TEKNISKA HÖGSKOLAN

HÖGSKOLAN I JÖNKÖPING

UTREDNING AV VPLS I STADSNÄT

Kristoffer Pettersson

Robert Sales

EXAMENSARBETE 2007
DATATEKNIK

TEKNISKA HÖGSKOLAN

HÖGSKOLAN I JÖNKÖPING

UTREDNING AV VPLS I STADSNÄT

INVESTIGATION OF VPLS IN A METROPOLITAN AREA NETWORK

Kristoffer Pettersson

Robert Sales

Detta examensarbete är utfört vid Tekniska Högskolan i Jönköping inom ämnesområdet datateknik. Arbetet är ett led i den treåriga högskoleingenjörsutbildningen och det ettåriga påbyggnadsprogrammet i datanätteknik. Författarna svarar själva för framförda åsikter, slutsatser och resultat.

Handledare: Lars-Olof Petersson

Omfattning: 10 poäng (C-nivå)

Datum: 21 maj 2007

Arkiveringsnummer:

Postadress:	Besöksadress:	Telefon:
Box 1026	Gjuterigatan 5	036-10 10 00 (vx)
551 11 Jönköping		

Abstract

Jönköping Energi AB (JEAB) is a local energy supplier for the county of Jönköping. JEAB also maintain the local Metropolitan Area Network (MAN). They have recently installed GPON in a portion of their network and have connected it to the MAN via an Extreme switch.

However JEAB would prefer to use Cisco equipment instead of Extreme since the MAN comprises of Cisco hardware. They require a solution to connect GPON to the MAN with a recently purchased line card (Cisco 7600 ES20) which can be installed in a Cisco 6500 Catalyst switch. There is also a possible solution with an Alcatel-Lucent 7450 ESS-1 switch. The proposed solution is to use Virtual Private LAN Service (VPLS), though the exact implementation required is unknown. Additionally JEAB have asked for research into GPON and VPLS in order to improve their understanding of both techniques. This would be of benefit to them both now and in the future.

In order to achieve the stated objectives the following questions are raised:

- How does GPON work?
- How does VPLS work?
- How can GPON be connected to the MAN via Cisco Systems 6500 Catalyst switch/7600 Router?
- How can GPON be connected to the MAN via Alcatel-Lucents 7450 ESS-1?

The research into GPON and VPLS provides the required background knowledge in order to investigate how GPON can be connected to the MAN. The main body of the work is to analyse the requirements of the company and build a configuration which satisfies them. The desired implementation via Cisco Systems solution was deemed unsuitable due to a feature of DHCP option 82 which did not function as required. The focus then turned to Alcatel-Lucents solution.

The resulting solution uses a part of VPLS via Alcatel-Lucents 7450 ESS-1. All the key elements are included, including hiding customer VLANs from the ISP and per-service QoS bandwidth management.

The conclusion is that whilst using Alcatel-Lucents solution means a deviation from the all-Cisco implementation that had been planned; the benefit of including all the desired functionality outweighs the mixing of manufacturers.

The techniques of GPON and VPLS are extremely versatile and can be used in a variety of networks. Therefore there is scope for further research into how these two techniques can be used together in other types of MAN.

Sammanfattning

Jönköping Energi AB (JEAB) är en lokal energileverantör i Jönköpingsregionen. JEAB är också ägare av ett lokalt Metropolitan Area Network (MAN). De har nyligen implementerat GPON i deras nätverk och har kopplat ihop det med MANet via en Extreme-switch.

Dock föredrar JEAB att använda Cisco Systems-utrustning istället för Extreme-switchen eftersom stadsnätet består av till största delen hårdvara från Cisco Systems. De behöver en lösning för att koppla GPON till stadsnätet med det nyligen inköpta modulkortet 7600 ES20, vilket kan användas i en Cisco Catalyst 6500-switch. Det finns också en möjlig lösning med en Alcatel-Lucent 7450 ESS-1 switch. Den föreslagna lösningen innefattar att använda Virtual Private LAN Service (VPLS), fastän den exakta installationens konfiguration är okänd. Ytterligare har JEAB bett om information inom GPON och VPLS för att öka deras förståelse av båda dessa tekniker. Detta är av stor nytta för dem både nu och i framtiden.

För att nå de uppsatta målen, ställdes följande frågor:

- Hur fungerar GPON?
- Hur fungerar VPLS?
- Hur kan GPON kopplas ihop med stadsnätet via Cisco Systems 6500/7600?
- Hur kan GPON kopplas ihop med stadsnätet via Alcatel-Lucents ESS-1 7450 switch?

Utredningen inom GPON och VPLS ger en god bakgrundskunskap för att undersöka hur GPON kan kopplas ihop med stadsnätet. Huvuddelen av arbetet är att analysera företagets krav och att hjälpa till att skapa en konfiguration som fyller deras behov. Den önskade implementationen med Cisco Systems-lösningen var tvungen att väljas bort för att den *feature* som hanterar DHCP option 82 inte fungerade som önskat. Istället flyttades fokus mot Alcatel-Lucents produkter.

Den resulterande lösningen använder delar av VPLS genom Alcatel-Lucents ESS-1 7450. Alla viktiga element är inkluderade, inklusive att dölja kundens lokala VLAN från tjänsteleverantören, och *per-service* QoS bandbreddshantering.

Man kan sammanfattningsvis säga att medan Alcatel-Lucent-lösningen är en avvikelse från den annars ”rena” Cisco Systems-miljön i stadsnätet, så uppvägs detta av att all den önskade funktionaliteten finns tillgänglig i den valda implementationen.

Både GPON- och VPLS-tekniken är mycket stora ämnen om man ser till alla de möjligheter som finns, vilket också ger att det finns stort utrymme för vidare utredning i hur dessa tekniker kan kopplas ihop med olika typer av stadsnät.

Nyckelord

Datanätverk, GPON, MAN, Quality-of-Service (QoS), VPLS, VPN

Innehållsförteckning

FIGURFÖRTECKNING

TABELLFÖRTECKNING

1 Inledning

1.1 Bakgrund

Jönköping Energi AB (JEAB) har ett stadsnät (Metropolitan Area Network, MAN), vilket är ett switchat nätverk baserat på hårdvara från Cisco Systems. JEAB har också nyligen implementerat Gigabit Passive Optical Network (GPON). Det senare är uppbyggt på Alcatel-Lucents produkter och är i startfasen. Man har önskemålet att i förlängningen kunna erbjuda bredband, IP-TV och IP-telefoni till kunderna genom GPON-nätverket, detta kallas allmänt för *triple-play*.

Fysiskt sett är stadsnätet och det nya GPON-nätet åtskiljda och det krävs en funktion/kopplingspunkt emellan dem för att få den funktionalitet som önskas. I och med att näten är uppbyggda kring utrustning från Cisco Systems och Alcatel-Lucent, har det hela tiden varit ett önskemål att använda utrustning från dessa företag i denna kopplingspunkt. Till en början önskades endast Cisco Systems produkter, men det såg ut att bli så pass dyrt att det inte ansågs värt att satsa de pengarna i hårdvaran som krävdes. Därför utreddes möjligheten att använda en tredje parts produkter, Extreme, för att sköta kopplingen näten emellan. Detta fungerar delvis, men en ny lösning söks. Enligt uppgift från Cisco Systems ska det vara möjligt genom en alldeles ny hårdvara, ett modulkort för den redan befintliga utrustningen. Samtidigt har också Alcatel-Lucent gett uppgifter om att deras 7450 Ethernet Service Switch – 1 (ESS-1) kan klara av samma funktionalitet.

Vi har getts i uppgift att utreda detta, hur man kan använda den hårdvaran för att sköta kopplingen mellan näten, och också att kunna se hur man kan använda den för ytterligare funktioner för att förbättra nätet. Givet i installationen är att tekniken Virtual Private LAN Service (VPLS) ligger som grund, varför funktion och användningsområden för detta är centralt. För att kunna utföra projektet, ställer vi oss frågorna:

- Hur fungerar GPON?
- Hur fungerar VPLS?
- Hur kan man koppla ihop GPON till JEABs stadsnät, genom Cisco Systems 6500/7600-serien?
- Hur kan man koppla ihop GPON till JEABs stadsnät, genom Alcatel-Lucent 7450 ESS-1?

Tyngdpunkten ligger i att förstå VPLS och att praktiskt kunna implementera detta i en Cisco Systems/Alcatel-Lucent-miljö. Eftersom GPON är en relativt ny teknik krävs också kunskap om hur det fungerar och är uppbyggt, specifikt i JEABs nät.

1.2 Syfte och mål

Huvudmålet med detta arbete är att implementera VPLS på JEABs Cisco-utrustning och samtidigt behålla deras underliggande nätverksstruktur. Cisco Systems 6500/7600-serien eller Alcatel-Lucent 7450 ESS-1 ska vara kopplingspunkten mellan stadsnätet och GPON installationen. Målet är också att utöka JEABs förståelse av VPLS och GPON så att lösningen kan implementeras skarpt och driftas med bra kompetens. För att kunna tillfredställa huvudmålet krävs att vi först lär oss GPON och VPLS från grunden.

Vidare ska strategier tillhandahållas ur både en Quality Of Service (QoS)- och säkerhetssynvinkel. En strategi för att kunna styra olika kunders bredbandshastighet krävs, samt strategier för att kunna förhindra lokal kommunikation mellan olika användare och skydd mot obehöriga användare som utnyttjar systemet.

Syftet med arbetet är att tillhandahålla en förutsättning för vidare implementation av GPON och stadsnätet så att de kan fungera som tänkt i en helhetslösning.

Arbetet som ska utföras innefattar instudering av teori kring GPON och VPLS, och de nyinlärda kunskaperna kan vara nyttiga både för oss och JEAB. Här läggs stor tyngd på den teoretiska delen, men vikt ges också på den praktiska implementationen.

Kravspecifikation finns i bilaga 1.

1.3 Avgränsningar

I och med att tiden är begränsad, måste vissa delar av teknikerna som kunde vara av intresse lämnas utanför detta projekt. Den information och kunskap som kommer användas och bearbetas kommer i stort sett vara det som har beröringspunkt till den praktiska installationen av det nät som Jönköping Energi AB har och planerar att fortsätta bygga ut. Företaget har vid den första installationen/implementeringen gjort vissa val som påverkar hur nätet i fortsättningen behöver byggas, såsom val av teknik, hur fiberdragning gjorts mm. Till stor del begränsas därför arbetet av detta.

Den hårdvara som används för GPON-nätet är från Alcatel-Lucent. Stadsnätet är uppbyggt kring Cisco Systems utrustning. Det finns andra företag med andra lösningar på de problem som finns i nätet i dagsläget, men dessa ges endast som reflektion eller lämnas helt. JEAB har i startläget valt att använda ett modulkort från Cisco Systems till en av deras Catalyst 6513. Men det finns också försök och laborationer med en Alcatel-Lucent 7450 ESS-1 switch.

Om man skulle täcka in alla nivåer från Open Systems Interconnection (OSI)-modellen, lager 1 till 7, finns det mycket att utreda med Gigabit Passive Optical Network (GPON). Projektets omfattning sträcker sig inte så långt, utan t ex OSI lager 1 nämns också mer eller mindre i förbigående. Det är en viktig bakgrund, men utreds inte till en större del. Projektet rör sig framförallt kring OSI lager 2 – 4.

Design av hur fiberdragning etc går till, lämnas också eftersom det skulle kunna utgöra ett helt eget projekt i sig själv om man skulle ge det den tid som skulle krävas.

1.4 Disposition

Denna rapport bygger på Tekniska Högskolan i Jönköpings mall för examensarbete på C-nivå. Det första momentet beskriver bakgrunden till arbetet och de frågeställningar som behöver användas och besvaras för att kunna utföra arbetet. Arbetets syfte och mål fastställs samt avgränsningar, så att arbetets omfattning blir mer hanterbart och målet mer nåbart.

De väsentliga ämnen som ligger till grunden för arbetet beskrivs i Teoretisk bakgrund. Framförallt tas upp teknikerna GPON och VPLS upp, men även en del om hårdvaran som kommer att granskas under arbetet.

Genomförande-delen granskar två olika hårdvarualternativ och jämför det med företagets krav: Cisco Systems 7600 ES20 modulkort och Alcatel-Lucents 7450 Ethernet Service Switch 1 (ESS-1). Här visas olika sätt på vilka man kan lösa de problem som ställts i inledningen.

Den hårdvarulösning som är mest lämplig för företaget presenteras i Resultat-delen tillsammans med konfigurationen av hårdvaran som krävs för att kunna implementera lösningen i produktionsnätet. Resultatet sätts också i relation till den kravspecifikation som arbetet fick i inledningen.

I Slutsats och diskussion tas kritik kring vad som kan förbättras upp, samt möjligheter till vidareutveckling av arbetet. Diskussionen omfattar också hur arbetet kan utnyttjas bortom det produktionsnät som arbetet inriktas mot.

Efter arbetets presentation ges en kortfattad Ordförklaringslista där viktiga begrepp och uttryck förklaras. Detta kan ses som referens under tiden som man läser rapporten om man inte är bekant med dessa begrepp/uttryck.

Till slut redovisas referenser till de böcker, webbsidor etc som använts under arbetet. En sökordlista samt bilagor finns också i slutet av rapporten för att underlätta läsningen och för att klargöra sådan information som inte får plats i rapportens huvuddel.

2 Teoretisk bakgrund

2.1 GPON – teknik och bakgrund

2.1.1 Historisk bakgrund över optisk fiber

Historiskt kan den optiska fiberns ursprung spåras tillbaka till 1800-talet där den Irländska fysikern John Tyndall upptäckte att ljus kunde föras i en kurva inom ett material (vatten) med total intern reflektion.[1] 1952 utförde fysikern Narinder Singh Kapany ett flertal experiment som ledde till skapandet av optisk fiber, baserad på Tyndalls tidigare arbete. 1965 föreslog Charles K. Kao och George A. Hockham från det brittiska företaget Standard Telephones and Cables, att en signalförlust som orsakades av föroreningar kunde tas bort. Om signalförlusten kunde sänkas till mindre än 20 dB per km skulle optisk fiber bli ett praktiskt medium för kommunikation.[2]

Optisk fiber i sin moderna form handlar om överföringen av information med ljus genom långa transparenta fibrer som är gjorda av glas eller plast. En ljuskälla reglerar en Light-Emitting Diode (LED) eller en laser som varierar ”på” eller ”av”, eller varierar i intensitet på ett sätt som representerar den elektriska informationens inkommande signal. En optisk detektor på andra sidan av den optiska kabeln mottager det modulerande (varierande) ljuset och konverterar den till en elektrisk signal som är identiskt i förhållande till originalet.

Det finns två huvudtyper av fiber som kan föra data. *Multi-mode* fiber betyder att flera ljussignaler förs i kabeln samtidigt. *Single-mode* fiber sänder en enda ljussignal längs fibern och denna kräver därmed en mindre tjock kabel.[3]

När internet blev tillgängligt för hemanvändare och företag krävde man mer bandbredd för att kunna få effektiv kommunikation oavsett var i världen man befann sig. Under de sista 15 åren har en vanlig hemanvändares eller ett företags krav på internet ökat och de kräver en snabbare, pålitligare internetanslutning. Därmed blev optisk fiber ett populärt val av medium för tjänsteleverantörer för att kunna tillfredställa denna efterfrågan.

Trots att optisk fiber representerade ett stort steg framåt i det hittills onåbara målet med obegränsad bandbredd, skapades Full Service Access Network (FSAN) våren 1995 för att vidareutveckla detta ännu mer och för att kunna implementera detta till hemanvändare.[4] International Telecommunications Union (ITU) utvecklade FSANs arbete vidare och har nu standardiserat två versioner av PON.

PON är en relativt ny teknik som betyder att fiberkabel kan dras ända ut mot kundens eget nät (Fiber-To-The-Premises, FTTP). Detta görs med en optisk splitter och innebär att man inte behöver någon aktiv nätverksenhet (och därmed ingen ström) mellan en tjänsteleverantör och kunden.

2.1.2 Översikt av GPON

ITU satte den första PON-standarden som kallades för ATM-PON eller APON, och den hade ATM (Asynchronous Transfer Mode) som underliggande teknik. APON utvecklades vidare och en ny standard skapades som fick namnet Broadband-PON eller B-PON. Den nya standarden var snabbare än APON och hade 622 Mbit/s nedströms bandbredd och 155 Mbit/s uppströms bandbreddskapacitet.

IEEE har också utvecklat en egen standard som kallas för IEEE 802.3 Ethernet PON eller EPON och en snabbare variant, Gigabit PON eller GPON. 2006 började även IEEE arbetet på en ytterligare snabbare 10 Gbit/s EPON-standard.

I mars 2003 standardiserade ITU-T en tredje standard, Gigabit-PON eller GPON (ej att förväxla med den GPON som IEEE har skapat). Det är denna standard som används hos Jönköping Energi AB. GPON var ännu snabbare än BPON och erbjöd ökad säkerhet jämfört med tidigare standarder. Standarden landade till slut på följande hastigheter.

- 155 Mbit/s uppström, 1.2 Gbit/s nedström
- 622 Mbit/s uppström, 1.2 Gbit/s nedström
- 1.2 Gbit/s uppström, 1.2 Gbit/s nedström
- 155 Mbit/s uppström, 2.4 Gbit/s nedström
- 622 Mbit/s uppström, 2.4 Gbit/s nedström
- 1.2 Gbit/s uppström, 2.4 Gbit/s nedström
- 2.4 Gbit/s uppström, 2.4 Gbit/s nedström

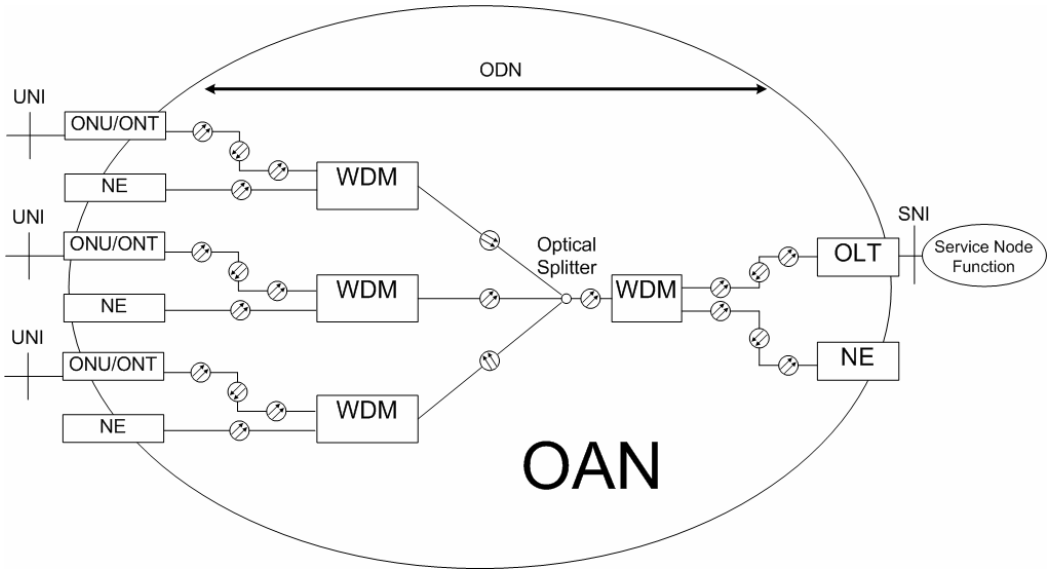
GPON-standarden är uppbyggd av flertalet komponenter. Optical Access Network (OAN) representerar den del av nätverket som ligger inom GPON och sträcker sig från User Network Interface (UNI) till Service Node Interface (SNI). UNI är en logisk gräns som separerar GPON-delen av nätverket (tjänsteleverantörens ansvar) från kundens eget nät. SNI är ett interface som tillhandahåller tillgång till övriga delar av tjänsteleverantörens nät, åt kunden.

En Optical Line Terminal (OLT) är tjänsteleverantörens sida av OAN och kopplas till en Optical Network Unit (ONU) via en eller flera splitters. ONU är kundens interface av OAN. Splittern kan ha en *split-ratio* på upp till 1:128 som max, men i dagsläget är 1:64 den normalt maximala *ration*. En Optical Network Terminal (ONT) är en ONU som används till Fiber-To-The-Home (FTTH). Optical Distribution Network (ODN) definieras som en instans av GPON mellan OLT och ONT.

Wavelength Division Multiplexing (WDM) används för att multiplexa olika våglängder (färger) av laserljus över en enda optisk kabel. Det är detta som möjliggör att stora mängder data kan föras över en fiber.

Man kan också använda flera enheter i nätverket, Network Elements (NEs). Till dessa använder man en annan våglängd än OLT och ONU och multiplexar ihop signalerna. På det viset kan man skicka t ex kabel-TV över ett GPON.

Ett maximalt logiskt avstånd från OLT till ONU har definierats i G.984-standarden till 60 kilometer (km). Däremot finns det en 10 km och 20 km fysisk gräns på avståndet mellan OLT och ONU på grund av begränsningar i det fysiska lagret av GPON.
Figur 2-1 visar en sammanfattning av alla komponenter och tekniker som finns i en typisk GPON-installation. [5]

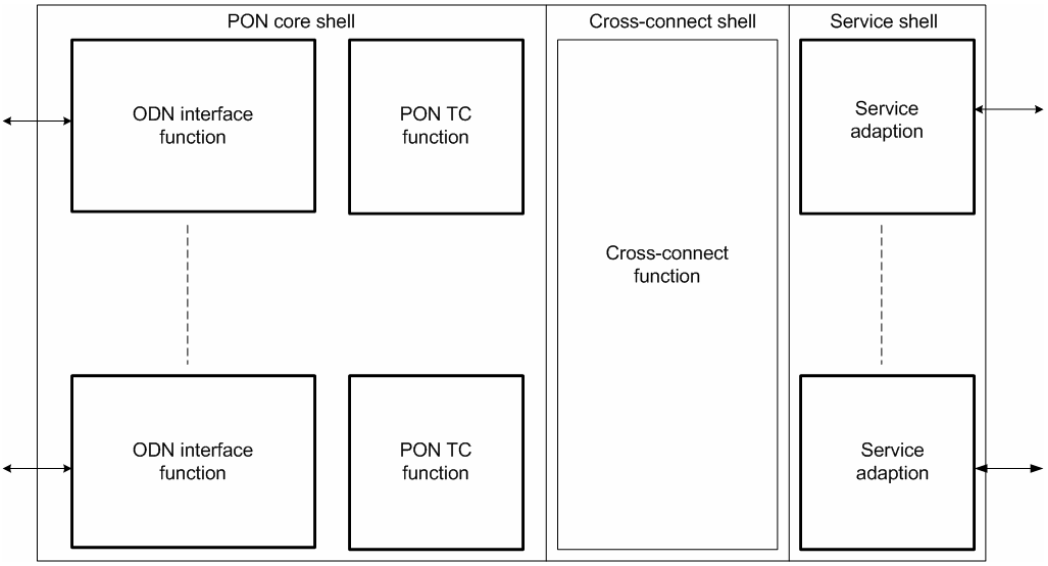


Figur 2-1 En typisk GPON-installation [6]

2.1.3 GPON-funktionaliet

2.1.3.1 OLT/ONU

OLT kopplas till ett switchat nät via standardiserade nätverksinterface. OLT består av tre huvuddelar; Service Port Interface-funktion, Cross-Connect-funktion och ODN-interfacet. Figur 2-2 visar hur de här huvuddelarna kopplas ihop:



Figur 2-2 OLTs logiska struktur och funktioner [7]

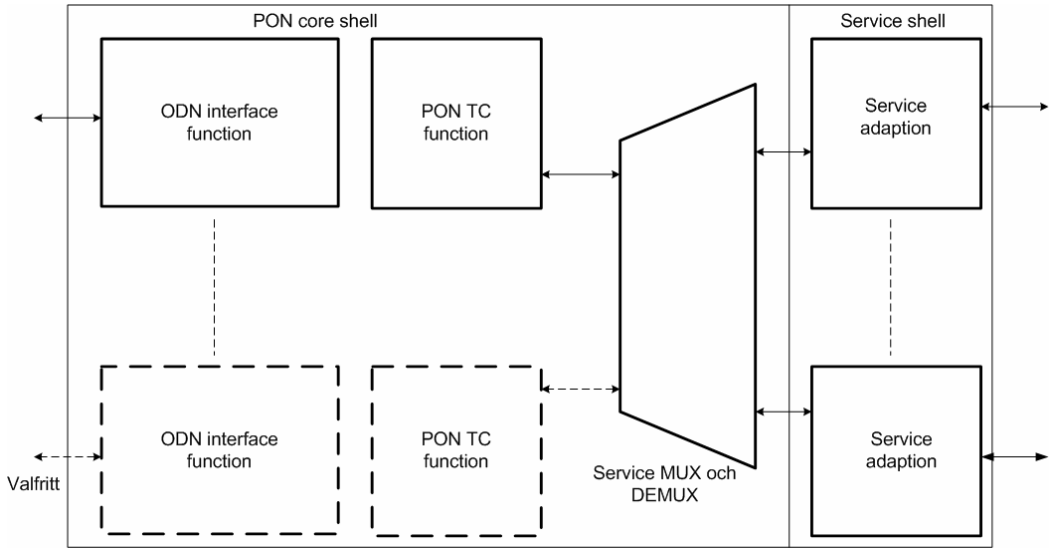
GPONs *core shell* består av två delar; ODN interface function (som är yttre gränsen på ODN) och GPON Transmission Control (GTC) function. GTC functions syfte är följande:

- Hantera ONUs och deras tillgång till den fysiska kabeln
- Hantera bandbreddstilldelning genom Dynamic Bandwidth Allocation (DBA)

Cross-connect shell fungerar som en förbindelse mellan *core shell* och *service shell*. Hur detta sker är beroende på tjänsterna som finns och OLTs interna arkitektur.

Service shell tillhandahåller översättning mellan service interfacen (mot det interna nätverket) och *Cross-connect shell*.

Med hänseende till ODN är ONUs funktionalitet i stort sett likadan som OLT men det behövs endast ett ODN interface (man kan använda två för redundans). Därmed behöver man då inte *cross-connect*-funktionen. Istället har en ONU en multiplex/demultiplex (MUX/DEMUX)-funktion för att multiplexa eller demultiplexa trafiken, beroende på i vilken riktning trafiken ska åt. Se figur 2-3 för en presentation av ONUs funktionsstruktur.



Figur 2-3 ONUs logiska struktur och funktioner [8]

2.1.3.2 Forward Error Correction

För att kunna göra uppströms- och nedströmstrafikflödet effektivt kan både OLT och ONU använda en funktion som kallas för Forward Error Correction (FEC). Den lägger till data i form av en extrabyte (paritetsbyte) till varje paket som skickas. Mottaggaren (OLT för uppströms trafik och ONU för nedströms trafik) kan då upptäcka och korrigera fel som finns i datapaket utan att behöva omsända dessa.

2.1.3.3 Säkerhet

Tekniken bakom GPON ger att all data från OLT till ONUs är broadcast. Detta betyder att någon kan programmera om sin ONU och lyssna på all trafik som skickas ned till alla andra ONUs i det segmentet. Däremot kan en ONU inte sniffa uppströmstrafik från andra ONUs på grund av den fysiska strukturen.

För att skydda sig mot obehöriga valde ITU Advanced Encryption Standard (AES) som kryptoalgoritm. AES konverterar klartext till chiffertext via en algoritm. Algoritmen genererar en 16-bytes krypteringsnyckel vilken används för att skapa chiffertexten från klartext. Processen är omvänd för att kunna få fram klartexten igen.

2.1.3.4 Dynamic Bandwidth Allocation

En ONU kan begära uppströms bandbredd dynamiskt från OLT. OLT levererar bandbredden dynamiskt genom ett av två modes, Status Reporting-DBA (SR-DBA) och Non-Status Reporting-DBA (NSR-DBA).

Alla OLTs måste enligt standarden stödja båda typer av rapporteringsmetoder så att alla ONUs får DBA-funktionalitet.

SR-DBA kräver att ONU sänder den relevanta informationen om OLT ber om det. När en ONU skickar en rapport till OLT, kan OLT bestämma sig för att antingen använda rapporten och modifiera bandbreddsallokeringen, eller att avstå från att göra detsamma.

NSR-DBA är då OLT kan ta reda på varje ONTs trafikflöde genom att själv bevaka det inkommande trafikflödet. Med andra ord, OLT skapar sin egen rapport och sedan avstår från eller använder rapporten enligt beslutsfattande som görs med SR-DBA. [9]

2.1.4 Fysisk och Logisk Struktur

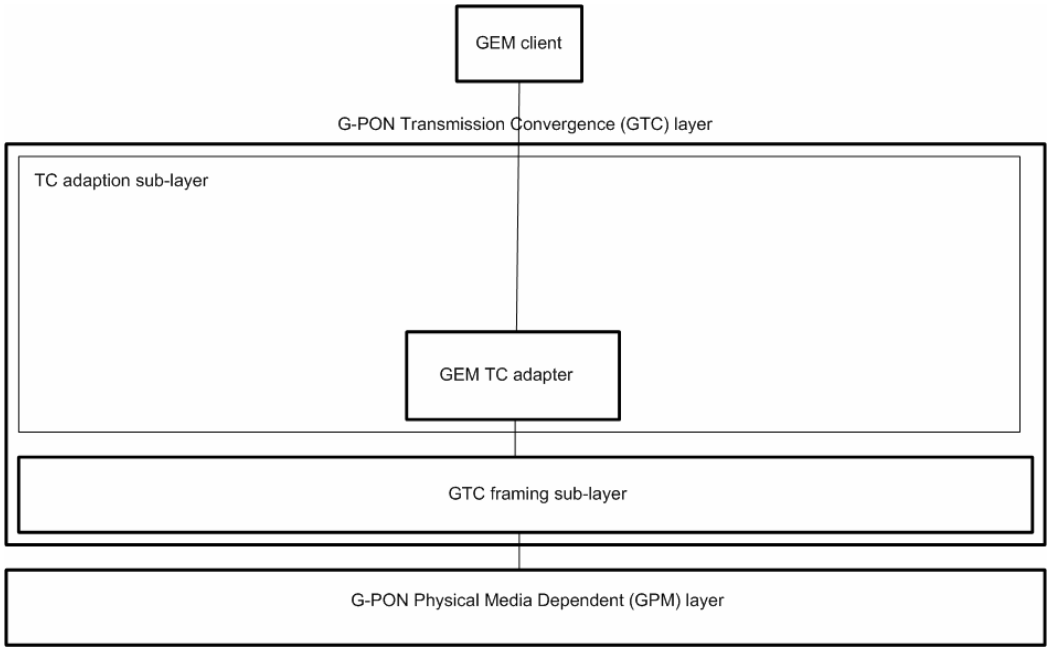
2.1.4.1 Fysiska lagret

Physical Media Dependent (PMD)-lagret motsvarar i stort sett Open Systems Interconnection (OSI) lager 1, alltså det fysiska lagret som representerar data som förs längs kablarna. GPON använder sig av Non-Return-to-Zero (NRZ) kodning som fastställer ett definitivt sätt att representera ettor och nollor (binärt). Med andra ord, det ska inte finnas någonting annat än ettor och nollor.

I praktiken representeras ettor och nollor med en hög nivå respektive låg nivå av ljus. Våglängder på ett singelfiber (simplex)-system har satts till 1480 nanometer (nm) - 1500 nm och på två-fiber-system (duplex) till 1260 nm -1360 nm (nedströmstrafik). Uppströmstrafik ska ha en våglängd av 1260 - 1360 nm. Standarden har också specificerat en maximal tolerans på 1 dB signalförlust. Signalförluster kan bero på flera saker som t ex dispersion (oönskad spridning av ljussignal i fibern).

2.1.4.2 Logiska lagret

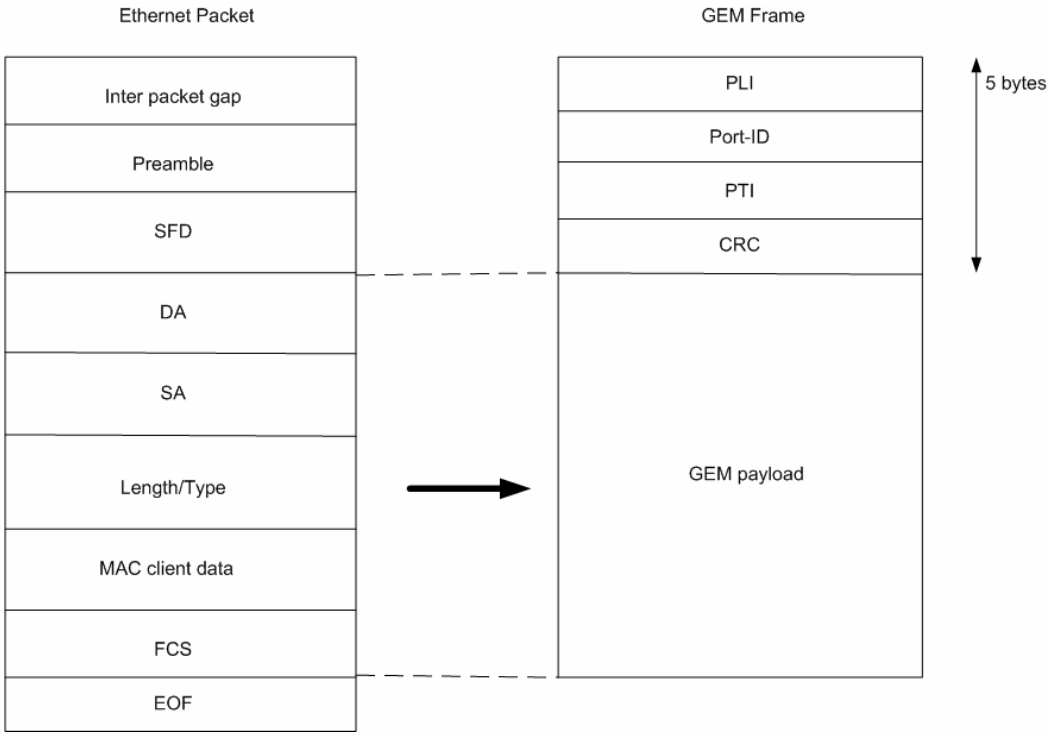
Ovanför PMD finns ett annat lager, GPON Transmission Convergence (GTC). GTC-lagret består av ett *Framing sub-layer* som ser till att all data i framen är uppdelad i lämplig längd och en TC adaption sub-layer som filtrerar trafik som mottages från GEM-klienter via OLTs eller ONTs port-ID. Figur 2-4 visar en förenklad presentation av GTC-lagret.



Figur 2-4 Protokoll-stack för GTC-systemet [10]

Uppströms- och nedströmsframe har en *timeslot* (d v s hur snabbt varje frame sänds) på 125µs för både 1,2 Gbit/s och 2,4 Gbit/s. Därför är framelängden 19440 bytes i 1,2 Gbit/s-systemet och 38880 bytes för 2,4 Gbit/s-systemet.

Figur 2-5 visar hur ett Ethernet-frame är konverterat till ett GEM-frame för överföring över GPON. Data kan uppdelas över flera frame genom att identifiera om vissa fragment är sista delen av framet eller inte, och om stockning i trafikflödet sker.



Figur 2-5 Ethernet-till-GEM frame mappning [11]

Ethernetframe

Inter packet gap – Varje enhet som ska sända trafik måste vänta 9,6 ms före varje paket kan skickas enligt IEEE 802.3

Preamble – Digital kodning som identifierar början av varje paket

SFD – Start Frame Delimiter som markerar slutet av Preamble

DA – Destination MAC adress

SA – Source MAC adress

Length/Type – Length och Type av Ethernetpaketet

MAC client data – Datat som ska föras i paketet

FCS – Frame Check Sequence som möjliggör kontrollering av att paketet inte har ändrats under transporten

EOF – End of Frame markerar att framet är slut här

GEM-frame

PLI – Payload Length Indicator – Längden av GEM-datat

Port-ID – Port-ID av OLT/ONU där Ethernetpaket mottages

PTI – Payload Type Indicator – Identifierar typen av GEM-datat

CRC – Cyclic Redundancy Check, motsvarighet till FCS

GEM payload – Består av Ethernetpaketet som ska transporteras över GPON

Detta sker både i ONT på kundens sida och i OLT på leverantörens sida. Tvärtom sker när paketen ska föras vidare till kundens eller leverantörens Ethernet-baserade nät.[12]

2.2 VPLS

2.2.1 Översikt och begrepp

Virtual Private LAN Service (VPLS) är en teknik för att emulera ett lokalt nätverk (LAN, Local Area Network) över geografiskt skilda platser. I dagsläget är VPLS-tekniken ”Proposed Standard” och alltså inte ”full standard”, men den väntas bli det inom nära framtid. VPLS är en Virtual Private Network (VPN)–teknik av variant multipoint, i motsats till point-to-point. VPN innebär att man skapar ett lokalt nätverk, fast över ett större område och över ett i sig själv osäkert nätverk som t ex internet. Multipoint är motsats till point-to-point och innebär att det finns flera enheter i varje ända av kopplingen.

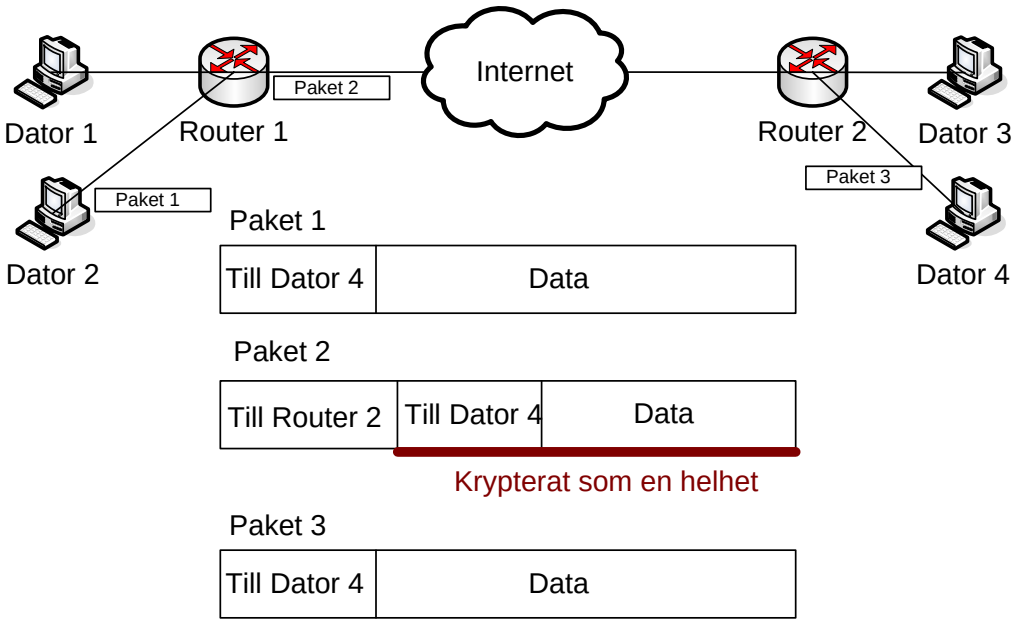
Syftet är att över ett osäkert eller delat nätverk kunna skapa ett avskilt lokalt Ethernet-nätverk. Målet är att alla de funktioner som finns hos VPLS-nätverket, ska likna det som ett genuint och ”vanligt” Ethernet-nätverk har, vad gäller inlärning av MAC-adresser, *flooding* av MAC-adresser vid okänd destination etc.

Tjänsteleverantören (Service Provider, SP) har ett antal punkter som de bygger upp nätverket på. Dessa punkter kallas för Provider Edge (PE, ~ leverantörspunkter) och är sammanbundna genom emulerade logiska länkar vid namn PseudoWires (PWs). De PE som finns inom domänen utgör tillsammans det emulerade nätet. En kund kan bli inkopplad och få tillgång till ett lager 2-nät genom kundsidan av nätverket som heter Customer Edge (CE).

För att förstå vad som händer i ett VPLS och nätverk över huvud taget finns det vissa begrepp som är viktiga att förstå. Två av dessa är inkapsling (*encapsulation*) och tunnling (*tunneling*). Inkapsling refererar till det som händer när data (information) paketeras och markeras med avsändar- och mottagarinformation. Exempelvis när man skickar ett e-post och har ett brev man vill skicka, så har denna information (data) en avsändare och mottagare. För att kunna transporteras över internet, måste datat passera många routrar och flera servrar. Datat ”inkapslas” därför med ytterligare information om IP-adress till mottagarens server, portinformation för paketet etc. Detta sker i det fallet lokalt på datorn och inkapslingen sker i olika ”lager” eller ”nivåer” som definieras i t ex Open Systems Interconnection (OSI)-modellen där varje lager lägger till lite ytterligare information till datat i form av *headers*, *footers* checksummor mm.

Allt detta sker helt enkelt för att ha ordning på att datat kommer fram säkert, på rätt sätt och i den ordning som man vill ha. Vid detta skeende delas också stora mängder data in i mindre delar innan det skickas.
När sedan datat med dess inkapsling kommer fram till mottagaren görs samma sak igen, fast tvärtom. Varje *header, footer* och checksummor mm, ”kläs av” för att till slut bara lämna datat kvar. Detta kallas *de-encapsulation* och sker alltså hos mottagaren.

Tunnling (*tunneling*) bygger på att man lägger ytterligare en nivå av IP-information till paketet som ska skickas. Detta sker genom inkapsling och kryptering där hela det ”riktiga” paketet med data, IP-adressinformation mm krypteras och inkapslas. Figur 2-6 ger ett exempel:



Figur 2-6 Tunnling, allmän teknik

Användaren med Dator 2 vill skicka ett paket till Dator 4, för enkelhetsskull kan vi säga ett ping-paket. Figur 2-6 är medvetet mycket förenklad för att göra presentationen mera tydlig. Användaren skickar ett ping till Dator 4. I bilden är detta Paket 1 med information om IP-adress som Dator 2 har, IP-adress till Dator 4 och annan information. Genom inkapsling passerar paketet nedåt i OSI-lagren lokalt på Dator 2, och skickas sedan till närmaste router, Router 1. Router 1 skapar sedan en tunnel mellan sig och Router 2. Därför inkapslas Paket 1 ytterligare en gång för att passera över internet till Router 2 som är slutet på tunneln. Hela det inkapslade Paket 1 är här också krypterat. Router 2 avslutar tunneln och de-krypterar samt ”klär av” Paket 2s extra inkapsling. Paket 3 ser alltså ut exakt på samma sätt som det första, Paket 1, gör. Det sista som händer i denna kedja är att Paket 3 levereras till Dator 4 som kan hantera den data som blev mottagen efter att de *headers*, *footers* etc har klätts av. [13]

När man bygger ett VPLS, finns det två tekniker och protokoll för att koppla upp det hela, VPLS-BGP och VPLS-LDP. BGP står för Border Gateway Protocol och är en variant av routingprotokollet med samma namn. Det andra protokollet är Label Distribution Protocol (LDP), och båda dessa används för att upprätta länkar inom ett VPLS, men har helt olika sätt att hantera det på. De är inte heller kompatibla med varandra. Både Cisco Systems och Alcatel-Lucent förespråkar VPLS-LDP, varför VPLS-BGP kommer att lämnas åt sidan och endast nämnas mycket kort. [14] [15]

2.2.2 LDP och MPLS

Som nämnts ovan finns det två sätt att hantera signalering och sessioner inom VPLS, genom VPLS-BGP eller VPLS-LDP. De får inte blandas ihop eftersom de inte är kompatibla med varandra. Och eftersom LDP används vid Cisco Systems och Alcatel-Lucents implementation, finns det anledning att ha grundläggande förståelse för LDP, som från början skapades för tekniken MultiProtocol Label Switching (MPLS). Detta tillsammans ger att även grundläggande insikt i MPLS är av nytta.

När grunden för MPLS lades, kallades tekniken för *Tag Switching* och var ett proprietärt protokoll från Cisco Systems. MPLS uppkom för att snabba upp routingbeslut i ett nätverksbackbone. Det är en transportteknik som man kan använda flera andra protokoll över, fast det är Internet Protocol (IP) som är det mest nämnda och använda.

Det första ett paket stöter på när det ska skickas över MPLS-nätet är *ingress router*. Denna router lägger till en label, etikett, till paketet. Denna etikett används för att ta de nödvändiga routingbeslut som krävs. Efter att paketet fått denna nya etikett och gjorts redo för att transporteras i MPLS-nätet, skickas det vidare genom nätverket. Alla routrar i MPLS-molnet har möjlighet att ta bort, lägga till eller ändra etiketter. Det vanligaste är det sistnämnda, *swapping*, att en etikett läses och ändras innan det skickas vidare.

MPLS-nätet ger snabba routingbeslut eftersom endast den översta etiketten läses av varje enhet som hanterar paketet. MPLS kombinerar information från olika lager i OSI-modellen när den väljer hur paket ska hanteras. Den kan använda t ex typ av tjänst eller IP-information för att välja hur och var paketet ska vidarebefordras. I ett klassiskt routat IP-nät används normalt bara IP-adressinformation när beslut tas, och varje paket inspekteras individuellt och inte som en ström eller ett flöde.
MPLS-paketet lämnar MPLS-nätet genom *egress router*n, och paketet återställs till sin ursprungliga form som det var innan det kom till *ingress router*n. [16] [17]

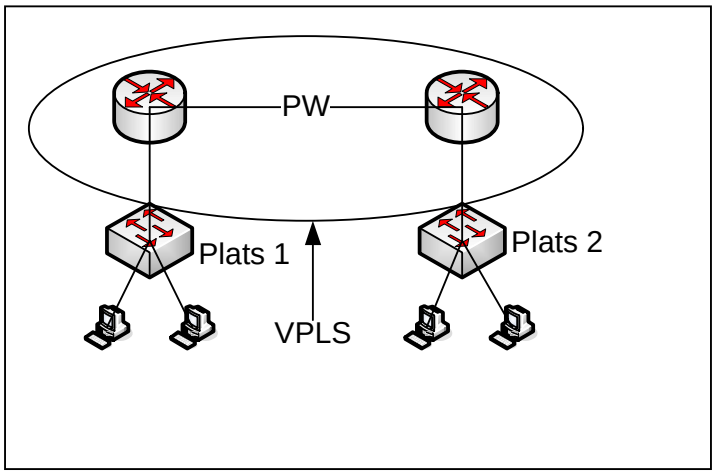
LDPs roll i detta är signalering mellan routrarna och hantering av sessioner mellan desamma. Det byggs upp relationer mellan routrarna för att hantera mappning av etiketter inom MPLS-nätet och en router kan t ex begära att få reda på en annan routers mappning av etiketter. För att hantera dessa sessioner använder LDP Transmission Control Protocol (TCP) och User Datagram Protocol (UDP). På samma sätt som med vanliga routingprotokoll skickas det ”hello-meddellanden” med en viss tidsintervall mellan de enheter som är direkt anslutna till varandra. Annan information som utbyts mellan LDP-routrarna är information om t ex hur en mappning ser ut för en specifik router, eller signalering om att en router inte ska finnas med i kontakten längre etc. Detta liknar i mycket ett vanligt routingprotokolls informationsutbyte. [18] [19]

2.2.3 PseudoWires (PWs) och VPLS

För VPLS och även andra tekniker och protokoll, används så kallade PseudoWires (PWs), vilket är en emulerad länk av exempelvis Ethernet mellan två punkter i ett IP-nät. Det innebär att man upprättar en logisk länk över t ex internet eller ett stadsnät med hjälp av protokoll som Layer 2 Tunneling Protocol (L2TP) eller IP Security (IPSec) för att få denna länk att verka precis som om det vore en fysisk Ethernetlänk.

I praktiken är det en tunnel som upprättas mellan de båda punkterna och sedan emuleras en Ethernet-förbindelse däremellan. Här finns det flera protokoll att använda för tunnlingen, några alternativ är MultiProtocol Label Switching (MPLS), L2TP och IPSec.

I figur 2-7 visas ett exempel där två routrar som genom IPSec upprättar en förbindelse för att sedan genom VPLS-teknik skapa ett virtuellt lokalt nätverk mellan Plats 1 och Plats 2. Alla enheter på Plats 1 och Plats 2 kan sedan ingå i samma broadcastdomän och dela t ex samma IP-nät. Det finns heller ingen begränsning i fysiskt avstånd mellan Plats 1 och Plats 2. Det är fullt möjligt att Plats 1 är ett LAN i San Jose, USA och Plats 2 är ett LAN i Bromölla, Sverige.



Figur 2-7 PseudoWire som används i ett VPLS

Ett VPLS-nätverk är uppbyggt som ”full mesh”, vilket innebär att alla noder i nätverket är fysiskt kopplade till alla andra noder. Det klargörs i specifikationen för tekniken (RFC4762) att om man väljer att inte följa det spåret, måste man ha en teknik för att inte få loopar inom nätet. Man kan då använda någon Spanning Tree-funktion.
Nackdelen med att använda ett full mesh-nätverk är uppenbar när det är många noder inkopplade, att det krävs många länkar eftersom alla enheter måste ha en förbindelse till varje annan enhet.

Man har emellertid kommit förbi problemet med kravet på full mesh, Hierarkisk VPLS (H-VPLS). Genom denna skapas *Spoke-PW*, och bygger på ytterligare lager av tunnling. För vidare information om det, läs vidare H-VPLS nedan.
[20]

2.2.4 Discovery / autodiscovery

För att det VPLS-nätverk som byggs upp ska fungera både smidigt och säkert, krävs det kunskap inom flera områden. Ett av dessa som behöver beaktas är hur man vill att enheterna i nätet ska identifieras.

Man kan välja att manuellt konfigurera alla enheter med identifikation om alla närliggande PEs och hur de är kopplade. Detta är naturligtvis ganska tungrott i längden när mer än två enheter är inkopplade. Det krävs då mycket tid till manuell konfiguration och misstagen från den som sätter upp nätet kan få stora konsekvenser. Det är dock det säkraste alternativet av de som finns tillgängliga, om det görs noggrant.

Man kan istället sköta detta helt automatiskt, och det kallas då för *autodiscovery*. VPLS-BGP förutsätter att en variant av Border Gateway Protocol version 4 (BGP) används för detta. Men i VPLS-LDP finns ingen sådan definition, utan det sägs endast att detta är upp till varje leverantör och installatör att avgöra hur det ska ske. Det enda som ges som krav är att det ska vara *möjligt* att sätta upp länkarna manuellt.

Av de idag ”aktiva” eller möjliga alternativ som används finns BGP, LDP, DNS (Dynamic Name Service) och RADIUS (Remote Authentication Dial In User Service). Alla dessa har olika sätt att identifiera och sprida information om länkarna i nätverket. De har alla också olika positiva och negativa sidor, varför en variant inte nödvändigtvis passar så bra i en implementation, medan den kan vara mycket lämplig i en annan. Så det är upp till varje leverantör att välja en eller flera varianter för just en viss produkt eller installation. Detta utreds inte närmare, utan ges endast som en reflektion eftersom leverantören gör det valet och specifikationen inte ger en färdig lösning. [21]

2.2.5 Säkerhet inom VPLS

Som namnet säger så ska det virtuella nät som byggs upp mellan kundnoderna vara *private* (=privat). Det betyder att vad som sker mellan dessa noder inte ska kunna läcka ut utanför detta nät, inte förändras eller avlyssnas etc. VPLS-nätet byggs upp dels av en kontrollplan-del och en dataplan-del. Datadelen är själva informationen som skickas och tas emot, medan kontrolldelen är den del som hanterar hur sessioner sätts upp, *hur* data överförs etc.

Några typiska hot som finns mot ett VPLS är:

- Sniffing, innebär att någon obehörig kan titta på och analysera vad som sker på kundens nätverk, eller en del av det. En obehörig kan även ha viss ”nytta” av att se krypterad information i form av vilka typer av paket som skickas, hur stora paketen är osv.

- Förändring av paket under tiden de förs över nätverket. En form av man-in-the-middle-attack. En obehörig person eller resurs sätter sig emellan två punkter utan att de märker det. Dessa ”punkter” i nätverket skickar därför information i tron att de har direkt förbindelse med mottagaren, men den obehöriga personen kan förändra paket och frames som de skickar till varandra.

- Spoofing av data. Det innebär att ytterligare data läggs till till den ström som skickas över nätverket. Detta liknar i stora delar punkten ovan, men med skillnaden att data endast läggs till, inte förändras eller nödvändigtvis sniffas/analyseras.

- Denial-of-Service-attacker (DoS-attacker). Det innebär att en tjänst eller del av ett nätverk sätts ur spel på olika sätt. Det kan göras genom att man överbelastar en tjänst så att det inte finns någon tid eller kapacitet kvar för de behöriga användarna till tjänsten, eller genom att modifiera konfigurationen på en enhet så att nätverket genom det blir överbelastat. Det kan också innebära att en länk blir överbelastad med trafik så att det inte finns tid till att svara på behörig trafiks förfrågningar.
  En variant av DoS-attacker är när routingprotokoll eller säkerhetsprotokoll angrips på samma sätt som ovan. På det sättet kan kunden tappa sin förbindelse eftersom inte kontrollplanstrafiken kommer fram som den ska över nätverket.

- *Cross-connect*. Det kan handla om både logisk och fysisk *cross-connect*. Fysisk kan det bero på att någon (behörig eller obehörig) kopplar en kabel fel. En logisk felkoppling är när det skapas en felkonfiguration från en administratör eller obehörig användare. Detta kan ge att två VPNs kan kopplas ihop felaktigt och få kontakt med varandra fast det inte alls var tanken från början. Vissa menar att *cross-connect* är en av de största säkerhetsaspekterna inom Virtual Private Network (VPN)-tjänster som erbjuds bland tjänsteleverantörer. [22]

Det finns flera sätt att skydda sig mot de här hoten. Vissa hot kan vara olika stora beroende på var installationen finns och beroende på vilken information som skickas etc. Ett grundläggande sätt att skydda sig mot DoS-attacker är att sätta en begränsning i antalet MAC-adresser som tillåts för inlärning av switcharna på varje nod (eller *site*). Detta rekommenderar specifikationen (RFC 4762) starkt att man gör. Den rekommenderar också att man har någon form av autentisering och kryptering, det vill säga att det finns någon mekanism för att kontrollera de enheter som finns inkopplade i nätverket, och att de som inte kontrolleras stoppas direkt samt att den information som skickas över länkarna och inom VPLS-nätet är krypterad. T ex så är LDP-meddellandena i VPLS i klartext, alltså öppet för vem som helst som har tillgång till nätverket att läsa. Men om man använder kryptering måste den ju naturligtvis knäckas först, innan den obehöriga användaren kan förstå vad som sägs. [23]

2.2.6 802.1Q

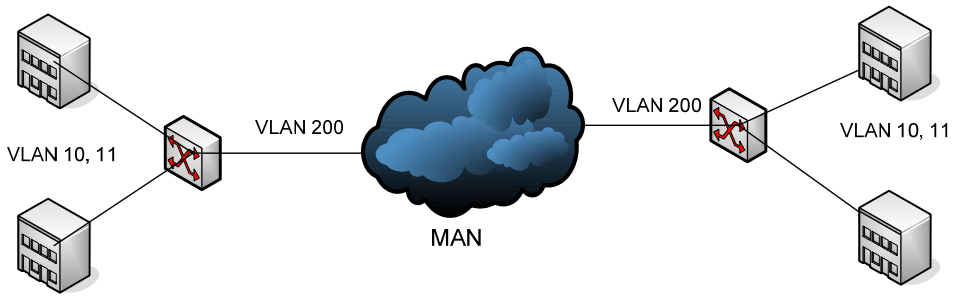
Virtual Local Area Network (VLAN) är en teknik för att gruppera olika användare efter ett sätt som nätverksbyggarna bestämmer sig för att följa. Denna gruppering kan bygga på geografisk placering av användare, eller funktion man har på företaget mm. Det fungerar på samma sätt som att de som är i samma VLAN sitter i samma switch och delar broadcast-domän, fast de egentligen kan vara utspridda i nätverket på olika ställen. Man kan på detta sätt gruppera användargrupper och tilldela grupperna t ex olika tillgång och bandbredd till internet eller vissa interna resurser. 802.1q är en standard som definierar vad ett VLAN är och hur sådana frames ska se ut och hanteras. Det är också en standard för att sända flera VLAN över en fysisk länk. Det sistnämnda sker genom att man *trunkar*, buntar ihop, ett antal VLAN över samma fysiska länk, trots att dessa är logiskt åtskiljda och alltså inte har någon nätverkskontakt på den nivån.

I avsnittet om q-in-q ges en illustration och förklaring i detalj av hur sådana frame ser ut. Kortfattat kan det sägas att man lägger till en *tag* där man dels anger att det är ett 802.1q-frame och dels vilken VLAN-tillhörighet detta har.

Det skulle kunna vara möjligt för den som vill och kan, att sniffa trafiken som passerar vid en viss punkt i nätverket och få tag på data som passerar. För att skydda sig mot sådana attacker eller intrång väljer man därför oftast att inte sprida alla VLAN på alla trunklänkar, utan endast till de platser som verkligen behöver dessa.

2.2.7 Q-in-Q

Q-in-q går under flera namn (bland annat 802.1q-in-q samt VLAN-Stacking) och är ett relativt sent daterat tillägg till 802.1q. IEEE har definierat den som 802.1ad och tekniken förklarar hur man kan tunnla en trunk (namnet kan förstås som ”802.1q-inuti-802.1q”), och har stor betydelse i VPLS-nätverk när de byggs hierarkiskt (mer info om det nedan).



Figur 2-8 Exempel på implementation av q-in-q

I figur 2-8 ovan visas en del av ett MAN (Metropolitan Area Network) vilket hanterar flera VLAN, fastän endast ett visas här, VLAN 200. Från den tjänsteleverantör som äger MANet, används endast detta VLAN när frames ska vidarebefordras. Kunden som har tjänsten använder sig av två egna *lokala* VLAN, nämligen VLAN 10 och 11. I exemplet ovan visas en kund, säg Kund 1. Kund 1 har blivit tilldelad VLAN 200 i *backbone* av MANet. Internt vill kunden dela upp sitt VLAN i två delar, t ex för att minska broadcast-trafik. VLAN 200 innehåller alltså två lokala VLAN, VLAN 10 och VLAN 11. Observera att flera kunder kan ha samma nummer på deras lokala VLAN utan att det uppstår några problem i nätverket, eftersom dessa är uppdelade i olika nivåer. I fallet ovan kan det alltså finnas VLAN 200, 201, 2004, 3789 etc, men alla kan använda ett lokalt VLAN 10. På det här sättet skapas flera nivåer, hierarkier, i lager 2-nätverket. De kunder som finns i det lokala VLANet 10 delar alltså inte broadcastdomän med de i VLAN 11, fast båda dessa switchas som VLAN 200 hos tjänsteleverantören.

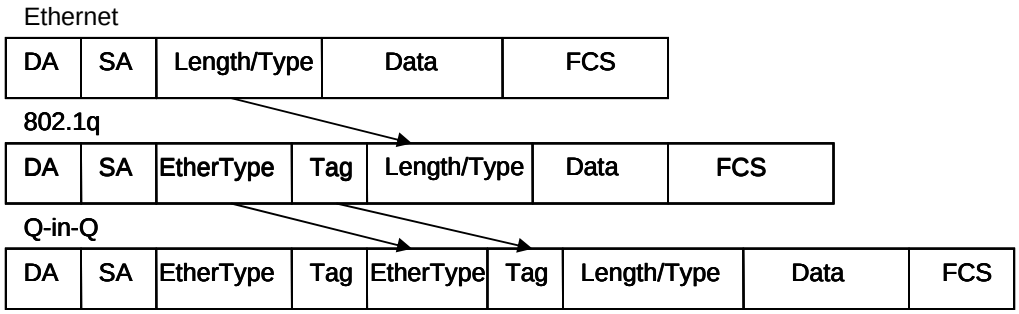
Ethernet-frame följer naturligtvis en standard, IEEE 802.3, och har därmed en viss struktur. Framen är uppdelade där varje del består av ett visst antal *bitar*. Den totala maximala längden för ett standard-Ethernetframe är 1518 bytes, där 1 byte = 8 bitar => 12144 bitar. Den första delen av ett frame är Destination Address som är 48 bitar långt och innehåller MAC-adressen av mottagaren. Eftersom alla enheter följer samma standard vet mottagaren var gränserna går mellan de olika fälten och behöver alltså inte tveka gällande detta. Allt som allt ser framet ut som följande (i fysisk ordning):

- Destination Address (DA), 6 bytes (= 48 bitar)
- Source Address (SA), 6 bytes (= 48 bitar)
- Length/Ethertype, 2 bytes (= 16 bitar)
- Data, 46 – 1500 bytes (= 368 – 12000 bitar)
- Frame Check Sequence (FCS), 4 bytes (= 32 bitar)

Data är själva informationen man vill skicka och ta emot. Det finns en minimigräns på 46 bytes, vilket måste användas. Om man vill skicka ett ”tomt” frame, måste man fylla ut detta fält med minst 46 bytes, annars tolkar mottagaren det som ett korrupt frame och kommer att *droppa* framet.

Den maximala storleken på ett frame (eller paket, *cell* etc) brukar betecknas med Maximum Transmission Unit (MTU). I fallet Ethernet är detta alltså 1518 bytes. Frame som är större än MTU har olika namn som ”jumbo frame” eller ”baby giant”. Hur dessa hanteras är upp till utrustningen som används och den konfiguration som för tillfället körs. Detta måste man se upp med eftersom standard-hanteringen vid för små eller för stora frames är att de *droppas*, slängs, utan att ens undersökas vidare. T ex när q-in-q används, krävs att man aktiverar stöd för större frames än standard eftersom man vill kunna utnyttja större frames för att bära VLAN-information.

Inkapsling vid 802.1q och 802.1ad (q-in-q) illustreras i figur 2-9:



Figur 2-9 Ethernetframe, 802.1q-frame och q-in-q-frame

Överst visas ett standard Ethernet-frame. När den första VLAN-inkapslingen sedan sker, läggs efter Source Address två fält till; EtherType och *tag*-information. Dessa fält har information om att det är ett 802.1q-frame, och vilket VLAN framet tillhör. Detta är steg 1.

Vid nästa steg, q-in-q, läggs ytterligare en uppsättning av dessa fält till. Det läggs direkt efter Source Address och ger information om att det är ett q-in-q-frame, och information om vilket ”yttre” VLAN-ID som framet tillhör. Som förklarat ovan, skapas här en hierarki, olika nivåer av VLAN-ID. Det är hela tiden den yttre som läses och används när frame vidarebefordras, varför här den inre taggen kan vara samma fastän de inte ska switchas till samma kund.

Ett q-in-q-frame ”kläs sedan av” *tag* för *tag*. Den yttre först, och sedan den inre. Efter att den yttre taggningen har tagits bort från framet, skickas det sedan vidare, då med den inre taggningen som enda och yttersta *tag*. Det sista som händer ur detta hänseende är att även denna *tag* tas bort innan framet kommer fram till sin slutgiltiga destination.

Om ett ”native VLAN” (otaggat frame) kommer in i tunneln, behandlas den som ett av de andra framen, det ges en EtherType- och *tag*information innan det skickas vidare in i nätverket. Vilka värden som där ges bestäms vid konfiguration av switchen. [24] [25]

2.2.8 Hierarkisk VPLS-uppbyggnad

Om man bygger ett stort VPLS-nät, blir det mycket kapacitet som går åt till signalering och LDP-protokollet. Det krävs också ett stort antal fysiska förbindelser eftersom man bygger nätet i full mesh, som standarden kräver. Det finns dock sätt att hantera detta problem på. Man kan använda sig av en hierarkisk VPLS-uppbyggnad. Det åstadkoms t ex genom q-in-q.

Så som beskrivits ovan, skapas det automatiskt en hierarki med q-in-q. Detta kan utnyttjas när man skapar VPLS, eller snarare H-VPLS. Det skapas då en eller flera ”kopplings-punkter” med funktionen att dela upp trafiken åt rätt håll. Dessa enheter kallas för *Multi-Tenant-Unit* (MTU), och de PWs som är kopplade till dessa kallas för *spoke-PW* (spoke betyder ungefär eker som används på t ex cykelhjul. Jämför analogi.). Detta fungerar liknande som en tunnling vilket beskrivits ovan, och kan användas effektivt för att minska antalet förbindelser i nätverket samt för att minska den övergripande belastningen som det innebär för de enheter som ingår i det annars helt plana VPLS-nätet.

När man skapar ett ”plant” VPLS finns det ett skydd mot att broadcast-loopar skapas genom mekanismen *Split Horizon*. Det innebär helt kort att ett frame inte skickas ut på samma port som det kom ifrån. I ett klassiskt VPLS räcker detta som skydd på grund av att man bygger nätet genom full mesh. Men när man bygger hierarkiskt som i H-VPLS krävs det ytterligare mekanismer för att hindra sådana loopar. Detta kan vara ett problem och IEEE-standarden ger inga färdiga svar på hur det ska hanteras, varför det är upp till varje tillverkare att skapa egna varianter för att lösa detta. Alcatel-Lucent t ex, har löst detta genom sin egna implementation och variant av *Spanning Tree*, VPLS-RSTP (VPLS-Rapid Spanning Tree Protocol). Det är utanför denna rapport att ta upp exakt hur Spanning Tree fungerar och hur Alcatel-Lucents variant och modifiering av denna fungerar, utan det lämnas vid att det är ett sätt att undvika lager 2-loopar i ett H-VPLS-nät (se kortfattad förklaring av Spanning Tree i Ordlistan, i slutet av rapporten). Eftersom det finns flera sätt att hantera detta på kan det också nämnas att Cisco Systems också har ett ytterligare sätt för att lösa detta problem på.

[26] [27]

2.3 Quality of Service

Quality of Service (QoS) är den process i ett nätverk där man konfigurerar enheterna så att vissa typer av trafik får en bättre service än andra. Detta gör man genom att definiera policys som sedan appliceras på fysiska eller logiska interface. Vissa typer av trafik som t ex IP-telefoni kräver högre tillförlitlighet än exempelvis när man skickar filer mellan datorer med File Transfer Protocol (FTP). QoS kan användas så att VoIP och annan fördröjningskänslig trafik får en högre prioritet i nätverket.

När trafik kommer in till ett nätverk kan det ha en viss prioritetsnivå. Vissa enheter (exempelvis en IP-telefon) kan fastställa sin egen prioritet. Det finns åtta olika prioritetsnivåer som omfattar 0 till 7. Noll är en ”*best effort*”, vilket innebär att den är okänslig för fördröjning och kan vänta i kön, varför denna är lämplig för FTP. Nivå 5 representerar Video och VoIP och nivå 6 interaktiv VoIP-trafik. På dessa nivåer har man inte tolerans för mer än 10ms fördröjning. Dessa högre nivåer ställer höga krav på garanterad bandbredd.

Detta arbete har ett stort fokus på Cisco Systems och Alcatel-Lucents hårdvara, varför det är lämpligt att diskutera hur QoS kan implementeras på dessa.

På Cisco Systems utrusning delar man in interface i *trusted* (=lita på) och *untrusted* (=litar ej på) vilket i praktiken innebär att nätverket litar på ett *trusted* interface medan ett *untrusted* interface inte hanteras på samma sätt.

Först tar man reda på vilka interface på nätverksenheterna som ska vara *trusted* och *untrusted*. Vissa enheter skapar sitt eget Class of Service (CoS)-värde (=prioritetsnivå) och litas på av utrustningen från Cisco Systems (till exempel har en 7940 IP telefon ett CoS värde av fem). Därmed kan interfacen där telefonen kopplas till konfigureras som *trusted*. På länkar mot andra nätverksenheter i nätverket ska interfacen också vara *trusted*. De andra interfacen blir därmed *untrusted*.

Alcatel-Lucents implementering av QoS har inte koncepten av *trusted* och *untrusted* interface utan man skapar policys per tjänst eller per interface som sedan appliceras på interfacen. Olika policys kan skapas för *ingress*- och *egress*interface. Man har här möjlighet att styra trafik på många olika sätt så som genom CoS-värden, IP-adress med mera.

2.4 Wetternet

2.4.1 Hårdvara i Wetternet

Wetternet är Jönköping Energi ABs stadsnät och spänner över stora delar av Jönköpingsregionen. Den mest betydande delen är dock i centrala Jönköping.

Wetternet är i huvudsak uppbyggt kring Cisco Systems produkter. Det finns dock vissa undantag, men företaget har som mål att kunna samla så många delar som möjligt av nätverket med Cisco Systems-utrustning.

Som grund används 6500-, 3550/3560/3750- och 2950-serierna. De allra flesta av de här serierna har varianter inom den specifika serien. T ex så är en 3550 och en 3560 inte likadana, men de följer samma övergripande struktur och uppbyggnad. De har dessutom så pass liknande funktion att de nästintill kan ses som samma modell. Dock kommer inte 3550 att fortsätta produceras framöver, utan ersätts därmed ofta med 3560 eller motsvarande. Sett till funktion kan tabell 2-1 underlätta förståelsen av Wetternets hårdvaruuppbyggnad:

Funktion	Serie	Kommentar
Core	Catalyst 6500	4 st. 6513
Distribution	Catalyst 3550/3560 Catalyst 3750	Det finns flera olika varianter av dessa serier. Dock har 3750 fler funktioner än 3550/3560. Det mesta som används är 3550 i dagsläget.
Access	Catalyst 2950 Catalyst 2960	Används för att koppla in kunder.

Tabell 2-1 Wetternets nätverksutrustning

Det finns flera protokoll att använda när man skickar VLAN över trunklänkar. Det mest förekommande och det som Cisco Systems rekommenderar är att 802.1q används. JEAB har tagit fasta på det och använder det som *trunk*protokoll över sitt nätverk. Det finns också flera av Jönköping Energi ABs kunder som vill hålla sina egna VLAN inom företaget privat, varför det krävs q-in-q på dessa ställen. Det leder också till att de inblandade switcharna måste kunna hantera frames större än standardstorleken för Ethernet. När man i Cisco Systems Internetwork Operating System (IOS) anger att det ska finnas stöd för så kallade ”jumbo frames” (frames större än standard Ethernet-storlek), är *default* att MTU sätts till 9216 bytes. Så är också fallet hos JEAB.

Det finns försök inom JEAB med multicast-trafik. Detta är än så länge i relativt liten skala, men finns aktiverat med ”sparse-mode” på vissa Core-switchar. Som nämndes i inledningen kommer multicast att tas upp i denna rapport i mån av tid, men på grund av brist på densamma så kommer inte detta att tas upp och utredas närmare här. Den konfiguration som finns för multicast lämnas därmed endast som reflektion och undersöks inte närmare.

Wetternet måste naturligtvis underhållas och förändras allteftersom nya installationer görs och kunder kopplas upp eller kopplas ned. I dagsläget sker en stor del av detta underhåll manuellt genom inloggning i switcharna på ett managementnät i Wetternet. För att underlätta sådana här arbeten och för att höja säkerheten finns det allmänt några olika alternativa lösningar. Jönköping Energi AB har valt att låta en Terminal Access Controller Access-Control System (TACACS)-server som finns på managementnätet sköta autentisering och inloggning.

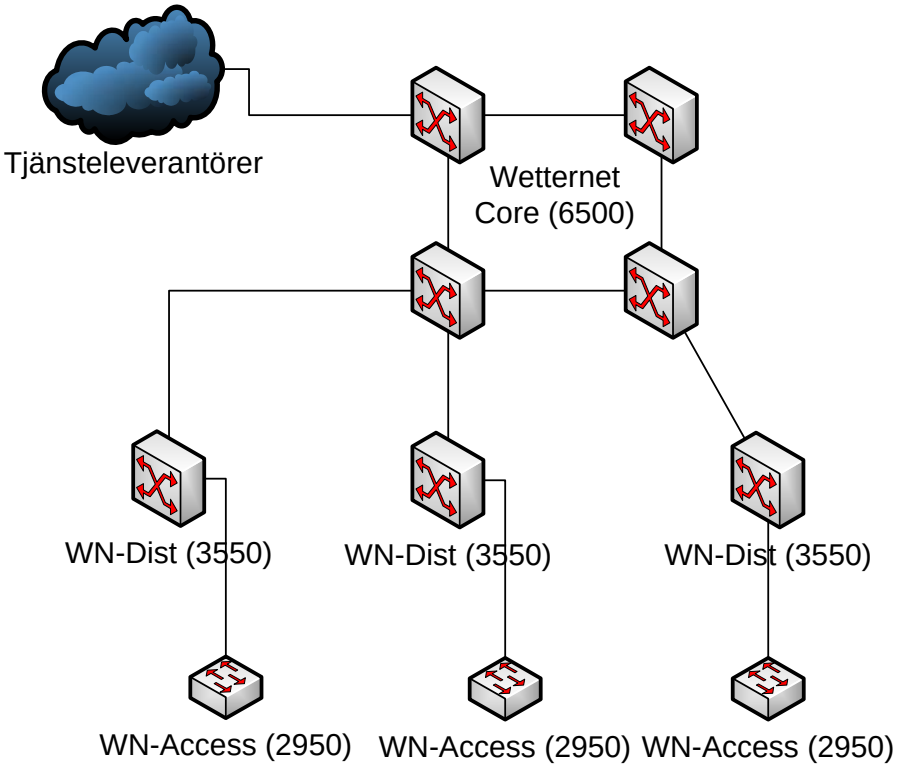
Allmänt i nätverksvärlden finns det ett stort intresse för Quality-of-Service (QoS) men i så pass snabba nät som finns i Wetternet (och i Sverige i allmänhet), har inte QoS så stor funktion utöver att styra bandbreddstilldelningen till kunderna. Detta kallas för *shaping*. Den QoS som finns på Wetternet är till största delen satt på distributionslagret, men även här finns det finns undantag med QoS på både Core- och Accesslagret. Funktionen hos den QoS som finns där är satt för att styra om kunderna i nätet ska ha 2 eller 5 Mbit/s. Om de vill ha 10, 100 eller 1000 Mbit/s sköts automatiskt genom att interfacet är satt till den hastigheten.

2.4.2 Nätverksstruktur

Cisco Systems förespråkar ofta trelagermodellen där de olika lagren har olika funktioner i nätverket, Core, Distribution och Access. Wetternet följer denna modell så långt det är möjligt. Det är inte i alla fall det är möjligt, och där görs då undantag. Som exempel kan nämnas att det finns vissa fall där kunder kopplas in direkt i en distributionsport, vilket inte följer trelagermodellen.

Wetternet har fyra Catalyst 6513 Core-switchar vilka utgör backbone i stadsnätet. Inom Core används det Gigabit fiber-länkar. Från Core ned till distributionsnivån är det också fiber-länkar av Gigabit-hastighet. På den här nivån finns också viss trafikmarkering/prioritering i form av Class of Service (CoS) och Quality of Service (QoS). Ytterligare en nivå i hierarkin, mellan distributions- och accessnivån, finns det Gigabit-länkar. Däremot är de portar där kunderna kopplas in, FastEthernet-portar, med 100 Mbit/s eller Ethernet-portar med 10 Mbit/s. Beroende på vad det är för kund som kopplas in där, är dessa portar accessportar eller trunkportar. I de fall då kunden vill behålla privata VLAN används q-in-q som protokoll/teknik för den trafiken.

Ur kundens perspektiv fungerar tekniken och användandet av nätet såhär: Kunden får tillgång till Wetternet, vilket är det stadsnät (MAN) som Jönköping Energi AB erbjuder. Kunden väljer sedan en internetlevarantör som Jönköping Energi AB har avtal med och finns tillgängliga för Wetternet. De är ca 5-10 till antalet. Tjänsteleverantören har en koppling in till Core i Wetternet, och erbjuder sin egen internettjänst till kunderna som finns inom Wetternet. Rent kostnadsmässigt betalar alltså kunden en avgift för nätkostnaden, Wetternet, och en avgift för internettjänsten. Till vissa kunder (ej privatkunder) erbjuder även Wetternet tjänsten internet. Wetternet illustreras mycket förenklat i figur 2-10 nedan:



Figur 2-10 Förenklad Wetternet-nätverksstruktur

2.5 Cisco 6500/7600-serien

2.5.1 Cisco Catalyst 6500-serien

Cisco Systems Catalyst 6500-serie är en kraftig switching-plattform och används i medelstora och stora företag samt hos tjänsteleverantörer. Switchen är väldigt skalbar och kan köra 1152 10/100-Mbps, 576 10/100/1000-Mbps eller 64 10-Gbps Ethernet-portar i ett enda chassi. Därmed har man möjlighet att skala systemet upp till 720 Gbps vilket ger 40 Gbps/slot (halv-duplex). Vidare finns det ett flertal chassi- och WAN-interface-modul-valmöjligheter.

[28]

2.5.2 Cisco 7600-serien routrar

Cisco 7600-serien erbjuder skalbara personaliga IP/MPLS-tjänster, Ethernet switching och 10-Gbps interface. Detta möjliggör för företag att leverera kund- och affärstjänster över ett enda *Carrier Ethernet* nätverk. Andra viktiga features inom Cisco Systems 7600-serie är:

- Hög prestanda med upp till 720 Gbps i ett enda chassi eller 40 Gbps kapacitet per *slot*.
- Breda Video on Demand (VoD), Voice over IP (VoIP) och WAN-carrier -funktioner
- IP/MPLS Provider edge routing [29]

2.5.3 Cisco 7600 Ethernet Services 20G (ES20) modulkort

Cisco Systems 7600-serie Ethernet Services 20G (ES20)-modulkort är ett Ethernet linjekort för Cisco 7600-serie routrar som har 20 Gbps trafik-hantering. Det finns två versioner av detta:

2-portars version: 7600-ES20-10G

20-portars version: 7600-ES20-GE

Skillnaden mellan dessa varianter är att 2-portars-modellen har 10 Gbit interface och använder XFP moduler och att 20-portars-modellen har 1 Gbit interface och använder Short Form Pluggable (SFP)-moduler. De här modulerna tillåter modulkortet att konfigureras för olika typer av media (koppar eller fiber) och olika optiska krav (d v s single mode eller multimode fiber). ES-7600-ES20-GE3C-varianten kan användas i ett Cisco Catalyst 6500 chassi och får därmed i stort sett samma funktioner som en riktig Cisco Systems 7600 router.

2.5.4 Features på ES20

ES20-modulkortet kan implementeras i en Cisco Catalyst 6513 för att då ge funktioner som Cisco 7600-serien har. Några av de funktioner som finns stöd för listas och beskrivs här lite noggrannare.

- Subinterface
- Switch Virtual Interface (SVI)
- Jumbo frames-hantering
- Lager 2 switching
- VLAN-översättning och Flexible q-in-q
- IGMP-snooping
- VPLS och Hierarkisk VPLS
- Modular QoS CLI (MQC), inkluderar bl a Traffic Shaping
- Stöd för att markera och prioritera frames på *ingress* eller *egress*

2.5.4.1 VLAN-översättning och Flexible q-in-q

ES20-kortet erbjuder flera tekniker för att hantera frames på lager 2-nivån. Det ges flera sätt på vilka man kan förändra VLAN-ID etc. Man kan genom Flexible q-in-q använda VLAN med endast lokal betydelse, genom att man byter VLAN-ID (VID) på framet. Detta är också möjligt att göra om man har dubbla taggar, alltså en q-in-q länk.

Som en del i Flexible q-in-q finns Selective q-in-q. Den tekniken lägger till en yttre *tag* till 802.1q-framen innan det switchas till den punkt i nätverket där taggningen termineras.

2.5.4.2 Subinterface

Subinterface är en logisk uppdelning av ett fysiskt interface. Det kan användas för att länka ett VLAN till en EVC, eller kan användas vid trunkning.

2.5.4.3 Switch Virtual Interface (SVI)

Switch Virtual Interface (SVI) används vid Multi Layer Switching (MLS) för att kunna koppla ett VLAN till en IP-adress. Detta möjliggör routing mellan VLAN.

2.5.4.4 Lager 2 switching

Det finns stöd hos 6500/7600-switchen/routern att hantera och switcha Ethernetframes och trunkar.

2.5.4.5 IGMP-snooping

Internet Group Management Protocol (IGMP) används vid MultiCast (MC)-trafik för att koppla vilka användare som finns i vilka multicast-grupper. Det normala är att en switch forwardar MC-frame på alla portar inom ett VLAN. Snooping-funktionen gör så att endast de klienter som är ämnade för just den trafiken får de framen. IGMP-snooping agerar på lager 2 i OSI-modellen. ES20 ger fullt stöd för dessa funktioner.

2.5.4.6 VPLS och Hierarkisk VPLS

ES20 stöder upprättandet av PseudoWires (PWs), vilket används vid Virtual Private LAN Services (VPLS). Detta sker ofta genom MPLS, men är möjligt även genom Internet Protocol (IP).

För ES20 gäller att när vanlig VPLS används, kan inte q-in-q användas samtidigt. Kortet stöder både Hierarkisk och klassisk, plan, VPLS-struktur.

2.5.4.7 Modular QoS CLI (MQC)

Cisco Systems Modular QoS Command-Line Interface (MQC) kan användas för att klassificera trafik, sätta policy på trafik och sedan lägga till policyn till ett interface. Trafiken kan klassificeras på ett antal olika sätt, exempelvis en Access Control List (ACL) som filtrerar trafik beroende på dess IP/MAC-adress, CoS-värden eller protokoll mm.

Ett exempel är en ACL som tar in trafik som matchar ett visst IP-nät. Kommandot kan vara **access-list** *100* **permit ip** *192.168.200.0 0.0.0.255* **any**. Man kan sedan skapa en klass genom kommandot **class-map**. Kommandots format är **class-map** *klass* där klass är en class-maps instansnamn. Genom ett **match**-kommando kan man fånga in trafik eftersom paketen kontrolleras. Exempelvis så betyder kommandot **match access-group** *100* att all trafik som filtrerades av accesslista 100 ska finnas i den *class-map*-instans som skapades.

När man har fått trafik till en viss klass kan man skapa en policy som styr hur trafiken ska behandlas. En *policy-map* skapas för en *class-map*-instans och sedan kan man ange ett flertal olika kommandon för att hantera trafik vid behov. Trafiken i exemplet ovan inkluderas i en *policy-map* via kommandot **policy-map** *policy* och sedan **class** *klass* och **shape average 30000000**. Alltså *shapar* man en bandbredd på 30 Mbit/s för de interface som policyn appliceras på. Mer avancerade kommandon kan användas med prioritering och köning av känslig trafik, exempelvis Low Latency Queuing (LLQ) där trafik av största betydelse skickas till en speciell kö.

Sista steget i Modular QoS Command-Line Interface är att applicera policyn till ett interface. Man kan bestämma om policyn ska appliceras på inkommande eller utgående trafik. Kommandot är alltså:

service-policy input *policy-namn* eller

service-policy output *policy-namn*

ES20 har endast stöd för *shaping* på *egress*, och inte *ingress*. Detta bör tas i beaktande när man implementerar denna funktion.

2.5.4.8 Stöd för att markera och prioritera frames på ingress eller egress

ES20-kortet erbjuder också möjligheten inom QoS att markera och prioritera frames på *ingress* och/eller *egress*-interfacen.

Markering av paket sker inom en *policy-map* som skapas inom MCLI. Markering används vanligast för att identifiera paket men kan även användas för speciella funktioner som kan *droppa* paket eller utföra prioritering. Följande gäller för markering på *ingress*- respektive *egress*interfacen.

- Ingress-markering är möjlig på fysiska interface, *subinterface* och *service*instanser
- *Egress* markering sätts endast på *subinterface* och *service*instanser
- Markering med policing har företräde över *class-based marking* om *service policyn* använder båda typer av markering
- *Set*-kommandot används inom en *policy class-map* för att specificera vilka typer av paket som ska markeras. Det finns många olika markeringar som kan göras med *set*-kommandot men endast *set cos* och *set cos inner* när man kör MPBE.

Ciscos Systems 7600-router har många kö-funktioner men endast följande funktioner fungerar med ES20:

- Aggregated Weighted Random Early Detect (WRED)
- Low Latency Queuing (LLQ)
- Class-Based Weighted Fair Queuing (CBWFQ)

När man lägger inkommande paket i en kö är *default*-beteendet att *droppa* paket när trafikstockning sker. WRED begär att enheterna minskar sändning av paket tills trafikstockningen har upphört. Detta fungerar bara med trafik som har TCP som protokoll och TCP kan snabbt komma igång igen när trafikstockningen har sänkts.

CBWFQ är ett sätt att dela upp bandbredden i olika klasser som har olika typer av trafik och därmed olika krav. Man kan också ange hur stor varje kö i varje klass ska vara i antal paket.

LLQ används också genom MCLI och ger en trafik-klass högsta prioritet genom **priority**-kommandot. Denna typ av köning används för trafik som har en låg tolerans för fördröjning t ex Voice over IP (VoIP). [30]

2.5.4.9 DHCP Relay agent med option 82

Cisco Systems ES20 har stöd för DHCP Relay agent option 82-funktion i vissa versioner av IOS. Detta tas också upp mer senare i rapporten.

2.6 Alcatel-Lucent 7450 Ethernet Service Switch (ESS)

2.6.1 Översikt

Alcatel-Lucents 7450 Ethernet Service Switch är en mångsidig switch som stöder LAN-, MAN- och WAN-tjänster och har designats för att vara lönsam både för kund- och affärsmarknader. Den har marknadsledande ethernettjänster så som Virtual Leased Line (VLL), VPLS och *Triple-Play*-tjänster över IP/MPLS-nätverk. Switchen är inriktad mot tjänsteleverantörer eftersom man kan konfigurera olika Service Level Agreement (SLA) med stöd för QoS (*shaping* med mera) per port och per tjänst.

Det finns fyra chassi-konfigurationer som kan hantera multi-Gigabit och 10 Gigabit Ethernet som listas i tabell 2-2 nedan:

Modell	Antal slot	Total Bandbredd	Bandbredd per slot
Alcatel-Lucent 7450 ES-12	10	400 Gbit/s full duplex	40 Gbit/s slot kapacitet
Alcatel-Lucent 7450 ES-7	5	200 Gbit/s full duplex switch	40 Gbit/s slot kapacitet
Alcatel-Lucent 7450 ES-6	4	80 Gbit/s full duplex	20 Gbit/s slot kapacitet
Alcatel-Lucent 7450 ES-1	1 (integrerad)	20 Gbit/s full duplex switch	20 Gbit/s slot kapacitet

Tabell 2-2 Alcatel-Lucent 7450 Ethernet Service Switch modeller

2.6.2 Features på ESS-1

I många delar och funktioner liknar Alcatel-Lucent 7450 ESS-1 Cisco Systems Catalyst 6513 utrustad med ES20-modulkortet, men det finns också skillnader. Vissa av ESS-1s funktioner listas och tas därför upp här.

- H-VPLS
- Selective MAC flush
- Non-stop service for VPLS and VLL
- IGMP snooping
- Per-service QoS och *traffic shaping*
- DHCP relay agent, med option 82-stöd
- DHCP snooping
- Anti-spoof filter
- Split-horizon per interface/per service

2.6.2.1 H-VPLS

Den IETF-standard som definierar VPLS är en grundstomme för tillverkare och leverantörer att bygga på, men det är fritt för varje tillverkare att skapa sina egna produkter. Så har Alcatel-Lucent gjort. De anser att standarden inte är fullt tillräcklig men följer standarden för att också bygga ut den. De var med och föreslog skapandet av Hierarchical VPLS (H-VPLS), vilket är ett sätt att komma undan det faktum att VPLS-tekniken egentligen kräver ett *full mesh*-system. Man kan genom H-VPLS t ex koppla ihop två VPLS-nät genom en ny ”nivå” av VPLS (därav *hierarkisk*).

I Alcatel-Lucents implementation av VPLS är det också upp till varje leverantör och nätägare att välja om kunderna använder lager 2- eller lager 3-enheter som koppling in i nätverket. Man kan välja att ha en router (lager 3), vilket ofta ses som en fördel. Då blir MAC-adress-inlärningen lättare att hantera för de switchar som ingår i näten, och färre MAC-adresser som behöver floodas eftersom routern bryter kedjan av MAC-inlärningen. Om man istället väljer att kunderna har en lager 2-switch som koppling in i nätverket, sprids många fler MAC-adresser i nätverket och fler adresser som behöver läras in i Forwarding Information Base (FIB) på switcharna. Detta kan i större nät bli ett problem.

En säkerhetsaspekt är att om man väljer att ha lager 2-enheter hos kunden, kan man styra vilka MAC-adresser som får tillgång till nätverket, och hur många. Ekonomiskt kan man också styra hur många enheter som en kund sedan använder och betalar för. Det vanligaste är dock enligt Alcatel-Lucent i dagsläget att man använder routrar som ändenheter hos kunden.[31] [32]

Den hierarkiska varianten av VPLS (H-VPLS) inför en ny typ av PseudoWires (PWs), Spoke PW. Dessa gränssnitt blir interfacet mellan de båda VPLS-näten som ska kopplas ihop. Tekniken kan liknas vid den som q-in-q använder sig av, där man skickar en tunnel i en annan tunnel, vilket skapar två nivåer av tunnling.

När man inom Hierarkisk VPLS vill skapa redundans, skapas länkar där loopar kan uppstå. För att lösa det problemet har Alcatel-Lucent utvecklat en egen teknik, VPLS-RSTP. Den bygger på Spanning Tree Protocol, med vissa förändringar.

2.6.2.2 Selective MAC flush

En nätverksenhet som är konfigurerad för VPLS och som upptäcker en port som har gått ner skickar ut ett ”flush-all-from-me”-LDP-meddelande. Detta skickas till alla PE i den VPLS-instansen. Alla PEs tar sedan bort alla MAC-inlägg som kommer från sändaren.

2.6.2.3 Non-stop service for VPLS and VLL

För protokoll som kör över Interior Gateway Protocols (IGPs) så som MPLS är det önskbart att kunna fortsätta utan att stoppa när en topolgiförändring sker. *Non-stop*-tjänster för VPLS och Virtual Leased Line försäkrar att detta kan ske genom användningen av tunnlar som skapas via bland annat LDP.

2.6.2.4 IGMP Snooping

Alcatel-Lucents implementering av IGMP snooping fungerar som standarden som beskrivs i RFC 3376. Man kan helt enkelt granska interfacen och bygga en tabell som kan visa vilka interface som har klienter som vill ingå i en multicast-grupp. Denna åtgärd spårar IGMP-meddelanden och noterar vilka interface som tillhör multicast-gruppen. Detta blir en säkerhets- och kapacitetsåtgärd p g a minskad multicast-trafik till interfacen som inte är deltagare i multicast-gruppen.

2.6.2.5 Per Service QoS och Traffic Shaping

Per service QoS handlar om förmågan att skapa specifika krav på en per tjänst-basis. Varje tjänst kan använda sig av multipla köer för att kunna möjliggöra *shaping*, *policing* och markering av olika trafikflöden.

QoS kan integreras med VPLS genom att köra flera tjänster inom en enda VPLS-instans med tydliga Service Level Agreements (SLAs) och även en sammanställd SLA per kund. Varje *service* kan få reserverad bandbredd men även ges lägre prioritet. Detta ger tjänster möjligheten att använda all tillgänglig bandbredd när de har en *burst* av data (en ovanligt stor mängd trafik som skickas innan trafikflödet sedan sjunker till en normal nivå).

2.6.2.6 DHCP relay agent med option 82

För att kunna tillhandahålla mer information för DHCP-servern så att IP-adresseringspolicyn kan följas används DHCP relay agent med ”option 82”. Det är helt enkelt ett tillägg till DHCP relay agent-funktionen. Exempelvis kan information om port-ID som DHCPREQUEST har kommit från inkluderas i DHCP-paketet. DHCP-servern kan sedan använda den informationen för sitt beslut beroende på vad som har konfigurerats.

2.6.2.7 DHCP snooping

När man aktiverar DHCP snooping på ett interface filtrerar switchen bort DHCP meddelande som vanligtvis kommer från en DHCP server. Detta sker på interfacen som har definierats som *untrusted*. Vidare skapas en DHCP-tabell som används som en kontrollering mot nya DHCP-paket som mottages på interfacen. I tabellen lagras vilka klienter som har vilka IP-adresser. Kontrolleringen sker inte på interfacen som har definierats som *trusted* (*trusted* är vanligtvis *uplink*-interface mot andra switchar).

2.6.2.8 Anti-Spoof filter

Routern har också en automatisk anti-*spoofing*-funktion där man kan filtrera ut IP- och MAC-adresspar för att kunna förebygga *spoofing* av IP/MAC adresser. Utan denna funktion kan man spoofa (d v s replikera en giltig adress) IP- eller MAC-adresser och delta i DHCP-processen och slutligen få tillgång till nätverket.

2.6.2.9 Split Horizon per interface/per service

Split horizon-funktionalitet finns per interface eller per service och används i detta fall för att hantera ogiltig peer-to-peer-kommunikation. Det fungerar genom att försäkra att paket som ska skickas vidare inte skickas genom interfacen där paketet har kommit från. [33]

3 Genomförande

3.1 Metoder

Från början av arbetet var tanken att en relativt stor del av tiden skulle gå åt till att göra laborationer på den nya utrustningen som JEAB har köpt in. Denna utrustning blev leveransförsenad varför laborationer då inte var möjligt. Det var också två konsultbolag som arbetade med samma uppgifter på den utrustningen. Därför har detta arbete handlat mer om att studera tekniker och konfiguration som andra personer har fysiskt implementerat. Kontakt med dessa och personal hos företaget har dock hållits för att kunna förstå och utreda de funktioner som används.

Det finns två möjliga hårdvarulösningar som har identifierats för att koppla GPON-installationen med det befintliga stadsnätet. Dessa är Cisco Systems 7600 ES20 modulkort i en Catalyst 6513 och Alcatel-Lucents 7450 Ethernet Service Switch 1. Eftersom företaget vill ha Cisco Systems lösning i första hand kommer därför denna att undersökas först.

3.1.1 Cisco 7600 ES20 modulkort

3.1.1.1 Multipoint Bridging over Ethernet

Under arbetet har företaget och deras tjänsteleverantörer gett specifika krav när det gäller hur dataöverföring ska ske på OSI lager-2. Från företagets sida vill man inte att tjänsteleverantören ska se kundens lokala VLAN utan endast de VLAN som genereras av stadsnätet för att representera kundens VLAN till tjänsteleverantören. Funktionen ska alltså vara att kundens lokala VLAN inte syns, utan endast *provider-VLAN* (Wetternets tilldelning av VLAN). Företaget själv vill att MAC-inlärning sker inom stadsnätet.

Cisco Systems 7600 ES20 modulkort erbjuder ett par lösningar för Ethernet LAN-tjänster; Flexible q-in-q och Multipoint Bridging over Ethernet (MPBE). Både Flexible q-in-q och MPBE erbjuder Single Tag Translation (översättning av kundens VLAN till ett definierat VLAN som representerar en eller flera kund-VLAN) men Flexible q-in-q erbjuder inte MAC-inlärning. Därför är MPBE bästa valet för att kunna tillfredställa kraven som beskrivs ovan.

En *service*-instans ska skapas för varje mappning av ett VLAN till ett annat. För att kunna definiera att det är det inkommande VLANet, säg VLAN 2000, som gäller, skriver man kommandot **encapsulation dot1q** *kund-vlan*. Kommandot som ersätter kundens VLAN med ett annat är *rewrite*. Det finns flera valmöjligheter med kommandot men i detta fall kräver man *ingress* som nyckelord (för det är kundens VLAN som ska översättas). Följande kod visar hur en liten del av konfigurationen kommer att se ut:

```
interface GigabitEthernet3/0/3
 description trunk to 3550-24

service instance 2000 ethernet
  encapsulation dot1q 2000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 399 split-horizon [34]
```

3.1.1.2 QoS

Enligt kravspecifikationen från företaget vill de styra trafiken per tjänst, d v s att gruppera ett antal kunder som har samma tjänst. Detta kan möjliggöras med Modular QoS Command Line Interface (MQC). En *class-map* kan användas för att matcha trafik på grund av dess Class of Service (CoS)-värde. En *policy-map* kan sedan skapas per tjänst för att koppla ihop den med den CoS *class-map* som man vill ha en policy till. En ytterligare *policy-map* behövs för att kunna styra *default* klass-trafik på tjänstens hastighet (i detta fall 30 Mbit/s). Ett *police*-kommando ska användas för trafik som är känslig för fördröjning, t ex rösttrafik. *Police*-kommandot *droppar* paket som överstiger en specificerad gräns (30 Mbit/s). Ett *shape*-kommando ska användas för *default* klass-trafik men ***shape*** behåller paket och skickar dem när trafikflödet sjunker. För trafik som inte är känslig för fördröjning ska *bandwidth percent*-kommandot användas med gränsen satt till 95 %. Detta för att se till att trafik som har CoS-värde 0 eller 1 får en större del av den tillgängliga bandbredden. Följande kod visar hur QoS-konfigurationen kommer att se ut:

```
class-map match-any BC-COS
  match cos  2  3
class-map match-any RT-COS
  match cos  4  5
class-map match-any BE-COS
  match cos  0  1
class-map match-any NC-COS
  match cos  6  7
policy-map CUST-30MBPS-QOS
  class BE-COS
    bandwidth percent 95
  class RT-COS
   police 300000
    priority
policy-map SHAPE-30MBPS
  class class-default
    shape average 30000000
   service-policy CUST-30MBPS-QOS [29]
```

3.1.1.3 DHCP

Ett ytterligare önskemål från kravspecifikationen är att implementera DHCP snooping på de interface som är *untrusted*. Det finns möjlighet att implementera DHCP snooping per interface och per VLAN. I detta fall ska båda valmöjligheterna användas.

Under arbetets gång framkom krav från en av Wetternets tjänsteleverantörer att DHCP Relay agent option 82 måste kunna användas. Cisco Systems och Alcatel-Lucent har i dagsläget olika sätt att implementera detta på. Det framkommer här också att den variant som Cisco Systems har valt att använda sig av, inte är lämplig i Wetternets miljö.

För att försäkra att interfacen är *trusted* när paket skickas som inkluderar DHCP option 82 användar man kommandot *ip dhcp relay information trust-all*. Däremot vill företaget att kommandot ger administratören möjligheten att ändra en sträng som ligger i DHCP-paketets struktur. Cisco Systems implementation av DHCP option 82 betyder att dess egna strängar används och dessa går inte att byta i dagsläget. Denna funktionsbrist betyder att JEAB inte kan fortsätta med Cisco Systems 7600 ES20 linjekort som lösning och vill hellre rikta sitt intresse på Alcatel-Lucents lösning (7450 Ethernet Service Switch). Däremot är rekommendationen att Cisco Systems implementation inte borde glömmas helt eftersom det kan komma en ny IOS-version som tillhandahåller DHCP option 82-funktionalitet på det sätt som företaget önskar. Följande avsnitt beskriver hur kraven kan tillfredställas med denna lösning. Se följande kod som kan ta hand om DHCP-kraven.

```
ip dhcp relay information trust-all
ip dhcp snooping vlan 999,1386
ip dhcp snooping [35]
```

3.1.1.4 MAC – spoof attackskydd

Modulkortet från Cisco Systems tillhandahöll ingen bra säkerhetsåtgärd när det gäller skydd mot MAC-spoofing. På den punkten misslyckas därför detta modulkortet på kravspecifikationens krav.

3.1.1.5 Multicast

Utredning av multicast skulle endast inkluderas i mån av tid. Eftersom fokus är på att få en lyckad koppling mellan GPON och stadsnätet har multicast-funktionalitet inte implementerats som en del av detta arbete. Däremot kommer funktionaliteten att användas i framtiden.

3.1.2 Alcatel-Lucent 7450 Ethernet Service Switch 1

3.1.2.1 VPLS

Kraven som har ställts av företaget är samma oavsett vilken hårdvarulösning som bedöms vara den bästa. Därmed kräver man fortfarande en *single tag translation* för att kunna hindra att kund-VLANen kommer ända fram till tjänsteleverantörens nät. I detta fall finns det en implementering av VPLS som kan klara av detta krav. Man behöver inte en fullständig VPLS-lösning utan bara att skapa en enkel översättning. Ett visst antal kund-VLAN kan översättas till en VPLS-instans (som ska representera ett VLAN som tjänsteleverantören kan mottaga).

Först behöver man konfigurera portarna som kopplas mot GPON och stadsnätet. Porten mot stadsnätet ska få mode access och encapsulation dot1q (som Cisco Systems hårdvara känner igen i Core-konfigrationen). En MTU på 9212 bytes skapas (jumbo frames) för framtida behov av q-in-q tekniken. För att säkra att obehöriga inte kan ta fördel av auto negotiate-säkerhetsbristen via en emulerad 802.1q trunk ställs porten i no autonegotiate. Porten är naturligtvis konfigurerad i ett no shutdown-tillstånd så att den kan användas.

Den här konfigurationen är replikerad på porten som GPON kopplas till, men nu finns det inget behov av **no autonegotiate**-kommandot.

När portarna har definierats kan man skapa en VPLS-instans vilkens ID-nummer representerar samma VLAN som tjänsteleverantören är konfigurerad att mottagga från stadsnätet. Ett unikt kund-ID (Service Access Point) skapas först med ett *sap*-kommando och inkluderas i en VPLS-instans. *Sap*-kommandot använder ett dot1q-format som ser ut såhär: port_id:qtag_id (802.1Q). Port-ID representerar porten där en eller flera kunders VLAN kommer in. Qtag-id representerar dot1q-inkapslingstyp och kan ha ett värde av 0-4094. Kund-VLAN representeras som qtag_id och sap-instansen identifieras med qtag_id. Sedan skapar man policyn per det lokala kund-VLAN som används. Följande kod visar hur konfigurationen ser ut.

```
port 1/1/1 (mot stadsnät)
      ethernet
         mode access
         encap-type dot1q
         mtu 9212
         no autonegotiate
      exit
      no shutdown
exit

port 1/1/8 (mot GPON)
     ethernet
         mode access
         encap-type dot1q
         mtu 9212
      exit
      no shutdown
exit

customer 614 create

vpls 843 customer 614 create
sap 1/1/8:2001 split-horizon-group "843" create
exit
```

3.1.2.2 *Quality-of-Service*

Företaget vill styra trafiken enligt texten i avsnitt 3.1.1.2 och därför behöver man QoS-funktionalitet som motsvarar den som skapades i lösningen med Cisco Systems hårdvara.

Först behöver man skapa alla tjänster som levereras genom stadsnätet. Detta behöver göras både för *ingress*- och *egress*-interfacen. Varje hastighet anges via *rate*-kommandot och skrivs i Kbit/s. Varje hastighet tillhör en *queue* som måste definieras. Följande del av konfigurationen visar hur detta ska se ut.

```
qos
      sap-ingress 30 create
         queue 1 create
            rate 30000
         exit
         queue 11 multipoint create
         exit
      exit
      sap-egress 30 create
         queue 1 create
            rate 30000
         exit
      exit
   exit
```

QoS-policyn som har skapats måste bindas till specifika interface/kund-VLAN så att man kan leverera tjänsterna på ett per interface-/per tjänst-underlag. Här behöver man använda *ingress*- och *egress*-kommandon och sedan *qos*-kommandot med den tjänst som man vill binda. I exemplet ovan blir det 30 som representerar tjänsten.

```
vpls 114 customer 114 create
         sap 1/1/8:2005 split-horizon-group "114" create
            ingress
               qos 10
            exit
            egress
               qos 10
            exit
         exit
         no shutdown
```

3.1.2.3 DHCP

Lösningen med Cisco Systems produkter kan inte tillhandahålla DHCP option 82 på det sättet som företaget vill ha. Däremot kan Alcatel-Lucents lösning göra detta.

För att kunna konfigurera DHCP-funktionaliteten så används *dhcp*-kommandot. För att kunna slå på DHCP snooping använder man *snoop*-kommandot. Ett *lease-populate*-kommando ska användas för att utföra leasehantering. Detta använder snooped DHCP ACK-paket för att bygga leasehanteringstabellen. Ett värde av 2 betyder att två platser finns i tabellen för ett visst SAP-interface. Option 82 möjliggörs med *option*-kommandot och sedan försäkrar *action replace*-kommandot att för uppströmstrafik ska option 82-fältet läggas till paketet (och skriva om de existerande option 82-fälten). För nedströmstrafik har option 82 tagits bort. DHCP-kommandot utförs per interface/kund. Följande konfiguration visar hur DHCP-implementationen ser ut som en helhet.

```
vpls 843 customer 614 create
  sap 1/1/8:2001 split-horizon-group "843" create
    dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
          exit
```

3.1.2.4 MAC – spoof attackskydd

Det finns ett enkelt kommando (**anti-spoof ip-mac**) som kan användas på varje interface/kund-VLAN. Kommandot filtrerar bort okända IP/MAC-adresser för att kunna säkra upp DHCP genom att källans IP- och MAC-adresser i en tabell kan kollas upp. Detta motsvarar de önskemål som ges av kravspecifikationen.

3.1.2.5 Multicast

Multicast-funktionalitet kommer inte att tas upp i rapporten. Enligt kravspecifikationen är detta krav önskad fast det finns tyvärr inte inom tidsramen som har fastställts. Funktionaliteten kommer att implementeras i framtiden.

4 Resultat

4.1 Kravspecifikationens mål

Företagets mål med arbetet har varit att få en större förståelse och insikt i GPON och i hur ett VPLS fungerar. JEAB förutsatte att detta skulle vara en viktig del i lösningen på deras problem med att koppla ihop de två näten. Önskemålet har också hela tiden varit att så långt det är möjligt använda sig av utrustning från Cisco Systems eftersom större delen av stadsnätet bygger på deras produkter.

För den kopplingspunkt som har utretts har det också funnits intresse för en produkt från Alcatel-Lucent, ESS-1, som är en *multilayer switch* och har liknande funktionalitet som en Cisco Systems 7600-router. Därför skulle båda dessa alternativ undersökas och utredas.

En kort lista över vissa krav och önskemål som finns från JEAB är följande:

- Ökad förståelse för VPLS och GPON
- *Shaping* av trafik, via QoS (per tjänst, 2, 5, 10, 30, 100 Mbit/s)
- DHCP snooping
- Skydd mot MAC-spoofing
- DHCP option 82

4.2 Vald lösning

Både Cisco Systems och Alcatel-Lucents lösningar tillfredställer de flesta krav som företaget hade. Däremot saknar Cisco Systems ES20-modulkort förmågan att köra DHCP option 82 per *subinterface*, någonting som Alcatel-Lucent klarar av. Därför är Alcatel-Lucents lösning mest lämplig som kopplingspunkt mellan GPON-installationen och stadsnätet.

Lösningen bygger på en del av VPLS-tekniken, fast endast delvis och inte som helhet, och VPLS är implementerad endast i denna kopplingspunkt. En *service*-instans skapas per kund och tjänsteleverantör och de kopplas till ett VLAN-ID. Vidare funktionalitet så som DHCP snooping och DHCP option 82 specifikt till vissa kunder kan sedan läggas till. Den här lösningen löser det huvudkrav som var att tjänsteleverantören inte ska se kundernas lokala VLAN utan bara de som representerar en grupp kunder.

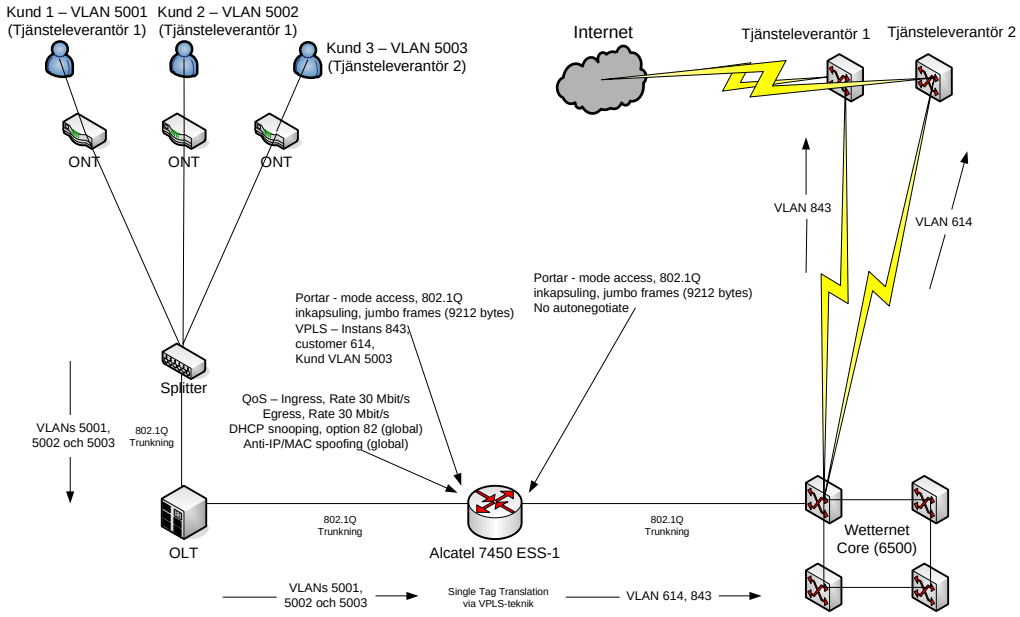
Ett annat viktigt önskemål var att kunna styra trafiken per tjänst. Detta möjligjordes med QoS-instanser som representerar alla typer av tjänster som finns i dagsläget. Varje tjänst fick sin motsvarande hastighetsbegränsning och sedan appliceras på både *ingress*- och *egress*portar.

Nedan visas en liten del av konfigurationen och kommenteras efteråt. Observera att detta endast är en liten del av den totala konfigurationsfilen. För fullständig konfig, se bilaga 2.

```
----
    service
        customer 114 create
            description "Tjänstelev. 114"
        exit
----
        vpls 114 customer 114 create
            description "Tjänstelev. 114"
            split-horizon-group "114" residential-group create
            exit
            sap 1/1/8:2005 split-horizon-group "114" create
                ingress
                    qos 10
                    filter ip 10150
                exit
                egress
                    qos 10
                exit
            exit
            sap lag-1:114 create
            exit
            no shutdown
        exit
----
    port 1/1/1
        description "lag-1_mot_cisco"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
            no autonegotiate
        exit
        no shutdown
    exit
----
    port 1/1/8
description "GPON-JKP-IF-02"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
        exit
        no shutdown
    exit
----
    qos
        sap-ingress 10 create
            queue 1 create
```

```
            rate 10000
         exit
         queue 11 multipoint create
         exit
      exit
      sap-egress 10 create
         queue 1 create
            rate 10000
         exit
      exit
   exit
```

En grafisk presentation av kopplingen mellan GPON och Wetternet hos Jönköping Energi AB ges av figur 4-11:



Figur 4-11 Implementerad lösning för kopplingspunkten mellan GPON och stadsnätet

För att en kund ska kunna få kontakt med tjänsteleverantören och därmed Internet sker följande:

Kunden vill nå exempelvis en webbsida. DNS-förfrågan skickas iväg från Kund 2 som ligger i VLAN 5003. Paketet som innehåller DNS-förfrågan skickas till ONT som passivt skickar det vidare till OLT. OLT känner att paketet har en destination som ligger i tjänsteleverantörens nät och därmed skickar paketet vidare längs en 802.1Q trunk som kan hantera flera VLAN samtidigt. Alcatel-Lucent 7450 ESS-1 mottagger paketet och märker att det ska skickas vidare. En single tag translation utförs på paketet och kundens VLAN tas bort och ersätts med 614. Paketet skickas sedan vidare för överföring över stadsnätet mot tjänsteleverantören. Det översatta VLANet 614 känns igen och kan hantera paketet.

När DNS-svaret återkommer översätts VLAN 614 tillbaka till kundens VLAN som skickade förfrågan.

Beroende på kunden, får paketet föras över en förbestämd tjänstehastighet (i detta fall 30 Mbit/s). Detta beslut hanteras i QoS-konfigurationen.

5 Slutsats och diskussion

Målet var att hitta en lösning som kunde koppla ihop Wetternets nya GPON-installation med deras befintliga stadsnät via VPLS. Deras önskemål var att detta helst skulle göras med hårdvara från Cisco Systems för att förenkla administrationen, eftersom stadsnätet byggs på Cisco Systems produkter. Däremot var detta inte möjligt eftersom funktionalitet i 7600 ES20-modulkortet inte tillät DHCP option 82 på subinterface. Därför valdes Alcatel-Lucents 7450 Ethernet Service Switch istället.

Denna lösning fungerar bra eftersom GPON-installationen bygger på Alcatel-Lucent-utrustning och kopplingen till stadsnätets Core kan möjliggöras med 802.1Q inkapsling.

5.1 Frågeställning

De inledande frågor som vi ställde oss och som låg till grund för arbetet var

- Hur fungerar GPON?
- Hur fungerar VPLS?
- Hur kan man koppla ihop GPON till JEABs stadsnät, genom Cisco Systems 6500/7600-serien?
- Hur kan man koppla ihop GPON till JEABs stadsnät, genom Alcatel-Lucent 7450 ESS-1?

5.1.1 GPON

Denna del krävde mycket arbete eftersom det var en okänd teknik för oss innan arbetet påbörjades. Vi hade flera poänger med att förstå det, framförallt behövde vi kunskap om GPON för att kunna utreda hur man kan koppla ihop det med ett stadsnätet, dels behövde vi lära oss mer om GPON för att vi ville tillföra JEAB extra kunskap inom ämnet, och till sist ville vi öka vår egen förståelse för tekniken och hur den används.

Det fanns mycket information i form av ITU-rekommendationer om GPON, så det krävdes sållning och urval av text för att få rätt information och kunskap inom ämnet.

Detta delmål nåddes, vi har ökat vår egen och JEABs förståelse. Och även det viktigaste vilket var att kunna använda den kunskapen för fortsättningen av arbetet.

5.1.2 VPLS

Från början var tanken helt att VPLS skulle vara grunden för den implementation som vi undersökte. Mycket kunskap inom ämnet har fåtts genom att läsa rekommendationer (RFC-dokument) och information från Cisco Systems och Alcatel-Lucent. Även denna teknik hade vi inte stött på tidigare, och allteftersom vi fick ökad förståelse inom ämnet, förstod vi att VPLS inte skulle vara implementerat på det sätt vi och JEAB trodde från början. Endast delar av tekniken användes till slut. Men målet har ändå uppnåtts i att förståelsen har ökat både hos oss och hos företaget.

Den praktiska tillämpningen av VPLS i Jönköping Energi ABs nätverk finns snarare i en kopplingspunkt än övergripande över hela deras nät. Detta var något vi fick förstå efter en viss tid in i arbetet.

5.1.3 GPON med Cisco Systems hårdvara

Företaget hade köpt in ett Cisco Systems 7600 ES20 modulkort med tanken att det kunde koppla ihop deras GPON installation med stadsnätet via VPLS-tekniken. Det fanns två möjliga lösningar; Flexible q-in-q och MPBE. Till slut valdes MPBE på grund av dess förmåga att komma ihåg MAC-adresser (*MAC-learning*).

Denna hårdvara hade dock en funktionsbrist med DHCP option 82. Företaget krävde att den här funktionen kunde ske per subinterface men ES20-modulkortet klarade inte detta. När så var fallet, flyttades arbetsfokus till Alcatel-Lucents lösning istället eftersom DHCP option 82 per subinterface var ett krav.

I dagsläget nåddes inte målet att koppla ihop GPON och stadsnätet med Cisco Systems utrustning, men det viktiga här är att båda delarna av nätverket kopplas ihop med full funktionalitet enligt de krav som företaget har. Och det målet nåddes.

5.1.4 GPON med Alcatel-Lucenthårdvara

Företaget var tvunget att inrikta sitt fokus på Alcatel-Lucents 7450 ESS-1 när funktionsbristerna i Cisco Systems ES20-modulkort identifierades. Företagets krav på lösningen med Alcatel-Lucent hade precis samma krav som ställdes på det första förslaget.

Lösningen som användes till slut använde en del av VPLS-tekniken som Alcatel-Lucents 7450 ESS-1 erbjuder. En single-tag translation användes för att dölja kundernas VLAN från stadsnätet och tjänsteleveranören. Switchens QoS-funktioner användes för att tillfredställa kraven att styra trafiken på en per tjänst basis. DHCP option 82 kunde implementeras på det av företaget önskade sättet.

Inkapsling via 802.1Q användes både mot stadsnätet och GPONs OLT. Den här inkapslingsmetoden fungerar med båda nätverksdelar och möjliggör att VPLS-tekniken fungerar fullständigt som önskas.

5.2 Resultat

Med hänsyn till ändringar som har gjorts när det gäller val av hårdvara och hur stor andel vi hade på den praktiska sidan, kan vi ändå vara nöjda med resultatet. Det vi har lyckats mest med har varit en utökad förståelse av GPON och VPLS som vi kan visa för företaget både i denna rapport och muntligt.

Trots att vi inte kunde delta i den praktiska implementeringen av lösningen som utvalts, har vi haft möjlighet att granska lösningen och förklarat hur den fungerar. Eftersom implementationen och underhållet av ESS-1 7450 har delvis *outsourcats* till leverantören kan vår analys vara nyttig för företaget.

5.3 Framtid

Från början ville JEAB använda Cisco Systems-utrustning i den kopplingspunkt som har utretts. På grund av problem med dess implementation av DHCP option 82 var det inte möjligt att fortsätta arbetet med deras produkt, och Alcatel-Lucent ESS-1 7450 används istället. Om Cisco Systems förändrar sin implementation av DHCP option 82 kan det vara rekommenderat, ur en ekonomisk och administrativ aspekt, att återgå till den första lösningen med Cisco 7600 ES20-modulkort.

Den slutliga lösningen med Alcatel-Lucent ESS-1 är också skalbar, vilket i praktiken innebär att om GPON-nätverket byggs ut kraftigt, så finns det stora möjligheter att kunna hantera det på ett kostnadseffektivt och praktiskt sätt.

Från början av detta arbete var tanken att VPLS skulle ha en mycket avgörande funktion i Wetternet, genom att bygga upp ett VPLS-nätverk. Vi har däremot sett och förstått att VPLS som en helhet här inte är speciellt önskvärt, utan endast vissa funktioner och delar av tekniken. I den switchpunkt som undersökts används VPLS-funktioner internt, men fullskalig VPLS i hela nätverket är enligt vår åsikt inte önskvärt i just den här situationen.

När det gäller arbetet som helhet finns det utrymme för vidareutveckling även fastän våra mål är uppnådda. Detta arbete har fokuserat på lösningar över ett lager 2-stadnät men en fortsättning på detta som kan vara av intresse, är utredning av lager 3-stadsnät som omfattar t ex MPLS-tekniken. Tillsammans med den lösning som presenterats här, över ett lager 2-stadsnät, kan andra stadsnät få nytta av detta arbete om de har ett liknande syfte, att koppla ihop ett PON med sitt befintliga stadsnät.

6 Ordförklaringslista

Eftersom det finns mycket trebokstavsförkortningar och många andra ord som kan vara svåra att ha full koll på, följer här en kortfattad ordlista med förklaringar av begrepp och uttryck som kan vara bra att känna till i sammanhanget.

Broadcast	Sändning av ett paket till alla nätverksenheter inom en broadcastdomän.
Cell	Används inom ATM, och motsvarar *frame* inom Ethernet. De är 53 byte långa.
Frame	Ett lager 2 datapaket som kan vara av fast eller varierande längd.
Interface	En kopplingspunkt mellan en nätverksenhet och en annan nätverksenhet. Översätts ibland med *gränssnitt*.
IPSec	En grupp av protokoll som säkra upp Internet Protocol (IP-kommunikation) genom att autentisera och/eller kryptera varje IP-paket i en dataström.
Multicast	En teknik vars syfte är att leverera information till flera destinationer samtidigt med den mest effektiva strategin som är möjlig.
Native VLAN	Ett VLAN som för frames över en trunk utan vara inkapslade med 802.1q. De kan ha flera funktioner i ett switchat nätverk.
OSI	Open System Interconnection modellen är en sju-lager-modell som beskriver kommunikation och nätverksprotokolls-design.
Paket	Ett formaterat datablock som kan föras över ett datornätverk. Finns på lager 3 i OSI-modellen. Ett paket består av tre delar: *Header*, *Payload* och *Trailer*.
Unicast	Datatrafik som skickas från *en* enhet till endast *en* annan enhet.
VLAN	En metod som kan skapa flera logiska nätverk inom ett fysiskt nätverk. Därifrån kan policy specifikt till vissa VLAN skapas, oberoende av varandra. VLANet själv kan inkludera avdelningar, vissa typer av nätverksenheter (t ex skrivare) med mera.
VLL	Ett sätt att tillhandahålla Ethernet-baserad punkt-till-punkt-kommunikation över IP/MPLS-nätverk via PseudoWire-inkapsling.

7 Referenser

[1] *Six Lectures on Light by John Tyndall – Project Gutenberg* (2006) http://www.gutenberg.org/etext/14000 (Acc. 2007-04-05)

[2] *Optical fiber – Wikipedia, the free encyclopedia* (2007) http://en.wikipedia.org/wiki/Optical_fiber#History (Acc. 2007-04-04)

[3] Chomycz, Bob (1996) *Fiber Optic Installations: A Practical Guide* McGraw-Hill, ISBN 0-07-011635-0

[4] *FSAN – Full Service Area Network* - http://www.fsanweb.org/history.asp (2007) (Acc. 2007-04-02)

[5] *G.984.1 : Gigabit-capable Passive Optical Networks (GPON): General characteristics* (2006) http://www.itu.int/rec/T-REC-G.984.1/en (Acc. 2007-04-15)

[6] *G.984.1 : Gigabit-capable Passive Optical Networks (GPON): General characteristics* (2006) http://www.itu.int/rec/T-REC-G.984.1/en Clause 5.2 (Acc. 2007-04-15)

[7] *G.984.3 : Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification* http://www.itu.int/rec/T-REC-G.984.3/en Clause 5.4.1 (Acc. 2007-04-11)

[8] *G.984.3 : Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification* http://www.itu.int/rec/T-REC-G.984.3/en Clause 6.4.2 (Acc. 2007-04-11)

[9] *G.984.3 : Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification* http://www.itu.int/rec/T-REC-G.984.3/en (Acc. 2007-04-17)

[10] *G.984.2 : Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification* http://www.itu.int/rec/T-REC-G.984.2/en Clause 7-1 (Acc.2007-04-19)

[11] *G.984.2 : Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification* http://www.itu.int/rec/T-REC-G.984.2/en Appendix 1 Clause I3 (Acc.2007-04-19)

[12] *G.984.2 : Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification* http://www.itu.int/rec/T-REC-G.984.2/en (Acc.2007-04-19)

[13] Forouzan, Behrouz A. (2006) *TCP/IP Protocol Suite* McGraw-Hill, ISBN 0-07-296772-2

[14] *Virtual Private LAN Service – Wikipedia, the free encyclopedia* (2007) http://www.wikipedia.org/VPLS (Acc. 2007-04-30)

[15] Cisco Systems (2003), *CCNA 1 and 2* Cisco Press, ISBN 1-58713-110-2

[16] *Multiprotocol Label Switching – Wikipedia, the free encyclopedia* (2007) http://en.wikipedia.org/wiki/MPLS (Acc. 2007-05-03)

[17] Kumar, Manjunath, Kuri (2004) *Communication Networking, An analytical approach* Elsevier, ISBN 0-12-428751-4

[18] Shneyderman, Casati (2003) *Mobile VPN. Delivering advanced services in next generation wireless systems* Wiley, ISBN 0-471-21901-0

[19] *RFC3036* (2001) ftp://ftp.rfc-editor.org/in-notes/rfc3036.txt (Acc. 2007-05-02)

[20] *RFC4762* (2007) ftp://ftp.rfc-editor.org/in-notes/rfc4762.txt (Acc. 2007-05-18)

[21] *vpls_wp.pdf (application/pdf object)* (2004) http://www.cisco.com/warp/public/cc/so/cuso/sp/vpls_wp.pdf (Acc. 2007-05-19)

[22] *RFC4111* (2005) ftp://ftp.rfc-editor.org/in-notes/rfc4111.txt (Acc. 2007-04-13)

[23] *RFC4111* (2005) ftp://ftp.rfc-editor.org/in-notes/rfc4111.txt (Acc. 2007-04-19)

[24] *IP Packet: IEEE 802.1Q-in-Q VLAN Tag (QinQ)* (2004) http://www.ippacket.org/blog/archives/2004/08/ieee_8021q-in-q.html (Acc. 2007-04-01)

[25] *Configuring 802.1Q and Layer 2 Protocol Tunneling* (2002) http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/1219ea1/3550scg/swtunnel.htm (Acc. 2007-05-01)

[26] *T0411-VPLS_deployment-EN.pdf (application/pdf object)* (2004) http://www1.alcatel-lucent.com/doctypes/articlepaperlibrary/pdf/ATR2004Q4/T0411-VPLS_deployment-EN.pdf (Acc. 2007-05-01)

[27] *19531_Resilient_HVPLS_an.pdf (application/pdf object)* (2005) http://www1.alcatel-lucent.com/doctypes/opgapplicationbrochure/pdf/19531_Resilient_HVPLS_an.pdf (Acc. 2007-03-30) [x] 7450_ESS_OS_Svcs_Guide_R5.0-03-01_tcm417-1249981635.pdf

[28] *Cisco Catalyst 6500 Series/Cisco 7600 Series Sup Eng 720-3BXL* (2006) [Cisco Network Modules] http://www.cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet09186a008033a479.html (Acc. 2007-04-07)

[29] *Cisco 7600 Series Routers – Products and Services – Cisco Systems* (2006) http://www.cisco.com/en/US/products/hw/routers/ps368/index.html (Acc. 2007-04-07)

[30] *Cisco 7600-ES20 Ethernet Line Card Configuration Guide*
Configuring the Cisco 7600 Series Ethernet Services 20G Line Card (2006) http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html (Acc. 2007-04-25)

[31] 19531_*Resilient_HVPLS_an.pdf (application/pdf object)* (2005) http://www1.alcatel-lucent.com/doctypes/opgapplicationbrochure/pdf/19531_Resilient_HVPLS_an.pdf (Acc. 2007-03-30)

[32] *Keys to a successful VPLS deployment* http://www1.alcatel-lucent.com/doctypes/articlepaperlibrary/html/ATR2004Q4/ATR2004Q4A09_EN.jhtml;jsessionid=OYCABS0IGMQ1HLAWFRSHJHNMCYWGQTNS?_DARGS=/common/atr/DATR_table_of_contents.jhtml_A&_DAV=/com/en/appxml/articlepaperlibrary/keystosuccessfulvplsdeploymenttcm172102411635.jhtml (2007-04-29)

[33] *7450_ESS_OS_Svcs_Guide_R5.0-03-01_tcm417-1249981635.pdf* http://www1.alcatel-lucent.com/doctypes/opgdatasheet/pdf/7450_ESS_R5_v2ds.pdf (Acc. 2007-04-28)

[34] *Cisco 7600-ES20 Ethernet Line Card Configuration Guide*
Configuring the Cisco 7600 Series Ethernet Services 20G Line Card (2006) http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f3f97.html (Acc. 2007-04-28)

[35] *Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*
Configuring DHCP Snooping (2007)
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080435791.html (Acc. 2007-04-29)

8 Sökord

9 Bilagor

Bilaga 1 Kravspecifikation

Bilaga 2 Fullständig Alcatel-Lucent lösning (konfiguration)

Bilaga 1 Kravspecifikation

Angående Examensarbete våren 2007 för Kristoffer Pettersson och Robert Sales på Jönköping Energi AB

Jönköping Energi har ett stadsnät som spänner över Jönköping med omnejd. Det har nyligen också tillkommit en del i detta befintliga nät, med tekniken Gigabit Passive Optical Network (GPON). För att koppla ihop detta med det redan befintliga stadsnätet finns i dagsläget ett par olika alternativ, vilket i nuläget inte fungerar optimalt. Extra utrustning från olika leverantörer används och det fungerar ändå inte exakt som det ska. Vi vill kunna gruppera kunder genom VLAN eftersom vi använder oss av ett VLAN per kund längst ut i nätet. Detta ska sedan grupperas och annonseras till olika tjänsteleverantörer för leverans av internet.

Enligt den information som Cisco givit, ska det vara möjligt att använda sig av ett speciellt kort (7600-ES20-GE3C) som de har, till en Cisco 6500. Detta kort är troligen det första i Sverige och är mycket nytt. Detta ger att det inte finns jättemycket dokumentation än. Här skulle examensarbetets tyngdpunkt ligga. Det naturliga ledet av detta är att förstå och kunna implementera funktioner av Virtual Private LAN Service (VPLS).

För att detta ska vara möjligt krävs dels kunskap om GPON och det redan befintliga stadsnätet. Det finns också flera områden inom GPON där kunskap saknas inom företaget. Därför ser vi också en poäng i att det finns utredande karaktär på GPON i det kommande arbetet.

Som en del i implementering av den kopplingspunkt som finns mellan stadsnätet och GPON, finns Quality of Service (QoS) där man önskar kunna styra t ex hur mycket bandbredd en kund har etc. Också funktioner som: förhindra lokal kommunikation mellan användare, förhindra spoofing av IP/MAC-adresser (anti-spoofing filter) och DHCP snooping.

På företaget kommer också tester av IP-TV att genomföras. I mån av tid och utrymme kan det finnas nytta av att examensarbetarna finns med i detta. Inom detta område används Multicast.

Vi hoppas att studenterna och Jönköping Energi kommer få ömsesidig nytta av detta arbete som planeras.

Martin Blomdahl
Jönköping Energi

Tel. 036-108360, 0703-968778
Jönköping, 15 mars 2007

Bilaga 2 – Fullständig Alcatel-Lucent-konfiguration

Observera att VLAN-ID och vissa andra siffror så som lösenord har ändrats. Dock ingenting som påverkar funktionen hos konfigurationen.

```
# TiMOS-B-5.0.R2 both/hops ALCATEL ESS 7450 Copyright (c) 2000-2007 Alcatel-Lucent.
# All rights reserved. All use subject to applicable license agreements.
# Built on Tue Mar 27 10:51:08 PST 2007 by builder in /rel5.0/b1/R2/panos/main
# Generated THU MAY 10 11:16:55 2007 UTC

exit all
configure
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        name "trans-jkp-hf-04"
        persistence
            subscriber-mgmt
                location cf1:
            exit
        exit
        snmp
        exit
        time
            ntp
                server 172.31.10.41 prefer
                no shutdown
            exit
            sntp
                shutdown
            exit
            dst-zone CEST
                start last sunday march 02:00
                end last sunday october 03:00
            exit
            zone CET
        exit
        thresholds
            rmon
            exit
        exit
    exit
#--------------------------------------------------
echo "System Security Configuration"
#--------------------------------------------------
    system
        security
            telnet-server
            ftp-server
            management-access-filter
                default-action deny
                entry 10
                    description "mgmnt_wn"
                    src-ip 172.34.0.0/22
```

```
                action permit
            exit
        exit
        user "admin"
            password "jiJEKLdjfiensKD42WESRSJdDFaE" hash2
            access console ftp
            console
                member "administrative"
            exit
        exit
        user "drift"
            password "ZpkgIjgIGEl,BNdsDmnDGERDfdsqbddD" hash2
            access console
            console
                member "default"
                member "administrative"
            exit
        exit
        snmp
            community "community" r version both
            community "community" rw version both
        exit
        no per-peer-queuing
    exit
exit
#--------------------------------------------------
echo "Log Configuration"
#--------------------------------------------------
    log
        snmp-trap-group 1
            trap-target "v3" address 172.34.1.1 snmpv1 notify-community "community"
            trap-target "v4" address 172.34.1.1 snmpv2c notify-community "community"
        exit
        log-id 1
            from main security change
            to snmp
        exit
    exit
#--------------------------------------------------
echo "System Security Cpm Hw Filters Configuration"
#--------------------------------------------------
    system
        security
        exit
    exit
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom-fkm-b
        mda 1
            mda-type w23-1hy-jri-b
        exit
    exit
#--------------------------------------------------
echo "Port Configuration"
```

```
#--------------------------------------------------
    port 1/1/1
        description "lag-1_mot_cisco"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/2
        description "lag-1_mot_cisco"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/3
        shutdown
        ethernet
            mode access
            mtu 9212
        exit
    exit
    port 1/1/4
        shutdown
        ethernet
            mode access
            mtu 9212
        exit
    exit
    port 1/1/5
        shutdown
        ethernet
            mode access
            mtu 9212
        exit
    exit
    port 1/1/6
        shutdown
        ethernet
            mode access
            mtu 9212
        exit
    exit
    port 1/1/7
        shutdown
        ethernet
            mode access
            mtu 9212
        exit
    exit
```

```
    port 1/1/8
        description "PON-JKP-VF-01"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
        exit
        no shutdown
    exit
    port 1/1/9
        description "PON-GRN-GF-01"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
        exit
        no shutdown
    exit
    port 1/1/10
        description "PON-HVA-HF-01"
        ethernet
            mode access
            encap-type dot1q
            mtu 9212
        exit
        no shutdown
    exit
#--------------------------------------------------
echo "LAG Configuration"
#--------------------------------------------------
    lag 1
        mode access
        encap-type dot1q
        port 1/1/1
        port 1/1/2
        no shutdown
    exit
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        sap-ingress 2 create
            queue 1 create
                rate 2048
            exit
            queue 11 multipoint create
            exit
        exit
        sap-ingress 10 create
            queue 1 create
                rate 10000
            exit
            queue 11 multipoint create
            exit
        exit
        sap-ingress 30 create
```

```
            queue 1 create
               rate 30000
            exit
            queue 11 multipoint create
            exit
         exit
         sap-egress 2 create
            queue 1 create
               rate 2048
            exit
         exit
         sap-egress 10 create
            queue 1 create
               rate 10000
            exit
         exit
         sap-egress 30 create
            queue 1 create
               rate 30000
            exit
         exit
         sap-egress 100 create
            queue 1 create
               rate 100000
            exit
         exit
      exit
#--------------------------------------------------
echo "Filter Configuration"
#--------------------------------------------------
      filter
         ip-filter 10150 create
            description "TjLev-56.125.34.150"
            entry 1 create
               match
                  src-ip 56.125.34.150/32
               exit
               action forward
            exit
         exit
      exit
#--------------------------------------------------
echo "Management Router Configuration"
#--------------------------------------------------
      router management
      exit
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
      router
         interface "system"
         exit
      exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
```

```
service
    customer 1 create
        description "Default customer"
    exit
    customer 114 create
        description "TjLev"
    exit
    customer 614 create
        description "TjLev2"
    exit
    customer 3931 create
        description "TjLev3"
    exit
    customer 3831 create
        description "TjLev4"
    exit
    customer 2831create
        description "TjLev5"
    exit
    vpls 843 customer 614 create
        description "TjLev"
        split-horizon-group "843" residential-group create
        exit
        stp
            shutdown
        exit
        sap 1/1/8:2001 split-horizon-group "843" create
            ingress
                qos 10
            exit
            egress
                qos 10
            exit
            dhcp
                snoop
                lease-populate 2
                option
                    action replace
                    no circuit-id
                    no remote-id
                exit
                no shutdown
            exit
            anti-spoof ip-mac
        exit
        sap 1/1/8:2002 split-horizon-group "843" create
            ingress
                qos 10
            exit
            egress
                qos 10
            exit
            dhcp
                snoop
                lease-populate 2
                option
```

```
            action replace
            no circuit-id
            no remote-id
         exit
         no shutdown
      exit
      anti-spoof ip-mac
   exit
   sap 1/1/8:2003 split-horizon-group "843" create
      ingress
         qos 30
      exit
      egress
         qos 30
      exit
      dhcp
         snoop
         lease-populate 2
         option
            action replace
            no circuit-id
            no remote-id
         exit
         no shutdown
      exit
      anti-spoof ip-mac
   exit
   sap 1/1/8:2004 split-horizon-group "843" create
      ingress
         qos 10
      exit
      egress
         qos 10
      exit
      dhcp
         snoop
         lease-populate 2
         option
            action replace
            no circuit-id
            no remote-id
         exit
         no shutdown
      exit
      anti-spoof ip-mac
   exit
   sap 1/1/8:2006 split-horizon-group "843" create
      ingress
         qos 10
      exit
      egress
         qos 10
      exit
      dhcp
         snoop
         lease-populate 2
```

```
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/8:2008 split-horizon-group "843" create
    ingress
        qos 10
    exit
    egress
        qos 10
    exit
    dhcp
        snoop
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/8:2066 split-horizon-group "843" create
    ingress
        qos 10
    exit
    egress
        qos 10
    exit
    dhcp
        snoop
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/8:2067 split-horizon-group "843" create
    ingress
        qos 30
    exit
    egress
        qos 30
    exit
    dhcp
        snoop
```

```
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/8:2068 split-horizon-group "843" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/8:2069 split-horizon-group "843" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/8:2070 split-horizon-group "843" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
```

```
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/8:2071 split-horizon-group "843" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/8:2073 split-horizon-group "843" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/8:2077 split-horizon-group "843" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
```

```
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2180 split-horizon-group "843" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2181 split-horizon-group "843" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2182 split-horizon-group "843" create
        ingress
            qos 10
        exit
        egress
            qos 10
```

```
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2183 split-horizon-group "843" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2288 split-horizon-group "843" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2999 split-horizon-group "843" create
        ingress
            qos 10
        exit
        egress
```

```
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap lag-1:248 create
        dhcp
            snoop
            no shutdown
        exit
    exit
    no shutdown
exit
vpls 943 customer 614 create
    description "TjLev6"
    split-horizon-group "943" residential-group create
    exit
    stp
        shutdown
    exit
    sap lag-1:943 create
        dhcp
            snoop
            no shutdown
        exit
    exit
    no shutdown
exit
vpls 53 customer 614 create
    description "TjLev6"
    split-horizon-group "53" residential-group create
    exit
    stp
        shutdown
    exit
    sap lag-1:53 create
        dhcp
            snoop
            no shutdown
        exit
    exit
    no shutdown
exit
vpls 114 customer 114 create
    description "TjLev"
    split-horizon-group "114" residential-group create
    exit
```

```
        stp
            shutdown
        exit
        sap 1/1/8:2005 split-horizon-group "114" create
            ingress
                qos 10
                filter ip 10150
            exit
            egress
                qos 10
            exit
        exit
        sap lag-1:114 create
        exit
        no shutdown
    exit
    vpls 614 customer 614 create
        description "TjLev3"
        split-horizon-group "614" residential-group create
        exit
        stp
            shutdown
        exit
        sap lag-1:614 create
            dhcp
                snoop
                no shutdown
            exit
        exit
        no shutdown
    exit
    vpls 3931 customer 3931 create
        description "TjLev4"
        split-horizon-group "3931" residential-group create
        exit
        stp
            shutdown
        exit
        sap lag-1:3931 create
            dhcp
                snoop
                no shutdown
            exit
        exit
        no shutdown
    exit
    vpls 3423 customer 3423 create
        shutdown
        description "TjLev3"
        split-horizon-group "3423" residential-group create
        exit
        stp
            shutdown
        exit
        sap 1/1/8:2000 split-horizon-group "3423" create
            ingress
```

```
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
                vendor-specific-option
                    string "sub-,84925-3452"
                exit
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2076 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/8:2079 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 100
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
```

```
        anti-spoof ip-mac
    exit
    sap 1/1/9:2000 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
                vendor-specific-option
                    string "sub-8645786-7687956"
                exit
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/10:2000 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
                vendor-specific-option
                    string "sub-8986-89767897"
                exit
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/10:2001 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 100
        exit
        dhcp
            snoop
            lease-populate 2
```

```
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/10:2002 split-horizon-group "3423" create
    ingress
        qos 10
    exit
    egress
        qos 10
    exit
    dhcp
        snoop
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/10:2003 split-horizon-group "3423" create
    ingress
        qos 10
    exit
    egress
        qos 100
    exit
    dhcp
        snoop
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/10:2004 split-horizon-group "3423" create
    ingress
        qos 10
    exit
    egress
        qos 100
    exit
    dhcp
        snoop
```

```
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/10:2005 split-horizon-group "3423" create
    ingress
        qos 10
    exit
    egress
        qos 10
    exit
    dhcp
        snoop
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/10:2006 split-horizon-group "3423" create
    ingress
        qos 10
    exit
    egress
        qos 10
    exit
    dhcp
        snoop
        lease-populate 2
        option
            action replace
            no circuit-id
            no remote-id
        exit
        no shutdown
    exit
    anti-spoof ip-mac
exit
sap 1/1/10:2007 split-horizon-group "3423" create
    ingress
        qos 10
    exit
    egress
        qos 10
    exit
    dhcp
```

```
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/10:2008 split-horizon-group "3423" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/10:2010 split-horizon-group "3423" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
         dhcp
            snoop
            lease-populate 2
            option
               action replace
               no circuit-id
               no remote-id
            exit
            no shutdown
         exit
         anti-spoof ip-mac
      exit
      sap 1/1/10:2011 split-horizon-group "3423" create
         ingress
            qos 10
         exit
         egress
            qos 10
         exit
```

```
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/10:2012 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 10
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                no circuit-id
                no remote-id
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap 1/1/10:2020 split-horizon-group "3423" create
        ingress
            qos 10
        exit
        egress
            qos 100
        exit
        dhcp
            snoop
            lease-populate 2
            option
                action replace
                circuit-id
                no remote-id
                vendor-specific-option
                    string "test-3232"
                exit
            exit
            no shutdown
        exit
        anti-spoof ip-mac
    exit
    sap lag-1:3423 create
        dhcp
            snoop
```

```
                no shutdown
            exit
         exit
      exit
      vpls 3454 customer 3454 create
         shutdown
         split-horizon-group "3454" residential-group create
         exit
         stp
            shutdown
         exit
         sap lag-1:3454 create
            dhcp
               snoop
               no shutdown
            exit
         exit
      exit
   exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
   router
   exit
#--------------------------------------------------
echo "System Time NTP Configuration"
#--------------------------------------------------
   system
      time
         ntp
         exit
      exit
   exit

exit all
```