IP-baserade kommunikationsprotokoll

kirei

IP-baserade kommunikationsprotokoll

Detta verk är licensierat under en Creative Commons
Erkännande-Ickekommersiell-IngaBearbetningar 3.0 Unported Licens.
http://creativecommons.org/licenses/by-nc-nd/3.0/deed.sv

© 2013 Kirei AB

F. Ljunggren, J. Schlyter, J. Strömbergson

Innehåll

Del 1

Översikt

1 Introduktion

På senare tid har det skett en stark konvergens mot IP-baserade kommunikationsnät inom alla sektorer i samhället. Standardiseringen på IP-teknik har fört med sig kostnadseffektiva lösningar med god interoperabilitet, men också att de IP-baserade kommunikationsnäten ska kunna bära en lång rad kommunikationstjänster med vitt skilda kapacitetsbehov och kvalitetskrav.

Internetprotokollet *Internet Protocol* (IP) är i grunden en paketförmedlad teknik som utgår från vad som kallas "bästa förmåga", det vill säga att IP-tekniken i sig själv inte garanterar en viss tjänstekvalitet. Olika tillämpningar som används i samma IP-nät konkurrerar om de tillgängliga resurserna, och kan på så sätt påverka varandras tjänstekvalitet på ett sätt som är svårt att förutse och styra.

Tillämpningars tjänstekvalitet påverkas även genom anslutningsformernas skiftande egenskaper. En IP-anslutning med en given dataöverföringskapacitet är ingen garant för en väl fungerande tjänst. Vid kravställning av tillämpningar måste hänsyn tas till anslutningarnas alla kvalitetsegenskaper för att kunna säkerställa att tillämpningen kommer fungera tillfredsställande.

Handledningens syfte

Denna publikation syftar till att ge vägledning vid utformning, kravställning och val av IP-baserade kommunikationstillämpningar genom att belysa de tydligaste samband som föreligger mellan olika IP-baserade anslutningsformers egenskaper och olika tillämpningars kommunikationsbehov, samt den tjänstekvalitet som kan förväntas till följd av detta.

Handledningens struktur

Handledningen består av två delar. Första delen ger en översiktlig beskrivning av olika typanslutningar och hur deras egenskaper påverkar olika tillämpningar, och visar på hur val av tillämpning kan få konsekvenser i användbarhet beroende på vilken typ av anslutning som används. Beskrivningen syftar till att ge stöd vid kravställning och val av tillämpningar och kommunikationstjänster, och visar på hur tjänsteupplevelsen kan förbättras givet olika förutsättningar.

Andra delen är en fördjupningsdel avsedd att i mer detalj belysa varför typanslutningarnas egenskaper påverkar tjänstekvaliteten. Denna del innehåller även en exempelkatalog över olika typer av transportmekanismer och tillämpningar, beskrivna utifrån de egenskaper de besitter, vilka kvalitetskrav som ställs, och den

störningskänslighet som kan förväntas följa vid den händelse att kvalitetskraven inte uppfylls.

Målgrupp

Översiktsdelen vänder sig till personer i kravställande och beslutsfattande positioner med ansvar för införande av kommunikationstjänster och tillämpningar. Läsare förväntas vara bevandrade inom informatik samt förtrogna med termer och begrepp som rör telekommunikation.

Fördjupningsdelen riktar sig i första hand till personal som bär ansvar för den direkta utformningen av informationssystem och telekommunikationsnät.

1.1 Ansatser

Utgångspunkten för den modell som presenteras här är en förenklad lagerstruktur i tre nivåer; anslutning, nätverksnivå (IP) och tillämpning.

Den kvalitet en anslutning erbjuder genom länklager och andra eventuellt mellanliggande lager summeras ihop till ett antal parametrar som kan observeras och mätas:

- dataöverföringskapacitet,
- fördröjning,
- jitter/varians,
- paketförluster,
- begränsningar i paketstorlek och
- intermittens.

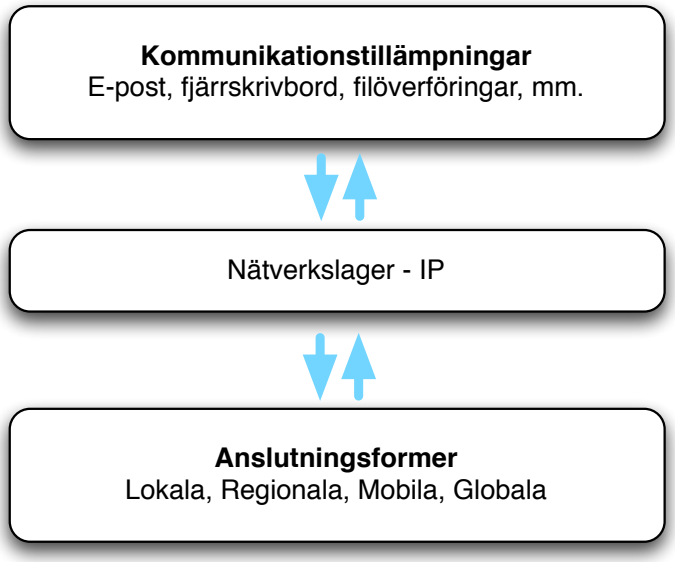
Ovanpå nätverkslagret analyseras de krav olika tillämpningar (inklusive deras transportmekanismer) ställer på anslutningars kvalitet. Anslutningarnas egenskaper och tillämpningarnas krav projiceras sedan på varandra för att skapa en kvalitetsmatris för ett antal olika typfall.

1.2 Begränsningar

Analysen utgår från att själva anslutningen i grunden är tillståndslös och levererar paketen efter bästa förmåga (*"best effort"*). Det antas vidare att det är tillämpningen och dess transportprotokoll som ansvarar för att hålla en kommunikationsanslutnings tillstånd.

För mer komplexa anslutningsformer eller transportmekanismer stämmer kanske inte antagandet om en tillståndslös anslutning fullt ut, t.ex. vid användning av:

- Tunnelmekanismer; IPsec, L2TP, MEF är exempel på vanliga tunnelmekanismer som etablerar ett tillstånd för kommunikationen.



Figur 1.1 – Lagerstruktur i tre nivåer

- Kodningar – kryptering, felkorrigering, komprimering.

Flera av dessa tekniker kan påverka tjänstekvaliteten högst avsevärt, och beskrivs närmare i fördjupningsdelen (del 2).

2 Anslutningars egenskaper

Anslutningar antas erbjuda funktionaliteten att flytta enskilda datapaket mellan två parter, i båda riktningarna. Anslutningarna består av en eller flera länkar över vilken paketen transporteras. Gemensamt för alla typer av anslutningar är att de karaktäriseras genom ett antal egenskaper:

- Dataöverföringskapacitet. Mängden data i bitar per tidsenhet (*bitar per sekund, bps*) som en anslutning kan överföra. Benämns även genomströmningskapacitet (*throughput*) eller bithastighet (*bitrate*).

  Ibland används ordet bandbredd (ofta felaktigt) som benämning för dataöverföringskapacitet. Med ordet bandbredd avses skillnaden mellan den övre och den lägre avbrytande frekvensen i det spann av frekvenser som används för en informationsöverföring i radiokommunikation eller i en kabel. Det kan emellertid vara stor skillnad på den teoretiska bandbreddskapaciteten och den verkliga/effektiva dataöverföringskapaciteten.

- Fördröjning. Tiden det tar att överföra en bit från en part till dess motpart över en anslutning. Kallas även för latens. Tiden inkluderar både den fysiska transporten genom kommunikationsmediat (radiovågor, ljus, elektrisk signal) och processtiden i utrustning (switchar, routers, mediakonverterare etc.).

  I praktiska tillämpningar påförs även fördröjningseffekter genom den tid som åtgår för serialisering och deserialisering av de datastrukturer som överförs. Det innebär att även dataöverföringskapaciteten är en parameter vid beräkning av den totala fördröjningen mellan de kommunicerande parterna.

  Svarstid är ett annat mått på fördröjning, som anger den minimala tid det tar att skicka ett IP-paket till en motpart och erhålla ett svar.

- Jitter. Den varians i fördröjning som en anslutning uppvisar över tid. Jitter är alltså inget som mäts eller anges för ett enskilt paket. Jitter påverkar applikationer med realtidskrav där data måste komma fram vid en viss tidpunkt för att vara användbar. Jitter kan även vara mer eller mindre skurigt, vilket innebär att mängden jitter i sig varierar över tiden med i normalfallet lågt jitter och perioder med stort jitter.

- Paketförluster. Mängden paket över en anslutning som förloras eller får så mycket fel att felkorrigeringsmekanismer hos mottagaren inte kan rekonstruera paketet. Beroende på typ av transport och tjänst som används kan paketförluster innebära omsändningar av paket, vilket i sin tur kan leda till att tjänsten får en lägre effektiv utnyttjandegrad av tillgänglig dataöverföringskapacitet.

- Minimal respektive maximal storlek på ett enskilt paket. För IP version fyra anges en minsta gräns av 576 oktetter. Den maximala paketstorleken över kommunikationslänkarna är vanligen 1 500 oktetter, men kan i vissa fall vara upp mot 9 000 oktetter. Mindre paketstorlek innebär större andel överskottsdata, medan större paket ökar risken för paketförluster genom överföringsfel.

- Intermittens. Ett mått på en anslutnings tillgänglighet över tiden, det vill säga hur ofta kommunikationen bryts och för hur länge. En anslutning där bortfallen är frekventa men korta, kan för vissa tillämpningar fungera väl, medan beteendet för andra tillämpningar kan tvinga fram omstarter så till den grad att tjänsten blir obrukbar.

För att kunna åstadkomma en bedömningmodell för tillämpningars kvalitetskrav inrättas en taxonomi av fyra typanslutningar, där en enskild nätverksanslutning anses falla inom ramen för den aktuella klassen endast om samtliga kvalitetskrav som ställts upp är uppfyllda.Genom denna indelning kan man på ett tidigt stadium skapa en översiktlig bild av i vilken mån en viss tillämpning kan tänkas fungera väl i ett visst sammanhang, eller om risk för kvalitetsproblem föreligger i det givna användningsfallet.

De fyra typanslutningarna som definieras är; *höghastighetsförbindelser*, *fjärrförbindelser*, *lågkapacitetsförbindelser* och *satellitförbindelser*.

2.1 De fyra typanslutningarna

2.1.1 Höghastighetsförbindelser

En höghastighetsförbindelse karaktäriseras av hög dataöverföringskapacitet, kort fördröjning och lågt jitter. Höghastighetsförbindelser har mycket få paketförluster och en hög tillgänglighet. Att etablera en logisk anslutning över en höghastighetsförbindelse tar som regel kort tid, och tjänstekvaliteten hos anslutningen motsvarar det som förekommer i stadsnät, områdesnät och lokala nätverk, *Local Area Network* (LAN), men kan även i vissa fall sträcka sig över längre avstånd.

Höghastighetsförbindelserna, som typiskt realiseras över elektriskt lokalnät eller optisk fiber, håller en god kvalitet där jitter, fördröjning och paketförluster kan förekomma främst som en följd av hög belastning. Dataöverföringskapaciteten varierar från 10 Mbps upp till 40 Gbps, och fördröjning från mindre än 1 ms upp till cirka 10 ms.

Vanligen används Ethernet som länklager i höghastighetsförbindelser. Däremot kan det skilja i underliggande bärare. För mer komplexa nätstrukturer som sträcker sig över större geografiska avstånd är det ofta fråga om tekniker som *Packet over SONET/SDH* (POS), *Metro Ethernet* eller *Multi Protocol Label Switching* (MPLS) som används.

IP fungerar mycket väl över denna typen av länkar. IP-stacken i dagens operativsystem är som regel optimerad efter de förhållandena som Ethernet med hög kapacitet och kort fördröjning erbjuder.

Höghastighetsförbindelser definieras genom följande egenskaper:

- Dataöverföringskapacitet: från 10 Mbps.
- Maximal paketstorlek från 1 500 oktetter, men kan t.ex. i lokalnät vara upp mot 9 000 oktetter.
- Svarstider: upp till cirka 10 ms.
- Jitter: Lågt. Ökande med avståndet, särkilt då kapacitetsutnyttjandet närmar sig sin maximala gräns.
- Mycket låga eller i normalfallet inga paketförluster.
- Mycket hög tillgänglighet.

2.1.2 Fjärrförbindelser

Fjärrförbindelser kännetecknas av att ha något lägre dataöverförings-kapacitet, men framför allt längre fördröjning än höghastighetsförbindelsen. Dataöverföringskapaciteten kan även vara asymmetrisk, det vill säga olika överföringskapacitet uppströms jämfört med nedströms. En fjärrförbindelse kan t.ex. realiseras genom mikrovågsteknik (radio), hyrda förbindelser med olika typer av digital anslutning över kopparkabel (t.ex. *Digital Subscriber Line* (DSL)) eller höghastighetsförbindelser som sträcker över stora geografiska avstånd och därigenom påför längre fördröjning än cirka 10 ms. Att etablera en logisk förbindelse över en fjärrlänk går oftast snabbt.

Fjärrförbindelser har som regel mycket låga paketförluster, men kan vid exempelvis användning av mikrovågslänkar påverkas av miljörelaterade faktorer, som väderförhållanden och fukt (se vidare avsnitt 2.2.8).

En annan anslutningform som under gynnsamma förhållanden kan leva upp till kraven för en fjärrförbindelse är 4:e generationens paketförmedlade mobilnät, *3GPP Long Term Evolution* (LTE)[LTE]. LTE utlovar högre kapacitet och kortare fördröjning än tidigare tekniker för mobil dataanvändning, genom bredare radiokanaler och förenklingar i nätarkitekturen.

Fjärrförbindelser definieras genom följande egenskaper:

- Dataöverföringskapacitet: från 1 Mbps i vardera riktning, kan vara asymmetrisk
- Maximal paketstorlek från cirka 1 500 oktetter.
- Svarstider: från omkring 10 ms upp till omkring 100 ms.
- Jitter: Varierande, beroende på anslutningsform och eventuell miljöpåverkan om länken realiseras genom radioteknik.
- Låg förekomst av paketförluster samt hög tillgänglighet.

2.1.3 Lågkapacitetsförbindelser

Med lågkapacitetsförbindelser avses digitala förbindelser med en överföringskapacitet från några kbps och upp till några Mbps. Begreppet inkluderar även traditionella modem, det vill säga en uppringd förbindelse där datakommunikationen omvandlas till analoga signaler kapabla att fångas upp och transporteras över ett traditionellt telefonsystem som om det vore röstkommunikation.

Vid användning av den här typen av länkar kan effekter av s.k. serialisering bli påtagliga, och medföra väsentlig påverkan på andra tjänster med vilka anslutningen delas. Paket fördröjs och jitter uppstår. Effekterna är särskilt påtagliga där realtidstrafik för t.ex. röstkommunikation blandas med asynkrona och transaktionsbaserade tjänster som tar mycket överföringskapacitet i anspråk.

Lågkapacitetsförbindelser används företrädesvis där kommunikationsinfrastrukturen är dåligt utbyggd. Uppringda förbindelser kan hålla särskilt låg kvalitet med mycket störningar och paketförluster, varpå modemen tvingas använda låga överföringshastigheter eller att anslutningen frekvent bryts.

Att etablera en logisk anslutning över en lågkapacitetsförbindelse kan ta relativt lång tid. Detta, särskilt i kombination med intermittens, kan göra det svårt att använda anslutningen till vissa typer tjänster.

Modemstandarder som V.90 och V.92 ger en dataöverföringskapacitet upp mot maximalt 56 kbps. Den fördröjning som erhålls beror mycket på hur långt avstånd det är mellan parterna och varierar från omkring 100 ms, men kan bli betydligt mer.

Mobilsystemet *Global System for Mobile Communications* (GSM) samt dess dataförmedlingsversioner *General Packet Radio Service* (GPRS) och *Enhanced Data rates for GSM Evolution* (EDGE) är etablerade former av trådlösa lågkapacitetsförbindelser. GPRS och EDGE erbjuder en asymmetrisk anslutning med kapacitet mellan 100-400 kbps. En GPRS-anslutning har lång fördröjning som i normalfallet är mellan 300 till 400 ms enkel väg, Fördröjningen kan också variera kraftigt.

GSM innehåller även en kretskopplad anslutning med dataöverföringskapacitet från 6,4 kbps till 64 kbps. För den kretskopplade tjänsten är emellertid fördröjningen under 100 ms.

Mobiltelefonstandarden *Universal Mobile Telecommunications System* (UMTS) (även kallat 3G) är efterföljaren till GSM. UMTS (med tillägget *High Speed Packet Access* (HSPA)) erbjuder ett antal olika paketdatalägen som under normal användning ger från 128 kbps upp till 21 Mbps (teoretiskt) nedströms i överföringskapacitet. Fördröjningen är lång, ofta över 100 ms och varierar också kraftigt. En terminal som växlar mellan olika paketdatalägen utsätts för intermittens som varar i upp till ett par sekunder, då inget data kan skickas.

Precis som i GSM finns i UMTS en kretskopplad anslutning. I UMTS ger denna anslutning 64 kbps och med en fördröjning under 100 ms.

Lågkapacitetsförbindelser definieras genom följande egenskaper:

- Dataöverföringskapacitet: från några kbps upp till några Mbps.
- Maximal paketstorlek upp till 1 500 oktetter, men kan vara väsentligt lägre.
- Svarstider: från cirka 100 ms upp till cirka 500 ms.
- Jitter: Högt i fallet med anslutningar via mobilnät. Lågt vid kretskopplade anslutningar, men även beroende på störningar som brus och överhörning.
- Förekomst av paketförluster samt varierande tillgänglighet.

2.1.4 Satellitförbindelser

Satellitbaserad kommunikation används för att från fasta eller mobila anläggningar kommunicera över långa avstånd. Satellitbaserad kommunikation används både för distribution av media från en sändare till många mottagare, men även för kommunikation mellan två enskilda parter.

De flesta kommersiella kommunikationssatelliterna befinner sig i geostationär bana, *Geostationary Orbit* (GEO). Detta innebär att satelliterna till synes står still över en given punkt på jorden. Geostationära satelliter befinner sig på ungefär 3 500 mils avstånd och i en bana runt ekvatorn. För en geostationär satellit är totala fördröjningen upp till satelliten och tillbaka omkring 240 ms. För en så kallad VSAT-länk, vilken kräver mindre antenner, men använder en markbaserad relästation ökar svarstiderna upp mot 900 ms.

Tillämpningar som ska kunna användas över satellitförbindelser bör vara sparsamma i sitt utnyttjande av dataöverföringskapacitet och klara långa fördröjningar väl. Kapaciteten hos en satellitanslutning är ofta asymmetrisk, det vill säga med olika dataöverföringskapacitet i upplänk och nedlänk. Asymmetrisk kapacitet medför ofta även olika fördröjning i upplänk respektive nedlänk, vilket ställer krav på tillämpningarna att även hantera detta.

Paketförluster förekommer över satellitförbindelser. Att etablera en logisk anslutning över en satellitförbindelse kan ta relativt lång tid. Däremot har satellitförbindelsen i sig ofta god tillgänglighet, men kan påverkas av miljörelaterade faktorer i atmosfären och rådande rymdväder.

Satellitförbindelser definieras genom följande egenskaper:

- Dataöverföringskapacitet: Från 200 kbps upp till några Mbps.
- Maximal paketstorlek på 1 500 oktetter.
- Fördröjning: från cirka 240 ms upp till 900 ms.
- Jitter: Varierande fördröjning.
- Viss förekomst av paketförluster men bra tillgänglighet.
- Stöder mobilitet.

Det finns även satelliter som befinner sig i lägre banor, exempelvis *Low Earth Orbit* (LEO). I dessa banor rör sig satelliterna i förhållande till marken. För en kommunikation som ska vara tillgänglig hela tiden används därför att terminalen kommunicerar via flera satelliter. Den kommersiella satellitoperatören Globalstar använder exempelvis 48 satelliter som går i en bana 140 mil över havet för att tillhandahålla röstkommunikation och dataöverföring i bithastigheter upp till 20 kbps. Globalstars teknik och den lägre banhöjden ger en fördröjning på omkring 60 ms, men är ofta inte ett alternativ för dataöverföring på grund av den starkt begränsade dataöverföringsakapaciteten.

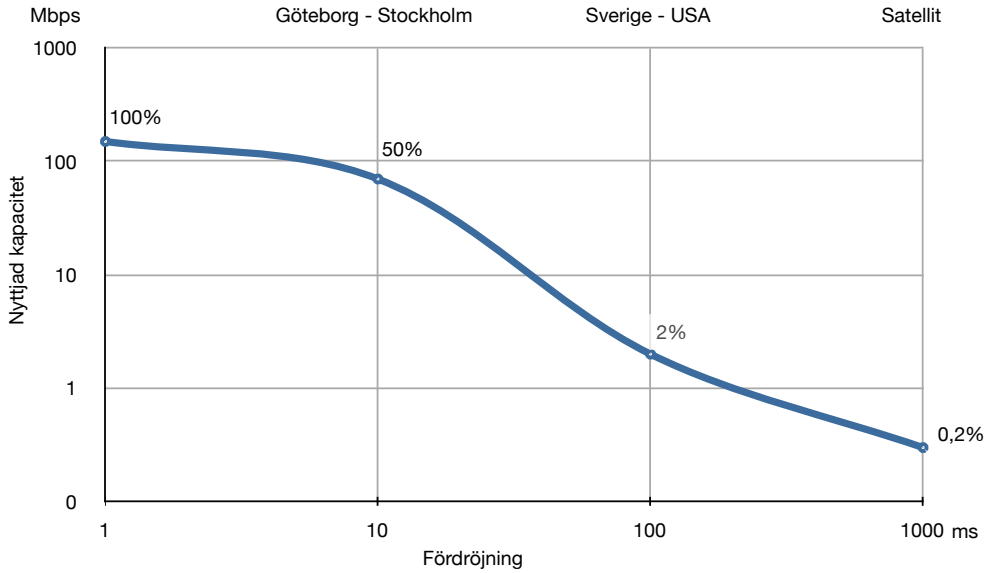
2.2 Ytterligare faktorer

2.2.1 Transportprotokollet TCP

För effektiv överföring av data mellan sändare och mottagare över ett IP-baserat nätverk krävs som regel någon typ av transportprotokoll. Transportprotokollet ansvarar för att dela upp data i lämpligt stora delar (i TCP kallas delarna *segment*) och säkerställa att styckena kommer fram till mottagaren på ett sådant sätt att datan kan återskapas efter överföringen. Det dominerande transportprotokollet på Internet är *Transmission Control Protocol* (TCP) [RFC793], och används exempelvis för filöverföring, e-post, fjärrskrivbord och webbaserade tjänster. TCP fungerar utifrån principen att skapa en virtuell kanal över den paketförmedlade anslutningen, och att optimera denna kanal så väl som möjligt utifrån de rådande omständigheterna. Hur väl TCP kan utnyttja den tillgängliga kapaciteten beror på flera faktorer. Två viktiga faktorer är hur lång fördröjning anslutningen har samt hur stor mängd paketförluster som uppstår vid överföringen.

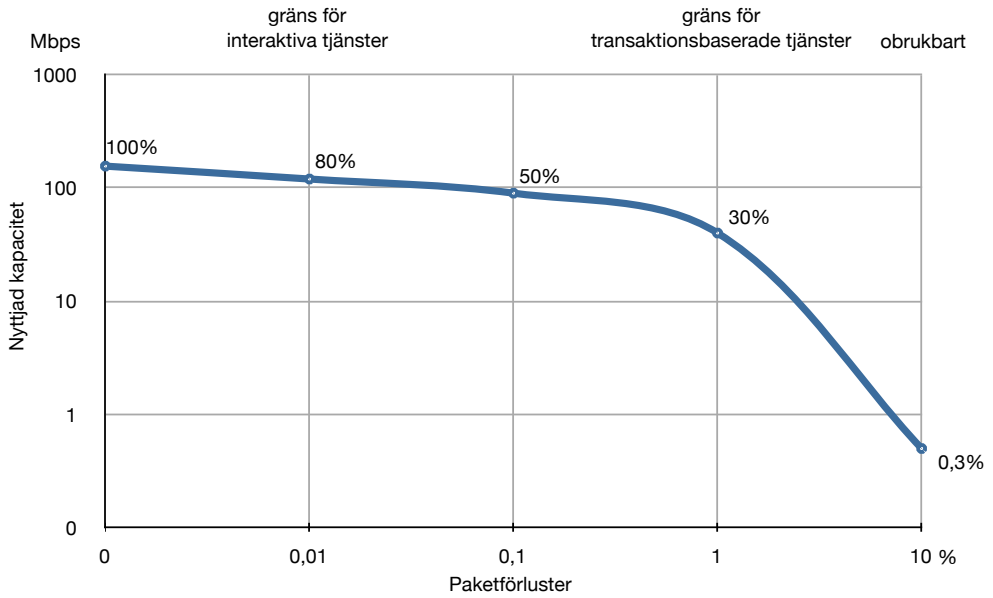
Figur 2.1 visar att oavsett tillgänglig kapacitet kommer den del av kapaciteten som TCP utnyttjar att sjunka ju längre fördröjning anslutningen har. Vid en fördröjning på 300 till 400 ms, dvs. typiska värden för en satellitanslutning, kan TCP bara utnyttja en liten del av anslutningens kapacitet, oavsett hur mycket överföringskapacitet som finns tillgängligt. TCP är relativt tåligt mot paketförluster, men när mängden förluster ökar bortom en viss gräns får felkorrigeringsmekanismerna allt svårare att fungera.

Figur 2.2 visar hur olika grader av paketförluster påverkar den överföringskapacitet TCP kan tillhandahålla tillämpningen. Vid stora mängder paketförluster, över 1%, faller den effektiva överföringskapaciteten drastiskt och tillämpningar som använder TCP blir snabbt obrukbara.



Figur 2.1 – Utnyttjandegrad hos TCP av underliggande kapacitet som funktion av anslutningens fördröjning

Moderna operativsystem har i dag beprövade och väl fungerande implementationer av TCP, som ofta är dynamiska med förmåga att anpassa viktiga parametrar till egenskaperna hos olika typer av anslutningar. För vissa användningsfall och ovanligare anslutningsformer kan det emellertid krävas manuella justeringar för att god prestanda ska erhållas. Exempel på anslutningar där detta kan krävas är satellitanslutningar eller mobilsystem. Att ändra TCP-inställningarna kan dock föra med sig sidoeffekter, som att tillgänglig kapacitet snedfördelas mellan tillämpningar och användare. Det kan innebära att vissa användare eller vissa tillämpningar tar oproportionerligt stor andel av anslutningens kapacitet i anspråk.



Figur 2.2 – Utnyttjandegrad hos TCP av underliggande kapacitet som funktion av mängd paketförluster

Då fördröjningar eller förekommande paketförluster är de faktorer som i första hand begränsar den effektiva överföringskapaciteten, är det ofta inte meningsfullt att tillföra mer överföringskapacitet. Att ändra på TCP-parametrar eller använda en bättre anpassad tillämpning är ofta åtgärder som har större inverkan än att öka tillgänglig överföringskapacitet.

2.2.2 Trådlösa lokalnät

Trådlösa lokala nätverk är en form av höghastighetsanslutning som vuxit kraftigt i popularitet på senare tid. Minskade implementations- och driftskostnader samt krav på mobilitet och effektiva arbetssätt är incitament som driver efterfrågan.

Tidiga implementationer byggde på dyr leverantörsspecifik teknik med blygsam prestanda. Idag är prisförhållandet mellan trådbundna och trådlösa nätverk snarare det omvända och trådbundna nätverk är ofta dyrare att installera. De trådlösa nätverkens kvalitetsegenskaper i termer av tillförlitlighet, skalbarhet och prestanda är dock inte jämförbara med de trådbundna till följd av radiomediats beskaffenhet.

Radiospektrat – det delade mediat

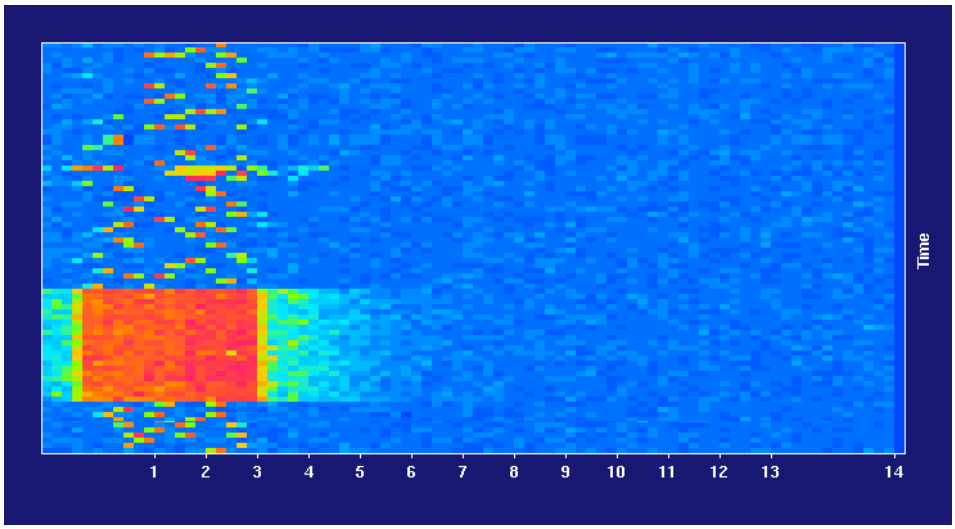
Radiovågors egenskaper att breda ut sig, reflekteras och tränga igenom vegetation, väggar, fönster och andra hinder gör det till ett delat media.

I den svenska frekvensplanen tillåts radioanläggningar för dataöverföring med bandspridningsteknik (“RadioLAN”) som uppfyller kraven i EN 300 328 v1.8.1 (2012-04)[etsi-en-300-328] eller motsvarande krav, att använda följande frekvensband:

- 2 400 – 2 483,5 MHz (del av S-bandet)

Internationellt refereras till frekvensbandet som ett av de licensfria ISM-banden[1]. Licensfritt innebär i detta fall att den utrustning som uppfyller kraven i EN 300 328 v1.8.1 (2012-04)[etsi-en-300-328] är formellt undantagen tillståndsplikt enligt 3 kap. §§ 125, 130 och 132 PTSFS 2012:3[ptsfs-2012-3]. Frekvensbandet är alltså inte oreglerat, eller på annat sätt fritt att använda på vilket sätt som helst. EN 300 328 v1.8.1 (2012-04)[etsi-en-300-328] ställer bl.a krav på att total utstrålad effekt, *Equivalent Isotropically Radiated Power* (EIRP) – ekvivalent isotropiskt utstrålad effekt, begränsas till maximalt 100 mW, samt att utrustningen implementerar så kallad bandspridningsteknik. Dessutom begränsas enheterna att aldrig emittera mer än 10 mW per MHz.

Bandspridningsteknik innebär att signalen delas upp i segment som fördelas över ett frekvensband som är bredare än den enskilda bärvågen. För mottagning krävs att en synkroniserad spridningssignal finns tillgänglig. Bandspridningsteknik har bl.a. till fördel att signalen blir mindre sårbar för interferens.

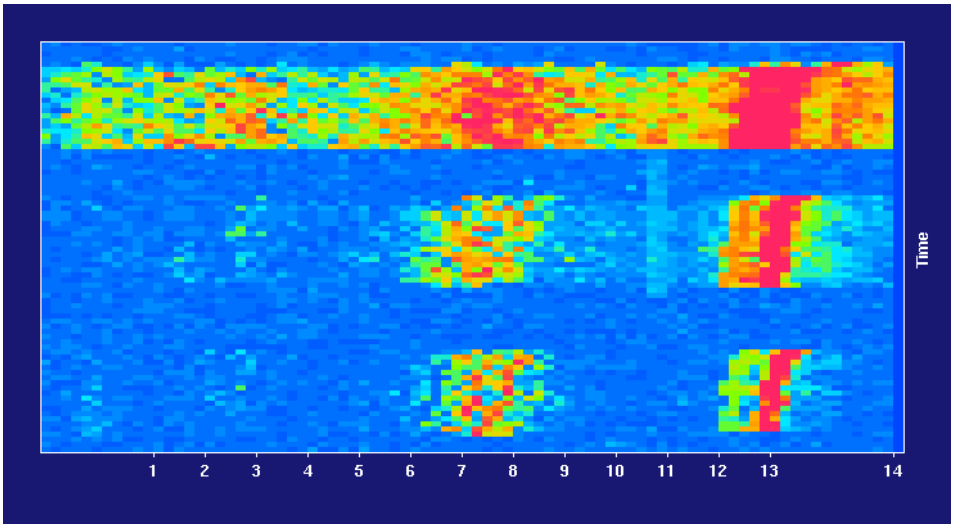


Figur 2.3 – Filöverföring (802.11g/OFDM)

Andra användningsområden som nyttjar samma del av S-bandet som

[1] ISM – Industrial, Scientific, Medical

radioanläggningar för dataöverföring är bl.a. blåtand[2] (“Bluetooth”), amatörradio (max 100 mW), militär radio och teknik baserad på *Radio-Frequency Identification* (RFID) (max 25 mW). Att frekvensbandet också är ett s.k. ISM-band innebär att man kan behöva acceptera och hantera interferens från enheter som emitterar radiofrekvent energi i annat syfte än radiokommunikation, t.ex. mikrovågsugnar, plastsvetsar och medicinsk utrustning.



Figur 2.4 – Mikrovågsugn (1 m/5 m/10 m)

I mitten av 2002 samordnade man inom standardiseringsorganet ETSI ytterligare frekvensband för dataöverföring undantaget tillståndsplikt:

- 5 150 – 5 350 MHz (del av C-bandet)
- 5 470 – 5 725 MHz (del av C-bandet)

För radioanläggningar i C-bandet gäller ytterligare restriktioner enligt EN 301 893 v1.7.0 (2012-01)[etsi-en-301-893]. I det undre frekvensbandet får utrustning endast användas inomhus då det bl.a. finns risk för interferens med radionavigering för luftfart, och med en maximal ekvivalent isotropiskt utstrålad effekt (EIRP) av 200 mW. I det övre frekvensbandet finns dock möjlighet att använda uteffekten 1 W (EIRP).

Den högre tillåtna effekten kompenserar i någon mån det faktum att effekterna av fädning är mer påtagliga i 5 GHz-banden, och att signalen har svårare att tränga igenom väggar, tak och andra hinder [WIFIFADING].

[2]Blåtand faller under definitionen för radioanläggning för dataöverföring

Luften är fri

En princip inom radiolagstiftningen är att etern är fri (se prop. 1988/89:124 s. 39) i meningen att bereda sig tillgång till data som överförs. Däremot ger 14 § EkomF ett i princip generellt förbud mot innehav av anläggningar som är avsedda att sända radiovågor i syfte att störa annan radiokommunikation. Detta är i praktiken det enda skydd som anläggningar för trådlösa lokalnät åtnjuter från lagen.

Det är alltså inte möjligt att äga eller licensiera frekvensutrymmet som används för trådlösa lokalnät, inte ens inom sina egna lokaler. Det går därför inte med säkerhet att skydda sig mot interferens från omgivningen med mindre än att skärma av det elektromagnetiska fältet kring sin anläggning.

Radioanläggningar för dataöverföring undantagna från tillståndsplikt är dessutom ett sekundärt användningsområde av radiospektrat. Utrustningen måste i mycket hög grad kunna acceptera störningar och interferens. Det finns heller inget som föreskriver att olika tekniker för trådlösa lokalnät ska vara kompatibla. Därför kan man förvänta sig interferens även mellan olika implementationer av väsentligen samma funktion.

Dataöverföringskapacitet

Dataöverföringskapaciteten i trådlösa lokalnät beror på ett flertal faktorer, vilka i huvudsak är:

bandbredden eller kanalbredden, som vanligen är 20 MHz eller 40 MHz, men kan vara upp till 160 MHz (802.11ac),

moduleringen som styr hur mycket data som kan överlagras på bärvågen,

förhållandet mellan signalstyrkan och bakgrundsbruset och utrustningens förmåga (känslighet) att urskilja signalen ur bruset,

graden av interferens från annan utrustning som använder samma frekvensband,

användningen av så kallad MIMO-teknik för att koordinera flera sändar- och mottagarenheter och därmed upprätta flera spatiella kanaler som kan användas parallellt vid överföring av data.

Det skall också understrykas att den teoretiska högsta linjeöverföringskapaciten inte är densamma som den effektiva dataöverföringskapaciteten. Kontrollmekanismerna för mediaåtkomst och felkorrektion tar omkring 40% av kapaciteten i anspråk, och lämnar således runt 60% för effektiv dataöverföring under optimala förhållanden. En anslutning med linjehastigheten 300 Mbps kan i bästa fall förväntas leverera en överföringskapacitet omkring 180 Mbps totalt, som också ska delas mellan alla enheter på den aktuella kanalen.

Cellplanering

Avgörande för ett erhålla ett stabilt och effektivt trådlöst lokalnät är cellplaneringen. Vid cellplaneringen görs en kravinsamling beträffande täckningsgrad och kapacitet,

varefter lokalernas och områdets beskaffenhet bedöms för att avgöra basstationernas placering, antennkonfiguration, uteffekt och vilka kanaler som ska användas.

För att kunna tillgodose kapaciteten för många klienter inom ett begränsat område kan cellindelningen i det trådlösa lokalnätet behöva krympas och göras tätare med fler basstationer. För att minska problem med samkanalinterferens kan basstationernas effekt behöva minskas.

I 2,4 GHz-bandet är kanalplanering och att undvika samkanalinterferens särskilt viktig, då det endast ryms tre icke-överlappande 20 MHz-kanaler i frekvensbandet. Detta är också orsaken till att 40 MHz breda kanaler är direkt olämpliga att använda i 2,4 GHz-bandet.

Centraliserade trådlösa nätverk

Centraliserade trådlösa nätverk definieras som en metod för att knyta samman ett närmast godtyckligt antal distribuerade basstationer (“trådlösa termineringspunkter”) för nätåtkomst till en centraliserad kontrollpunkt. På detta sätt kan administrationen av det trådlösa lokalnätet effektiviseras och komplexiteten minskas. Centraliseringen medger också möjlighet till sömlös överlämning mellan basstationer inom hela den trådlösa infrastrukturen, vilket gör att realtidstillämpningar får bättre förutsättningar att fungera. Slutligen kan kontrollenheterna övervaka täckningsområdet och alla ingående enheter, automatiskt koordinera effekt och kanalplanering, samt även tillhandahålla positioneringstjänster.

Tillgänglighetsaspekter

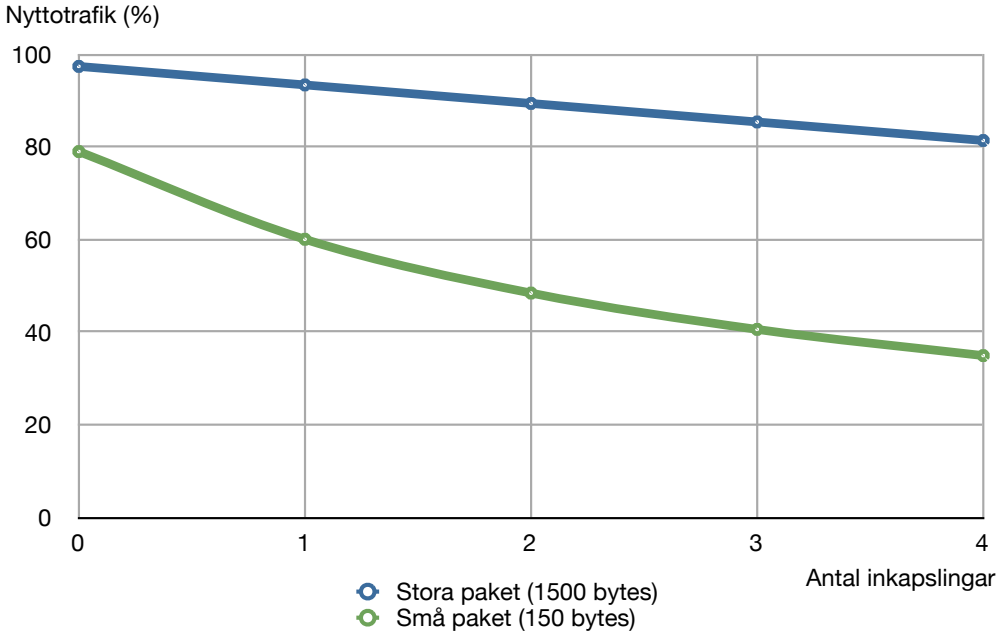
Trådlösa lokalnät är i dess natur också särskilt känsliga för sabotage. Kontrollramar skickas alltid i klartext, utan äkthetskontroll och utan integritetsskydd. Datalänknivån är därvid sårbar för många relativt enkla tillgänglighetsangrepp. Mer sofistikerade angrepp skulle kunna innefatta en modifierad klient som exploaterar den konkurrensbaserade åtkomstmetoden genom att simulera en överfull kanal, och därigenom stoppa all trafik. Slutligen går det även att störa ut det trådlösa lokalnätet på fysisk nivå med hjälp av störsändare.

Känsligheten för avsiktliga störningar, tillsammans med det faktum att det existerar en mängd tillämpningar som oavsiktligt kan påverka de trådlösa lokalnätens kvalitet och tillgänglighet, gör att den trådlösa infrastrukturen främst bör ses som ett komplement i verksamhetskritiska sammanhang.

2.2.3 Inkapslade anslutningar

I syfte att uppfylla erforderliga säkerhetskrav, eller för att kunna använda en specifik anslutningsform, kan den använda anslutningen behöva transporteras som nyttotrafik i en annan anslutning. Metoden att på detta sätt kapsla in en anslutning i en annan anslutning kallas generellt *tunnling*.

Inkapslingen i sig påverkar anslutningens egenskaper i form av att tillgänglig nyttokapacitet minskar, och att fördröjning och känslighet för olika typer av störningar ökar. Denna påverkan kan ge märkbara effekter på den tillämpning som bärs av den inkapslade anslutningen. Särskilt då inkapsling sker i flera nivåer, *tunnel i tunnel*, kan påverkan bli avsevärd.



Figur 2.5 – Maximal utnyttjandegrad av underliggande kapacitet vid inkapslade anslutningar (stora respektive små paket)

Kvaliteten i den slutliga tjänsten kan komma att påverkas på ett än mer märkbart sätt än ren TCP-överföring. Ett exempel är filöverföringar med Microsofts fildelningsprotokoll *Server Message Block* (SMB), även kallat *Common Internet File System* (CIFS) eller tjänster med hög interaktivitet och små paket.

Resultatet av tunnelmekanismers påverkan på tjänsterna kan sammanfattas i att ju bättre kapacitet en anslutning har, desto större blir påverkan på kvaliteten när man påför tunnelmekanismer, samt att tjänster som använder små paket (t.ex. IP-telefon och fjärrskrivbord) kommer ta en väsentligt större andel av nyttotrafiken i anspråk än tjänster som utnyttjar stora paket (filöverföring, e-post, mm.).

Tunnelmekanismer kan ha olika påverkan på olika tillämpningar och i olika anslutningsformer. Vid stora mängder små paket kan den effektiva överföringskapaciteten halveras.

2.2.4 Komprimering

Komprimering används för att reducera mängden data som en tjänst behöver överföra. Det finns tre huvudtyper av komprimeringsmekanismer: datakomprimering med informationsförlust, datakomprimering utan informationsförlust samt protokollkomprimering.

Datakomprimering med informationsförlust innebär att delar av den information i data som behandlas går förlorad. Som regel sker en avvägning mellan den resulterande informationens kvalitet och effektivitetsgrad i komprimeringen. Datakomprimering med informationsförlust används exempelvis i röstkodare för IP-telefon där delar av det talade ljudet utelämnas. Ett annat exempel är vissa fjärrskrivbord där antalet färger samt bildens upplösning kan reduceras när överföringskapaciteten hos anslutningen minskar.

Datakomprimering utan informationsförlust innebär att data skrivs om, eller transformeras innan överföring. Transformen är utformad så att mängden data som behöver överföras reduceras. På mottagarsidan återskapas orginaldata fullständigt. Ett exempel på datakomprimering utan informationsförlust är algoritmen DEFLATE [RFC1951] vilken bland annat används i protokollen *Transport Layer Security* (TLS) och *Internet Protocol Security* (IPsec).

Hur väl datakomprimeringen fungerar beror på innehållet i datamängden. Komprimeringen bygger på att det finns mönster och varierad förekomst av olika symboler i det data som ska komprimeras. Därför måste datakomprimering appliceras före t.ex. kryptering.

Protokollkomprimering innebär att mängden information i själva kommunikationsprotokollen reduceras, vilket därmed minskar behovet av överföringskapacitet. Protokollkomprimering innebär att fält i protokollens huvuden som inte ändras, eller som ändras på ett känt sätt, kan utelämnas vid överföringen. Protokollkomprimering innebär således att protokollen inte längre följer sina protokollstandarder under själva överföringen genom nätet. Ett exempel på protokollkomprimering är *Robust Header Compression* (ROHC) [RFC3095].

Komprimering och dekomprimering tar en viss tid, men tiden är jämförelsevis liten och sker ofta när sändande eller mottagande part väntar in andra händelser. Eftersom komprimering minskar mängden data som behöver överföras minskar istället den totala fördröjningen och komprimering förbättrar ofta en tjänst responsivitet.

För både datakomprimering utan informationsförlust och protokollkomprimering etableras ett tillstånd mellan sändare och mottagare. Om tillståndet förloras kan mottagaren inte längre återskapa datan. Konsekvenserna av förlorade paket kan även bli större med komprimering då en större del av ursprungsdatan kan påverkas eller förloras.

2.2.5 WAN-acceleration

En typ av utrustning som används för att förbättra användbarheten i tillämpningar som kommunicerar över anslutningar med begränsad kapacitet är WAN-acceleratorer. WAN-acceleratorer använder flera metoder för att reducera mängden trafik,

däribland datakomprimering, protokollkomprimering, temporär mellanlagring av data samt även efterhärmning (“spoofing”) av motparten för att påskynda vissa protokolloperationer.

WAN-acceleratorn kan även till viss del reducera påverkan av långa svarstider, men inför också nya tillstånd i nätverket och kan även skapa beroenden mellan annars oberoende trafikströmmar. För vissa typer av trafik, exempelvis trafik som är krypterad, ger WAN-acceleratorer oftast endast en marginell förbättring.

2.2.6 Kryptering

Kryptering är teknik som används för att på olika sätt skydda information som överförs mellan kommunicerande parter. I denna publikation belyses inte de informationssäkerhetsmässiga eller signalskyddsmässiga aspekterna av kryptering. Däremot kan kryptering i sig ställa krav på och också påverka den anslutning en tillämpning använder. Beroende på typ av kryptering och typ av tillämpning kan påverkan av att tillämpa kryptering bli väsentlig, huvudsakligen genom att:

- påföra fördröjningar,
- öka åtgången av överföringskapacitet,
- skapa tillstånd och beroenden mellan sändare och mottagare, vilket ökar den sammantagna störningskänsligheten i anslutningen.

För att etablera en kryptografiskt skyddad anslutning mellan parterna sker normalt först en initieringsfas där parternas identitet bekräftas och att parterna kommer överens om vilka mekanismer, algoritmer och nycklar som ska användas för att skydda kommunikationen. Initieringsfasen kan ta förhållandevis lång tid. För tillämpningar som frekvent startas om kan där med tiden för initiering påverka tjänstekvaliteten.

Efter initiering används vanligen symmetrisk kryptering för den fortsatta kommunikationen. Det finns två huvudtyper av symmetrisk kryptering; blockkrypton och strömkrypton. Blockkrypton bearbetar data i block med fix storlek, vilket ofta leder till en expansion av mängden data som ska överföras. Strömkrypton är i det avseendet som regel effektivare, men ställer krav på att sändare och mottagare har synkroniserade tillstånd och är i fas med varandra.

Vad som krypteras kan också påverka hur mycket krypteringen påverkar upplevelsen av tillämpningen. En kryptering som arbetar på enstaka fält i XML-strukturerad information kan kräva långt fler initieringar än ett transportkryptering där det sker en initiering för ett helt meddelande eller kommunikation.

Vilken typ av krypteringsteknik som används kan ha stor inverkan på tillämpningens upplevda kvaliteten.

2.2.7 Prioritet och tjänstekvalitet

IP-baserad kommunikation sker som regel utifrån nätverksutrustningens bästa förmåga (*"best effort"*) att vidarebefordra data mellan sändare och mottagare. Uppstår fel kan IP-paketet komma att kasseras eller fördröjas, och det är upp till de kommunicerande parterna att upptäcka och korrigera för fel som uppstår.

Transportprotokollet TCP innehåller funktionalitet för att skicka om paket som försvunnit på vägen och säkerställa ordningen på mottaget data. Beroende på typ av tillämpning kan omsändningar och fördröjningar i nätet vara mer eller mindre acceptabla. Filöverföring påverkas t.ex i mindre grad av omsändningar än IP-telefon eller fjärrskrivbord.

IP-trafik är som regel klasslös. All trafik behandlas lika av nätverkets noder. Det existerar emellertid mekanismer både i IP-protokollet och underliggande länklager för att klassificera och kategorisera trafik. Moderna nätverksenheter har ofta stöd för att prioritera trafiken utifrån dessa klassificeringsmekanismer.

I tjänstespecifika nät som ett mobilnät, och även i lokalnät där exempelvis trafik för lagringsnät blandas med andra tjänsters trafik, kan indelning av trafiken i olika tjänster bidra till att höja den upplevda kvaliteten hos tjänsterna. Men som generell mekanism för att lösa resursbrister i anslutningar fungerar prioritetsmekanismerna sämre.

Ett skäl till detta är att prioritetsmekanismerna ofta inrättas och implementeras lokalt. För att inte trafik ska prioriteras fel måste prioritetsinställningarna vara konsekventa genom hela nätet. Olika operatörer kan välja att tolka klassificeringsinformationen i paketen på olika sätt och göra andra prioritetsval. En operatör kan även välja att ignorera klassificeringsinformationen som finns i inkommande trafik. För en anslutning är det den totala prioritet och hantering av trafiken mellan sändare och mottagare som avgör vilken kvalitet trafiken får.

Som närmare beskrivs i del två finns det i operativsystem olika algoritmer som styr hur transportprotokollet TCP fungerar. Det gemensamma för dessa algoritmer är att de generellt gör antagandet att den tillgängliga kapaciteten i nätverket ska fördelas jämt mellan användare och tjänster. Genom att klassificera och därmed prioritera trafik som flödar genom nätet sätts dessa antaganden ur spel, vilket riskerar leda till att TCP-baserad kommunikation generellt fungerar sämre.

Att använda klassificering och prioritering innebär även ökad börda i form av teknisk administration. Prioritetstabeller ska samordnas och dokumenteras. Sedan ska prioritetsvalen distribueras ut till noderna i nätverket. När störningar och fel uppstår i nätverket kan prioriteringen av trafik försvåra felsökningen.

Att använda klassificering och prioritering kan underlätta i nät där det finns kapacitetsbrister, genom att försämra för vissa tjänster till förmån för andra. Men användning av dessa mekanismer för alltid med sig nackdelar och ställer krav på kontroll av nätet och de tillämpningar som använder nätet.

Trafikprioritering kan vara en effektiv metod att förbättra förutsättningarna för en viss tjänst inom ett begränsat nät, men på bekostnad av andra tjänster och medför också högre fördröjning.

2.2.8 Miljöpåverkan

En anslutnings egenskaper kan påverkas av faktorer i den fysiska omgivningen. Ett vanligt exempel är mikrovågsbaserade anslutningsformer som påverkas av väderförhållanden och andra miljöförutsättningar. Vid planering av mikrovågsbaserad kommunikation måste hänsyn till miljöpåverkan tas.

I det fall störningar och paketförluster uppkommer över en anslutning kan ett antal olika åtgärder vidtas i syfte att förbättra kvaliteten. Några åtgärder är att sänka bärfrekvens, byta radiosignalens polarisation eller använda fysisk diversitet med fler antennpar. Slutligen kan även avståndet mellan sändare och mottagare minskas genom att dela upp anslutningen i fler länkhopp.

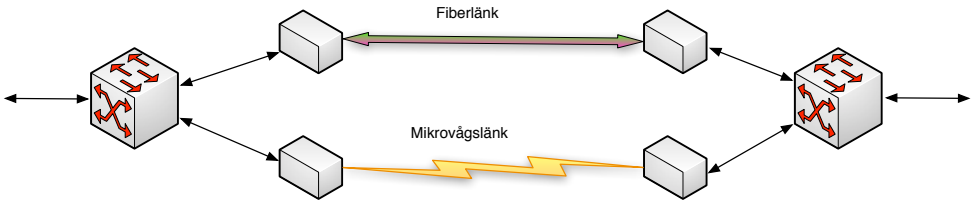
Tjänster som ska fungera över mikrovågsanslutning behöver utformas för att fungera tillfredsställande även när förutsättningarna för anslutningen är som minst fördelaktiga.

2.3 Feltolerans

2.3.1 Mediadiversitet

Mediadiversitet innebär att två parter sammankopplas genom minst två olika anslutningsformer. Skälet till att använda mediadiversitet är att öka motståndskraften mot störningar och öka förbindelsens tillgänglighet vid enkelfel. Exempelvis kan en anslutning mellan två noder realiseras genom en höghastighetsförbindelse över optisk fiber, samt en fjärranslutning baserad på mikrovågsteknik. Ett annat exempel kan vara att en fjärranslutning via traditionella kopparnätet (DSL) kompletteras med en anslutning via mobilnätet (UMTS) för att nå en högre grad av tillgänglighet.

Under normala förhållanden används den anslutning med högst kapacitet, det vill säga den primära anslutningen. Skulle den primära anslutningen sluta fungera flyttas trafiken över till den sekundära anslutningen.



Figur 2.6 – Exempel på anslutning med mediadiversitet baserad på optisk fiber och mikrovågsteknik.

Egenskaperna hos den primära och den sekundära anslutningen kan emellertid skilja högst avsevärt i termer av kapacitet, fördröjning och störningar. Om den sekundära anslutningens kapacitet är otillräcklig för normalt utnyttjande, kan klassificering av trafik bli nödvändigt för att prioritera de viktigaste tjänsterna.

Som komplement eller alternativ till mediadiversitet används ofta även geografisk diversitet. Geografisk diversitet innebär att anslutningarna är geografiskt skilda från varandra för att minska sannolikheten att en händelse som resulterar i ett avbrott påverkar båda anslutningarna samtidigt. I detta fall är det också vanligare att både den primära och den sekundära anslutningen erbjuder samma kvalitet, och att den kombinerade anslutningen då erbjuder full funktionalitet även då primäranslutningens funktion fallit ifrån.

2.3.2 Redundans

Redundans är en form av feltolerans som innebär att kommunikationstjänster kan fortsätta fungera trots att en eller flera förbindelser och/eller kommunikationsnoder i ett nät blivit otillgängliga. Redundansen i detta avseende kan implementeras på nät- eller applikationsnivå.

Redundans för förbindelser och nätelement

För att åstadkomma redundans för förbindelser och nätelement är det vanligt att använda multipla förbindelser i kombination med en redundant uppsättning utrustning. Vägvalsprotokoll på nätverksnivå används för att styra trafiken över tillgängliga förbindelser, och för att utesluta icke-fungerande nätelement (t.ex. routrar) som inte vidarebefordrar trafik.

Redundans för tillämpningar

För att tillämpningar ska kunna fortsätta fungera vid avbrott på en enskild server finns flera alternativ:

Redundans på protokollnivå innebär att applikationsnivåprotokollet i sig har stöd för att välja flera möjliga servrar. När kommunikationen upprättas, eller om den avbryts, väljer klienten mellan bland möjliga servrar och försöker ansluta mot dessa – parallellt eller sekventiellt. Valbara servrar för tjänsten publiceras vanligen i *Domain Name System* (DNS) eller någon annan katalogtjänst. Protokoll med väl utvecklat stöd redundans på protokollnivå är t.ex. DNS och *Simple Mail Transfer Protocol* (SMTP).

Lastbalansering används ofta också för att implementera olika former redundans på applikationsnivå, t.ex. genom att en lastbalanserare ansluts mellan klient och servrar, vanligen så nära serversidan som möjligt. Lastbalanseraren fördelar inkommande anrop mellan ansluta servrar och väljer automatiskt bort servrar som inte svarar alls eller som för stunden har otillräckligt med tillgängliga resurser.

Lastbalanseraren kan vara konstruerad så att den har kännedom om det protokoll som hanteras eller arbeta direkt på transportnivå, t.ex. TCP eller *User Datagram Protocol* (UDP). I de fall lastbalanseraren kan tolka det protokoll som hanteras kan denna information ligga till grund för hur fördelningen mellan

tillgängliga servrar ska ske. *Hypertext Transfer Protocol* (HTTP) är ett exempel på ett protokoll som ofta görs redundant med hjälp av lastbalanserare.

Anycast är en form av redundans som implementeras på nätnivå och där vägvalsprotokollet låter styra trafik mot närmaste tillgängliga server. Anycast kräver att serversidan av applikationen på något sätt är ihopkopplat med vägvalsprotokollet, och på så sätt indikerar sin tillgänglighet. Anycast fungerar normalt bäst för UDP-baserade protokoll med relativt kortlivade sessioner, t.ex. DNS.

De mekanismer som belyses ovan kombineras ofta i en mer komplexa strukturer, t.ex. genom att geografisk redundans implementeras på protokollnivå medan redundans för en grupp lokalt anslutna servrar implementeras genom lastbalansering.

En verksamhets behov av feltolerans kan även åstadkommas genom att ha stöd för alternativa tillämpningar som ställer enklare krav på den underliggande anslutningen. Exempelvis kan e-post vid behov till viss del ersätta telefon.

3 Tillämpningarnas kvalitetskrav

Tillämpningar kan grovt delas in i några olika typer beroende på hur de används, och därmed vilka krav som ställs på kommunikationsanslutningars kvalitetsegenskaper:

- **Synkrona tillämpningar**. Båda parter i kommunikationen är aktiva och för att tjänsten ska fungera ställs stränga krav på maximal fördröjning och varians, minsta tillgängliga dataöverföringskapacitet, bevarande av ordning på paketen samt maximal mängd paketförluster. För vissa synkrona tillämpningar blir ett paket värdelöst om det inte kommer fram vid en viss tidpunkt. Exempel på synkrona tillämpningar är IP-telefoni, videokonferens och *Time-Division Multiplexing over IP* (TDMoIP). realtidssimuleringar och nätverksspel med stöd för ett stort antal samtidiga användare som interagerar i realtid är synkrona tillämpningar med krav på mycket låg fördröjning. Synkrona tillämpningar är ofta interaktiva (se nästa punkt), men interaktiva tillämpningar behöver inte vara synkrona.

  När kraven för den synkrona tillämpningen inte kan uppfyllas sker ofta en snabb försämring av tjänsten som kan bli i det närmaste obrukbar även vid små försämringar av anslutningen.

- **Interaktiva tillämpningar**. En interaktiv tillämpning innebär att en människa finns bakom minst en av parterna i en kommunikation. Till skillnad från synkrona tillämpningar är kraven på maximal fördröjning, omsändning och ordning inte lika stränga. Ett exempel på en interaktiv tillämpning är fjärrskrivbord.

  När kraven som ställs av en interaktiv tillämpning inte kan erhållas sker ofta en gradvis försämring av tjänstekvaliteten. Vissa tillämpningar är kapabla att anpassa sig till försämringar. Exempelvis finns det fjärrskrivbord kapabla att skala ner mängden detaljer och hur saker på skrivbordet representeras i takt med att tillgänglig dataöverföringskapacitet minskar eller att fördröjningen ökar. En interaktiv tillämpning blir obrukbar över en viss maximal fördröjning oavsett hur lite data som skickas.

- **Transaktionsbaserade tillämpningar**. En transaktionsbaserad tillämpning innebär att den ena parten – klienten – begär resultat från motparten – servern. Resultatet leder till minst ett svar från servern, men kan även ge upphov till en uppsättning transaktioner mellan parterna. Exempel på transaktionsbaserade tillämpningar är webbåtkomst och direktmeddelanden, *Instant Messaging* (IM).

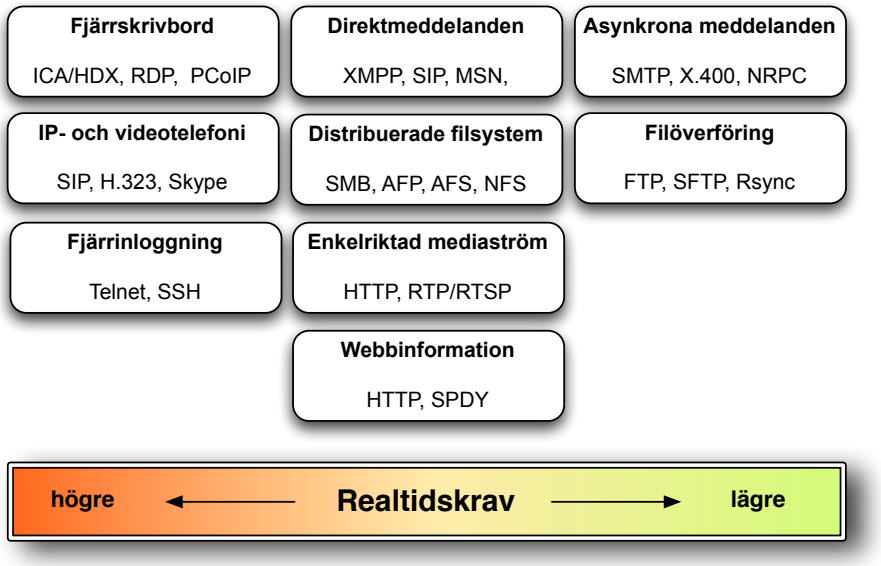
En viktig skillnad gentemot en interaktiv kommunikationstillämpning är att tiden från det att klienten gör ett anrop, till det att svaret erhålls, kan variera stort utan att tjänsten bryter samman. Detta gör en transaktionsbaserad tillämpning kapabel att anpassa sig eller vara relativt okänslig mot variationer i såväl dataöverföringskapacitet som fördröjning.

- **Asynkrona tillämpningar**. I dessa tillämpningar är parterna som utbyter data frikopplade från varandra. Överföringen ställer inga krav på att någondera parten är aktiv. Typiskt innehåller dessa tjänster stöd för att mellanlagra data samt att repetitivt försöka ansluta tills dess att data är överfört och kvitterat. Exempel på denna typ av tjänster är e-post, meddelandeköer och schemalagda dataöverföringar.

  En asynkron tillämpning är mycket tålig mot störningar och försämringar hos anslutningen. Det primära för många av dessa tjänster är att meddelanden till slut kommer fram.

Man kan se beskrivningen ovan som ett sätt att förhålla sig till och anpassa sin tjänsteanvändning till rådande kommunikationsförhållanden. Är förhållandena goda går det bra att använda tillämpningar som nätverksbaserad videokonferens. Om förhållandena försämras kanske man bör gå över till enbart ljudbaserad kommunikation eller interaktiva tillämpningar. När detta inte fungerar får man gå över till meddelandetjänster som direktmeddelanden. Till sist är det bara tillämpningar som e-post och schemalagda dataöverföringar som fungerar.

En klassificering av olika typer av tjänsteprotokoll måste även ta hänsyn till hur tillämpningen är uppbyggd samt hur den används. Att exempelvis använda det webbaserade dokumentverktyget *Google Docs* är en mycket mer interaktiv användning av webben än att läsa nyheter. Den senare är en typisk transaktionsbaserad tillämpning, medan den förstnämnda tangerar att bli en interaktiv tillämpning (även om mycket av verktygets funktion i praktiken utförs lokalt i klientprogramvaran).



Figur 3.1 – Olika tillämpningars realtidskrav

3.1 Synkrona tillämpningar

Som synkrona tillämpningar räknas tillämpningar där information utväxlas i realtid, och där informationen endast är användbar om den anländer i rätt stund.

Vanliga exempel på synkrona tillämpningar innefattar röst- och videosamtal samt nätverksspel och realtidssimuleringar där två eller flera användare interagerar via tillämpningen. Andra exempel på realtidstillämpningar är fjärrstyrningsmekanismer i olika former där åtgärder i realtid återkopplas till operatören genom överföring av bild, ljud eller annat data. Inom militära tillämpningar är fjärrstyrning av s.k. drönare ett exempel på en sådan realtidstillämpning.

Gemensamt för dessa tillämpningar är att de ställer mycket stringenta krav på korta svarstider. Interaktionen mellan de två parterna i kommunikationen måste kunna ske inom vissa givna tidsramar, inte sällan inom bråkdelar av en sekund. Normal språkväxling människor emellan fordrar som regel att svarstiden hålls väl under 0,5 sekunder för att upplevas som naturlig. När kraven för den synkrona tillämpningen inte kan uppfyllas sker ofta en snabb försämring av tillämpningens upplevda användbarhet.

3.2 Interaktiva tillämpningar

3.2.1 Textbaserad terminalåtkomst

En av de vanligast förekommande interaktiva tillämpningarna har varit och är fortfarande terminalåtkomst mot ett textbaserat gränssnitt. Exempel på kommunikationsprotokoll för detta ändamål är telnet och SSH, som i typtillämpningen

överför tecken för tecken. Tecknen skickas tillbaka till användaren allt eftersom de erhålls av servertillämpningen. Detta i motsats till t.ex. IBM 3270, som också är ett textbaserat gränssnitt, men som gör blocköverföringar av text, och därför mer är att kategorisera som en transaktionsbaserad tjänst.

Dessa terminalåtkomstprotokoll som överför tecken för tecken fodrar som regel endast mycket liten överföringskapacitet, men är i gengäld också synnerligen känsliga för fördröjningar. Redan svarstider på drygt 100 ms kan uppfattas som släpigt för användaren, och tillämpningen kan bli direkt oanvändbar över t.ex. en satellitförbindelse. Terminalåtkomsten är som regel också mycket känslig för intermittens, vilket kan tvinga återstarter och förnyad påloggning av användaren.

3.2.2 Fjärrskrivbord

Med fjärrskivbord avses tjänster som överför ett grafisk presentationsgränssnitt (eventuellt också inkluderande ljud eller annan återmatning) från en dator till användarens terminal. Från användarens terminal skickas tangentbordstryckningar, pekdonsrörelser och andra typer av inmatningar.

Det finns ett mycket brett spann av olika implementationer av funktionen fjärrskrivbord, som i många fall också ställer vitt skilda krav på kommunikationsanslutningarnas kvalitetsegenskaper. I del 2, avsnitt 9.3, redogörs i detalj för de tekniska egenskaper olika produkter och implementationer besitter.

Även om flera av de kommersiellt tillgängliga produkterna för fjärrskrivbord också implementerar funktioner som filöverföring och skrivardelning, så betraktas fjärrskrivbord i detta sammanhang så som funktionen beskrivs ovan, det vill säga med syftet att förmedla in- och utmatningar till en mänsklig användare. Detta medför att fjärrskrivbord är en interaktiv tjänst enligt definitionen i inledningen till kapitel 3.

En interaktiv tillämpning

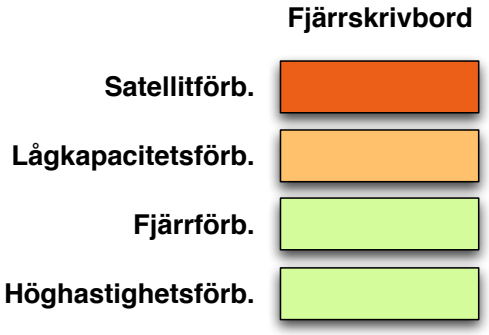
Givet denna förutsättning har tillämpning ett starkt asymmetriskt kapacitetsbehov, där den allra största mängden data flödar i riktningen nedströms mot användarens terminal. För den som redigerar och läser text kan fjärrskrivbord fungera bra med svarstider upp mot 200 ms samt en dataöverföringskapacitet på cirka 256 kbps. Generellt kan sägas att funktionen fjärrskrivbord ofta fungerar väl över höghastighetsförbindelser och fjärrförbindelser, men bör användas med stor försiktighet över lågkapacitetsförbindelser. Hur mycket interaktivitet användaren kräver av fjärrskrivbordet påverkar hur användaren märker av långa fördröjningar. Ett realisera funktionen över satellitförbindelser kan därför vara direkt olämpligt, just på grund av de höga fördröjningar som påförs vid överföringen, även om överföringskapaciteten skulle vara fullt tillräcklig.

Störningskänslighet

Funktionen fjärrskrivbord är särskilt känslig mot paketförluster och intermittens i anslutningen, både på grund av hur fjärrskrivbord normalt används, men också hur funktionen implementeras tekniskt. Korta men frekventa avbrott i anslutningen leder till ständiga återstarter där fjärrskrivbordet på nytt måste synkronisera tillståndet

med terminalen. Hela processen kan ta flera sekunder, då användaren upplever att funktionen är helt icke-responsiv.

Fjärrskrivbord har som regel också den egenskapen att de tar all tillgänglig överföringskapacitet i anspråk (upp till en viss gräns). Det medför att i situationer där överföringskapacitet är en begränsad resurs som måste delas med andra tjänster tjänster, kan fjärrskrivbord ta en oproportionerligt stor andel, vilket kan ha en negativ påverkan på andra tjänsters kvalitet.



Figur 3.2 – Förväntad användarupplevelse vid användning av fjärrskrivbord över respektive typanslutning

Figur 3.2 ger en grov bild av vilken användarupplevelse som kan förväntas vid användning av fjärrskrivbord över de olika typanslutningarna. Hur tjänsten upplevs, det vill säga hur responsiv den upplevs vara, är emellertid starkt beroende av hur användningen ser ut. Enklare användning, som t.ex. att ta del av ett meddelande eller att göra inmatningar i ett formulär, kan i vissa fall fungera mycket väl även då anslutningens överföringskapacitet är låg och har långa fördröjningar. Andra användningsfall, som t.ex. medför att stora mängder grafiska element överförs som punktmatriser, kan snabbt bli direkt oanvändbara på samma anslutning.

Upplevelsen är också avhängig vilken teknik som används för att realisera fjärrskrivbordet. Ett fjärrskrivbord där servern skickar kompletta skärmbilder utifrån användarens kommandon gör att enklare användningsfall ställer krav på hög överföringskapacitet och låg fördröjning.

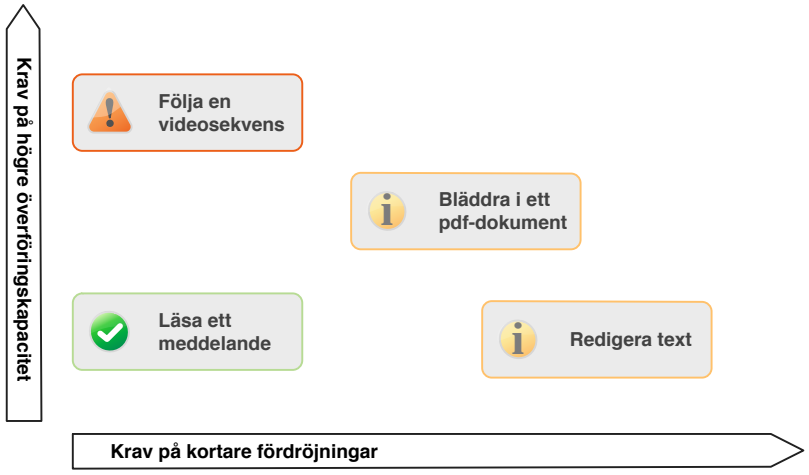
Ingående undersökningar och tester krävs för att kunna avgöra vilken teknik som är den mest lämpliga för ett visst användningsfall, och vilka kvalitetskrav detta då ställer på nätverksanslutningens egenskaper.

3.3 Transaktionsbaserade tillämpningar

3.3.1 Filöverföringar

Filöverföringar är ett typexempel på en funktion som kan realiseras på en mängd olika sätt beroende på tjänstens utformning och anslutningen kvalitet.

Filöverföringar kan sägas ligga till grund för en rad av de vanligaste tjänsterna vi använder idag. Ofta sker filöverföringen som en del av ett informationsanrop, och där



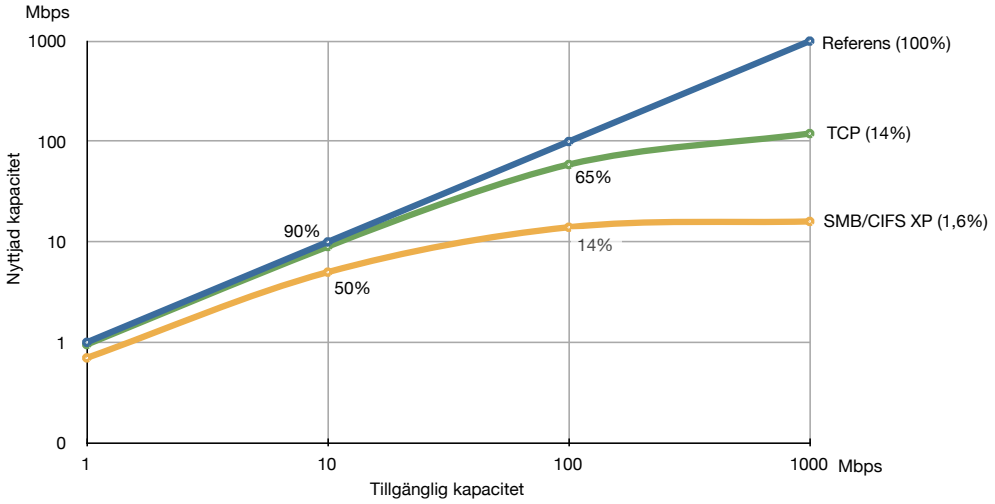
Figur 3.3 – Kvalitetskrav vid olika användningar av funktionen fjärrskrivbord

data överförs tillsammans med metainformation som t.ex. filnamn, filformat, kodning, tidstämpel, ägarskap, mm.

Val av filöverföringsmetod

Direkt åtkomst från utlokaliserade platser mot centrala resurser kan komma att kräva ett stort mått av eftertanke och varsamt val av rätt åtkomstform. Sker överföringen över långa geografiska avstånd eller över en anslutning med starkt begränsad kapacitet bör enkla åtkomstformer användas, som t.ex. HTTP.

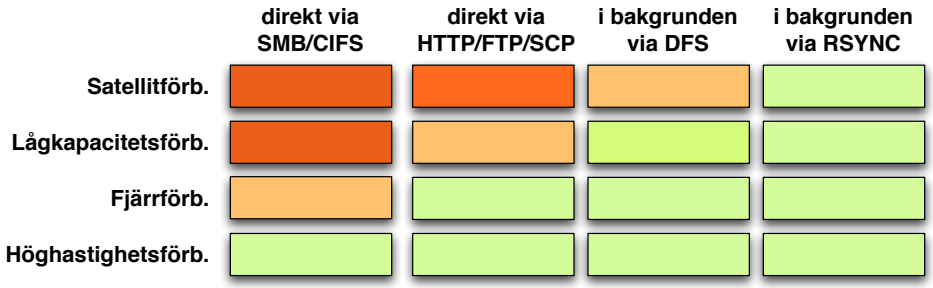
Filöverföring till särskilt avlägsna platser, t.ex. via en satellitförbindelse, kan behöva göras asynkront för att erhålla en acceptabel tjänstekvalitet. Lämpligen utformas tjänsten så att överföringen kan ske med ett filöverföringsprotokoll som har en mycket låg andel överskottsdata, låg grad av synkronism, och där överföringen kan optimeras genom att modifiera ändpunkternas TCP-parametrar. Ett sådant exempel är Rsync.



Figur 3.4 – Utnyttjandegrad av satellitförbindelse vid filöverföring med SMB/CIFS respektive TCP

En annan asynkron filöverföringstjänst är *Microsoft Distributed File System* (MS-DFS). MS-DFS använder glsSMB/CIFS som underliggande filöverföringsprotokoll, och ärver således dess känslighet mot fördröjningar, vilket kan leda till ett underutnyttjande av anslutningens kapacitet. Figur 3.4 visar vilken nyttjandegrad glsSMB/CIFS kan förväntas ha över en satellitlänk med olika kapacitet, jämfört med ett rent TCP-baserat protokoll som t.ex. Rsync [RSYNC].

De asynkrona egenskaperna i tillämpningen, att filöverföringarna sker klumpvis i bakgrunden mot de centrala resurserna, kan emellertid medföra en högre grad av användbarhet jämfört med om varje fil skulle överföras vid det tillfälle användaren behöver åtkomst. Figur 3.5 visar med en principiell indelning hur de olika användningssätten och protokollen kan tänkas fungera beroende på anslutningssätt.



Figur 3.5 – Relation mellan metoder för filöverföring och de kvalitetskrav dessa kan komma att ställa på nätverksanslutningarna

3.3.2 Databasåtkomst

Vid åtkomst till klassiska *relationsdatabaser* används protokoll som är av naturen transaktionsbaserade. Ett eller flera kommandon, ofta uttryckta i *Structured Query Language* (SQL), skickas till databasservern för bearbetning. Databasprotokollen använder som regel TCP på transportnivån, och en etablerad session används för flera påföljande transaktioner. Dessa egenskaper borgar för möjligheten att konstruera tillämpningssystem så att dessa blir relativt okänsliga för hög latens.

Det är emellertid vanligt att implementationer av tillämpningssystemen är bristfälliga i detta avseende, och endast utformade och testade för att fungera över högkapacitetsanslutningar. Effekten kan då bli att två olika tillämpningar som båda använder samma kommunikationsprotokoll, och som har likartade kapacitetsbehov, utan uppenbar anledning påverkas drastiskt olika av ökad latens.

Av denna anledning är det omöjligt att dra några allmänna slutsatser av hur databaskommunikation kan komma påverkas av de olika typanslutningarnas egenskaper, annat än att konstatera att det är möjligt att konstruera tillämpningssystem för att fungera även under mindre gynnsamma omständigheter. Tillämpningssystem måste därför noga kravställas och testas i detta avseende, då det är inte tillräckligt att göra en bedömning baserat på kommunikationsprotokollet.

3.3.3 Envägs strömmande media

Envägs strömmande media används ofta för distribution av ljud och video, både i fall där enskilda mottagare kan styra uppspelningen och där alla mottagare får samma dataström (multicast). Vanligt förekommande TV-tjänster, Internetradio och YouTube sänder dock en mediaström till varje mottagare, s.k. unicast.

Tillämpningen är ofta av karaktären att användaren begär del av en mediaström, varvid strömmen börjar skickas i den takt, med den kodning och i den kvalitet som begärts. Andra tjänster överför data i en väsentligt högre takt, eller så fort som möjligt, och liknar då mer en filöverföring.

Interaktiviteten i den här typen av tjänster är normalt mycket låg. Användaren kan styra strömmen genom att starta, stoppa och hoppa till en annan tidsposition, vilket kan signalleras genom protokollet *Real Time Streaming Protocol* (RTSP). Det vanligaste protokollet för överföring av mediaströmmar är *Real-time Transport Protocol* (RTP) över UDP. Varje RTP-paket innehåller en tidsstämpel och ett ordningsnummer, och implementationer kan därför kompensera för jitter och paket som anländer i oordning. Genom att kombinera RTP med *Real Time Control Protocol* (RTCP) så kan mottagaren informera sändaren om förutsättningarna för mottagningen, och dynamiskt anpassa kvalitet, kodning och sändningshastighet.

Mediaströmmen blir i dessa fall tämligen okänslig för såväl fördröjningar och jitter. Mängden paketförluster som kan tolereras beror på vilken typ av media som överförs, och hur den kodas och tolkas. Om mottagarsidan implementerar effektiva mekanismer för att dölja saknad information (*Packet Loss Concealment* (PLC)) kan en talström vara begriplig även med upp till 50% i paketförluster, dock med kraftigt försämrad kvalitet. För videotillämpningar är förutsättningarna sämre, då en liten grad av paketförluster

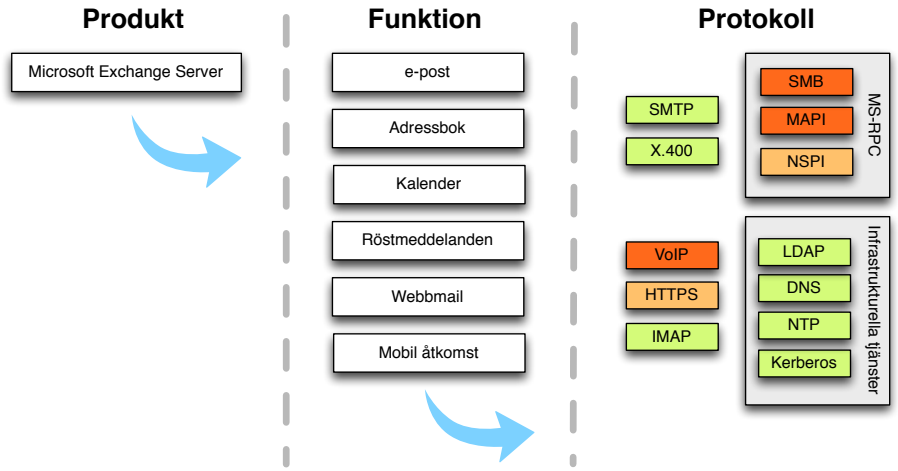
kan påverka en större andel av bildrutorna. Toleransen beror i mycket hög grad på vilken kodning som används och förmågan hos mottagaren att dölja den saknade informationen.

På det hela taget kan dock sägas att envägs strömmande media är mycket tåligt mot fördröjningar, jitter och även paketförluster. Mediaströmmens kvalitet är i första hand avhängigt av tillgänglig överföringskapacitet i riktning mot mottagaren (nedströms).

3.4 Asynkrona tillämpningar

3.4.1 Grupprogramvara

I många organisationer är funktionen grupprogramvara likställt med produkten Microsoft Exchange. Exchange är en mycket mångsidig produkt som innehåller ett stort antal funktioner och som går att integrera på en mängd olika sätt.

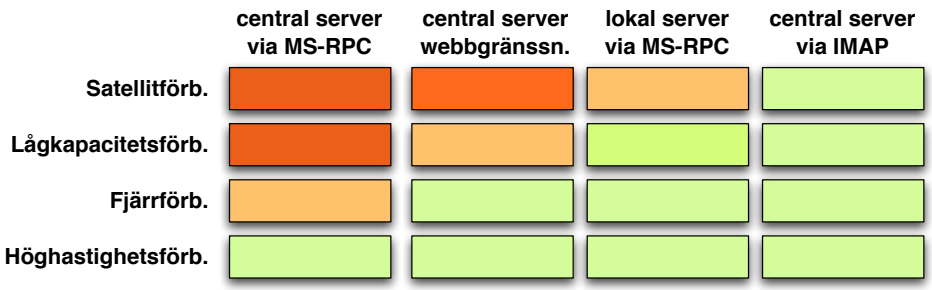


Figur 3.6 – Relation mellan en produkt, dess funktioner och de kvalitetskrav dessa kan komma att ställa på nätverksanslutningarna

Funktionerna i Microsoft Exchange går att nå genom ett flertal olika metoder; för lokala höghastighetsanslutningar används normalt *Messaging Application Programming Interface* (MAPI) över *Microsoft Remote Procedure Call* (MSRPC), för mobila enheter kan man använda Activesync, och det finns även ett webbgränssnitt för åtkomst från en generisk webbläsare.

Val av åtkomstmetod

Microsofts MAPI-protokoll är särskilt känsligt för fördröjningar, då varje operation användaren utför kräver ett stort antal turer över nätverksanslutningen. Tjänstens kvalitet kommer där med att snabbt degradera i takt med att fördröjningarna ökar och anslutningarnas kapacitet begränsas. Det kan därför vara direkt olämpligt att använda Outlook-klientens normala anslutningsmetod över t.ex. satellit- eller lågkapacitetsförbindelser.



Figur 3.7 – Exempel på hur kvaliteten för grupprogramvara beror på olika åtkomstmetoder.

En bättre åtkomstmetod kan då vara att använda webbgränssnittet eller funktionerna för mobil åtkomst. För platser med starkt begränsad kapacitet kan man välja att låta utlokalisera servrar närmare användarna, för att på så sätt förbättra upplevelsen i de mer interaktiva tjänsterna, medan servern sedan utför asynkrona överföringar av data gentemot omvärlden.

Anpassning av åtkomstmetoden efter rådande anslutningsförhållanden

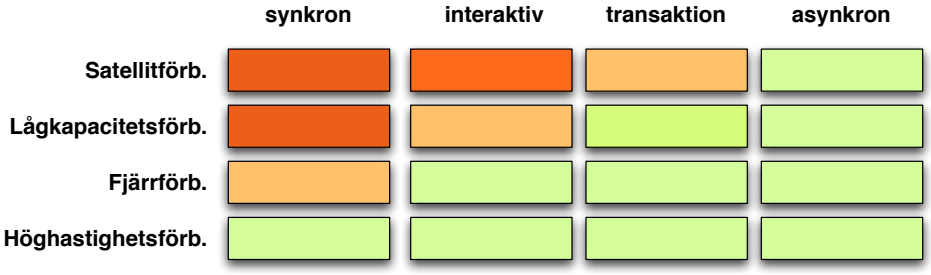
Det är emellertid också möjligt att använda en betydligt mer lättviktig åtkomstform som är konstruerad för att fungera över anslutningar med begränsad kapacitet eller som sträcker sig över stora avstånd. Ett sådant protokoll är *Internet Message Access Protocol* (IMAP) [RFC3501]. En grundtanke i konstruktionen av IMAP-protokollet är att senarelägga all överföring av data tills det verkligen behövs, och endast överföra efterfrågad data. Funktioner som gör IMAP särskilt användbart inkluderar:

- en hög grad av parallellisering där flera åtgärder kan utföras samtidigt utan att behöva vänta på att var och en ska avslutas innan nästa kan påbörjas,
- att kunna hämta delar av ett meddelande, eller t.ex. endast dess avsändare, mottagare och ämnesrad,
- server-baserade sökfunktioner, för att kunna undvika att överföra stora mängder data genom att endast behöva returnera sökresultatet till klienten.

IMAP är ett öppet standardiserat protokoll som finns implementerat i praktiskt taget alla e-postservrar, inklusive Microsoft Exchange. Figur 3.7 belyser på ett principiellt sätt vilka överväganden som kan behöva göras vid realisering av grupprogramvara på ett utlokaliserat arbetsställe, beroende på vilka anslutningsformer som finns tillgängliga.

4 Slutsats

Tillämpningarna och de IP-baserade kommunikationsprotokolletn ställer krav på den anslutning som används för att bära tjänsten. Genom att projicera olika tillämpningars krav på typanslutningarna ges en bild av hur väl en anslutning möter de krav tjänsterna ställer.



Figur 4.1 – Överensstämmelse mellan typanslutningarnas egenskaper och tillämpningars krav

Den beskrivning av tillämpningar, anslutningar och projicering av tillämpningars kvalitetskrav på olika anslutningsformer som presenterats är principiell och saknar den komplexitet som ofta finns ute i verkliga miljöer.

En sådan komplexitet är att att anslutningen ofta består av många fler lager än en den som beskrivits. Anslutningen kan byggas upp av ytterligare lager som ger olika typer av funktionalitet, som t.ex. tunnelmekanismer, komprimering och kryptering. Vissa av dessa lager är tillståndslösa, medan andra är kretskopplade och etablerar anslutningstillstånd.

Den metod som beskrivits här kan emellertid tillämpas som ett effektivt sätt att avgöra i vilken mån en djupare analys och tester behöver genomföras inför val av produkt, kommunikationsmetod, integrationssätt och anslutningsform. Det kan konstateras att fördröjning, som är en ofrånkomlig verkan av signalers utbredningshastighet, kan ha en mycket stor inverkan på tjänstekvaliteten även i välfungerande moderna kabelburna nät. En del tillämpningar kan hantera och i många avseenden kompensera för försämrade förhållanden, medan andra degraderar drastiskt även vid förhållandevis blygsamma försämringar.

Generellt kan också sägas att en tillämpning som konstruerats och dimensionerats för att fungera över den mest begränsande anslutningsformen, alltid kommer att kunna användas i andra sammanhang där anslutningarna har bättre egenskaper. Däremot gäller inte det omvända.

Del 2

Fördjupning

5 Radiobaserade anslutningar

Samtliga av de olika typanslutningarna kan realiseras genom radioteknik, men kan, beroende på en rad omständigheter, förväntas leverera olika kvalitetsegenskaper i olika situationer. Detta avsnitt syftar till att belysa dessa omständigheter i fall som rör några typiska användningsområden.

5.1 Trådlösa lokalnät

Med trådlösa lokalnät avses utrustning formellt undantagen från tillståndsplikt i enlighet 3 kap. §§ 125, 130 och 132. i PTSFS 2012:3[ptsfs-2012-3].

I den svenska frekvensplanen tillåts radioanläggningar för dataöverföring med bandspridningsteknik ("RadioLAN") som uppfyller kraven i EN 300 328 v1.8.1 (2012-04)[etsi-en-300-328], EN 301 893 v1.7.0 (2012-01)[etsi-en-301-893] eller motsvarande krav, att använda följande frekvensband:

- 2 400 – 2 483,5 MHz (del av S-bandet)
- 5 150 – 5 350 MHz (del av C-bandet)
- 5 470 – 5 725 MHz (del av C-bandet)

I föreskrifterna ställs krav på att total utstrålad effekt, *Equivalent Isotropically Radiated Power* (EIRP) – ekvivalent isotropiskt utstrålad effekt begränsas, samt att utrustningen implementerar så kallad bandspridningsteknik.

Bandspridningsteknik innebär att signalen delas upp i segment som fördelas över ett frekvensband som är bredare än den enskilda bärvågen. För mottagning krävs att en synkroniserad spridningssignal finns tillgänglig. Bandspridningsteknik har bl.a. till fördel att signalen blir mindre sårbar för interferens.

Följande är exempel på olika bandspridningstekniker:

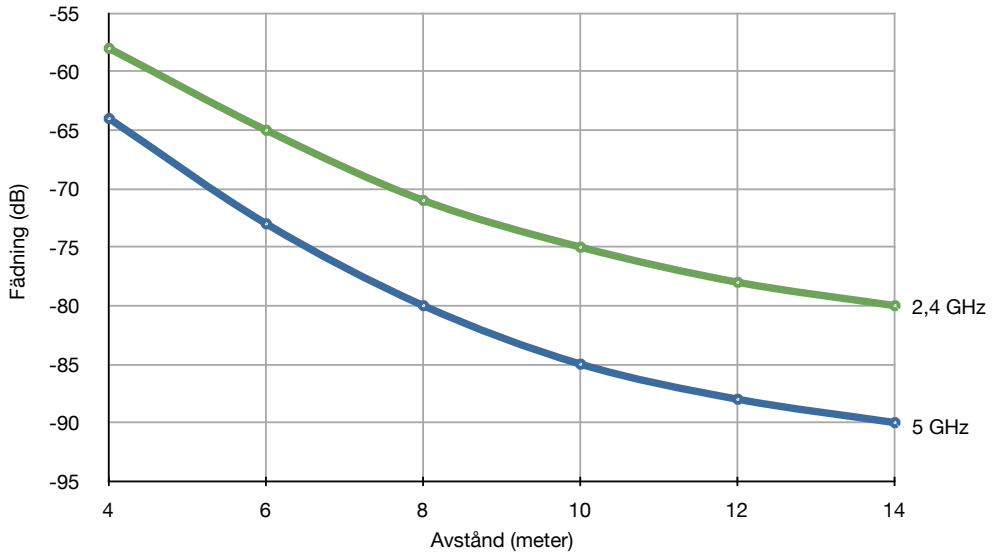
- *Frequency-Hopping Spread Spectrum* (FHSS) är en metod där data sänds i korta skurar åtföljda av ett skenbart slumpmässigt kanalbyte. De regulatoriska kraven på FHSS är att frekvensbandet skall delas in i minst 15 kanaler, och utrustningen får sända på en kanal i maximalt 40 ms innan byte sker.
- *Direct-Sequence Spread Spectrum* (DSSS) är en metod där datasignalen överlagras på en skenbart slumpmässig "brus-signal" med mycket högre frekvens än datasignalen själv. Därmed sprids signalen över ett bredare frekvensband. Bruset filtreras bort i mottagaren för att erhålla den rena datasignalen.

- *Orthogonal Frequency-Division Multiplexing* (OFDM) är en komplex metod där data delas upp och kodas på flera närliggande bärvågor i frekvensspektrat. Dessa är noggrant ordnade så att där en bärvåg har sin vågtopp är alla andra noll och bidrar på så sätt inte till vågformen.

För radioanläggningar i S-bandet gäller att maximal ekvivalent isotropiskt utstrålad effekt (EIRP) begränsas till 100 mW.

För radioanläggningar i C-bandet gäller emellertid ytterligare restriktioner enligt EN 301 893 v1.7.0 (2012-01)[etsi-en-301-893]. I det undre frekvensbandet får utrustning endast användas inomhus då det bl.a. finns risk för interferens med radionavigering för luftfart, och med en maximal ekvivalent isotropiskt utstrålad effekt (EIRP) av 200 mW. I det övre frekvensbandet finns dock möjlighet att använda uteffekten 1 W (EIRP).

Den högre tillåtna effekten kompenserar i någon mån det faktum att effekterna av fädning är mer påtagliga i 5 GHz-banden [WIFIFADING]. I figur 5.1 visas hur skillnaderna i fädning mellan de två frekvensbanden i en typisk kontorsmiljö, där signalen alltså obstrueras av väggar, inredning och andra föremål. Skalan på x-axeln skulle kunna variera högst avsevärt beroende på miljö, och det är i första hand skillnaderna mellan de två kurvorna som är relevant i diagrammet. Av de redovisade skillnaderna i diagrammet kan ca 3 dB kompenseras genom den högre uteffekt som tillåts, och som de flesta utrustningar är kapabla till.



Figur 5.1 – Effekter av fädning i 2.4 GHz-bandet jämfört med 5 GHz-bandet

Ekvivalent Isotropiskt Utstrålad Effekt (EIRP)

EIRP används som ett jämförelsetal för att ange en begränsning i den maximala effekt som en antenn får utstråla i någon riktning. Jämförelsen baseras på en perfekt isotropisk antenn som har förmågan att stråla med samma intensitet i alla riktningar.

Gränsvärdet som anges innebär att huvudloben i den aktuella antennen aldrig får stråla mer i någon riktning än den isotropiska skulle gjort, givet den totalt utstrålade effekten.

Effekten anges ofta i watt eller som skillnaden i decibel mellan en referenseffekt och den utstrålade effekten, t.ex. dBm (referenseffekten 1 mW).

Det krävs också att all utrustning som tillverkas för att användas i C-bandet implementerar funktionalitet för att detektera och undvika interferens med radarsystem – *Dynamic Frequency Selection* (DFS). DFS-funktionen behövs emellertid inte för de första 5 kanalerna i det undre bandet, d.v.s. 5 150 – 5 250 MHz.

Myten om mikrovågsugnen och vattenmolekylens egenfrekvens

Mikrovågsugnars magnetroner genererar radiofrekvent energi på S-bandet (mer specifikt 2,45 GHz). En vanlig missuppfattning är att denna frekvens skapar resonans hos vattenmolekylen eftersom den ligger nära dess egensvängningsfrekvens. Detta är en myt. Hade så varit fallet hade S-bandet varit fullständigt oanvändbart för radiokommunikation eftersom den elektromagnetiska energin hade absorberats av luftfuktigheten. Istället är det vattenmolekylens dipolära natur som får vattenmolekylen att svänga med det alternerande elektriska fält som mikrovågorna skapar. Vattenmolekylens egenfrekvens är betydligt högre (22,2 GHz).

5.1.1 IEEE 802.11

Arbetsgruppen 802.11 inom *Institute of Electronics and Electrical Engineers* (IEEE) har definierat de i princip allenarådande standarderna för trådlösa lokalnät.

Den grundläggande standarden och ramformatet för 802.11 skiljer sig inte radikalt från IEEE 802.3 (Ethernet). Man har låtit ärva ner egenskaperna från Ethernet och tillämpa dessa på radiolänkar. Det finns emellertid avgörande skillnader. Radiovågor breder ut sig på ett inte alltid förutsägbart sätt och interfererar. Det finns en konstant överföringskapacitet som måste delas mellan alla noder på kanalen, och när en nod sänder, måste alla andra noder på kanalen lyssna.

Traditionellt när trådbundet Ethernet använts i en kollisionsdomän (t.ex. bussnät eller stjärnnät sammankopplat med enkelt nav, *hub*), så har metoden att bryta ner nätverket i flera segment sammankopplade av en växel (*switch*) kunnat tillämpas. I trådlösa nätverk är detta inte möjligt, eftersom mediat (radiospektrat) förblir delat.

Radiomediat kräver därför en mekanism för att *undvika* kollisioner snarare än att detektera (och sända om), i syfte att möjliggöra ett effektivt utnyttjande och en hög mättnadsgrad av varje cell. Därför används i trådlösa lokalnät *Carrier Sense Multiple Access/Collision Avoidance* (CSMA/CA) istället för *Carrier Sense Multiple Access/Collision Detect* (CSMA/CD). En annan grundläggande skillnad är att i 802.11 används positiv bekräftelse av varje enskild ram som sänds över mediat. I det fall fel uppstår vid överföring av nätverksramar sker omsändning då bekräftelsen uteblir.

Mediaåtkomst

Grundläggande i arkitekturen för 802.11 är att enheterna tillämpar ett konkurrensbaserat sätt att nå tillgång till mediat. Detta sker genom att klienterna väntar en slumpmässig tidsrymd efter den senaste ramen som överförts i kollisionsdomänen, och den klient som slumpade fram den kortaste tidrymden blir den som får sända härnäst. Denna grundläggande metod kallas *Distributed Coordination Function* (DCF) och är den som traditionellt tillämpas.

I det fall det krävs att klienterna ges tillgång till mediat på ett koordinerat och icke-distribuerat sätt används en central koordineringsfunktion kallad *Point Coordination Function* (PCF). Denna funktion är integrerad i basstationen. Standarden kräver inte att PCF finns i alla produkter som stöder 802.11-gränssnittet, och är därför kompatibel med DCF.

För att PCF skall nå prioritet över DCF används konsekvent en kortare tidsrymd mellan ramarna med PCF än DCF. PCF bygger på att basstationen hämtar data från klienterna i tur och ordning och kan närmast jämföras med markör-baserade nätverksteknologier (t.ex. Token Ring). Nackdelen med PCF är att tiden för överföring av överskottsdata ökar markant inom kollisionsdomänen, och effektivitetsgraden sjunker.

Standarden 802.11e specificerar en hybridversion (HCF) för att medge flera olika tjänsteköer och balanserad tillgång till mediat, utan den rigorösa kontrollen som PCF medför. Detta gör att realtidstillämpningar kan ges företräde framför mindre tidskritiska tjänster. Delar av HCF ska finnas implementerade i produkter märkta med Wi-Fi Alliance *Wi-Fi Multimedia Extentions* (WMM).

Dataöverföringskapacitet

Dataöverföringskapaciteten i trådlösa lokalnät beror på ett flertal faktorer, vilka i huvudsak är:

Bandbredden eller kanalbredden, som vanligen är 20 MHz eller 40 MHz, men kan vara upp till 160 MHz (802.11ac). I 2,4 GHz-bandet används i praktiken uteslutande 20 MHz breda kanaler för att möjliggöra ett effektivt utnyttjande av frekvensbandet.

Moduleringen är det som avgör hur många bitar som kan moduleras per symbol på bärvågen. Förekommande modulering är binär fasskiftmodulering (BPSK), BPSK i kombination med amplitudskiftmodulering (ASK) eller

IEEE	Årtal	Frekvensband	Bandbredd	Kapacitet	Modulering
802.11	1997	2 400 – 2 483,5 MHz	20 MHz	$\leq$ 2 Mbps	FHSS, DSSS
802.11a	1999	5 150 – 5 350 MHz 5 470 – 5 725 MHz	20 MHz	$\leq$ 54 Mbps	OFDM
802.11b	1999	2 400 – 2 483,5 MHz	20 MHz	$\leq$ 11 Mbps	CCK
802.11g	2003	2 400 – 2 483,5 MHz	20 MHz	$\leq$ 54 Mbps	OFDM
802.11n	2008	2 400 – 2 483,5 MHz 5 150 – 5 350 MHz 5 470 – 5 725 MHz	40 MHz	$\leq$ 150 Mbps	OFDM + MIMO
802.11ac	2012	5 150 – 5 350 MHz 5 470 – 5 725 MHz	160 MHz	$\leq$ 866 Mbps	OFDM + MIMO

Tabell 5.1 – IEEE 802.11, standarder för trådlösa lokalnät

kvadraturamplitudmodulering (QAM). Den i dag vanligaste förekommande moduleringen i trådlösa lokalnät är QAM.

Förhållandet mellan signalstyrkan och bakgrundsbruset och utrustningens förmåga (känslighet) att urskilja signalen ur bruset.

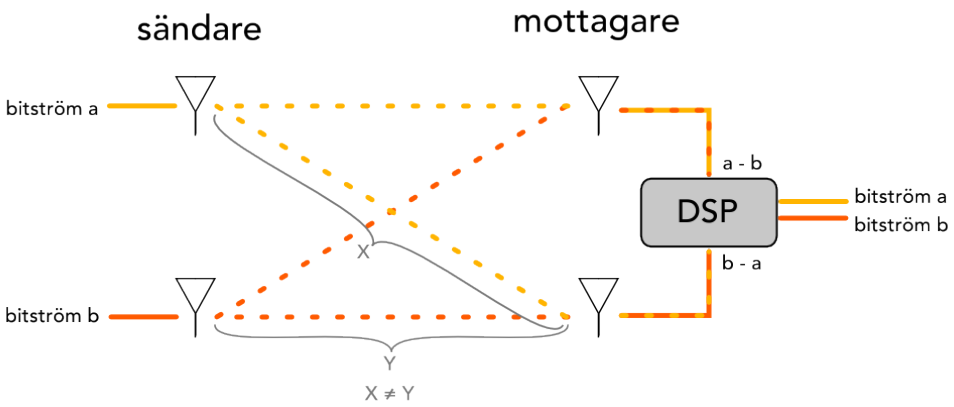
Graden av interferens från annan utrustning som använder samma frekvensband.

Användningen av så kallad MIMO-teknik för att koordinera flera sändar- och mottagarenheter och därmed upprätta flera spatiella kanaler som kan användas parallellt vid överföring av data (“spatiell multiplexering”, se figur 5.2) samt lobformning i syfte att förbättra signal/brus-förhållandet i den punkt där mottagaren befinner sig.

Merparten av den utveckling som skett i förbättrad dataöverföringskapacitet har skett dels genom att öka kanalbredden samt genom att införa MIMO. Som jämförelse kan nämnas att 802.11n med en spatial kanal och 20 MHz kanalbredd ger 80 Mbps, jämfört med 802.11a/g, som alltså erbjuder 56 Mbps.

Tabell 5.1 visar utvecklingen av 802.11, de olika standarderna och vilken teoretisk linjeöverföringskapacitet de erbjuder. För standarder som använder MIMO-teknik anges kapaciteten per spatiell dataström. I fallet med 802.11n är det vanligt att utrustningen använder två spatiella dataströmmar, och att utrustningen därför specificeras kunna erbjuda 300 Mbps i teoretisk linjeöverföringskapacitet.

Det skall också understrykas att den teoretiska högsta linjeöverföringskapaciten inte är densamma som den effektiva dataöverföringskapaciteten. Kontrollmekanismerna för mediaåtkomst och felkorrektion tar omkring 40% av kapaciteten i anspråk, och lämnar således runt 60% för effektiv dataöverföring under optimala förhållanden.



Figur 5.2 – MIMO - Spatiell multiplexering

Cellplanering

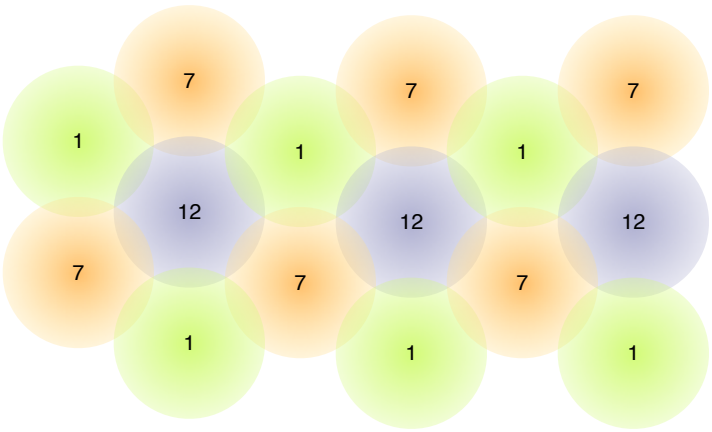
Avgörande för ett erhålla ett stabilt och effektivt trådlöst lokalnät är cellplaneringen. Vid cellplaneringen görs en kravinsamling beträffande täckningsgrad och kapacitet, varefter lokalernas och områdets beskaffenhet bedöms för att avgöra basstationernas placering, antennkonfiguration, uteffekt och vilka kanaler som ska användas.

För att kunna tillgodose kapaciteten för många klienter inom ett begränsat område kan cellindelningen i det trådlösa lokalnätet behöva krympas och göras tätare med fler basstationer. För att minska problem med samkanalinterferens kan basstationernas uteffekt behöva reduceras. Detta påverkar även stabiliteten i positiv mening, i det fall en basstation slutar fungera kan övriga basstationer fylla hålet genom att öka effekten tills dess att den trasiga basstationen blivit utbytt.

I 2,4 GHz-bandet är kanalplaneringen och undvikande av samkanalinterferens särskilt viktig, då det endast ryms tre icke-överlappande 20 MHz-kanaler i frekvensbandet. Detta är också orsaken till att 40 MHz breda kanaler är direkt olämpliga att använda i 2,4 GHz-bandet. Figur 5.3 illustrerar principen för planering av 20 MHz breda kanaler i 2.4 GHz-bandet.

Kanal	Huvudfrekvens	Frekvensband	Överlappande kanaler
1	**2,412 GHz**	**2,400 – 2,422 GHz**	**1 – 3**
2	2,417 GHz	2,405 – 2,427 GHz	1 – 4
3	2,422 GHz	2,410 – 2,432 GHz	1 – 5
4	2,427 GHz	2,415 – 2,437 GHz	2 – 6
5	2,432 GHz	2,420 – 2,442 GHz	3 – 7
6	2,437 GHz	2,425 – 2,447 GHz	4 – 8
7	**2,442 GHz**	**2,430 – 2,452 GHz**	**5 – 9**
8	2,447 GHz	2,435 – 2,457 GHz	6 – 10
9	2,452 GHz	2,440 – 2,462 GHz	7 – 11
10	2,457 GHz	2,445 – 2,467 GHz	8 – 12
11	2,462 GHz	2,450 – 2,472 GHz	9 – 13
12	2,467 GHz*	2,455 – 2,477 GHz	10 – 13
13	**2,472 GHz***	**2,460 – 2,482 GHz**	**11 – 13**

* ETSI. Endast tillgängliga i Europa.



Figur 5.3 – Exempel: kanalplanering av celler i 2,4 GHz-bandet

Distributionssystemet

Distributionssystemet är det nätverk som knyter samman basstationerna med omvärlden. I vissa fall kan även distributionssystemet använda radiogränssnitt. Mer vanligt är emellertid att ett trådbundet distributionsnät som en integrerad del i den befintliga nätverksinfrastrukturen.

Det är naturligtvis viktigt att distributionssystemet dimensioneras för att kunna hantera det hela antalet basstationer som finns installerade, och att det under full belastning inte stör den trådbundna kommunikationen.

Mobilitet

Mindre distributionssystem kan vara ett och samma datalänknät. Inom detta datalänknätverk hanteras överlämning mellan basstationerna (“roaming”, dvs. förflyttning av klient mellan basstationer) i enlighet med 802.11-standarden. Den basstation som f.n. har associationen med klienten kommer att plocka upp datapaketen från distributionssystemet och förmedla till klienten.

Består distributionssystemet av flera datalänknät, måste funktioner på högre nivå implementeras för att sköta överlämningen. Dessa högnivåfunktioner medger som regel inte tillräckligt snabb överlämning för strömmande media, som t.ex. röstsamtal. Dessutom krävs ytterligare programvara i den mobila klienten.

5.1.2 Centraliserade trådlösa nätverk

Centraliserade trådlösa nätverk definieras som en metod för att knyta samman ett närmast godtyckligt antal distribuerade basstationer (“trådlösa termineringspunkter”) för nätåtkomst till en centraliserad kontrollpunkt. Målen är bl.a. följande:

Centraliserad administration. Administration av autonoma basstationer blir snabbt en svår börda att hantera för de flesta organisationer, även för relativt begränsade trådlösa lokalnät.

Minskad komplexitet i basstationen. genom att implementera ett minimum av funktioner. I ett centraliserat trådlöst nätverk delas som regel funktionerna för datalänkkontroll (MAC) mellan det centraliserade kontrollsystemet och basstationen så att basstationen endast utför realtidsfunktioner.

Sömlös överlämning utan stöd av mjukvara i klienten. Mobilitet i 802.11 fungerar bara så länge distributionssystemet är litet nog att rymmas på ett och samma datalänknätverk (ofta Ethernet).

För att lösa detta används i centraliserade trådlösa nätverk tunnelteknik för att skicka datalänkramarna över IP till en central termineringspunkt. Denna termineringspunkt är samma oavsett vilken basstation en klient är ansluten till.

Stöd för mobilitet. Strömmande media över trådlösa nätverk kräver korta överlämningstider mellan basstationer. Överlämning mellan basstationer kan koordineras och ske på bråkdelen av en sekund (ofta några få tiondelar av en sekund).

Koordinering av effekt- och kanalplanering i realtid. Central koordinering av alla basstationer möjliggör dynamisk effekt- och kanalplanering i realtid vilket kan ha stor betydelse för tillgängligheten och stabiliteten.

Distribuerad nätövervakning. I produkter för administration av centraliserade trådlösa lokalnät finns ofta avancerade funktioner för övervakning av driftmiljön samt detektering av störningar och interferens.

Positionering. Genom den centraliserade kontrollen blir det möjligt att positionera enheter inom nätverkets täckningsområde.

Tillgänglighetsaspekter

Standarden 802.11i definierar kryptografiskt skydd på datalänknivå mellan klienten och basstationen. Skyddet upprättas genom att använda 802.1X för autentisering och nyckelutbyte (eller genom en på förhand utdelad nyckel, *Pre-shared key* (PSK)).

De kryptografiska åtgärderna ger förutom konfidentialitetsskydd, även skydd mot förfalskning, manipulation samt återuppspelning av data som skickas över länken. Det kryptografiska skyddet gäller emellertid bara datapaket – kontrollramar skickas utan något skydd.

Datalänknivån är därvid sårbar för många relativt enkla tillgänglighetsangrepp. Mer sofistikerade angrepp skulle kunna innefatta en modifierad klient som exploaterar den konkurrensbaserade åtkomstmetoden genom att simulera en överfull kanal, och därigenom stoppa all trafik. Slutligen går det även att störa ut det trådlösa lokalnätet med hjälp av en störsändare.

Dessa omständigheter, tillsammans med det faktum att det existerar en mängd tillämpningar som oavsiktligt kan påverka de trådlösa lokalnätens kvalitet och tillgänglighet, gör att den trådlösa infrastrukturen bör betraktas som ett komplement i verksamhetskritiska tillämpningar.

5.2 Mikrovågslänkar

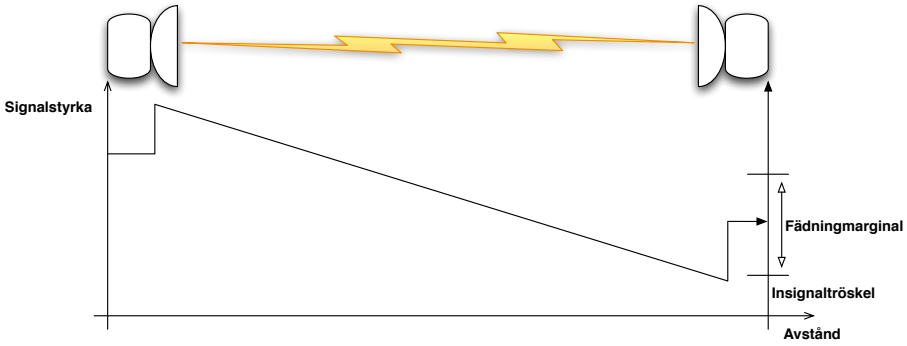
Mikrovågslänkar används för att skapa trådlösa punkt till punkt-förbindelser mellan två platser. En förbindelse kan bestå av flera mikrovågslänkar, där varje del benämns som ett länkhopp. Kapaciteten för mikrovågslänkar varierar från omkring 2 Mbps upp till flera Gbps, och kommunikationen använder vanligen frekvensband från 5 GHz upp till 60 GHz.

På grund av den väsentligt större dämpningen som radiosignalen utsätt för vid högre frekvenser används länkar som verkar i de högre frekvensbanden för kortare avstånd, omkring 2 till 3 km. För längre avstånd används därför vanligen länkar som verkar i frekvensområden på under 10 GHz. Länkhopp kräver väsentligen fri sikt, och jordens krökning sätter därmed gränser för avståndet på ett länkhopp. Även om avstånd på upp till 10 mil är möjliga, används sällan i praktiken hopp längre än 20 till 30 km.

Radiogränssnittet

Figur 5.4 visar hur signalstyrkan i ett länkhopp kan förväntas variera med avståndet. Signalen ut från sändaren förstärks av antennen innan signalen lämnar sändande part. Signalstyrkan minskar sedan successivt, i huvudsak med ökat avstånd, fram till mottagarens antenn. Mottagarantennen ger även den en förstärkning vilken till slut ger den insignalstyrka mottagaren tar emot.

För ett länkhopp finns det en undre insignaltröskel under vilken mottagaren får mycket svårt att återskapa trafiken i den mottagna signalen. För ett givet länkhopp finns även en maximal gräns för hur stark insignalen kan bli. Den dämpning som signalen utsätts för kallas för *fädning* och skillnaden mellan övre och undre signalgräns ger den marginal för påverkan av fädningseffekter som länkhoppet



Figur 5.4 – Signalstyrkans påverkan av antennförstärkning och avståndet

besitter. Marginalen kallas *fädningsbudget*. Det förekommer två huvudsakliga typer av fädning som påverkar mikrovågskommunikation:

Platt fädning är fädning som beror på nederbörd. Vattendroppar absorberar radiosignaler vilket dämpar radiosignalen och dämpningen varierar normalt långsamt över tiden. Högre frekvenser utsätts generellt för större absorption.

Flervägsfädning (*"Multipath fading"*) beror på att delar av radiosignalen studsar och reflekteras mot olika fysiska ytor på vägen. De reflekterade radiovågorna och huvudloben har då färdats olika lång sträcka. När signalerna kombineras i mottagarens antenn interfererar de reflekterade radiovågorna med huvudloben. Om de reflekterade radiovågorna är ur fas tar radiovågorna ut varandra och det sker en *utsläckning*. En signal som studsar påverkas även av en fasvridning på 180 grader, vilket ökar utsläckningen.

Flervägsfädning varierar snabbt över tiden. Går signalen över en sjö kan reflektionerna variera än mer. Om det uppstår inversionsskikt i luften kan radiosignalen även studsa på skiktgränsen.

Det kan även bildas luftskikt som leder bort signalen. Även detta ger upphov till relativt snabbt varierande fädning. För hopp över långa avstånd används höga master, men ökad höjd medför också större problem med luftskikt.

Storleken på fädningsmarginalen bestäms i samband med planering av länkhoppet och utifrån kapacitet, tillgänglighet samt väderdata (så kallad regndämpningsindex) samt information om andra lokala förutsättningar. I de fall störningar och paketförluster ändå uppkommer kan ett antal olika åtgärder behöva vidtas i syfte att förbättra kvaliteten:

Reducerat avstånd är den viktigaste parametern för signalstyrkan mellan sändare och mottagare. Att minska avståndet är ett säkert sätt att förbättra fädningsbudget, men kan alltså kräva fler länkhopp för anslutningen.

Sänkt bärfrekvensen minskar länkhoppets känslighet för regn, men kan samtidigt minska länkhoppets maximala överföringskapacitet.

Ökad antennförstärkning ger en snävare lob med högre fältstyrka, men leder ofta till att större antenner måste användas. Större antenner ger även ett större vindfång och vinden kan påverka antennens riktning.

Adaptiv modulation innebär att den modulation av informationen som bärs av utsignalen varierar beroende på den rådande signalmiljön. När signalförhållandet är gynnsamt används en avancerad modulation som ger hög överföringkapacitet. När signalförhållandena försämras används modulationer där energin i utsignalen används för att skicka färre bitar information per tidsenhet, och som möjliggör att mottagaren lättare kan särskilja informationen från bruset. Om adaptiv modulation används medför det således att mikrovåglänkens överföringskapacitet kan variera över tiden.

Antenndiversitet genom att komplettera länkhoppet med ett andra antennpar placerade ett antal halva vågländer bortom det första paret. Antenndiversitet är en robust men kostsam lösning för att hantera flervägsfädning.

Polarisation används som ett sätt att öka överföringskapaciteten i ett länkhopp genom att sända två kanaler samtidigt med 90 graders polarisation. Men polarisation kan även användas för att skapa redundans eller att att motverka väderberoende fädningseffekter. Vertikal polarisation påverkas mindre av platt fädning.

Länklager

Traditionellt har mikrovågslänkar använts för att transportera tidssynkrona protokoll som *Plesiochronous Digital Hierarchy* (PDH) och *Synchronous Digital Hierarchy* (SDH). Även om dessa protokoll fortfarande används är moderna mikrovågslänkar paketorienterade och använder ofta Ethernet som gränssnittsprotokoll. Modern utrustning för att realisera en mikrovågslänk implementerar vanligen en rad funktioner som syftar till att kunna optimera utnyttjandet av mikrovågslänken:

Felkorrektion som ger mottagaren möjlighet att kompensera för fel i den mottagna signalen och undertrycka störningar.

Trafikprioritering med stöd för att klassificera och prioritera trafik utifrån prioritetsinformation i Ethernet-, MPLS- eller IP-lager.

Protokollkomprimering I syfte att ge ökad överföringskapacitet och förbättrad tillgänglighet.

5.3 LTE

LTE är efterföljaren till standarderna *Global System for Mobile Communications* (GSM) och *Universal Mobile Telecommunications System* (UMTS) för mobilsystem. En viktig skillnad mellan *3GPP Long Term Evolution* (LTE) och tidigare mobilsystem är att LTE inte separerar telefon/rösttrafik och datatrafik på samma sätt som tidigare mobilsystem.

I GSM och UMTS (3G) finns en särskild så kallad kretskopplad domän, som ger fix dataöverföringskapacitet och en synkron transport mellan terminal och basstation för just telefonitrafiken. Datatrafik i GSM och UMTS hanteras i en separat paketbaserad domän.

I LTE säkerställs istället kvalitetskraven för telefoni genom prioritering av den paketförmedlade trafiken utifrån definierade trafikklasser. Standarden *Voice over LTE* (VoLTE), vilken bygger på *IP Multimedia Subsystem* (IMS) som definierar specifika trafikprofiler för kontrolltrafik respektive olika typer av datatrafik.

Utifrån trafikmodeller specificeras i LTE den teoretiska kapaciteten nedströms från basstationen till upp till 300 Mbps, (75 Mbps i motsatt riktning), samt ned till 10 ms fördröjning inom operatörsnätet. Ytterligare fördröjningar kan tillkomma för anslutning mellan operatören och kundens resurser, t.ex. via Internet. Radiospektrat i operatörens celler är emellertid en resurs som vanligen delas mellan operatörens abonnenter. Detta i kombination med att de rådande förhållandena för radiokommunikationen kan variera avsevärt gör att kapacitet i nätet sällan eller aldrig kan garanteras, varvid LTE kan antas i de flesta fall kategoriseras som en fjärrförbindelse.

6 Kodning och trafikprioritering

6.1 Komprimering

Komprimering används för att reducera mängden data som en tjänst behöver överföra. Det finns tre huvudtyper av komprimering: datakomprimering med och utan informationsförlust, samt protokollkomprimering.

6.1.1 Datakomprimering med informationsförlust

Vid datakomprimering med informationsförlust kastas delar av informationen i kommunikationen permanent bort. Vilken del som kastas bort styrs av en modell som tolkar informationen. Ett exempel på komprimering med informationsförlust är talkodare i IP-telefoni som filtrerar bort ljud som bedöms inte behövas för att mottagaren ska förstå den som talar. Talkodaren GSM-FR [GSMFR] utvecklades för att komprimera talkanalen i GSM, men används även för att komprimera tal i IP-baserad röstkommunikation. GSM-FR ger en datatakt på 13 kbps.

Vissa komprimeringsmetoder med informationsförlust ger även upphov till en variabel datatakt. Detta innebär att datatakten ut varierar beroende på informationen i det som komprimeras. OPUS [RFC6716] är ett exempel på en talkodare som kan ge variabel datatakt.

Datakomprimering med informationsförlust används även för att reducera mängden data i olika typer av filer. Exempel på denna användning är ljudformatet *MPEG-1 or MPEG-2 Audio Layer III* (MP3) [MP3] och bildformatet JPEG [JPEG].

Datakomprimering med informationsförlust kan i vissa fall införa tillstånd i anslutningen, t.ex. vid överföring av strömmande video. Kodningar som MPEG-4 överför skillnaden mellan bildrutor, vilket medför ett beroende mellan bilderna och därmed de paket som transporterar paketen.

6.1.2 Datakomprimering utan informationsförlust

Vid komprimering utan dataförlust sker en kodning av informationen som minskar mängden redundans i den digitala representationen av informationen. Kodningen är dock helt reversibel och informationen går att återskapa exakt. Exempel på datakomprimering utan informationsförlust är:

Variabel bitkodning. De symboler (tecken) som data består av har oftast en fix representation, vanligen 8 bitar per symbol. Variabel bitkodning innebär att längden på kodningen av en symbol beror av hur frekvent symbolen förekommer

i dataströmmen. Ju mer frekvent desto kortare kod. Ett exempel på variabel bitkodning är *Huffmankodning*.

Mönsterkodning. Sekvenser, mönster av olika tecken som förekommer mer än gång i dataströmmen ersätts med en hänvisning till tidigare observerade instanser av sekvensen. Ett exempel på mönsterkodare är algoritmen DEFLATE som bland annat används i WAN-acceleratorer samt i *Transport Layer Security* (TLS) och *Internet Protocol Security* (IPsec).

För samtliga metoder för komprimering utan informationsförlust sker en överföring av tillståndsinformation från sändare till mottagare, som används av mottagaren för att återskapa överförd data. Om tillståndsinformationen förloras eller förvanskas vid överföringen kommer inte avkodningen att ske på ett korrekt sätt. Konsekvenserna av förlorade paket kan även bli större med komprimering då en större del av orginaldata kan påverkas eller förloras. Metoder för komprimering utan informationsförlust behöver även bearbeta en del data innan de börjar bli effektiva. Exempelvis måste DEFLATE bearbeta antal sekvenser för att ha något att hänvisa till. Om komprimeringsalgoritmen frekvent måste startas om minskar därför komprimeringens effektivitet.

Det finns inte heller någon algoritm för komprimering utan informationsförlust som kan garantera några reduktioner i datastorlek. Vid datakomprimering finns det ett antagande om fördelningar av symboler som inte är likafördelad, eller att det finns mönstermässig redundans som går att utnyttja. Stämmer inte dessa antaganden blir effekten att komprimeringen inte ger någon reduktion, och kan till och med leda till att datamängden ökar. Data som krypterats med ett väl fungerande krypto innehåller inga mönster eller symbolfördelningar som en algoritm för datakomprimering utan informationsförlust kan utnyttja.

Komprimering och dekomprimering tar en viss tid, men tiden är jämförelsevis liten och och sker ofta när sändande eller mottagande part väntar in andra händelser. Exempelvis kan komprimering ske samtidigt som data läses in från ett lagringsmedia eller i samband med att data som ska skickas serialiseras för att stämma med den fysiska anslutningens datastorlek. Eftersom komprimering minskar mängden data som behöver överföras minskar istället den totala fördröjningen och komprimering förbättrar ofta en tjänst responsivitet.

6.1.3 Protokollkomprimering

Protokollkomprimering handlar om att försöka reducera den kapacitet som krävs för de strukturer och informationsfält (protokollhuvuden) som följer med i paketen vid överföringen av data med hjälp av olika protokoll. Delar av dessa strukturer, t.ex. IP-versionsnumret eller IP-adressen för sändaren och mottagaren, ändras sällan eller på ett på ett förutsägbart under en session. Några exempel på protokollkomprimering är Van Jacobson TCP/IP header compression [RFC1144] och *Robust Header Compression* (ROHC). ROHC används frekvent i mobilsystem som ett sätt att reducera det behov av överföringskapacitet som uppstår på grund av många lager av enkapsuleringar och har stöd för ett antal olika pakettyper, t.ex. *User Datagram Protocol* (UDP), *Real-time*

Transport Protocol (RTP), IPsec samt *Internet Protocol version 6* (IPv6). ROHC innefattar även olika metoder för att säkerställa att tillstånden i sändare och mottagare är synkrona, även om anslutningens kvalitet varierar.

Med protokollkomprimering betraktas inte enskilda paket som oberoende från andra paket. Istället jämförs paket i en sekvens med varandra och bara skillnaden mellan paketen skickas över till mottagaren. Detta innebär att tillstånd etableras mellan paketen. Om ett paket försvinner måste mottagaren antingen kunna återskapa rätt tillstånd själv, eller förmå sändaren att återskapa korrekt tillstånd.

Protokollkomprimeringsmetoderna innebär att innehållet i IP-paketen under överföring faktiskt bryter mot protokolldefinitionerna. En förmedlingsnod som inte stödjer protokollkomprimering och som analyserar de fält som komprimerats kommer därmed betrakta paketen som felaktiga, och kassera dem. Däremot kan komprimerade paket tunnlas och där i transporteras av underliggande anslutningar. MPLS kan t.ex. användas för att transportera IP-trafik som komprimerats med ROHC.

6.2 Kryptering

Det finns ett stort antal standarder och metoder för att kryptografiskt skydda kommunikation som transporteras över en nätverksanslutning, så kallade transportkrypton. Den kryptografiska skyddsmetoden är oftast transparent för tillämpningen, men metoden kan ändå påverka anslutningens egenskaper. Exempelvis kan kryptering påföra fördröjning och minska den effektiva överföringskapaciteten. Skyddsmetoden kan därför påverka tillämpningars förutsättningar att fungera tillfredsställande.

För att etablera en skyddad anslutning sker mellan parterna normalt först en initieringsfas där parternas identitet bekräftas, parterna kommer överens om vilka mekanismer och algoritmer som ska användas för att skydda kommunikationen samt utbyte av de krypteringsnycklar som ska används under det att den skyddade kommunikationen pågår. Denna initeringsfas kan ske manuellt, med stöd av separata mekanismer eller vara en integrerad del av transportkryptot.

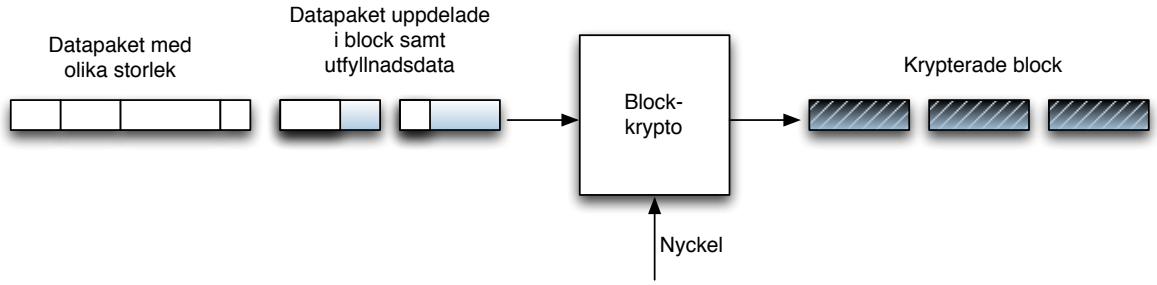
Initieringsfasen kan i vissa fall ta relativt lång tid i anspråk och kräva flera rundor av utbyten av meddelanden mellan parterna. Om initieringsfasen frekvent måste startas om kan den negativa påverkan i fördröjning, effektiv överföringskapacitet och därmed tjänstens kvalitet bli betydande.

Efter initieringsfasen vidtar en transportfas där data kryptografiskt transformeras innan överföring sker. I denna fas används normalt någon form av symmetriskt krypto. I ett symmetriskt krypto används samma nyckel för att kryptera och dekryptera informationen. Det finns två huvudtyper av symmetriska krypton – blockkrypton och strömkrypton.

Blockkrypto

Blockkrypton är funktioner som givet en nyckel transformerar ett datablock. Datablocket kryptot transformerar har en fix storlek, normalt 8, 16 eller 32 oktetter. För data vars storlek inte är jämnt delbar med blockstorleken måste blocken fyllas ut med extradata. Blockkrypton ger därför en expansion av mängden data som ska överföras.

För tjänster med små men frekventa datapaket kan expansionen medföra märkbara kapacitetsförluster. Ett exempel på denna typ av tjänst är IP-telefoni. Där skickas korta men frekventa datapaket, vilket gör att även små kontrollfält ger en stor relativ ökning av kapacitetsbehovet.



Figur 6.1 – Blockkrypto kräver att datapaket delas upp i block med fix storlek

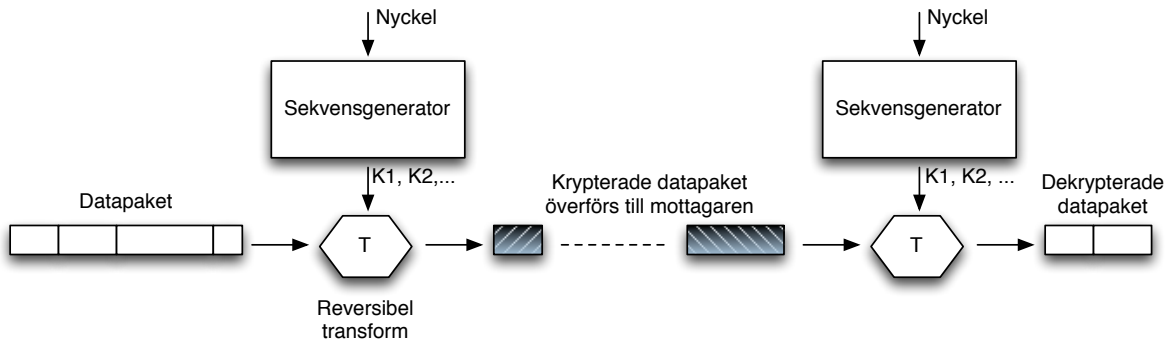
Att blockkrypton är funktioner innebär att de inte har något minne, samma nyckel och samma datablock ger alltid samma transformerade resultat. För att motverka detta beteende används alltid blockkrypton i någon slags kryptometod som skapar ett interntillstånd. Samtidigt ställer kryptometoden krav på ett definierat starttillstånd kallad *Initialvektor* (IV).

För att mottagaren ska kunna dekryptera ett meddelande måste starttillståndet på något sätt överföras från sändaren till mottagaren. Denna överföring kräver viss överföringskapacitet. Om sessionerna är korta kan mängden initialvektorer, och därmed mängden överskottsdata, bli betydande. Protokollet *IEEE MAC Security* (MACsec) använder t.ex. en IV baserad på innehållet i befintliga kontrollfält för att undvika denna påverkan. Protokollet IPsec däremot skickar med en IV varje paket.

Strömkrypto

Strömkrypton består i huvudsak av en sekvensgenerator. Givet ett startvärde, ett frö, skapar generatorn en sekvens skenbart slumpmässiga värden. Men generatorn är deterministisk och givet samma frö genereras därför alltid samma sekvens av värden. Generatorn är därmed en *Pseudo Random Number Generator* (PRNG). De genererade värdena används i tur och ordning för att transformera dataelement i det data som ska överföras. Strömkrypton genererar normalt nyckelvärden med samma bitlängdsmässigt maximal storlek som dataelementen. Detta innebär att strömkrypton inte ger någon dataexpansion.

Mottagaren använder samma sekvensgenerator för att efter överföring återtransformera överförd data. För att återtransformationen ska fungera måste mottagarens sekvensgenerator vara i fas med sändarens generator. Strömkrypton är därför känsliga för fel och den underliggande transportmekanismen måste kunna garantera att paket överförs och kommer i rätt sekvens. Det finns strömkryptoalgoritmer kapabla att återhämta sig efter fel, men om det använda strömkryptot ej stödjer detta måste sessionen startas om.



Figur 6.2 – Strömkrypto där sändarens och mottagarens sekvensgeneratorer måste vara synkroniserade

Beroenden mellan sändare och mottagare

Att sändare och mottagare måste vara i fas med varandra är ett exempel på de beroenden som upprättas mellan sändare och mottagare vid kryptering. Protokoll som MACsec och IPsec skapar inget beroende mellan två på varandra följande paket. Protokollet TLS däremot kan även införa beroenden mellan enskilda paket. Ett beroende mellan paket och segment ställer krav på att underliggande transport på ett bra sätt hanterar förluster av paket. Om inte förluster hanteras kan de beroenden kryptot inför få påverkan på tjänsten. Ett krypto som skapar beroenden mellan datapaket, och därför kräver stöd för omsändningar, kan därmed leda till att paket som inte längre är relevanta för tjänsten ändå måste skickas om.

Kapacitets- och kvalitetskrav

Den kryptografiska behandlingen kommer oundvikligen att ta viss tid i anspråk i den aktuella utrustningen, på samma sätt som tunnelteknik påför fördröjningar. Däremot kan val av t.ex blockkrypto kontra strömkrypto ge olika stor fördröjning.

Kryptering ställer även vissa kapacitetsmässiga krav på ändutrustningen. Speciellt om den ena parten tillhandahåller en tjänst till många samtidiga användare kan kraven bli betydande. Samtidigt bör det understrykas att kraven för de flesta typer av tillämpningar och anslutningar hanteras väl av moderna standarddatorer. För en tjänst som tillhandahåller högkvalitativ video till tusentals användare kan kraven på kryptokapacitet bli viktig, medan kraven för en mer normal webbaserad tjänst är marginella i sammanhanget.

Kryptering kan även öka åtgången av dataöverföringskapacitet. Skälet till detta, förutom eventuell expansion för att möta specifika blockstorlekar, är de kontrollfält som måste läggas till i datapaket för att kunna tolka och verifiera skyddet.

För att kompensera för ökad åtgång av dataöverföringskapacitet appliceras ofta datakomprimering på den trafik som ska överföras, innan krypteringen vidtas. Komprimeringen innebär även att fördröjningen genom utrustningen minskar och kan kompensera för den fördröjning krypteringen tillför.

6.3 Klassificerings- och prioriteringsmekanismer

I IP-protokollet finns ett informationsfält, *Differentiated Services* (DS), där sändaren kan ange en av flera prioritetsnivåer för respektive paket. Fältet används enligt standarden *Differentiated Services* (DiffServ) [RFC2474].

För länklager byggda med virtuella lokalnät, *Virtual Local Area Network* (VLAN), enligt Ethernetprotokollen 802.1Q, finns en del av VLAN-fältet kallat *Priority Code Point* (PCP). PCP möjliggör en grovkornig uppdelning av trafiken i olika trafikkategorier. Ethernetstandarden 802.1ad innebär att det finns två separata PCP-fält, ett för varje VLAN. Standarden *Metro Ethernet* använder Ethernets prioritetsfunktioner för att skapa anslutningstjänster enligt olika tjänsteavtal, *Service Level Agreement* (SLA).

Ett exempel där prioritet används är i moderna paketbaserade mobilsystem – *Mobile Backhaul* (MBH). I dessa nät ska både rösttrafik och datatrafik transporteras mellan basstationer, till och från bryggor mot Internet och andra externa nät. Dessutom behöver mobilnäten för sin funktion även transportera kontrollinformation, status, larm samt distribuera tid för synkronisering av basstationer. Genom indelning av trafik i olika tjänsteklasser och sedan använda protokollens prioritetsmekanismer garanteras att trafik för synkronisering och larm alltid transporteras före all annan trafik. Vidare får den trafik som bär samtalstrafiken alltid högre prioritet än ren datatrafik.

6.4 WAN-acceleration

En typ av utrustning som används i försök att förbättra användbarheten hos tjänster samt minska behovet av överföringskapacitet kallas WAN-acceleratorer. WAN-acceleratorer arbetar i par och skapar ett slags tunnel över vilken tjänsternas trafik flödar. En WAN-accelerator använder flera olika metoder för att reducera och eliminera delar av trafiken innan den skickas genom tunneln. Några av de vanligaste metoderna innefattar:

Temporär mellanlagring (*caching*). Genom att analysera trafiken identifieras dataobjekt som skickas över anslutningen. Dessa objekt lagras och när ett mellanlagrat objekt efterfrågas behöver inte förfrågan skickas över anslutningen.

Eliminering av kopior (*deduplication*). Multipla överföringar av samma objekt ersätts med referenser till den första förekomsten.

Datakomprimering. WAN-acceleratorer använder datakomprimering utan informationsförlust för att reducera mängden data som skickas. För att öka effektiviteten i komprimeringen appliceras den på all trafik över anslutningen, inte på separata strömmar. En effekt av detta är att oberoende strömmar kan komma att kopplas till varandra. Ett förlorat paket påverkar därmed flera strömmar.

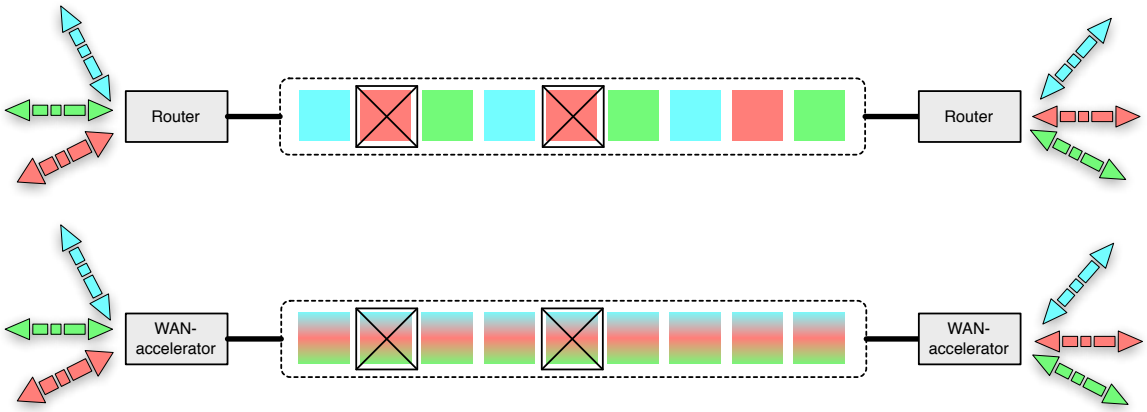
Protokollkomprimering. WAN-acceleratorer reducerar eller eliminerar informationsfält som olika kommunikationsprotokoll använder för sin funktion. Informationsfälten återskapas av WAN-acceleratorn innan paketen lämnar WAN-acceleratorns tunnel.

Protokolloptimering. WAN-acceleratorerna övervakar och genom ompaketering samt skapande av nya paket kan påverka olika protokolls funktion. Ett exempel är protokollet *Common Internet File System* (CIFS), vilket skickar små men frekventa paket där en WAN-accelerator kan slå samman flera CIFS-paket till ett större paket.

Härmning (*spoofing*). WAN-acceleratorer kan protokollmässigt härma enheter. Ett exempel är WAN-acceleratorer som i förväg bekräftar TCP-segment som skickas över WAN-anslutningen. WAN-acceleratorns bekräftelser döljer därmed WAN-anslutningens responstid för den sändande parten. En effekt av detta är att måste WAN-acceleratorn måste också själv kunna hantera de återsändningar av de TCP-segment den i förväg bekräftat.

Felkorrektion. WAN-acceleratorn applicerar felkorrektion för trafiken över anslutningen och kan därmed reducera mängden paket som behöver skickas om.

Klassificering och prioritering. Genom att indela olika strömmar i trafikklasser och sedan ge klasserna olika prioritet kan WAN-acceleratorn ge vissa tjänster en bättre upplevelse. Detta på bekostnad av andra tjänster som delar anslutningen.



Figur 6.3 – Till skillnad från en router slår en WAN-accelerator samman flera anslutningars strömmar till en gemensam ström. Förlust av ett paket kan därför komma att påverka flera strömmar.

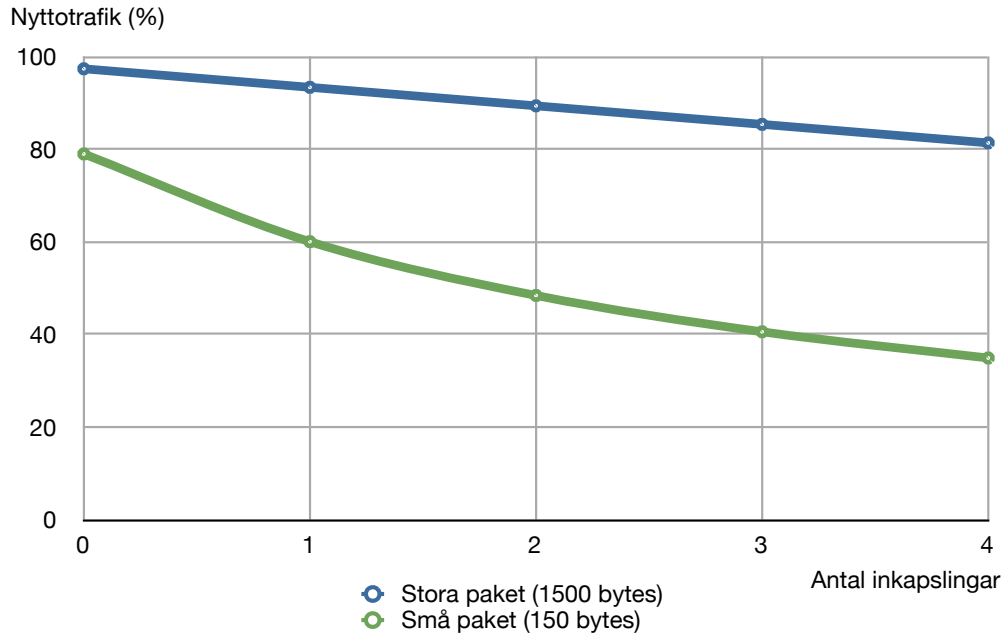
WAN-acceleration kan förbättra tjänsteupplevelsen när anslutningar med begränsad överföringskapacitet används och till viss del även reducera påverkan av lång fördröjning. WAN-acceleratorn påverkar trafiken och inför nya tillstånd i nätverket och kan även skapa beroenden mellan annars oberoende trafikströmmar. För vissa typer av trafik, t.ex. trafik som är krypterad, ger WAN-acceleratorer oftast marginell förbättring.

7 Tunnelmekanismer

7.1 Generellt om inkapslade anslutningar

En given anslutning kan av olika anledningar behöva transporteras över en annan anslutning. Den transporterade anslutningen kapslas in och sägs *tunnla* över den transporterande anslutningen.

Skälen till tunnling kan vara flera. Den underliggande anslutningens fysiska eller logiska egenskaper kan fordra att en tunnelmekanism tillämpas, t.ex. för att kunna uppfylla erforderliga säkerhetskrav eller för att kunna överföra ett visst ramformat (datalänkprotokoll). I situationer då den underliggande anslutningen levereras som en kommunikationstjänst snarare än en fysisk anslutning, är det vanligt att det redan existerar underliggande lager av inkapslingar på den faktiska fysiska anslutningen. Staplande av flera tunnelmekamismer (inkapslingar) påverkar den effektiva överföringskapaciteten och riskerar att mynna i en avsevärd kvalitetsförsämring.



Figur 7.1 – Nyttjandegrad hos TCP av underliggande kapacitet vid inkapslade anslutningar

Varje inkapsling får till följd att anslutningens effektiva överföringskapacitet minskar, eftersom inkapslingarna påför ytterligare överskottsdata. Behandlingen av detta överskottsdata, det vill säga in- och urkapsling på var sida om anslutningen, påför också ytterligare fördröjningar. Minskningen av effektiv överföringskapacitet är därför inte heller helt linjär.

Exempeldiagrammet i figur 7.1 visar hur lager av inkapslingar påverkar de effektiva överföringsakapaciteten för *Transmission Control Protocol* (TCP) över en lokal höghastighetsförbindelse med 100 Mbps (blå) samt en fjärranslutning med samma kapacitet (grön). Estimeringen utgår från inkapslingar av typen *Internet Protocol Security* (IPsec), och ett antagande att varje in- och urkapsling påför 0,5 ms fördröjning, vilket är en rimlig siffra för mindre avancerade routrar och brandväggsystem. Diagrammet ska läsas som en fingervisning i hur inkapsling generellt kan komma påverka tjänstekvaliteten. I en verklig situation med flera lager av inkapslingar består dessa sannolikt av olika inkapslingmetoder och format, och effekterna av dessa kan skilja sig från de som anges i diagrammet.

Det är också troligt att kvaliteten i den slutliga tjänsten påverkas på ett mer märkbart sätt än ren TCP-överföring. Ett exempel är filöverföringar med Microsofts fildelningsprotokoll SMB/CIFS eller tjänster med hög interaktivitet.

Resultatet av tunnelmekanismers påverkan på tillämpningars kvalitet kan sammanfattas i att ju lägre fördröjning anslutningen har, desto större blir påverkan på kvaliteten när man påför tunnelmekanismer. En tunnel över en höghastighetsanslutning ger mycket större påverkan än en tunnel över en satellitanslutning.

7.2 Transporterande tunnelmekanismer

En transporterande tunnelmekanism har som primärt syfte att transportera ett kommunikationsprotokoll över en annan anslutning. Det finns flera skäl att använda den här typen av tunnelmekanismer:

- Transportera en typ av trafik över en annan typ av anslutning och nät än vad den transporterade trafiken rent tekniskt är anpassad för. Ett enkelt punkt-till-punkt-protokoll kan tunnlas över ett eller flera nät baserade på *Internet Protocol* (IP).
- Konvergera flera separata kommunikationstekniker mot en gemensam kommunikationstyp. Inom mobiltelefonisystem är det vanligt att mobilnätstrafiken för flera generationer av system transporteras med ett gemensamt IP-baserat nät över Ethernet. *Global System for Mobile Communications* (GSM) är baserat på *Time Division Multiplexing* (TDM), *Universal Mobile Telecommunications System* (UMTS) på *Asynchronous Transfer Mode* (ATM) och *3GPP Long Term Evolution* (LTE) på *Internet Protocol version 6* (IPv6). Det gemensamma nätet behöver därför kunna möta kraven från synkron och asynkron trafik samt flera olika protokoll.
- Tillföra egenskaper som modifierar trafiken eller anpassar den till anslutningens egenskaper på delar av eller hela vägen mellan sändare och mottagare,

t.ex. genom att förbättra utnyttjandegraden av överföringskapaciteten genom komprimering.

Detta avsnitt behandlar de transporterande tunnelmekanismerna, vars primära syfte inte är att påföra ett säkerhetslager, till skillnad från de krypterande tunnelmekansismer som behandlas närmare i avsnitt 7.3.

7.2.1 GRE

General Routing Encapsulation (GRE) [RFC2784] är ett enkelt paketbaserat tunnelprotokoll. I första hand används det för att transportera andra nätverksprotokoll över ett IP-nät. GRE kan även användas för att transportera IP-trafik över ett IP-nät så att mellanliggande routrar ej hanterar de tunnlade paketen.

GRE-huvudet kräver i grundutförande 4 oktetter extra för varje paket. Det finns även en utökning av GRE [RFC2890] som introducerar två 32-bitars fält, nyckel[1] samt paketnummer. I GRE-huvudet anges (genom Ethernet-typ) vilken typ av trafik som transporteras i paketet. Detta gör det möjligt att transportera Ethernet, IP, MPLS och många andra protokoll över IP.

GRE är en tillståndslös anslutning. Det är upp till ändpunkterna för GRE-tunneln att övervaka att den fungerar. Även om utökningen av GRE inför paketnumreering och ID-nummer för strömmen, så finns det inget beroende mellan paketen. GRE erbjuder heller inget skydd av informationen i den tunnlade trafiken. Om detta krävs kan GRE kombineras med IPsec i transportläge.

7.2.2 L2TP

Layer Two Tunneling Protocol (L2TP) [RFC3931] är ett protokoll för att skapa virtuella datalänknät över IP-baserade nätverk. L2TP-trafiken inklusive L2TP-huvudet transporteras som en UDP-ström. L2TP är i sig en utökning av protokollet *Point-to-Point Protocol* (PPP) och den trafik som L2TP transporterar kapslas in i virtuella PPP-anslutningar.

Den ena av de kommunicerande parterna – kallad *L2TP Access Concentrator* (LAC) – initierar tunneln. Den andra parten – kallad *L2TP Network Server* (LNS) – inväntar förfrågningar från en LAC om att etablera en tunnel. Den tunnel som etableras mellan en LAC och en LNS är dubbelriktad, och den information som krävs för att upprätthålla tillståndet mellan LAC och LNS skickas som kontrollpaket i samma UDP-ström som nyttotrafiken.

Precis som GRE erbjuder L2TP inget skydd av informationen i den tunnlade trafiken. Istället kan IPsec används för att påföra skyddsmekanismer.

Layer Two Tunneling Protocol - Version 3 (L2TPv3) är en utökning av L2TP som ger L2TP funktionalitet för att kunna transportera Ethernet, Frame Relay och en mängd andra typer av anslutningar och protokoll utan att dessa behöver packas in i PPP.

[1] Nyckelfältet är inte en kryptografisk nyckel utan ett identitetsnummer för paketströmmen.

7.2.3 CES

Circuit Emulation Service (CES) är en standard från *Metro Ethernet Forum* (MEF) [MEF3] som specificerar hur synkron, tidsmultiplexerad trafik (TDM), t.ex. *Plesiochronous Digital Hierarchy* (PDH) och *Synchronous Digital Hierarchy* (SDH), ska kapslas in och transporteras över ett IP-baserat nät. Detta gör det t.ex. möjligt att transportera trafik från GSM-baserade mobilsystem tillsammans med paketbaserad trafik för LTE.

CES ställer krav på att den totala fördröjningen genom nätet från CES-ingress till CES-egress är låg. Kravet är en fördröjning på maximalt 25 ms och ett jitter på maximalt 10 ms. CES ställer även krav på mängden bitfel och anslutningens tillgänglighet.

För att kunna mata ut TDM-trafik i rätt takt och eliminera jitter sker buffring på egress-sidan. Den TDM-klocka som kan detekteras på ingress-sidan överförs till egress-sidan och används sedan för att mata ut TDM-trafiken i rätt takt. Därmed kan en gemensam tidsdomän upprätthållas mellan TDM-anslutningarna på respektive sida av CES-tunneln.

Även om utrustningen över en länk stöder CES direkt, är CES-trafiken i sig troligen tunnlad. Exempelvis sker detta med *Packet over SONET/SDH* (POS) [RFC2615], *Multi Protocol Label Switching* (MPLS) [RFC3031], men även passiva optiska nät t.ex. *Ethernet Passive Optical Network* (EPON) [IEEE8023AH] kan användas.

En konsekvens av de krav på fördröjning, jitter och tillgänglighet CES ställer är att tjänstekvalitetsmekanismer, *Quality of Service* (QoS), ofta används som ett sätt att möta kvalitetskraven. Om nätet inte är dimensionerat för att klara belastningen kan den samtrafik som transporteras över nätet tillsammans med CES-trafiken prioriteras ned och därmed påverkas av ökad fördröjning och sämre tillgänglighet.

7.2.4 Ethernet över SDH

För lokala högshastighetsförbindelser används i dag i princip uteslutande Ethernet som länklager. Ethernet används även allt mer som länklager även för andra typer av förbindelser, t.ex. fjärrförbindelser. När geografiskt skilda lokalnät, *Local Area Network* (LAN), ska anslutas till varandra är det vanligt att detta sker på ett sådant sätt att näten blir delar av ett gemensamt Ethernetbaserat länklagernät. Mellan lokalnäten transporteras Ethernetramar över olika typer av anslutningar.

Att transportera Ethernet över ett synkront fjärranslutningsprotokoll som SDH ger en förutsägbar tjänst med kort fördröjning, låg varians i paketfördröjning och samt stabil dataöverföringskapacitet. Vid transport av Ethernet över SDH används ofta ett mellanliggande ramprotokoll, t.ex. *Generic Framing Procedure* (GFP) [G7041].

Genom att transportera Ethernet över SDH erhålls funktioner för provisionering samt styrning och övervakning av trafik. Ethernet över SDH underlättar och förbättrar möjligheten att konstruera feltoleranta anslutningar med hög tillförlitlighet – feldetektering och automatisk överkoppling av trafik sker i SDH på under 50 ms.

7.2.5 Tillståndslösa protokoll över TCP

Synkrona och interaktiva tjänster ställer höga krav på anslutningens realtidsegenskaper. Vid IP-baserad telefoni är det t.ex. viktigt att röstdata i huvudsak kommer fram med tillräckligt låg fördröjning. Ett enskilt paket med röstdata som anländer för sent är inte längre användbart. Enstaka paket som försvinner, kommer försent eller som förvanskats under överföringen är oftast ett hanterbart problem.

Transportprotokollet *User Datagram Protocol* (UDP) är ett enkelt, tillståndslöst protokoll som i sig självt inte stöder omsändningar av paket. UDP har genom sin låga andel överskottsdata också en minimal inverkan på den effektiva överföringskapaciteten. För IP-telefoni med många små datapaket är låg andel överskottsdata viktig och UDP möter därför tjänstens krav väl. Protokollet *Real-time Transport Protocol* (RTP) [RFC3550] som ofta används för att överföra realtidsdata som IP-telefoni och andra typer av strömmande media, använder därför UDP som transportprotokoll.

För tjänster som filöverföring är det desto viktigare att alla paket kommer fram och att de inte har förvanskats under transport. För dessa tjänster är TCP, med dess interntillstånd för att hantera omsändningar och dynamisk anpassning till anslutningens beteende, som regel ett bättre alternativ.

Vid tunnling av trafik över TCP kommer tjänster som använder tillståndslös transport att få transport med tillstånd. Ett exempel på detta är när IP-telefoni transporteras över t.ex. ett *Secure Sockets Layer Virtual Private Network* (SSL-VPN).

Tester visar att så länge som anslutningen har bra kapacitet och med låg fördröjning medför transport av IP-telefoni över *Secure Sockets Layer* (SSL) inga problem. Det kan till och med förbättra upplevelsen av tjänsten. Skälet till detta är att TCP hinner med att hantera omordning eller omsändning av paket inom tjänstens realtidskrav. Resultatet är färre överföringsfel än vid UDP.

Då fördröjningen ökar eller då den tillgängliga dataöverföringskapaciteten minskar kan inte TCP hantera felmängden och samtidigt möta realtidskraven. TCP kommer därvid fortsätta med omsändningar, men för tjänsten är de omsända paketen redan förlorade och förbrukar bara onödig överföringskapacitet. Vidare kommer TCP-parametrarna att anpassas till anslutningens kapacitet, och reducera den effektiva överföringsakapacitet tjänsten och dess tillståndslösa transportprotokoll tilldelas. Resultatet är att när fel börjar uppstå, så leder TCP:s egenskaper snabbt till försämringar i tillämpningen.

7.2.6 TCP över TCP

Att transportera TCP över TCP innebär att en TCP-anslutning används som underliggande anslutning för andra TCP-baserade tillämpningar. Ett vanligt förekommande exempel är när s.k. SSL-VPN används för att bära tjänster som HTTP, fjärrskrivbord eller terminalåtkomst.

TCP är ett transportprotokoll med internt tillstånd som upprättas vid start av sessionen. Via statusmeddelanden synkroniseras tillståndet mellan sändare och mottagare under sessionens livslängd. Interntillståndet gör det möjligt för sändaren

att upptäcka fel i överföringen. TCP-implementationen skickar om de paket som försvunnit samt reglerar den takt med vilken paketen skickas iväg. Interntillståndet gör det även möjligt för mottagaren att sortera paket som anländer i oordning.

Ett exempel på en av de dynamiska tillståndsparametrar som TCP-implementationen justerar under anslutningens varaktighet är tidsgränsen för mottagarens bekräftelse av ett paket. När ett paket inte i tid bekräftats av mottagaren antar sändaren att paketet försvunnit och skickar om paketet. Sändaren ökar även tidsgränsen för att mottagaren ska bekräfta ett paket och reducerar sändningstakten.

Vid TCP över TCP kan den underliggande TCP-sessionens anpassning vid omsändning hindra den överliggande TCP-sessionen att skicka paket och ta emot bekräftelser. Detta leder till att den överliggande TCP-sessionen får ökat behov av omsändningar och reducerad sändningstakt. Det fenomen som kan uppstå är ett snabbt eskalerande problem för den överliggande sessionen med extremt långa tidsgränser och sammanbrott i transporten av trafik. Fenomenet kallas *TCP meltdown*.

TCP över TCP som används över anslutningar med lång fördröjning och låg dataöverföringskapacitet, t.ex. satellitanslutning, är särskilt känsliga för fenomenet.

Det finns tekniker som motverkar fenomenet genom att modifiera hur TCP hanterar omsändningar och justering av dynamiska parametrar. Två exempel på dessa tekniker är TCP *Selective ACK* (SACK) [RFC2018] och *Proportional Rate Reduction for TCP* (PPR) [PPR]. Ett annat sätt är att helt enkelt inte transportera TCP över TCP, utan att istället använda sammankopplade TCP-anslutningar.

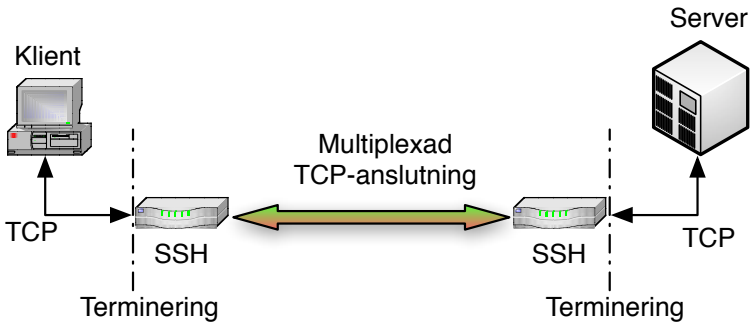
7.2.7 Sammankopplade TCP-anslutningar

Till skillnad från TCP över TCP innebär sammankopplade TCP-anslutningar, *TCP back to back*, att en TCP-anslutning tar vid där föregående slutar. Exempel på användning av sammankopplade TCP-anslutningar är *port forwarding* i *Secure Shell* (SSH) [RFC4251] och *SOCKS Protocol Version 5* (SOCKS5) [RFC1928].

En TCP-anslutning från en klient som ska transporteras med SSH termineras av SSH-noden på klientsidan. Innehållet i klientsidans TCP-anslutning lyfts över till den TCP-anslutning som skapats mellan SSH-noderna på klientsidan och serversidan. SSH-noden på serversidan lyfter i sin tur över innehållet till den TCP-anslutning som kopplar samman noden med servern.

Fördelen med sammankopplade TCP-anslutningar är bland annat ett högre kapacitetsutnyttjande, men också att man undviker problemen med de överlagrade interntillstånd som uppstår vid TCP över TCP. I vissa fall kan det emellertid vara en nackdel att det inte är ett och samma TCP-tillstånd mellan sändare och mottagare.

Värt att notera är att innehållet från flera TCP-anslutningar som transporteras över SSH inte behöver innebära flera separata SSH-anslutningar. Innehållet från de olika TCP-anslutningarna kan istället transporteras över en gemensam SSH-anslutning. SSH ansvarar för att kombinera (multiplexera) innehållet från de olika strömmarna till en gemensam ström inför transport. På mottagarsidan delar SSH upp strömmen av innehåll för de olika strömmarna och skickar ut dessa som separata TCP-anslutningar. En liknande teknik som fungerar på motsvarande sätt och används för att snabba upp webbtrafik, men som går att applicera för TCP-sessioner generellt, är *Speedy* (SPDY)



Figur 7.2 – TCP-anslutning mellan klient och server termineras och multiplexeras över SSH.

[SPDY].

7.3 Krypterande tunnelmekanismer

7.3.1 MACsec

IEEE-standarden 802.1AE [IEEE8021AE] kallad *IEEE MAC Security* (MACsec) definierar en skyddsmetod på länklagernivå. MACsec erbjuder en Ethernetbaserad länk med kryptografiskt konfidentialitets- och integritetsskydd.

MACsec definierar ett nytt ramformat samt krav på hur en säker sammankoppling, en *Secure Association* (SA), ska skapas och upprätthållas. MACsec är ett protokoll som beskriver hur Ethernetramar ska bearbetas utifrån de parametrar som överenskommits mellan parterna. Däremot innefattar MACsec inte några mekanismer för parterna att förhandla fram vilka parametrar att använda.

De parametrar som används, t.ex. krypteringsnycklar, definieras och förhandlas istället fram mellan parterna med hjälp av andra mekanismer och protokoll. Exempel på protokoll som kan användas för att etablera sammankopplingen är IEEE 802.1X [IEEE8021X].

Den huvudsakliga påverkan på trafiken som MACsec påför är att den totala ramstorleken ökar med upp till 32 oktetter. Detta innebär att den totala effektiva dataöverföringskapaciteten minskar något, typiskt i storleksordningen 2%. MACsec kan även medföra ökade ramförluster över anslutningar med hög felfrekvens, och där sannolikheten för att en dataram överförs intakt minskar med ramens storlek.

Att bearbeta en ram i enlighet med MACsec tar en viss tid och ger därmed en viss fördröjning. Den specificerade maximala fördröjningen som godkänd MACsec-utrustning får påföra anslutningen är 4 gånger tiden det tar att överföra en ram på 64 oktetter över det fysiska mediat. För Gigabit Ethernet innebär det en fördröjning på 0,5 μs.

Denna fördröjning gäller för en av ändpunkterna i en anslutning. För en överföring mellan två ändpunkter blir den extra fördröjningen således det dubbla. För en anslutning som består av flera fysiska eller logiska länkar måste varje ändpunkt räknas.

Att etablera eller återstarta en sammankoppling tar tid eftersom nya nycklar ska förhandlas fram. Nyckelförhandlingen får maximalt ta 0,1 sekunder. Dock ska förhandlingen kunna ske samtidigt som föregående SA är i bruk. Byte av SA och därmed nycklar ska kunna ske från en ram till nästa utan att trafiken påverkas.

Parameter	**Tillåtna värden**
Ändpunkts fördröjning vid sändning	< sändningstiden vid maximal ramstorlek + 4 gånger sändningstiden för en 64 oktetter stor ram
Ändpunkts varians i fördröjning vid sändning	< ändpunkts fördröjning vid sändning
Ändpunkts fördröjning vid mottagning	< sändningstiden vid maximal ramstorlek + 4 gånger sändningstiden för en 64 oktetter stor ram
Ändpunkts varians i fördröjning vid mottagning	< ändpunkts fördröjning vid mottagning
Fördröjning vid upprättande av säker sammakoppling	< 0,1 sekunder
Fördröjning vid aktivering av sändningsnyckel	< 1 sekund
Fördröjning vid byte av sändningsnyckel	< sändningstiden för en 64 oktetter stor ram
Fördröjning vid aktivering av mottagningssnyckel	< 1 sekund
Fördröjning vid byte av mottagningssnyckel	skall ske utan förlust av ramar

Tabell 7.1 – IEEE 802.1AE-2006, Kvalitetskrav för MACsec-implementationer

Det symmetriska blockkryptot *Advanced Encryption Standard* (AES) [AES] med kryptometoden *Galois/Counter Mode* (GCM) [GCM] och med en nyckellängd på 128 bitar måste stöjdas av alla MACsec-implementationer. GCM är en strömkryptometod som även ger äkthetsskydd. GCM kräver en *Initialvektor* (IV) vid start av en sekvens med datablock, där varje datablock är 16 oktetter. Det minimala antalet datablock i en MACsec-ram är 3 och det maximala antalet är 94.

Den IV som används i MACsec är implicit och skapas av fält i varje ram. Mer specifikt består IV av identitetsnumret för den säkra kanalen *Secure Channel Identifier* (SCI) samt ramens ordningsnummer *Packet Number* (PN). Detta innebär att kryptometoden startas om för varje ram, och att det inte finns ett sekvenstillstånd mellan olika ramar.

MACsec appliceras före eventuell VLAN-funktionalitet. Detta innebär att även VLAN-märkningen är integritetsskyddad samt krypterad och därmed oläslig för utrustning mellan MACsec-parterna. För att kunna använda VLAN-taggning för att separera MACsec-tunnlar går det att använda IEEE 802.1ad (*Provider Bridges*) [IEEE8021ad].

Sammanfattning MACsec

MACsec innebär att det etableras ett tillstånd, en säker sammankoppling mellan länkens ändpunkter. Däremot finns det ingen direkt koppling mellan enskilda ramar, utan sammankopplingen definieras av sessionsnummer och ramnummer, inte genom kryptotillstånd och databeroenden mellan ramarna.

MACsec innebär en expansion i ramstorleken, vilket kan leda till fragmentering. MACsec använder en viss del av den tillgängliga dataöverföringskapaciteten och ger även en ökad fördröjning. Den tillförda fördröjningen är dock relativt liten.

7.3.2 IPsec

Internet Protocol Security (IPsec) är en uppsättning protokoll för att säker kommunikation på nätverksnivå. Till skillnad från MACsec behöver ändpunkterna alltså inte vara anslutna till samma datalänknät. IPsec kan användas för att skydda kommunikation oavsett transport- och applikationsprotokoll. IPsec finns i två huvudsakliga varianter:

- *Encapsulating Security Payload* (ESP) [RFC4303]
- *Authentication Header* (AH) [RFC4305]

IPsec definierar inte hur nyckelutbyte och förhandling av andra parametrar ska gå till. För detta kan *Internet Key Exchange* (IKE) [RFC4306] eller IKEv2 [RFC5996]) användas, men kan även göras manuellt eller genom andra automatiserade metoder. Oavsett metod krävs att den inkluderar utbyte av det nyckelmaterial som ska används för att skydda kommunikationen under tiden sammankopplingen gäller. Detta innebär att även om IP-paketen inte är kopplade till varandra finns ett tillstånd upprättat mellan sändare och mottagare.

Oavsett om AH eller ESP används kan IPsec verka i två olika lägen:

- Transportläge (*transport mode*), där IP-paketets innehåll inkapslas, och där IP-huvudet behålls intakt. Då IP-huvudets adressfält är inkluderat i skyddet går det inte att i transportläge använda adressöversättning, *Network Address Translation* (NAT)[2].
- Tunnelläge (*tunnel mode*), där hela IP-paketet, inklusive IP-huvudet kapslas in i ett nytt paket. Adressöversättning och andra tekniker som ändrar adressfälten i IP-huvudet verkar på det nya protokollhuvudet. Nackdelen med tunnelläget är en lägre effektiv dataöverföringskapacitet på grund av det extra IP-huvudet.

I vissa implementationer av IPsec finns möjlighet att transportera IPsec- och IKE-paket över UDP. Denna teknik har i första hand utvecklats för att göra det möjligt

[2]IPsec i transportläge i kombination med NAT-T kräver ett icke-standardiserat tillägg kallat NAT-OA (*originating address*) där information om IP-huvudets ursprungsskick skickas i en separat kanal över UDP

att skicka IPsec/IKE-trafik genom adressöversättande enheter (NAT), och kallas därför *NAT-Traversal* (NAT-T [RFC3948]). Det förekommer även leverantörsspecifika utökningar av NAT-T för att göra motsvarande över TCP, men det bör noteras att tillståndsmekanismen i TCP kan göra en sådan tunnel förhållandevis känslig för paketförluster och andra störningar.

Authentication Headers

AH erbjuder skydd av IP-paketens integritet, det vill säga att det går att avgöra att paketet kommer från rätt avsändare och om paketet förvanskats vid överföringen. AH erbjuder även möjlighet till skydd mot återuppspelning.

AH erbjuder ett skydd för varje IP-paket individuellt, detta gör att AH inte inför något beroende mellan paketen. Det återuppspelningsskydd som finns i AH är implementerat som en 32-bitars räknare i AH-huvudet. Detta innebär att i en given skyddad sammankoppling kan maximalt 2^{32} paket skickas. Sedan måste en ny sammankoppling med en nytt nyckelmaterial förhandlas fram.

För IPv4 skyddar AH de egna fälten (i AH-huvudet) samt övriga fält i IP-paketets huvud som inte ändras vid vidarebefordran av paketet[3]. För IPv6 skyddas AH-huvudet, utökade huvuden, IP-paketets innehåll och de fält i IPv6-huvudet som inte ändras vid vidarebefordran[4].

AH använder funktionen *Keyed-Hashing for Message Authentication* (HMAC) [RFC2104], baserad på de kryptografiska envägsfunktionerna MD5 [RFC1321] eller SHA-1 [SHS] för att skapa integritetsskyddet.

Encapsulating Security Payloads

Inverkan på den effektiva dataöverföringskapaciteten för ESP är större än med AH. ESP är trots detta den klart vanligaste varianten av IPsec, av det skälet att ESP även erbjuder konfidentialitetsskydd genom att innehållet i paketet krypteras. Som namnet antyder kan ESP även användas för att upprätta en tunnel mellan två nätverk, och inte bara mellan två ändnoder.

Den vanligaste kryptometoden i ESP är *Cyclic Block Chaining* (CBC) [CBC]. Med denna metod delas det data som ska krypteras in i block, och blocken är kopplade till varandra. För att kunna dekryptera det första blocket i kedjan krävs ett startvärde (IV).

I IPsec initieras CBC en gång för varje paket och den IV som används skickas med i ESP-huvudet. Beroende på underliggande blockkrypto och hur stor andel av paketet som utgörs av nyttodata, kan den beräkningsmässiga inverkan för att initiera kryptot och CBC-metoden bli relativt stor. Detta riskerar att resultera i ökade fördröjningar.

ESP kan även ge integritetsskydd och ESP använder samma HMAC-baserade mekanism om AH. Till skillnad från AH omfattar skyddet inte adresserna i IP-huvudet

[3]De fält som kan ändras under transport, och där med inte skyddas är: DS, ECN, Flaggor, Fragment Offset, TTL och checksumman

[4]De fält i IPv6-huvudet som inte skyddas är: DS, ECN, Flow Label, och Hop Limit

när ESP används i tunnelläge.

Slutsatser om IPsec

IPsec är en mycket vanlig och flexibel metod för att skydda kommunikationen i IP-baserade nätverk. De två olika varianterna AH och ESP erbjuder möjlighet till avvägning mellan behovet av konfidentialitet och resursåtgång. I typfallet är emellertid de kapacitets- och fördröjningsmässiga fördelarna med att välja AH framför ESP marginella, och ESP den dominerande varianten av IPsec.

Fördelarna med ESP i form av skydd av fler fält i IP-huvudet och möjlighet att traversera nät med adressöversättning (NAT) överväger oftast ökad åtgång av överföringsskapacitet. Om inget konfidentialitetsskydd behövs går det även att använda så kallat *NULL-krypto* i ESP.

Varken AH eller ESP inför ett beroende mellan enskilda paket. Däremot kan vissa specialfall, t.ex. stora trafikströmmar bestående av många små paket medföra försämringar av anslutningens effektiva överföringskapacitet.

För både AH och ESP gäller det vid användning av IPsec att bedöma om transportläge eller tunnelläge är det som krävs. Tunnelläget har något större inverkan på den effektiva dataöverföringskapaciteten, men ger flexibilitet vid traversering av andra IP-nät.

7.3.3 TLS

Transport Layer Security (TLS) [RFC5246] är ett protokoll som ger kryptografiskt skyddad kommunikation på tr. Skyddet innefattar konfidentialitet, integritet och skydd mot återuppspelning. TLS är en vidareutveckling av föregångaren SSL och bär många likheter med SSL. I denna handledning används benämningen TLS för båda protokollen, även om det finns distinkta och betydelsefulla skillnader mellan protokollen.

Den vanligaste tillämpningen av TLS är sannolikt i kombination med webbprotokollet *Hypertext Transfer Protocol Secure* (HTTPS), och kallas då HTTPS [RFC2818]. TLS används även för att skapa kryptografiskt skyddade tunnlar, s.k. SSL-VPN, för att transportera andra protokoll.

TLS tillämpas ovanpå ett tillförlitligt transportprotokoll (t.ex. TCP), men finns även i en version – *Datagram Transport Layer Security* (DTLS) [RFC4347] – som kan tillämpas ovanpå ett otillförlitligt transportprotokoll (t.ex. UDP). I övrigt delar TLS och DTLS de flesta egenskaper. TLS består av flera interna lager – *TLS Handshake Protocol*, *TLS Alert Protocol*, *TLS Change Cipher Spec Protocol* och *TLS Record Protocol*:

TLS Handshake Protocol används för att förhandla fram villkoren för en säker sammankoppling, t.ex. vilka algoritmer och nyckellängder som ska användas. Protokollet utför även ömsesidig autenticering mellan parterna samt framställer sessionsunika kryptonycklar.

TLS Record Protocol används av överliggande protokoll, inklusive *TLS Handshake Protocol* och *TLS Alert Protocol*, och befinner sig direkt på TLS/DTLS

transportprotokoll. Protokollet erbjuder konfidentialitet genom symmetrisk kryptering och integritetsskydd, samt erbjuder även möjlighet till komprimering.

TLS Alert Protocol används för signalering, t.ex. för felrapportering.

TLS Change Cipher Spec Protocol används av endera part för att meddela en ändring av de överenskomna kryptomekanismerna. Efterföljande poster ska skyddas med de nya mekanismerna och med nya nycklar.

För att etablera en säker sammankoppling med TLS behöver parterna skicka ett relativt stort antal meddelanden till varandra. Upp mot 10 meddelanden i vardera riktningen kan krävas, förutom TCP-protokollets trevägshandskakning. Detta gör att etableringen kan ta förhållandevis lång tid. Att etablera den säkra sammankopplingen innebär även att relativt beräkningsmässigt krävande kryptografiska operationer utförs.

TLS har dock stöd för att behålla och även återuppta en tidigare sammankoppling. Detta ökar effektiviteten och gör det dessutom möjligt att minska ner antalet TCP-anslutningar som krävs för t.ex. webbåtkomst. Normalt skapas annars en ny TCP-anslutning för varje objekt som t.ex. en webbläsare efterfrågar. [5]

TLS delar in den användande tjänstens trafik i poster om upp till 16 kByte. Dessa fragment komprimeras och en kryptografisk baserad äkthetskod (*Message Authentication Code* (MAC)) framställs. Slutligen krypteras hela fragmentet och skickas med ett eller flera TCP-segment över förbindelsen. Detta innebär att det finns ett databeroende inom en post och att det även finns beroenden mellan de TCP-segment som transporterar posten.

Beroende på kryptometod som används samt version av TLS kan det även finnas ett beroende mellan posterna. I version 1.0 av TLS [RFC2246] utgörs IV för en post av det sista kryptoblocket i föregående post. I version 1.1 av TLS [RFC4346] ändrades detta till en IV skapad genom innehållet i den egna posten.

Sammanfattning TLS

För att sammanfatta de viktigaste egenskaperna:

- TLS är ett TCP-baserat protokoll.
- TLS ger förhållandevis stor påverkan vid etablering av tillstånd, vilket gör den känslig för anslutningens tillgänglighet och fördröjning. Det finns dock stöd i senare versioner för att återuppta en session.
- TLS delar in data i block om upp till 16 kByte med kryptografisk koppling över hela blocket. Detta medför ett beroende mellan de TCP-segment som transporterar varje block och ökar störningskänsligheten.

[5] Protokollet SPDY utnyttjar samma principer för att sammanfläta HTTP-trafiken i en enskild TCP-anslutning.

- TLS används för att bygga säkra tunnlar över *Hypertext Transfer Protocol* (HTTP) för olika protokoll och kallas då ofta SSL-VPN.
- TLS kan för vissa applikationer få en relativt stor inverkan på den effektiva dataöverföringskapaciteten.

7.4 Slutsatser om tunnelmekanismer

Alla former av tunnelmekanismer på länk- eller nätverksnivå påverkar den effektiva överföringsakapaciteten negativt, i någon grad. I de fall tunnelmekanismen är implementerad på nätverksnivå (IP) medför detta i sin tur att den maximala paketstorleken (*Maximum Transfer Unit* (MTU)) minskar. Denna minskning kan kompenseras genom fragmentering och ihopmontering vid tunnelns ändpunkter, eller hanteras genom att överliggande lager tar hänsyn till en reducerad MTU.

I tabellen 7.2[6] finns några exempel på hur mycket storleken på IP-paketen ökar vid användning av ett antal olika tunneltekniker.

Tunnelmekanism	Extra paketstorlek	IP MTU
GRE	4 oktetter	1 496 oktetter
L2TP	40 oktetter	1 460 oktetter
L2TPv3	12 oktetter	1 488 oktetter
IPsec Tunnel Mode ESP	60 oktetter	1 440 oktetter
IPsec Transport Mode ESP	52 oktetter	1 448 oktetter

Tabell 7.2 – Exempel på paketstorlek för ett antal tunnelmekanismer

Om flera tunnelmekanismer staplas på varandra sjunker snabbt den effektiva utnyttjandegraden av anslutningens överföringskapacitet, och påverkan kan komma att bli avsevärd. Tunnelmekanismer inför också ofta tillstånd i anslutningen. Tillämpningar och protokoll som transporteras genom tunneln kan ha egna tillstånd som kan komma i konflikt med tunnelns interntillstånd. Resultatet av fel i överföringen riskerar att bli en snabbt försämrad kvalitet i ovanliggande tjänster.

Vid tunnling behöver alltså de potentiella effekterna av underliggande tunnels tillstånd beaktas. Detta gäller inte minst vid anslutningar med låg kapacitet eller anslutningar som utnyttjas nära sitt kapacitetstak. Extra viktigt blir detta när anslutningen dessutom har hög fördröjning.

De tre krypterande tunnelmekanismer som beskrivits påverkar alla den trafik de skyddar. I huvudsak sker påverkan genom att:

- Påföra fördröjningar
- Öka åtgången av överföringskapacitet

[6] För IPsec anges paketstorlek vid användning av AES-128/SHA-1

- Skapa tillstånd/beroenden mellan sändare och mottagare vilket ökar störningskänsligheten.

Att den kryptografiska behandlingen tar tid är inte unikt för just kryptering, utan gäller för all form av behandling som sker av kommunikation. Andra exempel innefattar filtrering, komprimering och IP-vägval. Att den totala åtgången av dataöverföringskapacitet ökar beror på de kontrollfält som måste läggas till datapaket för att kunna tolka och verifiera skyddet.

Det beroende som upprättas mellan sändare och mottagare är de säkra sammankopplingarna. MACsec och IPsec skapar inget beroende mellan på varandra följande paket. TLS däremot skapar även beroenden mellan enskilda paket. Hur mycket en krypteringsmekanism påverkar är beroende av flera saker:

- Typ av krypteringsmekanism – algoritmer och protokoll
- Var i protokollhierarkin den appliceras
- Typ av trafik som skyddas

Ett exempel på en typ av trafik där krypteringsmekanismen kan få stor påverkan är IP-telefoni, *Voice over IP* (VoIP) över IPsec eller TLS [VoIPSec]. För att klara realtidskraven delas VoIP-trafiken in i många små paket. Ofta skickas dessa med RTP-protokollet [RFC3550]. Storleken på varje paket och den dataöverföringskapacitet en talkanal kräver beror på vilken talkodning som används och hur ofta paketen skickas. Med talkodaren G.729 [G729] och RTP som transportprotokoll blir dataöverföringskapaciteten för en röstkanal som lägst ca 34 kbps. Med IPsec ESP stiger behovet av dataöverföringskapacitet till 60 kbps och med TLS till drygt 80 kbps. Behovet av dataöverföringskapacitet kan alltså mer än fördubblas. Det bör noteras att för just RTP används ofta *Secure RTP* (SRTP) [RFC3711] – en krypteringsmekanism som innebär förhållandevis liten påverkan på paketstorleken.

8 Nätverksfunktionalitet i olika operativsystem

Operativsystem i datorer, kommunikationsutrustning och de många inbyggda system som finns omkring oss innehåller som regel funktionalitet för IP-baserad kommunikation. Denna funktionalitet, ofta kallad *IP-stack* eller *nätverksstack*, erbjuder bland annat möjlighet att skicka och ta emot IP-paket, samt initiera och använda transportprotokoll som *User Datagram Protocol* (UDP) eller *Transmission Control Protocol* (TCP) för att kommunicera med en motpart över en anslutning.

Den grundläggande funktionalitet de olika operativsystemen erbjuder är oftast likvärdig, även om nätverksalgoritmerna som implementerats kan använda olika strategier för att reglera och kompensera för t.ex. paketförluster och fördröjningar. De olika strategierna ger olika beteende och påverkar vilken effektiv överföringskapacitet tjänster erhåller över anslutningar med olika egenskaper.

I operativsystem som Windows, OS X, Linux, Solaris och FreeBSD är nätverksalgoritmerna till stora delar självreglerande och dynamiska med förmåga att anpassa sig till hur anslutningens egenskaper varierar över tiden. Men även om algoritmerna är dynamiska och självreglerande går det ändå att genom inställningar anpassa beteendet för att förbättra kapacitetsutnyttjandet vid särskilda förhållanden och användningsfall.

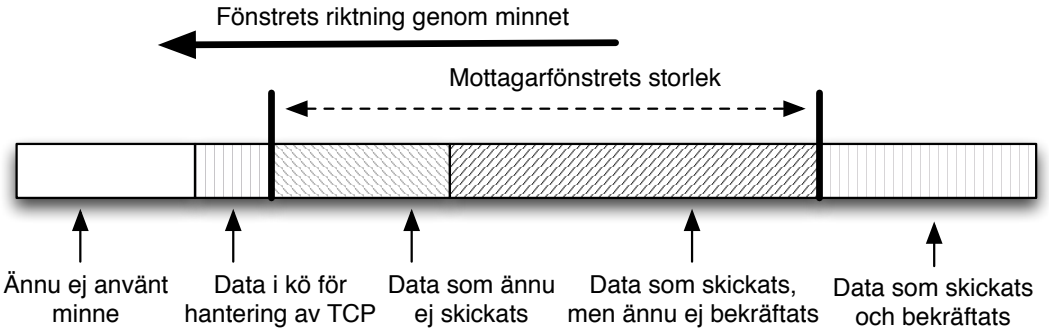
8.1 TCP

8.1.1 TCP och typanslutningar

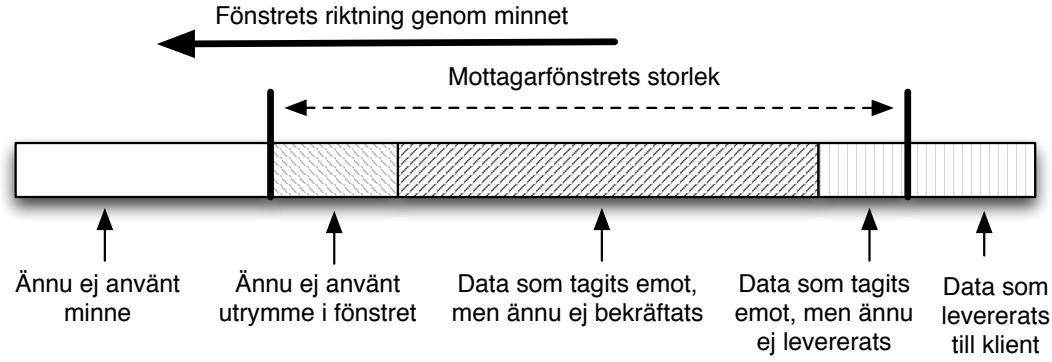
Protokollet TCP [RFC793] är det dominerande transportprotokollet som används på Internet. Vid överföring av data med TCP delas data upp i flera segment som sedan skickas med IP-paket. TCP har förmåga att hålla reda på flera utestående segment som skickats iväg.

När motparten bekräftar att ett segment mottagits, bockas segmentet av ur en sändningslista. Om ingen bekräftelse erhålls inom en viss tid betraktas segmentet som förlorat och segmentet skickas om.

När TCP-implementationen börjar skicka iväg segment ökar mängden utestående segment inledningsvis exponentiellt. Detta sker tills dess att mottagarens maximala fönsterstorlek har uppnåtts, eller när en paketförlust upptäcks av sändaren. Denna process kallas *slow-start*. Efter att slow-start har uppnåtts börjar TCP-implementationen justera sändningstakten i syfte att maximera och bibehålla kapacitetsutnyttjandet.



Figur 8.1 – TCPs sändarfönster med data från applikationen, data klart att skicka, data som skickats och data som bekräftats av mottagaren



Figur 8.2 – TCPs mottagarfönster med mottagen data som ej bekräftats, data som bekräftats och data som ska levereras till applikationen

Hur snabbt TCP-implementationen ökar eller minskar antalet utestående segment, samt hur lång tid den inväntar bekräftelser innan segment anses förlorade, är parametrar som justeras för att maximera kapacitetsutnyttjandet och samtidigt undvika att det uppstår köer och överbelastning i anslutningen. Strategin för hur parametrarna justeras bestäms av vilken algoritm – *Congestion Avoidance Algorithm* – som används. För att påverka dessa parametrar kan, när så är möjligt, ett byte till en algoritm som bättre stämmer överens med tjänstens trafikbeteende och anslutningens egenskaper ge en kvalitetsförbättring.

För TCP finns ett antal olika algoritmer utvecklade. Vissa algoritmer är optimerade för att hantera anslutningar med hög kapacitet, andra kan vara optimerade att ge bra kvalitet över anslutningar med låg och varierande kapacitet.

De tidigaste algoritmerna, vilka först implementerades i UNIX-operativsystemet BSD, kallas Reno och Tahoe. En vidareutveckling av Reno kallad NewReno [RFC3782] standardiserades av IETF och användes senare i ett stort antal operativsystem. I dag finns ett flertal antal algoritmer, med namn som BIC, CUBIC, CTCP och LEDBAT.

Kännetäcknande för är de nyare algoritmerna, t.ex. CTCP, CUBIC och LEDBAT, är att de är bättre anpassade för dagens anslutningsformer än äldre algoritmerna som Reno och NewReno. Flera av de nyare algoritmerna fungerar däremot sämre för anslutningar med särskilt hög fördröjning, anslutningar med stor varians i överföringskapacitet, frekventa avbrott eller med en stor andel paketförluster. Andra algoritmer, t.ex. Veno, Westwood+ [Westwood+] och TCP-FIT [TCP-FIT] är utvecklade för att fungera särskilt väl över mobilsystem och satellitsystem, och som för denna typ av anslutningar vanligen resulterar i väsentligt bättre kvalitetsegenskaper för den överliggande tjänsten. Dessa algoritmer är som regel inte förvalda i operativsystem för skrivbordet. Däremot kan de läggas till i de operativsystem som stödjer utbyggnad av denna typ av funktionalitet, t.ex. Linux.

8.1.2 TCP Window Scaling och SACK

För vissa anslutningar kan det krävas många utestående segment för att utnyttja den kapacitet som finns. Detta gäller särskilt anslutningar med hög kapacitet och hög fördröjning. För dessa anslutningar kan mängden data som samtidigt befinner sig under transport mellan två parter bli betydande. Anslutningen kan sägas ha en hög *datahållningsskapacitet*, och kallas ibland *Long Fat Networks* (LFN).

Ett mått på hur stor datahållningskapacitet en anslutning har, ges av formeln:

$$överföringskapacitet \times fördröjningen = datahållningskapacitet$$

En anslutning, där produkten ovan överstiger 10^6 bitar, definieras i [RFC1072] som en LFN-anslutning. Ett exempel på en LFN-anslutning är satellitlänk där anslutningen kan hålla närmare 2 Mbit samtidigt. Även dagens högkapacitetsförbindelser, t.ex. byggda med Gigabit Ethernet, kan hålla betydande mängder data i ett givet ögonblick.

Internt använder TCP buffertar kallade *fönster* för att hålla reda på vilka segment som skickats, vilka som bekräftats och vilka som är försenade. Att använda stora buffertar påverkar interaktiva tjänster negativt. Därför introducerades i [RFC1323]

en metod för att dynamiskt kunna anpassa fönsterstorleken, för att bättre utnyttja LFN-anslutningar.

En aspekt på LFN-anslutningar, och särskilt där anslutningens tillgängliga kapacitet varierar, är att sändande nod kan erhålla skurar med bekräftelser, alternativt att tidsgränsen för ett stort antal utestående segment går ut mer eller mindre samtidigt. Då dessa händelser normalt ligger till grund för flödeskontrollen för TCP, kan resultatet bli en synnerligen instabil överföring. En teknik för att motverka detta beteende är *Selective ACK* (SACK) [RFC2018].

Både Window Scaling och SACK finns implementerat och används i någon form i väsentligen alla moderna operativsystem.

8.1.3 TCP-implementationen i några vanliga operativsystem

I följande avsnitt beskrivs översiktligt nätverksfunktionaliteten i några vanligt förekommande operativsystem. Fokus för beskrivningen är stödet för transportprotokollet TCP och hur olika inställningar kan användas för att styra TCP-implementationens beteende för olika typer av anslutningar. Listan av operativsystem samt inställningarna för dessa ska ses som principexempel på hur olika system stödjer anpassningar av nätverksfunktionaliteten.

Det finns några typiska parametrar som går att justera i de flesta operativsystem. En sådan parameter är storleken på TCP-implementationens sändar- och mottagarfönster. Ju större fönster, desto fler segment kan vara under överföring mellan sändare och mottagare samtidigt. För en anslutning med hög överföringskapacitet är storleken på fönstret avgörande för att TCP-implementationen verkligen ska kunna utnyttja den tillgängliga kapaciteten. Nackdelen med att öka fönsterstorleken är att anslutningens kapacitet alltför snabbt kan nå sitt tak, vilket kan leda till onödigt stora paketförluster vid uppstart och att fler paket än nödvändigt måste sändas om. Det kan också medföra att andra användare och tillämpningar, som inte optimerat sina TCP-inställningar, erhåller försämrad kapacitet i det gemensamma kommunikationsnätet.

Hur lång tid TCP-implementationen väntar på en bekräftelse från mottagaren att ett segment kommit fram är en viktig parameter för att avgöra om paket försvunnit eller inte. När TCP-implementationen avgjort att ett paket försvunnit justerar den upp tiden den väntar, men sänker även samtidigt takten den skickar iväg nya segment.

Om det är känt att en anslutning har en lång fördröjning kan det för korta sessioner ge stor förbättring att förlänga tiden TCP-implementationen väntar så att den redan från början använder tider som bättre stämmer överens med svarstiden för anslutningen. Särskilt viktigt blir detta för en anslutning som även har en låg överföringskapacitet.

För dessa anslutningar innebär en kort tid innan omsändning att den tillgängliga kapaciteten utnyttjas till omsändning av segment som faktiskt kommer fram. Att förlänga tiden TCP-implementationen väntar är dock inte riskfritt. Om anslutningen har problem att överföra segment och TCP-implementationen väntar för lång tid innan omsändning försämras tjänstens responsivitet.

Windows

Windows XP och tidigare versioner av Windows använde algoritmerna TCP Reno och NewReno. När Microsoft lanserade Windows Vista introducerades en ny algoritm kallad *Compound TCP* (CTCP). CTCP användes inte som standard i Vista, men går att aktivera via kommandoradsgränssnittet. I uppdaterade versioner av Windows Vista, Windows 7 och Windows Server 2008 är CTCP den förvalda algoritmen.

Skillnaden mellan de tidigare använda algoritmerna och CTCP är att CTCP snabbare anpassar sig till anslutningens maximala kapacitet. CTCP är avsedd att bättre utnyttja kapaciteten hos moderna bredbandsförbindelser och LFN-anslutningar. CTCP använder mängden data som väntar på att få skickas iväg som mått på hur belastad anslutningen är.

I Windows Vista och senare versioner av Windows har TCP-funktionaliteten gjorts adaptiv och i stort sett självreglerande. Storleken på sändar- och mottagarfönster justeras automatiskt upp för att kunna utnyttja anslutningar med Gbps-kapacitet. I Windows Vista och Windows 7 används inte den adaptiva, självreglerande funktionaliteten om inte svarstiderna överstiger 1 ms. Det går emellertid att aktivera, avaktivera och modifiera det adaptiva beteendet från kommandoradsgränssnittet.

Från äldre till nyare versioner av Windows gäller en generell trend mot högre adaptivitet och mindre manuell styrning, och Microsoft har plockat bort parametrar för att styra TCP:s beteende. Däremot finns kvar möjligheter att styra hur nätverkskorten hanteras av operativsystemet. Ett exempel på detta är möjligheten att knyta olika nätverkskort till olika processorer eller processorkärnor. I maskiner som tillhandahåller tjänster till många användare kan denna funktion förbättra systemets svarstider.

OS X och iOS

Från och med version 10.5 av OS X har Apple använt självreglerande TCP-algoritmer. Den TCP-algoritm som använts i tidigare versioner av OS X har varit NewReno, men med version 10.7 (*Lion*) ersattes denna med en ny algoritm kallad *LEDBAT*. Den nya algoritmen syftar särskilt till att förbättra vid överföring av större block av data samt minimera påverkan på andra flöden.

Som standard i OS X är funktioner för SACK samt *Window Scaling* aktiverade. Sedan version 10.5 av OS X har den maximala storleken på TCP-buffrar varit 4 MByte. Ytterligare en parameter, *win_scale_factor*, styr hur storleken på en TCP-buffert kan förändras. Som förval är parametern satt till 3, vilket medför att buffrarna inte kan bli större än 512 kByte.

För att förbättra TCP-protokollets förmåga att utnyttja tillgänglig överföringskapacitet vid anslutningar med hög kapacitet och långa fördröjningar, kan man i OS X öka storleken på maximala antalet buffrar samt justeringsfaktorn via kommandoradsgränssnittet. I OS X är det kommandot *sysctl* som används för att läsa och sätta parametrar.

Linux

Linux har genom åren använt flera olika TCP-algoritmer. Ursprungligen användes Reno, och senare (upp till och med version 2.6.18) algoritmen BIC. Sedan version 2.6.19 är CUBIC den förvalda algoritmen. CUBIC är en algoritm avsedd att bättre utnyttja LFN-anslutningar, men samtidigt vara mindre aggressiv och ge ett jämnare kapacitetsutnyttjande än BIC. Precis som i FreeBSD är implementationerna av TCP-algoritmerna i Linux modulariserade och går att byta ut under drift.

Linux-kärnan inkluderar i dagsläget fler än tio olika TCP-algoritmer. Flera av dessa, t.ex. Veno och Westwood+, är anpassade för trådlösa anslutningar med stor variation i kapacitet, fördröjning och tillgänglighet.

Precis som i FreeBSD och Windows är TCP-implementationen i Linux adaptiv där fönsterstorlekar och buffrar kan behöva justeras för att ge optimalt utnyttjande av tillgänglig kapacitet i anslutningar med hög överföringskapacitet och långa fördröjningar.

En intressant egenskap hos Linux är att inställningar av storleken på fönstret för TCP även används för UDP. För att med ett Linux-system kommunicera med UDP över en anslutning med hög överföringskapacitet (mer än 3 till 4 Gbps) bör alltså fönsterstorleken i TCP ökas till minst 4 MByte.

FreeBSD

FreeBSD, som är en direkt vidareutveckling av BSD-systemet, använde ursprungligen TCP-algoritmerna Reno och senare NewReno. Med version 7 av FreeBSD gjordes TCP adaptiv och i version 8 introducerades två nya TCP-algoritmer: CUBIC och H-TCP.

Version 9 av FreeBSD introducerade ett nytt modulärt system där TCP-algoritmen går att byta ut genom enkla kommandon. Det modulära systemet inkluderar i dag fem olika algoritmer däribland NewReno, CUBIC och H-TCP. Som förval används fortfarande NewReno.

8.1.4 Avlastning av TCP-funktionalitet

Vissa kombinationer av operativsystem och nätverksgränssnitt erbjuder möjlighet att flytta delar av nätverksfunktionaliteten ned på särskilt anpassad hårdvara. Därmed avlastas operativsystemet från en del arbete. Metoden kallas *TCP-offloading*, och typiska funktioner hårdvaran kan utföra är:

- Dela upp ett större TCP-segment i flera IP-paket som skickas iväg.
- Ta emot och sätta samman flera paket till ett större segment.
- Kontrollera checksummor.

De flesta moderna operativsystem – med undantag för Linux – stöder avlastningsmekanismer, ibland i kombination med särskilda drivrutiner eller tjänster.

8.2 Hänsynstagande till andra tjänster

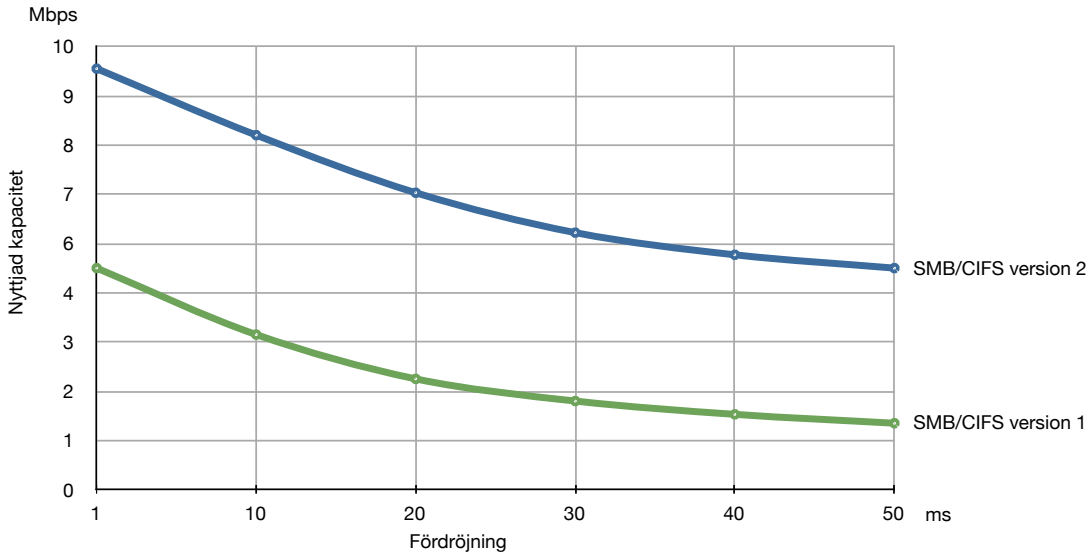
En viktig aspekt vid val av algoritmer och inställningar är hur nätverksbeteendet påverkar andra tjänster och datorer som helt eller delvis använder samma anslutning. En värddator med *aggressivt nätverksbeteende* skulle kunna belägga så mycket av den gemensamma kapaciteten att andra värddatorer får svårt att kommunicera. Exempel på aggressivt nätverksbeteende skulle kunna vara en TCP-anslutning som inte inväntar bekräftelser tillräckligt länge, och därför upprepade gånger skickar om samma segment.

För att undvika denna typ av problem finns det regler om hänsynstagande protokoll emellan. Eftersom TCP är det dominerande transportprotollet brukar regeln normalt formuleras som att ett nytt protokoll inte ska vara mer aggressivt än en normal TCP-session. Även om inte protokollet är nytt kan ändringar i inställningar sätta hänsynstagandeaspekten ur spel. Om inställningar ändras för att optimera kvaliteten för en tjänst och ett användningsfall, bör man säkerställa att detta inte medför att andra tjänsters förutsättningar försämras på ett otillfredsställande sätt.

9 Tillämpningar

9.1 Filöverföring

Funktionen filöverföring ligger till grund för många av de vanligaste transaktionsbaserade och asynkrona tjänsterna. Även om funktionen synes enkel – att flytta en bestämd mängd data från avsändaren till mottagaren – så finns ett flertal parametrar som påverkar tjänstekvaliteten.



Figur 9.1 – Utnyttjandegrad som funktion av fördröjning vid användning av SMB/CIFS i version 1 och version 2

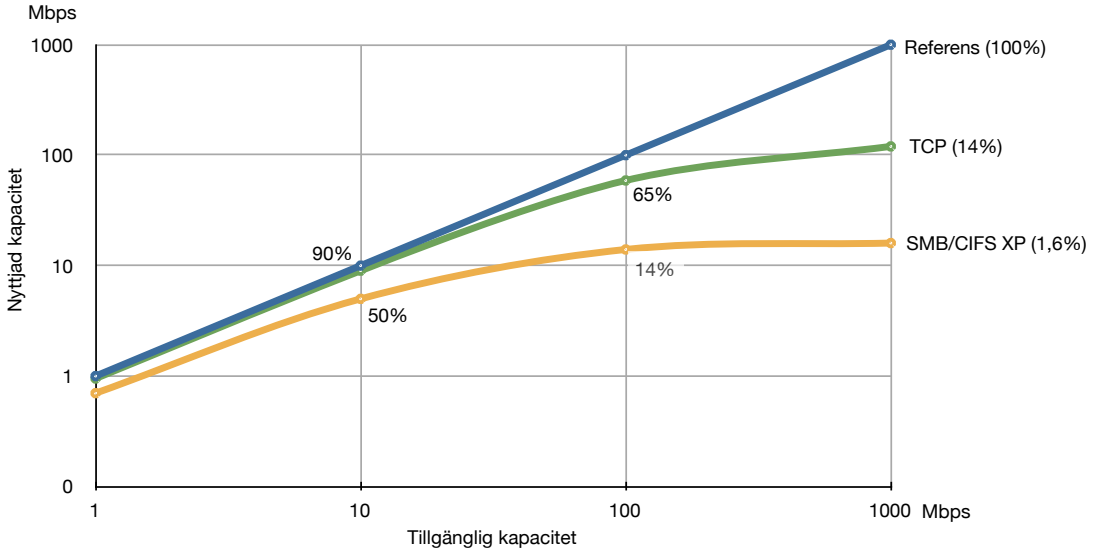
Den kanske mest uppenbara parametern – dataöverföringskapaciteten – är ofta underordnad flertalet andra parametrar. Valet av filöverföringstjänst (vilket nätverksprotokoll som används) samt fördröjning i anslutningen kan ha större påverkan på tjänstekvaliteten än dataöverföringskapaciteten.

De flesta filöverföringstjänster baseras på *Transmission Control Protocol* (TCP), och utnyttjar detta för att reglera flödeskontroll, felkorrigering och omsändningar. Andra filöverföringsprotokoll kan använda egna kontrollmekanismer och blockuppdelning ovanpå TCP, och därmed minska effektivitetsgraden i överföringen.

Ett exempel på ett filöverföringsprotokoll med egna kontrollmekanismer är Microsofts filöverföringsprotokoll *Server Message Block* (SMB), även kallat *Common*

Internet File System (CIFS). I sin ursprungliga version implementerad i Microsofts operativsystem fram till och med Windows XP, är SMB/CIFS särskilt känsligt för fördröjningar i anslutningen.

Skillnaden mellan version 1 och version 2 av SMB/CIFS (implementerad i Windows 7/Windows 2008), är emellertid mycket stor (figur 9.1). Utnyttjandegraden förbättras i normalfallet 2–3 gånger med version 2 jämfört med version 1.



Figur 9.2 – Utnyttjandegrad av fjärrförbindelse vid filöverföring

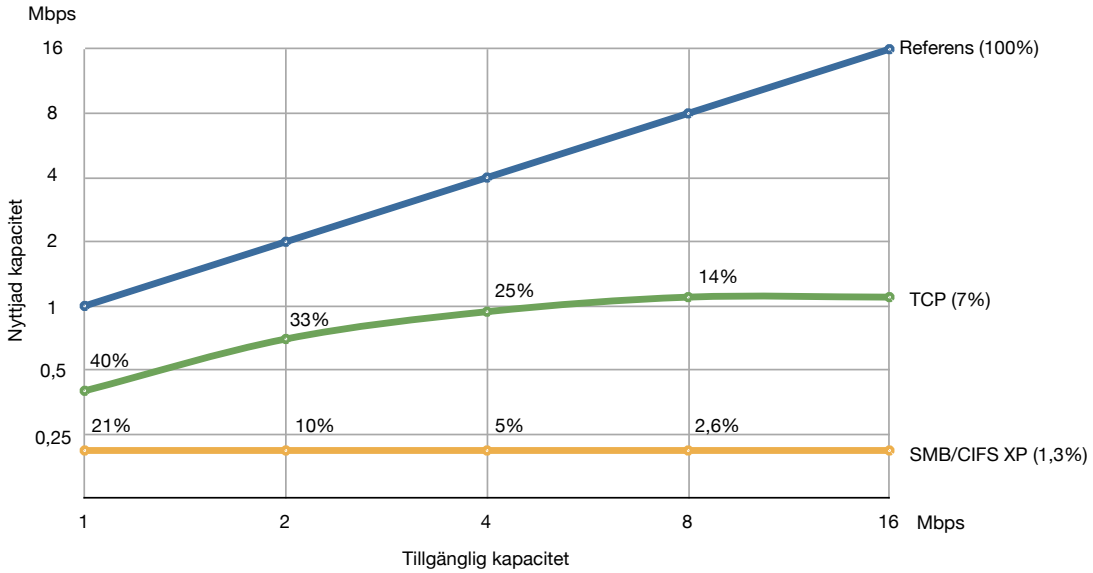
SMB/CIFS version 1 delar upp datamängden som ska överföras i 64 kByte stora block som sedan krypteras och signeras. Kontrollkanalen som vävs in i samma TCP-anslutning inkluderar över 100 olika operationer vilket påför en hög grad av synkronism, som i sin tur leder till lägre utnyttjandegrad av anslutningen.

Effekterna av protokollets egenskaper kan observeras genom att mäta utnyttjandegraden av några av typanslutningarna vid användning av SMB/CIFS version 1, jämfört med en ren TCP-anslutning.

I figur 9.2 visas utnyttjandegraden vid olika dataöverföringskapaciteter för en fjärranslutning som har 10 ms fördröjning. Skalan i diagrammet är logaritmisk med basen 10. Kapacitetsökningar över 100 Mbps ger över huvudtaget inga kvalitetsförbättringar för SMB-protokollet, och endast marginella förbättringar för TCP.

Vid 100 Mbps ger ren TCP cirka fem gånger så hög utnyttjandegrad som SMB-protokollet, och vid 1 Gbps är skillnaden hela 10 gånger.

I figur 9.3 visas utnyttjandegraden vid olika dataöverföringskapaciteter för en satellitanslutning som har 200 ms fördröjning. Skalan i diagrammet är logaritmisk med basen 2. Som visas i diagrammet ger SMB-protokollet ingen som helst kvalitetsförbättring vid ökning av dataöverföringskapaciteten över 1 Mbps. Även ren TCP ger en mycket låg utnyttjandegrad på väsentligt under 50% oavsett anslutningens överföringskapacitet. Över 4 Mbps är ökningen försumbar.



Figur 9.3 – Utnyttjandegrad av satellitlänk vid filöverföring

Eftersom fördröjningen som regel är mycket svår att påverka är lösningen för att kunna utnyttja anslutningens fulla kapacitet istället att välja den filöverföringstjänst som är mest lämpad för ändamålet och anpassa protokollen till anslutningen. En enkel sak som att anpassa TCP-parametrarna efter de rådande förhållandena kan under dessa omständigheter tredubbla överföringskapaciteten.

9.2 Lagringstjänster

9.2.1 Lagringsnät

Lagringsnät, *Storage Area Network* (SAN), är en teknik som används för att fysiskt separera lagringsenheter från de maskiner som använder lagringsenheterna. Fördelen med lagringsnät är att olika maskiner, i första hand servrar, inte behöver vara bestyckade med egna uppsättningar av hårddiskar eller enheter för t.ex. säkerhetskopiering. Istället kan dessa lagringsenheter centraliseras vilket därmed förenklar underhåll, förbättrar tillgänglighet och borgar för ett effektivare resursutnyttjande.

De maskiner som använder lagringsenheterna får tillgång till dessa via ett nätverk. Protokollen som används i lagringsnäten baseras på de lokala överföringsmekanismer som traditionellt används internt i maskinerna, men modifierats för att kunna transporteras över ett nätverk. Exempel på lokala diskprotokoll som förlängts på detta sätt är SCSI, *Fibre Channel* (FC) och *AT Attachment* (ATA).

Att återanvända protokollen på detta sätt ger smidig integration och lagringsnätens enheter på nätet uppträder som lokala fysiska enheter, t.ex. en hårddisk. En maskin som använder en SAN-ansluten enhet läser och skriver block av data direkt till

enheten.

Att använda de lokala diskprotokollen över ett nätverk ställer emellertid mycket hårda krav på korta fördröjningar och hög dataöverföringskapacitet. Därför använder lagringsnät traditionellt i huvudsak särskilda nätverkslösningar med egna länkar och separata växlar för att uppnå detta. Dessa lagringsnät har i normalfallet kapacitet att överföra flera Gbps, med fördröjningar i storleksordningen mikrosekunder. Ett typexempel på teknik för lagringsnät är det seriella datalänkprotokollet FC.

I dag används dock i första hand Ethernet, och i allt högre grad även *Internet Protocol* (IP) för att bygga lagringsnät. Eftersom detta är samma teknik som används i andra nät byggs allt mer sällan separata lagringsnät. Istället transporteras lagringsnätets trafik i ett och samma nätverk, tillsammans med trafik för andra tjänster.

Nätverkskopplad lagring (NAS)

Ett med lagringsnät närbesläktat begrepp är nätverkskopplad lagring – *Network Attached Storage* (NAS). NAS-tjänster arbetar på filer, inte enskilda block. NAS-tjänster ger i jämförelse med SAN lägre överföringskapacitet och används ofta mer direkt mot slutanvändaren. NAS är även mindre transparent för användaren – användaren ser att filen finns på en nätverksenhet och kan behöva utföra andra handgrepp för att komma åt en fil i NAS än en fil lagrad på lokal disk. Exempel på NAS-tjänster är SMB/CIFS, *Network File System* (NFS) och *Andrew File System* (AFS). Även tjänsterna *File Transfer Protocol* (FTP) och *Web Distributed Authoring and Versioning* (WebDAV) skulle kunna betraktas som NAS-tjänster.

9.2.2 iSCSI

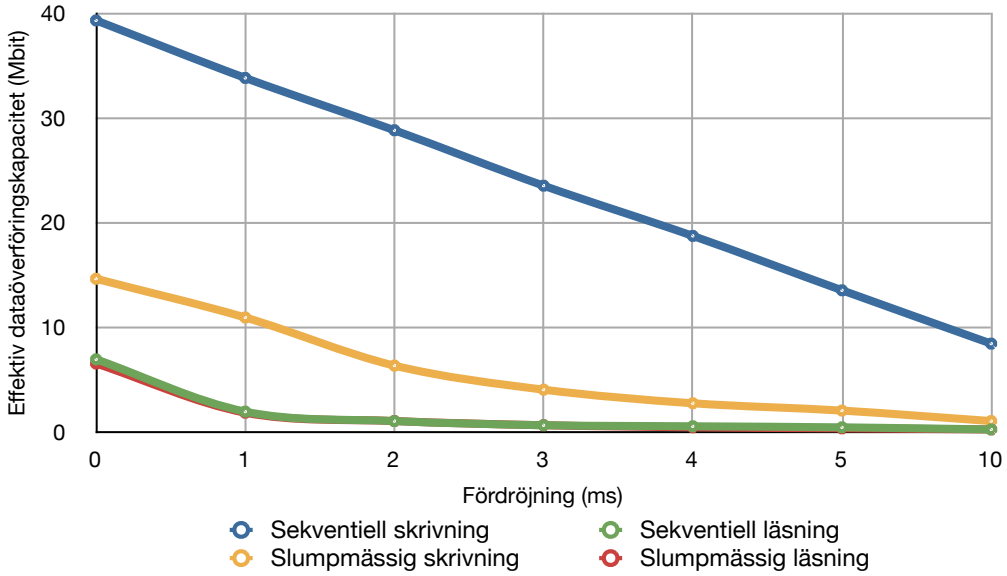
Small Computer System Interface (SCSI) är en standard för att ansluta lokala lagringsenheter till en dator. SCSI byggde från början på parallellkablar och hade stöd för att ansluta upp till 8 enheter över ett maximalt avstånd på ett par meter. Sedan mitten av 1980-talet har dock SCSI utvecklats till ett seriellt höghastighetsprotokoll *Serial Attached SCSI* (SAS) med stöd för många fler enheter och på allt längre avstånd.

SCSI är ett transaktionsbaserat protokoll där en klient kallad initierare (*"initiator"*), skickar en förfrågan om ett datablock till en målenhet. Målenheten svarar på anropet och klienten inväntar svaret. På grund av SCSI:s arv som överföringsteknik över mycket korta avstånd, krävs fortfarande korta fördröjningar för att SCSI skall fungera väl, och är närmast att betrakta som ett synkront protokoll.

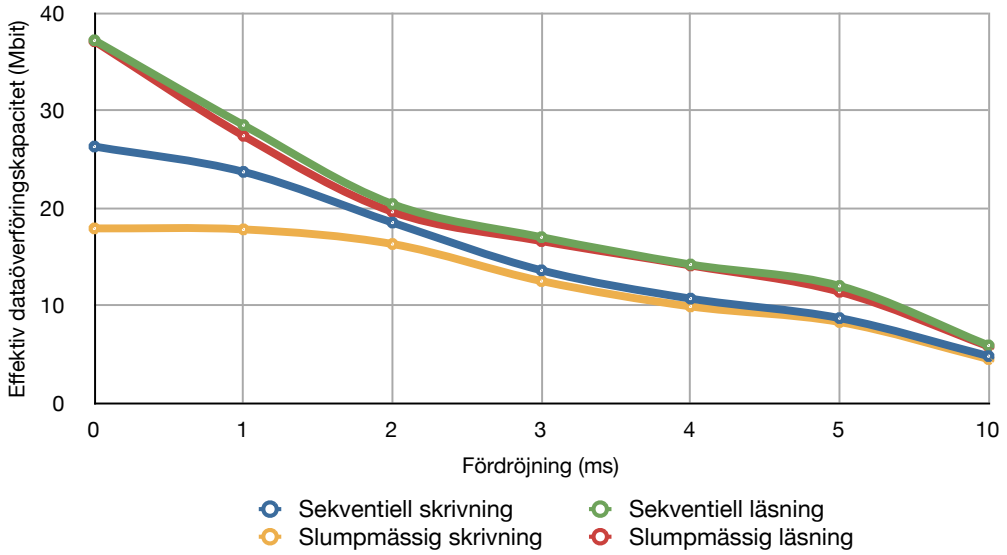
Protokollet *Internet Small Computer System Interface* (iSCSI) [RFC3720] gör det möjligt att använda TCP för att transportera SCSI-kommandon över ett IP-baserat nät. Genom iSCSI kapslas SCSI-protokollets frågor och svar in i en eller flera TCP-segment. För att skydda iSCSI-trafiken kan *Internet Protocol Security* (IPsec) användas som ett säkerhetslager. Fördelen med iSCSI är att det gör det möjligt att bygga lagringsnät med standardiserad nätverksteknik som TCP, IP och Ethernet. Nackdelen med iSCSI i jämförelse med t.ex. Fibre Channel är lägre förväntad överföringskapacitet och större känslighet för fördröjningar.

En viktig parameter för iSCSI är storleken på de datablock som skickas. Normalstorleken är 4 kByte. Tester visar att en ökning av storleken till 256 kByte

ger en väsentlig ökning av den utnyttjade kapaciteten, jämför figur 9.4 och 9.5. Större datablock ger även en något lägre känslighet för fördröjningar. Med dessa optimeringar uppnås omkring 33% kapacitetsutnyttjande vid 5 ms fördröjning.



Figur 9.4 – Effektiv överföringskapacitet vid olika operationer över iSCSI med ökad fördröjning och 4kByte stora datablock.



Figur 9.5 – Effektiv överföringskapacitet vid olika operationer över iSCSI med ökad fördröjning och 256 kByte stora datablock

Stora datablock ställer dock ytterligare effektivitetskrav på operativsystemets

nätverksfunktionalitet. De stora datapaketen ska delas upp i ett stort antal TCP-segment och IP-paket. På mottagarsidan ska segmenten sammanfogas till block. En teknik för att minska belastningen för operativsystem är att använda hårdvara för nätverksgränssnitt som implementerar TCP-funktionalitet. Operativsystemet kan då avlastas genom att hårdvaran, oberoende av operativsystemets inblandning, delar upp segmentet i flera IP-paket och sedan skickar iväg dessa. På mottagarsidan används den omvända hårdvarufunktionen för att foga samman lasten i paketen till datablock.

En annat teknik för att förbättra dataöverföringskapaciteten är att använda extra stora ramar i länklagret. Ethernet *Jumbo Frames* kallas Ethernetramar som är större än de drygt 1 500 oktetter som Ethernet har som standard. Jumboramar kan vara upp till 64 000 oktetter, men i lagringsnät är 9 000 oktetter en vanligare storlek. Fördelen med dessa stora ramar är att mängden data som transporteras per ram blir mycket större och mängden överskottsdata som måste behandlas minskar. Jumboramarna ställer dock krav på att såväl samtliga dataväxlar och anslutna enheter kan hantera de stora ramarna.

9.2.3 Fibre Channel

Fibre Channel (FC) är en standardiserad nätverksteknik för att bygga lagringsnät. FC används för att med FC-specifika växlar och länkar bygga upp lokala nät över vilket data mellan lagringsenheter och servrar transporteras. Länkarna i FC kan vara antingen optiska eller elektriska. FC har en ramstorlek på maximalt 2 148 oktetter och en maximal datastorlek per ram på 2 112 oktetter. FC implementerar också mekanismer för flödesreglering, feldetektering och omsändning.

Över FC transporteras sedan olika specifika lagringstekniker. Exempelvis används *Fibre Channel Protocol* (FCP) för att transportera ATA och SCSI över FC. Det förekommer även teknik för att transportera IP-paket över FC.

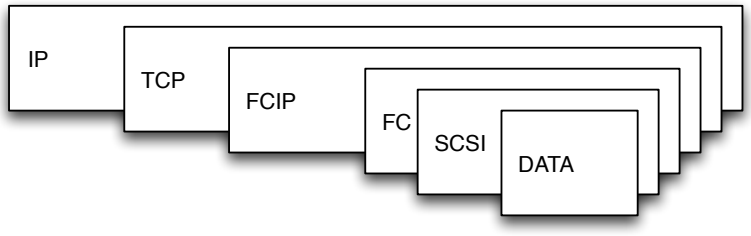
Förutom de FC-specifika fysiska anslutningarna är det möjligt att transportera FC över Ethernet med *Fibre Channel over Ethernet* (FCoE) samt över IP. För transport över IP finns det två olika standarder: *Fibre Channel over IP* (FCIP) och *Internet Fibre Channel Protocol* (iFCP).

Fibre Channel över Ethernet

Fibre Channel over Ethernet (FCoE) är en standard där specifika FC-länkar och växlar ersätts av Ethernetbaserad utrustning. Syftet med FCoE är att kunna använda billigare Ethernetutrustning för att bygga lokala FC-baserade lagringsnät. Fördelen med FCoE i jämförelse med exempelvis FCIP är lägre kapacitetskostnad för IP- och TCP-huvuden. Nackdelen att använda FC direkt ovanpå Ethernet och datalänknivån är att trafiken inte kan adresseras utanför det egna lokala nätet (dvs via routing). Dessutom ställer FCoE krav på stöd på prioritetsfunktioner och flödeskontroll i Ethernetutrustningen. Dessa funktioner implementeras ofta som en del av *Data Center Bridging* (DCB).

FCIP

Fibre Channel over IP (FCIP) [RFC3821] är ett tunnlingsprotokoll för att koppla samman två separata FC-nät. FCIP använder TCP som transportmekanism. FCIP är en transporterande tunnelmekanism där hela FC-ramen, inklusive kontrollsummor och stödfält, överförs.



Figur 9.6 – IP-lagerstrukturen för FCIP.

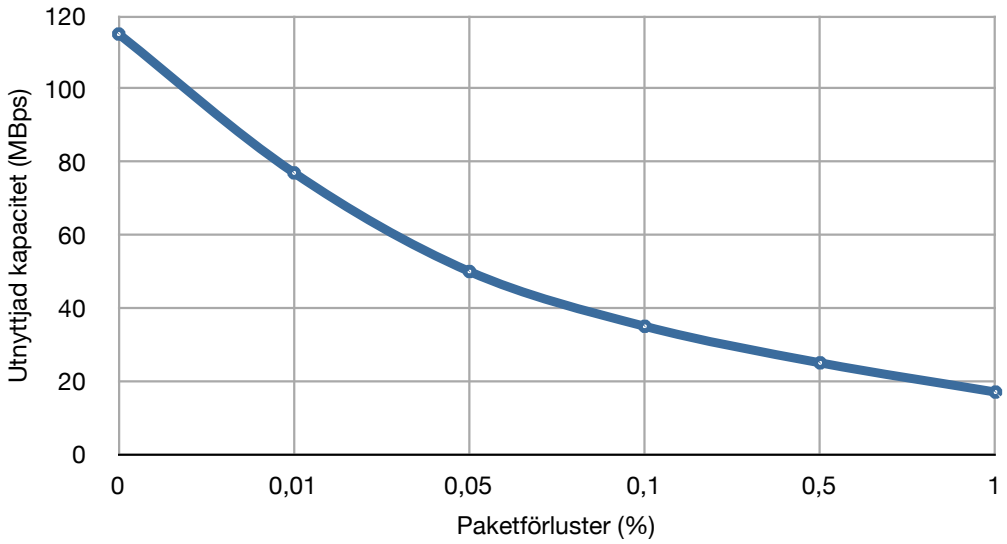
Att FCIP är en transporterande tunnelmekanism innebär även att FCs egna mekanismer för felhantering och omsändning används, förutom de mekanismer TCP har. Detta gör att TCP:s mekanismer kan behöva anpassas för att stämma överens med egenskaperna hos de specifika FC-näten som kopplas samman. FC är även ett skurigt protokoll, vilket kan få TCP att överreagera med onödiga omstarter och omsändningar. Vid användande av FCIP bör därför *Selective ACK* (SACK) användas.

FC-ramens maximala storlek är 2 148 oktetter, vilket är större än den normalt maximala paketstorleken (*Maximum Transfer Unit* (MTU)). För att undvika fragmentering bör MTU sättas upp till 2 300 oktetter. Alternativt bör om möjligt *Jumbo Frames* användas.

FC kan arbeta som en synkron tjänst eller en asynkron tjänst. När FC arbetar som en synkron tjänst kräver sändaren en bekräftelse från mottagaren på varje skickat meddelande. FCIP, som alltså använder TCP som transportmekanism, erhåller redan bekräftelser på skickade meddelanden. De synkrona FC-bekräftelserna ger däremot upphov till en motriktad ström av meddelanden, från mottagaren till sändaren. Eftersom FC-sändaren väntar in dessa meddelanden blir synkron FC och därmed FCIP känslig för fördröjningar och därvid snabbt försämrad utnyttjandegrad av anslutningens kapacitet. Vid större fördröjningar på anslutningen bör därför asynkron FC användas.

I de rekommendationer för design av FCIP-nät som Cisco [CISCOFCIP] tagit fram, redogörs för vilken effektiv överföringskapacitet som kan förväntas uppnås med FCIP över olika anslutningar. För en anslutning med en kapacitet på 1 Gbps samt en responstid på 100 ms bör FCIP kunna nå en kapacitet på drygt 110 MBps. För att nå denna effektiva överföringskapacitet får det dock inte förekomma några paketförluster. Vid 0,01% paketförluster minskar den effektiva överföringskapaciteten till under 80 MBps, se figur 9.7.

Precis som i iSCSI innehåller inte FCIP några egna säkerhetsfunktioner, utan dessa behöver tillföras med ett annat protokoll, t.ex. IPsec.



Figur 9.7 – Tillgänglig kapacitet i en FCIP-anslutning över Gigabit Ethernet minskar med ökad mängd paketförluster.

iFCP

Protokollet *Internet Fibre Channel Protocol* (iFCP) [RFC4172] används för att koppla samman FC-nät eller enskilda FC-element med varandra över IP. Till skillnad från FCIP är iFCP inte ett tunnelprotokoll. Istället lyfts innehåll och signalering ut ur FC-ramarna och transporteras med TCP över IP-nätet till mottagarsidan. På mottagarsidan återskapas sedan FC-kommunikationen.

Fördelen med iFCP är högre dataöverföringskapacitet. Med iFCP kan innehållet i flera små FC-ramar transporteras i samma TCP-segment. Vidare överförs inte heller hela huvudet från FC-ramen, vilket minskar mängden överskottsdata. Med iFCP är det bara TCPs egna mekanismer för trafikreglering och felhantering som används.

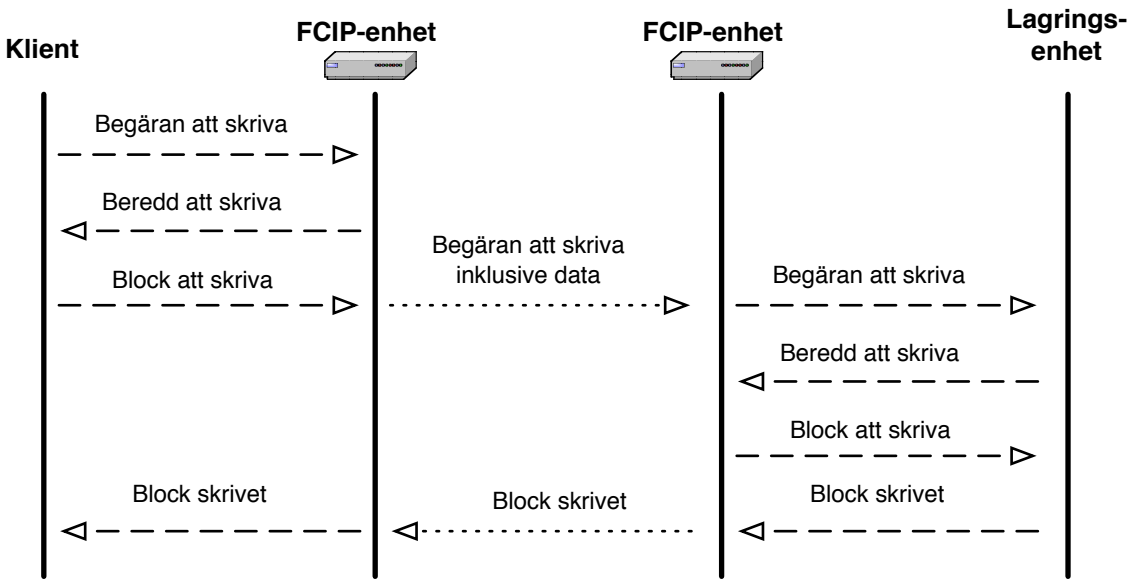
Precis som iSCSI och FCIP används IPsec för att skydda iFCP-kommunikation.

9.2.4 Effektiv överföringskapacitet och möjliga förbättringar

Precis som iSCSI används FCIP och iFCP för att transportera närmast synkron trafik med förväntat låga fördröjningar över ett IP-nät. Detta gör att FCIP och iFCP generellt är känsliga för ökad fördröjning.

Det finns dock typiska användningsfall för FCIP och iFCP där fördröjning och försämring i utnyttjad kapacitet lättare går att hantera. Ett sådant fall är spegling av data mellan två fysiskt separerade platser. Vid spegling är det även lämpligt att använda mekanismer som gör FCIP och iFCP mer asynkrona, t.ex. *fast write*.

FC, och särskilt när FC används för att transportera SCSI, innefattar stora mängder handskakningar mellan kommunicerande ändnoder. Vid skrivning av ett block talar sändande enhet om att den vill skriva ett block. Målenheten svarar att den är beredd att ta emot data och först när detta svar har tagits emot skickas blocket som ska skrivas.



Figur 9.8 – Handskakning vid användning av fast write

Fast write innebär att exempelvis FCIP-enheterna i kommunikationskedjan emulerar handskakningen för att få parterna att kommunicera snabbare. Enheten närmast sändaren genererar ett meddelande om att målenheten är beredd att ta emot blocket, detta även om målenheten inte ens fått begäran om skrivning. Det genererade meddelandet gör att sändaren skickar blocket direkt, vilket sedan överförs över IP-nätet.

Enheten närmast målenheten ser till att vänta in responsen från målenheten innan den skickar blocket. Sedan överförs målenhetens bekräftelse på genomförd skrivning till sändaren.

För iSCSI finns en i stort sett direkt motsvarighet till *fast write* kallad *phase collapase*. Med *phase collapse* förmås en SCSI-enhet skicka meddelanden för kommando respektive datablock direkt efter varandra. Dessa meddelanden kombineras till ett TCP-segment och skickas över IP-nätet.

Det finns även protokollmässiga optimeringsmekanismer som används för att förbättra den effektiva överföringskapaciteten hos iSCSI, FCIP och iFCP. De komprimeringar som används är av två huvudsakliga typer:

1. Eliminering av fält i överförda protokollhuvuden.

2. Överföring av flera små ramar i samma IP-paket.

En metod som används för att förbättra den effektiva överföringskapaciteten i lagringsnät är att differentiera trafiken i nätet. Detta gäller särskilt IP-baserade nät där trafiken för lagringsnätet delar länkar och anslutningar med annan trafik. I dessa nät används klassificeringsmekanismer för att särskilja lagringstrafiken och ge denna

trafik högre prioritet genom nätet. I specifikationen för FCIP finns en rekommendation att använda prioritet som ett sätt att säkerställa att FCIP får bra överföringskapacitet och låg fördröjning.

9.3 Fjärrskrivbord

9.3.1 Olika typer av fjärrskrivbord

Med fjärrskrivbord avses tjänster där användaren via en nätverksanslutning får tillgång till en dators, ofta en servers, grafiska gränssnitt. Nätverksanslutningen överför skärmbild och annan in- och utmatning, men kan även inkludera tjänster som filöverföring och skrivardelning. Fjärrskrivbord används på flera olika sätt, t.ex.:

- För att kunna arbeta på maskiner med annan kapacitet och funktionalitet än den lokala maskinen. Att via fjärrskrivbord arbeta på utvecklings- och beräkningsmaskiner är ett exempel.
- För att centralisera datorresurser. Användarens dator är antingen en fysisk eller virtuell maskin som användaren når med fjärrskrivbordet. Användarens klientmaskin är endast kapabel att visa fjärrskrivbordet samt hantera tangentbord och pekdon.
- För IT-stöd där personal kan koppla upp sig mot användarens dator för att lösa problem.

Gemensamt för dessa användningsfall är att fjärrskrivbord är en interaktiv tjänst. Fjärrskrivbord är ofta asymmetriska med stor skillnad i kapacitetskrav i de olika riktningarna. Från användaren skickas normalt tangentbordstryckningar och pekdonsrörelser. Till användaren skickas grafik, ljud och stödinformation som krävs för att fjärrskrivbordet ska kunna visas på klientmaskinen.

Hur fjärrskrivbordet överförs mellan server och klient skiljer mellan olika implementationer. Tre huvudsakliga metoder kan urskiljas:

1. Klientbaserad rendering. Servern skickar över ritkommandon eller det exakta innehållet i olika element på skärmen. Klienten ansvarar för att tolka kommandona och skapa den bild som slutligen visas. Exempelvis kan ritkommandon i Microsofts skärmspråk *Graphics Device Interface* (GDI) eller 3D-språk som OpenGL skickas från servern.
2. Skärmavbildning (*screen scraping*). Servern skapar en komplett skärmbild av det lokala skrivbordet. Den färdiga skärmbilden skickas till klienten som visar bilden för användaren. För att minska åtgången av dataöverföringskapacitet används ofta datakomprimering samt metoder som att bara skicka skillnaden mellan två bilder.
3. Serverbaserad rendering (*host based rendering*). Servern skapar grafiska element för olika delar av bilden och kodar dessa som olika typer av grafiska strömmar. Ofta används grafikprocessorer i servern för att utföra avancerad kodning och

komprimering. Klienten tar emot de olika strömmarna, avkodar och fogar samman delarna till den färdiga bilden. Klienten måste kunna hantera olika typer av kodningar och behöver viss beräkningskapacitet för skapa skärmbilden.

Metod 1 har potentiellt lägst krav på dataöverföringskapacitet, samtidigt som den ställer störst krav på beräkningskapacitet och funktionalitet hos den lokala klienten. Ytterligare en skillnad är att i metod 1 skickas det faktiska innehållet i de element som ska visas över till klienten, t.ex. överförs texten i ett textdokument från servern till klienten. I metod 2 och 3 är det en bild som visar texten som skickas över.

Metod 2 ställer lägst krav på klientens beräkningskapacitet, men riskerar att ställa högst krav på anslutningens dataöverföringskkapacitet. Att metod 2 behandlar alla delar av bilden på samma sätt gör det svårare att bibehålla en bra användarupplevelse när tillgänglig kapacitet minskar.

Den stora skillnaden mellan metod 2 och 3 är att fjärrskrivbordet i metod 3 inte behandlas enhetligt, utan att olika delar kan kodas på olika sätt och därmed även anpassas till förändringar. Om en del av skärmbilden innehåller en videosekvens kan fjärrskrivbordet välja en mer destruktiv komprimering av videosekvensen när den tillgängliga dataöverföringskapaciteten minskar.

De fjärrskrivbord som finns på marknaden i dag använder inte renodlat en av metoderna. En relativt ny utveckling är exempelvis att lägga hantering av Adobe Flash eller *Hypertext Markup Language version 5* (HTML5) på klienten (metod 1), även om den huvudsakliga metoden är 2 eller 3. Syftet med detta är att minska behovet av dataöverföringskapacitet samt öka interaktiviteten i Flash- eller HTML5-baserade tillämpningar genom lokal behandling. Metoden avlastar även fjärrskrivbordsservern beräkningsmässigt.

9.3.2 Användarupplevelse

Hur mycket interaktivitet användaren kräver av fjärrskrivbordet påverkar hur användaren märker av långa fördröjningar. För den som redigerar och läser textdokument kan fjärrskrivbord fungera bra med svarstid upp mot 200 ms samt en dataöverföringskapacitet på cirka 256 kbps.

Men om det istället är ett PDF-dokument användaren läser är det mycket möjligt att den visas som en bild vilket ökar behovet av dataöverföringskapacitet drastiskt. En applikation som ställer stora krav på interaktivitet kan bli oanvändbar när fördröjningen ökar även om behovet av dataöverföringskapacitet är lågt.

9.3.3 Uppstart av fjärrskrivbord

Vid uppstart av fjärrskrivbordstjänst sker alltid en förhandling mellan klient och server för att etablera en session som anpassas till anslutningens egenskaper. Vissa typer av fjärrskrivbord övervakar anslutningen när sessionen pågår och anpassar sessionen om anslutningens egenskaper ändras.

En del typer av fjärrskrivbord sparar parametrar från tidigare anslutningar för att snabbare uppstart. Förhandlingen kan annars ta relativt lång tid, särskilt om det som del av uppstartsförfarandet även sker uppmätning av anslutningens egenskaper.

Detta innebär att fjärrskrivbordstjänsten blir känslig för anslutningens tillgänglighet. En anslutning som är intermittent kan göra fjärrskrivbord särskilt svåra att använda då uppstart av session måste ske om och om igen.

9.3.4 ICA och HDX

Protokollet *Independent Computing Architecture* (ICA) är ett leverantörsspecifikt tjänsteprotokoll utvecklat av Citrix Systems. Huvudsyftet med protokollet är just fjärrskrivbord och det används i Citrix produkter, t.ex. WinFrame, XenApp/MetaFrame och XenDesktop. År 2009 bytte Citrix namn på ICA-protokollet till *High Definition Experience* (HDX). ICA använder TCP som transportprotokoll och skickar sitt data i små paket inuti denna anslutning. Protokollet inkluderar även komprimering och kryptering.

ICA:s inbyggda mekanismer för att minska behovet av dataöverföringskapacitet – komprimering samt temporär, lokal lagring av data (*cache*), gör att behovet varierar mycket med vad användaren gör. I Citrix egen utredning kan en enskild användare behöva från några få kbps till hundratals kbps för en skrivbordssession. Eftersom ICA används för interaktiva, och i vissa fall även synkrona tjänster, ställer det höga krav på fördröjningen. Enligt Citrix bör fördröjningen ligga under 150 ms för en god användarupplevelse. De av Citrix Systems program som använder ICA-protokollet har stöd för mjuk degradering av tjänsten vilket innebär att bildkvalitet och viss funktionalitet begränsas för att möta variationer i dataöverföringskapacitet och fördröjning.

ICA var från början baserad på klientbaserad rendering. HDX har dock stöd för såväl klientbaserad hantering av Adobe Flash som serverbaserad rendering. HDX kan dessutom använda Microsoft RemoteFX för rendering. ICA och HDX använder både datakomprimering med och utan informationsförlust. HDX inkluderar även funktionalitet motsvarande en WAN-accelerator och kan dynamiskt tillämpa komprimering och prioritering, och kan därigenom kontinuerligt anpassa tjänsten till anslutningens egenskaper.

För att sammanfatta ICA-protokollets egenskaper:

- Är ett TCP-baserat, leverantörsspecifikt protokoll för synkrona och interaktiva tjänster.
- Skickar små paket – vilket kan begränsa utnyttjandegraden av anslutningens kapacitet.
- Krypterar trafiken, vilket gör att WAN-acceleratorer som använder datakomprimering kommer att ge marginell effekt. Istället får ICA-protokollets inbyggda komprimering användas.
- Kräver relativt låga svarstider, mindre än 150 ms. Har dock stöd för att skala ner tjänstekvaliteten vid försämringar i anslutningens egenskaper.

9.3.5 RDP och RemoteFX

Remote Desktop Services (RDP) är namnet på den underliggande tjänsten som brukar kallas Microsoft Terminal Server. RDP var från början en fjärrskrivbordstjänst byggd på klientbaserad rendering, men i nuvarande version sker rendering även delvis på servern. RDP skickar GDI-element till klienten i komprimerad form. Klienten packar upp dessa element och tolkar dem, vilket genererar uppdateringar av klientens skärmbild.

Videorendering skedde tidigare helt på servern och då med enklare form av komprimering, mer av typen skärmavbildning. Detta innebar att en videouppspelning kunde påverka upplevelsen av hela fjärrskrivbordet genom en relativt stor ökning av behovet av dataöverföringskapacitet. I de senare versionerna kan videorendering i RDP ske lokalt.

Microsofts nya teknik för fjärrskrivbord kallas RemoteFX. Det är en teknik för serverbaserad rendering där grafikprocessorer i servern används för att accelerera bildkodning och komprimering. RemoteFX används i första hand som del i RDP, men även andra leverantörers tillämpningar kan utnyttja RemoteFX, t.ex. ICA/HDX.

Från version 7 av RDP-klienten stöds så kallad *client hint*. Detta är ett sätt för användaren att ange vilken typ av anslutning som används mot servern. Parametrarna skickas till servern vid start av en anslutning och används för att anpassa fjärrskrivbordet till de förväntade egenskaperna hos kopplingen. Några kategorier som finns är:

***Local Area Network* (LAN)** 10 Mbps eller bättre med låg fördröjning.

***Wide Area Network* (WAN)** 10 Mbps eller bättre med hög fördröjning.

Satellit 2 till 16 Mbps med hög fördröjning.

9.3.6 PCoIP

PC over IP (PCoIP) är ett protokoll för fjärrskrivbord definierat av företaget Teradici. PCoIP används i första hand i produkter från Teradici, men även i tredjepartsprodukter som VMware View.

PCoIP använder i huvudsak serverbaserad rendering. Grafikprocessorn i servern ansvarar för att bildkoda skärmbilden och komprimera dess olika delar, för att sedan skicka delarna till klienten med transportprotokollet *User Datagram Protocol* (UDP). Klienten fogar samman de olika delarna till den färdiga skärmbilden.

PCoIP använder både datakomprimering med och utan informationsförlust. Vilken metod som används för ett bildelement beror både på vad bildelementet innehåller och vilken dataöverföringskapacitet och fördröjning som uppmätts hos anslutningen. Så länge anslutningen har bra tillgänglig dataöverföringskapacitet och låg fördröjning används komprimering utan informationsförlust. När fördröjningen ökar och den tillgängliga dataöverföringskapaciteten minskar går PCoIP över till komprimering med informationsförlust där allt större mängd av bildens information sållas bort.

Teradici hävdar att PCoIP är okänslig för fördröjning. Men även om protokollet är okänslig för fördröjning kommer en ökad responstid göra interaktiva tjänster,

där användarens musrörelser och tangentbordstryckningar ska överföras, mindre användbara.

9.3.7 NX Technology

NX Technology (NX) är ett protokoll för fjärrskrivbord baserat på protokollet och fönstersystemet *X Window System* (X11). NX använder klientbaserad rendering och det som skickas över är X11-element. NX använder *Secure Shell* (SSH) för komprimering, kryptering och transport.

9.3.8 VNC

Virtual Network Computing (VNC) är ett fjärrskrivbord som ofta används för enklare typer av fjärrstyrning.

Det underliggande protokollet heter *Remote Frame Buffer* (RFB). RFB hanterar överföring av skärmbilder (*frame buffer*). För att minska kraven på överföringskapacitet skickas skillnaden mellan olika skärmbilder. RFB, och därmed VNC, är ett exempel på ett fjärrskrivbord baserad på ren skärmavbildning.

Den stora fördelen med VNC är portabiliteten. Eftersom det är rena skärmbilder som överförs är VNC i det närmaste systemagnostiskt. Det förekommer VNC-servrar och klienter till ett stort antal operativsystem och plattformar, vilket ger stor flexibilitet att välja server- och klientsystem.

Nackdelen med VNC är dåligt resursutnyttjande av tillgänglig dataöverföringskapacitet samt avsaknad av förmåga till anpassning till anslutningens egenskaper.

9.3.9 Jämförelser och slutsatser om fjärrskrivbord

Under 2011 presenterades resultaten av ett omfattande test [rdptest] av olika fjärrskrivbordsprodukters förmåga att hantera begränsningar i dataöverföringskapacitet, fördröjning och paketförluster. De fjärrskrivbordsprodukter som testades var:

- Microsoft RDP samt RDP 7.1 med RemoteFX
- Citrix ICA och HDX för XenApp och XenDesktop
- VMware/Teradici PCoIP
- Quest EOP
- Ericom Blaze
- HP RGS

Metodmässigt har testerna genomförts genom ett antal programstyrda, simulerade användningsfall. Fjärrskrivbordets beteende på klientsidan har sedan dokumenterats genom videoupptagning. Videoupptagningar för samma användningsfall, men med

olika fjärrskrivbord har sedan satts samman till en videofilm. Den sammansatta filmen gör det möjligt att observera de skillnader i kvalitet och användarupplevelse de olika fjärrskrivborden ger för varje användningsfall.

De testade användningsfallen inkluderar applikationer som använder text och enklare 2D-grafik, video- och animeringar, 3D-grafik samt interaktivitet i scriptmiljöer som Flash och Silverlight. Exempel på testfall är:

- Öppna, läsa och redigera text i Wordpad.
- Öppna och läsa PDF-dokument. Både att rulla mellan enskilda rader och hoppa hela sidor i dokumentet.
- Spela upp videofilmer i format som *Windows Media Video* (WMV) och QuickTime inklusive att styrt från klientsidan hoppa i videofilmen.
- Animationer och webbtillämpningar skapade i Flash och Silverlight.
- 3D-grafik med DirectX 9, DirectX 10, OpenGL och WPS (tekniken som används i Google Earth).

Anslutningen mellan klient och server har modellerats med en WAN-emulator från Apposite. WAN-emulatorn har även använts för att observera hur fjärrskrivborden använder den tillgängliga överföringskapaciteten vid kommunikationen mellan klient och server.

De begränsningar som använts är:

- Begränsning av dataöverföringskapacitet ned till 2 Mbps.
- Varierade fördröjningar från 0 till 200 ms.
- Paketförluster på upp till 1%, men i första hand satt till 0,01%. Målnätet som emulerats är MPLS-baserat företagsnät på nationell WAN-nivå.

I de jämförande tester som gjorts framkommer att HDX och EOP är de protokoll som bedömdes ge den bästa användarupplevelsen vid låg dataöverföringskapacitet och långa fördröjningar. Dessa produkter innebär rendering på klientsidan av flera tillämpningar, till exempel Flash, Silverlight och *Portable Document Format* (PDF).

Protokollen och produkterna är som regel resursgiriga och tar all tillgänglig dataöverföringskapacitet i anspråk. För en bra användarupplevelse krävs ungefär 2 Mbps. För en godtagbar användarupplevelse bedöms 256 kbps vara en nedre kapacitetsgräns.

Vid en responstid på 50 ms inträder en märkbar försämring av tjänstens kvalitet för de flesta av protokollen och produkterna. I de mer interaktiva användningsfallen inträder försämringar redan vid 20 ms. En fördröjning på 100 ms enkel väg anses vara den övre gräns i fördröjning som krävs för att fjärrskrivbordet ska vara användbart.

Paketförlusterna bör vara väsentligt mindre än 1%, och ingen av de testade produkterna fungerar tillfredsställande med en sådan nivå av paketförluster. De som utfört testet har prövat att använda WAN-acceleratorer. Deras bedömning är att

WAN-acceleratorer kan förbättra användarupplevelsen vid en nivå av paketförluster på upp mot 1%.

De nyare protokollen och produkterna[1] kräver GPU-hårdvara i såväl servern som klienten. Moderna tunna klienter är därför utrustade med särskilda hårdvaruacceleratorer för just RemoteFX.

En viktig skillnad mellan de olika fjärrskrivborden är vilka transportprotokoll som används. ICA/HDX och RDP/RemoteFX använder TCP, och ärver både styrkor och svagheter. PCoIP bygger däremot på UDP. Detta innebär att PCoIP har lägre andel överskottsdata för transport och kan reglera omsändningar i den mån det alls behövs. En annan konsekvens av olika transportprotokoll är hur de fungerar tillsammans med skyddmekanismer och tunnlar. Körs t.ex. ett UDP-baserat fjärrskrivbord över TCP påförs ytterligare mekanismer för omsändningar och ordnande av paket som kan leda till försämrad användbarhet och ökad kapacitetsförbrukning.

Några saker att beakta med fjärrskrivbord är:

- Fjärrskrivbord kan betraktas som en tunnelmekanism. Hur fjärrskrivbordet ska användas och vilken interaktivitet som krävs påverkar i hög grad på hur anslutningens egenskaper upplevs.

- Om det är grafiskt krävande applikationer som ska användas bör man överväga att använda implementationer av fjärrskrivbord som lägger delar av renderingen i klienten.

- Att om möjligt använda *client hint* och liknande mekanismer för att optimera förutsättningarna för fjärrskrivbordet.

- Anslutningens tillgänglighet kan vara kritisk. Om anslutningen bryts tar det lång tid att starta om fjärrskrivbordet – särskilt om anslutningen har hög fördröjning. Detta beteende kan snabbt göra fjärrskrivbordet oanvändbart även vid måttliga fördröjningar och användningsfall som inte ställer stora krav på interaktivitet.

- Om underliggande tunnelmekanismer används, beakta dess egenskaper och hur dessa fungerar tillsammans med transportprotokollet som används av fjärrskrivbordet.

- Fjärrskrivbord är som regel resursgiriga och kan i vissa fall ta oproportionerligt stor andel av tillgänglig dataöverföringskapacitet i anspråk. Tjänsterna använder dessutom ofta små datapaket, vilket begränsar utnyttjandegraden av anslutningens kapacitet.

[1] t.ex. RDP 7.1 med RemoteFX, Citrix HDX 3D och Teradici PCoIP

9.4 Grupprogramvara

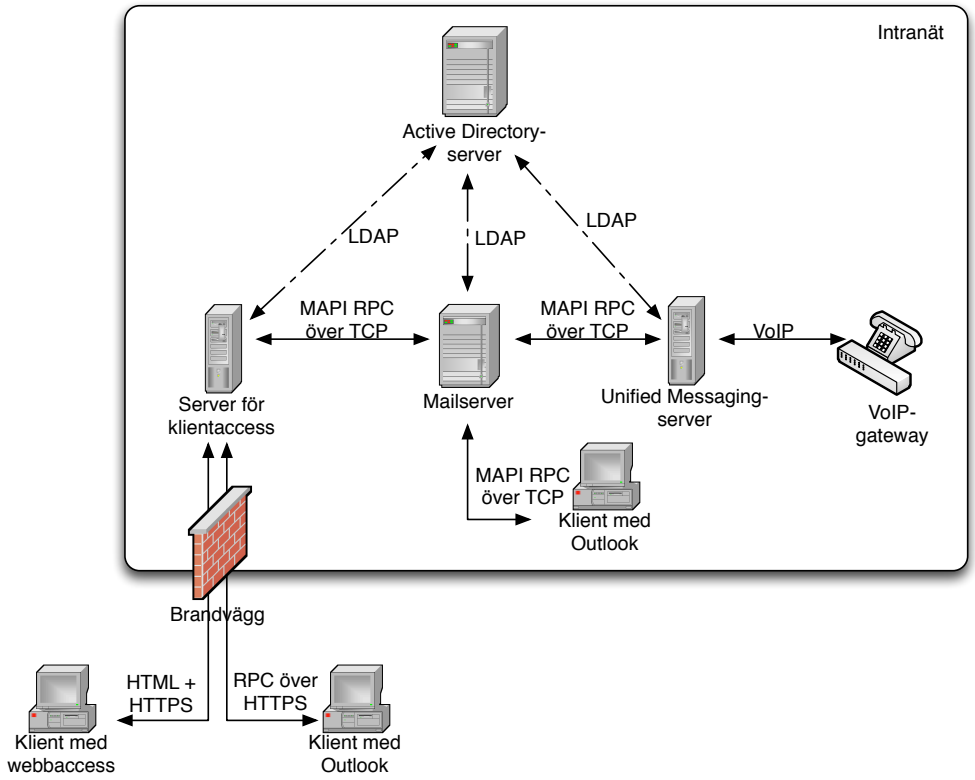
9.4.1 Microsoft Exchange Server

Microsoft Exchange Server (*Exchange*) tillhandahåller funktionalitet för e-post, kalender, adressbok och röstmeddelanden. Exchange används av ett stort antal företag och organisationer, och är en typtillämpning med en mängd beroenden till den övriga Microsoft-miljön.

Mängden tjänster en Exchangeserver kan tillhandahålla, vilka tjänster den kan bero på och därmed vilket möjligt kommunikationsbehov servern kan kräva varierar kraftigt beroende på hur servern ställts in.

En minimal Exchangeserver fungerar med *Messaging Application Programming Interface* (MAPI) över *Microsoft Remote Procedure Call* (MSRPC) mot användarna, samt *Simple Mail Transfer Protocol* (SMTP) [RFC2821] mot omvärlden. Om alla tjänster och funktioner slås på kan fler än 20 primära anslutningar krävas, och beroende på antalet samtidiga användare väsentligt fler än så.

Figur 9.9 illustrerar kommunikationsvägar mellan serverfunktioner i en Exchange-baserad tjänst för e-post, kalender och direktmeddelanden. *Client Access*, *Mailbox Server* och *Hub Transport* kan vara samma Exchange-server.



Figur 9.9 – Kommunikationstjänster och protokoll i en Microsoft-miljö

En typisk installation av Exchange inkluderar följande tjänster:

Mailbox Server är den funktion som lagrar användarens e-post och utbyter e-postmeddelanden med andra servrar, vilket sker med SMTP-protokollet. Mailbox server är också den funktion med vilken Outlook-klienten kommunicerar genom protokollet MAPI/MSRPC.

Hub Transport är en relä-funktion för att knyta samman flera Mailbox Server inom en och samma Exchange-installation. Kommunikationen sker med hjälp av protokollet X.400.

Client Access inkluderar stöd för *Outlook Web Access*, *Exchange ActiveSync* samt klientåtkomst till e-post via protokollen *Post Office Protocol - Version 3* (POP3) [RFC1939] och *Internet Message Access Protocol - Version 4* (IMAP4) [RFC3501].

Unified Messaging hanterar integration av röstmeddelanden från telefonsystemet via *Voice over IP* (VoIP), (*Session Initiation Protocol* (SIP) [RFC3261] och *Real-time Transport Protocol* (RTP) [RFC3550]).

Vidare krävs åtkomst till katalogtjänsten *Active Directory* för autentisering och behörighetsstyrning. Ska Exchange även kunna hantera extern e-post krävs *Edge Transport*-funktionalitet. Detta innebär i sin tur att det krävs en fungerande DNS-resolver för denna externa namnrymd.

De flesta av de funktioner som Exchange tillhandahåller är av typen transaktionsbaserade eller asynkrona tjänster. Detta innebär att tjänsterna kan förväntas fungera väl även över anslutningar med låg kapacitet och långa fördröjningar. Om Exchange ställs in för att hantera meddelandetjänster och särskilt för integration mot telefonisystem ökar dock kvalitetskraven på kommunikationslänken drastiskt. Valet av åtkomstmetod kan också vara avgörande för användarupplevelsen.

9.4.2 IBM Lotus Domino

IBM Lotus Domino (*Domino*) är en serverprodukt från IBM som tillhandahåller e-post- och gruppanvändartjänster. Domino kallades tidigare Lotus Notes Server, men namnet ändrades till Domino efter IBMs köp av Lotus.

Det primära klientprogrammet är IBM Lotus Notes (Notes), men många av Dominos tjänster går att använda med andra klienter och webbläsare.

De grundläggande tjänsterna Domino erbjuder är:

- E-post via protokollen *Notes Remote Procedure Call* (NRPC), POP3, *Internet Message Access Protocol* (IMAP), SMTP samt webbklienten iNotes (tidigare kallad Domino Web Access)
- Applikationsserver
- Webbserver
- Databasserver

- Katalogtjänst med *Lightweight Directory Access Protocol* (LDAP)

Domino kan även erbjuda tjänster för:

- Direktmeddelanden och webbaserade möten med IBM Sametime
- Dokumenthantering med Domino Document Manager
- Samarbetstjänst innefattande delat skrivbord med Domino Quickplace
- Applikationsserver för mobila klienter med Domino Everyplace
- Push-tjänster för handhållna enheter med Lotus Notes Traveler, vilken ger stöd för e-post, kalender, kontakter och aktiviteter (*tasks*)

Domino använder standardprotokoll, t.ex. IMAP, POP3 och *Hypertext Transfer Protocol* (HTTP) tillsammans med *Hypertext Markup Language* (HTML) för kommunikation med klienter. För Notes används däremot i första hand det leverantörsspecifika protokollet NRPC. Domino kan även utbyta objekt med andra applikationer med hjälp av objektstandarden *Common Object Request Broker Architecture* (CORBA).

All kommunikation mellan klienter och Domino samt mellan Domino och andra applikationer sker över TCP. Domino kan även använda *Network Basic Input/Output System* (NetBIOS) över *Internetwork Packet Exchange* (IPX). Dock är stödet för dessa i dag föråldrade protokoll normalt avstängt.

9.5 Strömmande media

Strömmande media innebär att information (vanligen ljud och/eller bild) skickas från en sändare till en mottagare i den takt som mottagaren använder informationen. Strömmande media skiljer sig därmed från tjänster som Poddradio (*Podcast*) där filerna skickas över i sin helhet till mottagaren innan innehållet i filen börjar användas.

Eftersom mediadata används i en viss sekvens och med en viss takt finns det en bortre gräns för hur försenat ett paket får bli för att vara användbart. Denna egenskap kan jämföras med nedladdning av en fil, där det viktigaste är att alla paket med alla delar av filen till slut kommer fram. Strömmande media ställer därmed större krav på överföringskapacitet, fördröjning, jitter och intermittens än vad filöverföring gör.

Några exempel på typiska tillämpningar som använder strömmande media är:

IP-telefoni – t.ex. SIP, Skype, Google Talk

Internetradio – t.ex. SHOUTcast och Microsoft Windows Media Services

Webb-TV – t.ex. HTML5 Streaming Media, Adobe Flash, Microsoft Windows Media Services

Fjärrsamarbeten – t.ex. IBM Lotus Sametime, Microsoft Lync, Cisco WebEx, Google+ Hangout och Adobe Connect.

Flera olika aspekter skiljer tjänsterna åt – aspekter som ställer olika krav på egenskapen hos den anslutning som används vid överföringen. Kommunikationen mellan parterna kan vara i huvudsak envägs, eller vara tvåvägs. Vid Internetradio är kommunikationen envägs och vid IP-telefoni är den tvåvägs.

Hur mediaströmmarna distribueras kan ske centraliserat, distribuerat, eller direkt mellan två parter (*peer to peer*). Strömmen kan också nätverksmässigt skickas till en enskild mottagare (*unicast*), till en grupp (*multicast*) eller i en öppen distribution (*broadcast*).

Olika tjänster och applikationer använder även olika signaleringsprotokoll för att initiera, upprätthålla och avsluta sessioner. Vidare används i vissa fall protokoll och mekanismer för att tillföra transportskydd.

Fjärrsamarbeten och fjärrskrivbord är i sammanhanget komplexa tjänster som kan inkludera flera olika typer av kommunikation, distribution, protokoll och mekanismer i samma produkt.

9.5.1 Envägs strömmande media

Envägs strömmande media innebär att en sändare skickar en ström med mediadata som sedan tas emot av en eller flera mottagare. Exempel på tjänster för envägs strömmande media är Internetradio och webb-TV. Envägs strömmande media används även för distribution av föreläsningar, tal och andra framträdanden.

SHOUTcast är ett protokoll för envägs strömmande media som används av många Internetradiostationer. Protokollet använder HTTP som transportprotokoll och skickar en ström till varje mottagare.

Den populära videotjänsten YouTube använder två olika överföringsmetoder, beroende på klient. För mobila klienter kontrolleras uppspelningen med *Real Time Streaming Protocol* (RTSP) [RFC2326], och för transport av mediaströmmen används RTP. Youtube stödjer även RTSP och RTP för HTML5-baserade klienter. För klienter som endast har stöd för Adobe Flash sker överföring och kontroll av mediaströmmen med HTTP.

Windows Media Services (WMS) är en produkt från Microsoft för att initiera tjänster för strömmande media. WMS stöder både ljud- och videotjänster och kan skicka strömmande media till flera olika klienter, däribland Windows Media Player. WMS är i grunden ett rent klient-server-baserat system som skickar strömmar till enskilda mottagare, grupper eller öppet. WMS kan använda UDP, TCP eller HTTP samt ett par leverantörsspecifika protokoll som transportprotokoll. WMS kräver från ca 2,4 kbps i dataöverföringskapacitet för mono-ljud till 6 Mbps för högkvalitativ video.

Tjänster med envägs strömmande media är oftast inte interaktiva. Dessa tjänster ställer därför låga krav på anslutningens fördröjning och fördröjningen går att dölja genom lokal buffring i klienten.

Multicast och broadcast kombineras normalt inte med stöd för klienter att få servern att starta, stoppa och hoppa i mediaströmmen, men med lokal buffring kan klienten själv hantera denna interaktivitet.

9.5.2 Tvåvägs strömmande media

Tvåvägs strömmande media innebär att två eller flera parter utbyter strömmande media med varandra. Tvåvägs strömmande media är därför oftast interaktiva realtidstjänster som ställer höga krav på anslutningens kvalitet, inte minst anslutningens fördröjning. Exempel på tjänster med tvåvägs strömmande media är IP-telefoni och fjärrsamarbeten.

Skype är kanske den idag vanligaste IP-telefonitjänsten på Internet. Skypeklienterna kommunicerar med varandra distribuerat och via andra klienter (*peer to peer*). Klienter kan inte själva välja om dom vill hjälpa till att transportera trafik mellan andra klienter. Om en klient har tillräckligt med dataöverföringskapacitet och beräkningskapacitet kan klienten av Skypes server automatiskt klassificeras som en supernod och kommer då att börja hantera trafik mellan olika klienter. Skype använder ett leverantörsspecifikt protokoll för signalering och överföring av mediaströmmar. Signaleringsdelen använder TCP som transportprotokoll och överföringsdelen av protokollet använder UDP eller TCP.

IBM Lotus Sametime är ett tillägg till grupprogramvaran IBM Lotus Domino och klienten IBM Lotus Notes. Sametime gör det möjligt för en grupp av användare att i realtid fjärrsamarbeta. Sametime stöder bland annat möjligheten att dela på och arbeta på gemensamma dokument, videokonferens samt meddelandeutbyte. Sametime använder både TCP och UDP för transport och kan nyttja *Extensible Messaging and Presence Protocol* (XMPP) [RFC6120] för signalering gentemot andra klienter.

Microsoft Lync, tidigare kallad Microsoft Office Communicator, är en produkt för fjärrsamarbete som stöder IP-telefoni, videokonferens, meddelandeutbyte, delade arbetsytor m.m. Lync använder RTP för mediatransport, TCP för meddelandetransport och SIP för signalering.

9.5.3 Signalering i strömmande media

Även om transporten av mediaströmmar sker med UDP och RTP [RFC3550], vilka är enkla protokoll som inte kräver mycket kapacitetsutrymme, behöver parterna i kommunikationen där mediaströmmen används kunna signalera till varandra. Signaleringen används för att initiera mediaströmmen, kontrollera mediaströmmen när den pågår samt för att kunna avsluta mediaströmmen. Flera vanliga protokoll som används för signalering förekommer:

SIP [RFC3261] används för att etablera, kontrollera samt avsluta sessioner mellan två eller fler deltagare. En session kan innehålla en eller flera mediaströmmar med olika egenskaper. SIP används av ett stort antal tjänster och produkter, bland annat i 3GPP IP Multimedia Subsystem och Microsoft Lync.

XMPP [RFC3550] är ett protokoll baserat på *Extensible Markup Language* (XML). XMPP används i första hand för meddelandetjänster, men används även av Google Talk som signaleringsprotokoll [Jingle]. XMPP stöds även av Microsoft Lync.

För att övervaka en RTP-transporterad ström finns signaleringsprotokollet *Real Time Control Protocol* (RTCP) [RFC3550]. Det huvudsakliga syftet med RTCP är att kunna

övervaka anslutningens kvalitet och göra det möjligt för det RTP-kommunicerande parterna att anpassa sig till anslutningens egenskaper. Protokollet RTSP [RFC2326] används för att att initiera och styra en mediaström skickad från en server för att göra det möjligt att från klienten starta, stoppa och hoppa i mediaströmmen.

9.5.4 Kryptering och strömmande media

Strömmande media kan av olika skäl kräva säkerhetsfunktioner. Eftersom transporten av strömmande media ofta sker med små paket bör storleken på stödinformationen som krävs för säkerhetsfunktionerna hållas minimal.

För de tillämpningar som använder RTP för transport och RTCP för signalering finns två motsvarande varianter av protokollen kallade *Secure RTP* (SRTP) [RFC3711] och *Secure RTCP* (SRTP) [RFC3711]. Dessa varianter lägger till säkerhetsfunktioner för äkthetskontroll, integritetsskydd, konfidentialitetsskydd samt mot bedräglig återuppspelning av mediaströmmen.

För konfidentialitetsskydd används i SRTP det symmetriska blockkryptot *Advanced Encryption Standard* (AES). För autenticering, integritetsskydd samt skydd mot återuppspelning används i SRTP *Keyed-Hashing for Message Authentication* (HMAC) med den kryptografiska hashfunktionen SHA-1.

Signaleringsprotokollet XMPP kan använda separata säkerhetsprotokoll som *Simple Authentication and Security Layer* (SASL) och *Transport Layer Security* (TLS) för att tillföra säkerhetsfunktioner. Även SIP kan använda TLS som säkerhetsmekanism.

Skype använder strömkryptot RC4 för att försvåra tolkning av signaleringsdelen av Skype-protokollet, dock sker nyckeldistribution inuti anslutningen utan stark autentisering. Skype använder AES för konfidentialitetsskydd av mediadata.

9.6 Infrastrukturella tjänster

9.6.1 DNS

Protokollbeskrivning

Katalogtjänsten *Domain Name System* (DNS) [RFC1034][RFC1035] används för översätta domännamn till olika former av data. Det absolut vanligaste användningsfallet är översättning av domännamn (t.ex. www.example.org) till IPv4- och IPv6-adresser, men systemet används även för att slå upp information som styr dirigering av e-post, IP-telefonisamtal och direktmeddelanden. Andra katalogsystem, t.ex. Microsoft *Active Directory* (AD), har ofta direkt eller indirekt koppling till DNS då information om hur man kontaktar katalogsystemen publiceras via DNS.

På senare år har DNS, som i grunden helt saknar säkerhetsfunktioner, kompletterats med säkerhetstillägget *Domain Name System Security Extensions* (DNSSEC) [RFC4033]. Med hjälp av DNSSEC erhålls säkerställande av ursprung (*Data Origin Authentication*) samt integritetsskydd (*Data Integrity*).

DNS är ett asynkront, meddelandebaserat protokoll som i huvudsak använder sig av transportprotokollet UDP. En DNS-förfrågan består oftast av ett enskilt

UDP-datagram med en maximal längd på 512 oktetter. Svaret på en DNS-förfrågan består normalt av ett enskilt UDP-datagram med en maximal längd på 512 oktetter.

När större meddelanden krävs kan DNS-meddelanden antingen transporteras över TCP, alternativt kan en utökning (*Extension Mechanisms for DNS* (EDNS) [RFC2671]) användas för att förhandla fram att UDP-datagram med en maximal längd på 65 535 oktetter får användas. Det senare fallet kan innebära att ett meddelande kan komma att fragmenteras om det skickas via UDP. Det bör också nämnas att det finns implementationer av DNS som endast använder TCP, liksom implementationer som endast använder UDP.

Nätkrav

DNS innehåller stöd för omsändningar, normalt görs en omsändning om inget svar erhållits på en förfrågan inom 3–5 sekunder. De flesta implementationer som används idag mäter kontinuerligt svarstiden, *Round Trip Time* (RTT), mot de DNS-servrar de kommunicerar med, och justerar baserat på svarstiderna kontinuerligt sina parametrar för omsändning. Detta gör att DNS är förhållandevis robust mot både långa fördröjningar och paketförluster.

I klassisk DNS är både frågor och svar alltid mindre än 512 oktetter. Introduktionen av DNSSEC (och därmed EDNS) har dock medfört att mängden data som överförs ökat, dock håller sig de flesta DNS-meddelanden under 1 500 oktetter och undviker därför fragmentering av UDP alternativt omsändning via TCP. Vid transport över en nätinfrastruktur som har en maximal paketstorlek (MTU) på 1 500 oktetter är därmed risken för fragmentering relativt liten. Vill man trots detta eliminera risken för fragmentering kan de flesta DNS-programvaror ställs in att alltid använda TCP om ett meddelande överstiger en i förväg bestämd paketstorlek.

9.6.2 LDAP

Protokollbeskrivning

LDAP [RFC4511] är ett protokoll för att kommunicera med katalogtjänster. Protokollet har till stora delar influerats av X.500 *Directory Access Protocol* (DAP) och var ursprungligen tänkt att fungera som ett enklare protokoll för att kommunicera med X.500-baserade kataloger. Idag är LDAP är en komplett protokollsvit innefattande kommunikationsprotokoll (LDAPv3), en datamodell och tillhörande syntaxbeskrivningar.

LDAP transporteras över TCP, oftast med skyddat med TLS [RFC5246].

Nätkrav

De krav som LDAP ställer på underliggande nätinfrastruktur beror till stor del på hur protokollet används av bakomliggande applikation (klient). Ett exempel på en LDAP-klient med krav på korta svarstider är *Microsoft Exchange Server*, vars funktion riskerar störas om tiden för en LDAP-fråga överskrider 50 ms. Ett sätt att hantera detta problem är att LDAP-databasen replikeras till en maskin nära klienten.

9.6.3 Kerberos

Protokollbeskrivning

Autentiseringsprotokollet Kerberos [RFC4120] används för verifiera identiteten hos en entitet (*principal*) över ett öppet nätverk. Verifieringen sker med hjälp av en betrodd tredje part – *Key Distribution Center* (KDC). Flera KDC kan finnas i ett nätverk och data kan replikeras mellan dessa.

Vanliga implementationer av Kerberos är *MIT Kerberos*, *Heimdal* och *Microsoft Active Directory* (AD).

Nätkrav

Kerberos transporteras normalt sett över UDP, men kan även transporteras över TCP. På samma sätt som för LDAP är det den bakomliggande applikation som ställer krav på svarstid, men generellt bör lokalt placerad KDC finnas om fördröjningen i nätverket är särskilt hög. Kerberos kräver förhållandevis lite dataöverföringskapacitet och ett komplett nyckelutbyte hanteras på 4 UDP-paket, alla under 600 oktetter.

9.6.4 DHCP

Protokollbeskrivning

Protokollet *Dynamic Host Configuration Protocol* (DHCP) [RFC2131] och *Dynamic Host Configuration Protocol for IPv6* (DHCPv6) [RFC3315] används för att kommunicera dynamiska nätverksparametrar till enheter på ett TCP/IP-nätverk. Primärt används protokollet för att tilldela enheter IP-adresser tillsammans med andra viktiga parametrar, t.ex. DNS- och NTP-servrar. DHCP är från början konstruerat som en utbyggnad av *Bootstrap Protocol* (BOOTP) [RFC951], men har under åren tillförts allt mer funktionalitet.

DHCP transporteras över unicast-UDP för *Internet Protocol version 4* (IPv4) och unicast/multicast-UDP för *Internet Protocol version 6* (IPv6). I de fall klient och server inte är anslutna till samma länknät används ett reläfunktion (*DHCP Relay Agent*) för att vidarebefordra meddelanden mellan klient till server. Reläfunktionen är transparent för klienten, men klienten får efter svar från servern kännedom om serverns adress och kan i vissa fall kommunicera direkt med servern i efterföljande transaktioner.

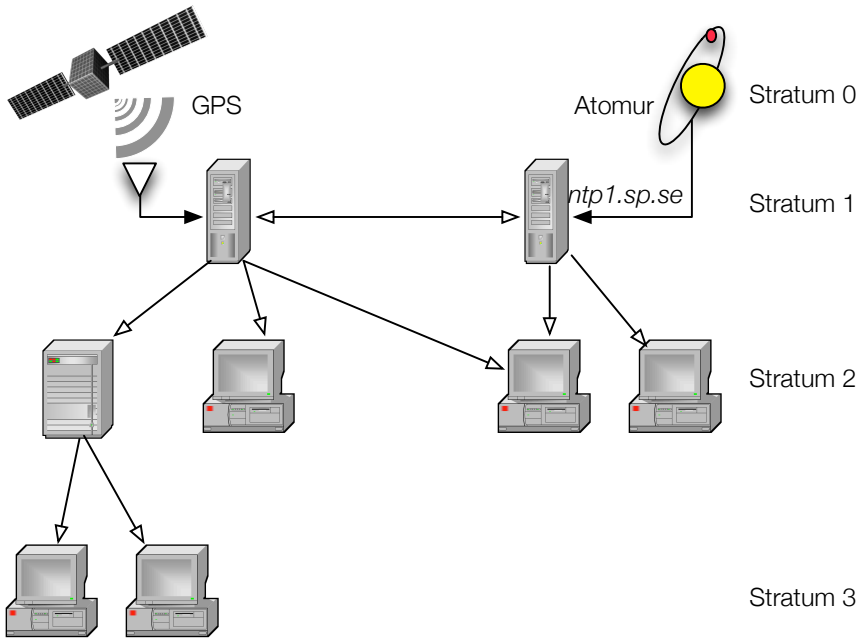
Nätkrav

Då DHCP använder sig av UDP krävs att protokollet själv ansvarar för omsändning vid paketförlust. En normal DHCP-begäran ligger på ca 400 oktetter och en klient förväntar sig normalt svar inom 2 till 4 sekunder, vilket gör att protokollet skulle kunna få problem över länkar med särskilt lång fördröjning. Det bör påpekas att DHCP-servrar vanligen placeras förhållandevis nära sina klienter, och att långa svarstider därför sällan är ett problem.

9.6.5 NTP

Protokollbeskrivning

Tidsgivningsprotokollet *Network Time Protocol* (NTP) [RFC5905] används för att synkronisera och koordinera distribution av tid.



Figur 9.10 – Två olika stratum 1-maskiner är kopplade till var sin fysisk tidskälla. Servrarna delar ut tid till ett antal klienter som blir Stratum 2. Klienterna kan i sin tur agera server åt Stratum 3-klienter.

NTP bygger på en hierarki av enheter som tillhandahåller tidsinformation till användare av enheten såväl som andra enheter. Enheterna klassificeras i *stratum*-nivåer där precisionen minskar med ökande nivå. Stratum 0 utgörs av fysiska källor till tid, typiskt olika typer av atomur, exempelvis vätemaser eller oscillatorer byggda av Cesium. Stratum 1-enheterna kan vara direkt anslutna till Stratum 0-källorna, men kan även hämta tidsinformationen trådlöst, exempelvis som del av GPS-signalen.

Exempel på en Stratum 1-server är *ntp1.sp.se* som tillhandahålls av SP i Borås. Tiden denna Stratum 1-server tillhandahåller går att spåra till den svenska officiella tidsskalan kallad *Coordinated Universal Time* (UTC) (SP).

Coordinated Universal Time (UTC)

UTC är den primära standarden i världen för att reglera klockor och tid. Tiden i UTC bygger på *International Atomic Time* (TAI), ett beräknat tidsmått som skapas utifrån ett stort antal atomur runt om i världen, däribland SPs atomur i Borås. Utifrån TAI skapas sedan UTC genom att när det behövs justera tiden med skottsekunder, så att tiden aldrig avviker med mer än en sekund från dygnstiden för jordens rotation, kallad UT1.

Stratum 1-enheterna tillhandahåller i sin tur tidsinformation till Stratum 2-enheterna. Stratum 2-enheterna är oftast klienter till Stratum 1-enheter, men kan i sin tur dela ut tidsinformation till Stratum 3-enheter. En organisation kan etablera en lokal Stratum 2-enhet som fungerar som lokal tidsserver. NTP-klienter kan även hämta tid från flera källor.

I de fall där inte all funktionalitet som erbjuds av NTP krävs, t.ex. när ett ändsystem endast ska mottaga korrekt tid från en eller flera gemensamma tidsservrar, kan den enklare varianten *Simple Network Time Protocol* (SNTP) användas. SNTP är i praktiken en profilering av NTP, där endast de grundläggande funktionerna används.

NTP använder sig enbart av UDP-datagram och paketlängden är i praktiken aldrig större än 128 oktetter.

Nätkrav

NTP är konstruerat och väl optimerat för de flesta typer av förbindelser, och fungerar väl även i nätverk med höga fördröjningar. NTP ställer inte heller några krav på vare sig flödeskontroll eller omsändningsmekanismer – de algoritmer som används justerar sig automatiskt, men kan kräva längre tid för att erhålla full synkronisering vid stora paketförluster. NTP kan också kompensera för jitter genom att skicka flera frågepaket istället för ett. Dessa egenskaper gör att NTP uppvisar hög robusthet och inte ställer några särskilda krav på underliggande nätverk.

9.6.6 Icke IP-baserade protokoll för takt och tid

PTP

Precision Time Protocol (PTP) är ett Ethernetbaserat protokoll med egen Ethernettyp som PTP-enheter måsta känna till. I ett lokalnät kan PTP ge synkronisering med precision på delar av mikrosekunder.

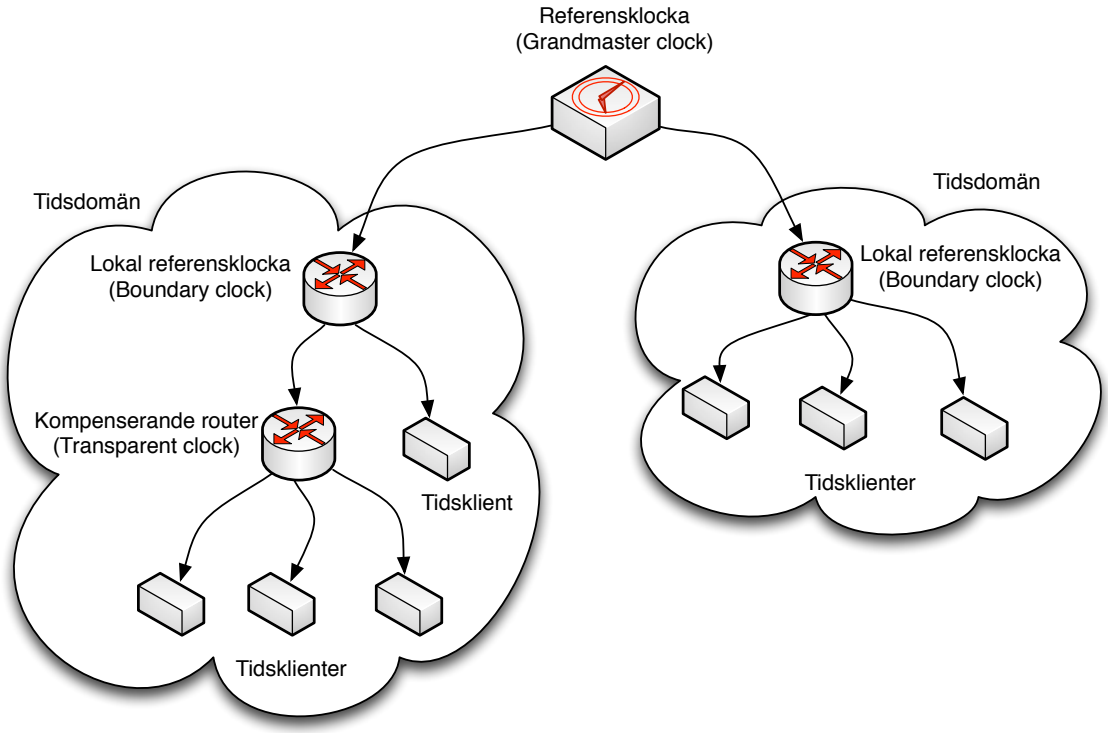
PTP-meddelanden kan även skickas över IP-baserade nät och använder då UDP-datagram för transport. Referensklockan skickar ut meddelanden adresserade till en grupp av klockor (*multicast*-adresser). I IEEE 1588v2 infördes även möjligt att direkt adressera enskilda klockor och använda *unicast*.

Protokollet utvecklades från början för att synkronisera industriella styr- och mätutrustningar, militära system samt eldistribution. I dag används PTP i flertalet tillämpningar, från t.ex. klockor för offentliga miljöer) till att synkronisera tid i stora nätverk, exempelvis mobilnät.

Den första versionen av PTP, IEEE 1588 [IEEE1588] publicerades 2002. År 2008 punlicerades en ny version av specifikationen, IEEE 1588v2. Den nya versionen ger bättre precision, tillförlitlighet och robusthet, och är inte bakåtkompatibel med den tidigare versionen.

Principen bakom PTP är att det i ett nät finns en klocka som fungerar som referensklocka (*Grandmaster clock*). I en grupp av klientklockor, en domän, lyssnar en lokal referensklocka kallad *Boundary clock* på meddelanden från referensklockan. Den lokala referensklockan ser sedan till att distribuera klockmeddelanden till klienterna inom domänen. Klienterna uppdaterar sina klockor utifrån dessa meddelanden. IEEE 1588 stödjer även möjligheterna till att ha flera domäner, flera referensklockor samt att klockorna sinsemellan kan bestämma vilken klocka som ska agera referensklocka.

IEEE 1588v2 introducerade transparenta klockor, *Transparent clock*. Transparenta klockor är nätelement som övervakar fördröjningen av meddelanden genom nätelementet självt. När ett meddelande från referensklockan passerar nätelementet uppdateras meddelandet för att kompensera för fördröjning och varians.



Figur 9.11 – PTP: En *Grandmaster clock* skickas till två separata domäner. En lokal referensklocka, *Boundary clock* distribuerar sedan klockinformationen till klienter inom sin domänen, i vissa fall via utrustning som kompenserar för sin egen fördröjning, en s.k. *Transparent clock*.

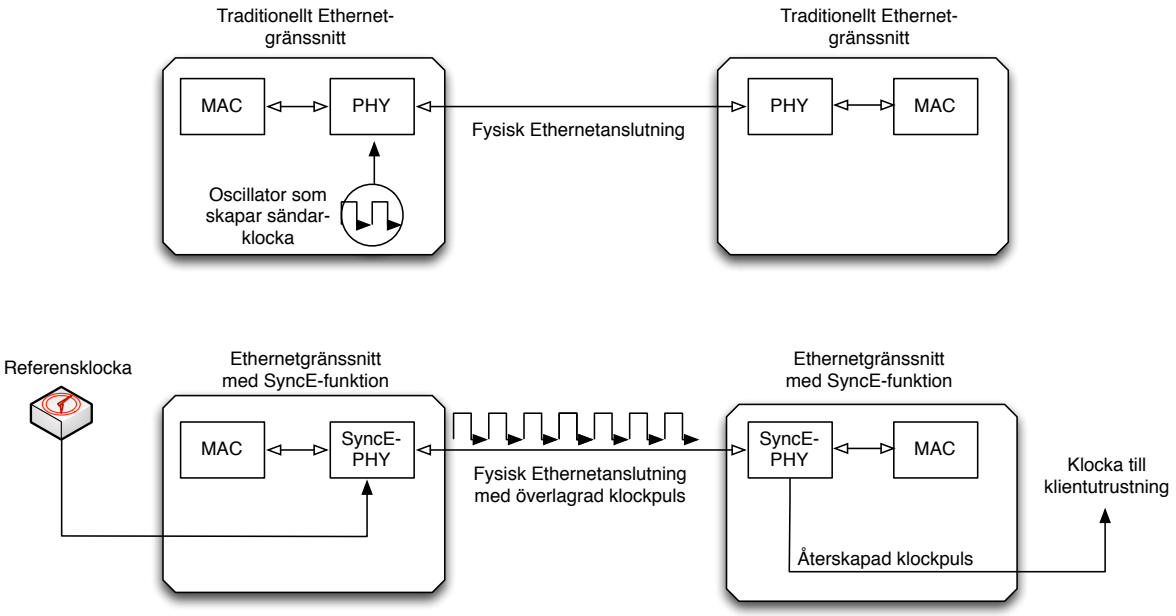
SyncE

Synchronous Ethernet (SyncE) [SYNCE] är en standard från ITU-T för att synkronisera klockor över ett Ethernetbaserat nätverk. SyncE är ett protokoll som verkar på lager ett i OSI-modellen, det vill säga det fysiska lagret. Frekvensinformationen överlagras på den fysiska signal som används för att bära Ethernetramen. Detta innebär att de fysiska portar som ska användas för SyncE måste stödja protokollet.

SyncE används för att distribuera synkroniseringsinformation i Ethernetbaserade nät. Till skillnad från NTP och PTP ger SyncE ingen information om tid, utan bara en frekvens. SyncE gör det möjligt för generatorer av klockpulser (oscillatorer) i olika nätelement att generera pulser som sinsemellan är synkrona.

Utifrån en frekvensnormal som genererar frekvensinformation propageras informationen från ett nätelement till nästa. Eftersom varje element i en kedja tillför varians försämras synkronismen ju längre bort från normalen ett element befinner sig. Detta ställer även krav på precisionen hos frekvensnormalen.

SyncE ställer krav på fördröjning och varians ett element får införa på den transporterade frekvensinformationen. För ett nät med ett djup på fyra element kan SyncE ge stabil frekvens med ett fel på under 25 ns.



Figur 9.12 – Synkroniseringspulser från en referensklocka överlagras Ethernetsignalen via SyncE-anpassade Ethernetgränssnitt.

2 MHz-synkronisering

Mikrovågsutrustning från Ericsson kapabel att transportera synkron trafik (*TDM-trafik*) som *Plesiochronous Digital Hierarchy* (PDH) och *Synchronous Digital Hierarchy* (SDH) har även stöd för att lägga ut en synkroniseringspuls på en separat

port. Synkroniseringssignalen har en frekvens på 2,048 MHz och kallas därför för 2 MHz-synkronisering.

2 MHz-synkroniseringen är en ren synkroniseringssignal som inte innehåller information om tid eller datum. Signalen är en elektrisk puls med signalnivåer enligt standarden G.703.

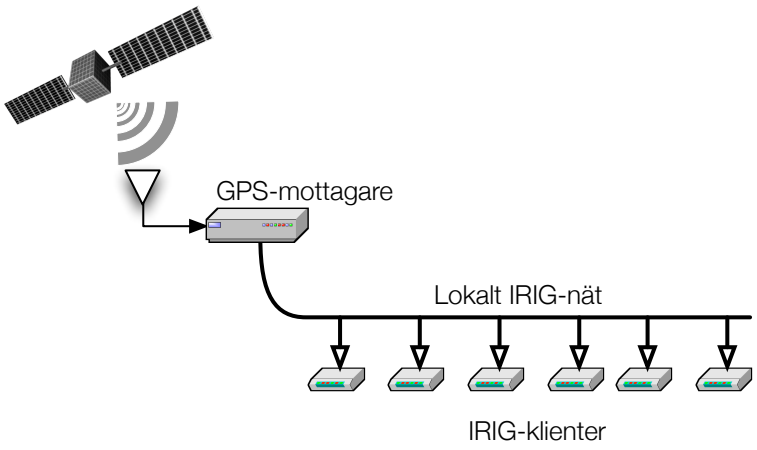
Synkroniseringssignalen kan traversera ett eller flera mikrovågshopp och kopplas till en godtycklig källa, antingen en extern källa eller synkroniseringskällan som driver PDH, SDH, SyncE eller PTP.

IRIG

Inter-Range Instrumentation Group (IRIG) är en uppsättning protokoll avsedda att distribuera datum och tid. Protokollen härstammar från 1970-talet och kommer i flera olika versioner – A, B, C, D, E, G och H. Skillnaderna mellan de olika versionerna är hur ofta tidsinformationen uppdateras. För IRIG-B är uppdateringsfrekvensen en gång per sekund. IRIG distribueras med hjälp av en bärfrekvens och bärfrekvensen ger precisionen på tidsinformationen. För IRIG-B122 är precisonen en millisekund.

Protokollet är ett enkelt länklagerprotokoll för distribution av tid i en lokal anläggning. Det förekommer bryggor som gör det möjligt att koppla IRIG till NTP eller PTP. Det finns även utrustning kapabel att transportera IRIG över Ethernet. Normalfallet för IRIG är att det är ett länklagernät kopplat till en lokal klocka. Klockan kan antingen innehålla en klockkälla eller hämta klockinformation från exempelvis *Global Positioning System* (GPS).

IRIG har haft stor användning inom industriell kontroll och automation, inte minst inom kraftproduktion och kraftdistribution. IRIG-protokollets enkelhet gör det lätt att i en anläggning få industriella enheter att lyssna på samma IRIG-signal och vara synkroniserade.



Figur 9.13 – En GPS-mottagare tar emot tidssignaler och skickar ut tidsinformation på ett lokalt IRIG-nät till vilket ett antal klienter är anslutna.

IRIG-protokollet har dock börjat ersättas av det modernare protokollet PTP.

Ordlista

Anslutning

En nätverksmässig förbindelse mellan två parter när parterna kommunicerar.

Asynkron tjänst

I en asynkron tjänst är parterna som kommunicerar frikopplade från varandra. Överföringen ställer inte krav på att båda parterna är aktiva. Typiskt innehåller dessa tjänster stöd för att lagra meddelanden samt att repetitivt försöka skicka meddelanden tills dess att de kommer fram. Exempel på asynkron tjänst är e-post.

bps

Förkortning. Bit per sekund. Används för att ange överföringskapacitet. Anges oftast med prefix för kilo (k), Mega (M) eller Giga (G).

Bps

Förkortning. Byte per sekund. Används för att ange överföringskapacitet i antalet oktetter av bitar. Anges oftast med prefix för kilo (k), Mega (M) eller Giga (G).

Blockkrypto

En funktion som givet en nyckel transformerar ett datablock. Enbart utifrån det transformerade datablocket är det ytterst svårt att återtransformera datablocket. För att återtransformera datablocket krävs att samma nyckel används. Datablocket kryptot transformerar har en fix storlek, normalt 8, 16 eller 32 oktetter.

En funktion som givet en nyckel transformerar ett datablock. Enbart utifrån det transformerade datablocket är det ytterst svårt att återtransformera datablocket. För att återtransformera datablocket krävs att samma nyckel används. Datablocket kryptot transformerar har en fix storlek, normalt 8, 16 eller 32 oktetter.

Bästa förmåga

En anslutning som arbetar efter principen bästa förmåga, (*"best effort"*) ger inga garantier om eller bekräftelse på att överförd information når mottagaren.

Anslutningen ger inte heller några löften om kvalitet i fråga om fördröjning eller prioritet.

I en anslutning som arbetar efter principen bästa förmåga binds inga resurser upp i förväg inför att information ska överföras, utan de resurser som krävs för överföringen allokeras när överföringen sker.

Ett exempel på anslutning som arbetar efter principen bästa förmåga är IP-baserad kommunikation.

Dataöverföringskapacitet

Mängden data per tidsenhet en anslutning kan överföra. Begreppet används även för att ange den mängd data per tidsenhet en tjänst behöver kunna överföra för sin funktion. Dataöverföringskapacitet benämns även genomströmningskapacitet (*throughput*) eller bithastighet (*bitrate*).

Ibland används ordet bandbredd (ofta felaktigt) som benämning för dataöverföringskapacitet. Med ordet bandbredd avses skillnaden mellan den övre och den lägre avbrytande frekvensen i det spann av frekvenser som används för en informationsöverföring i radiokommunikation eller i en kabel. Det kan emellertid vara stor skillnad på teoretiska bandbreddskapaciteten och den verkliga/effektiva överföringskapaciteten.

Diversitet

Kommunikation över olika typer av fysiska media. Exempelvis fiber i kombination med mikrovågslänk. Diversitet används för att öka robustheten hos en anslutning. De olika fysiska media som används kan även vara geografiskt separerade.

Ethernet

En typ av protokoll för paketbaserad kommunikation som används för kommunikation på länklagernivå. Från början avsedd för enklare lokalnät men har genom olika tillägg, exempelvis 802.1Q och 802.1ad blivit ett generellt nätverksprotokoll för lokalnät (*Local Area Network – LAN*), stadsnät (*Metro Area Network – MAN*) och i vissa fall även fjärranslutningar (*Wide Area Network – WAN*). Ethernet används ofta för att bära IP-baserad trafik.

Fördröjning

Den tid det tar enkel väg att överföra en bit från en part till dess motpart över en anslutning. Fördröjning kallas även för latens. Tiden inkluderar både den fysiska överföringen genom mediet (radiovågor, ljus, elektrisk signal) och processtiden i utrustning (switchar, routers, mediakonverterare, nätverksprocessorer etc).

I praktiska tillämpningar påförs även fördröjningseffekter genom den tid som åtgår för serialisering och deserialisering av de datastrukturer som överförs. Det innebär

att även dataöverföringskapaciteten är en parameter vid beräkning av den totala fördröjningen mellan de kommunicerande parterna.

Interaktiv tjänst

En interaktiv tjänst innebär att en människa finns bakom minst en av parterna i en kommunikation. Till skillnad från en synkron tjänst är kraven på maximal fördröjning, omsändning och ordning inte lika hårda. Ett exempel på en interaktiv tjänst är fjärrskrivbord.

Intermittens

Ett mått på en anslutnings tillgänglighet över tiden, det vill säga hur ofta kommunikationen bryts och för hur länge. En förbindelse där bortfallen är frekventa men korta, kan för vissa tjänster fungera väl, medan beteendet för andra tjänster kan tvinga fram omstarter i en sådan omfattning att tjänsten blir obrukbar.

Jitter

Den varians i fördröjning som en kommunikationskanal utsätts för över tiden. Jitter är alltså inget som mäts eller anges för ett enskilt paket. Jitter påverkar applikationer med realtidskrav där data måste komma fram vid en viss tidpunkt för att vara användbar. Jitter kan även vara mer eller mindre skurigt, vilket innebär att mängden jitter i sig varierar över tiden.

Länk

Punkt till punkt-anslutning på lager länklagernivå. En eller flera länkar bär en anslutning mellan två kommunicerande parter. Ett exempel på länk är en Ethernetförbindelse.

Nätverksprotokoll

Specificerade regler och datastrukturer som tillsammans definierar hur olika parter ska kommunicera med varandra. Exempel på nätverksprotokoll är IPv4 och IPv6. Nätverksprotokollen är implementerade i operativsystem och i nätverksutrustning.

Paketbaserad kommunikation

Digital kommunikation där den information som överförs delas upp i separata delar, paket. Paketen transporteras var för sig från sändare till mottagare över en eller flera olika anslutningar. Mottagaren sätter samman paketen för att erhålla den överförda informationen.

Roaming

Förflyttning av en klient mellan två olika basstationer i en infrastruktur för trådlös kommunikation, t.ex. mobildatanät eller trådlöst lokalnät.

Robusthet

Förmåga att stå emot olika typer av störningar. Robusthet kan gälla tjänster, anslutningar, när och enskilda fysiska enheter.

Serialisering

Serialisering är en process där en datastruktur omvandlas till ett format lämpligt att skickas över en anslutning. Datastrukturen återskapas vid mottagning till sitt ursprungliga format med en omvänd process kallad deserialisering.

Spoofing

Spoofing innebär att en nätverksenhet protokollmässigt utger sig för att vara en annan enhet genom att härma enhetens beteende. Ett exempel på spoofing är WAN-acceleratorer som i förväg bekräftar TCP-segment som skickas över WAN-anslutningen. WAN-acceleratorns bekräftelser döljer därmed WAN-anslutningens responstid för den sändande parten. Däremot måste WAN-anslutningen själv hantera omsändningar som uppkommer för de TCP-segment den i förväg bekräftat.

Strömkrypto

Strömkrypton består i huvudsak av en sekvensgenerator. Givet ett startvärde, ett frö, skapar generatorn en sekvens slumpmässigt utvalda värden. Men generatorn är deterministisk och givet samma frö genereras därför alltid samma sekvens av värden. Generatorn är därmed en *Pseudo Random Number Generator* (PRNG). De genererade värdena används i tur och ordning för att transformera dataelement i det data som ska överföras. Strömkrypton genererar normalt nyckelvärden med samma bitlängdsmässigt maximal storlek som dataelementen.

Svarstid

Svarstid är ett annat mått på fördröjning, som anger den minimala tid det tar att skicka en bit till en motpart och erhålla ett svar.

Synkron tjänst

Båda parter i kommunikationen är aktiva och för att tjänsten ska fungera finns det stränga krav på maximal fördröjning och varians, minsta tillgängliga

dataöverföringskapacitet, bevarande av ordning på paketen samt maximal paketförlust. För vissa synkrona tjänster blir ett paket värdelöst om det inte kommer fram vid en viss tidpunkt. Exempel på synkron tjänst är IP-telefoni.

Transaktionsbaserad tjänst

En transaktionsbaserad tjänst innebär att den ena parten – klienten – begär resultat från den andra parten – servern. Resultatet leder till minst ett svar från servern, men kan även ge upphov till en uppsättning transaktioner mellan parterna. Exempel på transaktionsbaserad tjänst är webbsurf.

Transportprotokoll

Ett protokoll som givet ett nätverk med adresserbara noder transporterar information från en nod till en annan genom nätverket. Ett exempel på transportprotokoll är TCP.

Tunnling

Tunnling innebär att trafik transporterad med en typ av kommunikationsprotokoll kapslas in och överförs mellan två noder i ett nät. Tunnling används för att transportera äldre typer av kommunikationsprotokoll över nyare, exempelvis PDH över Ethernet. Tunnling kan även användas för att tillföra den transporterade trafiken nya egenskaper, exempelvis skydd mot avlyssning eller robusthet mot störningar.

Förkortningar

AD Active Directory

AES Advanced Encryption Standard

AFS Andrew File System

AH Authentication Header

API Application Programming Internet

ATA AT Attachment

ATM Asynchronous Transfer Mode

BOOTP Bootstrap Protocol

CBC Cyclic Block Chaining

CDMA Code Division Multiple Access

CES Circuit Emulation Service

CIFS Common Internet File System

CLI Command Line Interface

CORBA Common Object Request Broker Architecture

CSMA/CA Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD Carrier Sense Multiple Access/Collision Detect

CTCP Compound TCP

DAP Directory Access Protocol

DCB Data Center Bridging

DCF Distributed Coordination Function

DFS Dynamic Frequency Selection

DHCP Dynamic Host Configuration Protocol

DHCPv6 Dynamic Host Configuration Protocol for IPv6

DiffServ Differentiated Services

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

DS Differentiated Services

DSCP Differential Services Code Point

DSL Digital Subscriber Line

DSSS Direct-Sequence Spread Spectrum

DTLS Datagram Transport Layer Security

EDGE Enhanced Data rates for GSM Evolution

EDNS Extension Mechanisms for DNS

EIRP Equivalent Isotropically Radiated Power

EPON Ethernet Passive Optical Network

ESP Encapsulating Security Payload

FC Fibre Channel

FCIP Fibre Channel over IP

FCoE Fibre Channel over Ethernet

FCP Fibre Channel Protocol

FHSS Frequency-Hopping Spread Spectrum

FTP File Transfer Protocol

GCM Galois/Counter Mode

GDI Graphics Device Interface

GEO Geostationary Orbit

GFP Generic Framing Procedure

GPRS General Packet Radio Service

GPS Global Positioning System

GPU Graphics Processing Unit

GRE General Routing Encapsulation

GSM Global System for Mobile Communications

HDX High Definition Experience

HMAC Keyed-Hashing for Message Authentication

HSPA High Speed Packet Access

HTML Hypertext Markup Language

HTML5 Hypertext Markup Language version 5

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

ICA Independent Computing Architecture

IEEE Institute of Electronics and Electrical Engineers

iFCP Internet Fibre Channel Protocol

IKE Internet Key Exchange

IM Instant Messaging

IMAP Internet Message Access Protocol

IMAP4 Internet Message Access Protocol - Version 4

IMS IP Multimedia Subsystem

IP Internet Protocol

IPsec Internet Protocol Security

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IPX Internetwork Packet Exchange

IRIG Inter-Range Instrumentation Group

iSCSI Internet Small Computer System Interface

IV Initialvektor

KDC Key Distribution Center

L2TP Layer Two Tunneling Protocol

L2TPv3 Layer Two Tunneling Protocol - Version 3

LAC L2TP Access Concentrator

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

LEO Low Earth Orbit

LFN Long Fat Networks

LNS L2TP Network Server

LTE 3GPP Long Term Evolution

MAC Message Authentication Code

MACsec IEEE MAC Security

MAN Metropolitan Area Network

MAPI Messaging Application Programming Interface

MBH Mobile Backhaul

MEF Metro Ethernet Forum

MIMO Multiple-input, Multiple-output

MP3 MPEG-1 or MPEG-2 Audio Layer III

MPLS Multi Protocol Label Switching

MS-DFS Microsoft Distributed File System

MSRPC Microsoft Remote Procedure Call

MTU Maximum Transfer Unit

NAS Network Attached Storage

NAT Network Address Translation

NetBIOS Network Basic Input/Output System

NFS Network File System

NRPC Notes Remote Procedure Call

NTP Network Time Protocol

NX NX Technology

OFDM Orthogonal Frequency-Division Multiplexing

PCF Point Coordination Function

PCoIP PC over IP

PCP Priority Code Point

PDF Portable Document Format

PDH Plesiochronous Digital Hierarchy

PLC Packet Loss Concealment

PMTU Path MTU Discovery

PN Packet Number

POP3 Post Office Protocol - Version 3

POS Packet over SONET/SDH

PPP Point-to-Point Protocol

PPR Proportional Rate Reduction for TCP

PRNG Pseudo Random Number Generator

PSK Pre-shared key

PTP Precision Time Protocol

QoS Quality of Service

RDP Remote Desktop Services

REST Representational State Transfer

RFB Remote Frame Buffer

RFC Request for Comments

RFID Radio-Frequency Identification

ROHC Robust Header Compression

RTCP Real Time Control Protocol

RTP Real-time Transport Protocol

RTSP Real Time Streaming Protocol

RTT Round Trip Time

SA Secure Association

SACK Selective ACK

SAN Storage Area Network

SAS Serial Attached SCSI

SASL Simple Authentication and Security Layer

SCI Secure Channel Identifier

SCSI Small Computer System Interface

SDH Synchronous Digital Hierarchy

SHA Secure Hash Algorithm

SIP Session Initiation Protocol

SLA Service Level Agreement

SMB Server Message Block

SMTP Simple Mail Transfer Protocol

SNTP Simple Network Time Protocol

SOCKS5 SOCKS Protocol Version 5

SPDY Speedy

SQL Structured Query Language

SRTP Secure RTCP

SRTP Secure RTP

SSH Secure Shell

SSL Secure Sockets Layer

SSL-VPN Secure Sockets Layer Virtual Private Network

SyncE Synchronous Ethernet

TAI International Atomic Time

TCP Transmission Control Protocol

TDM Time Division Multiplexing

TDMoIP Time-Division Multiplexing over IP

TLS Transport Layer Security

TOS Type of Service

UDP User Datagram Protocol

UMTS Universal Mobile Telecommunications System

UTC Coordinated Universal Time

VLAN Virtual Local Area Network

VNC Virtual Network Computing

VoIP Voice over IP

VoLTE Voice over LTE

VPN Virtuellt privat nätverk

WAN Wide Area Network

WebDAV Web Distributed Authoring and Versioning

WLAN Wireless Local Area Network

WMM Wi-Fi Multimedia Extentions

WMS Windows Media Services

WMV Windows Media Video

X11 X Window System

XML Extensible Markup Language

XMPP Extensible Messaging and Presence Protocol

Sakregister

Referenser

[AES] Advanced encryption standard (aes). NIST, November 2001. FIPS-197. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[CBC] NIST. Recommendation for Block Cipher Modes of Operation. SP 800-38A, December 2001. http://csrc.nist.gov/publications/nistpubs/800-38a/SP-800-38a.pdf.

[CISCOFCIP] Cisco. Cisco mds 9000 family fcip wan deployment guidelines. http://www.cisco.com/en/US/netsol/ns516/networking_solutions_white_paper09186a00801c6074.shtml.

[etsi-en-300-328] ETSI; European Telecommunications Standards Institute. Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive. http://www.etsi.org. ETSI EN 300 328, v1.8.1, 2012-04.

[etsi-en-301-893] ETSI; European Telecommunications Standards Institute. Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive. http://www.etsi.org. ETSI EN 301 893, v1.7.0, 2012-01.

[G7041] ITU-T. Generic Framing Procedure (GFP). http://www.itu.int/rec/T-REC-G.7041/en.

[G729] ITU-T. Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP). G.729, Januari 2007. http://www.itu.int/rec/T-REC-G.729-200701-I/en.

[GCM] NIST. Recommendation for Block Cipher Modes of Operation: Galois/C. SP 800-38D, November 2007. http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

[GSMFR] ETSI; European Telecommunications Standards Institute. Digital cellular telecommunications system (phase 2+) (gsm); full rate speech; transcoding

(gsm 06.10 version 8.1.1 release 1999), 2000.
http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=11074.

[IEEE1588] NIST. Ieee 1588 standard for a precision clock synchronization protocol for networked measurement and control systems.
http://www.nist.gov/el/isd/ieee/ieee1588.cfm.

[IEEE8021ad] Ieee standard for local and metropolitan area networks—virtual bridged local area networks—amendment 4: Provider bridges. IEEE, 2005.
http://standards.ieee.org/findstds/standard/802.1ad-2005.html.

[IEEE8021AE] IEEE. Ieee standard for local and metropolitan area networks: Media access control (mac) security. IEEE, 2006.
http://standards.ieee.org/findstds/standard/802.1AE-2006.html.

[IEEE8021X] IEEE. Ieee standard for local and metropolitan area networks–port-based network access control. IEEE, 2010.
http://standards.ieee.org/findstds/standard/802.1X-2010.html.

[IEEE8023AH] IEEE. Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks. 802.3ah-2004.
http://www.ieee802.org/21/doctree/2006_Meeting_Docs/2006-11_meeting_docs/802.3ah-2004.pdf.

[Jingle] Jingle.
http://xmpp.org/about-xmpp/technology-overview/jingle/.

[JPEG] Information technology – digital compression and coding of continuous-tone still images: Requirements and guidelines. ISO/IEC 10918-1:1994, 1994.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902.

[LTE] 3GPP. 3GPP Long Term Evolution, 2008.
http://www.3gpp.org/ftp/Specs/html-info/36-series.htm.

[MEF3] Metro Ethernet Forum. Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks. MEF3, April 2004.
http://metroethernetforum.org/PDF_Documents/technical-specifications/MEF3.pdf.

[MP3] ISO. Information technology – generic coding of moving pictures and associated audio information – part 3: Audio. ISO/IEC 13818-3:1998, 1998.
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=26797.

[PPR] Y. Cheng N. Dukkipati, M. Mathis och M. Ghobadi. Proportional Rate Reduction for TCP, November 2011.
http://research.google.com/pubs/pub37486.html.

[ptsfs-2012-3] PTS; Post- och telestyrelsen. Post- och telestyrelsens föreskrifter om undantag från tillståndsplikten för vissa radiosändare. http://www.pts.se. PTSFS, 2012:3, 2012-09-11.

[rdptest] B. Tritsch och S. Bass. Microsoft RDP and RemoteFX, ICA/HDX, EOP and PCoIP: VDI Remoting Protocols Turned Inside Out. Presentation Microsoft Tech Ed 2011, May 2011.
http://channel9.msdn.com/Events/TechEd/NorthAmerica/2011/VIR401.

[RFC1034] P.V. Mockapetris. Domain names - concepts and facilities. RFC 1034 (Standard), november 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.
http://www.ietf.org/rfc/rfc1034.txt.

[RFC1035] P.V. Mockapetris. Domain names - implementation and specification. RFC 1035 (Standard), november 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966.
http://www.ietf.org/rfc/rfc1035.txt.

[RFC1072] V. Jacobson och R. Braden. TCP Extensions for Long-Delay Paths. RFC 1072 (Proposed Standard), October 1988. Obsoleted by RFC 6247.
http://www.ietf.org/rfc/rfc1072.txt.

[RFC1144] V. Jacobson. Compressing TCP/IP Headers for Low-Speed Serial Links. RFC 1144 (Proposed Standard), februari 1990.
http://www.ietf.org/rfc/rfc1144.txt.

[RFC1321] R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321 (Informational), april 1992. Updated by RFC 6151.
http://www.ietf.org/rfc/rfc1321.txt.

[RFC1323] V. Jacobson, R. Braden och D. Borman. TCP Extensions for High Performance. RFC 1323, May 1992.
http://www.ietf.org/rfc/rfc1323.txt.

[RFC1928] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas och L. Jones. SOCKS Protocol Version 5. RFC 1928 (Proposed Standard), mars 1996.
http://www.ietf.org/rfc/rfc1928.txt.

[RFC1939] J. Myers och M. Rose. Post Office Protocol - Version 3. RFC 1939 (Standard), maj 1996. Updated by RFCs 1957, 2449, 6186.
http://www.ietf.org/rfc/rfc1939.txt.

[RFC1951] P. Deutsch. DEFLATE Compressed Data Format Specification version 1.3. RFC 1951 (Informational), May 1996.
http://tools.ietf.org/html/rfc1951.

[RFC2018] M. Mathis, J. Mahdavi, S. Floyd och A. Romanow. TCP Selective Acknowledgment Options. RFC 2018 (Proposed Standard), oktober 1996.
http://www.ietf.org/rfc/rfc2018.txt.

[RFC2104] H. Krawczyk, M. Bellare och R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Informational), februari 1997. Updated by RFC 6151.
http://www.ietf.org/rfc/rfc2104.txt.

[RFC2131] R. Droms. Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard), mars 1997. Updated by RFCs 3396, 4361, 5494.
http://www.ietf.org/rfc/rfc2131.txt.

[RFC2246] T. Dierks och C. Allen. The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard), January 1999.
http://www.ietf.org/rfc/rfc2246.txt.

[RFC2326] H. Schulzrinne, A. Rao och R. Lanphier. Real Time Streaming Protocol (RTSP). RFC 2326 (standard), April 1998.
http://www.ietf.org/rfc/rfc2326.txt.

[RFC2474] K. Nichols, S. Blake, F. Baker och D. Black. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2774 (Proposed Standard), December 1998. Updated by RFC 3168, RFC 3260.
http://www.ietf.org/rfc/rfc2474.txt.

[RFC2615] A. Malis och W. Simpson. PPP over SONET/SDH. RFC 2615 (Proposed Standard), juni 1999.
http://www.ietf.org/rfc/rfc2615.txt.

[RFC2671] P. Vixie. Extension Mechanisms for DNS (EDNS0). RFC 2671 (Proposed Standard), augusti 1999.
http://www.ietf.org/rfc/rfc2671.txt.

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer och P. Traina. Generic Routing Encapsulation (GRE). RFC 2784 (Proposed Standard), mars 2000. Updated by RFC 2890.
http://www.ietf.org/rfc/rfc2784.txt.

[RFC2818] E. Rescorla. Http over tls. RFC 2818 (Informational), May 2000.
http://www.ietf.org/rfc/rfc2818.txt.

[RFC2821] J. Klensin. Simple Mail Transfer Protocol. RFC 2821 (Proposed Standard), april 2001. Obsoleted by RFC 5321, updated by RFC 5336.
http://www.ietf.org/rfc/rfc2821.txt.

[RFC2890] G. Dommety. Key and Sequence Number Extensions to GRE. RFC 2890 (Proposed Standard), september 2000.
http://www.ietf.org/rfc/rfc2890.txt.

[RFC3031] E. Rosen, A. Viswanathan och R. Callon. Multiprotocol Label Switching Architecture. RFC 3031 (Proposed Standard), januari 2001. Updated by RFC 6178.
http://www.ietf.org/rfc/rfc3031.txt.

[RFC3095] C. Bormann, C. Burmeister, M. Degermark, H. Fukushima, H. Hannu, L-E. Jonsson, R. Hakenberg, T. Koren, K. Le, Z. Liu, A. Martensson, A. Miyazaki, K. Svanbro, T. Wiebke, T. Yoshimura och H. Zheng. RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed. RFC 3095 (PROPOSED STANDARD), July 2001. Updated by RFCs 3241, 3843, 4019, 4362, 4815.
http://tools.ietf.org/html/rfc3095.

[RFC3261] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley och E. Schooler. SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard), juni 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630, 5922, 5954, 6026, 6141.
http://www.ietf.org/rfc/rfc3261.txt.

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins och M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315 (Proposed Standard), juli 2003. Updated by RFCs 4361, 5494, 6221, 6422.
http://www.ietf.org/rfc/rfc3315.txt.

[RFC3501] M. Crispin. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. RFC 3501 (Proposed Standard), mars 2003. Updated by RFCs 4466, 4469, 4551, 5032, 5182, 5738, 6186.
http://www.ietf.org/rfc/rfc3501.txt.

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick och V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. RFC 3550 (Standard), juli 2003. Updated by RFCs 5506, 5761, 6051, 6222.
http://www.ietf.org/rfc/rfc3550.txt.

[RFC3711] M. Baugher, D. McGrew, M. Naslund, E. Carrara och K. Norrman. The Secure Real-time Transport Protocol (SRTP). RFC 3711 (Proposed Standard), mars 2004. Updated by RFC 5506.
http://www.ietf.org/rfc/rfc3711.txt.

[RFC3720] J. Satran, K. Meth, C. Sapuntzakis, M. Chadalapaka och E. Zeidner. Internet Small Computer Systems Interface (iSCSI). RFC 3720 (Proposed Standard), April 2004. Updated by 3980, 4850, 5048.
http://www.ietf.org/rfc/rfc3720.txt.

[RFC3782] S. Floyd, T. Henderson och A. Gurtov. The NewReno Modification to TCP's Fast Recovery Algorithm. RFC 3782 (Proposed Standard), April 2004. Obsoletes RFC 2582.
http://www.ietf.org/rfc/rfc3782.txt.

[RFC3821] M. Rajagopal, E. Rodriguez och R. Weber. Fibre Channel Over TCP/IP (FCIP). RFC 3821 (Proposed Standard), July 2004.
http://www.ietf.org/rfc/rfc3821.txt.

[RFC3931] J. Lau, M. Townsley och I. Goyret. Layer Two Tunneling Protocol - Version 3 (L2TPv3). RFC 3931 (Proposed Standard), mars 2005. Updated by RFC 5641.
http://www.ietf.org/rfc/rfc3931.txt.

[RFC3948] A. Huttunen, B. Swander, V. Volpe, L. DiBurro och M. Stenberg. UDP Encapsulation of IPsec ESP Packets. RFC 3948 (Proposed Standard), januari 2005.
http://www.ietf.org/rfc/rfc3948.txt.

[RFC4033] R. Arends, R. Austein, M. Larson, D. Massey och S. Rose. DNS Security Introduction and Requirements. RFC 4033 (Proposed Standard), mars 2005. Updated by RFC 6014.
http://www.ietf.org/rfc/rfc4033.txt.

[RFC4120] C. Neuman, T. Yu, S. Hartman och K. Raeburn. The Kerberos Network Authentication Service (V5). RFC 4120 (Proposed Standard), juli 2005. Updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113.
http://www.ietf.org/rfc/rfc4120.txt.

[RFC4172] C. Monia, R. Mullendore, F. Travostino, W. Jeong och M. Edwards. iFCP - A Protocol for Internet Fibre Channel Storage Networking. RFC 4172 (Proposed Standard), September 2005. Updated by RFC 6172.
http://www.ietf.org/rfc/rfc4172.txt.

[RFC4251] T. Ylonen och C. Lonvick. The Secure Shell (SSH) Protocol Architecture. RFC 4251 (Proposed Standard), januari 2006.
http://www.ietf.org/rfc/rfc4251.txt.

[RFC4303] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303 (Proposed Standard), december 2005.
http://www.ietf.org/rfc/rfc4303.txt.

[RFC4305] D. Eastlake 3rd. Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH). RFC 4305 (Proposed Standard), december 2005. Obsoleted by RFC 4835.
http://www.ietf.org/rfc/rfc4305.txt.

[RFC4306] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), december 2005. Obsoleted by RFC 5996, updated by RFC 5282.
http://www.ietf.org/rfc/rfc4306.txt.

[RFC4346] T. Dierks och E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346 (Proposed Standard), April 2006.
http://www.ietf.org/rfc/rfc4346.txt.

[RFC4347] E. Rescorla och N. Modadugu. Datagram Transport Layer Security. RFC 4347 (Proposed Standard), april 2006. Updated by RFC 5746.
http://www.ietf.org/rfc/rfc4347.txt.

[RFC4511] J. Sermersheim. Lightweight Directory Access Protocol (LDAP): The Protocol. RFC 4511 (Proposed Standard), juni 2006.
http://www.ietf.org/rfc/rfc4511.txt.

[RFC5246] T. Dierks och E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), augusti 2008. Updated by RFCs 5746, 5878, 6176.
http://www.ietf.org/rfc/rfc5246.txt.

[RFC5905] D. Mills, J. Martin, J. Burbank och W. Kasch. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5905 (Proposed Standard), juni 2010.
http://www.ietf.org/rfc/rfc5905.txt.

[RFC5996] C. Kaufman, P. Hoffman, Y. Nir och P. Eronen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 5996 (Proposed Standard), september 2010. Updated by RFC 5998.
http://www.ietf.org/rfc/rfc5996.txt.

[RFC6120] P. Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. RFC 6120 (Proposed Standard), mars 2011.
http://www.ietf.org/rfc/rfc6120.txt.

[RFC6716] JM. Valin, K. Vos och T. Terriberry. Definition of the Opus Audio Codec. RFC 6716 (Proposed Standard), september 2012.
http://www.ietf.org/rfc/rfc6716.txt.

[RFC793] J. Postel. TRANSMISSION CONTROL PROTOCOL. RFC 793 Standard, September 1981.
http://www.ietf.org/rfc/rfc793.txt.

[RFC951] W.J. Croft och J. Gilmore. Bootstrap Protocol. RFC 951 (Draft Standard), september 1985. Updated by RFCs 1395, 1497, 1532, 1542, 5494.
http://www.ietf.org/rfc/rfc951.txt.

[RSYNC] A. Tridgell och P. Mackerras. Rsync, June 1996.
http://rsync.samba.org/.

[SHS] NIST. Secure Hash Standard. FIPS 180-3, October 2008.
http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf.

[SPDY] Google. Spdy: An experimental protocol for a faster web.
http://dev.chromium.org/spdy/spdy-whitepaper.

[SYNCE] ITU-T. G.8262 : Timing characteristics of a synchronous Ethernet equipment slave clock, 2010.
http://www.itu.int/rec/T-REC-G.8262-201007-I/en.

[TCP-FIT] J. Wang, J. Wen, J. Zhang och Y. Han. Tcp-fit - an improved tcp congestion control algorithm and its performance.
http://media.cs.tsinghua.edu.cn/~multimedia/tcp-fit/.

[VoIPSec] Miroslav Voznak. Speech bandwith requirements in IPsec and TLS environment, 2009.
http://www.wseas.us/e-library/conferences/2009/rodos/COMPUTERS/COMPUTERS31.pdf.

[Westwood+] S. Mascolo. Tcp westwood+ congestion control.
http://c3lab.poliba.it/index.php/Westwood.

[WIFIFADING] D. Cheung och C. Prettie. A path loss comparison between the 5 ghz unii band (802.11a) and the 2.4 ghz ism band (802.11b). Intel Labs, January 2002.