Anteckningar gällande datakomm

Författare: Jack-Benny Persson
Datum: 2013-10-31

OSI-modellen

Lager	Beskrivning
Application	Själva nätverksprogrammen
Presentation	Presentation av nätverksdata, t.ex. kryptering m.m.
Session	Sessioner för binda samman kommunikationen
Transport	Sändning/mottagning av data, t.ex. TCP/UDP
Network	IP protokollet och den logiska adresseringen
Data Link	Den fysiska adresseringen med MAC-adresser
Physical	Den fysiska kommunikationen i form av kablar och ström

DoD-modellen

Lager	Beskrivning
Application	Själva programmen
Transport	Sändning/mottagning t.ex. TCP/UDP
Internet	IP protokollet och den logiska adresseringen
Network Access	Den fysiska länken med kablar, ström, NIC, MAC-adress m.m.

RFC

Request for comment. RFC-dokumenten bestämmer standarder, t.ex. standarden för hur FTP ska se (den först RFC för FTP är #114 och utkom i april 1971). Först skapas en draft (förslag) sedan antas denna som en standard och därefter kan denna bli föråldrad (obsolete) av att det kommer en nyare RFC för t.ex. FTP.

1. Förslag/draft
2. Standard antas
3. Nytt dokument ersätter tidigare RFC och gör denna föråldrad/obsolete.

Topologier

Fysiska

Stjärnnät

Detta är den viktigaste, det är det som är det vanligaste idag. Ett stjärnnät är när man kopplar samman alla datorer med varsin kabel som sammanstrålar i en koncentrator (t.ex. en switch eller hubb). Det heter stjärnnät för att switchen är i "mitten" och datorerna strålar ut från den och topologin liknar då en stjärna.

Meshnät

Denna är också ganska viktig och vanlig förekommande i trådlösa nätverk. Meshnätverk innebär att det finns flera olika förbindelser mellan varje enhet, alltså flera olika vägar som trafiken kan ta.

Bussnät

Gammalt och används inte idag såvida inte någon fortfarande har kvar sitt gamla BNC-nätverk hemma. Det var BNC-nät eller bussnät som det korrekt heter som jag själv började med en gång i tiden. Bussnät innebär att man har en lång kabel som alla datorerna kopplar in sig på. Denna kabeln är alltså själva "bussen". Bussen eller kabeln måste termineras i båda ändarna. I BNC-näten gjordes detta med 50-ohms motstånd.

Ringnät

Mycket gammalt och användas inte idag. Token Ring är ett exempel på ringnät. I ett ringnät kopplar man samma alla datorer i en ring, kabeln blir således en "ring".

Point-to-point

En dator ihopkopplad direkt med en annan dator via t.ex. en korsad kabel

Point-to-multipoint

T.ex. TV och radioutsändningar. En mast som sänder till många mottagare.

Geografiska

PAN = Personal Area Network, t.ex. när man kopplar ihop sin laptop med mobil, skrivare och headset med bluetooth.

LAN = Local Area Network, det som våra vanliga lokala nätverk är.

MAN = Metropolitan Area Network, stadsnät som sträcker sig över en stad eller stadsdel. T.ex. Öresundskrafts stadsnät i Helsingborg.

WAN = Wide Area Network, t.ex. ett företag som kopplar samma alla sina kontor över hela världen i ett stort WAN över flera länder. Även internet benämns ibland som ett WAN.

GAN eller Global (W)AN. Detta är vår vanliga internet.

Enterprise WAN, t.ex. Internet2 där man inte vill ha allt "löst folk".

Olika typer av LAN

Peer-to-peer

Alla datorer har samma status i nätverk och det finns ingen direkt server som har hand som saker utan alla delar med alla. Max ca 20 datorer.

Client/Server

Den vanligaste formen där man har en server och många klienter som ansluter till denna.

CSMA/CD

Carrier Sense Multiple Access / Collision Detection. Detta är något som används i alla våra Ethernet LAN. Tekniken går ut på att alla delar samma media (hubb/kabel) och alla har samma rättighet till mediet. När en dator ska börja skicka data känner den första av om mediet är ledigt (Carrier Sense) och börjar då skicka om det är ledig. Däremot kan en annan nod börja skicka samtidigt (Multiple Access). Krocken upptäcks då (Collision Detection) och noderna slutar skicka mer data. Noderna väntar sedan en slumpmässig tid och börjar sedan om igen med att känna av mediet blivit ledigt (Carrier Sense).

Alla *casten

Unicast

Nod till nod. En dator skickar ett paket till en annan dator. Här är alltså bara två datorer inblandade.

Broadcast

En dator till alla datorer i samma logiska nät. T.ex. en ny dator som vill ha en IP-adress skickar en broadcast till hela nätet på 255.255.255.255 för att få en IP av en server som upptäcker broadcasten.

Multicast

Från en dator till en specifik grupp av datorer. T.ex. för mediaströmning. Detta är detta som 224 nätet används för t.ex.

Anycast

Detta är specifikt för IPv6. En nod skickar en förfrågan till EN adress. Denna adressen kan då flera noder ha. Den snabbaste eller bästa noden svarar då på förfrågan. Detta kan t.ex. användas för att få redundans. Flera servrar har samma adress. Skulle en gå ner så finns det fler servrar kvar med samma adress som kan svara på anropen.

NIC

Ett NIC (Network Interface Card) har en MAC-adress som består av 48-bitar. Dessa är representerade som hexadecimala fält med två tecken i varje fält. T.ex. XX:XX:XX:XX:XX:XX. Sammanlagt sex stycken fält alltså.

Varje fält innehåller 8 bitar, varje enskilt tecken är alltså 4 bitar.

```
F  =  15
8  4  2  1
1  1  1  1
```

8+4+2+1 = 15

```
128 64 32 16 8 4 2 1
1    1  1  1  1 1 1 1
```

128+64+32+16+8+4+2+1 = 255 = FF

Vidare innehåller ett NIC en RJ-45 hona.
IP adressen är logisk och tilldelas i operativsystemet antingen statiskt eller av en DHCP-server.

IP

IP adresser är 32 bitar långa.

11111111.11111111.11111111.11111111

Två typer av broadcast finns, 255.255.255.255 som är en generell broadcast oberoende av nät och 192.168.0.255 som är en broadcast för hela 192.168.0.0 nätet.

Klasser

```
Klass A  -->  0xxx (1-126)   (00000001 = 1 & 01111111 = 127 men 127 får vi
inte använda, det är loopback adresser)
Klass B  -->  10xx (128-191) (10000000 = 128 & 10111111 = 191)
Klass C  -->  110x (192-223) (11000000 = 192 & 11011111 = 223)
Klass D  -->  1110 (224-239) (11100000 = 224 & 11101111 = 239)
Klass E  -->  1111 (240-254) (11110000 = 240 & 11111111 = 255 men 255 får vi
inte använda, det är en broadcast adress)
```

Adresser

Privata

Klass A ---> 10.0.0.0 till 10.255.255.255 (ett jätte nät)
Klass B ---> 172.16.0.0 till 172.32.255.255 (32 mellanstora nät)
Klass C ---> 192.168.0.0 till 192.168.255.255 (256 små nät)

Specialadresser

169.254 ---> APIPA adresser (Automatic Private IP Addressing)
127.0.0.1 (och hela 127 serien) ---> Loopback adresser
224 till 239 ----> Multicast

Hubb & Switch

En hubb skickar trafiken till alla portarna. En switch däremot håller redan på vilken/vilka MAC-adresser som sitter i varje port och skickar därför trafiken enbart till den porten. En multiport bridge är en switch. Bara en bridge eller L2-brygga kopplar ihop 2 eller flera segment och har oftast bara ett fåtal (två) portar. Multiport bridge indikerar alltså att den har många portar medan bara bridge har två portar. En brygga används också för att koppla ihop segment av flera olika kabeltyper t.ex. fiber med koppar.

Collision domain

En hubb är en enda stor collision domain medan på en switch är varje port en collision domain. En collision domain är alltså där kollisioner kan inträffa.

Loopar

Kopplar man samman flera switchar är de inte medvetna om varandra och en nod verkar således finnas i alla tre switcharna. När datorn då skickar ett paket till en annan så kommer paketet börja att gå runt runt runt eftersom den tror att datorn finns i alla switcharna. En loop har bildats. En loop kan också bildas om man kopplar in en TP kabel i två portar på samma switch. Till skydd mot detta använder man STP, Spanning-Tree Protocol. STP är något gammalt och ibland långsamt på att öppna upp portar vid start

m.m. (som i Packet Tracer övningarna). Därför har man utvecklat ett nytt protokoll som heter RSTP och står för Rapid Spanning-Tree Protocol. Hemma-switchar är dumma och har inte STP.

Failure Domain

Den del av nätverket som påverkas vid fel.

Broadcast domain

Inom vilken del av ett nätverk som en broadcast finns på, d.v.s. det logiska nätet. Broadcasts traveserar inte routrar och routern blir alltså en avgränsning för broadcast.

ARP

ARP står för Address Resolution Protocol håller reda på vilket IP nummer som går till vilken MAC-adress.

1. ARP Requst (broadcast till alla på nätverket)
2. ARP Reply (unicast svar tillbaks)
3. Updated ARP Information (kommunikationen kan inledas)

Routrar

ANDing används för att kolla om hosten är på samma nät eller ej. Routerns uppgift är att dirigera trafik till andra nätverk. AND:ing är Bitwise Logical AND Operation. Boolsk algebra säger att 0+0=0, 0+1=0 och 1+1=1.
Nu tar vi adressen från Rikards slide 140.179.240.200 med subnätmasken 255.255.0.0. Nu ställer vi upp adressen och nätmasken binärt ovanför varandra och utför sedan boolsk algebra på den.

```
IP:       10001100.10110011.11110000.11001000
Nätmask:  11111111.11111111.00000000.00000000
Nät-ID:   10001100.10110011.00000000.00000000
```

Nu vet vi alltså att Nät-ID:t är 10001100.10110011.00000000.00000000 i binärt vilket blir 140.179.0.0 decimalt. Datorn vet nu alltså vilket nät som IP-adressen tillhör, alltså nätet 140.179.0.0.

Routern behöver veta följande:

- Destinationsadress
- Neighbour routers (grannroutrar)
- Möjliga vägar att skicka paket till andra fjärrnätverk
- Bästa väg
    - Inte nödvändigt

Default gateway använder både hostar och routrar för att ha en standardväg ut från sitt eget nätverk.

RIT = Routing Information Table

Exempel 192.168.2.0 nås via 172.31.0.2

MAC-adresser kan inte travesera routrar. När ett paket lämnar routern för nästa hopp visas routerns MAC-adress som avsändare tills nästa router tar vid osv. När en dator ska skicka ett paket till en dator som inte är i det lokala nätet används MAC-adressen till default gateway som MAC till IP-numret på fjärrdatorn.

Statisk routing så använder man RIT-tabeller. Vid dynamisk routing används protokoll som RIP, OSPF, BPG, IS-IS osv.

Felsökning

Med ping

1. Pinga först 127.0.0.1 för att kolla så TCP/IP protokollet är korrekt installerat
2. Pinga det egna IP-numret
3. Pinga routerns (default gateway) IP-nummer
4. Pinga en host på insidan
5. Pinga routerns utsida (WAN-adressen)
6. Pinga ISP:ns gateway (nästa hopp)
7. Pinga ett IP på internet vi känner till 8.8.8.8
8. Pinga ett hostname på internet och se om det resolvar

Andra verktyg för felsökning

- netstat
- ifconfig / ipconfig
- traceroute
- nslookup
- dig
- host
- nm-tool
- nmap

Kabeltyper

TP-kablar

RJ45 hanar i ändarna. TP står för Twisted Pair och partvinningen är till för att motverka egengenererade störningar. TP-kablar finns i olika utföranden med olika skydd mot yttre störningar. Partvinningen avgör kvalitén på kabeln.

UTP = Unshielded Twisted Pair(den vanligaste)
FTP = Foiled Twisted Pair
STP (FTP + shielded) (både folielindning samt en sköld för att skydda paren), kallas ibland SFTP.

Kategorier

- Cat3 --> 10 mbit/s, används även för telefonkablar m.m.
- Cat5 --> 100 mbit/s
- Cat5e --> 1000 mbit/s
- Cat6 --> 1000 mbit/s till 10 gbit/s men 10 gbit/s är inte rekommenderat. Mellan varje par ligger en separator för att separera paren.
- Cat7 --> 1000 mbit/s till 10 gbit/s men 10 gbit/s är inte rekommenderat. Varje par ligger inlindande i en sköld och sedan är alla paren också inlindande i en gemensam sköld.

Fiber

Fiberkablar använder alltid två kablar, en för sändning och en för mottagning. Sändning och mottagning

kan således inte ske samtidigt i samma kabel. Det finns två typer av fiberkablar, Multimode och Singlemode.

Multimode

Den vanligaste förekommande formen av fiber. Den är billigare och använder vanliga LED's i varje ända för att skapa ljuset. Den heter multimode för den använder multipla ljusstrålar som alla tar sin egen väg genom kabeln. Klarar ca 2 km i avstånd

Singlemode

Den dyrare formen av fiber som ibland används i NOC m.m. Den använder laser LED istället för vanliga LED vilket gör tekniken mycket dyrare. Heter singlemode för att den använder bara en ljusstråle åt gång som går rakt fram. Klarar ca 3 km i avstånd.

RS-232

Vanlig seriell kabel. Används bland annat mellan modem och dator, mellan router och dator för att göra en första konfiguration. Ciscos RS-232 kablar är ofta blå och har en COM-ports kontakt i ena ändan och en RJ45 i andra ändan och kallas ibland Console kabel. Kopplas i Console uttag på Ciscos routrar. RS-232 måste ställas in så att den kommunicerar med rätt hastighet, antal stoppbitar m.m. Högsta hastighet är 115200 bps och den vanligaste default hastigheten vid routrar etc är 9600 bps.

ISP

En ISP är en Internet Service Provider och tillhandahåller internetuppkopplingar och tillhörande tjänster som mail, webhotell m.m. ISP:erna kopplas sedan samman med varandra genom IXP:er (Internet eXchange Point).

POP (Point of Presence)

En ISP kan man många POP's. En POP är en plats där kommunikationsutrustning finns för att tillhandahålla sammankoppling och uppkoppling för exempelvis en viss region, stadsdel etc. Användarens uppkoppling går till ISP:ns POP och sen från POP till NOC, MDF. Det är alltså mot POP:en som användaren ansluter sig i slutändan. POP:en länkar samman t.ex. PSTN (Public Switched Telephone Network, telenätet) och CPE (Customer Premise Equipment). CPE är alltså den utrustning som användaren har hos sig i form av ADSL-modem, Fiber-koppar konverter, ISDN-modem, kabelmodem etc.

NOC (Network Operations Center)

NOC:en är en ISP:s centrala plats för deras verksamhet. Här finns servrar, switchar, routrar, lagring m.m. Allt är skyddat av UPS:er, backuper, dieselaggregat, fire suppression (brand bekämpning), Raised Floor (upphöjda golv för att skydda vid översvämningar m.m.), Network Monitoring (nätverksövervakning, serverövervakning m.m.), enviornmental control (miljökontroll i form av kylanläggningar m.m.)

IDF (Intermediate Distribution Facility)

Detta är t.ex. en wiring closet eller telerum. Här finns switchar, AP:s m.m. och eventuellt AC och UPS:er.

MDF (Main Distribution Facility)

Denna kan ingå i NOC:en. Här finns servrar, switchar, routrar, lagring m.m och länkar till olika IDF och

POP.

Adressering m.m.

Supernetting är när man slår samman många små nät till ett större nät, här lånar man bitar från nätdelen.

Subnetting är när man gör flera nät istället, man lånar alltså av hostbitarna.

Man använder subnetting och supernetting för att klasserna är väldigt oflexibla. Med subnettning behöver man alltså inte hålla sig till "hela" oktetter utan kan bolla hur man vill med bitarna. Subnetting är det vanligaste man använder, supernettning används nästan bara för att slå samman nät i en router för att minska på RIT:en (Routing Information Table).

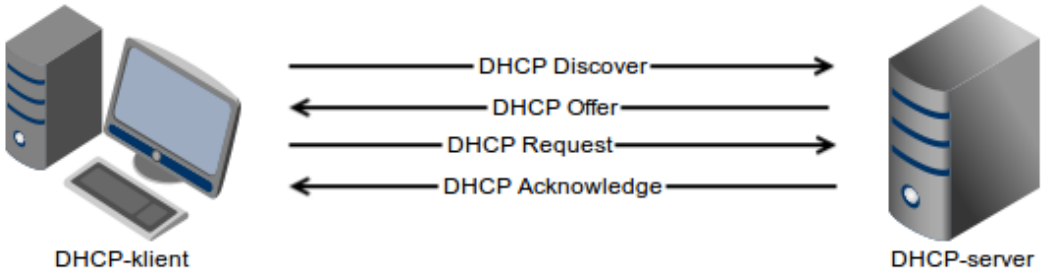
När man subnettar kallas detta för CIDR som står för Classless Inter-Domain Routing.

RFC950 säger att vi måste plocka bort första och sista nätet!
Denna reviderades 1995 till **RFC1878** och vi får nu använda alla näten.
Det måste specificeras vilken RFC man menar.

DHCP

DHCP står för Dynamic Host Configuration Protocol och används för att dynamiskt tilldela IP-adresser till hostar i nätverket. I denna ordning sker DHCP-förfarandet.

1. DHCP Discover skickas ut på den generella broadcast adressen 255.255.255.255 som DHCP-servern snappar upp.
2. DHCP Offer skickas till hosten med ett erbjudande av en IP-adress. Klienten testar nu även om IP-adressen är ledig så ingen annan host på nätet har just det IP-numret.
3. DHCP Request skickas till servern om ingen annan har adressen.
4. DHCP Acknowledge skickas tillbaks till klienten från servern att han nu har fått IP-adressen tilldelad sig och att den är reserverad hos servern åt honom.



Förnyelse av IP-adressen sker vid uppstart av klienten eller vid halva utlåningstiden (kan också framtvingas med ipconfig /renew eller dhclient restart).

I nät med många ledig adresser kan man sätta lång lease-time på uppåt 30 till 60 dagar. I mindre nät brukar man bara sätta mycket kortare lease-time.

Viktigt att tänka på

- Alltid skapa spannet av IP-adresser i samma nät som ens eget interface.
- Aldrig låta två DHCP-servrar överlappa varandras spann av IP-adresser.

Flera DHCP-servrar

- Kan behövas om man har flera logiska nät.
- Om man använder VLAN.

Detta går dock att lösa med hjälp av DHCP relays som kan kommunicera med DHCP:n genom routern.

NAT

Network Address Translation döljer interna IP-nummer ut mot Internet. NAT är adressöversättning för att omvandla privata adresser till publika adresser på Internet. Exempelvis 100 privata adresser bakom en NAT delar på en och samma publika IP-nummer. NAT:en håller reda på IP och MAC till klienten på insidan för att kunna skicka tillbaks svaret till klienten.

DNAT (Dynamic NAT)

Använder en pool adresser som är dynamisk. T.ex. 10 interna IP nummer och 10 externa IP nummer, det interna IP-numren kan översättas dynamiskt till någon av de 10 externa IP-numren. Här används alltså samma portar både internt och extern, d.v.s det sker inget portöversättning. Det hela är som om det vore en direkt förbindelse.

PAT eller NAPT (eller SNAT)

Detta är portöversättning eller port redirection. Det är detta som är vanligaste förekommande. Det kallas även overloading (för att inte poolen med externa IP-adresser räcker till alla hostar på insidan). När poolen inte räcker till övergår routern automatiskt till PAT, Port Adress Translation. Man använder alltså här portar istället för adresser för att "trycka in så många hostar som möjligt" på de få externa IP-numren som finns att tillgå. Det är därför det kallas Port Översättning, för att man översätter portar istället för IP-nummer. Används också när man vill skydda server i t.ex. sin DMZ. Observera att en port bara kan användas en gång för port forwarding om man bara har en IP-adress.

Portar

Det finns 65536 portar att tillgå. Dessa sköts via TCP eller UDP i transportlagret. Över 30000 samtidiga sessioner kan nå internet samtidigt på ett enda IP-nummer. Behöver man fler sessioner än så får man skaffa fler IP-nummer. Port kallas ibland även för service adress. Alla vanliga portar finns i /etc/services filen i Unix-system. Dessa kallas ofta well-known ports och är de lägre 0-1023 portarna. Registered port 1024-65536 som är registrerade till något program eller tjänst. Random ports som slumpas fram källportar systemet. Några vanliga portar listas här.

Portnummer	Applikation/tjänst	Transportprotokoll
21	FTP	TCP
20	FTP-data	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP

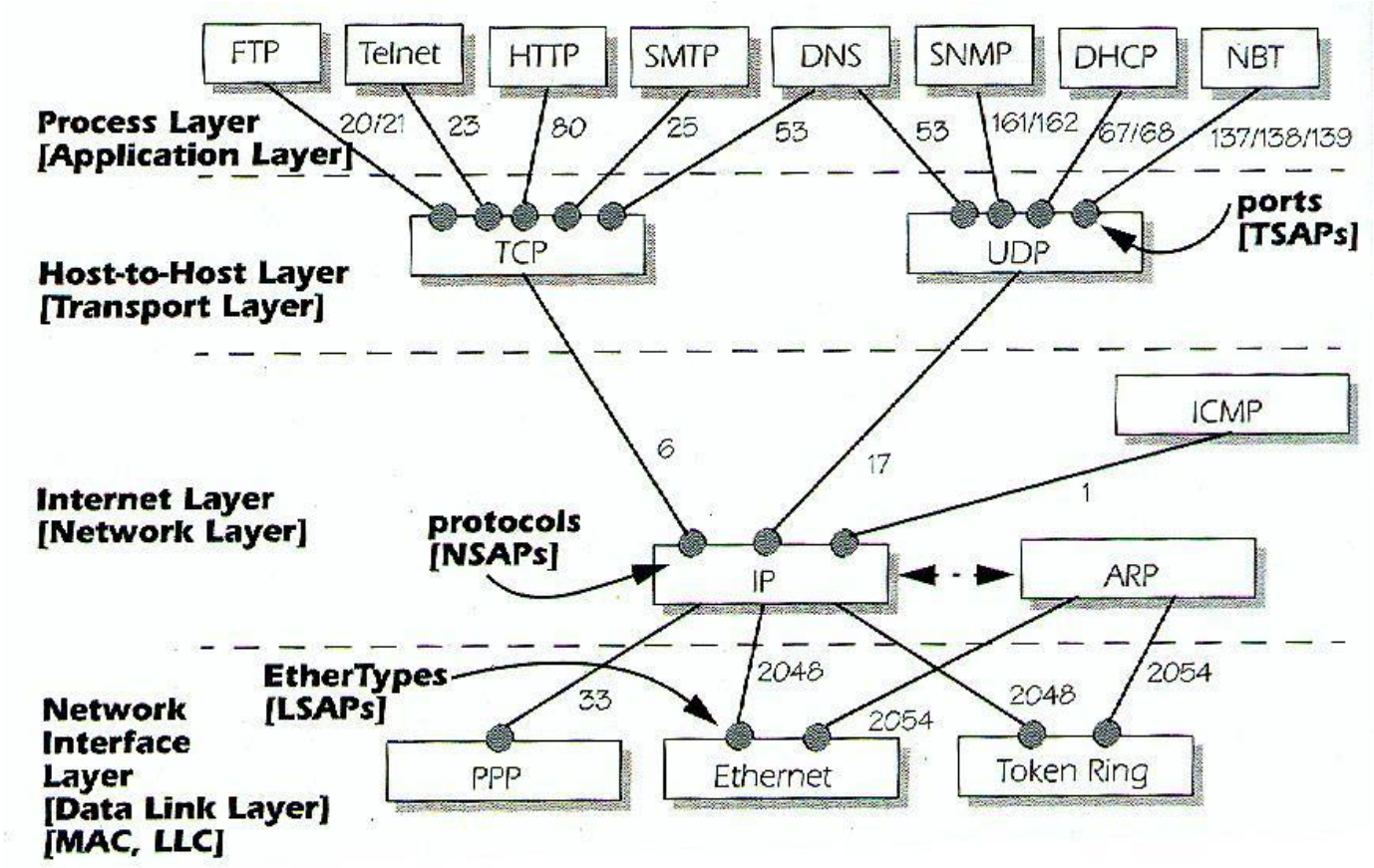
53	DNS	TCP/UDP
67	DHCP (till server)	UDP
68	DHCP (till klient)	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
123	NTP	UDP
137	Netbios-ns	UDP
138	Netbios-dgm	UDP
139	Netbios-ssn	UDP
161	SNMP	UDP
143	IMAP4	TCP
443	HTTPS	TCP

TCP/IP SAP

SAP står för Service Access Point och finns i flera "lager" baserat på DoD-modellen fast med något annorlunda namn.

SAP	DoD	Innehåll
SAP	Application	FTP (21/20), Telnet (23), SSH (22), DNS (53), HTTP (80)
TSAP	Transport	TCP, UDP
NSAP	Internet	IP, ARP, ICMP
LSAP	Network Access	PPP, Ethernet, Token Ring

SAP-bilden från Rikards slide



Transport protokoll

- TCP (Transmission Control Procotol). TCP kontrollerar alltid att paketet har kommit fram och vid fel sker automatiskt omsändning av paketet.
- UDP (User Datagram Protocol). I UDP sker inga som helst protokoll och data ska bara skickas så fort som möjligt. Eventuella kontroller av att datan har kommit fram sker i applikationen.
- RTP (Real Time Protocol). Ett nytt protokoll för t.ex. IP-telefoni m.m.
    - RTCP (Real Time Control Procol). Ett underprotokoll till RTP som hjälper till med synkningar, QoS m.m.

DNS

DNS ligger i sessionslagret.

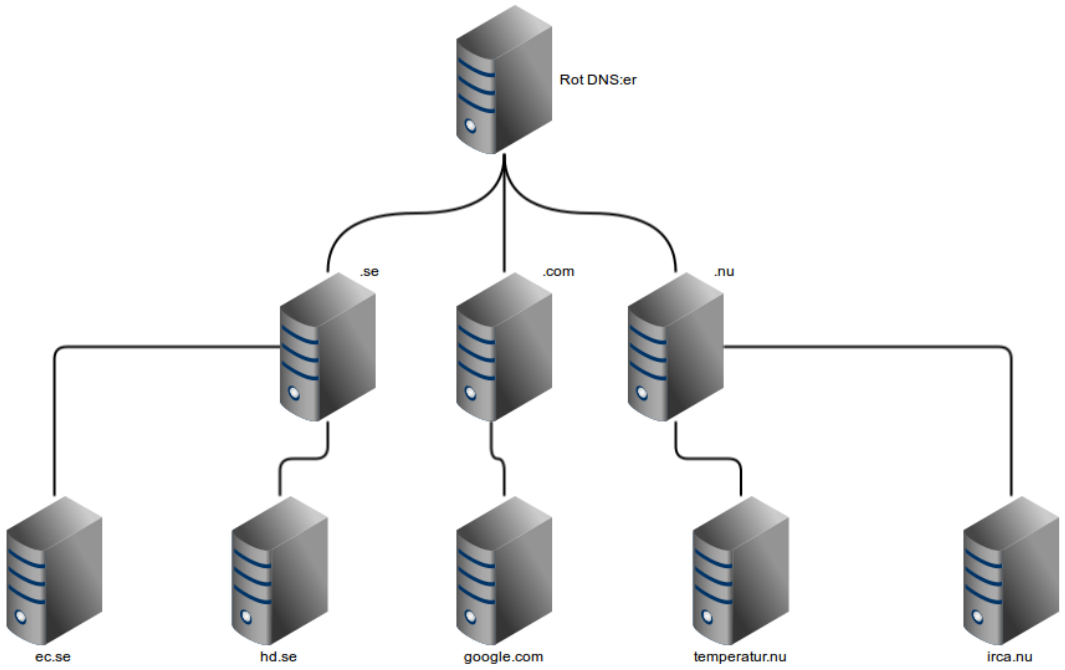
Forward zone översätter namn till IP-nummer.
Reverse zone översätter IP-nummer till namn.

Innan DNS fanns hade man bara hosts-tabeller/filer. Dessa används fortfarande för att laborera m.m.

DNS är hieraktiskt uppbyggt med 13 st rot-entries i toppen (flera faktiskt servrar). En rot-entry pekar alltså på många IP-nummer till andra rot-DNS:er. Rot-entries finns i en fil i Linux-system som heter **root.hints**.

Under rot-DNS:erna finns TLD:erna (Top Level Domain).

Under TLD:erna finns de auktoritära DNS:erna, d.v.s. domänernas egna DNS:er, typ hd.se, google.com, ec.se osv. Dessa ansvarar för sin egen domän.



Själva processen att upplösa ett namn till ett IP-nummer kallas Name Resolution.

Klienten använder sig av en resolver i OS:et. Resolvern skickar i sin tur en resolution request till DNS-servern.

Om DNS-servern inte själv kan upplösa namnet så skickas förfrågan vidare till nästa DNS.

DNS-frågans väg

Först försöker datorn slå upp namnet via sin ISP:s DNS. Finns inte namnet här skickas frågan vidare till en av rot-servrarna. Rot-servrarna känner bara till TLD:erna och skickar frågan vidare till rätt TLD. TLD:n DNS skickar då i sin tur frågan vidare till den auktoritära DNS:en som då slår upp rätt hostnamn sin DNS och svarar på förfrågan.

Transportprokoll vid DNS

Mellan klient och DNS-server används UDP (för snabbheten)
Mellan DNS-server och DNS-server (zone transfers) används TCP för att säkerställa att hela zonen blev rätt överförd. Här behöver det heller inte gå så fort.

Olika typer av DNS-servrar

Primary DNS har all sin data lokalt lagrad i konfigurationsfiler.

Secondary DNS (eller Slav DNS) får sin data genom zone transfers från den primära DNS:en.

Caching Only DNS cachar och forwardar bara DNS-förfrågningar.

Zoner

I den omvända zonen vänder man på adresserna. Exempelvis nätet 192.168.0 nätet heter 0.168.192in-addr.arpa.

Resursposter

De resursposter som MÅSTE finnas är:

- SOA (Start of Authority) som talar om att zonen är auktoritär d.v.s. kontrolleras av denna DNS.
- NS (Name Server). Här anges namnservrarna för domänen. Den egna namnservern måste också vara med här.
- A (Adress). Upplösning av vanliga hostar. "kalle IN A 192.168.0.100".

Andra resursposter är:

- CNAME (Common Name) som skapar alias för hostar med A-record. "kalle IN CNAME erik.ec.se".
- MX (Mail eXchange) anger mailservrarna för domänen.

Reverse lookup zone

- PTR (Pointer) pekar på A-records. Sista oktetten används t.ex. "2 IN PTR oby.ec.se".

Trådlöst

Bluetooth

Med Bluetooth bygger man PAN (Personal Area Network) med t.ex. mobiltelefon, headset, läsplatta och laptop. Det finns tre klasser av bluetooth vilka är:

- Klass 1 --> 100 meter (100 mW)
- Klass 2 --> 10 meter (2,5 mW)
- Klass 3 --> 2 meter (1 mW)

Det finns Bluetooth AP's för att enklare nå alla sin enheter i PAN:et. Dessa AP kan även sammankoppla PAN:et med LAN:et och kan även erbjuda tjänster som gemensam FTP-server i PAN:et m.m. Dock blev aldrig Bluetooth AP någon större hit och är idag svåra att få tag på.

Man kan använda TCP/IP med Bluetooth även om det är ganska ovanligt idag.

Nackdelar med Bluetooth

Det finns flera olika stackar, där varje tillverkare har egna tjänster m.m. Svårt att veta vilken stack som medföljer en enhet och vilka tjänster denna har. Dessutom behöver inte alltid uppdateringar vara gratis, ibland tar företagen betalt för dessa.

WLAN (Wireless LAN)

Fördelar

WLAN är har en del fördelar mot kabelnät, t.ex. att man slipper kabeldragning och därmed blir mindre installationskostnad. Det är dessutom snabbt att bygga ut då man inte behöver dra nya kablar till nya kontor eller byggnader vilket annars hade behövts.

Nackdelar

Det finns en del nackdelar med WLAN och dessa är framförallt att hastigheten minskar med antalet användare, alltså ju fler användare ju sämre hastighet. En annan nackdel kan vara att det krävs många

AP's om stora nät ska byggas. Dessutom är WLAN känsligt för störningar från andra trådlösa enheter som andra WLAN, Bluetooth m.m. Även mikrovågsugnar och generatorer m.m. kan störa ut kommunikationen. En annan nackdel är att standarderna ändras ofta.

Standarder

- IEEE 802.11 (1-2 Mbps)
- IEEE 802.11a (54 Mbps, 5 Ghz bandet, ovanlig standard)
- IEEE 802.11b (11 Mbps, 2,5 Ghz bandet)
- IEEE 802.11g (54 Mbps, 2,5 Ghz bandet)
- IEEE 802.11n (300 Mbps, både 2,5 & 5 Ghz bandet)

Säkerhetsstandarder

- IEEE 802.11i
  - Krypterad trafik
  - Implementerat som WPA2 (säkrast)
- IEEE 802.1x
  - Autentisering (inloggning), används för både LAN och WLAN (är alltså inte specifik för WLAN)

Olika modes

Ad-hoc mode

Detta är detsamma som peer-to-peer, alltså man kopplar ihop enheterna direkt till varandra utan en AP. T.ex. laptop till laptop eller telefon till laptop. Max 9 klienter stöds.

Infrastructure mode

Det vanligaste förekommande, här har man AP som är en brygga mellan LAN och WLAN, d.v.s man kopplar in sig på samma logiska nät som det trådburna nätet. En trådlöst router arbetar dock med flera logiska nät. Det finns är trådlösa routers som ger tillgång till t.ex. skrivare, 3G, LAN, Internet, NAS-enheter m.m.

En klient sänder ut ett probe request och lyssnar efter probe respons från AP:n.

Antenner

Rundstrålande antenner stålar 360 grader runt antennen men bara lite uppåt och nedåt. Dessa har kortast räckvidd men bäst täckningsområde. Riktantenner används när långa avstånd måste uppnås. En riktantenn kan klara upp till flera mil med den lagliga effekt på WLAN på 100 mW. För att det ska vara lönt att köpa fina riktantenner måste man även köpa dyrare lågförlust kablar annars försvinner effekten i kabeln.

SSID

Service Set Identifer, är det trådlösa nätets ID. SSID:t sänds ut med *beacon frames.* Som en fyr.

Hot & risker

Avlyssning av trafik, intrång om dåligt lösenord eller öppen AP. Andra hot och risker är:

- Fake AP, en öppen AP som låter alla ansluta sig. Jätte bra tycker kanske den som surfar på den AP:n, men AP:n ägs av en hacker som sniffar åt sig alla trafiken!
- Rouge AP, en otillåten AP på t.e.x ett företag som släpper in trafik på nätet bakom brandväggen.
- Öppna nät, farligt för avlyssning

- WEP är osäkert! Knäcks på kort tid!
- DoS attacker

Modes på WLAN-kortet

Monitor mode stöds inte av alla chipset men är väldigt användbart. Med monitor mode kan man lyssna på trafik utan att behöva vara ansluten till en AP. Monitor mode tar alltså in ALL trafik som passerar i etern. Promiscous mode stöds däremot av alla chipset och är detsamma som för ett vanligt LAN NIC. D.v.s. väl anslutet till en AP kan man med detta mode lyssna på all trafik som passerar kortet.

Säkerhet

De olika steg är:

- Footprinting
  - Samla in information om målsystemet
  - Öppen information, google, telefonkataloger, e-post-listor m.m.
  - Portscanning, pingsweepers.
- Enumeration
  - Skaffa sig mer detaljerad information om målet så som
  - Användare, maskiner, versioner, programvaror
  - Några vanlig tjänster som ofta används som läcker är
    - NetBIOS
    - RPC
    - SMB
    - DNS
    - SNMP
    - AD/LDAP

Brandväggar

Minst tre NIC för LAN, DMZ och WAN. Med bara två NIC blir det svårt att skapa bra regler och skydd.

SPI = Stateful Packet Inspection innebär att brandväggen håller koll på alla sessioner. Alla paket som inte ingår i en session kastas. SPI kollar på flaggan på TCP/UDP paketen så att denna har "established" och tillhör en session.

Dual-Homed Gateway

En proxy med två NIC, trafiken routas inte utan passerar en proxy-programvara. Användaren måste ofta autentsiera sig.

Proxyservern var den första ursprungliga brandväggen. Skickar godkända paket till LAN-hosten. HTTP-proxys kan även cacha webbsidor, t.ex. Squid.

Screened Host (Bastion Host)

Befinner sig i nätet innanför brandväggen. Inkommande trafik dirigeras till screened hosten. Utgående trafik dirigeras till SH:n eller direkt till brandväggen.

Screened subnet

- Två paketfiltrerande brandväggar

- Litet LAN mellan dem
    - En DMZ
    - För t.ex. webb, mail och FTP-servrar

Felsökning

Ställa öppna frågor först, sedan stängda. Var noga med att dokumentera allt!