Nätverk

Inledning

Vi i datagruppen har varit på studiebesök på Ernst & Young, ett mycket stort revisionsföretag med kontor i ett flertal länder. Vi besökte kontoret i Jönköping som är beläget på Östra Storgatan mitt i centrum. Det finns 80 kontor i Sverige och sammanlagt ca 2000 användare, Jönköping har det fjärde största kontoret i Sverige. Vår kontakt är Peter Karlsson, utbildad ekonom med dataintresse och som dels arbetar med ekonomi och dels med att vara dataansvarig på kontoret i Jönköping. Vi blev varmt välkomna och fick en mycket trevlig pratstund med Peter som villigt svarade på våra frågor.

Nätets uppbyggnad och beståndsdelar

Detta nät är lite annorlunda uppbyggt än ett vanligt LAN (Local Area Network). Alla kontor skall ha kontakt med varandra och detta sker via en huvudserver i Stockholm. Alla kontor har emellertid en lokal server. Enligt vår uppfattning är nätet ett WAN (Wide Area Network) som är uppbyggt av LAN från de olika kontoren och sammankopplingen sker i Stockholm.

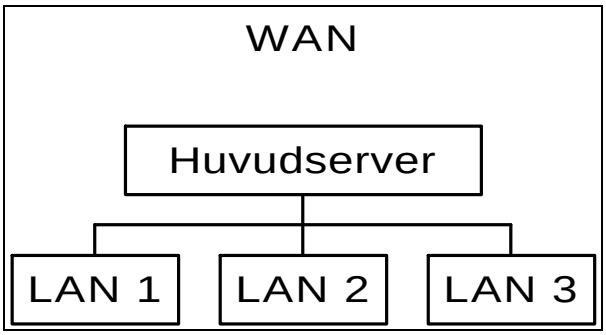

Fig. 1.1
Schematisk bild på WAN bestående av
Flera LAN

All administration av nätverket sker ifrån Stockholm, det vill säga inga användarkonton eller tilldelning av resurser sker lokalt utan via Stockholm. Även uppkoppling till Internet sker via Stockholm. Företaget i Jönköping har via Tele2 köpt in sig på en höghastighetskabel till Stockholm så de har en mycket bra uppkoppling till sin servern.
All personal som jobbar mycket ute på fältet har även en bärbar dator som de kan koppla upp till nätverket via ett 020 nummer till Stockholm för att inte belasta kunden. Det har även med säkerhet att göra.

Lokalt

I Jönköping så är det ca 50 användare och det finns en server. En Compaq P II 300 MHz med 3x8 Gb speglade diskar. Med spegling menas att om du sparar en fil så kommer servern att göra en kopia av filen (spegelbild) och lägga originalfilen på en av hårddiskarna och spegelbilden på en annanDetta är rent säkerhetsmässigt och det sköter ett program i servern. Man har valt att använda sig av serveroperativsystemet Windows NT 4.0. NT har en begränsning vid resurstilldelning. I NT så har alla användare samma resurstilldelning och det ligger på administratören att begränsa resurserna. Till skillnad från Novell där man får tilldela en användare resurser och inte ta bort resurser som i NT. Nätverkstypen är Ethernet 10Base-T och är ett stjärnnät som använder UTP kabel kategori 5 mellan 24 ports hubbarna och servern. På grund av att de använder en gammal telekabel som är dragen i väggen så nätverket har en maximal överföringshastighet på 10 Mbit/s. Det finns inga switchar eller repeaters.

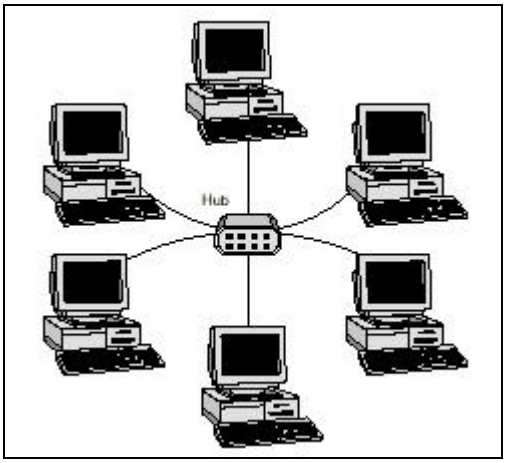

Fig.1.2
Schematisk bild av ett ringnät.

Det finns också två stycken seriekopplade 3 Com. 24 portars hubbar samt två stycken 8 portars hubbarEn av dem sköter skrivardelningen och den andra är till för att flera personer i samma arbetsrum skall kunna kopplas in. Utan hubben i skulle en användare stå utanför nätverket. Via en router kan kontoret kommunicera med andra kontor och Internet via Stockholm.

På arbetsburkarna är Windows 95 installerat och detta på grund av att de program som används kräver detta operativsystem. De ser ingen vinning på att uppgradera till NT Workstation eller ”en buggad Windows 98” eller Windows 2000 enligt Peter. På burkarna ligger också Officepaketet samt en del andra applikationer så som Lotus Notes.

Problem och kostnader

Dataansvarige har inte någon direkt administrativ roll utan fungerar som en lokal support när det händer småsaker. Det kan vara allt från kabelproblem till datorer som ”hänger” sig. Alla större problem som en kraschad server eller e-post problem sköts via Stockholm. De flest kostnaderna sköts också via Stockholm så det är svårt att uppskatta detta. Förut arbetade vår kontakt en dag i veckan med datorerna men nu har han tagit hjälp av andra arbetskamrater på kontoret.

Säkerhet

Detta är en mycket viktig hörnsten när det gäller att ha ett fungerande nätverk fungerande. Att ha ett väl uppdaterat virusprogram installerat, göra regelbundna backuper och ha en regelbunden fortbildning inom data gör det enklare att administrera ett nätverk. Många företag vill inte att viss information skall vara offentlig och då måste kryptering ske.

Ernst & Young tycker vi har en mycket väl utbyggd säkerhet när det gäller skydd av virusangrepp och dataintrång. Vid uppkoppling mot nätet sker detta via en så kallad brandvägg. Brandväggar består av en kombination av routrar, servrar och olika program. De sitter mellan den mest sårbara punkten mellan ett företags nätverk och Internet. Det finns många olika typer av brandväggar, men de flesta består av samma sorts delar. Den enklaste formen av brandvägg använder paketfiltrering, där en avläsande router undersöker sidhuvudet i varje datapaket som färdas mellan Internet och företagets nätverk. Paketets sidhuvud innehåller information om bl. a avsändarens och mottagarens IP-adresser, vilket protokoll som används och annan liknande information. Baserat på den informationen vet routern vilken typ av Internet-tjänst (T.ex. FTP) som används för att skicka data, liksom avsändarens och mottagarens identitet. Med ledning av det kan routern hindra speciella paket från att
skickas mellan Internet och det interna nätverket.

T.ex. kan routen stoppa trafik till och från misstänka destinationer. Andra vanliga komponenter i brandväggar är "bastionvärdar". De är servrar som tar hand om alla inkommande förfrågningar från Internet till företagets nätverk, T.ex. FTP-förfrågningar. Bastionvärdar är befästa motanfall. Genom att bara ha en enda dator som tar hand om inkommandeförfrågningar är det lättare att upprätthålla säkerheten och spårattacker. I händelse av intrång är det bara den enda värden som har blivit utsatt för fara, inte hela nätverket. Något annat som är vanligt i brandväggar är "proxy- servrar". När någon på insidan av ett företagsnätverk vill komma åt en server på Internet, ställs en fråga från datorn till Proxyservern, som i sin tur kontaktar en server på Internet. Sedan skickar proxy-servern informationen från Internet-servern till datorn på insidan av företagets nätverk. Genom att agera mitt emellan på detta sätt, kan Proxyservern upprätthålla säkerheten och dessutom slussa all trafik mellan Internet och nätverket."

På alla datorer finns det antivirusprogram installerade, det är Norton Antivirus 4.0. Alla disketter viruscheckas även all mejl kollas innan de tas emot och detta sker latent i bakgrunden och det är ingenting användaren kan styra över. Allt detta sker automatiskt och kontoret i Jönköping har aldrig blivit smittat datavirus. Enligt dataansvarig så klarar även antivirusprogrammet av att scanna zippade filer även om de är zippade i flera nivåer. Backuper tas varje natt på DAT band, de fungerar ungefär som ett kassettband men kan lagar mycket mer information. Ett band i månaden sparas.
De som jobbar ute på fältet har bärbara datorer och kan logga in på servern i Stockholm när de är ute på företagen och arbetar, de kopplar upp sig via ett 020 nummer. Även här har företaget ett väl utarbetat säkerhetstänkande. När användaren kopplar upp sig mot Stockholm så måste de ange ett användarnamn som innehåller bokstäver och siffror. I varje laptop så krävs det ett Secure reader card, det är ett kort som man sätter in i datorn och när man skall logga in på servern i Stockholm ger kortet ett sexsiffrigt nummer som kommer fram på skärmen. Detta nummer får användaren knappa in som ett slags lösen, numret byts var 30: e sekund. Det har aldrig varit några problem med detta.