

# Kapitel 6

## TCP/IP i praktiken

### 6.1 Konfigurationsfiler

Var inställningar sparas varierar mellan de olika distributionerna. Men det är förstås i textfiler, även om man även kan göra det grafiskt är det bra att känna till hur man gör det i Vim eller Emacs.

### 6.2 Konfigurationsfiler Red Hat

I Red Hat-baserade distar sparas IP och mask för varje interface i en separat fil under `/etc/sysconfig/network-scripts/`. Till exempel `ifcfg-eth0`, `ifcfg-eth1` och `ifcfg-eth0:0` (den sistnämnda ifall man har flera IP på samma kort).

Innehållet kan se ut så här för en dator som får dynamiskt tilldelat IP:

```
# nVidia Corporation MCP55 Ethernet
DEVICE=eth0
HWADDR=00:1D:60:CB:F1:34
ONBOOT=yes
BOOTPROTO=dhcp
```

Och för ett interface med statiskt IP (som man oftast har på servrar):

```
# VIA Technologies, Inc. VT6105 [Rhine-III]
DEVICE=eth0
HWADDR=00:11:95:86:29:A2
IPADDR=85.231.1.37
IPV6ADDR=
IPV6PREFIX=
NETMASK=255.255.254.0
BROADCAST=85.231.1.255
NETWORK=85.231.0.0
GATEWAY=85.231.0.1
ONBOOT=yes
```

Denna dator har bara IPv4 konfigurerat, men man ser nyckelorden även för IPv6. Första raden är bara en kommentar. Raden med DEVICE är lätt att glömma att ändra om man kopierar en fil, som från `ifcfg-eth2` till `ifcfg-eth1` om man vill byta plats på dem. Numrering av korten börjar med 0. HWADDR är MAC-adressen. De andra är ganska uppenbart vad de är. Har man glömt bort vad nyckelorden heter kan man kolla dokumentation med:

```
less /usr/share/doc/initscripts-*/sysconfig.txt
```

(jag anger \* i stället för versionsnummer som kan variera).

Nätverksinställningar som är gemensamma för alla interface sparas i `/etc/sysconfig/network` Den kan se ut så här:

```
NETWORKING=yes
HOSTNAME=einstein.df.lth.se
```

(I äldre versioner angav man även GATEWAY i den filen). För att starta om nätverket efter ändringar kör man:

```
/etc/init.d/network restart
```

Inget ändras alltså direkt när man ändrar i filerna. Vill du byta IP-nummer på en maskin som du är inloggad på utifrån kan du alltså ändra i `ifcfg-eth0`, dubbelkolla att allt är rätt, eventuellt även ändra i `/etc/hosts` och `/etc/resolv.conf` och sen köra `sudo reboot`. Du bör avinstallera Network-Manager på servrar och andra maskiner med statiskt IP-nummer. Det gör man med:

```
sudo rpm -e NetworkManager NetworkManager-gnome
```

(Den med `-gnome` finns bara om du har grafiskt gränssnitt installerat.)

## 6.3 Konfigurationsfiler Debian

I Debian och Ubuntu sparas nätverksinformationen i en fil som heter `/etc/network/interfaces` Den kan se ut så här:

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 93.182.128.66
    netmask 255.255.255.248
    network 93.182.128.64
    broadcast 93.182.128.71
    gateway 93.182.128.65
    dns-nameservers 93.182.182.85
    dns-search adderat.se

auto eth1
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
```

Man anger alltså inställningar för alla interface i samma fil. Raden med `auto eth0` anger att `eth0` ska startas vid boot, och rader med `iface` inleder konfiguration för respektive interface. I filen har man ofta indrag som gör texten mer tydlig.

## 6.4 ifconfig och ip

För att kolla vilka IP-nummer och annat som används kan man köra `/sbin/ifconfig`. Utdata från det kommandot kan

se ut så här:

```
eth0 Link encap:Ethernet HWaddr 00:24:8C:56:9D:0A
inet addr:194.47.250.234 Bcast:194.47.250.255
Mask:255.255.255.0
inet6 addr: fe80::224:8cff:fe56:9d0a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:89181382 errors:0 dropped:0 overruns:0
frame:0
TX packets:42064625 errors:0 dropped:0 overruns:0
carrier:0
collisions:0 txqueuelen:1000
RX bytes:45161883888 (42.0 GiB)
TX bytes:52540751326 (48.9 GiB)
Interrupt:25 Base address:0x8000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:30869 errors:0 dropped:0 overruns:0 frame:0
TX packets:30869 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:47404698 (45.2 MiB) TX bytes:47404698 (45.2
MiB)
```

Det man bör kolla i utdatan från ifconfig är att IP-nummer och mask är rätt, att det står UP och att räknarna för olika fel står på 0. Gränssnittet lo är loopback, det måste alltid finnas och har alltid adressen 127.0.0.1. Vanliga nätverkskort har namn som eth0 och eth1.

Med ifconfig kan man även göra tillfälliga ändringar, till exempel genom `sudo /sbin/ifconfig eth1 192.168.0.12` för att tilldela detta IP-nummer. Nätmask blir den som är standard för klass A, B och C, vill man ha en annan får man ange det:

```
ifconfig eth1 192.168.0.12 netmask 255.255.255.240
```

Ändringar som man gör på detta vis sparas inte över en reboot, så mer permanenta ändringar bör göras i konfigurationsfilerna.

Vill du tilldela en extra adress till ett befintligt interface använder du ett alias, som anges med kolon. Till exem-

pel `sudo /sbin/ifconfig eth0:0 192.168.22.100`, då behåller det vanliga `eth0` sina inställningar. Du kan ha många olika adresser med `eth0:0`, `eth0:1`, `eth0:2` osv.

För att ange default gateway kan man använda kommandot `route`. Så här:

```
sudo /sbin/route add default gw 192.168.0.1
```

För att visa routingtabellen skriver man endast `route` eller `netstat -rn`. Kommandot `netstat` funkar även på andra UNIX-system där kommandot `route` inte finns eller har annan syntax.

Ett nyare kommando för att ändra nätverksinställningar är `ip`, även det brukar ligga i katalogen `/sbin`. Med `ip` kan man göra samma ändringar som med `ifconfig`, `route` och mycket mera. Se man `ip` för mer info.

## 6.5 Felsökning av nätverk

Ett vanligt kommando för att kolla om två datorer kan nå varandra är `ping`. Det skickar ICMP echo request och tar emot echo reply. Exempel:

```
[ao@a GLAN]\$ ping google.se
PING google.se (173.194.69.94) 56(84) bytes of data:
64 bytes from bk-in-f94.1e100.net (173.194.69.94):
  icmp_seq=1 ttl=45 time=48.0 ms
64 bytes from bk-in-f94.1e100.net (173.194.69.94):
  icmp_seq=2 ttl=45 time=48.1 ms
64 bytes from bk-in-f94.1e100.net (173.194.69.94):
  icmp_seq=3 ttl=45 time=48.1 ms
^C
--- google.se ping statistics ---
3 packets transmitted, 3 received, 0% packet loss,
  time 2498ms\
rtt min/avg/max/mdev = 48.072/48.115/48.172/0.042 ms
[ao@a GLAN]$
```

Du avslutar alltså med **ctrl-c**, eller anger antalet ping med `-c` siffra. Det är inte alla datorer, routrar och brandväggar som släpper igenom ping, men `google.se`, `ping.lu.se` och `ping.se` är tre man kan testa med.

Vill du bara slå upp en dators namn i DNS är det bättre med `dig` eller `nslookup` än att pinga dem.

Felsökning bör man göra systematiskt. Till exempel först pinga din egen dator, det IP som ifconfig visar. Sen din gateways IP och eventuellt en annan dator på samma LAN. Går de att nå via IP-nummer, men inte via namn så är det /etc/resolv.conf du ska titta på. Går de inte ens att nå via IP-nummer kan du kolla kablar och switchar, utdata från `dmesg|grep eth` och köra kommandot `ethtool`. Ifall du har kontakt med LAN men inget utanför bör du kolla så du har rätt gateway. Om du har kontakt utåt men inte alla datorer på LAN:et bör du kolla nätmasken.

Två andra bra kommandon vid felsökning är `traceroute` och `tracepath`. Dessa visar vilken väg paketet tar till mottagaren:

```
[ao@a ~]$ tracepath ping.lu.se
1:  h87-96-232-78.dynamic.se.alltele.net (87.96.232.78)
    0.049ms pmtu 1500
1:  h87-96-232-1.dynamic.se.alltele.net (87.96.232.1)
    0.775ms
1:  h87-96-232-1.dynamic.se.alltele.net (87.96.232.1)
    0.671ms
2:  93.182.178.145 (93.182.178.145)
    1.476ms
3:  h87-96-255-42.dynamic.se.alltele.net (87.96.255.42)
    1.443ms
4:  sema10001-rc3.ip-only.net (82.99.32.69)
    1.076ms
5:  sema10001-rc2.ip-only.net (62.109.44.126)
    4.133ms
6:  c2sth-ge-5-1-0.sunet.se (195.69.117.19)
    1.292ms
7:  t1fre-ge-5-1-1.sunet.se (130.242.82.101)
    10.722ms asymm 9
8:  m1fre-ae1-v1.sunet.se (130.242.83.45)
    10.701ms asymm 9
9:  lu-br1-xe-1-2-0.sunet.se (130.242.85.2)
    20.295ms asymm 10
10: lu-g.sunet.se (193.11.20.10)
    29.109ms asymm 11
11: c002--x001.net.lu.se (130.235.217.13)
    25.302ms asymm 12
12: d001a--c002.net.lu.se (130.235.217.34)
    23.842ms asymm 13
```

```
13: nomina.net.lu.se (130.235.132.90)
    20.500ms reached
    Resume: pmtu 1500 hops 13 back 242
[ao@a ~]$
```

Där ser man vägen från min dator till ping.lu.se (även kallad nomina). (Raderna är brutna här i boken, egentligen kommer tiden direkt efter namnet.) Först på alldeles nät, sen på IP-Onlys och i Stockholm (Netnod) över till Sunet och ner till Lund igen. Det är inte heller alla routers som släpper igenom de paket som traceroute och tracepath använder. Ofta visas enbart \* i stället för namn. Ibland funkar den ena men inte den andra. Men när de funkar kan man se vilka ställen som tar mest tid (t.ex. hopp över Atlanten). Och om det inte funkar kan man se var det stannar. Ibland hoppar paketen fram och tillbaka mellan två eller tre routrar, så kallad loop. Det beror ofta på felkonfiguration eller annat tillfälligt fel.

En annan vanlig källa till fel och problem är felkonfigurerad brandvägg. Se mer om den i nästa kapitel.

## 6.6 ethtool

Jag nämnde tidigare ethtool. Det är ett bra program för att felsöka på länknivån. Så här kan utdata se ut för ett gigabitkort kopplad till en switch med 100 Mbps:

```
$ sudo /sbin/ethtool eth0
Settings for eth0:
Supported ports: [ TP MII ]
Supported link modes:   10baseT/Half 10baseT/Full
                       100baseT/Half 100baseT/Full
                       1000baseT/Half 1000baseT/Full

Supported pause frame use: No
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
                       100baseT/Half 100baseT/Full
                       1000baseT/Half 1000baseT/Full

Advertised pause frame use: Symmetric Receive-only
Advertised auto-negotiation: Yes
Link partner advertised link modes:
                           10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
```

```
Link partner advertised pause frame use: Symmetric
Link partner advertised auto-negotiation: Yes
Speed: 100Mb/s
Duplex: Full
Port: MII
PHYAD: 0
Transceiver: internal
Auto-negotiation: on
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x00000033 (51)
      drv probe ifdown ifup
Link detected: yes
$
```

Det man bör kolla är sista raden, att det finns länk. Även att Speed och Duplex är rätt. I de fall där auto-negotiation inte fungerar rätt så kan du sätta hastighet manuellt, till 100 Mbps och FD med:

```
ethtool -s eth0 speed 100 duplex full autoneg off
```

Om du glömmer att stänga av autoneg så kommer switchen kanske att förhandla fram fel hastighet eller halv duplex. Bäst är förstås om det blir rätt automatiskt, men jag har råkat ut för switchar som gör fel, ibland enbart på vissa portar. Om det är möjligt bör du även låsa switchporten till samma hastighet och duplex som datorn. Ibland kan man även behöva låsa hastigheten till 10 Mbps, men det är en nödlösning. Du får prova dig fram, och kolla inställningarna med `ethtool`, gärna med några `ping -f` av din gw mellan testerna. Symtom på felaktiga duplexinställningar är paketförlust, kollisioner och låg prestanda.