



Rapport Network Traffic Audit

Banverket ICT

Genomförd av MAX16 Limited

MAX16 slutsatser och rekommendationer görs i god tro och baserade på de uppgifter MAX16 har vid tidpunkten för offentliggörandet. Vi medger att detta dokument inte avser att innehålla all information som kan krävas och att mottagarna är ansvariga för att fatta egna beslut.



SAMMANFATTNING

MAX16 Limited utsågs av Banverket ICT att utföra en mätning och analys på ICTs del av nättrafiken inom Banverkets IT plattform. Mätningen av nättrafiken har i huvudsak gjorts med hjälp av Banverket lånad analysutrustning, en Procera PLR7720, och av Max16 inhyrda Nätverkstappar. Max16 har driftsatt, installerat och konfigurerat nätutrustning samt övervakat och analyserat all avtappad nättrafik. Avtappning och analys av nättrafik har skett vid en punkt, närmare bestämt punkten innanför den brandvägg som används för att ansluta ut mot Internet och andra externa resurser.

Kapaciteten är ut mot internet är väl anpassad och fungerar effektivt - dvs. bra prestanda, bra kapacitet och god upplevd kvalitet (QoE), **endast 1 %** av användarna har någon typ av kvalitetsstörning per dag. Ingen malware eller annan skadlig kod/aktivitet har observeras, vilket troligen medför att brandväggar och antivirusprogram i stort sett gör sitt jobb. Generellt så är det ingen nämnvärd skillnad på fördelningen av nättrafiken mellan enheten ICT och resten av Banverket genererade/konsumerade nättrafik. I de fall det förekommer så finns det beskrivet i resultatsammanställningen.

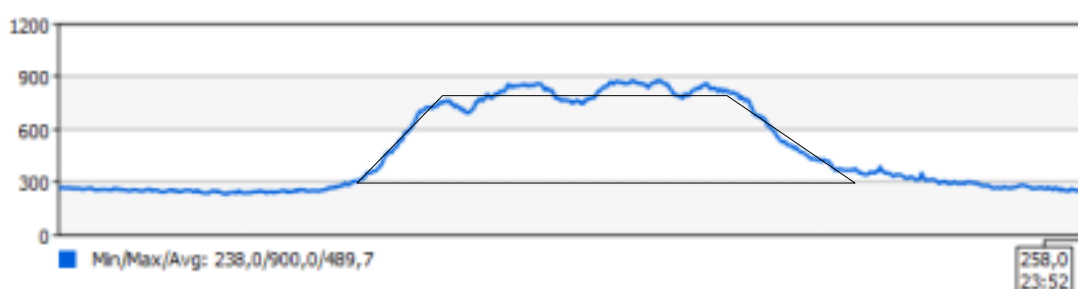
Storleksmässigt så motsvarar Banverket ICT trafik cirka **20 %** av Banverkets totala trafik.

I mitten av Mars så uppmärksammades ICTs ledningsgrupp på några delresultat, som i huvudsak indikerade på **högt "Icke-jobb relaterat"** nyttjande av Internet. Beslut togs att ett informations- och åtgärdsprogram skulle startas och att Max16 projektet skulle fortsätta med mätningen samt analysera och utvärdera utfallet av dessa åtgärder. Det har hittills **inte konstateras någon förändring av trafikmönster** eller förändring av användarnas utnyttjande av nätet.

Sammanfattningsvis vill vi uppmärksamma ICTs ledning på några karakteristiska resultat gällande fördelning av Banverkets (totala) nättrafik.

- Cirka **58 %** av trafiken är inkommande Backuptrafik (RPC2), **19 %** Webtrafik och **16 %** Streaming media trafik
- Cirka **65 %** till **75 %** av Webtrafiken (http) bedöms vara av "Social" eller icke jobbrelaterad karaktär.
- Cirka **90 %** av inkommande Streaming media bedöms vara av "Social" eller icke jobbrelaterad karaktär.
- Cirka **3 %** av .com trafik för februari bedöms vara av ren "Sex/Porr".
- Cirka **88 %** av Banverkets Totala Internettrafik passerar en ISP (Lidero Network).

Man uppskatta antalet anslutna användare (hela Banverket) som använder IT-infrastrukturen över mätpunkten vid en given tidpunkt. Detta ger en bild som är korrelerat med hur många arbetstimmar som produceras över just den delen av IT infrastrukturen



Figur 1

- Cirka **4500** Mantimmar per dag produceras över mätpunkten*(**har ökat efter 1 april och Trafikverkets bildande.**)
- Cirka **225-250** mantimmar motsvaras av dippar
- Om merparten av http och streaming media trafiken som bedöms som "Social" och icke direkt jobbrelaterad skulle översättas i icke direkt jobbrelaterade mantimmar så motsvarar detta i medeltal ca **3375** Mantimmar per dag vilket borde motsvara **många** miljoner kronor.
- **10 %** ökad produktivitet kan uppnås med **6 + 6 + 6** minuters minskning av tiden av förmiddag, lunch och eftermiddagspauser.

Den mest dominerade tjänsten är inkommande RPC2 trafik (periodisk Backup). Den påbörjas oftast kl 22.00 och pågår hela natten fram till 05.00. Att genomföra större underhållsarbeten under nattetid (vilket oftast är normalt) som medför avbrott är direkt olämpligt. Det är även en betydande del RPC2 (Backuptrafik) under helger och vid månadsslut. Det perioder på dygnet som har minst nätaktivitet är **05.00-07.00** samt **20.00-22.00**. De är därför också lämpliga kandidater för att genomföra olika typer av trafikstörande underhållsarbeten (dvs. arbetsfönster), typ konfigurations ändringar samt omstarter av nätutrustning.

Nätverksaktivitet följer i allmänhet en förväntad nivå. Varje arbetsdag under normal arbetstid är användningen av IT infrastrukturen karakteriserat av en ökad aktivitet från 06.00 och avtagande från 15.00 . Aktiviteten följer ett konsekvent och regelbundet



mönster där den faller kraftigt tre gånger om dagen. Varje period varar på ca 1 timme (09.00-09.45, 11.10-12.30, 13.45-14.45).

Socialt bruk av nätverksresurser under arbetstid är inte ovanligt. I Banverkets fall är den andelen betydligt högre än förväntade nivåer. Max 16 rekommenderar att Banverket ICT tar fram strategier och åtgärder för hur man kan komma ner till en önskad nivå. En minskning av dessa höga nivåer borde ge ett utrymme för Banverkets medarbetare att öka sin produktivitet.

Som ett resultat av dessa resultat och omfattningen av ny kunskap, gör MAX16 följande rekommendationer

1. Banverket ICT bör Internt tydliggöra sin egen IT policy, om och hur den förändras i samband med övergången till Trafikverkets organisation från 1 april, samt avsätta nödvändiga resurser och ta fram en strategi för hur man effektivt uppnår den.
2. Banverket ICT bör utforma och driftsätta en **kommersiell tjänst** där man erbjuder en i realtid flexibel/kundanpassad (olika organisationer och företag) policy och volyms anpassning av **Internet användning**, som tar hänsyn till företagets mål och medarbetarnas behov, med säkerhetsmekanismer på olika nivåer som förhindrar missbruk och medverkar till en förbättrad uppföljning och ett ökat utrymme för produktivitetssökning.
3. På grundval av resultaten från detta projekt fullfölja ambitionen och sätta upp ett **permanent system** baserat på Max16 konceptet, anpassat till Banverkets behov, som kommer att övervaka, avkoda, mäta, analysera och vid behov **justera** nätverkstrafiken i realtid så att ledningen och driftorganisation kan följa upp användning av nätresurser samt uppföljning av investeringar och konsolidering av IT infrastruktur. Detta kommer för första gången att skapa en i realtid enhetlig och opolitisk bild hur IT-infrastrukturen används. Genom en konsekvent och regelbunden information och rapporterings process kommer detta föreslagna system tillhandahålla alla mekanismer och möjligheter till att skapa utrymme för **lägre investeringar och operativa kostnader**.

Framför allt så skulle ett sådant system vara en del i effektiv mekanism för att få bort icke-jobbrelaterad användning av internet och på sikt spara miljontalskronor.





1)

Innehållsförteckning

SAMMANFATTNING	2
1 INLEDNING OCH SYFTE	7
2 MAX16 METODIK OCH INKOPPLING MOT NÄTET	8
3 ANTAGANDEN OCH BEGRÄNSNINGAR.....	11
4 RESULTAT.....	13
4.1 BANVERKET TOTALT	14
4.2 INTERNET PEERING TOTALT	16
4.3 BANVERKET ICT	18
4.4 BANVERKET (10 NÄTET).....	20
4.5 ANALYS AV ICT´S WEBTRAFIK	23
4.6 ANALYS AV HELA BANVERKETS WEBTRAFIK	27
4.7 ANALYS STREAMING MEDIA ICT	30
4.8 ANALYS NÄTVERKSTRAFIK ICT	34
4.9 MANTIMAR FÖR HELA BANVERKET	35
4.10 TJÄNSTER OCH PROTOKOLL	39
4.11 QUALITY OF EXPERIENCE.....	43
4.12 ANOMALIER	44
4.12.1 <i>MobiSIR</i>	44
4.12.2 <i>Sex och porr</i>	44
4.13 SPECIALSTUDIE AV FACEBOOK ANVÄNDNING	45
4.14 RESULTAT OCH KONSEKVENSER	47
5 REKOMMENDATIONER	49
6 BILAGOR	51



1 INLEDNING OCH SYFTE

Uppdraget påbörjades den 1 februari med en veckas förstudie samt en detaljerad informations- och kravinsamling.

Den 8 februari utsågs "MAX16 Limited" av ICTs ledningsgrupp att fullfölja och utföra en granskning av den nätverkstrafik som omfattar ICT nättrafik inom Banverkets nät med hjälp av ett Banverksanskaffat Deep Packet Inspection (DPI) och Deep Flow Inspection (DFI) verktyg (Procera PLR7720). För att tappa av nättrafik så användes en av Max16 hyrt nätverkstapp (SMART Tap från Network Critical).

Uppdraget skulle även omfatta, en utveckling av policyregler för möjlig "Enforcement" enligt direktiv från ICTs ledningsgrupp, kundanpassat gränssnitt för "mantimmar" samt en valfri seminarieutbildning.

För att effektivt och med säkerhet kunna avgöra vilka användare, organisationer, eller andra grupper som genererar/konsumerar nättrafiken så bedömdes det att en överföring av information från Banverkets Active Directory **AD** plattform till Procera 7720 var nödvändig. Detta skulle lösas av ett färdigt pluginscript.

För framtagning av kundgränssnitt och ev. anpassning/utveckling av det **existerade AD pluginet** så fanns det en option att genomföra detta via ett mjukvaruföretag (Symbio). Upphandling och avrop av nödvändig mjukvaruutveckling skulle vid behov avropas separat av Banverket ICT.

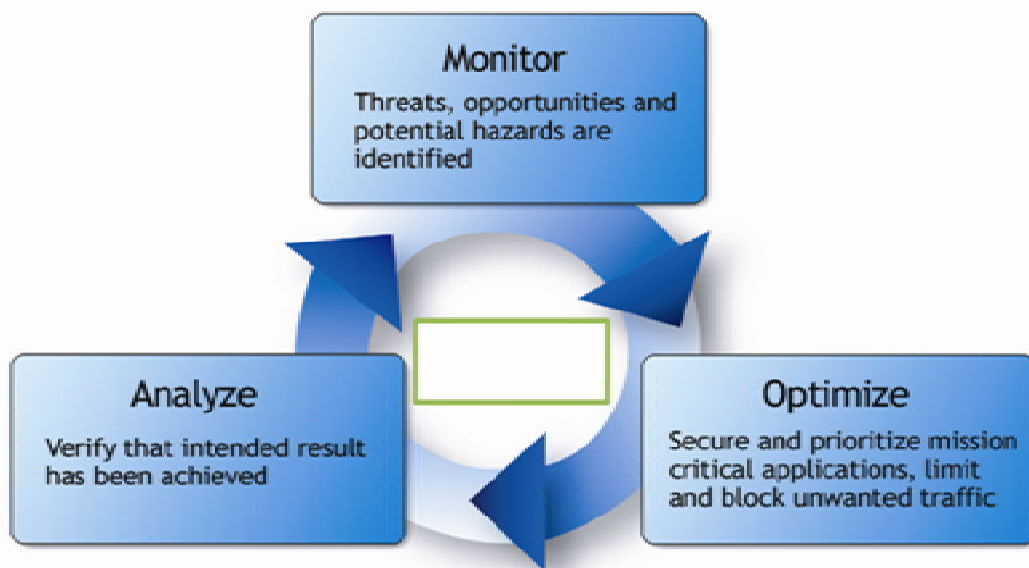
Syftet med projektet var att mäta och analysera ICTs del av nätverkstrafik i Banverks ICT nät med syfte att:

- (i) Beskriva hur olika användare, grupper, program och servrar använder nätet,
- (ii) Avkoda och kategorisera nätverkstrafiken samt avgöra vilka tjänster och protokoll mekanismer som verkligen används i nätverket,
- (iii) Kartlägga användarens aktivitet i form av mantimmar och nyttjandemönster över tid.
- (iv) Föreslå policy och enforcement regler.
- (v) Genomföra policy och enforcement efter godkännande och prioritering av ICTs ledningsgrupp.
- (vi) Identifiera potentiella flaskhalsar eller möjligheter att förbättra prestanda i nätet.
- (vii) Markera alla fynd av skadlig kod, virus eller anomalier och vid behov isolera eventuella säkerhetsrisker.
- (viii) Identifiera ev. missbruk eller otillåten användning (enligt ICTs IT policy) av

2 MAX16 METODIK OCH INKOPPLING MOT NÄTET

MAX16 använder följande process för granskning och analys av nätverkstrafik. Granskningen och övervakningen av nättrafiken är utformad för att ge Banverket ICT en nulägesbeskrivning av aktiviteten i nätet samt en insamling av statistik, detta under en given tidsperiod vid en eller flera förutbestämda punkter i ICTs nätplattform. Därefter används den insamlade informationen tillsammans med en genomförd revisionen av potentiella hot och möjligheter för att fastställa och utforma lämpliga åtgärder och optimeringar. För att undvika att optimeringarna blir en statisk engångsföreteelse så mäter man och analyserar nätverkstrafiken efter genomförda optimeringar och följer upp effektiviteten för genomförda förändringar samt de naturliga förändringar som inte har något med de genomförda förändringarna.

1. Aktivt övervaka och analysera nättrafiken och blida ett beslutsunderlag för förändringar och optimeringar i nätet (*Baseline*).
2. Utforma optimeringar och hantera dem grundade på korrekt information (Beslutsunderlag) och en tydlig uppsättning av mätbara mål.
3. Kontinuerligt utvärdera och kontrollera att Optimeringar och förändringar uppnår de förväntat effekt och resultat.



Figur 2



Konceptet som Max16 använder är en integrerad **kostnadseffektiv** kombination av intelligenta nätverkstappar som tappar av nättrafik **utan** att påverka varken nätet eller trafiken genom nätet samt en nättrafikanalysutrustning som avkodar och analyserar hela den avtappade nätverksströmmen.

Nätverkstappen (från Network Critical) tillhandahåller en **exakt** duplicering av trafiken, både trafikalt och tidsmässigt. Om och när man vill så kan man aktivera (remote) nätverkstappen så att trafiken leds igenom analysutrustningen (Procera PLR7720). Detta sker normalt då man vill på något sätt påverka trafiken i nätet t.ex. vid filtrering och prioritering. Nätverkstappen kan samtidigt anslutas till **flera olika mätpunkter** i nätet (olika nät) och aggregera/filtrera upp nättrafiken till utrustningen som avkodar och analyserar trafiken, på detta vis användes analysutrustningen mer optimalt. Det möjliggör en central placering av analysutrustning för nättrafik med en samtidig avtappning av trafik på flera olika platser i nätet .

Figur 3



Inkopplingen mot Banverkets nät för detta projekt gjordes via en Nätverkstapp som kopplades in på förbindelsen som ansluter Banverkets nät med Internet. Inkopplingen gjordes på insidan av brandväggen för att få med all nätverkstrafik både den som bara går/kommer från Banverkets DMZ och den som kommer in och ut från Internet.

Figur 4



3 **ANTAGANDEN OCH BEGRÄNSNINGAR**

Detta uppdrag genomfördes under perioden februari och mars. Insamlad information och data som anses relevanta för att nå viktiga slutsatser, men också för att spegla kvaliteten på datainsamlingen och på utredningens resultat, bör bedömas utifrån nedan beskrivna antaganden och begränsningar.

Vi vill rikta Banverkets uppmärksamhet på följande antaganden:

- a) Att den information som tillhandahållits av Banverket angående vilka IP adresser som tillhör servrar och annan fast kommunikations utrustning är korrekt och att den inte ändrat sig under projektiden.
- b) Att IP planen, dvs. den plan som används för dynamisk tilldelning av IP adresser till användare (via DHCP) och statisk utdelning av IP adresser för de olika ICT kontoren och näten stämmer, är korrekt samt att den inte har ändrat sig under projektiden.
- c) Att av Banverket tillhandahållen analysutrustning (PLR7720) är tillgänglig, är fullt fungerande och att inte innehåller odokumenterade funktioner och buggar för den aktuella mjukvara som användes under projektiden.
- d) Att support finns för all tillhandahållen utrustning och mjukvara.
- e) Att den av Procera supporten tillhandahållna mjukvaran har korrigerat de problem som fanns initialt map funktionalitet och stabilitet.
- f) Det antas att det dominerande antalet användare använder endas 1 IP adress per dag.



Vi vill rikta Banverkets uppmärksamhet på följande begränsningar:

- i) Begränsningar ang. förmåga att effektivt kunna avgöra om och vem som genererar/konsumerar den observerade nätverkstrafiken. Eftersom inget AD plugin kunde användas så gjordes det istället en **manuell** uppdelning av alla nät i olika nätobjekt med **geografisk** och organisatorisk tillhörighet. Denna statiska uppdelning skiljer inte om användare sitter från olika organisationer sitter blandade på samma nät, men bedöms som tillräckligt representativ för att avgöra huruvida trafiken kommer från ICT eller från andra delar av Banverket.
- ii) Begränsningar angående osäkerhet kring stabilitet och bakåtkompatibilitet för analysutrustningens (PLR 7720) API och begränsningar angående stöd och konfiguration av "Volume Based Shaping" funktionen för analysutrustningen medförde att en uppdatering av mjukvara hos PLR7720 efter rekommendation från Proceras support
- iii) Begränsningar angående tillgång till Banverkets egen analysutrustning. Banverkets egna PLR 7720 levererades av Procera först i mitten på februari. Har medfört att mätning och analys av nätverkstrafik har i huvudsak genomförts med lånad utrustning, Kallad Demo PLR 7720. Det har medfört att konfiguration och insamlad statistik har tvingats flyttas över till Banverkets egen analysutrustning först efter att Banverkets egna nya analysutrustning har installerats. Detta har inneburit ett avbrott i lagrad statistik 26/3-16/4.



4 RESULTAT

Nättrafiken har delats upp i huvudsakligen i tre bitar.

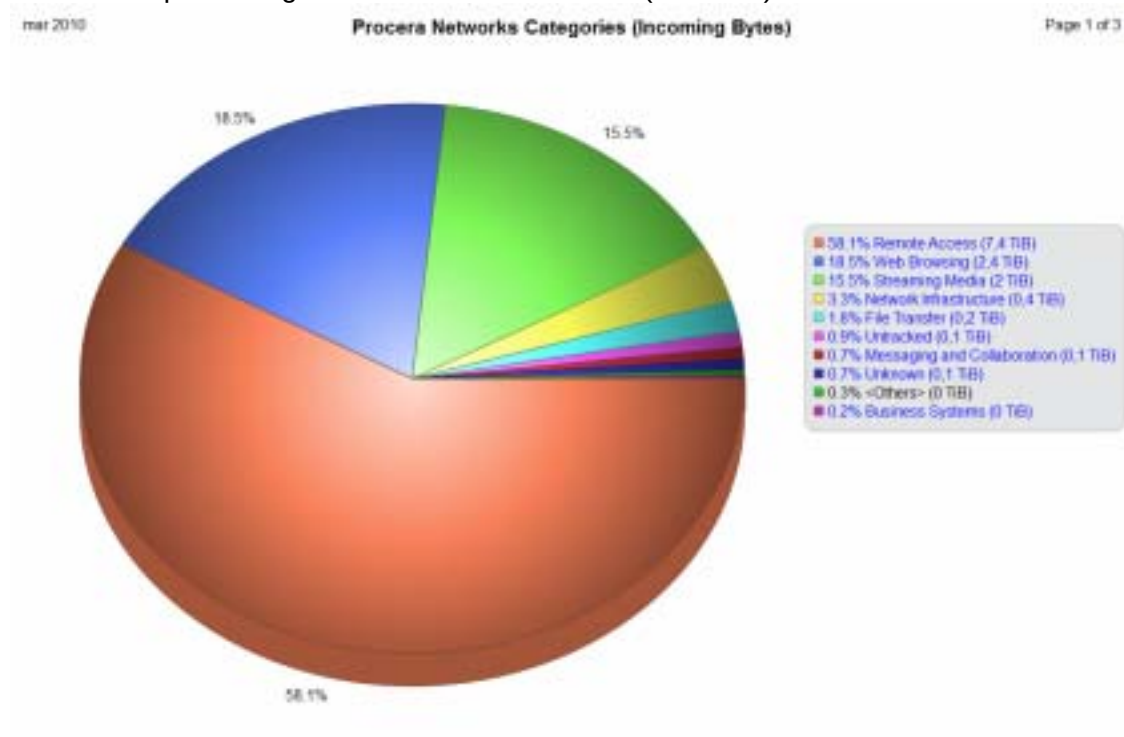
- En del som tillhör hela Banverket (**10 nätet**).
- En del som tillhör Banverket ICT, **ICT** delen är en delmängd av (10 nätet).
- En del som tillhör nättrafik som kopplas till **Serverar** och annan liknande nätinфраstruktur.

Uppdelningen har skett genom att manuellt ange vilka nät och orter som tillhör respektive organisation.

Det har visat sig att fördelningen (använda protokoll och tjänster etc.) mellan Banverket (10 nätet) och Banverket ICT är i stort sätt densamma. Banverket ICT representerar strax under hälften (44 %, 49 %) av Banverkets (10 nätet) trafikmängd detta gäller både inkommande, utgående trafikmängd och antalet anslutningar.

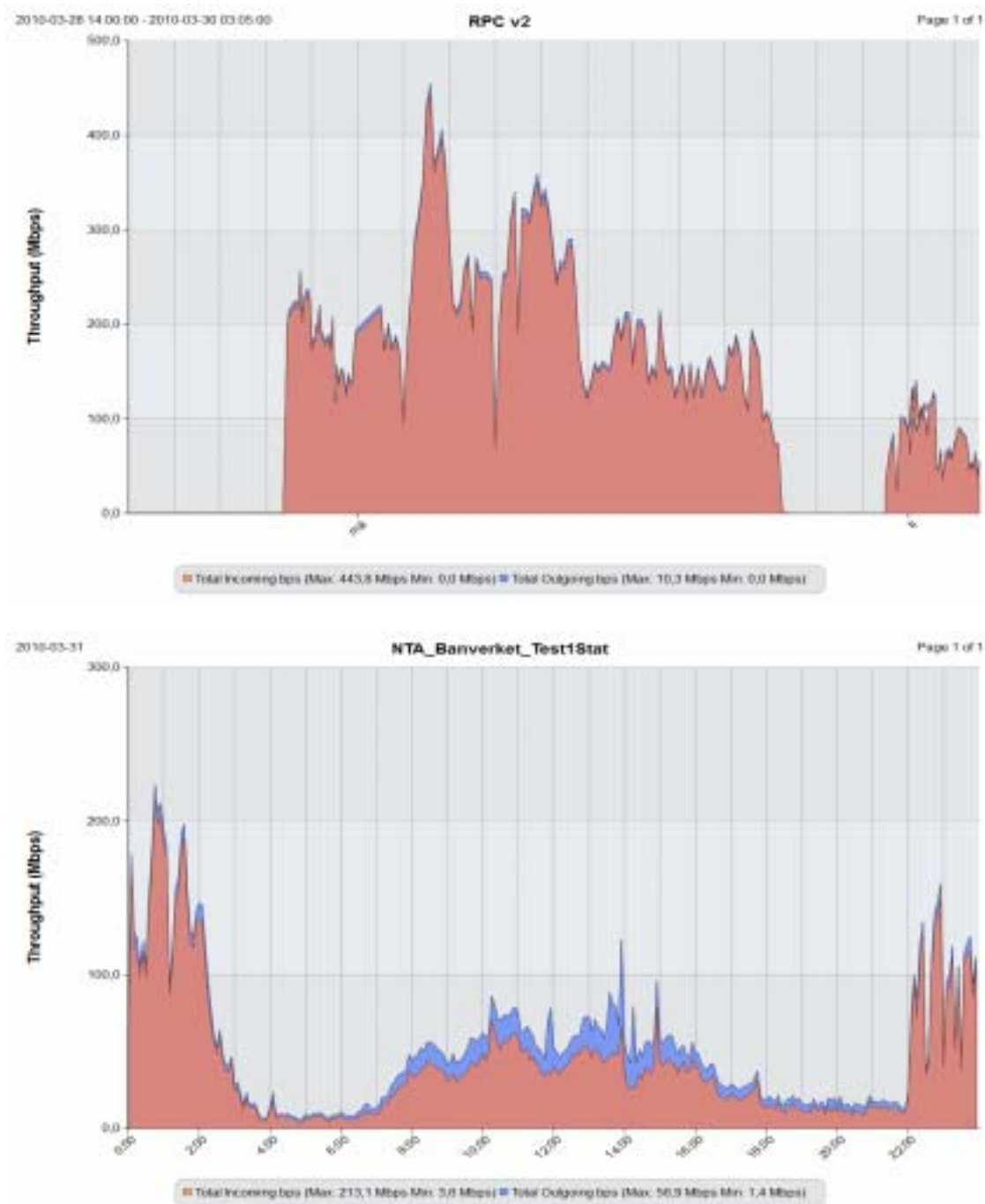
4.1 BANVERKET TOTALT

Banverkets totala nättrafik (**inklusive server trafik**) till och från DMZ och Internet visade sig till större delen bestå av, inkommande Backuptrafik (RPC2). Backuptrafiken går över samma förbindelse (Interface) som resten av nättrafiken.



Figur 5

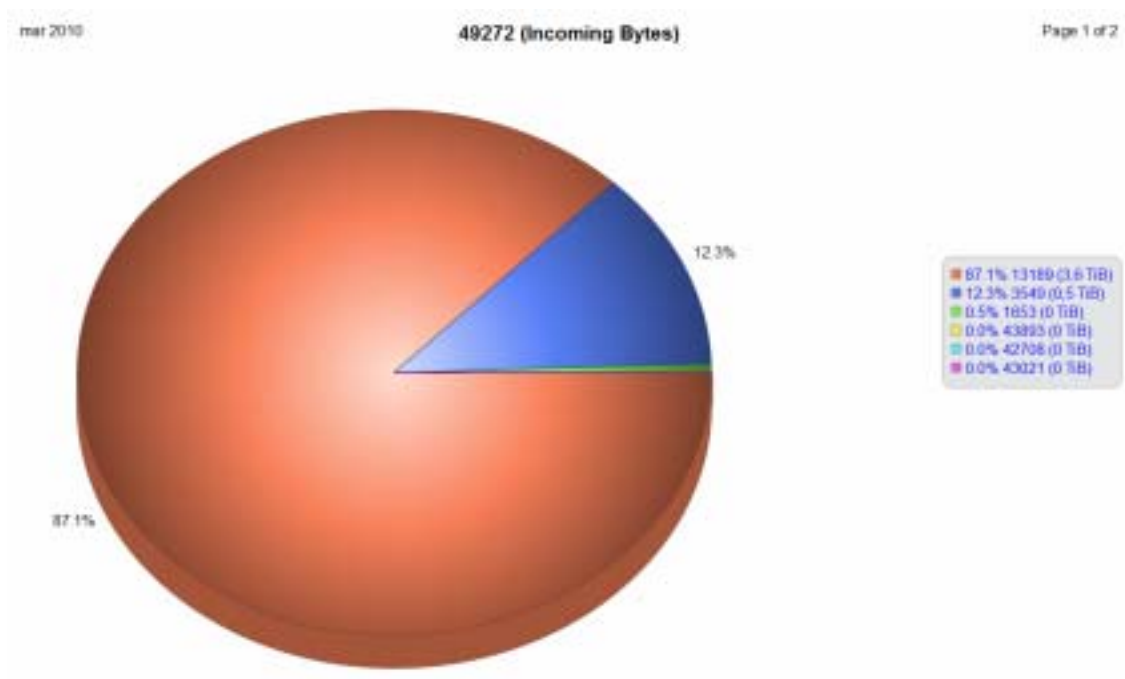
Denna Backuptrafik (RPC2) startar oftast kl 22.00 varje kväll och pågår oftast större delen av natten. Vid månadsslut så har det visat sig att den ökar avsevärt och som maximalt så har **cirka 500Mbps** uppmätts. Det är dock inte ovanligt att Backuptrafiken även körs mitt på dagen. Backuptrafiken är större än både Webtrafiken och Streaming media trafiken.



Figur 6

4.2 INTERNET PEERING TOTALT

All nättrafik till och från Internet (för hela Banverket) kommer i princip från 2 stycken Internet leverantörer. Den ena Lidero Network (AS13189) som hanterar cirka **85-87%** av all trafik och den andra Global Crossing (AS3549) som hanterar cirka **13-15%** av all trafik.



Figur 7

Värt att notera är att t.ex. vägverket dvs. **vv.se** nås genom att hoppa 2 stycken AS över internet, trots att det finns en egen fiber mellan dessa två administrativa domäner. Det finns ett litet antal AS som Banverket har direkt peering men där går det nästan ingen trafik alls



Figur 8

Trots att banverket har redundanta anslutningar mot Lidero så kan problem hos internetleverantören Lidero påverka **upp till 90 procent** av banverkets trafik till och från Internet.

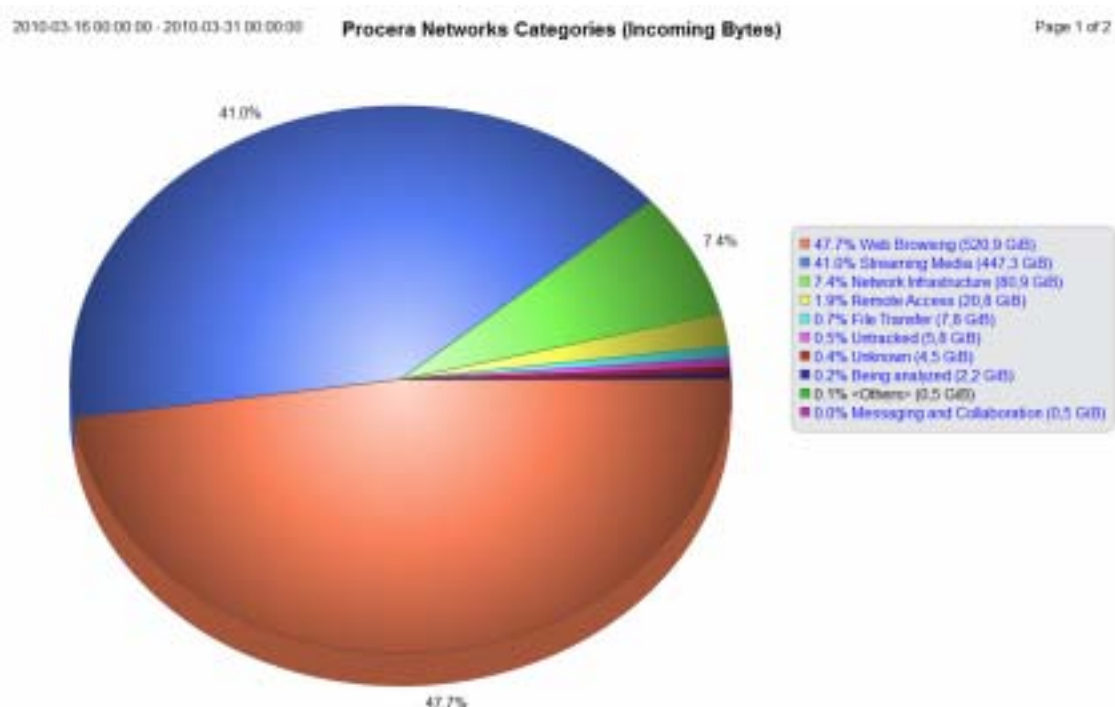
En relevant jämförelse är att under 2008 så kunde en felaktig uppdatering av BGP protokollet få merparten av Junipers routrar (Junos operativsystem) att stänga BGP sessionen och starta om den, vilket resulterade till en riktad **denial-of-service** attack mot routrar av en viss tillverkare och mjukvara. Juniper är en av de mest dominanta och välansedda företagen som tillverkar stora peering routrar som hanterat mycket trafik.

Banverket har relativt bra prisbild gentemot sina två internetleverantörer men det bedöms dock att det finns utrymme för att förhandla ner dessa priser

4.3 BANVERKET ICT

Nättrafiken för ICT delen har delats upp på de orter (kontor) som ICT har personal. Nät och IP adresser som används av ICT personal har manuellt lags in i systemet (Procera 7720) för att kunna skilja på ICT och resten av Banverket.

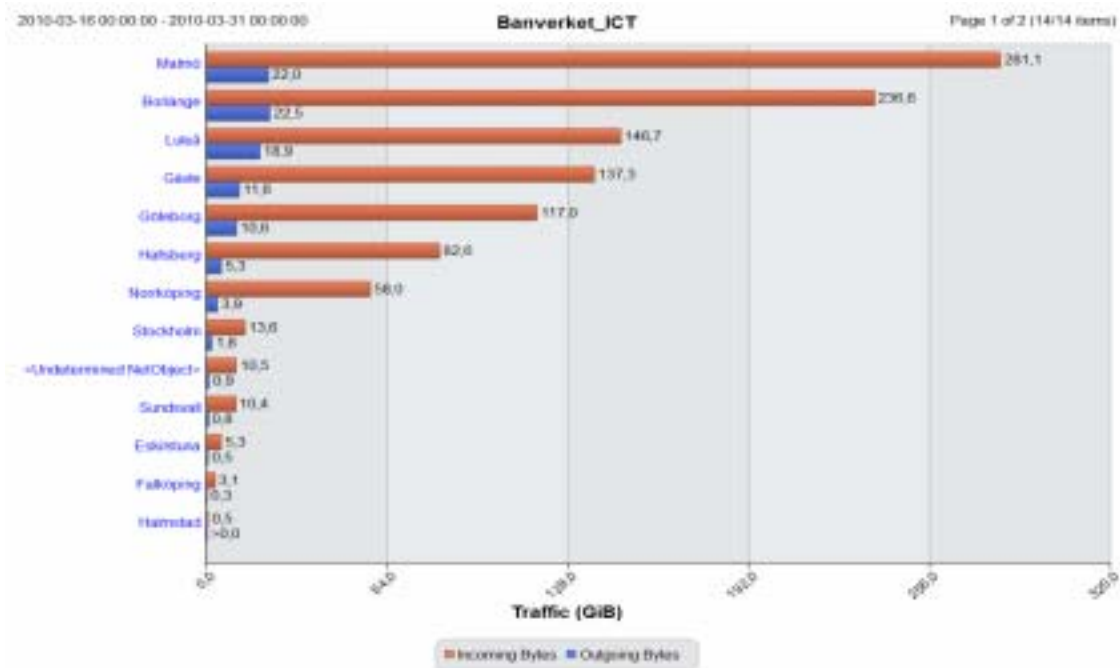
I de fall som ICT personal sitter blandat med personal från andra delar av Banverket så har det inte kunnat skilja på dessa användare.



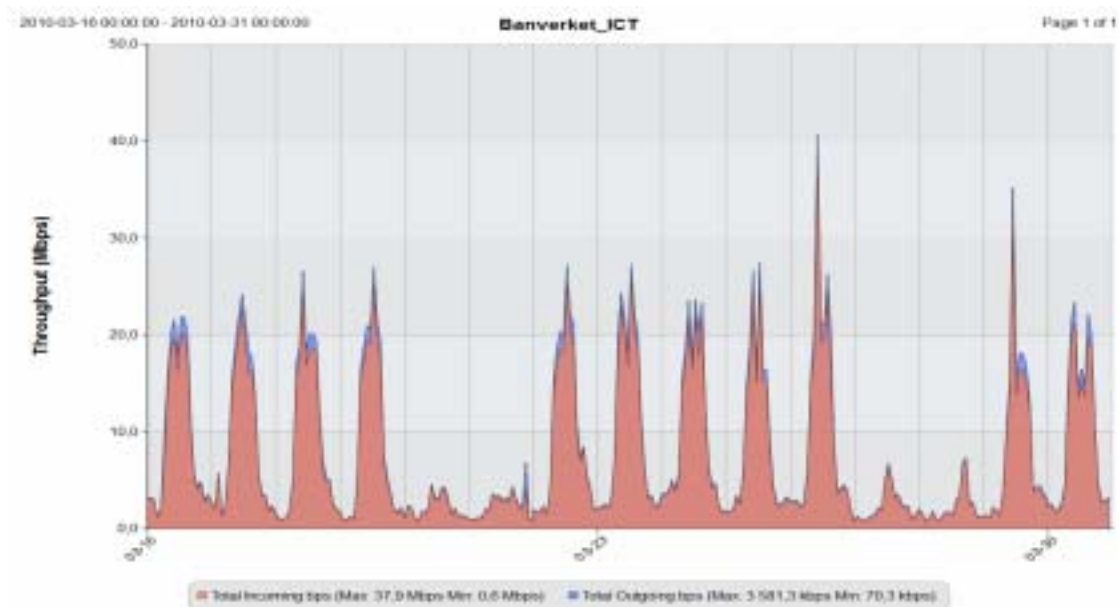
Figur 9

ICTs nättrafik domineras av Webtrafik **47 %** och Streaming media trafik **41 %**. Network infrastucture är i huvudsak SSL trafik.

Malmö, Borlänge och Luleå är de tre kontoren/platserna som konsumerar/genererar mest nättrafik för ICT



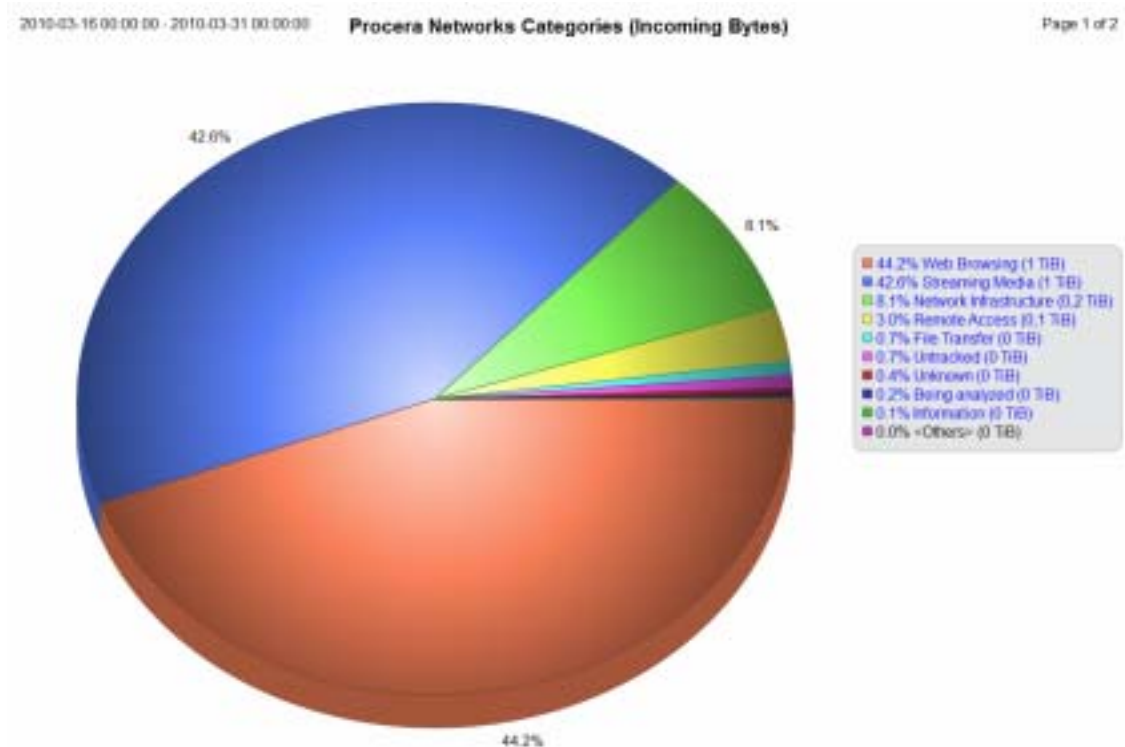
Figur 10



Figur 11

4.4 BANVERKET (10 NÄTET)

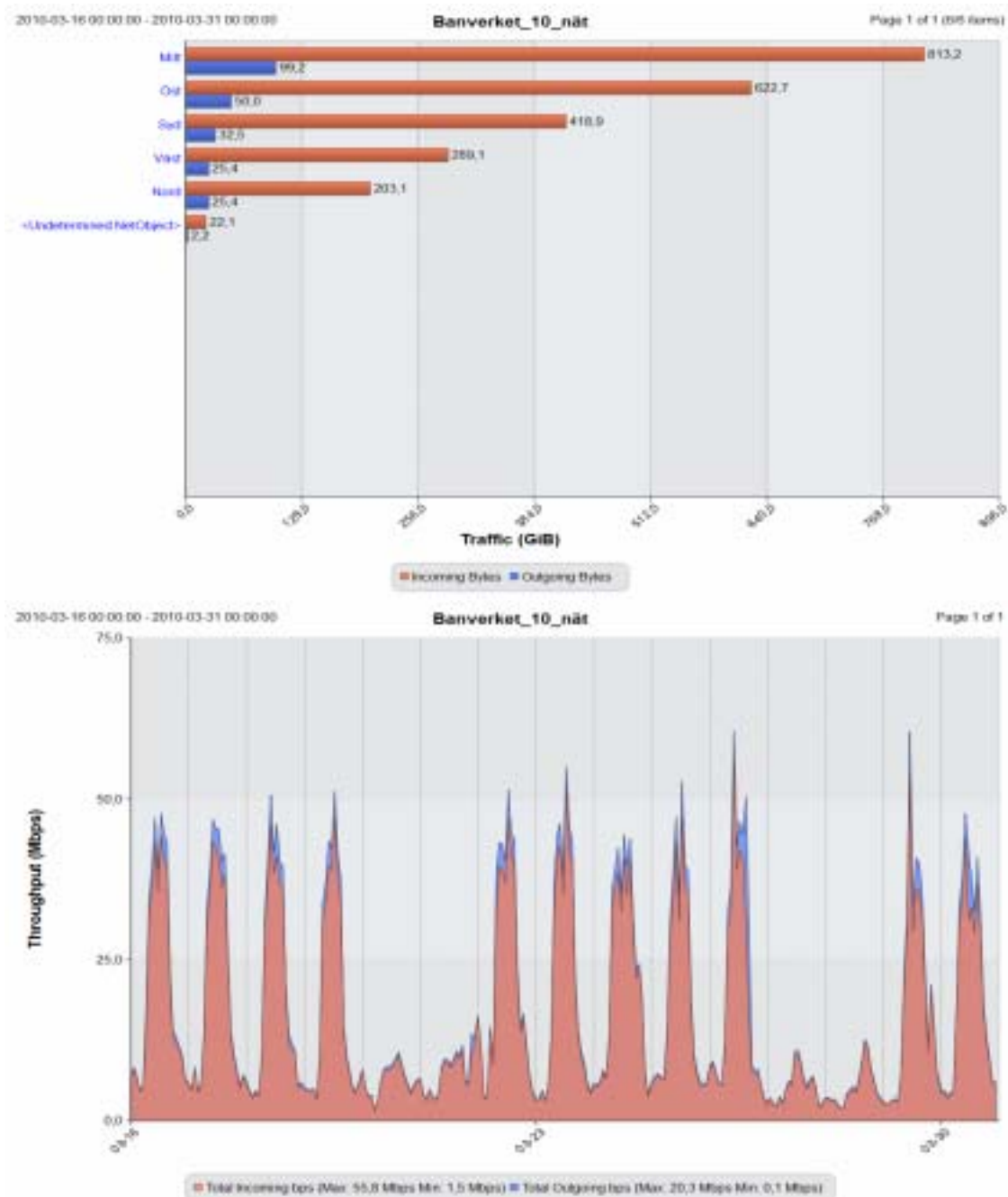
Banverket totalt motsvaras av all Banverks trafik (10 nätet) inklusive ICTs del



Figur 12

Banverkets nättrafik domineras å samma sätt som ICTs av **Webbrowsing 43 %** och **Streaming media trafik 44 %**. Även här så har den rena servertrafiken räknats bort.

Region Mitt, Region Öst och Region Syd är de tre regionerna som konsumerar/genererar mest nättrafik för hela Banverket.

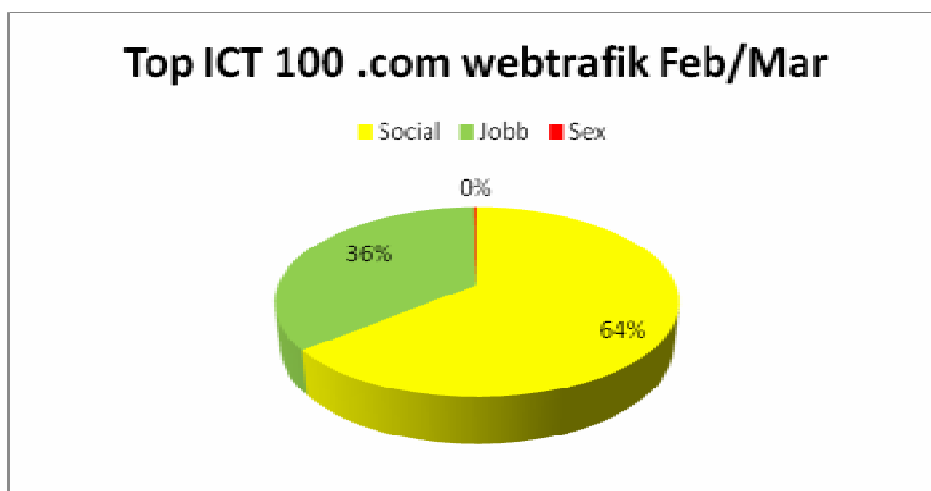


Figur 13

4.5 ANALYS AV ICT'S WEBTRAFIK

Analys av ICTs Webtrafik har visat att en stor del att Webtrafiken är kopplat till "Social Networking" relaterade siter.

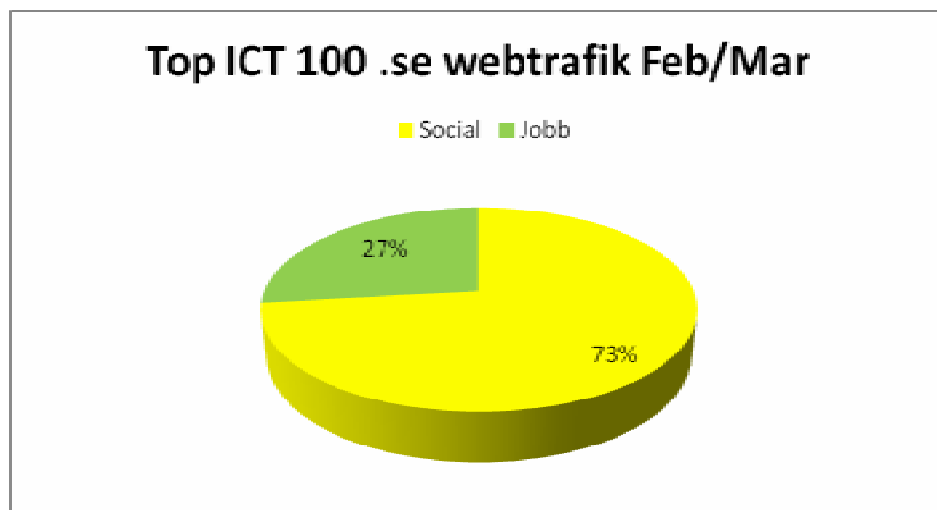
Av mängden (MB) nättrafik till och från de två största domänerna.com och se så uppskattas att **64 % -73 %** är med största sannolikhet icke jobbrelaterad. En liten del trafik är tom till och från rena "Sex/Porr" siter.



Figur 14

Topp 10 besökta siter för .com domänen (gul färg "Social", grön "jobb").

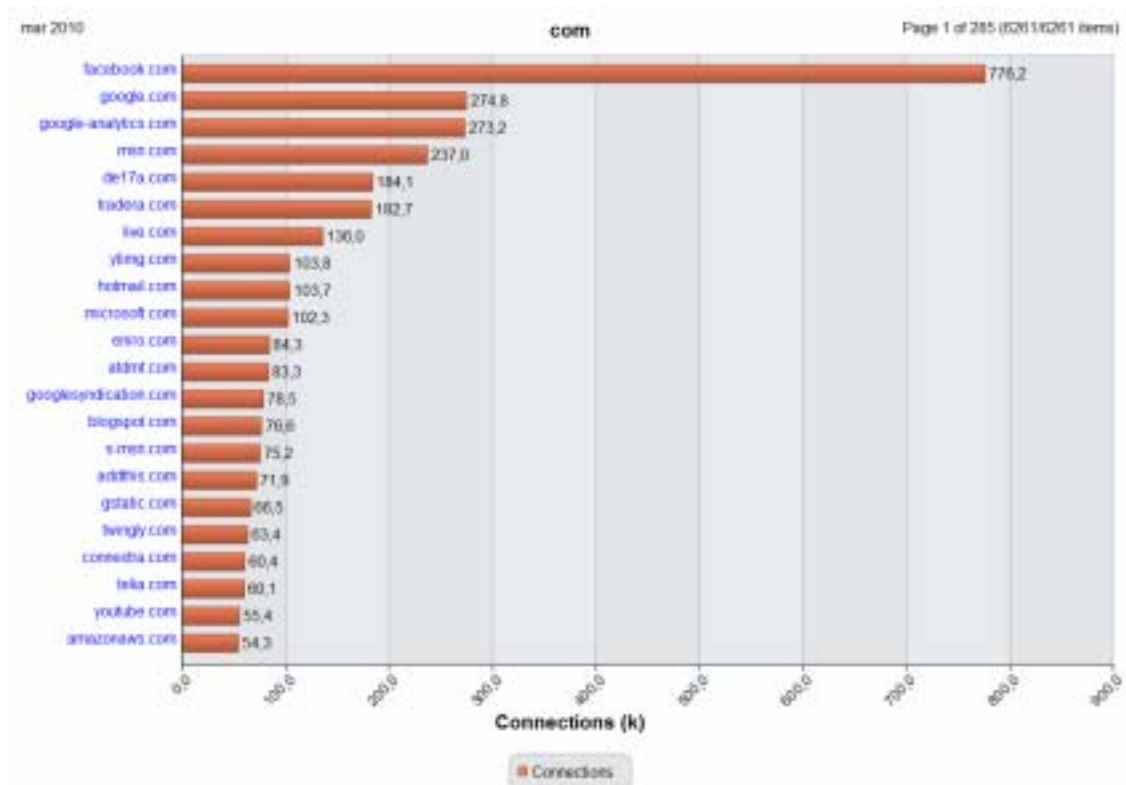
youtube.com
microsoft.com
qbrick.com
eniro.com
google.com
facebook.com
farmville.com
apicasystem.com
de17a.com
msdn.com

**Figur 15**

Topp 10 besökta siter för .se domänen (gul färg "Social", grön "jobb")

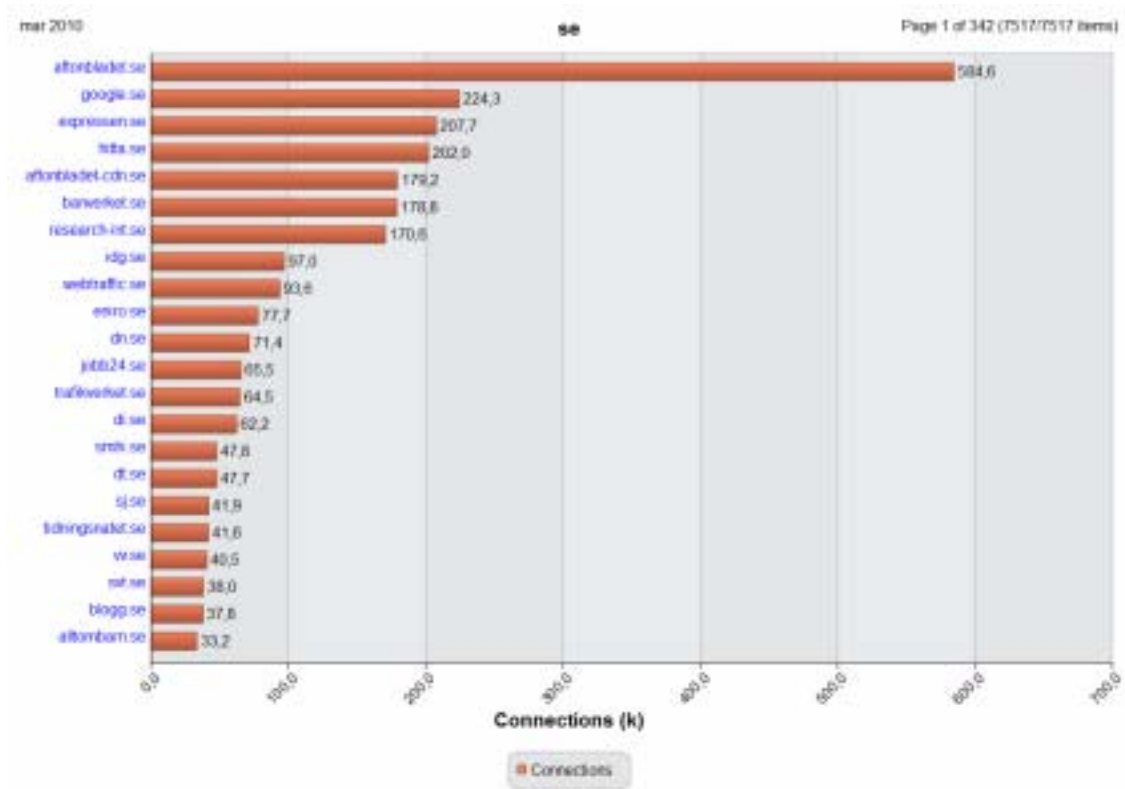
aftonbladet-cdn.se
expressen.se
banverket.se
vv.se
aftonbladet.se
hitta.se
idg.se
webtraining.se
di.se
xmc.se

Om man väljer att undersöka antalet förbindelser mot en viss domän, antalet förbindelser är ofta korrelerat till aktiviteten, så ändras bilden lite. För ICTs del av trafiken mot t.ex. .com så är facebook den mest aktiva domänen. Den motsvarar cirka **17 %** av alla .com förbindelser under mars månad.



Figur 16

Totalt sätt så är **facebook** tillsammans med **aftonbladet** och **google** de tre mest aktiva siterna domänerna som Banverket ICT utnyttjar. Jämfört med hela banverket som låg på **25 % respektive 19** facebook i februari respektive mars så ligger ICT procentuellt lite lägre användning av facebook än hela Banverket

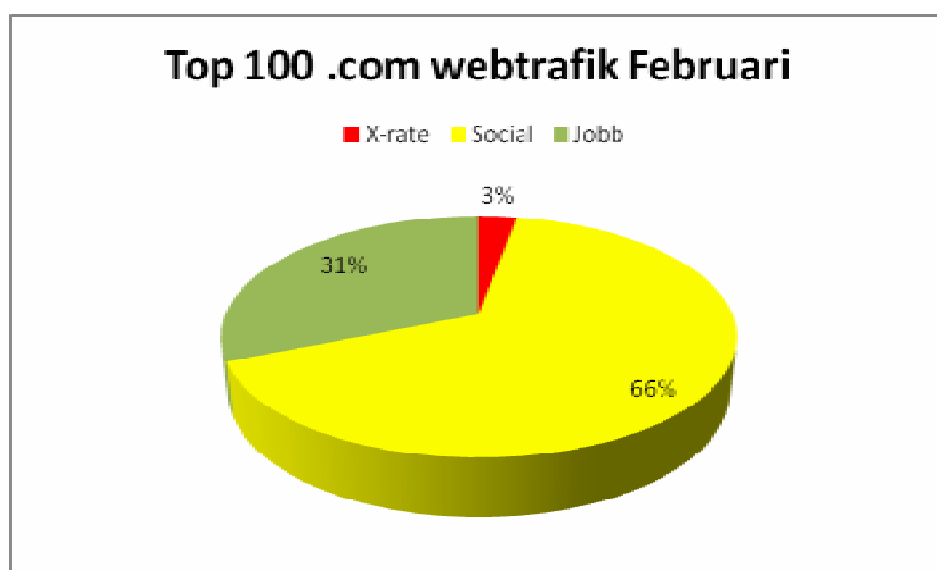


Figur 17

4.6 ANALYS AV HELA BANVERKET'S WEBTRAFIK

Analys av Banverket webtrafik (inkluderat ICTs del) har visat att en stor del att webtrafiken är kopplat till "Social Networking" relaterade siter.

Av mängden (MB) nättrafik till och från de två största domänerna .com och .se så uppskattas att **66 % -73 %** är icke jobbrelaterad. En relativt stor del 3 % trafik är tom till och från rena "Sex/Porr" siter.



Figur 18

Topp 10 besökta siter för .com domänen (gul färg "Social", grön "jobb", röd "Sex/Porr").

youtube.com
qbrick.com
eniro.com
facebook.com
google.com
microsoft.com
farmville.com
pornrabbit.com
panthercustomer.com



garmin.com



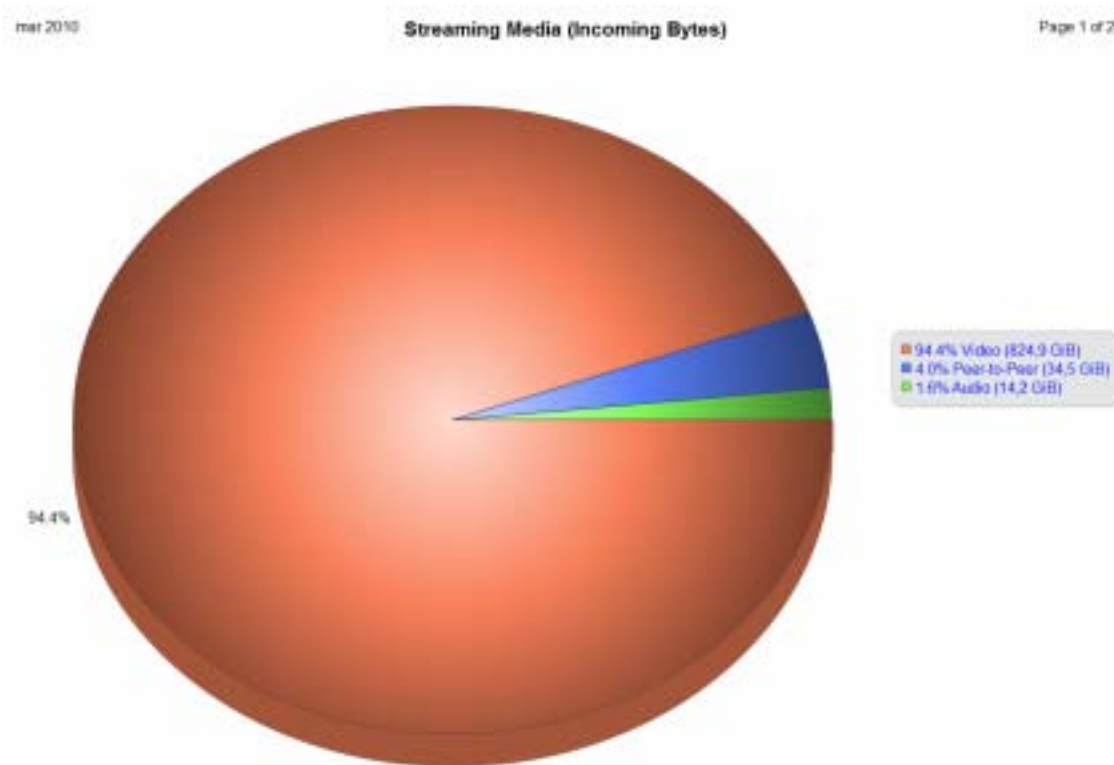
Figur 19

Topp 10 besökta sites för .se domänen (gul färg "Social", grön "jobb")

aftonbladet-cdn.se
expressen.se
banverket.se
aftonbladet.se
hitta.se
svt.se
sr.se
dn.se
di.se
dt.se

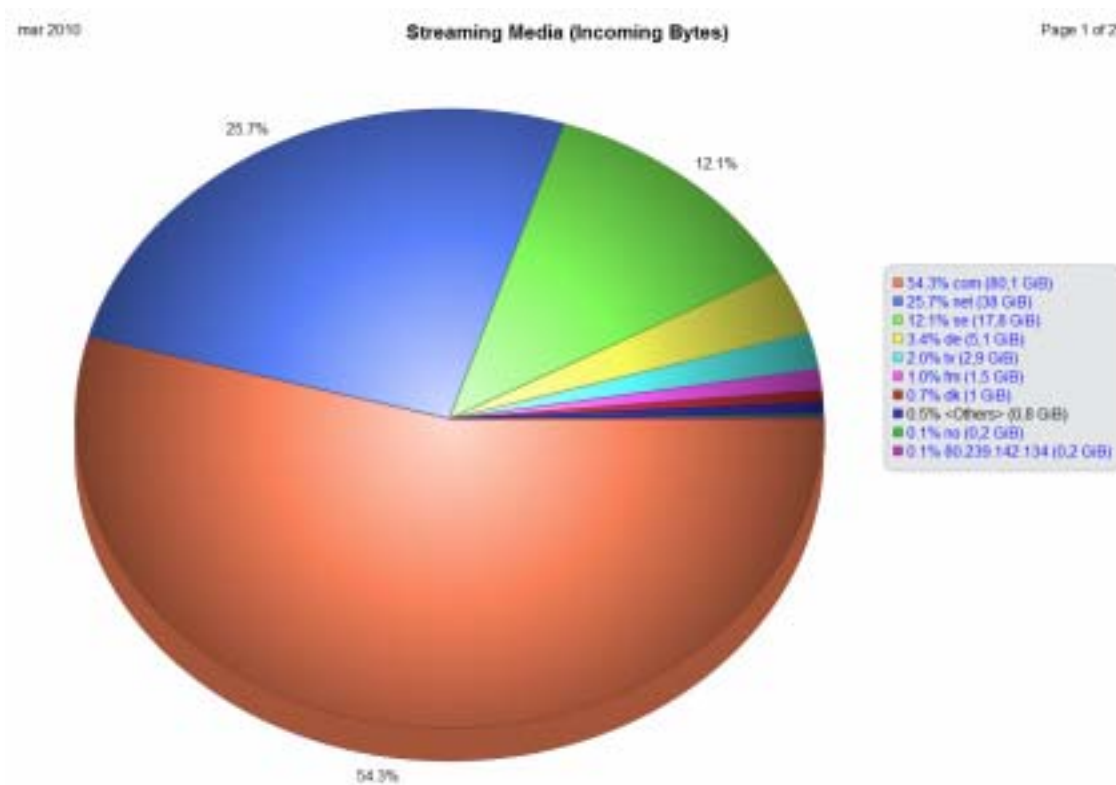
4.7 ANALYS STREAMING MEDIA ICT

Video är den viktigaste streaming media tjänst några ljud och lite peer-to-peer streaming. Strömmande media är främst streaming av video och musik från sajter som svt.play och bahnhof.net.



Figur 20

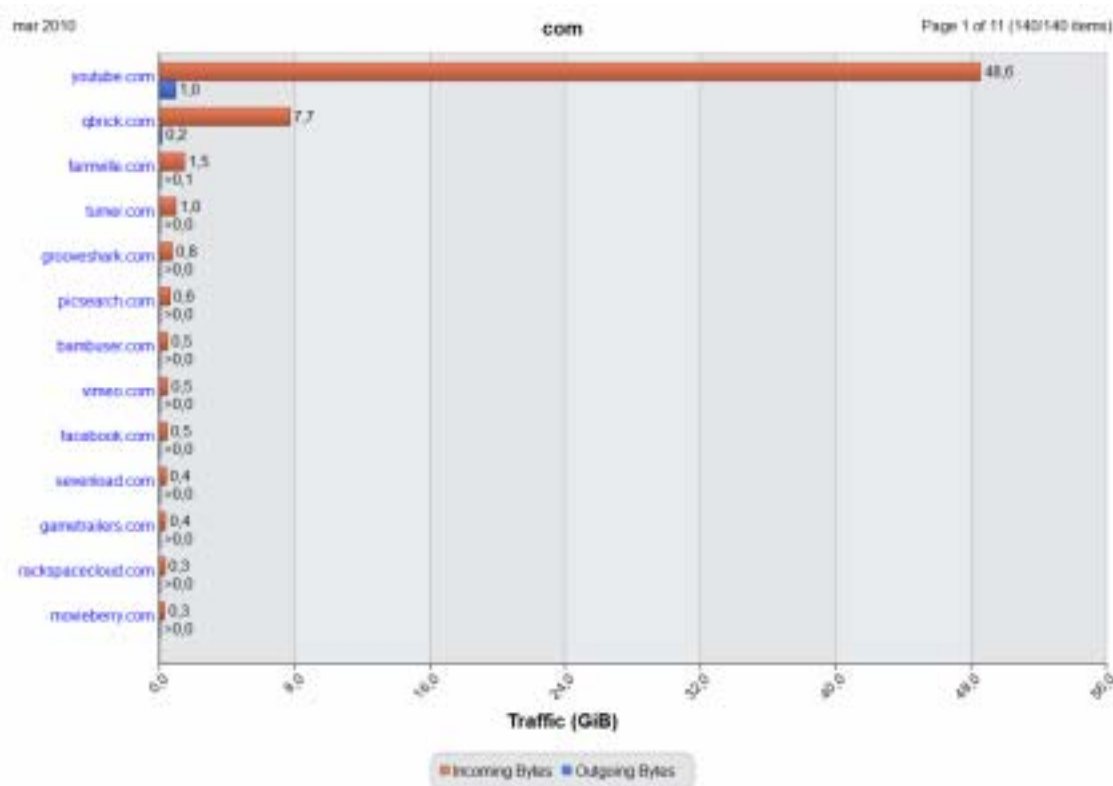
Bahnhof.net representerar 50 % av strömmande medier som är en typisk webradio tjänst. En minst lika stor del är streaming media (för ICT) som jämförelsevis är lika stor som webtrafiken (http) fast till en **större del än http** är ren social eller ej direkt jobbrelaterad . Uppskattningsvis så ligger upp till **90 %** av inkommande streamingmedia på den sociala/ icke jobbrelaterade delen.



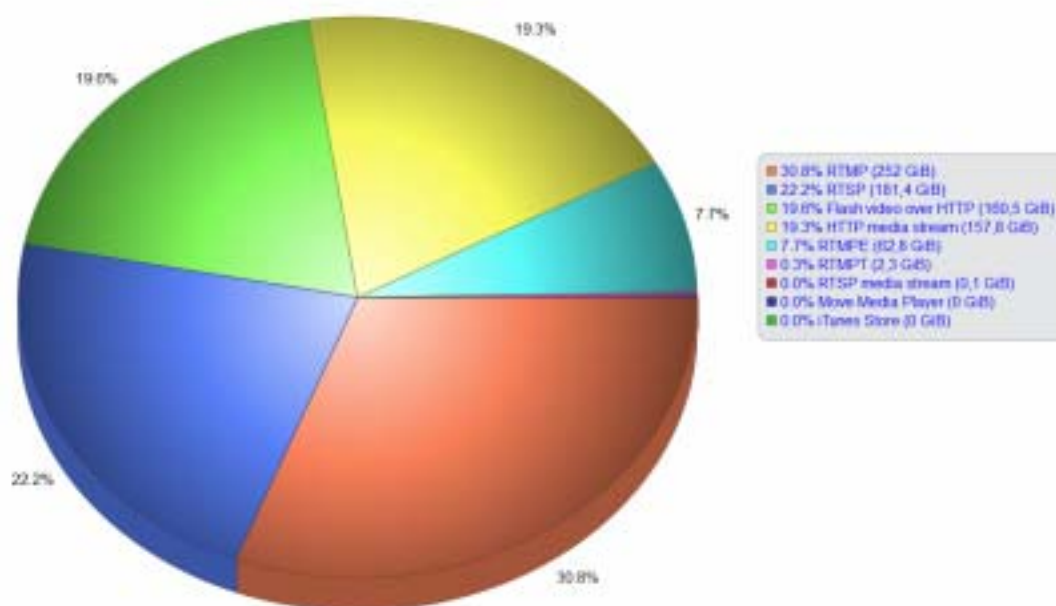
Figur 21

Det går att hitta lite banverket och vägverket relaterad streaming media, typ mindre än 0,5 %

- 54 % Youtube
- 26 % Bahnhof.net = webradio etc
- 10 % av .se (xmc, sbsradio, svt, viasat)



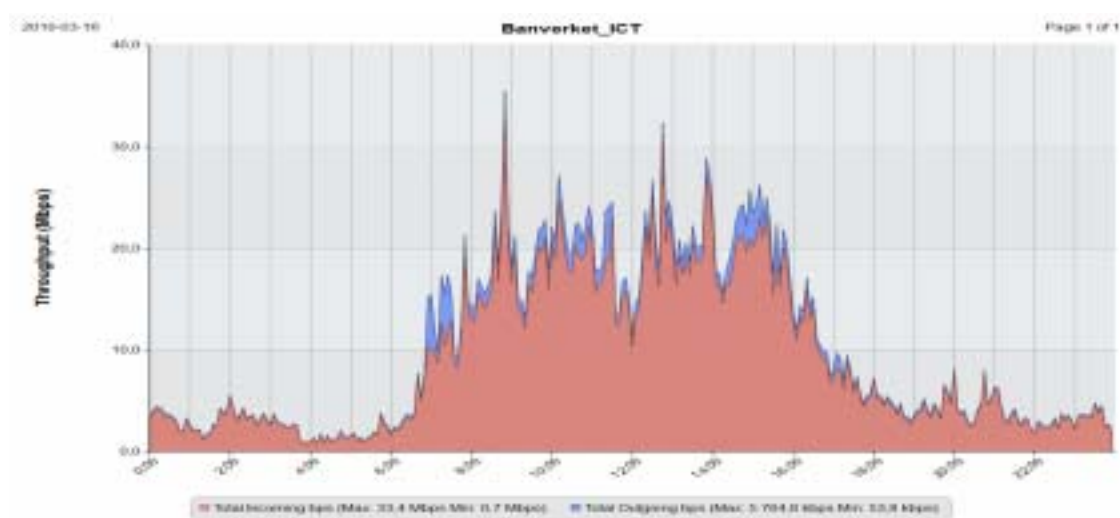
Figur 22



Figur 23

4.8 ANALYS NÄTVERKSTRAFIK ICT

Graferna nedan beskriver en typisk fördelning av dygnstrafiken under en normal arbetsdag. Trafiken avtar signifikant under helger. Det är relativt få användare som står för större del av trafiken fördelningen är att cirka **10 % av användarna står för 60 % av den totala trafiken**. Det är med andra ord oftast väldigt få som står för den största delen av trafiken.

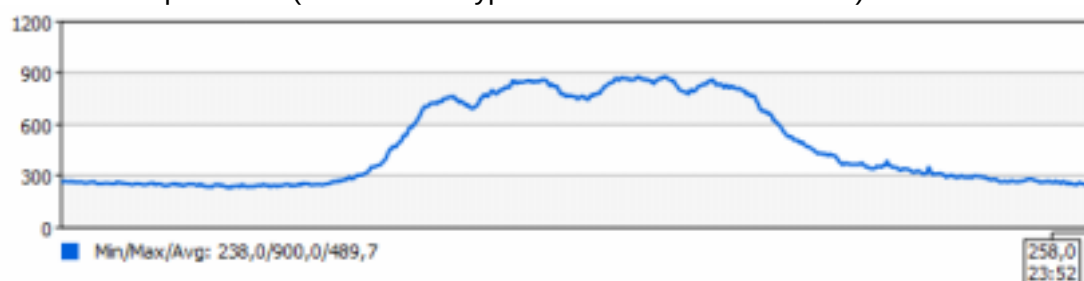




Figur 24

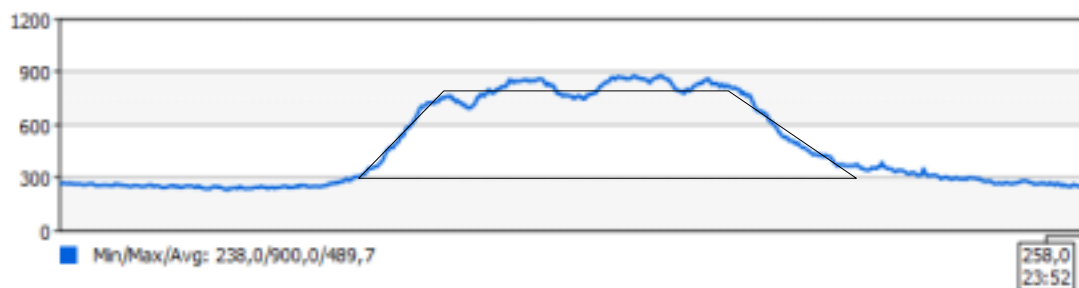
4.9 MANTIMAR FÖR HELA BANVERKET

Antalet samtidigt anslutna värdar (burkar, användare), egentligen IP-adresser, är i genomsnitt cirka **500** med högsta topp på strax över **900** värdar per dag och lägst strax under **300** på natten (se nedan en typisk 24h intervall 2010-03-09).



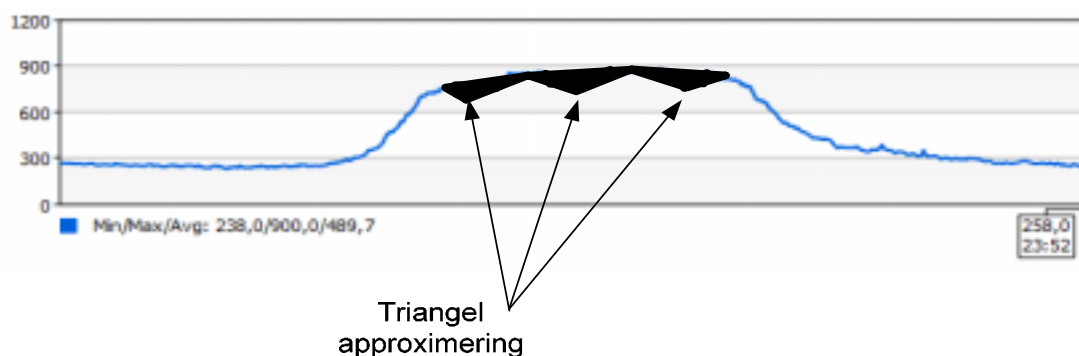
Figur 25

Ytan under denna kurva korrelerar mot de mantimmar som produceras över denna punkt i nätet (eg. Banverkets IT infrastruktur).



Figur 26

Nedgång i kurvan för anslutna användare representeras av största sannolikhet av fenomenet fika-lunch-fika.



Figur 27

Dessa nedgångar (se fig 27) approximeras med trianglar vilket medför att man kan ta fram ett **jämförelseindex som korrelerar** mot de mantimmar när användarna inte använder nätet. Man ska inte tolka det att det är exakt så mycket potentiell arbetstid som försvinner vid dessa tillfällen. Det är sannolikt mer då inte alla loggar ur eller stänger sina datorer som också har en förmåga att generera trafik själva.

host	780		856		872		850
		714		756		806	
tid	8.30	9.15	10.40	11.50	13.10	14.15	15.02

Antalet mantimmar som motsvaras av dipparna ligger normalt kring **225-250**



Mantimmar per arbetsdag. Det går att visa att om man "spetsar" till fika-lunch-fika med cirka **18 minuter** så får utrymme för produktivitetshöjning på över 10 %.

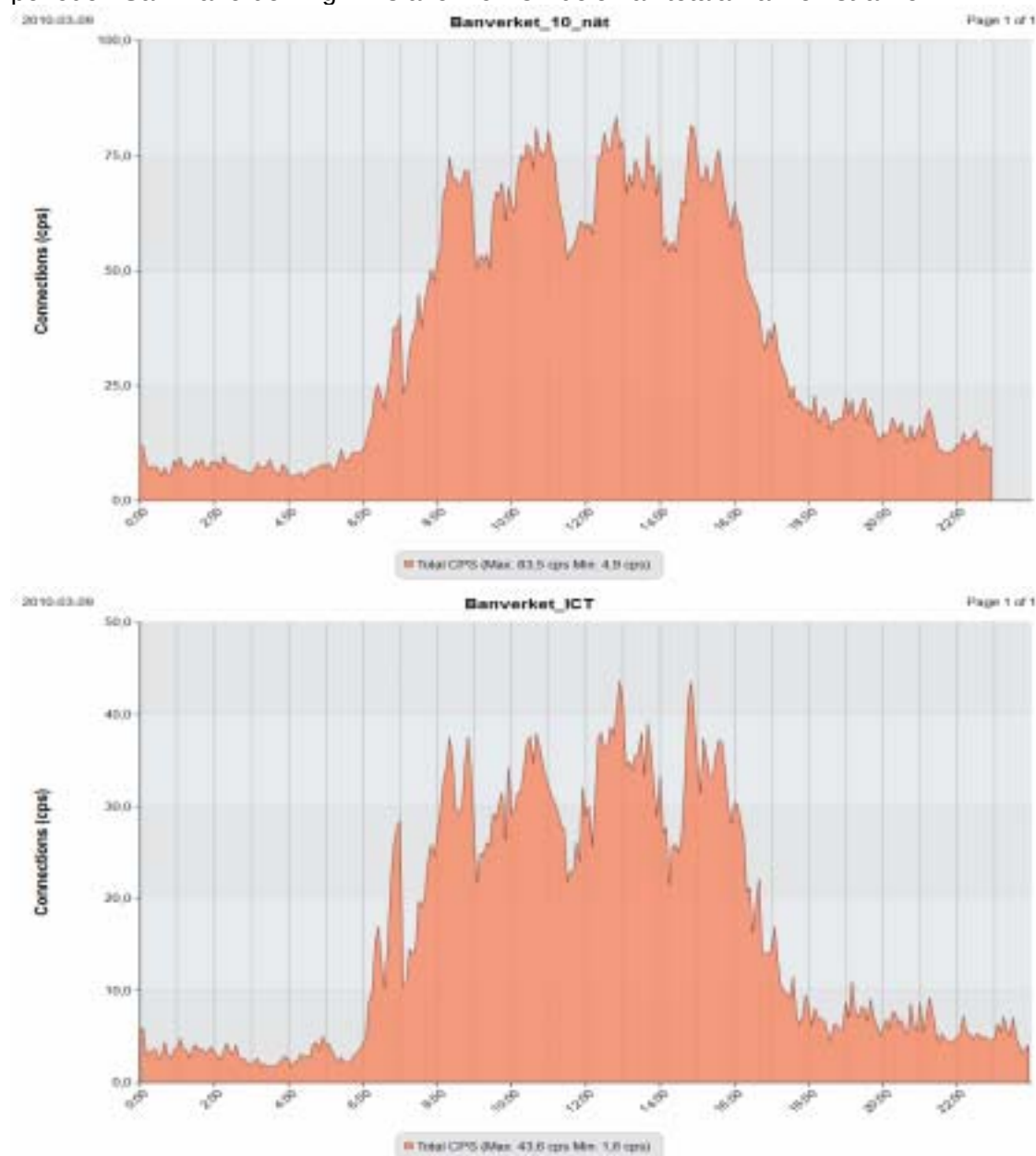
Antalet mantimmar som i medeltal produceras och passerar denna punkt i nätet ligger på cirka **4500** Mantimmar.

Ett Excel ark har tagits fram för att göra dessa beräkningar halvmanuellt (se Bilaga 2,3 och 4).

Detta har inte kunnat göras automatiskt då ingen mjukvara/script har utvecklats för denna kundanpassade funktion.

*Efter sammanslagning till ny organisation 1 april så har antalet anslutna användare ökat, max samtidigt anslutna cirka **1100** och totalt så har antalet mantimmar som produceras över samma punkt ökat till cirka **5500**, dropparna i trafiken motsvaras numera av **470** mantimmar vilket motsvaras 8-9% av en normal arbetsdag (detta har ökat jämfört med 5-5% som det var innan).*

Antalet förbindelser (För Banverket som helhet) har under samma tid har följande typiska fördelning. Man kan alltså se en tydlig nedgång i nätaktivitet under dessa perioder. Samma fördelning finns även för ICT delen av totala Banverkstrafiken.

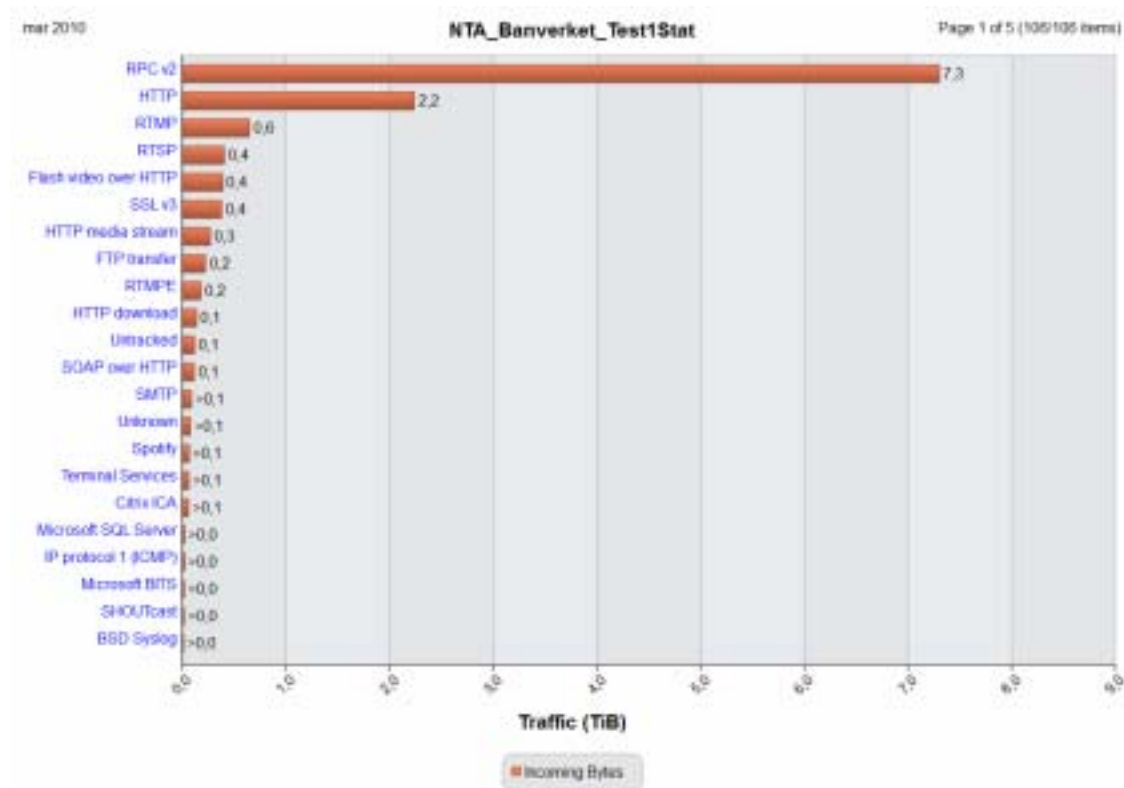


Figur 28

4.10 TJÄNSTER OCH PROTOKOLL

De mest använda protokollen för hela Banverket är **RPC2** och **HTTP**.

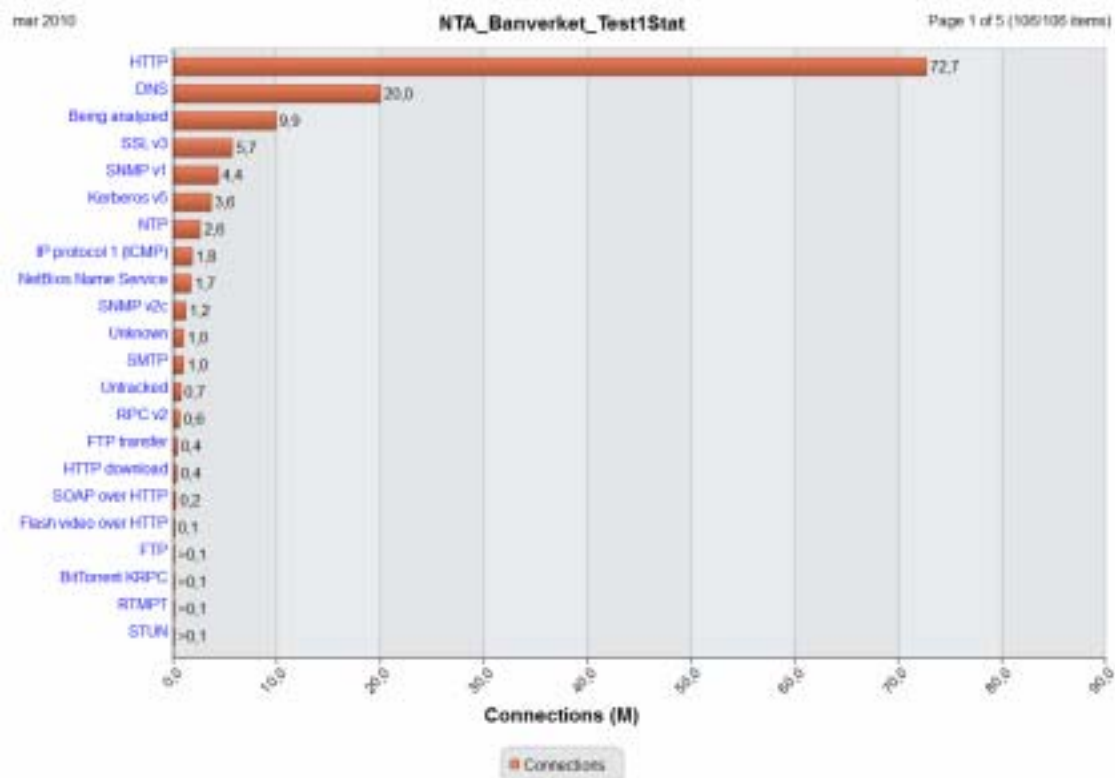
Det totala antalet observerade protokoll är **106** stycken. RPC2 är det enskilda protokoll som används mest resten är i huvudsak web och streaming media relaterad protokoll. SSL används för någon typ av säker login mot olika sites. Man kan observera att Spotify är relativt populärt det finns förekomst av andra protokoll såsom Skype, Bittorrent och iTunes.



Figur 29

Antalet protokoll som verkligen används är förhållandevis många.

Om man jämför antalet anslutningar (connections) så är http det mest popular protokollet.



Figur 30



HTTP

HyperText Transfer Protocol är det kommunikationsprotokoll som används för att överföra webbsidor på informationsnätverket WWW, World Wide Web på Internet.

RTMP

Real Time Messaging Protocol (RTMP) är ett proprietär protokoll som utvecklats av Adobe Systems för strömmande ljud, video och data över Internet.

RTSP

Real Time Streaming Protocol (RTSP) är ett nätverk Control Protocol för användning i underhållnings- och kommunikationssystem för att kontrollera strömmande media servrar.

Flashvideo over http

Flash Video är ett s.k. container filformat som används för att leverera video över Internet med hjälp av Adobe Flash Player .

SSLv3

Secure Sockets Layer v3 (SSL v3) protokollet tillhandahåller privat kommunikation via Internet för att förhindra avlyssning, manipulering eller förfalskning av meddelanden mellan klient/server applikationer.

FTP

File Transfer Protocol (FTP) är en standard nätverksprotokoll som används för utbyte och överföring filer via ett TCP/IP-baserade nätverk, t.ex. Internet. FTP är byggd på en klient-server arkitektur och använder separata kontroller och dataanslutningar mellan klient- och serverprogram.

RTMPE

Krypterade Real Time Messaging Protocol (RTMPE eller RTMPTE) är ett proprietärt protokoll skapad av Macromedia som används för strömmande video och DRM.

SMTP

Simple Mail Transfer Protocol (SMTP) är det vanligaste kommunikationsprotokollet för att leverera elektronisk post. Kommunikationen sker via TCP, normalt på port 25

SPOTIFY

Spotify-klienten är ett program, och således inte en webbaserad tjänst. Spotify-applikationen finns idag för Windows och Mac OS X,

DNS



Domain Name System eller domännamnssystemet, är ett system för att förenkla adressering av datorer på IP-nätverk som till exempel Internet. DNS är ett distribuerat system, där zoner av IP-nummer delegeras till ansvariga företag och organisationer. DNS är ett klient–server-system.

Kerberos v5

Kerberos är ett datornätverk Authentication Protocol, vilket gör noder kommunicerar via ett icke-säkert nätverk för att bevisa sin identitet till varandra på ett säkert sätt.

NTP

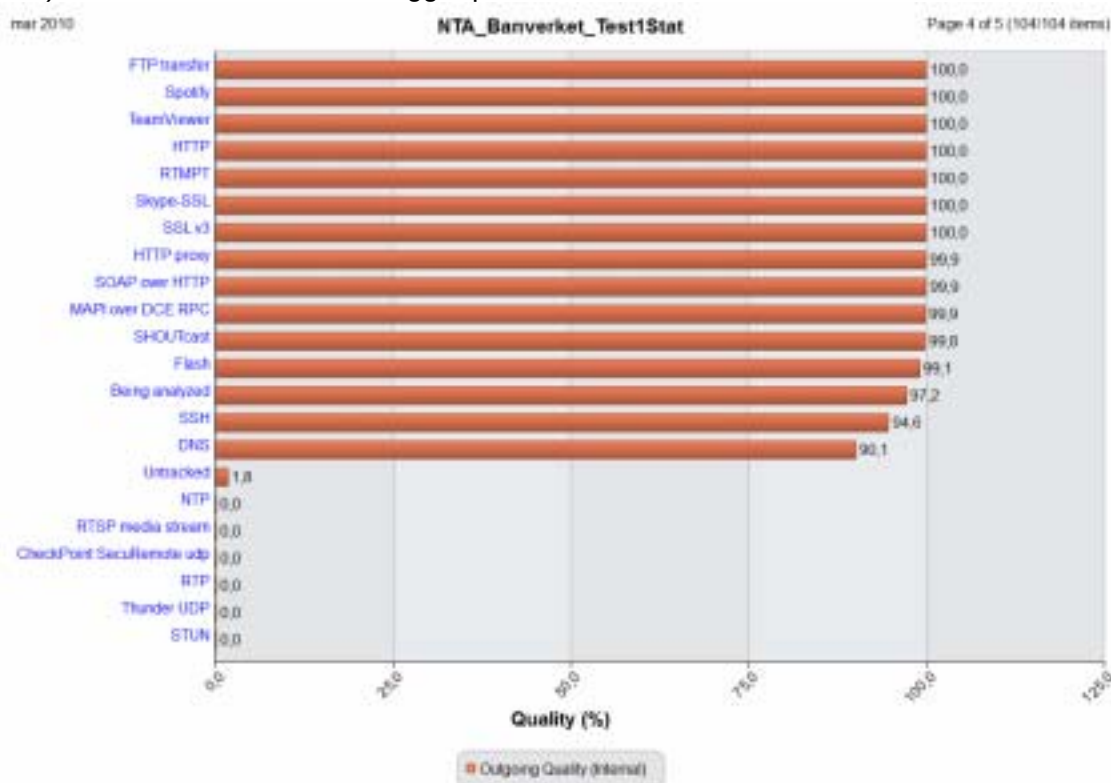
NTP eller Network Time Protocol är ett protokoll för att synkronisera tiden i ett nätverk med varierande svarstider.

SNMP

Den SNMPv1 och SNMP v2c tjänst använder mest anslutningar. Det finns också en stor mängd av ICMP-trafik, d.v.s. Pings som förmodligen används för nät drift, utan också skulle kunna användas för ping svep som är ett nätverk skanning teknik som, om de genereras externt skulle med ont uppsåt.

4.11 QUALITY OF EXPERIENCE

PacketLogic analyserar den upplevda kvaliteten på **TCP-anslutningar**. De värden som presenteras för kvalitet QoE beräknas som en procentandel, av antalet "droppar" eller vidareändring av antalet paket dividerat med totala antalet paket. Kvaliteten sker separat för varje riktning och varje kanal. De allra flesta användare, tjänster protokoll har ett index på 100 vilket maximalt (och normalt, ingen omsändning/dropp). Vid olika typer av degenerering och problem i nätet så minskar detta jämförelseindex (QoE). För Banverket ICTs allra flesta användare så är den upplevda kvaliteten god, det är **bara cirka 1 %** av användarna som ligger under 90 % på en dag, vilket motsvarar ett 10 tal IP adresser (användare). Samma fördelning gäller för hela Banverket. De allra flesta protokoll har god upplevd kvalitet (cirka 100), utom DNS och SSH som ligger på cirka 90-94 %.



Figur 31

Det finns en relativt stor del protokoll (RTP, SIP etc.) med QoE = 0 dessa protokoll

använder UDP och omfattas ej av QoE algoritmen.

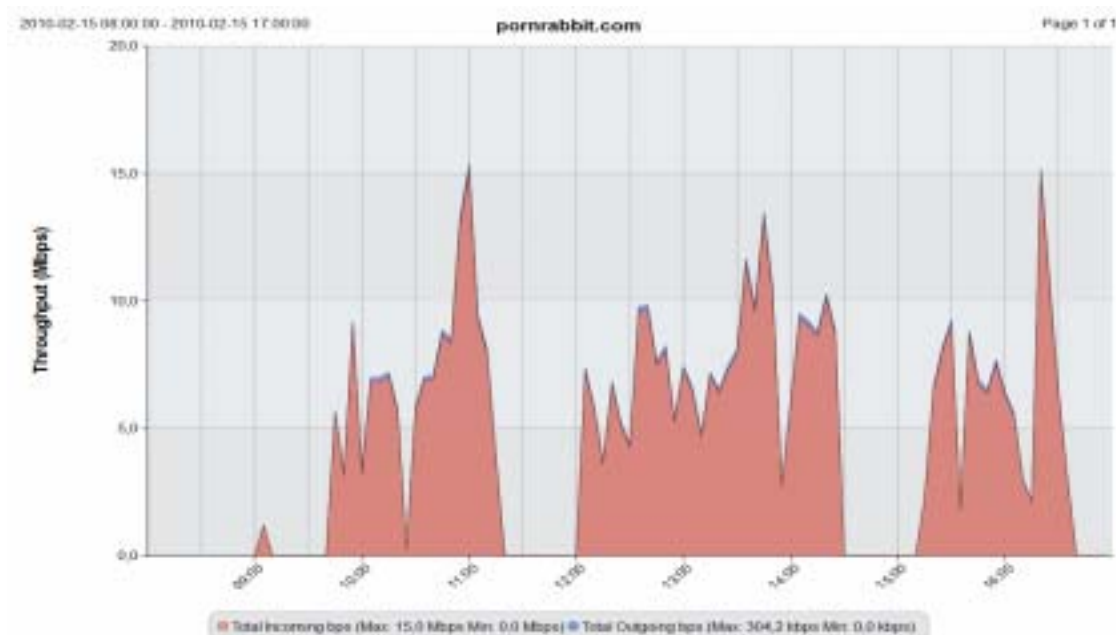
4.12 ANOMALIER

4.12.1 MOBISIR

Det är upptäckt att ett okänt nät (det visade sig vara **MobiSIR** efter flera dagars utredning) hade en märkligt stor **NTP trafik**. Efterforskningar visade på en felkonfigurering av MobiSIR enheter (t.ex. GPRS anslutna informationsskyltar/Tidtabeller) där tid hämtades från USA 7 autonoma system bort istället för att hämta tid från Banverkets egna NTP servrar.

4.12.2 SEX OCH PORR

Det upptäcktes att det var en enda användare som genererade hela trafiken till sex-siten www.pornrabbit.com. Information om detta gavs direkt till Banverkets säkerhetsavdelning för vidare utredning.

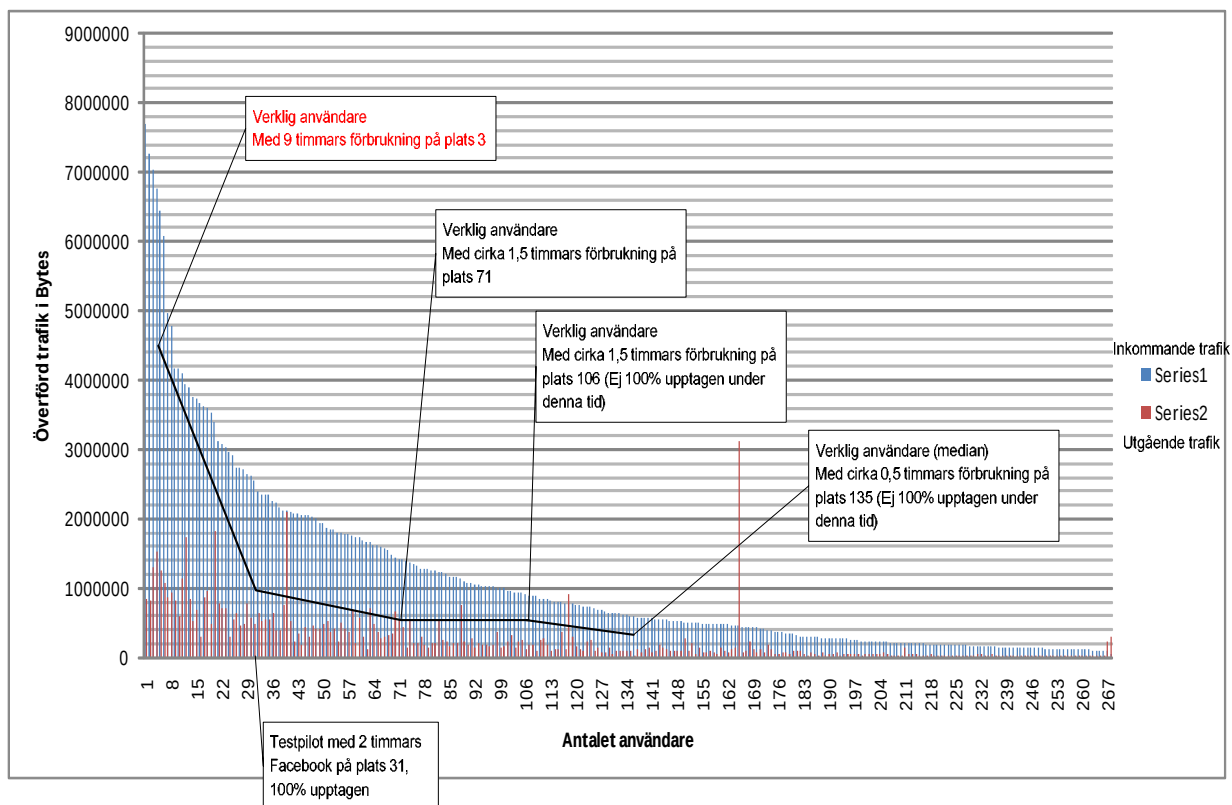




4.13 SPECIALSTUDIE AV FACEBOOK ANVÄNDNING

En testpilot har kört facebook i **2 timmar** mellan 22.00 och 00.00 med 100 % fokusering på icke jobbrelaterade uppgifter Chat, upp och nedladdning mm. Testpiloten har sedan kört Facebook, utan någon aktivitet från användaren mellan 04.00 och 08.00 (detta kallas för "idle"). Detta har gjorts för att få fram en signifikant facebook signatur för att kunna tolka Banverkets nyttjande av facebook

- Cirka **270** stycken hosts (d.v.s. antalet användare) kör facebook varje dag.
- Cirka **30 %** verkar ha Facebook på "idle".
- Cirka **40%** av användarna tillhör ICT
- Det visar sig att cirka **30 % av användarna** har högre dagligt nyttjande av facebook som är **1 timme eller mer**.
- Det är inte helt trivialt att uppskatta hur mycket tid dessa "top" användare förbrukar på facebook men uppskattningsvis så finns det extremfall på **8 till 9 timmar** facebook per dygn (se fig 32), medeluppskattas till cirka **4 timmar**.



Figur 32



4.14 RESULTAT OCH KONSEKVENSER

Som tidigare beskrivits i MAX16 granskningen av nätverkstrafiken har en del fynd, varit allvarliga nog för att motivera ICT ledningens omedelbara uppmärksamhet.

För den första så visade granskningen av nättrafiken att det är **möjligt** att få en **detaljerad bild** av nätanvändning för tjänster, protokoll, bandbredd, anslutningar, kvalitet, "source/destination" samt användare. Detta visar att "Max16 konceptet" som använts både kan presentera informationen om nättrafiken **i realtid** men också förbereda skraddarsydda rapporter/statistik och med bestämda intervall, t.ex. vecko-/månads-/kvartalsvis. Detta är en detaljerad information som ledning och driftpersonal, tidigare inte har haft tillgång till och om den används korrekt skall kunna ge konkreta fördelar för hela organisationen.

Denna information kommer att bli mycket mer exakt och mer användbar, speciellt vid policy enforcement, när man lyckas kombinera den med information från Banverkets Active Directory om vem/vilka som använder IP adressen.

När det gäller resultaten, slutsatserna om nätverkets prestanda, kapacitet och den upplevda kvaliteten generellt vara god. Endast ett fåtal användare och protokoll verkar ha mindre kvalitetsproblem.

Användarna verkar dock använda nätet till **betydande del** för icke direkt jobb relaterade uppgifter. Sådant beteende har vissa negativa konsekvenser såsom:

1. Slöseri av nätets resurser, vilket i sin tur kan påverka nätverkets prestanda för yrkesmässig användning och leder i längden till överdimensionering av nätet
2. Potential för att en statlig organisation kan bli utsatta för olaglig/olämplig användning av IT infrastruktur, t.ex. ladda ner olaglig skyddad musik och videomaterial.
3. Skapa möjligheter för virusattacker så många hackare utvecklar angrepp som bygger på sociala nätverk - det faktum att Facebook har de flesta förbindelserna för alla tjänster på nätet visar en potentiell sårbarhet.
4. Osäkerhet kring personalens produktivitet och huruvida användandet av icke direkt jobbrelaterade uppgifter, t.ex. privata bankärenden via företaget, verkligen har en negativ påverkan på den totala produktiviteten.



Det är dock viktigt att inse att det är typiskt för organisationer som inte aktivt övervakar, analyserar användandet av IT infrastrukturen **och** saknar effektiva mekanismer/metoder för att detaljerat och selektivt påverka nätverkstrafiken.

Max 16 har därför **tagit fram och testat olika typer av mekanismer** och regler vars mål är få ner det "sociala" användandet av internet till acceptabla och rättvisa/rimliga nivåer. Dessa regler har testats och validerats på den riktiga avtappade nätrafikentrafiken. Dessa regler/metoder kan tas i drift om Banverket bestämmer vilka "sociala nivåer" ska gälla och vilka mekanismer/åtgärder man planerar att genomföra.

En annan viktig observation är den dagliga användarprofilen och de tre arbetstidsdroppar, som är med största sannolikhet är korrelerat till medarbetarnas aktivitetsnivåer och hur de planerar sin arbetsdag. Statistiken är bara en indikator på vad som kan vara ett betydande problem, särskilt intresse tilldrar sig längden för för- och eftermiddags droppar, cirka en timme var.

Vad dessa droppar beror på, fika eller på planerade möten utan användning av IT plattformen är givetvis svårt att skilja på. Det är med mest troligt att detta är en kombination.

Konsekvenserna för Banverket är en fråga för ledningen, men det är möjligt att inleda debatten genom att upphovet till en rad utmanande frågor:

1. Hur mycket produktiv tid är verkligen gått förlorad på grund av (a) sociala aktiviteter på nätet under arbetstid (b) kultur för långa regelbundna pauser? Har detta uppnått en sådan nivå att ledningen måste agera nu för att åtgärda det?
2. Hur mycket heltidsekvivalent personal och vad är den totala kostnaden av denna förlust av mantimmar?
3. Kan Banverket använda Max16 konceptet inte bara för att aktivt övervaka användningen av nätet men också mildra eller förhindra oönskad användning genom att kontrollera/begränsa tillträdet och att inrätta lämpliga nätverks policy?
4. Har Banverket i praktiken överdimensionerat sitt nät och kan man genom noggrann analys undvika framtida CAPEX-investeringar genom att generera ledig kapacitet genom minska nyttjandet av sociala medier?



5 REKOMMENDATIONER

På grundval av resultaten som beskrivs i tidigare avsnitt i denna rapport, har MAX16 tagit fram ett antal rekommendationer till Banverkets ICTs ledningsgrupp. I samband med överlämning av rapporten till Banverket ICT har rekommendationerna summerats i ett separat exceldokument för att förenkla ev. vidare uppföljning och statusrapportering.

- 1) Banverket ICT bör tydliggöra IT policy för personal och konsulter där det framgår tydligt att all användning övervakas och att metoder och mekanismer finns driftsatta för att upprätthålla gällande IT policy och förhindra eventuellt missbruk
- 2) Banverket ICT bör utforma och driftsätta en **kommersiell tjänst** där man kan tillhandahålla en flexibel kundanpassad (olika organisationer och företag) policy och volyms anpassade användning av Internet, som tar hänsyn till företagets mål och medarbetarnas behov, med säkerhetsmekanismer som förhindrar missbruk och medverkar till en förbättrad uppföljning och ett ökat utrymme för produktivitetssökning.
- 3) Banverket ICT bör utreda om man kan ekonomiskt och resursmässigt kan utforma en **intern drifttjänst** som utnyttjar möjligheten att via MAX16s (Procera/Tapp koncept) i realtid övervaka och påverka nättrafiken oberoende av underliggande infrastruktur. Detta för att garantera existerande tjänsteleveranser samt användas vid konsolidering av nät och infrastruktur, uppföljning av investeringar och vid minskning av kostsamma utredningar vid t.ex. felsituationer.
- 4) Banverket ICT bör säkerställa att information från Banverkets **Active Directory** (AD), angående användar- och gruppstillhörighet för inloggade användare kan överföras till Banverkets analysplattform för nättrafik (PLR7720) för att på ett säkert och kostnadseffektivt sätt kunna analysera trafik och vidta lämpliga åtgärder.
- 5) Banverket ICT bör utvärdera Proceras PSM plattformen för att kunna genomföra detaljerad policy hantering i större omfattning.
- 6) Banverket ICT bör undersöka möjligheten att minska det **cirka 90 %** beroendet av en ISP (Lidero Network) för att minska konsekvenserna t.ex. vid riktade denial-of service attacker. Målet bör vara ha 2 till 3 jämfördelade internetleverantörer.
- 7) Banverket ICT borde undersöka möjligheten med **direkt Peering** till operatörer eller andra administrativa system där trafikmängden är tillräckligt stor eller av andra skäl



t.ex. intern trafik till vv.se. Detta skulle minska det totala behovet av Internet transit samt ökad tillgänglighet och säkerhet.

- 8) Banverket ICT bör undersöka möjligheten att skapa **arbetsfönster** förlagt på tider där användningen av nätet är som lägst (05.00–07.00) samt (20.00–22.00). Detta borde rimligen medföra mindre kostsamt nattarbete och mindre störningar för trafiken.
- 9) Banverket ICT borde införa en **Quality-of-Service** struktur i Gemininätet som tar hänsyn till existerande trafikfördelning. Utgångspunkten borde vara att en 4 klasser borde vara lämpligt för att kunna hantera och erbjuda en kommersiellt gångbar QoS tjänst.
- 10) Banverket ICT bör se över om den stora mängden **RPC2 trafik** måste gå över samma interface som alla annan trafik till och från Internet. Samt införa säkerhetsmekanismer som garanterar tillgänglighet och kvalitet på de resterande 105 protokollen som konkurrerar som samma nätverksresurser.
- 11) Banverket ICT bör tydliggöra vilka **systemägare/nätägare** som använder och ansvarar för de olika IP nät som tillhör Banverkets IP adressrymd. Detta är viktigt för att följa upp och avgöra om den (IP)trafik som transporteras i/över Banverkets ICT infrastruktur är korrekt och uppfyller sitt huvudsakliga syfte.
- 12) Banverket ICT bör återkoppla till **systemägare/nätägare ang** felkonfigureringar, som t.ex. i MobiSIR fallet då deras default NTP konfigurering, felaktigt pekade ut en NTP server i USA istället för Banverkets interna.
- 13) Banverket ICT bör införa "**Key Performance Indikator**" värden för sin IP infrastruktur som följs upp kontinuerligt vars syfte är att på ett mätbart sätt visa hur bra IT infrastrukturen gör sitt jobb sett från olika dimensioner, t.ex. ett värde QoE för alla användare, visar upplevd kvalitet.



6 BILAGOR

Bilaga 1 Excel dokument för uträkning av mantimmar

Bilaga 2 Excel dokument för sammanställning av rekommendationer