

MAGISTERUPPSATS I INFORMATIK
VID INSTITUTIONEN FÖR DATA- OCH AFFÄRSVETENSKAP
1997:M01

Översättning av nätverksadresser

Bilaga B – Installationsanvisningar

Johan Sanneblad

Handledare: Fil. Dr. Bertil Lind

vt 1998



HÖGSKOLAN
I BORÅS

Förord

Denna bilaga är det arbetsdokument jag sammanställde för att garantera en homogen installation på samtliga i projektet involverade datorer. För att själv kunna följa instruktionerna och skapa ett eget system krävs det både kunskap om operativsystemet UNIX tillsammans med viss kännedom om installationsprogrammet till distributionen Redhat Linux 5.0. UNIX-kunskapen sträcker sig som mest till vetenskapen om hur man redigerar filer, startar program eller förflyttar sig mellan olika kataloger i filsystemet.

Skulle det vara så att man vill spara in den mindre summa pengar som Redhat Linux 5.0 kostar, så går det bra att gratis hämta samtliga installationsfiler och användardokumentationen över Internet. Det krävs då att man samtidigt installerar och anpassar en så kallad FTP-server på en av de övriga anslutna datorerna i det lokala nätverket. Detta krävs även om den blivande serverdatorn ej har någon inbyggd CD-Rom läsare.

Jag vill slutligen påpeka att detta arbetsdokument, till skillnad från huvuddokumentet, främst riktar sig till nätverkskunnig personal, med viss kunskap om hur bakomliggande tekniker fungerar och med arbetsvana i såväl Windows- och UNIXmiljöer. Denna tekniska nivå märks tydligt då det här nämns ett flertal tekniker såsom DNS, WINS och NetBIOS vilka ej är definierade i huvuddokumentet. Man ej behöver ha kunskap om teknikerna för att förstå systemets funktionalitet, men man måste känna till dem för att kunna installera och administrera systemet. Skulle dessa teorier även tas upp i huvuddokumentet skulle det bli så stort och otympligt att det troligtvis ej skulle passa någon läsare.

Johan Sanneblad

Borås, den 14 april 1998

Innehållsförteckning

1	INSTALLATION AV LINUX	1
1.1	NYHETER OCH UPPDATERINGAR	1
1.2	FÖRBERED INSTALLATIONEN	2
1.3	INSTALLATION	2
1.3.1	<i>Förberedande åtgärder</i>	<i>3</i>
1.3.2	<i>RedHat installation.....</i>	<i>3</i>
1.3.3	<i>Efter omstart.....</i>	<i>5</i>
1.3.4	<i>Programuppdatering</i>	<i>6</i>
1.3.5	<i>Skrivare</i>	<i>7</i>
2	INSTALLATION AV ÖVRIGA DATORER.....	9
2.1	NÄTVERKSKONFIGURATION.....	9
2.1.1	<i>Gateway.....</i>	<i>9</i>
2.1.2	<i>DNS</i>	<i>9</i>
2.1.3	<i>WINS.....</i>	<i>9</i>
2.1.4	<i>Egenheter med Windows 95, 98 och NT.....</i>	<i>10</i>
3	LINUX PPP	11
3.1	INSTÄLLNINGAR.....	11
3.2	TEST	12
4	LINUX SOM BRANDVÄGG	13
4.1	HOSTS.....	13
4.2	IP MASQUERADE	13
4.2.1	<i>Rättigheter och funktionalitet.....</i>	<i>13</i>
4.2.2	<i>IP_Forward.....</i>	<i>14</i>
4.2.3	<i>Dynamiskt IP</i>	<i>14</i>
4.2.4	<i>Tidsbegränsning</i>	<i>15</i>
5	LINUX DIAL-ON-DEMAND	17
5.1	KONFIGURATIONSFILER	17

6	FELSÖKNING.....	19
6.1	PAKETÖVERVAKNING	19
6.2	SESSIONSFEL.....	19
6.3	LOGFILER.....	20
7	REKOMMENDERAD LÄSNING	23
7.1	LINUX MANUALFILER.....	23
7.2	INTERNETSIDOR	23
7.3	LITTERATUR	23

1 Installation av Linux

1.1 Nyheter och uppdateringar

Även om det mesta som krävs för en komplett installation av Linux som nätverksadressöversättare följer med som standard finns det en del filer som saknas. Följande tre filer krävs för en fungerande installation:

**ftp://ftp.redhat.com/pub/contrib/hurricane/i386/
diald-0.16-3glibc.i386.rpm** (98-01-19)

**ftp://ftp.meme.com/pub/software/diald-config
diald-config-1.2.1-1.noarch.rpm** (98-01-19)
diald-config-metered-0.2-2.noarch.rpm (98-01-08)

Då samtliga datorprogram innehåller fel, är ej heller Redhats Linuxdistribution felfri. Följande uppdateringar är det absolut nödvändigt att man tar hem innan installationsarbetet påbörjas.

**ftp://ftp.redhat.com/pub/redhat/redhat-5.0/updates/i386/
initscripts-3.30-1.i386.rpm** (97-12-30)
ppp-2.3.3-2.i386.rpm (98-01-16)

För att kunna använda filerna då Linuxsystemet väl är installerat rekommenderas att nedhämtning sker före det att installationen påbörjats. Filerna kan under tiden placeras temporärt på en av datorerna i det lokala nätverket för senare överflyttning till Linuxservern.

De revisionsnummer i uppgraderingarna som redovisats ovan är säkerligen ej aktuella då detta dokument kommer i tryck. Man bör därför söka efter uppdateringar med samma namn, men annat suffix (exempelvis ppp-?.?.?-?.i386.rpm och initscripts-?.?.?.i386.rpm).

1.2 Förbered installationen

För att installera Redhat Linux krävs det att filerna som behövs finns tillgängliga. För erhålla dessa filer kan man antingen beställa hem dem från RedHat software då man samtidigt får hem en tryckt användardokumentation och installationsanvisning, eller genom att låta en valfri dator hämta samtliga installationsfiler och dokument över Internet, för att senare installera Linuxsystemet från denna över det lokala nätverket. Denna sistnämnda metod måste även användas om Linuxsystemet ej är utrustad med en CDRom-läsare, eftersom man kan använda CDRom-läsaren hos en annan dator för installationen. Tekniken som används då kallas för FTP-installation.

För att utföra denna typ av installation ansluts den blivande Linuxservern till en annan dator på nätverket med hjälp av BNC- eller TP-anslutning, varvid den andra datorn konfigureras som FTP-server. Detta innebär att det kommer att vara möjligt att hämta filer från den över det lokala nätverket.

En lämplig plats att hämta hem en FTP-server från är amerikanska tu cows, där den svenska speglingen ligger på adress <http://ftp.sunet.se/tucows/server95.html>. En passande FTP-server som går att starta under både Windows95 och Windows NT är WarFTP, som går att ta hem på adressen <http://home.sol.no/~jarlaase/tftpd.htm>.

I installationen som redovisas under stycke 1.3 använder jag en WarFTP-server på IP-adress 192.168.1.2, som är en av datorerna i det lokala nätverket. Microsofts Peer Webservices 3.0 under WindowsNT-workstation bör ej användas som FTP-server, då den förstör uppkopplingen efter ett slumpmässigt tidsintervall.

För att tilldela adresser till datorerna inom det lokala nätverket hänvisas till huvuddokumentet, stycke 2.2.1. Jag kommer i detta dokument att placera det lokala nätverket i klassC-nätet 192.168, med subnät 1 som är ett av de rekommenderade näten för lokala nätverk. Linuxservern kommer att placeras på adressen 192.168.1.1, med övriga datorer placerade i intervallet 192.168.1.2 -> 192.168.1.253. IP-adressen 192.168.1.254 kommer senare att nyttjas av programmet DialD på Linuxservern vilket gör att tilldelning ej får ske på denna adress.

1.3 Installation

Här kommer samtliga installationsalternativ jag valde för att installera Linuxsystemet att redovisas. För mer information om specialanpassning av systemet rekommenderas RedHat Linux användarmanual. Man bör dock

välja minst de installationspaket som jag valt då systemet riskerar att ej fungera om nödvändiga komponenter selekteras bort.

Datorerna som jag installerar RedHat Linux 5.0 på har följande konfiguration:

CPU: Intel 486-66mhz
Ram: 16mb (1x16mb Simm)
Grafik: Cirrus Logic CL-5424 VLB
Hårddisk: Connor CFS210A, 203mb
Nätverkskort: Novell NE-2000 ISA

Observera att när datorn väl är installerad behövs varken skärm, tangentbord eller mus, eftersom det då är möjligt att styra hela operativsystemet via nätverket från en annan dator (det går till och med att stänga av eller starta om datorn). Fördelarna är flera med att ej koppla några tillbehör till datorn, bland annat så får man en relativt kompakt låda som kan undanrömmas praktiskt taget var som helst.

1.3.1 Förberedande åtgärder

För att installera RedHat Linux 5.0 krävs det två stycken floppydisketter. Dessa skapas från cd-skivan eller från hemtagna filer med hjälp av kommandot *rawrite.exe*. Filerna som krävs av *rawrite.exe* ligger under katalogen *images* och heter *boot.img* samt *supp.img*.

1.3.2 RedHat installation

Nedan följer en exakt kopia av de val jag personligen gjort vid installationen av Linux. Antagligen behöver värden som påverkar skärmval, grafikkort, nätverkskort och partitionsstorlekar av hårddisk att justeras individuellt för olika system. För mer information hänvisas till användarmanualen som följer med distributionen. Finns det CDRom-läsare på datorn och skivan med installationsfiler finns tillgänglig bör ej ftp-installation väljas som nedan.

```
Color monitor          yes
Welcome to Redhat Linux <ok>
Keyboard               se-latin1
Package media         ftp
Insert supplemental disk <ok>
New system             install
Scsi                   no
Disk setup             disk druid
```

Följande är den partitionsstruktur jag använder för att organisera datorernas hårddiskar:

```
Disk Druid
Mount point  Device      Requested  Actual    Type
/            hda1        156M      156M     Linux native
            hda5        32M       32M     Linux swap
/var         hda6        15M       15M     Linux native
```

Namnet på partitionerna (hda<x>) samt ordningen är ej relevant. Om Linux skall installeras parallellt med ett befintligt dossystem så måste alltid dospartitionen skapas först med hjälp av doskommandot *fdisk*. Lämplig mount-point för denna dospartition är i så fall */mnt/dos1* eller motsvarande. Det är mycket viktigt att man *först* installerar Windows95 eller annat operativsystem före det att Linux installeras, annars försvinner hårddiskens bootsektor som innehåller LiLo (Linux Loader) som ser till att Linux startas. Visserligen går det att säkerhetskopiera bootsektorn till diskett men det innebär då onödigt merarbete.

```
Active swap space      <ok>
Load module            NE2000 and compatible
Module options         Autoprobe
```

Nu följer nätverksinställningarna. Då det lokala nätverket skall ligga på klassC-nätverket 192.168.1.0, och min ISP's nameserver är 10.0.0.1 kommer det att se ut enligt följande (10.0.0.2 är den sekundära nameservern). Namnet på linuxservern har jag satt till "linuxsrv", vilket kan ersättas med valfritt alternativ. Om CDRom-baserad installation väljs kommer nedanstående information om FTP-parametrar ej att redovisas.

```
Configure TCP/IP
[_] Configure device with bootp
IP address:            192.168.1.1
Netmask:               255.255.255.0
Default gateway (IP):
Primary nameserver:    10.0.0.1

Configure Network
Domain name:           .
Host name:             linuxsrv
Secondary nameserver (IP): 10.0.0.2
Tertiary nameserver (IP):

FTP Setup
FTP site name:         192.168.1.2
Red Hat directory:    /

Format partitions:    <samtliga partitioner markerade, med check>

Components to install:
[X] Printer support
[X] X Window System
```

```

[X] Print Server
[X] Networked Workstation
[X] Dialup Workstation
[X] Network Management Workstation

Install log:                <ok>
Probing result (mouse):    <ok>
Configure mouse:           Microsoft compatible, [X] Emulate 3 buttons

Choose a card:              Cirrus logic GD542X
Monitor setup:              Custom (Non-Interlaced SVGA, 50-70)
Screen configuration:       Probe
Probing finished:           <Let Me Choose>, 800x600x8bit
Network configuration:      Keep this setup
Configure Timezones:        [_] Hardware clock GMT, Europe/Stockholm
Services:                   <ok>

Configure Printer:          <Yes>, Local, <Next>, <Next>
Configure Printer:          PostScript printer
Configure Printer:          a4, 600x600, [_] Fix stair-stepping of text

Root Password:              hemligtlösen
Root Password (again):     hemligtlösen

Lilo installation:          /dev/hda (Master Boot Record)
Lilo installation:          [_] Use linear mode

```

1.3.3 Efter omstart

Efter omstart ansluter man till datorn som root-användare och startar X-Windows (startx). Det är här viktigt att göra samtliga inställningar vad gäller användare, skrivare, modeminställningar och PPP-anslutningar (nätverksinställningar) genom kontrollpanelen så att man senare slipper förlita sig på endast konfigurationsfiler.

Det är mycket viktigt att snarast skapa ytterligare en användare förutom root. Till detta används user-id ≥ 100 , samt usergrp = 100. Orsaken är att det ej går att ansluta till Linuxmaskinen som root över nätverket om något skulle gå snett.

Följande saker bör vara avklarade innan man går vidare till nästa stycke:

- En ny användare med förslagsvis id 500, grupp 100 bör ha skapats
- Modemet bör ha konfigurerats till att nyttja korrekt com<x> port
- En ppp-anslutning bör ha definierats genom nätverksinställningarna.

När ppp-anslutningen skapas går det utmärkt att acceptera standardvalen. Endast om datorn (liksom min i exemplet) ej har avancerade serieportar (16550A eller bättre) behöver man välja "customize" och ändra portens hastighet till ett värde mindre än 115200 (jag använder 38400 bps). Avseende

val av verifikationsmetod bör PAP väljas, då samtliga ISP i Sverige idag använder denna standard och man då slipper använda skriptfiler för verifikation. Används en extern ISDN-adapter är det viktigt att korrekta parametrar även anges för att boxen skall fungera som ett vanligt modem, fast då med 64kbits synkron överföringshastighet.

1.3.4 Programuppdatering

För att uppdatera programmen i systemet ansluter man först som rootanvändare och skapar sedan katalogen */tmp/rpms*. Efter det ansluter man sig mot den FTP-Server som innehåller de uppdateringar som hämtades tidigare, varvid samtliga filer förs över (6 stycken totalt) till denna katalog. Det går även att utföra detta genom att spara filerna till en floppydisk och senare läsa denna från Linuxsystemet.

Installera sedan följande uppdateringar genom att skriva:

- `rpm -U initscripts-3.30-1.i386.rpm`
- `rpm -U ppp-2.3.3-2.i386.rpm`

Installera sedan dial-on-demand genom att skriva:

- `rpm -i diald-0.16-3glibc.i386.rpm`
- `rpm -i diald-config-1.2.1-1.noarch.rpm`
- `rpm -i diald-config-metered-0.2-2.noarch.rpm`

För att få information om var ett paket placerar sig kan man skriva:

```
rpm -q -l -p <paketnamn.rpm> | more
```

För att få information om ett specifikt paket är installerat kan man skriva:

```
rpm -q -a | grep <tecken i paketnamnet>
```

Då datorn ej skall fungera som epostserver, finns det utrymme att spara på hårddisken genom att även avinstallera en del paket. Följande procedur raderar hela programsviten sendmail från systemet, vilket görs genom att skriva följande:

- `rpm -e exmh-2.0zeta-4`
- `rpm -e mh-6.8.4-4`
- `rpm -e sendmail-8.8.7-12`

1.3.5 Skrivare

Om man vill använda den nya brandväggen även som skrivarserver så är detta mycket enkelt:

1. Först skapas skrivaren i Linux grafiska kontrollpanelen
2. Efter det att skrivaren skapats registreras namnen på de datorer som skall kunna skriva ut på den i filen */etc/hosts.lpd*. Denna fil skall struktureras med ett namn per rad, och namnen skall vara desamma som fält 2 i filen */etc/hosts*¹. Skall dessa datorer även kunna komma åt andra resurser, som att ansluta via en annan dator etc. kan det vara lämpligt att i stället lägga till dessa datorer i filen */etc/hosts.equiv*, vars struktur är identisk.
3. Om WindowsNT används på klientdatorn lägger man sedan till tjänsten TCP/IP printing, skapar en ny port (LPR) för skrivaren som ansluter till serverns IP-nummer (i det här fallet 192.168.1.1), samt väljer skrivarkö till 'lp'.

Används Windows95 eller Windows98 i det lokala nätverket måste programmet Samba installeras på Linuxservern för att datorerna kunna ansluta till skrivaren, se dokument på Redhats websida som förklarar detta i detalj. Det blir med Samba möjligt att granska skrivaren på Linuxservern under den vanliga Windowsutforskaren, och att ansluta till den blir lika lätt som att klicka med höger musknapp och välja "Anslut".

¹ Se kapitel 4.1 för mer information om filen */etc/hosts*.

2 Installation av övriga datorer

2.1 Nätverkskonfiguration

För information om hur det lokala nätverket bör konfigureras så rekommenderas den utmärkta guiden "Linux IP Masquerade mini HOWTO" [10].

2.1.1 Gateway

"Default Gateway" på respektive maskin sätts till Linuxserverns IP-adress, 192.168.1.1.

2.1.2 DNS

Adressen till den DNS som används skall peka på den av Internetleverantören utsedd dator. För Telia 020 är primär nameserver 10.0.0.1, och sekundär nameserver 10.0.0.2.

2.1.3 WINS

Det existerar en mängd specialfall som leder till att Linuxservern oönskat ansluter sig till Internet. Den största orsaken till detta är att Microsoft Windows, när den hittar en dator i nätverket, försöker använda sig av tjänsten DNS för att se vilket namn datorn har. När denna DNS-server finns hos Internetleverantören innebär det att Windows vid varje kontroll kommer att begära namnet hos datorn där, vilket ej är önskvärt då det trots allt är relativt liten sannolikhet att datorns namn och adress är registrerade hos leverantören. En lösning på problemet är att installera ytterligare en dator i det lokala nätverket som en WindowsNT-server, och på den lägga till tjänsten

Windows Internet Name Service (WINS). Då detta kan bli kostsamt ges i nästa stycke några tips för att undvika detta dilemma.

2.1.4 Egenheter med Windows 95, 98 och NT

Man bör framförallt tänka på att kontrollera så att WINS-klienten är avstängd på samtliga i nätverket anslutna datorer, och att alternativ som "Enable DNS for Windows Resolution" är avstängt på de arbetsstationer som använder WindowsNT. Detta alternativ brukar leda till att WindowsNT-klienterna använder sig av DNS för att se namnen på övriga datorer som är anslutna till nätverket, vilket i sin tur kommer att leda till oönskade uppkopplingar till Internet för att begära namnet av ISP's nameserver med en frekvens på ungefär en uppkoppling per minut.

Om Windows95 eller Windows98 skall användas som klientoperativsystem så bör bindningen "Klient för Microsoftnätverk" stängas av för protokollet TCP/IP. Det enklaste är att lägga till protokollet Netbios och binda den till Microsoftnätverk istället, då Netbios ej kommer att leda till uppkoppling mot Internet hos Linuxservern.

3 Linux PPP

3.1 Inställningar

Följande filer konfigureras automatiskt genom kontrollpanelen. Det är dock viktigt att man för säkerhets skull verifierar så att innehållet i filerna överensstämmer med de angivna önskemålen (bland annat användarnamn, telefonnummer och serieportens hastighet).

```
/etc/sysconfig/network-scripts/chat-ppp0
'ABORT' 'BUSY'
'ABORT' 'ERROR'
'ABORT' 'NO CARRIER'
'ABORT' 'NO DIALTONE'
'ABORT' 'Invalid Login'
'ABORT' 'Login incorrect'
'' 'ATZ'
'OK' 'ATDT020-333355'
'CONNECT' ''
```

```
/etc/sysconfig/network-scripts/ifcfg-ppp0
PERSIST=yes
DEFROUTE=yes
ONBOOT=no
INITSTRING=ATZ
MODEMPORT=/dev/modem
LINESPEED=38400
ESCAPECHARS=no
DEFABORT=yes
HARDFLOWCTL=yes
DEVICE=ppp0
PPPOPTIONS=
DEBUG=no
PAPNAME=u33hemlig
REMIP=
IPADDR=
BOOTPROTO=none
MTU=
MRU=
DISCONNECTTIMEOUT=
RETRYTIMEOUT=
```

```
USERCTL=no
```

```
/etc/ppp/pap-secrets  
# client      server  secret          IP addresses  
u33hemlig    ppp0   hemliglösen
```

3.2 Test

För att vid det här laget testa om anslutningen mot Internet fungerar skaffar man först rootåtkomst på datorn (su -), och skriver sedan "ifup ppp0". Man kan nu pröva att anropa valfri dator genom till exempel FTP. För att koppla ner överföringen skriver man "ifdown ppp0". Skulle överföringen ej lyckas är det möjligt att aktivera utökad logg genom att i filen */etc/syslog.conf* lägga till raden "*daemon.info /dev/console*". Observera att det skall vara <Tab> och ej mellanslag mellan kommandona.

4 Linux som brandvägg

4.1 Hosts

Samtliga datorer i det lokala nätverket bör läggas till i filen */etc/hosts* för att de skall få tillgång till Internet. Denna fil används sedan av diverse program på servern för att verifiera åtkomsträttigheter och för att strukturera logfiler.

```
/etc/hosts
127.0.0.1      localhost      localhost.localdomain
192.168.1.1    linuxsrv      linuxsrv
192.168.1.2    pii266        pii266
192.168.1.3    pro200        pro200
192.168.1.254 slipgate      slipgate
```

I filen ovan så är det absolut nödvändigt att åtminstone IP nummer 127.0.0.1, 192.168.1.1 samt 192.168.1.254 är definierade. IP nummer 192.168.1.254 används av Linuxservern för att simulera en fast uppkoppling mot ISP'ns router.

4.2 IP Masquerade

4.2.1 Rättigheter och funktionalitet

Eftersom vi ej vill att personer från Internet skall kunna komma åt det lokala nätverket genom vår brandvägg skall dessa låsas ute. Det viktigaste är att användarna i det lokala nätverket kommer ut på Internet. Detta innebär samtidigt krav på att man specificerar för brandväggen vilka datorer som skall tillåtas Internetåtkomst och ej.

Lägg till följande rader i filen */etc/rc.d/rc.local*:

```
/sbin/depmod -a
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_irc

/sbin/ipfwadm -F -p deny
/sbin/ipfwadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0
```

Denna konfiguration förutsätter att man valt klassC-nätverket 192.168.1.0 som förespråkas i kapitel 2 och 3. Orsaken till att man specifikt måste välja att tillåta paket från ftp och irc är att de som standardinställning är avstängda. Om det finns intresse att spela Quake mot Internet bör även följande rad läggas till (detta gäller ej Quake2):

```
/sbin/modprobe ip_masq_quake
```

4.2.2 IP_Forward

På grund av säkerhetsrisker är ip_forwarding genom brandväggen ej aktiverat som standardvärde i Linux kernel. Detta leder till att man antingen tvingas kompilera om Linux kernel för hand och slå på detta alternativ, eller också kan man lägga till följande rad i filen */etc/rc.d/rc.local*:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Observera att denna inställning samtidigt innebär att samtliga paket släpps ut genom brandväggen utan restriktion, vilket i praktiken leder till att brandväggens funktionalitet utåt stängs av. Det finns då en risk att anställda använder olovliga program såsom spel eller annan programvara då ingen kontroll på utgående paket existerar.

4.2.3 Dynamiskt IP

I det fall då vald ISP (eng. *Internet Service Provider*) ej kan ge möjligheten till fast IP nummer utan alltid tilldelar klienten ett dynamiskt nummer måste stöd för detta aktiveras i Linux kernel. Detta kan ske genom att kompilera om kerneln, även om det enklaste är att även här lägga till följande rad i filen */etc/rc.d/rc.local*:

```
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
```

Observera att detta ej fungerar om man använder sig av den modifierade pppd med ISDN-stöd (ipppd). Denna pppd skall dock endast användas vid bruk av interna ISDN-modem.

4.2.4 Tidsbegränsning

Följande rader läggs till för att begränsa uppkopplingen mot Internet till vardagar mellan klockan 07.00 -> 18.00:

/etc/diald.conf

Följande information har ändrats/lagts till:

tillägg

```
restrict      18:00:00      *          1-5 * *
or-restrict   *                7:00:00    1-5 * *
or-restrict   *                *          0,6 * *
down
restrict      *                *          * * *
```

```
include /tmp/diald-ppp0.filter
```

förändring

```
#include /usr/lib/diald/standard.filter
```

De sista två stjärnorna används för att specificera månadsdagar och årsdagar, vilket gör det möjligt att begränsa åtkomst till Internet över större ledigheter och semestrar.

5 Linux Dial-on-Demand

5.1 Konfigurationsfiler

Vid installation av DialD och Diald-config skapas automatiskt ett flertal konfigurationsfiler. Nedan visas de förändringar och tillägg jag har gjort i filerna, vilka kan behövas anpassas för att passa individuella behov.

```
/etc/sysconfig/dialdcfg
```

```
Följande information har ändrats/lagts till:
```

```
förändring
```

```
# (js)Denna parameter bestämmer nedkopplingstid på övriga TCP paket  
OTHER_TCP_TIMEOUT=120      ;# Koppla ner förbindelsen efter 2min  
# (js) Versionen på RedHats konfigurationsprogram.  
CONFPROGVER="5.0"
```

```
/etc/sysconfig/network-scripts/dialdcfg-ppp0
```

```
Följande information har ändrats/lagts till:
```

```
förändring
```

```
LINK_DOWN_IPADDR=192.168.1.1  
LINK_DOWN_REMIP=192.168.1.254
```

```
/etc/diald/diald-ppp0.conf
```

```
Följande information har ändrats/lagts till:
```

```
tillägg
```

```
# (js) Sätt transmit och receive till samma värde (default=1500)  
#      ...vilket krävs i kernel 2.0.32-2  
mtu 576  
mru 576  
# (js) Minska storleken på samtliga TCP-segment till 2kb  
window 2048
```


6 Felsökning

6.1 Paketövervakning

För att se vilken trafik som förekommer över både det lokala nätverket och mot Internet kan man använda ett program som heter tcpdump. Tcpdump är det bästa verktyget att använda om datorn kopplar upp sig trots man ej specifikt begärt det. Kommandot används enligt:

```
tcpdump -i <interface>      (interface är antingen eth0 eller ppp0)
```

Om man är ansluten till Linuxservern via telnet och vill granska det lokala nätverkets trafik kommer tcpdump att gå i evighetsloop (trafik via telnet visas via tcpdump, som leder till ny trafik etc). Det går då att filtrera bort ett valfritt antal paket genom valet '!port <portnummer>'. Exempel:

```
tcpdump -i eth0 '!port telnet'  
(visar ej telnettrafik över det lokala nätverket)  
  
tcpdump -i eth0 '(!port telnet) && (!port http)'  
(visar varken telnet- eller http-paket över det lokala nätverket)
```

6.2 Sessionsfel

Den första begäran som skickas till Linuxservern är den som leder till uppkoppling. Då detta första paket hamnar i den gamla routingtabellen innan serverdatorn är ansluten till Internet kommer detta paket alltid att gå förlorat. Problemet är att det idag inte finns stöd i TCP under Linux att internt flytta paket mellan olika routingtabeller. Om begäran skickas på nytt när routingtabellen är uppdaterad fungerar det dock som förväntat. Detta uppstår endast om direktadressering sker. Används DNS för att skicka paket till mottagarens dator försvinner endast ett av DNS-paketerna, som omedelbart sänds om.

Ett sätt att komma förbi detta är att skicka en ekobegäran till valfri destination på Internet före det att den faktiska trafiken inleds. Under Windows görs detta enklast genom att skapa en batchfil som startas genom en genväg på skrivbordet. Om denna döps till "Anslut brandvägg" eller motsvarande är det lätt för samtliga på nätverket att förstå dess betydelse. En passande destination att pinga är ett IP på motsvarande subnät 192.168.2.0, som ej kommer att lyckas. Genvägen bör lämpligen startas minimerad så att användare på det lokala nätverket slipper onödig statistik. Orsaken till att man väljer en icke existerande destination är att kommandot *ping* under Windows ej har funktionen att pausa mellan varje skickad begäran. Man får då istället ange hur länge ICMP-paketet kommer att vara aktivt innan att det skall anses förlorat, vilket innebär att det alltid måste gå förlorat för att vi skall uppleva en paus. Min egen konfigurationsfil *gateconnect.bat* ser ut enligt följande:

```
gateconnect.bat
@echo off
echo -
echo - Detta skript ser till att din firewall alltid
echo - är ansluten till Internet.
echo -
ping 192.168.2.1 -n 1
:1
ping 192.168.2.1 -n 1 -w 25000
goto 1
```

En genväg till denna skriptfil har sedan lagts i användarkatalogen 'C:\winnt\profiles\All Users\start menu\programs\Anslut brandvägg'. Genvägen är inställd på att startas minimerad, och kan avbrytas genom att högerklicka på det minimerade fönstret och välja 'stäng'. Linuxservern kommer då att avbryta uppkopplingen efter maximalt 30 sekunder som är timeoutvärdet för ICMP-meddelanden.

Programmet kan även användas då man ej vill att Linuxservern skall koppla ner från Internet, till exempel vid bankaffärer över websidor. En nedkoppling i det här fallet skulle innebära att all data som är inmatad på sidan går förlorad eftersom användaren tvingas till en ny TCP-anslutning mot webservern

6.3 Logfiler

När installationen är fungerande och har blivit verifierad kan det vara lämpligt att plocka bort loggningsfunktionen av Diald så att den inte lagrar *all* uppkopplingsstatistik i filen */var/log/messages*. Detta görs genom att ändra följande värde:

/etc/sysconfig/dialdcfg

Följande information har ändrats/lagts till:

förändring

VERBOSE_LOGGING="no"

7 Rekommenderad läsning

7.1 Linux manualfiler

1. ipfwadm
2. diald
3. lpd
4. pppd
5. printcap
6. tcpdump

7.2 Internetsidor

7. Red Hat Software, Inc.
<http://www.redhat.com>
8. The Diald homepage
<http://www.loonie.net/~eschenk/diald.html>
9. Linux IP Masquerade Resource
<http://ipmasq.home.ml.org/>
10. Linux IP Masquerade mini HOWTO
<http://ipmasq.home.ml.org/ipmasq-HOWTO.html>
11. Curtis Consulting – Linux Networking
<http://www.clark.net/pub/ray/>

7.3 Litteratur

12. Andréasson, T., Skansholm, J. (1993). "Unix och X från början", Studentlitteratur

Samtliga referenser mot Internet är kontrollerade 1998-04-14