Debian-router på 20 minuter

För Virtualisering och molntjänster

Anders Jackson

2023-04-25

1 Introduktion

Vi kommer att sätta upp ett lokalt, privat litet nätverk, på i Linux-distributionen Debian enklast möjliga sätt.

ANVÄND EJ I PRODUKTION, ENDAST I UTBILDNINGSSYFTE.

2 Konventioner

1. NIC som används skrivs `eth0` och `eth1`. De verkliga NIC:en kan heta något annat. Vad de heter tar ni reda på med hjälp av kommandot `ip address show`.

2. Nätverk som används är private IPv4-nät och skrivs exempelvis `10.0.0.0/24` på CIR-format. Nätmaskens storlek är normalt 24 bitar, eller `255.255.255.0` enligt äldre konventioner.

3. Ni skall själva ange ett lämplig lokal IP-nätverk. Ni väljer här ett av de privata nätverken som finns, men helst inte `192.168.0.0/24`, `192.168.1.0/24` eller `10.0.2.0/24`. Detta eftersom dessa kan blandas ihop med de nät som normalt används av hemma-routrar eller av VirtualBox. VirtualBox väljer `10.0.2.0/24` som det privata nätverket när man väljer att ansluta en virtuell maskins virtuellt NIC till NAT-nätverk.

3 Debian

Som router behöver vi en virtuell maskin som har Debian installerad samt har två virtuella NIC. Detta eftersom en router är normalt ansluten till mer än en NIC. I Debian kommer de heta något liknande `enp0s2`. Kommandot `ip address show` visar vilka maskinen har.

I denna text så använder vi `eth0` för externa nätverket och `eth1` för det interna nätverket. Men enligt ovan så skall ni alltås inte använde dessa namn, utan byta ut dessa mot de som maskinen har själv.

NIC `eth1` kommer att få IPv4-adresser från ett privat nätverk, som ni väljer själva. Ni bör INTE välja någon av näten `10.0.2.0/24`, `192.168.0.0/24` eller `192.168.1.0/24`, enligt konventionerna ovan, eftersom det kan störa er router.

3.1 Konfigurera routerns nätverk

Normalt så kommer den yttre NIC:en `eth0` få sina inställningar från det nät som den ansluts mot via dess `DHCP`.

Det inre nätverket, som ansluts via NIC:en `eth1` måste få en statisk adress på routern. I denna text så används adresser ur nätet `192.168.1.0/24`, men det måste ni byta mot någon annan privat adress, se ovan.

Så ni behöver välja en adress och nätmask för `eth1`, exempelvis `192.168.1.1/24`. Det formatet på IPv4-adressen är angiven enligt CIDR-format, dvs ip-adress och nätmask, där de är åtskilda med `/`-tecken och nätmaskdelen anger hur många av de första bitarna är nätverksdelen. Så i exemplet ovan är alltså nätets adress `192.168.1.0`, dvs det går 3 bytes om 8 bitar på de 24 bitarna. Dvs de tre första talen är nätverk, och det sista är en maskins unika adress i det nätet (dvs `1`:an i slutet är maskinens nummer i nätet.

Maskinen kommer att få både `gateway` (dvs router) och DNS-server via den yttre NIC:en `eth0`, så maskinen skall alltså inte ha någon router eller DNS-server angiven för vare sig `eth0` eller `eth1` när man konfigurerar routern. De kommer via `DHCP` på `eth0`.

Men på alla andra maskiner i det lokala nätverket så skall man alltså ange både IPv4-adress, nätmask, router och DNS-server.

Så lägg till/ändra i filen `/etc/network/interfaces` enligt listningen 3.1 på routern.

```
# Interna LAN-interfacet eth1
allow-hotplug eth1
iface eth1 inet static
        address 192.168.1.1/24 # IPv4-adress och nätmask
```

För att detta sedan skall gälla så kan man starta om routern, eller starta om NIC:en med `sudo ifdown eth1` följt av `sudo ifup eth1`.

Kontrollera inställningarna med kommandona i listning 1.

```
ip address show
ip route show
cat /etc/resolv.conf
sudo apt update
```

Figur 1: Kontrollera nätverksinställningarna för `eth0` och `eth1`.

3.2 Konfigurera DNS (och DHCP-server)

Nästa lämpliga steg är att kontrollera att `/etc/hosts` har korrekta ipv4-adresser. Exempelvis så skall routerns statiska adress bytas från `127.0.1.1` till den adress som angavs i listningen 3.1 ovan.

För att maskinerna i det interna LAN:et skall kunna översätta domän-namn till IPv4-adresser, så behöver man en DNS-server. Det kan tillhandahållas av programmet `dnsmasque`.

Programmet konfigureras genom att redigera `/etc/dnsmasq.conf` eller lägga till en fil i katalogen `/etc/dnsmasq.d/`. Raderna som skall ändras/läggas till finns i listningen 3.2.

När man konfigurerar `dnsmasq` skall man tala om att den skall lyssna på NIC `eth1` och då använda ipv4-adressen `192.168.1.1`, dvs samma som routerns i det interna nätverket. Kontrollera gärna att `dnsmasq` är installerad med kommandot `sudo apt install dnsmasq`.

```
# Vad skall DNS och DHCP lyssna på?
interface=eth1
listen_address=192.168.1.1
domain=example.com
# Inställningarna för nätets DHCP, behövs kanske inte 30 IPv4-adresser
dhcp-range=192.168.1.50,192.168.1.79,6h
```

För att kontrollera att dns-uppslagningen fungerar, så kan man använda kommandot `sudo apt update`. Om det inte fungera, läs felkoderna. Det kan vara DNS eller IP som inte fungerar. DNS funerar inte om IP inte fungerar.

Man kan även prova med att slå upp en adress med kommandot `getent(1)`, som exempelvis `getent ahosts www.hig.se`.

Det kan vara värt att lägga till alla andra maskiner till `/etc/hosts`, eftersom `dnsmasq` läser den filen vid start och gör dessa namn och adresser tillgängliga för alla maskiner som använder programmet som DNS-server.

3.3 Tillåta routing

Normalt fungerar Linux-maskiner som vanliga maskiner och inte som router. Så för att aktivera router-funktionen, så måste man aktivera `ip_forward` i Linux.

Det gör man enklast genom att i filen `/etc/sysctl.conf` leta reda på följande rad och ta bort kommentarstecknet `#` först på raden `net.ipv4.ip_forward=1`, om det inte redan är gjort.

Det kan kontrolleras att `ip_forward` är aktiverat med kommandot `sudo sysctl net.ipv4.ip_forward`. Om den skriver ut `1`, så betyder det att maskinen har satt den funktionen till sant. Annars om värdet är `0`, så måste man in och ändra i filen.

3.4 NAT-funktion

Eftersom det interna nätverket har ett privat nät, så måste man slå på NAT-funktionen i Linux. Det gör att routerns externa IPv4-adress på `eth0` används istället för den privata adressen host dator i det interna nätverket. Dvs de som är anslutna via `eth1`.

Detta görs genom att aktivera det i brandväggen i Linux.

Det är flera delar eller regler. De regler som är i sektionen `*nat`, är de som har med NAT-funktionen att göra.

De som är i sektionen `*filer` har att göra med tillåtelse att ta emot data till routern, `INPUT`, att skicka ut data från routern, `OUTPUT`, samt skicka vidare data som kommer till routern, `FORWARD`.

Så i exemplet lägger vi till så att anslutningar som kommer in på `80/tcp`, skickas vidare till samma port på maskinen `192.168.1.11` i det interna nätverket. Allt som går ut från NIC:en `eth0`, som markeras med `-o eth0` i regeln, kommer att gömmas bakom NAT. Vilket kallas `MASQUERADE` i Linux.

Hur en sådan inställning kan se ut ser ni i listning 3.4. Den listningen har bara aktiverar port forwarding för SSH (22/tcp). Notera att ni behöver anpassa den

för att passa era inställningar. Notera även att denna inställning av brandväggen är bara för att få laborationen att fungera. Vill ni göra det på riktigt, så använd kommandot `ufw(8)` eller liknande för att ställa in brandväggen.

En korrekt inställd brandvägg kan lätt bli 50-100 rader lång.

```
*nat
-A PREROUTING -i eth0 -p tcp -m tcp --dport 22 -j DNAT --to_destination 192.168.1.11:22
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT

*filter
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -j DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
COMMIT
```

Inställningarna kan kontrolleras om de är korrekta med kommandot `iptables-restore < /etc/iptables.rules`. Det aktiverar även brandväggen temporärt. När kommandot kan köras utan felmeddelande, så går det att se hur inställningarna blev med kommandot `sudo iptables -t nat -S` och `sudo iptables -t filer -S`.

Notera att för att aktivera detta varje gång nätverket startar, så behöver man spara aktiveringen av brandväggens inställningar för `eth0` i filen `/etc/network/interfaces`, så att de aktiveras varje gång maskinen startat.

Dvs sätt in raden `pre-up iptables-restore < /etc/iptables.rules` efter raden som börjar med `iface eth0` i filen.

4 De andra maskinerna

De andra maskinerna i det lokala nätet, skall ställas in så att de får en statiskt ipv4-adress i samma nät som `eth1` på routern har. Vilka adresser väljer ni själva, bara de blir i samma närverk, samt inte används av de som `dnsmasq` delar ut via sin `DHCP`-funktion. Se inställningarna för `dnsmasq` i listningen 3.2.

Ni behöver även ställa in `gateway` (router) till den ipv4-adress, som routern har. I detta exempel är det `192.168.1.1`.

Sedan vill man har DNS-funktionen att fungera. Till det kan man använda `dnsmasq`, som har en DNS-funktion för interna nätverk. Så sätt bara `dns-nameserver` i `/etc/network/interfaces` för det interna närverket till routerns ipv4-adress.

4.1 Testa nätverket

När detta är gjort och router samt klient i nätverket är konfigurerade, så kan ni testa med följande kommandon i listningen 2.

```
sudo apt update # fungerar det så är nog allt korrekt
ip address show # adress och nätmask
ip route show # default router
cat /etc/resolv.conf # dns-serverns ip-adress.
```

```
nmap 192.168.1.1 # se vilkan funktioner som är aktiverade
getent hosts www.hig.se  # testa dns-funktion
getent ahosts www.hig.se
ping 192.168.1.1 # testa ip-funktion
ping 192.168.1.10
ping www.hig.se # testa dns- och ip-funktion
```

Figur 2: Testa att nätverket och DNS fungerar.

5 Om inte det fungerar

Kontrollera att alla maskiner sitter på rätt interna nätverk i VirtualBox.

Kontrollera att alla maskiner som sitter i det interna nätverket har olika MAC-adresser på respektive NIC. Det går att generera ny i VirtualBox.

Gå igenom listan:

- Testa att nätverket fungerar på routern, i första hand. Om inte routern fungerar, är det inte någon ide att testa de andra maskinerna. Kontrollera att DNS fungerar samt ipv4 till internet.
- När det är gjort kontrollera att de andra maskinerna kan komma åt routern via routerns ipv4-adress och omvänt.
- Kontrollera att DNS fungerar för de andra maskinerna.
- Kontrollera de inställningar som är relevanta i routern och i de andra maskinerna SAMT i VirtualBox.

Om ni inte hittat felet, börja om från början i listan.

Felen kan vara felstavning av ett ett namn eller fel maskin ändrar i. Så kontrollera allt igen, och gå igenom testerna. Be någon annan att lyssna när ni går igenom era inställningar, och kanske även läsa dem med er eller själv.

Lycka till.
