Introduktion till Linux och små nätverk

Grunder i nätverk

För att kunna kommunicera mellan datorer, så måste det finnas ett media samt överenskommelser om hur kommunikationen skall ske för att överföra data mellan datorerna, sk protokoll.

Normalt använder man i dag antingen trådbundet nätverk som kallas Local Area Network (LAN) och/eller trådlös kommunikation som kallas Wireless Local Area Network (WLAN) mellan datorer (noder) i små nätverk.

Internet Protokollet

Internet Protocol (IP) är det protokoll som man vanligtvis använder för att kommunicera mellan datorer i nätverk. Det finns i två varianter, det äldre IPv4 och det nya IPv6. De kan inte direkt kommunicera med varandra, så en dator som använder IPv4 och en som använder IPv6 kan inte kommunicera. Så varför har man då tagit fram den nya varianten?

Redan under 90-talet så kom man på att det fanns så många brister i IPv4 så att man behövde ta fram en ny variant. Den mest uppenbara bristen var att det inte skulle finnas IPv4-adresser så det räcker till alla maskiner på internet. Detta eftersom varje dator på internet måste ha en unik adress.

IPv4 använder bara 32-bitar för att ge en dator på internet en adress. Det innebär att det finns maximalt 2^{32} = 4 294 967 296 adresser (dvs ca 4 miljarder adresser). Av dessa kan många inte användas pga hur nätet ser ut samt att vissa adresser är reserverade för speciella funktioner. Dessutom så delar adresserna ut i block för varje lokalt nätverk (LAN), och de som inte används i ett LAN kan inte användas i något annat nät. Så 3 februari 2011 tog den sista IPv4-adressen slut centralt. Så nu finns det inte några nya nät att dela ut om man skulle behöva, exempelvis till nya Internet Service Providers (ISP är företag/organisation som tillhandahåller internet, som Tele2, Telia, Sunet etc).

IP-nät

Dataöverföring mellan datorer sker logiskt i princip på samma sätt i IPv4- och IPv6-nät. Därför kommer vi bara att tala om IP-nät och adresser här, och då menar vi i huvudsak IPv4.

Varje dator på internet som skall sända eller mottaga data har en egen IP-adress. Denna adress skall vara unik för alla datorer på internet. En IP-adress delas upp i två delar, först en nätadress och sedan en nodadress. Nätadressen väljer vilket LAN som datorn används i, och den andra är vilken dator, nod, i LAN:et som datorn är.

På så sätt kan man lättare hålla reda på vad varje LAN är, istället för varje dator på internet.

Paket

För att kunna skicka data mellan två datorer, så skickas datat i ett eller flera paket. Skickar man lite data så räcker det med ett paket. Sänder man mycket data, så skickas flera paket.

Dessa paket innehåller en del nödvändig data för att sändare och mottagare skall veta vad som skickas. Till att börja med så måste det finnas en avsändar- och en mottagaradress, så att. Det måste även finnas angivet vilken typ, IP-protokoll som skickas. De vanligaste IP-protokollen är Internet

Control Message Protocol (ICMP), User Datagram Protocol (UDP) och Transmission Controll Protocol (TCP).

ICMP används för att skicka information om nätverk och datorer, vanligaste är om maskinen lever (ICMP Echo, sk ping) eller om en port hos mottagaren är stängd och varför.

UDP skickar ett paket med data, och hoppas att det kommer fram. Det fungerar lite som att man lägger ett brev på brevlådan, sedan kommer det fram. Skillnaden är att här så kan ett paket försvinna, samma paket kan komma fram i som två eller fler kopior eller så kan två paket komma fram i omvänd ordning mot hur de skickades. Fördelen är dock att det går ganska fort, så det används exempelvis för ljud, video och annan liknande överföring som det är viktigare att data kommer fram i en strid ström än att allt kommer fram i rätt ordning.

TCP skapar en förbindelse mellan avsändare och mottagare, och sedan så garanterar TCP att det kommer fram på samma sätt som det sänder. Inget förlorat data, inga dubbletter eller omkastad ordning på datat som skickas. Men tyvärr betyder det att om ett paket med data förloras så kommer det att behöva sändas om. Vilket gör att dataöverföringen kan hacka. Så TCP används när det är viktigare att överföra data korrekt än med en strid ström.

När det gäller UDP och TCP, så måste mottagaren (och sändaren) veta vilket program på datorn som skall ha datat. Så både UDP och TCP sk portnummer för att identifiera var datat skall skickas. Så när datorn tagit emot data så tittar den på portnumret och skickar det till rätt dator. Notera att samma portnummer hos UDP och TCP inte behöver vara till samma program, de är oberoende av varandra. Även värt att veta är att avsändaren och mottagaren vanligen har olika portnummer.

Routing (vägval)

När data skickas från en dator till den andra så kommer datorn först att kontrollera om de två datorerna befinner sig i samma nät. Detta görs genom att jämföra nätadressen hos mottagaradressen och alla nätverksadresser på den enheter som är anslutna till nätverk. Om det finns någon som har samma nätverksadress, så sitter de ju då på samma nätverk. Då skickar datorn datat direkt till den andra datorn. De flesta datorer är bara anslutna till ett nätverk, men om de är anslutna till

När en dator sedan mottar data, så kontrollerar den om det är rätt adress. Om det är det, så tar den emot datat och skickar det till det program som skall ha datat. Hur vet datorn vilket program som skall ha datat? Det kommer vi att titta på längre ned, men i IP så finns det i huvudsak tre olika sätt att skicka data. ICMP, UDP och TCP. ICMP skickar information om noder mellan varandra, som om datorn lever (ICMP ECHO, eller ping) eller om det inte finns något program som lyssnar efter datat som skickats. UDP och TCP skickar data mellan program. Så för att välja vilket program som skall lyssna, så använder man sig av ett 16-bitars portnummer. TCP och UDP egen uppsättning av portnummer, så att ett program kan lyssna på port 80 för TCP och ett annat program kan lyssna på port 80 för UDP. Avsändare och mottagare behöver heller inte använda samma port, så avsändaren kan använda TCP och port 40923, och mottagaren kan då lyssna på port 80 (dvs HTTP-porten).

De flesta datorer i nätverket är bara ansluten till ett nätverk, så då är det enkelt. Antingen har det data som mottagits kommit till rätt adress, eller så slänger datorn det data eftersom det inte skall till den här datorn.

Men vissa datorer är anslutna till flera nätverk, och har till uppgift att skicka data mellan olika nätverk, om datat inte skall till datorn själv. En sådan dator kallas router (vägväljare).

Så när en router får ett paket, så tittar den på mottagaradressen. Är det dess egna adress, så gör den som en vanlig dator, som är beskrivet tidigare. Men om det inte är det, så tittar datorn på adressen

och ser vilket nät den skall till. Om det är ett nät som routern är direktansluten till, så skickas datat vidare till den maskinen på det nätet. Den ”routar”, vidareförmedlar, paketet till rätt nät och dator.

Problemet blir om nätadressen som skall skickas till inte är något av de som routern är ansluten till. Då tittar den i en tabell över vilka nätverk den känner till, och så skickar den till nästa router i rätt riktning, så att det till slut kommer till rätt dator. Om det nu skulle vara att den inte heller vet något alls om det nät som paketet skall skickas till, så kommer den att skicka till en speciell router, defaultroutern som den är ansluten till. Den routern antas veta hur datat skall skickas vidare till rätt maskin. Så därför har varje maskin, även Den andra datorn får datat och kontrollerar om mottagar-adressen är samma som sin egna. Om det inte är rätt adress, så kommer en vanlig dator att ignorera datat. Om det är rätt, så kommer datat att sändas till ett program som får ta hand om det.

Men vad händer om datat skall skickas till en dator som sitter på ett annat nätverk? Då ser datorn som sänder att mottagarens nätadress och sin egna nätadress skiljer sig åt. Då skickas paketet till en router, vidarebefordrare, på det lokala nätet. Den ser till att datat inte är ämnat för den egna datorn, utan en annan, och skickar det vidare i rätt riktning för att det skall nå den andra datorn.

För att man skall kunna skicka data mellan olika datorer i olika nät, så har alla datorer i samma nät samma nätadress. Så skall en dator skicka något till en annan dator som sitter på samma nätverk, så kan datorn skicka datat direkt till den andra datorn.

IPv4-adresser

Hur ser då en dator om datat skall skickas till en dator i samma nätverk eller i ett annat? Och hur vet den vilken maskin på det egna nätet som är en router?

En IPv4-adress består av 32 bitar, och de skrivs normalt med fyra decimaltal åtskilda med en punkt. Exempelvis så kan en IPv4-adress se ut så här: `130.243.0.29`. Så den adressen består egentligen av 32 st 1:or och 0:or. Så med hjälp av programmet ipcalc så kan vi se hur det ser ut.

```
$ ipcalc -c 130.243.0.9
Address:   130.245.8.12         10000010.11110101.00001000.00001100
...
Hosts/Net: 65534                 Class B
$
```

Av detta kan vi se att adressen inleds med 10, vilket säger att det är en B-klass. B-klass delar adressen i 16-bitar nät och 16-bitar maskin. I det här fallet är alltså nätet `130.243.0.0` och nodens adress `0.9`.
Det finns ett antal klasser, beroende på hur de första bitarna i IP-adressen ser ut.

`0`	A-klass (8/24)	8 bitar nät (256 st)
`10`	B-klass (16/16)	16 bitar nät (65 534 st)
`110`	C-klass (24/8)	24 bitar nät (16 777 216 st)
`1110`	D-klass (32/0)	Experimentell

Normalt använder man dock inte så stora nät, eftersom det rymmer 65534 noder. Så därför brukar man dela upp näten i delnät, med hjälp av en subnätsmask. Av historiska skäl så använder delar man dock alltid mindre delar av klassnäten, även om man inte använder klasserna längre.

Nätmasken är lika lång som IPv4-adressen, dvs 32-bitar lång, och varje bit från vänster till höger i

nätmasken som är en etta talar om att det är del av nät-adressen. För att skriva det så kan man antingen skriva det som en nätmask, exempelvis `255.255.255.0`, eller hur många bitar som är nätdelen med `/24` efter IP-adressen, eftersom nätmasken har 24 ettor till vänster (255 är 8 ettor).

Så då kan vi se vad vi får av `ipcalc` nu då:

```
$ ipcalc -c 130.245.8.12/24
Address:   130.245.8.12          10000010.11110101.00001000. 00001100
Netmask:   255.255.255.0 = 24    11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255             00000000.00000000.00000000. 11111111
=>
Network:   130.245.8.0/24        10000010.11110101.00001000. 00000000
HostMin:   130.245.8.1           10000010.11110101.00001000. 00000001
HostMax:   130.245.8.254         10000010.11110101.00001000. 11111110
Broadcast: 130.245.8.255         10000010.11110101.00001000. 11111111
Hosts/Net: 254                    Class B
```

Som man kan utläsa så går två stycken noder bort, nämligen nodadressen med nollor och med ettor, dvs högsta och lägsta. Nodadressen med bara nollor är nätets adress, som 130.243.8.0 i exemplet ovan. Nodadressen med bara ettor kallas broadcast, och skickas till alla datorer i samma nätverk. Så `130.243.8.255` är broadcast-adressen för alla datorer i nätet `130.234.8.0/24`.

Hur vet datorn vilken adress routern har? Det vet den inte automatiskt, utan det måste datorn få veta av nätverksadministratören. För att se vilka inställningar som datorn har, så kan man använda kommandot `ip`, följt av olika argument. För IP-adresser, använd `ip add list` (eller förkortat `ip add`). För varje nätverksenhet dess inställningar. Exempelvis så kan man så något som liknad detta: IPv4-adress: `inet 192.168.122.10/24`, MAC-adress: `link/ether 0a:59:77:93:29:88` samt IPv6-adress: `inet6 fe80::226:b9ff:fe7b:68e3/64`.

Kommandot `ip route` list ger lista av vilka maskiner som är routrar: Så `ip route list` ger information om standardrouter: `default via 192.168.222.1 dev eth0`, dvs den har IPv4-adress `192.168.122.1` och sitter på enhet `eth0`.

För att se vilka maskiner som finns i samma nät, så kan man använda `ip neigh`.

I Debian så ställer man in nätverksinställningarna i filen `/etc/network/interfaces`[1]. Där skriver man olika ”stanza” för hur nätverket skall ställas in. Exempelvis så kan man tala om för Debian att nätverksinställningar skall komma från nätet via DHCP-protokollet.

```
auto eth0
iface eth0 inet dhcp
```

Vill man ställa in manuellt, så kallat statiskt, så gör man så här:

```
auto eth0
iface eth0 inet static
     address 192.168.222.10
     netmask 255.255.255.0
     gateway 192.168.222.1
     dns-servers 8.8.8.8 8.8.4.4
```

Här sätter vi IPv4-adressen till `192.168.222.10` och nätmasken till `/24`. Routern finns på `192.168.222.1` och för att hantera DNS-uppslag så använder vi Google publika DSN-servrar.

1 Glöm inte att titta i manualsidan för `interfaces(5)` med `man interfaces` eller `man 5 interfaces`

NAT

Eftersom alla IPv4-adresser tagit slut, så får vanliga Internet Service Provider (ISP)-kunder riktiga IP-nät utan de får privata nät. Dessa IPv4-adresser skall och får användas i privata nätverk. Så de får inte skickas ut på internet. Det för att många kan ha samma privata IP-adresser.

Så hur hanteras detta då? Jo genom något som kallas Net Address Translation (NAT). Det innebär att routern som skickar vidare data till andra nät även har en NAT-tjänst. När den skall skicka vidare data till en IP-adress utanför det lokala privata nätet, så kommer det att låna sin egna globala adress ut på internet. Så alla datorer som en dator i det privata nätet kommunicerar med ser ut att prata med routern med NAT. Så när de skall skicka tillbaka data, exempelvis från en web-server, så skickar den till routern och NAT-tjänsten. Den kommer ihåg att den har bytt ut en privat adress mot sin globala adress, så då tar den och byter tillbaka från sin globala adress till den privata adress som den som skickade hade. Så nu får den dator som skickade datat tillbaka ett svar.

Vilka privata adresser finns det då? Följande adresser får man använda på sina egna nät (enligt RFC 1918):

```
10.0.0.0/8       ett A-nät[2] delas normalt i /24-nät
172.16.0.0/12    16 B-nät     delas normalt i /16 eller /24-nät
192.168.0.0/16   256 C-nät    delas normalt i /24-nät
```

Här ser ni de vanligaste adresserna som finns i hemmaroutrar, som även har NAT. Nämligen `192.168.0.0/24` och `192.168.1.0/24`. Ni kan om ni vill byta ut dem mot vilken som helst av de nät som anges ovan.

Fysiska nätverk

Det finns många olika sätt att få datorer att samarbete i lokala nätverk, och de vanligaste är att använda Ethernet. Ethernet består av ramar, som bland annat innehåller avsändare- och mottagaradresser av ramen i form av Media Access Control Addresses (MAC-adress). Ethernetramen innehåller även vad det är för typ av data som sänds och sedan själva datat. Typen kan vara IPv4 eller IPv6. De datorer som har rätt mottagar-MAC-adress tar hand om datat.

Det finns i huvudsak två vanliga sätt att skicka dessa Ethernet-ramar mellan datorer. Antingen i trådbundet LAN eller i trådlöst WLAN.

Local Area Network

Ett trådbundet LAN använder sig av kabel av typen Twisted Pair-kabel, som består av åtta stycken kopparledare som är uppdelade i par som är svagt roterad runt varandra, dvs fyra roterade par (Twisted pair). Dessa kablar är av olika kvalitet, men vanligast är sk Category 6 eller Category 6a. Dessa tillåter överföringshastigheter på upp till 10 Gbp/s[3]. Lägre kvalitet, cat 5, klarar upp till 1 Gbp/s. Så har man snabb nätutrustning, så skall man ha tillräckligt bra kablar.

I ett trådbundet nät, så ingår det några olika komponenter, nämligen

1) Datornoder, som exempelvis datorer och skrivare.
2) Switch/Hub, som används som kommunikationsnav i ett nät mellan olika datornoder.

2 A-nät är /8, B-nät är /16 och C-nät är /24. De finns egentligen inte längre, men är bra att veta om. Man använder idag CIDR, Classless Inter-Domain Routing, vilket vi gör när vi använder nätmask.

3 1G är Giga som är 1000 miljoner. Överföringshastighet mäts i bps, som är bitar per sekund. En viss del av överföringshastigheten försvinner i protokollet, så maximal praktisk överföringshastighet är lägre.

3) Router, som används för att ansluta det lokala nätet, brukar ha NAT-funktion

Man ansluter då datornoderna till switchen eller direkt till switchen i routern, om den har en sådan. Då kan datorerna kommunicera med varandra och via routern med resten av Internet.

Wireless Local Area Network

I ett trådlöst WLAN så anslutes de olika noderna med radiosignaler med frekvensen 2,4GHz eller 5G Hz. Det finns några olika protokoll för WLAN som är vanliga, och de vanligaste i dag är IEEE 802.11b, 802.11g, 802.11n samt 802.11a. De har den teoretiska överföringshastigheten på 11Mbps till 54Mbp/s eller 600 Mbps (802.11n) men den är vanligtvis lägre, beroende på hur mycket störningar från annan utrustning, som exempelvis mikrovågsugnar, mobiltelefoner samt andra i närheten använda WLAN det finns. En ny och snabbare version håller på att lanseras nu, som heter 802.11ad, och har en betydligt högre hastighet, upp till 7Gbps.

Det finns flera sätt att koppla ihop datorer i ett WLAN, som Ad-Hoc eller infrastrukturnät. Det vanligaste är att man använder ett infrastrukturnät. I ett sådant nät ingår följande delar.

1) En accesspunkt (AP) som är den som kommunicerar med de i nätet ingående datornoder.
2) Datornoder, som exempelvis datorer och skrivare som är anslutna mot vald AP.

En AP är inställd på en viss kanal samt har ett namn, Service Set Identifier (SSID), som alla inblandade datornoder använder. Vilka radiokanaler som är godkända skiljer mellan olika länder, och det är du som själv ansvarar för att använda rätt kanal. Dessa kanaler ligger för nära varandra, så om två AP som är nära varandra använder grannkanaler, så kan de störa ut varandra. Därför är det viktigt att det finns minst två tomma kanaler mellan de AP som kan nå varandra. Vanligtvis använder man kanal 1, 6 och 11 (och där det är godkänt kanal 14). Om det är trångt i etern, så är det bättre att dela samma kanal med en annan AP än att använda någon kanal som ligger för nära. De kan nämligen dela på kanalen.

WLAN säkerhet

Eftersom alla datornoder kommunicerar över radiosignal med AP:n, så kan vem som helst avlyssna trafiken. Om man vill hindra avlyssning och icke godkänd användning av AP:n, så måste man kryptera det. Det finns kryptering som kallas Wired Equivalent Privacy (WEP) som man inte skall använda. Den är så dålig så att program kan bryta krypteringen på mindre än en minut. Det ersattes med Wi-Fi Protected Access(WAP) som är mycket bättre, men numera bör man använda version två av WAP, nämligen WAP2. Notera att man kan ställa in sin AP att acceptera både WAP och WAP2, men då får man inte någon förhöjd säkerhet, eftersom datornoderna kan använda WAP istället för WAP2.

WAP/WAP2 använder EPA som kryptering och då behövs en nyckel[4] för krypteringen. Den nyckeln kan hanteras på två sätt. Dels kan man använda EAP-PSK (Pre Shared Key) och det innebär att man ställer in en nyckel för alla datorer i AP:n. Det andra sättet är EAP-TLS, och innebär att nyckeln sätt av en server när man har loggat in. Så varje användare har får en egen nyckel. För att det skall fungera behöver man en RADIUS-server, vilket gör att EAP-PSK är det som nästintill uteslutande används i hemmanätverk.

Vanliga missförstånd med WLAN när man försöker höja säkerhet, men som är kontraproduktivt och faktiskt sänker säkerheten, är att antingen göra SSID osynligt och/eller bara tillåta vissa maskiner

4 Nyckel är en form av lösenord som används vid kryptering.

beroende på den sk Media Access Control (MAC) adressen. Ingen av dem höjer säkerheten nämnvärt men gör nätverket svårare att administrera. Osynligt SSID gör bara att datanoderna måste fråga om AP:n finns i närheten, och då kan en falsk AP svara. MAC-adresser kan ändras i nätverkskorten.

Referenser

- http://sv.wikipedia.org/wiki/Internetprotokoll
- http://sv.wikipedia.org/wiki/IPv4
- http://sv.wikipedia.org/wiki/Internet_Control_Message_Protocol
- http://sv.wikipedia.org/wiki/User_Datagram_Protocol
- http://sv.wikipedia.org/wiki/Transmission_Control_Protocol
- http://sv.wikipedia.org/wiki/IPv6
- http://en.wikipedia.org/wiki/Private_network
- http://sv.wikipedia.org/wiki/Network_Address_Translation
- http://sv.wikipedia.org/wiki/Local_Area_Network
- http://sv.wikipedia.org/wiki/Wireless_Local_Area_Network
- http://se.wikipedia.org/wiki/Kategori_6_kabel
- http://sv.wikipedia.org/wiki/IEEE_802.11
- http://en.wikipedia.org/wiki/IEEE_802.11i
- http://en.wikipedia.org/wiki/MAC_address