

Maria Kihl

Datakommunikation

En inledande översikt

7 Från användare till användare

Fram till nu har vi diskuterat nätarkitekturer, det vill säga hur kommunikationsnät måste vara uppbyggda för att kunna transportera data från en sändare till en mottagare. Men vid varje värddator sitter det en människa som använder sig av någon tjänst eller applikation. Denna användare kanske använder nätet för att ringa eller för att surfa på Internet. I vilket fall ställer användaren vissa krav på kvalitén på den tjänsten som han eller hon utnyttjar och i de flesta fall betalar för.

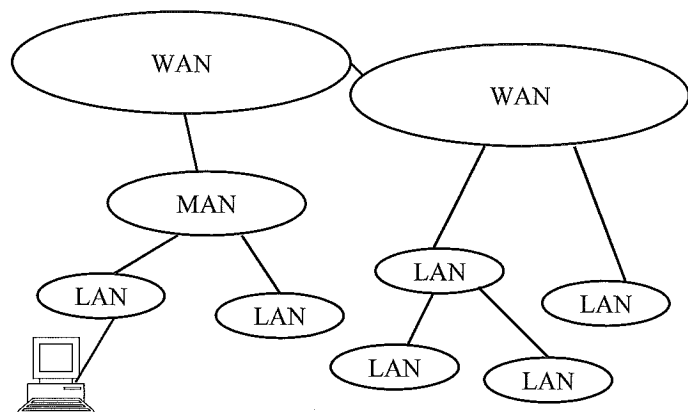
I detta kapitlet kommer vi att beskriva de grundläggande nätfunktioner som krävs för paketförmiddad datorkommunikation mellan två användare, så kallad *end-to-end communication*. Hur telefoni går till beskrivs i Kapitel 12.

7.1 Kommunikation över flera nät

I fortsättningen kommer vi inte längre att diskutera kommunikation över bara ett nät, utan istället över flera sammankopplade nät, se Figur 7.1. Man brukar prata om två typer av nät, *accessnät* och *ryggradsnät* (backbone network). Alla värddatorer är anslutna till ett accessnät, ofta ett LAN. LAN:et är sedan i sin tur anslutet till ett ryggradsnät, som i sin tur kan vara accessnät till ett annat ryggradsnät. Accessnäten är för det mesta privatägda. De flesta länder har stora ryggradsnät som binder samman olika accessnät i landet. Dessa ryggradsnät är oftast statligt ägda.

Adressering

Inom ett nät kan varje dator ha en unik adress som lagras i alla vägväljare i nätet. Ett exempel på sådana adresser är MAC-adressen som används i alla lokala nät som är standardiserade enligt IEEE 802. Men eftersom denna adress inte säger något om till vilket nät datorn är ansluten går det inte att använda MAC-adressen för att hitta en dator i ett annat nät. För att kunna



Figur 7.1 Sammankopplade nät. LAN = Local Area Network, MAN = Metropolitan Area Network, WAN = Wide Area Network.

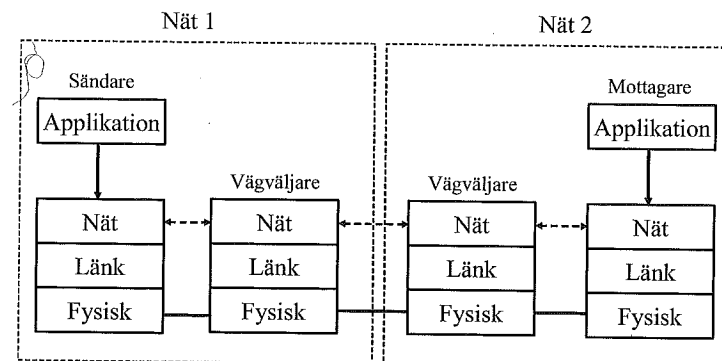
hitta en dator i ett annat nät behövs det därför ytterligare en adress, en nätadress. Vilken nätadress en dator har beror på var i världen datorn finns, precis som den vanliga postadressen.

Nätprotokoll

För att olika nät skall kunna samarbeta och se till att data transporteras från ett nät till ett annat, krävs det att de har ett gemensamt protokoll. Detta protokoll kallas för nätprotokoll. Nätprotokollets huvusakliga uppgift är att hålla reda på adresseringen och att i vägväljarna bestämma nästa nät för ett paket. Alla noder i näten måste använda samma nätprotokoll. Figur 7.2 visar två värddatorer som finns i olika nät. Nätprotokollet används för att kommunikationen skall fungera mellan de två näten. Ett exempel på ett nätprotokoll är Internet protocol (IP) som används i Internet. IP beskrivs i Kapitel 8.

Transportprotokoll

När du som användare sitter vid din dator och skall utbyta information med en annan dator någonstans i världen, vill du inte behöva bry dig om vilket nät du använder. Detsamma gäller för applikationen som du använder. Man kan se det som om två datorer kommunicerar via ett "moln" och



Figur 7.2 Två värddatorer i olika nät.

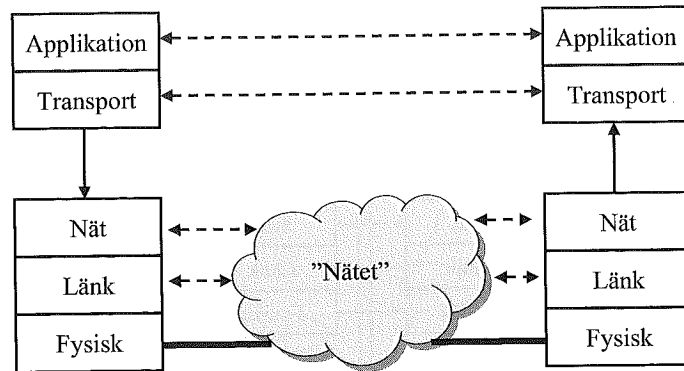
där ingen av datorerna skall behöva veta vad molnet egentligen består av, se Figur 7.3.

För att detta skall fungera behövs det ett protokoll i varje dator, som ser till att informationen som kommer från en applikation kan skickas över nätet utan att applikationen skall behöva veta hur nätet är uppbyggt. Protokollet kallas för ett *transportprotokoll* och är ett så kallat *end-to-end protocol*, vilket innebär att protokollhanterarna i de två värddatorerna kommunicerar direkt med varandra över hela nätet, se Figur 7.4. Två exempel på transportprotokoll är Transmission Control Protocol (TCP) och User Datagram Protocol (UDP) som används i Internet. TCP och UDP finns beskrivna i kapitel 8.

Transportprotokollet ser alltså till att kommunikationen mellan två applikationer fungerar. För att inkommande data skall nå rätt applikation används en så kallad *portadress*. Med hjälp av portadresserna kan en dator ha flera applikationer igång samtidigt. De flesta applikationer har en så kallad standardport. När en applikation vill starta en dialog skickar den ett



Figur 7.3 Ett kommunikationsnät från användarens perspektiv.



Figur 7.4 Funktionen hos ett transportprotokoll.

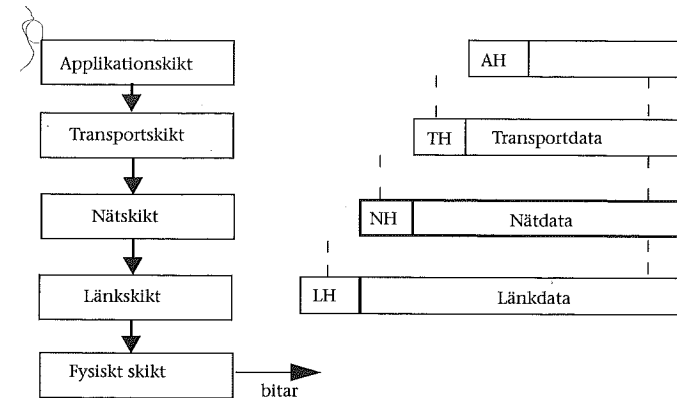
meddelande till mottagarapplikationens standardport. Sändar- och mottagarapplikationerna kan sedan komma överens om att fortsätta dialogen på en annan port så att standardporten lämnas fri igen.

7.2 Databehandling i flera protokollskikt

I Figur 7.4 ser man att det behövs flera protokoll för att två datorer skall kunna kommunicera med varandra. Man har valt att göra så här för att göra näten mer flexibla och för att göra det enklare att utveckla nya applikationer till näten. Eftersom kommunikationer sker i flera steg, så kallade skikt (layers) behöver ett skikt inte veta vad som pågår i ett annat skikt. Man har istället utarbetat gränssnitt mellan skikten så att ett skikt utför tjänster åt skiktet ovanför.

Figur 7.5 visar vad som händer med datapaketet i varje protokollskikt. Varje skikt behandlar paketet från föregående skikt som ren data och lägger därför till sitt eget pakethuvud. När ett inkommande paket behandlas i ett protokollskikt i mottagaren tas headern bort och resten av paketet skickas till nästa protokollskikt.

Om det kommer mer information från ett protokollskikt än vad nästa skikt kan överföra i ett enda paket sker så kallad segmentering (segmentation). Segmentering innebär att datapaketet från ett skikt delas i två eller flera delar i nästa skikt. Varje del får en egen header och behandlas sedan som en egen så kallad Protocol Data Unit (PDU).

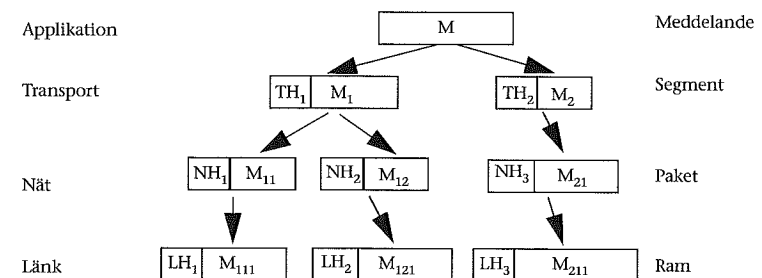


AH=Applikationsheader TH=Transportheader NH=Nätheader LH=Länkheader

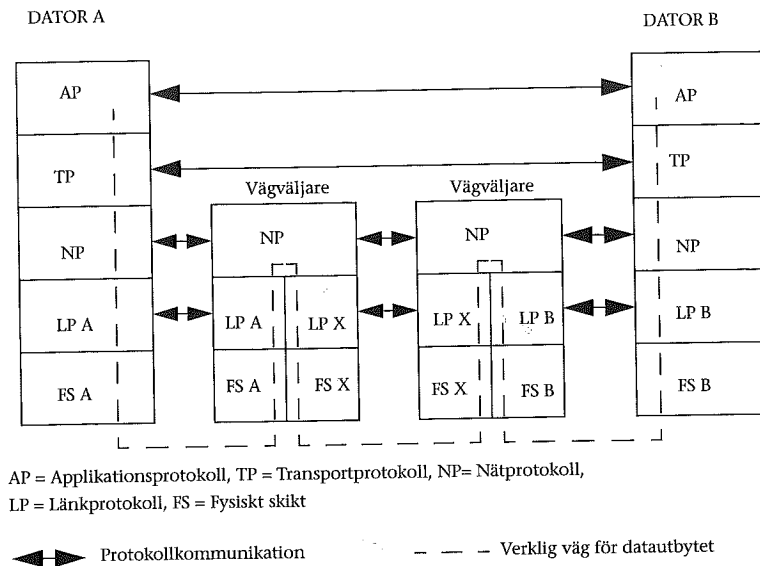
Figur 7.5 Protokoll i flera skikt.

Antag att en applikation skall skicka meddelandet M till en annan dator. Figur 7.6 visar vad som kan hända med meddelandet i de olika skikten. I figuren finns också de namn som brukar användas för en PDU i de olika skikten.

I Transportskiktet delas meddelandet upp i två så kallade *segment* och varje segment får sin egen header (TH). De två segmenten lämnas sedan över till nätskiktet. I nätskiktet behandlas de som ren data, dvs. även headern i varje segment ses som data. Det visar sig att segment 1 måste delas upp i två mindre *paket* eller datagram som får varsin header (NH). Segment 2 behöver inte delas upp ytterligare. Paketet skickas sedan över till länkskiktet. I länkskiktet behöver inget av paketet delas upp ytterligare. En länkheader (LH) läggs till varje paket som nu bildar tre *ramar* som skall skickas ut på länken.



Figur 7.6 Segmentering.



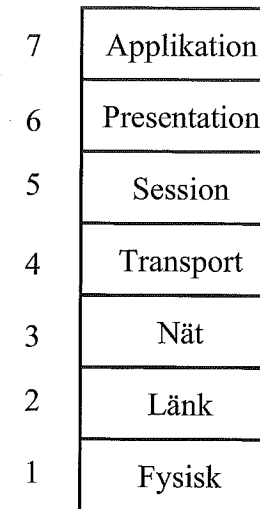
Figur 7.7 Datakommunikation över flera nät.

I mottagaren sker så kallad ihopsättning (reassembly) för att foga samman uppdelade PDU:er igen. Varje skikt tar bort sin header, fogar samman de PDU:er som är uppdelade och lämnar sedan över de färdiga paketen till nästa skikt.

Figur 7.7 visar hur olika protokoll samverkar för att möjliggöra datorkommunikation över olika nät. Genom att använda sig av flera protokollskikt där varje skikt har sina bestämda funktioner behöver en applikation inte veta vilka nät den kommunicerar över. Applikationsprotokollet skall inte behöva veta om informationen den söker finns på samma dator och eller på en dator någon annanstans.

7.3 OSI-modellen

I mitten på 70-talet insåg datorvärlden att det krävdes en gemensam standard så att olika datorer skulle kunna kommunicera med varandra oberoende av tillverkare eller operatör. Därför började International Organization for Standardization (ISO) sitt arbete med att utveckla en gemensam arkitektur. 1983 presenterades Open Systems Interconnection (OSI) Refe-



Figur 7.8 OSI-modellens 7 nivåer.

rence Model som ett resultat av detta arbete. OSI-modellen var ett ramverk för kunna definiera standarder för att möjliggöra kommunikation mellan olika datorer och datanät.

OSI-modellen bygger på en protokollstack med 7 skikt (layers) eller nivåer, se Figur 7.8. Varje nivå har ett eller flera standardiserade protokoll. Tyvärr fick inte OSI-modellen något större genomslag som standard. Idag används istället OSI-modellen som en referensmodell, det vill säga som ett sätt att förklara hur kommunikationsnät bör vara uppbyggda. En kortfattad beskrivning av varje skikt finns nedan.

Fysiska skiktet (OSI-nivå 1)

Det fysiska skiktet är ansvarigt för att sända en bitström över ett transmissionsmedium. Det innehåller till exempel regler för hur ett or och nollor skall representeras när de skickas över länken. Det ser också till att överföringshastigheten blir korrekt samt att sändare och mottagare är synkroniserade.

Länkskiktet (OSI-nivå 2)

Länkskiktet är ansvarigt för att dataöverföringen mellan två intilliggande noder blir tillförlitlig. Det innehåller regler för hur data skall paketeras i ramar så att mottagaren skall kunna veta betydelsen av de mottagna bitarna. För att dataöverföringen skall bli tillförlitlig finns det funktioner för flödeskontroll och felhantering. Om flera noder delar på samma länk måste varje nod ha en fysisk adress, så att skickad data kommer fram till rätt mottagare. Dessutom måste det finnas funktioner för att kontrollera tillgången till länken.

Nätskiktet (OSI-nivå 3)

Nätskiktet är ansvarigt för transporten av data över ett eller flera nät. Det innehåller därför regler för adressering så att ett paket kan komma fram till rätt mottagare oavsett till vilket nät mottagaren är ansluten. Det finns också funktioner för att hitta en lämplig väg genom nätet.

Transportskiktet (OSI-nivå 4)

Transportskiktet är ansvarigt för att applikationsdata kommer fram korrekt och i rätt ordning till mottagaren. Därför finns det till exempel funktioner för flödeskontroll och felhantering. Det finns också funktioner för att dela upp applikationsdata i segment som sedan kan skickas var för sig genom nätet. Segmenten skall sedan sättas ihop i rätt ordning hos mottagaren. Om ett förbindelseorienterat transportprotokoll används, finns det funktioner för att sätta upp, underhålla samt stänga ner en förbindelse. Det finns också en adresseringsfunktion så att data kommer fram till rätt applikation hos mottagaren. Detta för att mottagaren skall kunna ha flera applikationer igång samtidigt.

Sessionsskiktet (OSI-nivå 5)

Sessionsskiktet används då två datorer är involverade i en dialog som kräver till exempel synkronisering. Därför finns det regler för hur dialoger sätts upp, underhålls samt synkroniseras. Det finns funktioner för hur dialogen går till, till exempel om båda datorer skall kunna sända samtidigt eller om de måste turas om.

Presentationsskiktet (OSI-nivå 6)

Presentationsskiktet är ansvarigt för att informationen från sändarapplikationen omvandlas till binärdata som mottagaren kan förstå. Därför finns det regler för hur informationen skall kodas. Det finns också funktioner för komprimering av data samt för kryptering.

Applikationsskiktet (OSI-nivå 7)

Applikationsskiktet ser till att användaren, som i detta fallet kan vara både en människa eller programvara, kan komma åt nätet. Det innehåller användargränssnitt och tillhandahåller tjänster som elektronisk post, filöverföring, databashantering och andra typer av distribuerade informationstjänster.

7.4 Vägvaljare

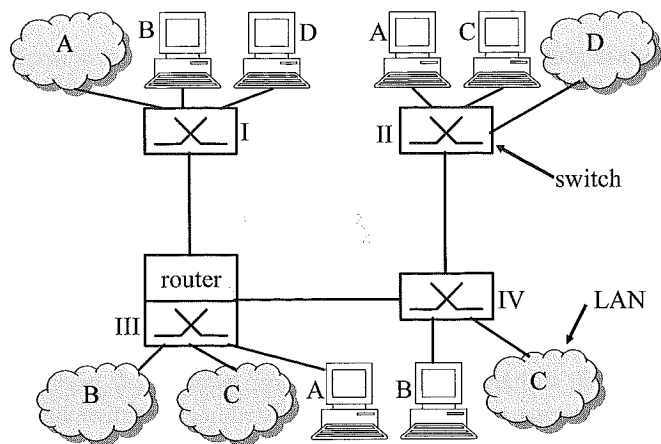
Vägvaljarna finns både inne i näten samt mellan näten. Vägvaljarna kan arbeta på olika OSI-nivåer och olika termer brukar användas för en vägvaljare beroende på vilken OSI-nivå vägvaljaren arbetar. En förklaring av de olika termerna finns nedan.

Switch

I denna boken används termen switch för en vägvaljare som arbetar på OSI-nivå 2. Termen switch är annars ett allmänt begrepp som egentligen behöver ett prefix för att specificera vad som avses, till exempel Ethernet-switch, ATM-switch, eller Frame Relay-switch. I Ethernet-sammanhang avses med switch en brygga med flera portar, underförstått för partvinnad kabel.

Router

En router är en vägvaljare som kopplar samman flera nätverkssegment eller nät vilka sinsemellan kan vara olika och arbeta enligt olika protokoll på OSI-nivå 1 och 2. Routern arbetar på OSI-nivå 3. Den utgör en gräns för



Figur 7.9 Nätstruktur, OSI-nivå 1.

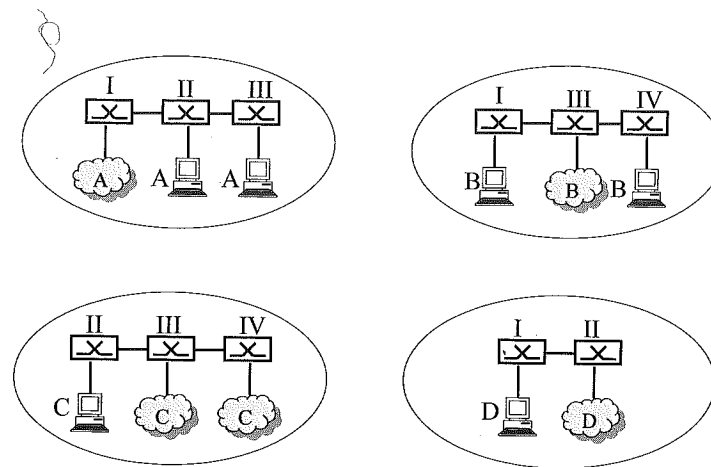
broadcastdomäner på OSI-nivå 2 (notera att det kan finnas broadcast även på OSI-nivå 3).

Gateway

En gateway används för att koppla samman nät på OSI-nivå 4 och högre. Den är en översättare mellan olika protokoll och applikationer. Tidigare användes begreppet gateway även för en router.

7.5 Nätstruktur på olika OSI-nivåer

Ett stort datanät består ju som sagt av ett antal fysiska länkar som utgör OSI-nivå 1. Men över dessa fysiska länkar sätts ett antal logiska länkar upp, som sedan utgör länknivån eller OSI-nivå 2. Detta innebär att nätet ser olika ut beroende på vilken nivå man tittar på. Detta fenomen förklaras enklast med ett exempel.



Figur 7.10 Nätstruktur, OSI-nivå 2.

OSI-nivå 1

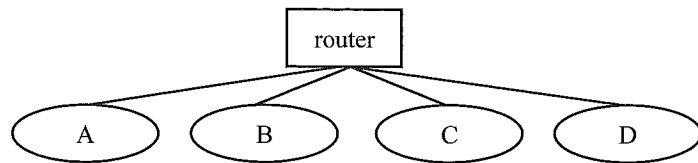
Antag att vi har ett nät som består av fyra switchar (I-IV), ett antal LAN, och ett antal värddatorer som alla är sammankopplade på OSI-nivå 1 enligt Figur 7.9. Som bilden visar innehåller en av switcharna även en router.

OSI-nivå 2

Nätet använder någon multiplexeringsteknik för att dela på länkarnas kapacitet i olika logiska kanaler, till exempel tidsmultiplexering eller genom att varje logisk kanal får ett fiberpar (förutsatt att optiska fibrer används).

Switcharna använder Virtual LAN-tekniken (VLAN). Varje fysisk switch delas upp i virtuella switchar, en virtuell switch för varje logisk kanal på länkarna. En switchs uppgift är att ta emot dataramar på sina ingångar och vidareförmedla dataramarna till rätt utgång beroende på ramens destinationsadress (MAC-adressen). Switchen behöver för detta dataingångar och datautgångar, minnesbuffertar, adresstabeller med mera. Genom att dela upp switchens resurser på ett sådant sätt att varje del fungerar som en enskild switch, har vi skapat virtuella switchar i den fysiska switchen.

Varje virtuell switch tilldelas några av den fysiska switchens in- och utgångar. Likaså tilldelas varje virtuell switch en av kanalerna på de multiplexerade länkarna. Trafikflödet igenom varje virtuell switch flyter helt oberoende av de övriga virtuella switcharna i den fysiska switchen. I vårt



Figur 7.11 Nätstruktur, OSI-nivå 3.

fall kommer nätet att på OSI-nivå 2 bestå av fyra separata nät av sammankopplade LAN och datorer (se Figur 7.10). Notera att det inte finns, och inte får finnas, någon förbindelse mellan de fyra delnäten på denna nivå.

OSI-nivå 3

Routern kopplar samman de fyra näten. Om näten har ett gemensamt nätprotokoll är samtrafik mellan näten möjlig. Figur 7.11 visar hur nätet ser ut på OSI-nivå 3.

8 Internet

Internet är ett globalt datanät med användare över hela världen. Datorer kopplade till Internet kommunicerar med hjälp av ett antal standardiserade Internetprotokoll. I detta kapitlet beskrivs hur Internet är uppbyggt.

8.1 Internets struktur

Den första frågan som kan ställas är om Internet finns eller inte. Om vi med "finns" menar att det existerar ett nät, som leds, drivs och underhålls av en organisation så finns inte Internet. Visserligen finns det en organisation som kan sägas styra över Internet i någon mening. Den heter Internet Society (förkortas ISOC), som under sig har IETF (Internet Engineering Task Force), IAB (Internet Architecture Board) med flera undergrupper, men ISOC har inget eget nät att driva och påverkar ej heller hur trafik skall flöda i Internet.

Internet utgörs istället av ett flertal sammankopplade fristående nät, allt från stora nät med global täckning till en liten organisations lokala nät. Längst ut i näten finns värddatorerna (hosts). Näten har alla det gemensamt att de använder protokollsviten TCP/IP för transporten av data. Även om det inte finns någon huvudorganisation för driften av Internet så kan man ändå se en viss hierarki. Globala Internet Service Providers (ISP) levererar det som kallas Internetaccess till nationella eller regionala ISP. Dessa i sin tur levererar Internetaccess till företag och organisationer med lokala nät och till allmänhetens enskilda datorer. Tillsammans utgör alla dessa nät Internet.

Nätstrukturer

Nät delas ofta upp i accessnät och ryggradsnät (backbone network). Även globala eller nationella ISP:ers nät delas upp i accessnät och ryggradsnät.

Det krävs oftast olika utrustning och fysisk uppbyggnad för accessnäten och ryggradsnäten, liksom det krävs olika teknik i ett företags nät och en ISP:s nät. Till företagets accessnät ansluts enskilda datorer, till en ISP:s accessnät ansluts kundernas ryggradsnät.

Det lilla nätets uppbyggnad med bara några få datorer anslutna skiljer sig naturligtvis från det stora med flera 10.000-tals datorer. Det lilla nätet kan i sin enklaste form bestå enbart av en Ethernet-switch. Företagets datorer ansluter till switchen. Till en av switchens portar ansluter man den så kallade upplänken (uplink) det vill säga anslutningen till företagets ISP. ISP:n i sin tur ansluter det lilla nätet till en så kallad accessrouter.

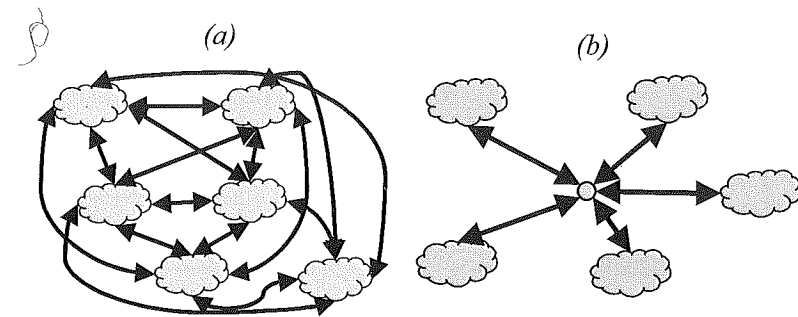
Det stora nätet däremot innehåller en blandning av switchar och routrar med länkar mellan dessa. Det finns ofta en hierarkisk struktur med många accessnät dit datorerna ansluts, och med ett eller flera ryggradsnät och flera upplänkar till en eller flera ISP:er. Medan det lilla nätets struktur på OSI-nivå 1 avspeglar sig tydligt på OSI-nivå 2 och 3, ser det stora nätets struktur ofta mycket olika ut på de olika OSI-nivåerna.

Trafikutbyte mellan nät

Trafikutbytet mellan näten som utgör Internet styrs av bilaterala avtal. Detta innebär att om två organisationer med var sitt nät önskar utbyta datatrafik med varandra så avtalar man om att så skall ske och vilka förutsättningar som gäller för trafikutbytet. Sedan kopplar man ihop de två näten på något sätt. Men trafikutbyte som bygger på principen att alla nät har direktkontakt med alla andra kan inte växa av praktiska skäl, se Figur 8.1a. Modellen, som kallas "full mesh", går inte att skala upp.

Därför har flera olika sätt att komma ifrån "full mesh" tagits fram. De flesta ISP:er har till exempel avtal om så kallad transittrafik. Detta innebär att de tillåter att trafik mellan två nät som inte har direktkontakt kan få passera genom denna ISP:s nät.

Ett annat exempel är de knutpunkter (Internet Exchange, IX) som skapats. I knutpunkterna kan flera nät mötas och utbyta datatrafik med varandra, se Figur 8.1b. En knutpunkt utgörs av ett lokalt nät. Den kan i sin enklaste form utgöras av till exempel en Ethernet-switch. Knutpunkten ägs och drivs visserligen av en organisation eller ett företag men ingår inte i någon organisations nät, inte ens ägarens. Den är alltså helt neutral i förhållande till alla nät som utbyter trafik där, en så kallad "demilitariserad zon" (DMZ). De organisationer som önskar utbyta trafik med varandra "möts" på detta



Figur 8.1 (a) Full mesh; (b) Knutpunkt.

neutrala nät. Knutpunkter finns på olika geografisk nivåer: globala, nationella, regionala och lokala.

8.2 Internetprotokollen

De protokoll som får användas på Internet standardiseras av en organisation som heter Internet Engineering Task Force (IETF). Alla deras rekommendationer, så kallade Request For Comment (RFC), finns tillgängliga för alla. Detta gör att nya protokoll och applikationer snabbt kan spridas och börja användas. Internetprotokollen består av tre skikt: nät, transport och applikation, se Figur 8.2.

På nätnivån finns först Internet Protocol (IP). Det finns två versioner av IP, version 4 och 6. Version 5 slopades innan den hann bli en standard, eftersom man insåg att den inte var bra nog. Sändare, mottagare och samtliga routrar på vägen måste använda samma IP-version. I fortsättningen kommer vi att beskriva de funktioner och protokoll som tillhör IP version 4 (IPv4).

På transportnivån finns två protokoll: Transport Control Protocol (TCP) och User Datagram Protocol (UDP). På applikationsnivån finns en mängd olika protokoll som alla används av olika applikationer. Några exempel på Internetapplikationer är World Wide Web, elektronisk post och filöverföring. Dess applikationer använder sig till exempel av följande protokoll: Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) och File Transfer Protocol (FTP).