den lokale host til **unv8**, gøres det således:

```
tftp unv8 put fil nyfil
```

Her kopieres den lokale fil til filen **nyfil** på den anden host.

Opgave

Formål: - at afprøve de forskellige metoder til at kopiere filer.

1. **Opret en lille fil i din hjemmekatalog på unv7.**

2. **Send en kopi af denne fil til dit eget login på unv3**

   Det skal først gøres ved hjælp af ftp, derefter ved hjælp af tftp.

3. **Forsøg nu at kopiere filen til din nabos login på unv3 ved hjælp af ftp.**

   Hvad sker?

4. **Start FTP op fra PC'en og kopier filen c:\users\default\admincfg.exe fra FTP serveren ka-srv.**

   Du skal logge dig på som anonymous og gi' din E-mail adresse som identitet.

10.2.2 TFTP sikkerhed

Tftpd er en farlig ven: Brugere fra andre hosts kan læse filer som f.eks. /etc/passwd, og på den måde lure af hvilke logins, der findes på maskinen, og endda hvilke der ikke er password på.

Der findes dog mekanismer, der tillader systemadministratoren at følge med i, hvad der kopieres med tftp og endda at begrænse brugen af det.

10.2.3 Logning af tftpd

tftp dæmonen er så snedigt indrettet, at den kan sættes til at overvåge, hvem der henter/bringer hvad.

Det gøres ved at benytte kommandoen **tftpc** således:

```
tftpc
logging on
<ctrl + d>
```

Herefter logges tftp anmodninger fra andre hosts i filen **/usr/spool/tftpd/log.**

Status for om der logges kan ses med kommandoen:

```
tftpc status
```

Output fra kommandoen vises på den terminal tftpd er startet op fra, således at hvis det er startet fra konsollen, vil status også blive vist på konsollen, selvom kommandoen er afgivet fra en anden terminal.

Foruden at starte og stoppe logning kan **tftpc** kommandoen også anvendes til at stoppe **tftpd** (tftp dæmonen).

```
tftpc
exit
<ctrl + d>
```

Check om tftp dæmonen er stoppet med:

```
/etc/net status
```

eller

```
ps -e ^grep tftpd
```

10.2.4 Begrænsning af kopiering med tftp

Man kan starte **tftpd** op, så der kun tillades adgang til et angivet katalog:

```
/etc/tftpd -r /tmp
```

vil tillade brugere fra andre hosts at kopiere til/fra /tmp kataloget, men ikke andre kataloger.

Hvis man benytter **-r** uden katalog-angivelse, benyttes kataloget **/usr/spool/uucppublic** som standard.

Det katalog der kan kopieres til/fra vil nu blive opfattet som rodkatalog, når tftp anvendes fra en anden maskine.

Skal filen /tmp/nyfil kopieres vha. tftp, og /tmp er det katalog der er adgang til, ser kommandoen således ud:

```
tftp <maskinnavn> get nyfil <tilfil>
```

Skal der logges, når tftp dæmonen er startet op restricted, må man oprette den samme katalogstruktur til logfilen, som når der logges unrestricted, men nu relativt til den nye rod. Dvs. er det /tmp kataloget der er adgang til, er stivejen til logfilen /tmp/usr/spool/tftpd/log.

Opgave

Formål: - at afprøve tftp brug, begrænsning samt logning.

1. **Sæt logning på tftp på unv7**

2. **Udfør fra unv3 en række tftp-kommandoer, der opererer på unv7. Se hvorledes dette logges på unv7.**

3. **Begræns nu det mulige tftp-område på unv7 til /tmp kataloget.**

4. **Forsøg nu tftp fra unv3 til unv7, både indenfor området og udenfor. Kontroller logfilen på unv7.**

11. Remote Utilities

I et lokalnet, der anvender TCP/IP som netværksprotokol, kan brugerne anvende såkaldte remote utilities, som giver dem mulighed for:

- at logge ind på en host fra en anden host
- at udføre kommandoer på en anden host (uden at logge ind først).
- at kopiere filer mellem to hosts

Dette kan ske uden afgivelse af login og password, når visse betingelser er opfyldt:

- Brugeren er oprettet som bruger på remote hosten (eller har fået overladt en anden brugers login, jf. senere).
- På den "remote" host har brugeren i sit hjemmekatalog en fil ved navn **.rhosts**, der definerer hvilke hosts, han/hun må logge ind fra. (Filen laves vha. vi-editoren, med kommandoen rhosts eller fra Sysadm).

Eksempel på .rhosts fil på hosten unv6 (host2) i hjemmekataloget for brugeren mes:

```
unv2
unv4
ka7 jst
ka7 mes
```

Filen giver altså brugeren selv (mes) mulighed for at benytte r-utilities mod unv6 fra unv2, unv4 og ka7. Endvidere giver det brugeren jst på ka7 mulighed for at bruge mes' login til det samme.

Hvis man i en .rhosts fil skriver "+" (et plus) i stedet for evt. login, betyder det at man tillader alle brugere fra pågældende host at foretage rlogin eller lave en remsh.

11.1 /etc/hosts.equiv

Filen tillader brugere fra en anden host, at logge ind på denne host uden at angive et password, hvis de er oprettet som brugere på denne host.

Dette kan man have glæde af, hvis man benytter r-utils (programmerne **remsh**, **rcp** eller **rlogin**).

De hosts, der er defineret i **hosts.equiv** filen, kan altså opfattes som betroede hosts, hvor brugerne på disse har "samme rettigheder" som brugerne på den lokale host, hvis der findes en bruger med det samme login der.

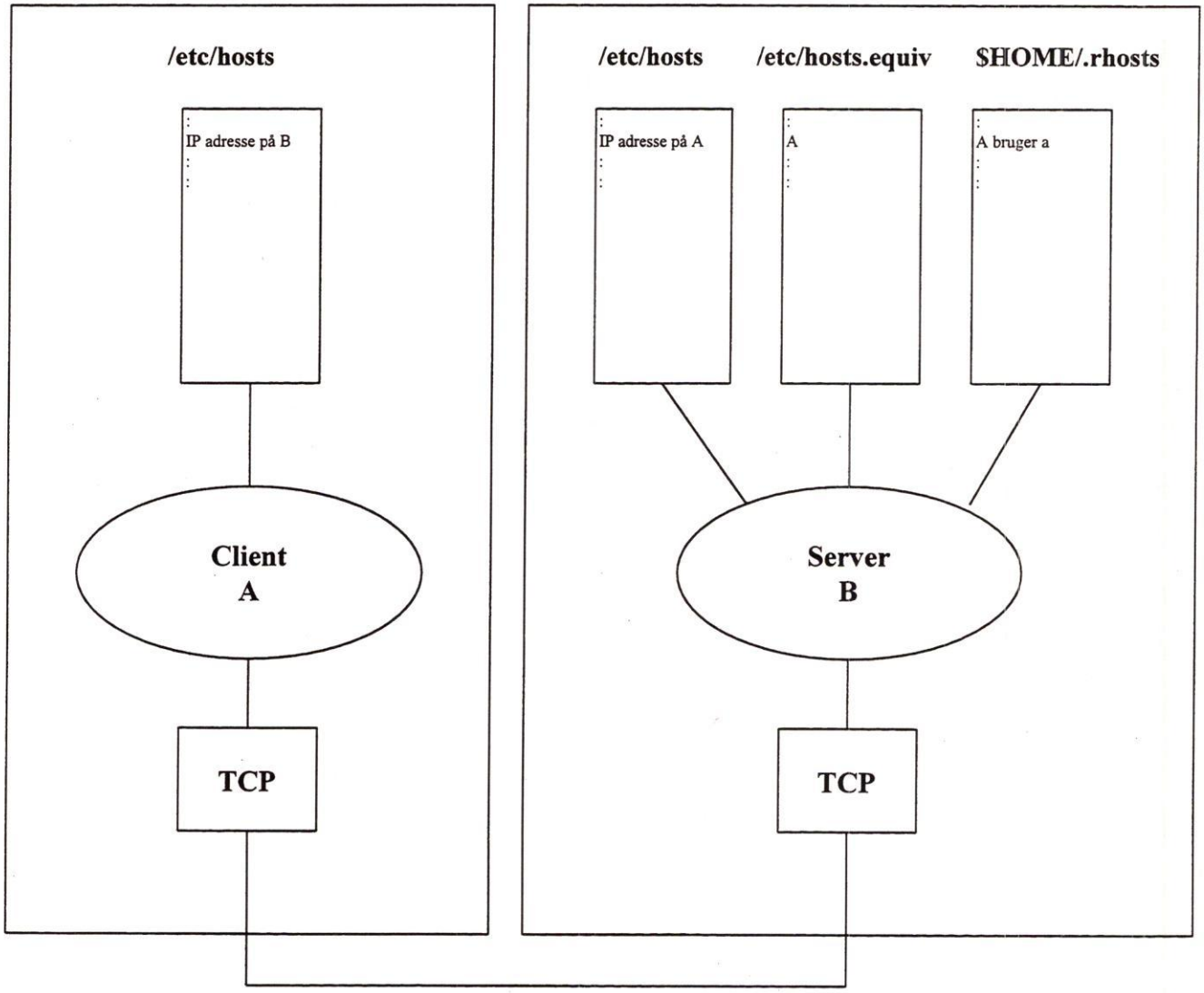
Hvis hosten **sigurd** har hosten **Wilhemine** i sin **hosts.equiv**, vil brugerne på **Wilhemine** kunne logge sig på **sigurd** ved brug af **rlogin**, men ikke omvendt.

Den eneste bruger, der vil blive promptet for et password alligevel, er superbrugeren, **root**.
Hvis superbrugeren, root, skal have tilsvarende rettighed, skal man oprette en .rhosts fil i roden.

Filen /etc/hosts.equiv kan oprettes/redigeres ved at benytte indgangen **system** fra **sysadm**.

Denne fil indebærer en stor sikkerhedsrisiko, og bør derfor kun bruges efter nøje overvejelser. Anvend .rhosts for brugerne i stedet.

Remote Utilities



rlogin, remsh, rcp

1. Serveren kontrollerer, at clientens source port er i intervallet 0 - 1023
2. Serveren undersøger om clienten er anført i /etc/hosts eller kendt af en nameserver
3. Serveren modtager et brugernavn fra clienten
4. Serveren skifter til brugerens hjemmekatalog
5. Serveren undersøger om clienten er anført i /etc/hosts.equiv, hvis userid er forskellig fra 0
6. Hvis userid er forskellig fra 0 eller 5) fejler: Serveren undersøger om clienten er anført i $HOME/.rhosts

11.2 Login på en anden host vha. rlogin

Fra hosten ved navn ka7 (host1) kan brugeren mes nu med følgende kommando logge direkte ind på host2 uden afgivelse af login og password, **/etc/profile** og **.profile** vil blive udført på den anden host på sædvanlig måde:

```
rlogin unv6
```

Det samme kan imidlertid også bruger jst, som mes har anført i sin .rhosts fil på unv6 (host2). Jst skal på ka7 (host1) afgive kommandoen:

```
rlogin unv6 -l mes
```

Man skal således være klar over den sikkerhedsrisiko man løber, når man som i eksemplet her "overlader" andre ens login.

Eksempelvis kan en superbruger på ka7 skifte til mes bruger-identitet og dernæst logge sig ind på unv6.

Når man ønsker at afbryde forbindelsen til den anden host, kan man skrive: ~. (tilde efterfulgt af punktum), eller logge ud på helt sædvanlig vis, men hvis man f.eks. har forsøgt at logge på en host, der er nede, vil **login** fortsætte med at forsøge at skabe forbindelsen i et stykke tid, inden den giver op. Dette kan dog også afbrydes med <Ctrl + C>.

VTI håndteringen vil med rlogin foregå fra den lokale host, så man behøver ikke sende terminology i sin **.profile**, når man kører **rlogin**.

11.3 Udførelse af kommandoer på en anden host vha. remsh

Fra hosten ka7 (host1) kan brugeren mes udføre flg. kommando, der udskriver passwd-filen på unv6, host2, vha. en spoolerkø på unv6:

```
remsh unv6 lp -dprint10 /etc/passwd
```

- og brugeren jst kan fra ka7 udføre kommandoer således:

```
remsh unv6 -l mes lp -dprint10 /etc/passwd

remsh unv6 -l mes grep :: /etc/passwd
```

Hvis der benyttes omdirigering:

```
remsh unv6 ls -l > filliste
```

vil der blive oprettet en ny fil ved navn **filliste** på den lokale host. Ønsker man, at omdirigeringen skal ske på den anden host, skal omdirigeringstegnet skrives i anførselstegn:

```
remsh unv6 ls -l ">" filliste
```

En sidste mulighed er, at man kan benytte **remsh** til at logge på en anden host ved at skrive:

```
remsh unv6
```

uden at angive kommando efter. Her gælder samme regler som for **rlogin.**

I kataloget /usr/hosts ligger en kommandofil ved navn **MAKEHOSTS**. Udførsel af denne vil lave et link fra hver af de symbolske navne i **/etc/hosts** til filen **/usr/bin/remsh**, således at der efter denne kommando for hver linie i **/etc/hosts** vil ligge en fil i kataloget **/usr/hosts**, der er linket til **/usr/bin/remsh**.

Hvis man har sti til **/usr/hosts**, vil man kunne udføre kommandoen **who** på hosten **unv10** ved at skrive:

```
unv10 who
```

eller køre **rlogin** til hosten **unv10** ved simpelthen at skrive navnet.

11.4 Kopiering af filer ved hjælp af rcp

rcp fungerer ligesom UNIX kommandoen **cp**. Hvis man har rettighed til at læse en fil, har man også rettighed til at kopiere den. Forskellen er, at **rcp** også fungerer mellem to forskellige hosts, hvis man har adgang til en anden hosts ved hjælp af .rhosts eller /etc/hosts.equiv:

```
rcp unv8:/usr/lanman/users/jst/cls unv8.cls
```

Man angiver hostnavnet først, og derefter angives sti til den fil, man ønsker at kopiere.

Hvis der angives relativ sti, vil det blive fortolket som relativt til brugerens hjemmekatalog på den anden host.

Rcp prompter ikke for password. Det anvendte login skal også eksistere på den anden host og tillade remote udførsel med **remsh**.

Man kan også kopiere fra en anden bruger på den anden host ved at benytte følgende syntax:

```
rcp unv8.afs:fil unv10.modt:unv8.fil
```

Her kopieres fra brugeren afs på unv8 til brugeren modt på unv10.

For at dette er muligt, skal **.rhosts** filen på unv10 i brugeren modt's hjemmekatalog, og i brugeren afs' hjemmekatalog på unv8 begge indeholde en linie med den bruger, der afgiver kommandoen på unv8.

Denne remote processing bliver udført ved at køre fra brugerens login shell. Brugerens .profile vil blive udført inden filnavne fortolkes, så derfor kan shell-variable benyttes i remote filnavne.

Med kommanndoen **rcp** kan man kopiere hele katalogstrukturer ved at benytte option **-r**, som beskriver, at kopieringen skal ske rekursivt:

```
rcp -r unv8:katalog unv8.kat
```

Her kopieres hele katalog strukturen **katalog** fra brugerens hjemmekatalog på unv8 til et underkatalog på den lokale host ved navn **unv8.kat**.

Opgave

Formål: *- at afprøve de forskellige former for remote utilities*

- at sætte op til at kunne køre rlogin, remsh og rcp

1. **Prøv, at logge dig på unv3 med rlogin med samme login, som du er logget på med nu på unv7.**

2. **Se med kommandoen tty, hvilken tty du er logget på.**

3. **Sørg for at du har password på unv3.**

4. **Gå tilbage til unv7 ved at taste exit.**

5. **Link /usr/bin/remsh til en fil i dit hjemmekatalog på unv7 ved navn unv3 ved at give kommandoen:**

   ln -s /usr/bin/remsh $HOME/unv3

6. **Benyt denne fil til at logge dig på unv3.**

7. **Opret filen .rhosts på unv3 i dit hjemmekatalog, så du kan logge dig på unv3 uden at afgive password.**

8. **Afprøv at det virker ved at benytte din unv3-fil på unv7.**

9. **Rediger nu i din .rhosts fil på unv3, så din nabo kan logge sig på unv3 med dit login. Afprøv sammen med din nabo, at det virker.**

10. **Gå tilbage til unv7, og udfør kommandoen who på unv3 ved hjælp af remsh, som jo er den unv3 fil, du har oprettet i dit hjemmekatalog.**

11. **Udfør nu kommandoen igen på unv3, men under din nabos login.**

...opgaven fortsættes på næste side

12. **Kopiér en fil fra dit hjemmekatalog på unv7 til dit hjemmekatalog på unv3.**

13. **Kopiér en fil fra dit hjemmekatalog på unv7 til din nabos hjemmekatalog på unv3. Hvorfor kan du få lov til det?**

12. Appendiks, PC/TCP

PC/TCP er en TCP/IP program pakke til PC'er, der leveres af et firma, der lidt forvirrende hedder **FTP**. Mange kender bedst PC/TCP ved, at det er "dem med de grønne mapper".

Tidligere var FTP's PC/TCP, den mest udbredte TCP/IP pakke til PC'er, men Microsoft har efterhånden taget den største del af kagen, ved at levere TCP/IP med sammen med Windows for Workgroups, LAN Manager, Windows 95 og NT.

12.1 Konfiguration af PC'er

Det følgende beskriver konfigurationen af en PC af typen NCR 316L med 4,6 Mb RAM og 40 Mb harddisk med SMC's EtherCard PLUS, Elite Netkort (tidl. Western Digital).

Med disse netkort leveres en række disketter. Her findes bl.a. et konfigurations program **EZSETUP**.

Her vælges følgende for PC'er uden BOOT Prom:

I/O BASE	280
IRQ	5 (Bruges normalt af LPT2:)
RAM base	C8000
Add wait states	Yes
ROM size	Disabled
ROM base	Disabled

og for PC'er med aktiv BOOT Prom:

I/O BASE	280
IRQ	5 (Bruges normalt af LPT2:)
RAM base	D0000
Add wait states	Yes
ROM size	16 K
ROM base	CC000

Ved indtastning af RAM base skal man kun indtaste 5 cifre, således at tallet **D0000** indtastes som **D000**.

Herefter kopieres følgende filer fra original disketterne til et katalog på harddisken, **C:**:

HOSTS	Svarer til Supermax'ens /etc/hosts
IFCONFIG.EXE	Konfigurationsprogram til netværks interface software device driver modulet
INET.EXE	
IPCONFIG.EXE	Konfigurationsprogram til Internet protokollens software device driver modul
NETBIOS.EXE	
PING.EXE	
WD8003.EXE	TCP/IP kerne programmet
WD8003.SYS	Netværks interface software device driver modul
IPCUST.SYS	Internet protokollens software device driver modul

Konfiguration:

- **Skift til kataloget C:\FTP, og giv følgende kommandoer:**

```
IFCONFIG WD8003.SYS <IP-adresse>
IFCONFIG WD8003.SYS BASE 0x280
IFCONFIG WD8003.SYS MEMORY 0xC800
                (med BOOT Prom dog 0xd000)
IFCONFIG WD8003.SYS INT 5
IFCONFIG WD8003.SYS SUBNET 0

IPCONFIG IPCUST.SYS WINDOW 4380
IPCONFIG IPCUST.SYS HOSTTABLE C:
IPCONFIG IPCUST.SYS USERID <login>
```

Ved andre NCR PC'ere (3210) skal memory dog også sættes til **D0000**.

Konfigurationen af **WD8003.SYS** kan kontrolleres ved kommandoen:

```
IFCONFIG WD8003.SYS SHOW
```

og konfigurationen af **IPCUST.SYS** kan kontrolleres ved kommandoen:

```
IPCONFIG IPCUST.SYS SHOW
```

- **Lav en host tabel, C:\FTP, hvis der skal køres f.eks. Terminalemulering med DDE-Term:**

```
89.11.0.11      unv4
89.11.0.12      unv10
89.11.0.13      unv8
```

- **Indsæt følgende to linier i CONFIG.SYS:**

```
DEVICE=C:\FTP\WD8003.SYS
DEVICE=C:\FTP\IPCUST.SYS
```

- **Indsæt følgende to linier i AUTOEXEC.BAT:**

```
C:\FTP\WD8003 -P 10 -T 3
C:\FTP NETBIOS -S ""
```

- **Boot PC'en**

Den første linie i **AUTOEXEC.BAT** afsætter en række buffere. De angivne parametre vil være nok til 3 TCP forbindelser, hvilket svarer til en LM/X server og en terminalopkopling. Hvis man ønsker flere TCP forbindelser, må dette sættes op.

Herefter kan man teste, om der er "hul" igennem ved at taste:

```
PING UNV8
```

hvis **UNV8** er en host, der er defineret i filen **C:\FTP\HOSTS**.

Opgave

Formål: - at se på konfigurationen af PC'en

1. **List indholdet af ipcust.sys ved hjælp af ipconfig.**

   Hvilket username er knyttet til PC'en?

2. **List indholdet af wd8003.sys ved hjælp af ifconfig.**

   Hvilken interruptvektor benyttes?
   Hvad er PC'ens IP adresse?

3. **Hvilke hosts er defineret i PC'ens hostfil?**

Index

—S—

—T—

—U—

—V—

—W—

Dansk Data Elektronik A/S
Herlev Hovedgade 199
DK 2730 Herlev
Tel.: (+45) 42 84 50 11
Fax: (+45) 42 84 52 20