SISU

PUBLIKATION 96:24

BEVAKNINGSRAPPORT – OKTOBER 1996

Datornätverk: Teknik och Trend

– en rapport från Networld+Interop

Mathias Johanson

Jan Örnstedt

SVENSKA INSTITUTET FÖR SYSTEMUTVECKLING

Innehåll

Inledning

Den del av databranschen som för närvarande genomgår den största tekniska revolutionen är tveklöst kommunikationsområdet.

Nätverken blir snabbare och snabbare både vad gäller lokala nätverk och långdistansnät. Detta öppnar möjligheter för utveckling av distribuerade system som tidigare inte varit realiserbara. Helt nya applikationsområden såsom videokonferenssystem, telemedicin och video on demand håller på att växa fram.

Denna rapport är tänk att ge en introduktion till de nya teknologierna och trenderna inom datakommunikationen och presentera nyheter och intryck från nätverksmässan/ konferensen **Networld+Interop**, som hölls 16–20 September 1996 i Atlanta, och samlade folk från hela världen verksamma inom området datakommunikation och datornätverk.

Huvudfokus för konferensen var höghastighetsnätverk, men även ämnen som säkerhet, Internet och intranetteknik behandlades utförligt.

Alla de ledande nätverkstillverkarna fanns på plats på utställningsgolvet för att demonstrera sina produkter, liksom ett stort antal mjukvaruleverantörer och andra relaterade företag.

Höghastighetsnätverk – en teknisk introduktion

Fast Ethernet

Fast Ethernet är en uppgradering av den välbekanta Ethernettekniken som idag är den vanligaste typen av lokala nätverk. Ethernet, som ger en överföringshastighet på 10 Mbits/s, har med egentligen exakt samma teknik gjorts 10 gånger snabbare, d v s överföringshastigheten för Fast Ethernet ligger på 100 Mbits/s. För att beskriva hur man kunnat åstadkomma detta repeterar vi först grunderna för Ethernet.

Ethernet är ett s k CSMA/CD-nätverk (Carrier Sense Multiple Access, Collision Detection), vilket innebär följande: Alla maskiner på samma nätverkssegment delar på samma fysiska transmissionsmedium. Detta medför att en algoritm behövs för att undvika att flera maskiners transmissioner kolliderar.

I Ethernet lyssnar maskinerna på transmissionsmediet innan de börjar sända; om någon annan sänder väntar man en liten stund och försöker sedan igen. Om två maskiner börjar sända ungefär samtidigt måste båda upptäcka kollisionen och vänta en slumpmässigt vald tidsperiod (för att undvika att de börjar samtidigt igen) för att sedan försöka på nytt. För att båda skall upptäcka kollisionen krävs att paketen som sänds är minst så långt att tiden det tar att sändas är minst lika lång som den dubbla propageringstiden för elektronerna mellan de båda sändarna. För att inse detta betrakta värstafallssitiuationen att maskin A börjar sända och precis innan paketet når fram till B börjar B sända. Paketen kolliderar, vilket B upptäcker omedelbart, men A upptäcker inte detta förrän den första biten som B sänt har propagerats fram till A. Tiden från det att A börjar sända tills det att A upptäcker kollisionen är följaktligen två gånger propageringstiden för elektronerna mellan A och B. Propageringstiden beror på elektronernas hastighet i koppar (som är konstant) och avståndet mellan maskinerna. I Ethernetspecifikationen har man satt en begränsning på det längsta segment som får förekomma i ett nät till 2800 m. Utifrån detta kan man räkna ut att den minsta paketlängden som tillåts om man sänder med hastigheten 10 Mbits/s är 68 bytes.

För att man skall kunna utnyttja samma teknologi med en hastighet på 100 Mbits/s måste man antingen minska den maximalt tillåtna segmentlängden, eller öka minsta tillåtna paketlängd, eller en kombination av de båda. Eftersom alternativet att öka den minimalt tillåtna paketlängden gör att man får sämre bandbreddsutnyttjande har man valt att skala ner den maximala segmentlängden med en faktor 10. På grund av vissa praktiska faktorer har 210 m specificerats som den maximalt tillåtna segmentlängden i Fast Ethernet.

Ett sätt att göra ett ethernet effektivare är att dela upp det i flera separata kollisionsdomäner med hjälp av bryggor. En brygga är en utrustning som har två eller flera ethernetportar mellan vilka den vidarebefordrar paket. När den tar emot ett ethernetpaket på en port inspekterar den adressfältet och lär sig att stationen som sänt paketet finns på just denna porten. När den sedan får ett paket som är adresserat till denna station vidarebefordras paketet endast på den rätta porten. Detta gör att man slipper kollisioner på de segment där aktuell sändare och mottagare inte befinner sig.

Växlat Ethernet

I stället för att koppla samman alla maskiner via ett delat medium, alternativt uppdelat av bryggor, kan man installera en växel som ett nätnav. En växel fungerar som en brygga med den skillnaden att den kan ta emot och skicka paket på flera portar parallellt. Detta innebär att maskiner som är sammanlänkade med ett växlat nät inte behöver tävla med andra om bandbredd. En vanlig typ av ethernetväxel har ett antal portar för 10 Mbits/s där arbetsstationer ansluts och en eller flera 100 Mbits/s-portar för filservrar eller kopp-

lingar till andra nät. Nätverkskort för Fast Ethernet kan automatiskt ställa om från 10 till 100 Mbits/s så att maskiner med gamla Ethernetkort kan kopplas på ett växlat Ethernet där till exempel fileservern är ansluten med Fast Ethernet. Detta gör det naturligtvis attraktivt att uppgradera till ett växlat Ethernet för organisationer som redan har ett stort antal ethernetstationer installerade.

Full duplex

Vissa ethernetkort har idag möjligheten att använda full duplex. Detta innebär att olika partvinnade koppartrådar används för sändning och mottagning och fungerar således endast för punkt-till-punktförbindelser. Då växlade ethernet består av punkt-till-punkt-förbindelser mellan arbetsstationer och växel går det utmärkt att utnyttja denna teknik härvidlag. Full duplex ger en fördubbling av bandbredden och eliminerar begränsningen av hur långa segment som maximalt kan nyttjas.

Gigabit Ethernet

Efter den lyckade uppgraderingen av Ethernet till Fast Ethernet ställer man sig naturligtvis frågan om man på samma sätt kan skala upp tekniken ytterligare. Svaret är att det pågår redan standardiseringsarbete för en Ethernetvariant som kallas Gigabit Ethernet. Problemet är att om man i denna standard går tillväga på samma sätt som för Fast Ethernet kommer den maximala segmentlängden att bli endast omkring 20 m, vilket ju är för kort för de flesta nät. Alternativt kan man ändra på begränsningen för hur små paket som får sändas, men detta medför andra komplikationer. Det är alltså inget trivialt problem att förbättra Ethernettekniken med ytterligare en tiopotens.

Förmodligen kommer Gigabit Ethernet att utnyttjas endast över växlade nät vilket ju gör att segmenten kan göras godtyckligt långa. En standard för Gigabit Ethernet beräknas finnas i mars 1998. Prototypversioner existerar redan.

FDDI

Fiber Distributed Data Interface (FDDI) är en nätverksteknologi som existerat några år och blivit populär främst som backbone för medelstora lokala nätverk. Logiskt består ett FDDI-nätverk av två ringar, varav den ena är redundant. På ringen cirkulerar ett special-paket som kallas *token*. När en nod på ringen vill sända måste den invänta token, sända ett paket och sedan lämna ifrån sig token igen. På detta sätt kommer inga kollisioner att uppstå. Vid händelse av ett brott på ringen kan den redundanta ringen användas för att koppla förbi brottet. Vid två eller flera brott kommer nätet att segmenteras.

Stationer kan anslutas antingen direkt till båda ringarna, eller via en typ av utrustning som kallas koncentrerare. Med hjälp av koncentrerare kan träd av stationer byggas upp och anslutas utan att varje station behöver ha två nätverksanslutningar. En station som är ansluten via en koncentrerare kan vara ur funktion utan att ringen bryts. En station kan också anslutas till två koncentrerare för att ge ökad feltolerans. Detta kallas för *dual homing*.

FDDI har en maximal kapacitet på 100 Mbits/s och en maximal utbredning på ca 100 km. Det som begränsar kapaciteten för ett FDDI-nätverk är i första hand den tid det tar för token att propageras ett varv på ringen (TRT, Token Rotation Time). Denna tid beror naturligtvis på hur stort avstånd ringen sträcker sig över och hur många stationer som är anslutna.

Det finns två prioritetsklasser vilka kallas synkron service (hög prioritet) respektive asynkron service (låg prioritet). För synkron service är fördröjningen uppåt begränsad av 2*TRT, vilket gör den lämplig för realtidsdata.

FDDI-nät med endast två stationer kan utnyttja full duplex, d v s maskinerna sänder när de vill och behöver inte vänta på token. Detta fördubblar bandbredden och ger kortare fördröjningar.

Trots sitt namn kan FDDI även implementeras över koppar. Man ser ibland beteckningen CDDI för detta.

100VG-AnyLAN

Denna nätverksteknologi, som också är känd under namnet *Demand Priority Access LAN*, bygger på att en central instans delegerar tillstånd att sända till övriga noder enligt en schemaläggningsalgoritm. Nätverket är strukturerat i en trädhierarki, där löven är arbetsstationer och noderna är maskiner som hanterar schemaläggningen av transmissioner. När en station önskar sända skickar den en begäran härom till noden ovanför, vilken upprätthåller en kö över de stationer som för tillfället vill sända. Noden ifråga skickar sedan i sin tur en begäran uppåt i hierarkin. När en nod får tillåtelse att sända låter den sina "barn" få sändningstillståndet i tur och ordning. Stationerna i trädets löv sänder ett paket när de får tillstånd till det och paketet repeteras sedan genom trädet till sin destinationsadress.

Paketformatet i 100VG-AnyLAN kan följa standarden för antingen Ethernet eller Token Ring. Detta betyder att nätverkskort för dessa mycket allmänt förekommande nätverk kan användas vilket potentiellt kan göra en migrering till 100VG-AnyLAN billigare. Endast ett MAC-format kan användas i samma fysiska nät.

100VG-AnyLAN tillåter två prioritetsnivåer, vilket implementeras med prioritetsköer i trädets noder. En nod kan få sitt sändningstillstånd återkallat om en överordnad nod har fått en begäran av högre prioritet från en annan gren i trädet.

ATM

Bakgrund

ATM, som står för Asynchronous Transfer Mode, är en kommunikationsstandard som definieras av CCITT parallellt med en sammanslutning av tillverkare som kallas ATM Forum. ATM är tänkt att vara basen för nästa generations ISDN, Broadband ISDN, som skall tillhandahålla kommunikationstjänster med överföringshastigheter över 2 Mbits/s.

ATM är sprunget ur ett behov från telekombranschen att ersätta sina analoga telenätverk med en digital motsvarighet. Eftersom telenäten blir alltmer datoriserade vore det önskvärt om datakommunikationen mellan teleoperatörens utrustningar och den normala telefontrafiken kunde utnyttja samma teknologi. Dessutom vill man naturligtvis kunna erbjuda nya datakommunikationstjänster till sina kunder.

En av grundtankarna med ATM är att det skall vara lämpat för flera olika typer av digital kommunikation – såväl telefoni som digital television och traditionell datakommunikation.

Fibernätverk

Även om man idag kan köra ATM över såväl koppar som radiolänk så utvecklades det ursprungligen för att utnyttja fiberoptik. Telefonbolagen satsar stora resurser på att byta ut sin kopparbaserade infrastruktur mot fiber, på grund av fiberns överlägsna transmissionsegenskaper.

När en ljusstråle passerar från ett material till ett annat kommer en del av ljuset att passera genom det andra materialet, medan övrigt ljus reflekteras. Hur stor del som passerar gentemot hur stor del som reflekteras beror på infallsvinkeln och förhållandet mellan de två materialens brytningsindex. Om infallsvinkeln är större än ett visst värde reflekteras allt ljus. Det är denna egenskap som utnyttjas i optiska kablar.

En fiberoptisk kabel består av en mycket tunn kärna av glas som omges av ett lager glas med lägre brytningsindex. Materialen är valda så att man skall få total reflektion om en ljusstråle skickas in i fibern och kabeln inte böjs alltför mycket.

Det är värt att påpeka att ljusets hastighet i glasfiber är ungefär lika hög som elektronernas hastighet i en kopparkabel, d v s ungefär två tredjedelar av ljusets hastighet i vakuum. Det är alltså inte denna egenskap som gör att det går att skicka information snabbare i fiber än i koppar, utan att signalpulserna kan göras kortare.

På grund av vissa fysiska faktorer kan ljus inom tre band av det optiska spektrat sändas effektivt genom glasfiber. Vart och ett av dessa band är ungefär 25 THz brett, vilket innebär att man beroende på kodning kan skicka mellan 50 och 70 Tbits/s.

Cellnätverk

ATM är ett exempel på en typ av nätverk som kallas cellnätverk. Grundidén med cellnätverk är att informationen skickas i mycket små paket av fix storlek som kallas celler. I traditionella paketbaserade nätvek (t ex Ethernet) är paketen av varierande storlek och man eftersträvar så långa paket som möjligt för att reducera overhead. I ATM är cellernas storlek 53 bytes, varav 5 bytes är kontrollinformation, vilket ger en overhead på ca 9% vilket är väldigt mycket jämfört med andra teknologier. Detta är också en anledning till att många är skeptiska till ATM.

Fördelen med att ha paket av en fix längd är att det gör det mycket enklare att bygga växlar och multiplexorer. Därför är det attraktivt inom telekombranschen.

När en sändare skall skicka iväg data i ett cellnätverk måste informationen fragmenteras för att passa i cellerna. Den sista cellen kommer att bli endast partiellt fylld såtillvida inte datamängden som man vill sända råkar vara en multipel av cellstorleken. Alltså kommer i genomsnitt halva datafältet av den sista cellen för varje transmission av data att vara tomt. Ju mindre celler man har desto mindre blir naturligtvis detta spill. Detta är en av fördelarna med att ha små celler.

Den förmodligen viktigaste anledningen till att cellnätverk blivit intressanta är att de reducerar fördröjningar. Betrakta till exempel situationen att man vill sända tal i realtid över ett digitalt nätverk (t ex ett telefonsamtal). Ljudet från den som talar måste då digitaliseras till samples som packas ner i celler och skickas ut på nätverket. Ju längre celler man måste fylla, desto längre fördröjningar uppstår till följd av paketeringen. En annan oönskad effekt som man kan reducera i cellnätverk är så kallade serialiseringsfördröjningar som uppkommer då en växel skall multiplexera två inkommande förbindelser till en. Antag att en cell med realtidsdata kommer på den ena förbindelsen men att det precis innan den skall växlas anländer ett stort paket på den andra förbindelsen som börjar växlas först. Den tidskritiska cellen måste då vänta tills det långa paketet har hanterats färdigt, eller också måste transmissionen av det långa paketet avbrytas. I båda fallen får man oönskade effekter som man slipper om man har små celler av fix längd.

SONET och SDH

SONET (Synchronous Optical Network) är ett signaleringsprotokoll för fibernätverk som är en del av en större CCITT-standard som kallas SDH (Synchronous Digital Hierarchy). SDH definierar hur multiplexering sker på länkar med höga överföringshastigheter och specificerar därmed ett antal standardiserade överföringshastigheter.

ATM i fibernät brukar implementeras ovanpå SONET/SDH. De överföringshastigheter som brukar nämnas i samband med ATM (155 Mbits/s, 622 Mbits/s, etc) faller tillbaka på de hastigheter som SDH-standarden definierar. ATM-tekniken i sig har ingen fast övre gräns för överföringshastighet.

Cellformat i ATM

Det finns två typer av gränssnitt för hur ATM-utrustningar skall kommunicera med varandra. Användarens utrustning (typiskt en ATM-adapter i en dator) använder ett gränssnitt som kallas UNI, User-Network Interface. Två växlar som kommunicerar inuti ett ATM-nätverk utnyttjar ett lite annorlunda gränssnitt som kallas NNI, Network-Network Interface. Tanken bakom detta är att det i ett UNI skall finnas skyddsmekanismer mot utrustning som inte följer specifikationen.

En ATM-cell består som nämnts tidigare av 53 bytes varav de första fem utgör ett huvud. Cellhuvudet innehåller adresseringsinformation (samt en del annan kontrollinformation) som modifieras av varje nod i nätverket. Adresserna är alltså lokala och identifierar *nästa nod* på vägen till destinationen. Vägvalsinformation fås ur tabeller som upprättas när förbindelsen kopplas upp. Den lokala adressen kan användas som ett index till dessa tabeller. Adresserna består av två fält; Virtual Path Identifier (VPI) och Virtual Channel Identifier (VCI). VPI kan ses som en logisk länk bestående av flera kanaler som identifieras av sin VCI. Ett cellhuvud som genereras vid ett NNI har 28 bitar långa adresser, varav 12 bitar är VPI och 16 är VCI. Vid ett UNI är VPI-fältet endast 8 bitar och VCI fältet 16 bitar. Normalt när en cell skall vidarebefordras vid ett NI används enbart VI vid vägvalet.

Virtuella förbindelser

ATM är en förbindelseorienterad tjänst, vilket innebär att en förbindelse, eller med ATM-terminologi, en kanal, kopplas upp mellan sändare och mottagare innan några celler skickas.

När förbindelsen kopplas upp tilldelas varje nod på vägen en VCI/VPI-adress. För att detta skall kunna ske dynamiskt finns det för ändamålet ett signaleringsprotokoll.

Adaptionslager

När information skall skickas ut på ett ATM-nät måste den fragmenteras till segment om 48 bytes för att passa i cellerna. Detta kan göras på olika sätt enligt protokoll som kallas för ATM Adaption Layers, AAL. Ursprungligen utvecklades fyra olika protokoll (AAL1, AAL2, AAL3/4 och AAL5) avsedda för fyra olika klasser av applikationer. AAL5 som är avsedd för traditionell datakommunikation har visat sig fungera för det mesta och är det mest använda idag.

Jämförelse mellan olika lokala höghastighetsnät

I tabellen nedan görs en sammanfattande jämförelse mellan de nätverksarkitekturer som diskuterats. Det måste emellertid påpekas att jämförelsen mellan ATM och övriga teknologier inte är riktigt adekvat, eftersom ATM inte är en teknik för delat media som de övriga.

Jämförelse	FDDI	Fast Ethernet	100VG-AnyLAN	ATM
åtkomstprotokoll	token	CSMA/CD	round robin	cellväxling
delat/växlat	delat	delat	delat	växlat
antal stationer	500	1024	ospecificerat	obegränsat
paketstorlek	4500 bytes	1518 bytes	1518 eller 4500	48 bytes
utsträckning	100 km	210 m	2.5 km	obegränsat
komplexitet	medium	låg	medium	hög
standardisering	komplett	komplett	komplett	delvis komplett
fysiskt lager	fiber, STP, UTP Cat 5	fiber, STP, UTP Cat 3, 5	fiber, STP, UTP Cat 3, 5	fiber, STP, UTP Cat 5
hastighet	100 Mbits/s	100 Mbits/s	100 Mbits/s	implement.-beroende, tex 622 Mbits/s
topologi	dubbel ring	delad kabel	tråd	mesh av växlar
tjänsteklasser	2	1	2	4

Effektivitet

Ett nätverksprotokolls effektivitet definieras som kvoten mellan den bandbredd som är tillgänglig för användaren och den bandbredd som MAC-lagret erbjuder. I tabellen[1] nedan ges ett antal effektivitetsvärden för olika konfigurationer av nätverk och för olika paketstorlekar. Observera återigen att jämförelsen med ATM haltar något. Antalet stationer som är anslutet till ATM-nätet påverkar inte effektiviteten eftersom mediet inte är delat.

Paket-storlek (bytes)	FDDI 20 stationer 2.2 km	Fast Ethernet 20 stationer 210 m	100VGAnyLAN 20 stationer 200 m	100VGAnyLAN 20 stationer 2.2 km	ATM n stationer n km
64	84 %	65 %	46 %	19 %	58 %
128	91 %	74 %	63 %	32 %	78 %
256	96 %	80 %	77 %	49 %	78 %
512	98 %	83 %	87 %	86 %	85 %
1024	99 %	86 %	93 %	79 %	85 %
1518	99 %	87 %	95 %	85 %	86 %

Trender

Den absolut största delen av alla installerade nätverk idag (ca 80%) utgörs av Ethernet. Detta gör att Fast Ethernet förutspås bli den dominerande teknologin för lokala nätverk inom en snar framtid, eftersom en migrering är enkel att genomföra och tekniken är välbekant. Försäljningssiffror visar också att Fast Ethernet är den snabbast växande teknologin för lokala nätverk. Fast Ethernet kommer förmodligen också att konkurrera ut FDDI som den ledande tekniken för stamnät inom medelstora företag. En annan trend, vad gäller lokala nätverk i allmänhet och Ethernet i synnerhet, är att växlade nät blir allt mer populära. Ett växlat nät ger bättre prestanda och ökad skalbarhet, men är dyrare att installera, eftersom man måste byta ut billiga hubbar och bryggor mot dyrare växlar. Växlade nät erbjuder också möjligheten att utnyttja full duplex, vilket ytterligare förbättrar prestanda.

ATM implementeras idag i stor utsträckning av telebolagen som bärare av integrerade tjänster, som telefoni, video och traditionell datakommunikation. Vissa specialiserade företag kommer säkert att utnyttja ATM även lokalt för att man har behov av att kunna transportera video och annan bandbreddskrävande realtidsdata ända ut till arbetsstationerna. Rent allmänt kommer förmodligen inte ATM att ha någon större spridning som lokalt nätverk på grund av sin relativt höga komplexitet och investeringskostnad. För företag med riktigt stora stamnät kommer ATM eventuellt utnyttjas på grund av sin goda skalbarhet och för att underlätta anslutningar till publika integrerade tjänster.

FDDI är idag en stabil teknologi som ger bra prestanda och används framförallt som stamnät i medelstora nätverk. Det verkar emellertid som att Fast Ethernet kommer att ersätta FDDI inom en snar framtid, inte därför att det är bättre, utan snarare eftersom det är en enklare teknik. I sådana situationer där Fast Ethernet inte kan utnyttjas därför att avstånden är för stora, till exempel för att koppla samman nätverk i olika byggnader (campusnätverk), kommer kanske FDDI att fortfarande ha en marknad. Man skall dock komma ihåg att dylika stamnät kan realiseras med växlade Ethernet, vilket eliminerar avståndsbegränsningen.

100VG-AnyLAN är en teknik som inte verkar växa i popularitet lika fort som Fast Ethernet. Vad detta beror på är svårt att säga. 100VG-AnyLAN har två stora fördelar

[1] Referens: Cronin, Hutchinson & Yang, "A Comparison of High Speed LANs", Proceedings of EEE 19th Conference on Local Computer Networks, Minneapolis, Oktober 1994.

jämfört med Fast Ethernet; dels kan segmenten vara avsevärt längre och dels finns två prioritetsklasser. Jämfört med FDDI är det svårt att hitta några direkta fördelar.

Virtuella LAN

Ett virtuellt LAN (VLAN) är en logisk gruppering av stationer så att de kan kommunicera som om de vore ansluta till samma lokala nät, även om de i praktiken är belägna på olika fysiska nätverkssegment. Detta gör det enklare att flytta och lägga till maskiner på det virtuella nätet, vilket gör att man undviker kostsamma administrativa ingrepp.

Motiveringar för att använda VLAN-teknik är bland annat att projektgrupper ofta formas dynamiskt, medarbetare kommer och går och man vill kunna koppla upp sig mot sitt vanliga LAN även när man inte är på sin arbetsplats. Utvecklingen av växlade nät gör att virtuella LAN kan realiseras på ett enklare sätt än annars.

Ett VLAN kan konstrueras utifrån tre grundprinciper:

- De fysiska portarna i en växel eller hub grupperas för olika VLAN. De arbetsstationer som skall tillhöra samma VLAN ansluts till samma grupp av portar. Detta är enkelt att konfigurera men mobiliteten för användarna blir begränsad.

- VLAN-grupper kan bildas utifrån datalänksadresser, d v s användare som skall tillhöra samma grupp identifieras via arbetsstationernas MAC-adress. Detta kräver mer konfiguration och administrativt arbete för att upprätthålla.

- VLAN konfigureras baserat på information i nätverksprotokollet. Till exempel kan man ha olika virtuella LAN för olika IP-subnät, eller separata VLAN för DECnet och IP-trafik. Detta gör förflyttningar av arbetsstationer enkelt. Administrationen förenklas också.

VLAN trunking

Om man använder sig av portbaserade VLAN måste man på något sätt kunna signalera mellan de olika växlarna i nätet vilket virtuellt LAN som varje paket som utväxlas tillhör. Detta kan åstadkommas med hjälp av en teknik kallad *VLAN trunking* som går ut på att man lägger till nya protokollfält i datalänkslagrets paketformat. Problemet med detta är att man härvidlag bryter mot protokollspecifikationen och gör paketen längre än vad som är tillåtet.

Nästa generations Internet

En mycket intressant fråga är hur Internet kommer att kunna anpassas till den snabba utvecklingen av nätverksteknikerna. Tekniken som bygger upp dagens Internet utvecklades till stora delar redan på 70-talet då antalet anslutna värddatorer var lågt och överföringskapaciteterna låga. De protokoll som Internet baseras på (TCP/IP) behöver modifieras för att kunna dra nytta av de nya förbättrade nätverksteknologierna. Arbetet med detta har påbörjats genom specifikationen av en ny version av IP (Internet Protocol), nämligen IP version 6 (IPv6, eller IP next generation, IPng), och förbättrade TCP-implementationer som medger större fönsterstorlekar.

IP version 6 – bakgrund

Den främsta anledningen till att IETF (Internet Engineering Task Force) har börjat arbeta med en ny version av IP (Internet Protocol) är att adresserna i IPv4 (främst klass B adresserna) börjar ta slut. Adresserna i IPv4 är 32 bitar långa, vilket teoretiskt innebär att man kan adressera 2^32 datorer, men i realiteten är adressrummet uppdelat i en hierarki för att underlätta routing, vilket betyder man får ett spill av adresser. I IPv6 har det föreslagits att adresserna skall vara 128 bitar långa, vilket beräknas vara tillräckligt för all överskådlig framtid.

I IPv6 kommer dessutom ett antal förbättringar gentemot IPv4 att realiseras, såsom ökad säkerhet, möjlighet att ha flera olika kvalitetsklasser (Quality of Service) och policybaserad routing. Grundprinciperna kommer däremot att vara de samma som i IPv4. Dessutom är det tänkt att de båda protokollen skall kunna samexistera under en obestämt lång tid, för att underlätta en stegvis övergång. Att åstadkomma en smidig migrering är ett av de främsta målen vid utvecklingen av IPv6.

Adressering

Tre typer av adresser existerar; unicast, anycast och multicast. Unicastadresser identifierar ett nätverkskort precis som vanliga IPv4-adresser. Anycastadresser är en nyhet i IPv6 och identifierar en mängd nätverkskort. Ett paket som skickas till en anycastadress kommer att levereras till endast ett nätverkskort i mängden. Multicast-adresser identifierar också en mängd nätverkskort, men på ett sådant sätt att ett paket som skickas till en multicastadress levereras till alla nätverkskort i mängden.

Adresserna i IPv6 är 128 bitar långa, vilket teoretiskt kan adressera 2^128 nätverkskort. I praktiken införs, liksom i IPv4, en hierarki för att underlätta routing. Typen på en adress ges av de första bitarna som kallas för formatprefix. En preliminär lista över dessa prefix ges i följande tabell.

Typ	Prefix	Del av adressrummet
Reserverad	0000 0000	1/256
Reserverad för NSAP	0000 001	1/128
Reserverad för IPX	0000 010	1/128
Unicastadress	010	1/8
Geografisk unicast	100	1/8
Link Local Use	1111 1110 10	1/1024
Site Local Use	1111 1110 11	1/1024
Multicast	1111 1111	1/256

Adresser med prefix som inte finns i ovanstående tabell (ca 85%) är ännu inte definierade. Anycastadresser finns inte med eftersom de i realiteten är unicastadresser använda på ett speciellt sätt.

Unicastadresser

Det finns flera olika typer av unicastadresser. Den största delen är leverantörsbaserade adresser som skall användas för global kommunikation. En dylik adress kan delas upp i följande struktur:

3 bitar	n bitar	m bitar	o bitar	p bitar	125-n-m-o-p
001	Reg. id	Leverantör id	Abonnent id	Subnet-id	Interface id

De första tre bitarna identifierar adressen som en leverantörsbunden unicastadress. De nästa n bitarna identifierar den organisation som har hand om registreringen av adresser, och som tilldelar Internetleverantörer adresser, som de i sin tur tilldelar sina abonnenter. Leverantörens identifikation ges av de nästa m bitarna. Abonnent ID används för att adressera enskilda abonnenter. Subnet och interface ID används för att identifiera lokala nätsegment respektive enskilda nätverkskort inom en organisation.

Lokala adresser

Lokala adresser (Link local, site local) är unicastadresser som bara routas lokalt. Dessa är tänkta att användas inom en organisation för enbart lokal trafik. En fördel med detta är att de kan utnyttjas av organisationer som ännu inte har kopplat upp sig mot det globala internätet. När aktuell organisation sedan beslutar att ansluta sig kan subnet id och interface id behållas och kombineras med ett nytt globalt prefix. Detta betyder att enskilda nätverkskort inom organisationen inte behöver numreras om, vilket kan spara mycket arbete.

Anycastadresser

En anycastadress identifierar som nämnts en mängd nätverkskort. Ett paket som adresseras till en anycastadress levereras till det av nätverkskorten i mängden som är närmast i något avseende. Detta är tänkt att utnyttjas tillsammans med en ny funktion för routing som finns i IPv6. I IPv6-paketens huvud finns nämligen en option som gör det möjligt att räkna upp ett antal adresser på noder som paketet skall passera på sin väg till destinationen. Genom att ange en anycastadress i denna lista kan man påverka routingen så att paketet väljer en väg över ett eller flera specifika nät, t ex det nät vars operatör man har tecknat ett avtal med. Detta kallas för policybaserad routing.

Multicastadresser

En multicastadress identifierar en mängd interface. När ett paket sänds till en dylik adress kommer det att levereras till alla nätverkskort i mängden. Multicast existerar även i IPv4 och kommer att fungera på ungefär samma sätt i IPv6.

Autokonfigurering av adresser

Det är önskvärt att en maskin som kopplas på ett nätverk automatiskt skall kunna härleda en adress, så att manuell konfigurering inte behövs. Detta kan i IPv4 åstadkommas genom Bootstap protokollet (BOOTP) eller Dynamic Host Configuration Protocol (DHCP) varigenom maskinen ifråga får sin adress från en server som hämtar den ur en databas. I IPv6 finns två mekanismer för autokonfigurering, som kallas *stateless* respektive *stateful*. I den förstnämnda varianten finns ingen server med databas att hämta adressen ur, utan adressen härleds genom att nätverkskortets MAC adress (t ex en Ethernetadress) ges ett "link-local"-formatprefix. Detta ger en adress som kan användas på det lokala nätet. För att erhålla en global adress måste "stateful" konfigurering nyttjas. Detta sker genom att ett nätverkskort skapar en global adress genom att kombinera sin MAC-adress med ett prefix som en router eller server på det .

Övergångsmekanismer

Ett av huvudmålen vid utvecklingen av IPv6 är att en migrering från IPv4 skall vara enkel att genomföra. Övergången skall kunna ske stegvis och de båda protokollen måste kunna samexistera under en period av obestämt lång tid.

För att man skall kunna utväxla IPv6-trafik mellan noder som är sammanknutna av en routingtopologi som enbart stödjer IPv4-routing har det föreslagits ett antal olika tunnlingsmekanismer. Tunnlingen bygger på att man kapslar in IPv6-paket i IPv4-paket, skickar dem över IPv4-routingstrukturen och därefter packar upp paketen igen.

Internetsäkerhet

Allteftersom nya Internetapplikationer utvecklas ställs också högre krav på att kommunikationen skall vara säker. Betalningar över nätet, banktransaktioner och distribuerade databaser med känslig information är exempel på applikationer som kräver avancerade säkerhetsmekanismer. Det bör noteras att de flesta exempel på dålig säkerhet på Internet idag (såsom obehöriga intrång) beror på dålig säkerhet inom systemen i ändpunkterna av kommunikationen, och situationen härvid kommer inte att bli bättre av att säkerhetsmekanismer införs på nätverksnivån.

Under 80-talet var dom största problemen med Internet att folk hade dåliga lösenord och delade konton med varandra. Det fanns även en hel del buggar i login och sendmail.

På 90-talet har attackerna främst gällt Internets infrastruktur. Dock förekommer det fortfarande dåliga lösenord och buggar i diverse program. Nu attackeras främst Webservrar och Mailservrar.

Typ av attack	**Resultat**
Nätverkslyssnare	Samlar lösenord och känslig information
IP spoofing	Lurar säkerhetssystem på mottagande dator att tro att det är en dator från lokala nätet som ansluter.
Connection hijacking	Används för att ta över befintliga sessioner t ex telnet
Data spoofing	Adderar information i en befintlig kommunikation mellan två datorer. På detta sätt kan man förändra program som körs över ett nätverksfilsystem.

Vanliga attacker under 90-talet.

Flera av dessa attacker förutsågs redan för mer än 10 år sedan. Ändå har inte Internet skyddats mot dem. Skälen till detta är flera. Bland andra så förutsåg inte utvecklarna att vi skulle få ett så stort problem med legitima användare som utsätter Internet för dessa attacker i lönndom. Utvecklarna såg då mer till problem med bristfälliga länkar vilket medför att Internet har en bra förmåga att hantera avbrott i länkar och hitta alternativa vägar till målet.

Att tänka på är att Internet är uppbyggt på TCP/IP vilket på många sätt fortfarande är ett experiment protokoll. Dock utvecklas det hela tiden och i IPv6 så finns det flera nya funktioner som förhoppningsvis skall lösa flera av ovanstående problemen.

IPv6 introducerar två säkerhetsmekanismer. Den första som kallas "IPv6 Authentication Headers" bygger på att pakethuvudena krypteras. Denna metod ger autenticitet och integritet, men inte konfidentialitet. Detta innebär att IP spoofing kan undvikas. Den andra mekanismen "IPv6 Encapsulating Security Header" ger konfidentialitet och integritet, vilket innebär att informationen i paketen inte kan läsas av obehöriga, eller manipuleras, dvs skydd mot data spoofing.

Säkerhetsproblem med kommunikation över Internet

Det finns två huvudproblem med att kommunicera över Internet, dels att kunna skicka information som man ej vill att någon annan skall kunna ta del av samt att kunna säkerställa källan till informationen.

Idag kan vems som helst fejka ett e-post brev. Det är lätt att förstå problemet om man tittar på detta lilla exempel.

To: Alla anställda
From: Chefen
Subject: Extra ledighet
Hej!

Eftersom vårt företag har haft ett exceptionellt bra bokslut i år så har jag bestämt att vi stänger kontoret denna vecka redan på onsdag. Ha en trevlig lång helg och kom tillbaka utvilade nästa vecka så tar vi i med nya krafter för ytterligare ett bra år.

Mvh
Anders Andersson
VD

I dagsläget kan man ej lita på ett e-post brev med detta innehåll. Det kan vara skickat av vem som helst. Det är självklart att man i en framtid måste kunna verifiera att e-post brev kommer ifrån den avsändare som anges. Detta är ett krav för att e-post skall kunna få samma funktion som vanliga brev.

Det finns några mailprogramvaror som löser detta idag men de är inte spridda i någon nämnvärd omfattning. Ett av dessa program heter Pretty God Privacy (PGP). Tekniken som den använder är en teknik som är uppbyggd på asymmetriskt kryptografi. Med denna teknik är det både möjligt att signera, kryptera e-post.

Asymmetrisk kryptografi består av två olika nycklar vilka hör ihop. Meddelanden krypterade med ena nyckeln kan packas upp med den andra och tvärtom. Denna teknik används i Public Key krypton. Här döljer man den ena nyckeln för omvärlden och det är bara användaren som känner till denna. Denna andra nyckeln läggs ut publikt så att vem som helst kan få tag i denna. Om nu jag vill skicka ett hemlig meddelande till en person vars publika nyckel jag känner så signerar jag brevet först med min hemliga nyckel och sedan krypterar jag det med hans publika nyckel. Då kan bara mottagaren läsa detta men för att kunna det måste han dekryptera brevet med sin privata nyckel det är även möjligt för honom att verifiera att brevet kommer ifrån mig med hjälp av min publika nyckel.

Digitala signaturer använder även de Publik Key kryptografi. En signatur är ett beräknat hashvärde av brevet som sedan krypteras med den hemliga nyckeln detta resultat läggs sedan till på slutet av brevet. Då kan mottagaren med hjälp av den publika nyckel verifiera att det är rätt avsändare som har skrivit brevet och att inget har förändrat innehållet.

Problemet med Publik key tekniken är spridningen av de publika nycklarna. Hur kan man avgöra att man inte har blivit lurad när man hämtade den publika nyckeln. Fick jag verkligen Anders nyckel eller var det Pers. Detta är ett av de stora problemen med denna teknik men det jobbas hårt på att hitta en struktur på Internet med certifieringsdatabaser som certifierar publika nycklar. I PGP är det upp till användaren att ange vems nycklar man litar på och därur härleda förtroende kedjor. PEM en annan programvara för mail kryptering förlitar sig på en strikt infrastruktur av certifieringsmyndigheter till skillnad mot PGPs lösa förtroendesystem där användaren själv avgör vem han skall lita på.

Ett annat problem uppstår om min privata nyckel blir stulen. Då måste jag på något sätt kunna annullera min publika nyckel så att ingen förfalskar min namnteckning. Därför bör man redan när man skapar sina nycklar skapa en annulleringsnyckel som kan skickas ut till certifieringsdatabaserna om nyckeln har stulits eller förkommit. Denna nyckel bör lagras säkert i t ex bankfacket.

Sammanfattning

Teknikutvecklingen inom datakommunikationsområdet har under de senaste åren gått mycket fort. Datornätverken har blivit mycket snabbare både vad gäller tekniker för lokala nät och långdistansförbindelser. Dessa tekniska landvinningar har gjort att nya typer av distribuerade system har börjat utvecklas, där bandbreddskraven är mycket höga. Detta gäller exempelvis applikationsområden som videokonferens, video on demand och telemedicin. I takt med att nätverken blir allt snabbare ställs också nya krav på de nätverksprotokoll som används. Arbete pågår med att modifiera TCP/IP-protokollen, som används på Internet, för att möta dessa nya krav.

Den ökade användningen av distribuerade system ställer också ökade krav på säkerhet, tillförlitlighet och tillgänglighet. Vad gäller säkerheten på Internet finns mycket kvar att göra, men det finns också en hel del programvaror tillgängliga idag för den som önskar skydda sig. Införandet av IPv6 kommer att lösa problemet med att IP-adressrummet börjar ta slut, samtidigt som det medför förbättrad säkerhet och anpassning för att stödja flera tjänsteklasser.

Vilken teknologi eller vilka protokoll som kommer att dominera morgondagens datakommunikation får framtiden utvisa. Vad som är helt klart är att framtidens distribuerade system kommer att erbjuda mycket bättre prestanda än dagens och att användningsområdena kommer att vidgas.

SISU PUBLIKATIONER

❒ 96:24	Bevakn.rapp	Datornätverk: Teknik och Trend. En rapport från Networld+Interop. *Mathias Johanson, Jan Örnstedt, SISU, Okt -96*
❒ 96:23	Dokument	Complex Concept Management and Manipulation. *William Song, SISU, Okt -96*
❒ 96:22	Rapport	ITs roll i produkt/tjänsteutveckling för bank-, försäkring- och finansföretag samt telekom-operatörer. En enkät- & intervjustudie. *L Bergman, D Rexed, S-E Öhlund, SISU, Okt -96*
❒ 96:21	Rapport	Workflow Management, State of the Art. Att effektivisera och koordinera arbete med hjälp av IT. *Jan Ljungberg, Göteborgs Universitet, Okt -96*
❒ 96:20	Rapport	Metoder för att hitta användbarhetsproblem hos datorsystem. *Per Fossum, SISU, Okt -96*
❒ 96:19	Rapport	Exploring the Potentiality of Local/Global Communication via A Case in Regional Organizing. *Klara Pihlajamäki, SISU, Sept -96*
❒ 96:18	Dokument	Cobis – ett verktyg för gemensam omvärldsinformation och kunskapsbaser. *SISU, Sept -96*
❒ 96:17	Rapport	IT för omvärldsbevakning. Översikt av produkter och tjänster. *Peter Rosengren, SISU, Sept -96*
❒ 96:16	Rapport	Införandet av ny teknologi. Ett organisatoriskt/kommunikatoriskt perspektiv på förändringsarbete. *Klara Pihlajamäki, SISU, Aug -96*
❒ 96:15	Rapport	Affärsapplikationer i 3D på Internet – VRML ny Internetstandard. *Tommy Isaksson, SISU, Aug -96*
❒ 96:14	Bevakn.rapp	Data Warehouse World 96, *Stig Berild, SISU, Aug -96*
❒ 96:13	Rapport	Yrkesanvändning av WWW i Sverige. En interaktiv enkätstudie. *M Ahlsén, A Segerberg, P O Svärd, U Wingstedt, SISU, Juni -96*
❒ 96:12	Bevakn.rapp	WWW'96 – den 5te internationella konferensen om WWW. *M Ahlsén, P Rosengren, SISU, Juni -96*
❒ 96:11	Rapport	En introduktion till Hybrid-dbms (object-relational dbms). *Stig Berild, SISU, Juni -96*
❒ 96:10	Bevakn.rapp	Produkter och lösningar. Spring Internet World 1996. *P Johansson, U Wingstedt, SISU, Maj -96*
❒ 96:09	Bevakn.rapp	Multimedia och media. Rapport från NAB'96. *M Johanson, L-Å Johansson, SISU, Maj -96*
❒ 96:08	Rapport	IT-strategisk planering – att affärsutveckla med informationsteknologi. *M Hällström, SISU, Maj -96*
❒ 96:07	Bevakn.rapp	CHI 96. En konferens om människa-datorinteraktion. *Per Olof Svärd, SISU, Maj -96*
❒ 96:06	Rapport	Gruppdatorteknik. Användningsmodeller för distansundervisning. *M Hällström, SISU, Maj -96*
❒ 96:05	Rapport	Objektorienterade databashanterare – en introduktion. *Stig Berild, SISU, Apr -96*
❒ 96:04	Dokument	Betalsystem för Internet – en överblick. *Mathias Axling, SISU, April -96*
❒ 96:03	Dokument	Systemutvecklingens roll i produktutvecklingen för bank-, försäkr- och finansföretag. *D Rexed, SISU, Feb-96*
❒ 96:02	Dokument	ESPITIs enkätundersökning i Sverige med tema "Förbättringsarbete vid programvaruutveckling".
❒ 96:01	Rapport	Prestanda för interaktiva Web-system – en arbetsmetod för test och optimering av Web-system. *Peter Johansson, SISU, Jan -96*

Publikationerna kostar 200:-/st exkl moms

Jag beställer ovanstående publikationer.

Namn .....

Företag .....

Adress .....

Tel/Fax .....

Skicka eller faxa till:

SVENSKA INSTITUTET FÖR SYSTEMUTVECKLING • SWEDISH INSTITUTE FOR SYSTEMS DEVELOPMENT

ELECTRUM 212, 164 40 KISTA • BESÖK: ISAFJORDSGATAN 26 • TEL 08-752 1600 • FAX 08-752 6800 • http://www.sisu.se • Org.nr 812000-2657

SISU