2009-12-01

Open Access Fiber to the Home Networking

Roger E. Timmerman
Brigham Young University - Provo

Open Access Fiber to the Home Networking

Roger Timmerman

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Joseph J. Ekstrom, Chair
Michael G. Bailey
Barry M. Lunt

School of Technology

Brigham Young University

December 2009

ABSTRACT

Open-Access Fiber-to-the-Home Networking

Roger Timmerman

School of Technology

Master of Science

The concept of open-access networks appeals to communities that want to invest in and improve their access to modern telecommunications services. By investing in, or building their own open-access telecommunications networks, communities can create an environment where several telecommunications service providers can co-exist on a common open-access infrastructure. This model promotes innovation and competition among several smaller service providers rather than having a monopoly or oligopoly from those companies that can afford the investment of infrastructure in the community.

This research provides an analysis of two large open-access fiber-to-the-home networks in Utah to determine a set of recommendations and best-practices for other communities that are considering building their own community networks. The networks analyzed in this research are the Utah Telecommunications Open Infrastructure Agency (UTOPIA) and the Provo City network (iProvo).

Keywords: open access, fiber-to-the-home, FTTH, municipal networks, triple play, UTOPIA, iProvo, fiber

ACKNOWLEDGMENTS

I would like to express love and appreciation to my dear wife, Jenny, and my wonderful kids, Emma and Ethan. The nature of working in the technical aspects of the telecommunications field requires many long hours, early morning maintenance windows, and late night emergency phone calls. They have always been supportive of the work that I do. I dedicate this work to my wonderful family.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

ADS – Access Distribution Switch is the aggregation switch that sits between the CPE and the DCS

AMI – Advanced Metering Infrastructure refers to systems and devices with capability to communicate with a central utility management system, including power meters, water meters, and gas meters.

CAT5E – A standard for twisted pair copper cabling typically used for Ethernet networking and telephone lines.

ClearQAM – QAM signals that are not encrypted, that can be viewed with any QAM-enabled TV without the use of an external set top box.

CoS – Class of Service is a 3 bit value in Ethernet frame headers that may be used for traffic classification and is commonly used to prioritize traffic.

CPE – Customer Premises Equipment – refers to the device provided by the service provider or network provider that serves as the demarcation point of services to the customer.

DCS – Distribution Core Switch is an aggregation switch used to aggregate ADS footprints back to the core distribution network. It sits between the ADS and the RCS

DHCP – Dynamic Host Configuration Protocol is a protocol defined in RFC 2131 for distribution of configuration information for IP clients.

DSL – Digital Subscriber Line is a set of point to point digital transmission standards that use common telephone lines to communicate.

DVR – Digital Video Recorder is a device that records video content for later viewing and for buffering paused live TV viewing.

Ethernet – A set of networking technologies that are standardized as IEEE 802.3.

FTTH – Fiber to the Home is a general term used for any fiber based network deployment that reaches customer homes with actual fiber lines.

FTTx – Fiber to the X refers to any of the last-mile fiber deployments where it be to the home, premises, curb, etc.

FTTP – Fiber to the Premises is a general term similar to FTTH, but differs in that it would include premises such as businesses, MDUs, or other locations that are not homes.

FTTC – Fiber to the Curb is a term that references fiber deployments that deliver fiber connectivity close to premises, but use some other infrastructure type to extend the network connectivity to the actual home or premises.

GPON – Gigabit-capable Passive Optical Network is a standard of passive optical networking that delivers 2.488 Gbps of downstream bandwidth and 1.244 Gbps of upstream bandwidth

HD – High Definition is a term that refers to video of resolutions of 704 x 480 (480p) and higher.

Headend – A facility that houses various equipment for the reception and signal of video signals for use in video distribution networks.

Hut – Term used by the iProvo and UTOPIA projects to describe large shelters that house electronics and other equipment.

IGMP – Internet Group Management Protocol is a network protocol for managing the memberships to various multicast streams.

IP – Internet Protocol is a layer-3 protocol for delivering datagrams across communications networks.

iProvo – Name of the Provo City fiber-to-the-home network

LAG – Link Aggregation Group

LNB – Low Noise Block is a device used to convert very high frequency satellite signals to lower frequencies that suffer from less loss as they traverse cabling.

LSP – Label Switched Path is a one-way path configured through an MPLS network.

MAC – Unique identifier issued in blocks to network device manufacturers. It is used to uniquely identify each device on a network and to populate switching and routing tables.

MPEG – Moving Picture Experts Group set standards for audio and video compression and transmission

MPEG-2 – Set of standards first introduced in 1995 that include standards for audio and video compression and transmission.

MPEG-4 – Set of standards first introduced in 1998 that includes Advanced Simple Profile and Advanced Video Coding

MPLS – Mutliprotocol Label Switching is a high performance switching protocol that creates layer-2 paths through a network with out of band management and redundancy features.

NEBS – Network Equipment Building System is a set of guidelines for telecommunications equipment that includes airflow, fire suppression, vibration resistance and other requirements.

OSPF – Open Shortest Path First is a routing protocol used in IP networks

PON – Passive Optical Network is a point-to-multipoint FTTx architecture that uses passive splitters to distribute the access

POTS – Plain old telephone service refers to typical analog phone service.

PPPoE – Point to Point Protocol over Ethernet is a protocol for establishing private connections between two end points - usually a customer and a service provider.

QAM - Quadrature Amplitude Modulation refers a method of modulating a signal used by cable service providers who offer digital video service.

QinQ – Is a the process of applying multiple levels of VLAN tags to Ethernet frames, enabling more flexible use of VLANs through a service provider network.

QoS – Quality of Service are mechanisms to prioritize and manage traffic flows through a network that include prioritization, queuing, and rate limiting.

RCS – Regional Core Switch is an aggregation switch that aggregates the DCS connections as well as ties to other core interconnections. All traffic

RSTP – Rapid Spanning Tree Protocol is used to provide redundancy and eliminate loops in Layer 2 networks

SFP – Small Form-factor Pluggable is a type of port that allows hot-pluggable transceivers.

SNMP – Simple Network Management Protocol is a set of standards used for configuration and monitoring of network devices.

STB – Set Top Box is a device connects to a customer television and provides the customer interface for accessing various TV channels, VOD content, and other features. It also decrypts and decodes the video streams received from the network.

Syslog – A standard for the sending, receiving, and handling of log messages from computers and network devices.

TLS – Transparent LAN Services refers to a point to point link that to the end user appears to be a LAN connection, but in reality may traverse a large network.

ToS – Type of Service is an 8 bit value used to designate priority, throughput, reliability and delay requested for the transfer of IP packets.

Triple Play – refers to the combination of Voice, Video, and Data services.

UPS – Uninterruptible Power Supply provides continuous power from utility or battery backup power.

UTOPIA – Utah Telecommunication Open Infrastructure Agency is a consortium of 14 cities in Utah that formed an agency to build and maintain a FTTH network in their cities.

VOD – Video on Demand is a term that references video that can be watched when requested by the client.

VOIP – Voice over IP refers to various methods and protocols for transporting voice traffic over IP encapsulated networks.

VLAN – Virtual Local Area Network is an identifier that separates Ethernet traffic into different broadcast domains.

1 INTRODUCTION

1.1 Background

Demand for higher-speed network access has been rapidly increasing and will continue to do so as new services become available that utilize high-speed networking. These services include high-definition television, high-definition video-on-demand, video conferencing, security services, high speed internet access, VOIP (voice over IP), home automation, remote access to media, telemedicine, remote education, remote workplace, etc. However, telecommunications companies in the United States have been slow to provide networks that are capable of delivering such services. This is due primarily to the high costs associated with building the necessary infrastructure to support these services. Telecommunications companies often benefit from somewhat monopolistic conditions in areas where they have built their own infrastructure. The lack of competition gives them little incentive to upgrade their networks despite the market demands or the desires of their customers. In many cases, they also offer higher speed services to only those areas that are most profitable or near existing infrastructure, leaving many without the option of purchasing upgraded services.

This situation has prompted several municipalities to build their own networks to meet those demands, offer services at lower prices, and make services equally available to all that live within the municipality. In Utah, several cities including Spanish Fork, Provo, and a consortium of 18 Utah cities known as the Utah Telecommunication Open Infrastructure Agency (UTOPIA)

decided to build municipally owned telecommunications networks. Spanish Fork was the first and built a fiber/coax hybrid network providing video and data services on their network. While the other cities were still in the early phases of their projects, the 2001 Municipal Cable Television and Public Telecommunications Services Act in Utah was passed. This act restricts municipalities to act only as a wholesaler of telecommunications services to retail service providers instead of selling services directly to consumers. Spanish Fork was grandfathered into the previous legislation allowing them to act as a retail provider. However, iProvo (Provo City's network) and UTOPIA were forced to adopt a wholesale model.

While this act was considered to be an obstacle to municipalities, Provo City and UTOPIA decided to proceed with their plans to build open access municipal networks, and to solicit service providers who would act as retail service providers on their networks. This model allows telecommunications companies to benefit from a municipal network instead of having to compete with it. The open access model also promotes greater competition between service providers as any given service provider can enter a market with an open access network without having to build their own network infrastructure.

The open access requirement for networks is increasingly being encouraged at a global level. Several networks in Europe have implemented open-access and regulators there continue to pressure closed networks to become open access. In April 2009, the Australian government announced their intent to build a country-wide, $43 billion open access network. [Adamski 2009] In July 2009, President Obama announced the availability of $7.2 billion in funds as part of the American Recovery and Reinvestment Act of 2009 to build out broadband infrastructure with a stated preference towards open access projects.[Adamski 2009]

1.2 Problem Statement

Open access fiber networks have requirements that are not typically supported by a traditional network. There is no existing technical standard or set of guidelines for how to build and operate an open access fiber network. By utilizing a fiber infrastructure combined with the capabilities of modern IEEE 802.1/802.3 Ethernet network design, a network can allow multiple service providers to share an open access municipal network. However, the municipality must design and manage their network in a way that meets both their own requirements for city services as well as those of various service providers that may operate on their network.

There are several aspects of network design that are affected by the additional complexity of the wholesale municipal network model. They include:

- Network Segmentation
- Traffic Management
- Automated Device Provisioning
- Monitoring
- Security

Each of these concepts must be carefully applied to the design of an open access network to allow for successful co-existence of competing service providers on the shared network infrastructure.

1.3 Research and Questions

There are only a few open access fiber networks currently operating in the United States. Unfortunately, they are known more for their own financial difficulties, than for the economic and technological benefits they have brought their communities. These first few networks

struggled with various technology limitations, interoperability issues, political influences, and legal challenges. Their struggles are frequently used to dissuade other communities from taking on similar ventures. However, after time, several of these networks have become operationally successful, despite their difficult beginnings.

It is the intent of this research to identify "best practices" and other recommendations for the design and implementation of open access fiber networks. It is hoped that these results will enable communities that are considering or in the early stages to benefit from the lessons learned by their predecessors. This will be accomplished by analyzing the design and implementation of the UTOPIA and iProvo networks. The UTOPIA and iProvo networks represent two of the largest open access fiber networks in the United States.

1.4 Justification

As of this research, very little documentation is available that details the design and management of an open access network with multiple service providers providing triple-play services (video, voice, and data). UTOPIA and Provo are among the first communities to attempt to do so on a large scale within the United States. The results of this research are needed by other municipalities or telecommunications providers that are considering, or are in the early stages of building open access fiber networks. As other municipalities contemplate building their own open-access network, it is hoped that this research will allow them to benefit from the experiences, both good and bad, of the iProvo and UTOPIA networks.

1.5 Methodology

The intent of this research is to develop best practices and recommendations building and managing open access fiber networks in a manner that is scalable and manageable. To accomplish this, the research will include case studies of the iProvo and UTOPIA networks. By examining the practices of these networks and comparing them to existing documentation, this research will produce a set of design and operational guidelines that other open access networks may follow.

1.6 Assumptions

There are several network designs and network technologies that can be used to deliver services in an open access fiber network environment. The iProvo and UTOPIA networks are Fiber to the Home (FTTH) designs using active Ethernet star topology for the last mile connection to the customer. This design is often referred to as a Point to Point (P2P) type architecture. However, there are many other types of network designs that may theoretically support an open access style network. Some examples of these are fiber-coax hybrid networks and various types of passive optical networks (PON). While these other models will be mentioned occasionally in this research, it is not the intent of this research to prove one design method over the other. Both the iProvo and UTOPIA networks were built based on active Ethernet star over fiber architecture for the last mile connection to the customer. For this research we will only discuss open-access networking based on an active Ethernet star topology.

1.7 Delimitations

This research will not attempt to establish recommendations for all aspects of building a fiber to the home network. In any case where a fiber to the home network is being considered, a feasibility study should first be conducted to identify the costs and market conditions for delivering telecommunications services in the proposed area. Environmental conditions, terrain, existing infrastructure, market competition, and political factors may all affect the strategy used for delivering a fiber to the home network.

Depending on the specific implementation being considered, the network requirements may vary widely. For example, as of this research, the iProvo network has a video service that includes approximately 260 channels of digital television. About 20 of those channels are high-definition (HD) channels each requiring about 16 Mbps of bandwidth. The standard definition channels require about 4Mbps per channel. The UTOPIA network currently has two co-existing video services, each with approximately 280 channels. About 60 of these channels are HD. Of all of the channels, there is a mix of MPEG-2 and MPEG-4 encoded video feeds varying anywhere from 2 Mbps to about 20 Mbps. Any given IPTV service is likely to have a different mix of channels, with different bandwidth requirements depending on that providers IPTV strategy. Also, the iProvo network deals more closely with the city entities and provides several specialized services across its network that may be unique to Provo City including the following:

- Private multi-point business connections
- Public school system
- City office interconnections
- Energy department automated meter reading

- City traffic cameras
- City water SCADA

Any given municipality will have to take into consideration its own throughput requirements and priorities and design the network to meet those requirements.

This research does not attempt to identify specific products as solutions. The iProvo network is primarily based on Ciena (formerly World Wide Packets) equipment that supports standard Ethernet protocols. The UTOPIA network is based primarily on Alcatel-Lucent and Riverstone (now part of Alcatel-Lucent) equipment. Although this research will attempt to make conclusions that apply to all networking technologies, it is possible that certain features available through Ciena and/or Alcatel-Lucent equipment may not be available on other manufacturer's devices. This is also true for features on other manufacturer's devices that may not be available on Ciena and/or Alcatel-Lucent equipment. However, this research does identify minimal features required by the network equipment for each type of service.

2 REVIEW OF LITERATURE

2.1 Introduction

The open access network is a new approach to delivering telecommunications services. There is little existing literature that specifically targets this type of network. However, being that open access networks are likely to be based on existing networking technologies, there is value in reviewing standard networking techniques and designs that are used to create the open access network model.

2.2 Justification

Why do municipalities enter the telecommunications industry? Many studies have been done to determine the needs for, and results of, municipally provided telecommunications networks. In many ways the debate of whether municipalities should ever enter into markets where private enterprises exist, is a political one. Many feel that municipalities have unfair advantages because of access to public resources such as easements, real estate, pole attachment rights, etc. They also benefit from their tax-exempt status, access to public bond rates, and potential subsidies from other city operations. However, others argue that for those same reasons, municipalities should enter the telecommunications business and treat it like any other publicly provided utility.

In the article, “A Historical, Economic, and Legal Analysis of Municipal Ownership of the Information Highway,” Steven Carlson lists several benefits for municipalities to build broadband infrastructure networks. They include the following:

1. Better Cable Television, Local Telephone, and Internet Service
2. Improved Efficiency in Electricity Distribution
3. Longer Lifetimes of Streets
4. Improved Governance
5. Magnets for Attracting Business

Carlson also compares municipal broadband projects to early municipal electric utility projects. Electricity was originally considered to be a novelty that over time evolved into a service that was critical for any community. Private companies would not invest in electrical infrastructure for rural or otherwise less-profitable areas. They would also use monopolistic control of their areas to artificially inflate the prices. Municipalities stepped in and formed their own electric utilities. From 1894 to 1925, fifty or more municipal electric utilities were formed every year. These projects were costly, and faced similar opposition by private companies that municipal fiber projects face today. However, they were hugely successful at lowering costs for electrical service and providing services where private industry would not. During the presidential campaign of 1932, Franklin Delano Roosevelt proclaimed the following:

> Where a community, or a city, or a county, or a district, is not satisfied with the service rendered or the rates charged by the private utility, it has the undeniable right as one of its functions of government... to set up... its own governmentally owned and operated service... The very fact that a community can, by vote of the electorate, create a yardstick of its own, will, in most cases, guarantee good service and low rates to the population. I might call the right of the people to own and operate their own utility a "birch rod in the cupboard,' to be taken out and used only when the child gets beyond the point where more scolding does any good. [Carlson 1999]

Provo City's interest in entering the cable television market stemmed from TCI's unwillingness to provide cable television services to areas other than the more prosperous areas of Provo. TCI's only competitor in Provo at the time, Provo Cable, was at the time entering bankruptcy. To prevent TCI (acquired by AT&T and later sold to Comcast) from obtaining a complete monopoly on cable television in Provo, Provo City stepped in and acquired Provo Cable. Provo City then built a fiber optic network with the intent of connecting the electrical substations, schools, fire stations, and other city services. [Cherry 2006]

Provo City leaders felt that its residents were not being offered adequate services from the incumbent telecommunications providers. With a municipally owned cable television network, citywide fiber network, and electric utility, Provo was well positioned for expanding to a triple play Fiber-to-the-home network.

2.3 Fiber Infrastructure

Several methods exist for delivering high-speed telecommunications services to consumers. Coaxial cable, telephone lines, wireless, fiber and combinations of those are all commonly used. However, only fiber is future-proof. All other mediums suffer from bandwidth limitations, interference, distance limitations, and other problems. The following image shows the relative throughputs per neighborhood footprint of various network mediums.

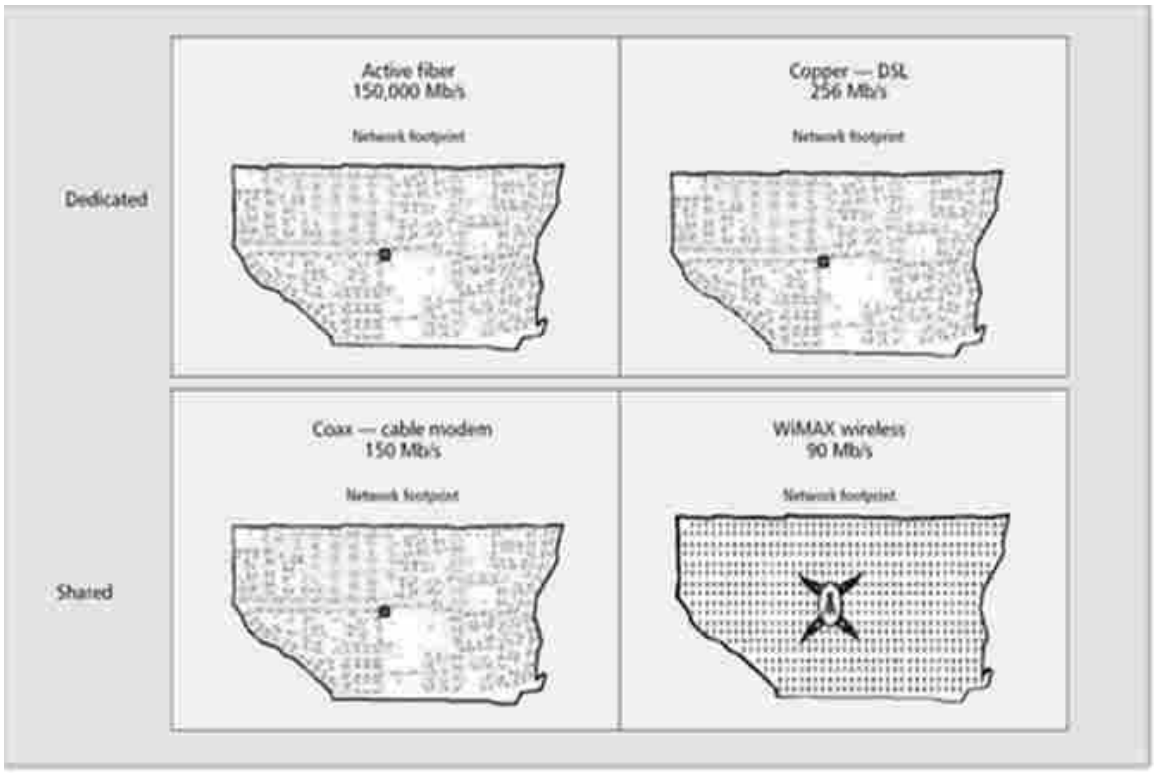


Figure 1 – Symmetric Bandwidth Capacity per Footprint by Transport Medium [Moerman 2005]

The figure above is based on fiber limited at 100 Mbps per fiber. However, the bandwidth of fiber transmission is only truly limited by the capabilities of the interfaces put at the ends of the fiber. As the needs of high speed networking increase, the interfaces on fiber connections can be upgraded to meet those needs without replacing the fiber. This figure was based on the original UTOPIA design. However, since that time, many of the UTOPIA areas have been upgraded to devices with GigE capable interfaces, increasing the available bandwidth ten-fold. The other mediums represented in this diagram, have also improved somewhat over recent years with Docsis 3.0 for cable and VDSL for twisted copper, but the relative increases are significantly less than for fiber.

In a 2005 report by Technology Futures Inc., they predict that "by 2010, U.S. broadband penetration of 75% is likely, and 10% to 20% of U.S. households will subscribe to very high-

speed-broadband. In the process, most of the local exchange carrier's current investment in copper cable will be made obsolete." Fiber is the only network medium that can meet future demands. The only reason that fiber deployments are not more common is because of the high costs associated with them. Fiber is much more fragile, must be physically managed to maintain proper bend radiuses, and requires expensive splicing equipment to make connections. However, the costs of fiber have been rapidly falling resulting in it becoming the preferred medium for new telecommunications infrastructure.

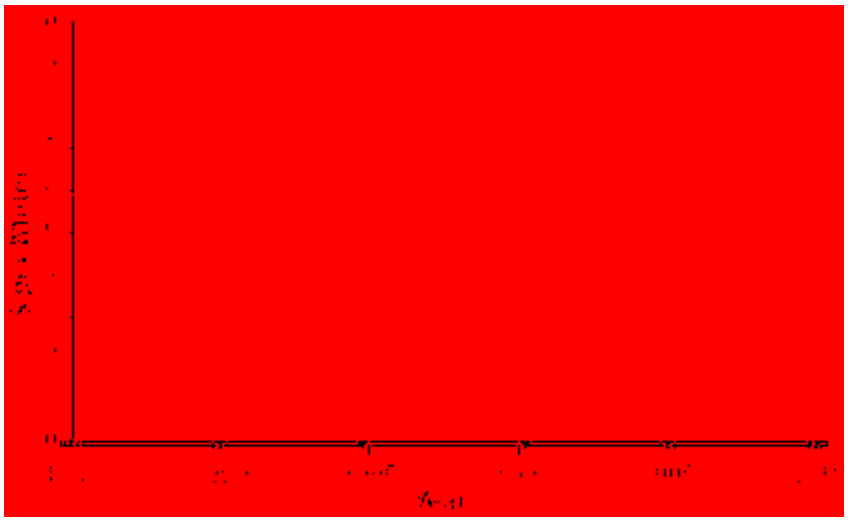


Figure 2 - Cost of a 48-Fiber Cable Curve [WWP 2005]

Over the same time period, the price of copper has increased significantly. Fiber deployments continue to cost more than copper deployments. However, it is expected that fiber will eventually rival copper in cost and perhaps become less expensive as these trends continue. Currently, the justification of fiber over copper is based on its capacity, longevity, and maintenance costs, but may someday become a lower cost alternative to copper.

2.4 Open Access

While Provo and UTOPIA are required to wholesale services to retail service providers who then sell those services directly to the consumer, they are not required to have an open access model where several service providers operate simultaneously on the network. They could simply choose a single service provider to retail the network services to consumers. This model does, however, present a political problem. This approach would simply seem to replace one monopoly with another, and to subsidize the new monopoly with public funds. However, a fully open access that allows multiple simultaneous service providers addresses the concern that municipalities are stifling competition and competing unfairly.

A municipal open access network can be compared to a municipal airport. Any city of significant size has a great need of an airport. It is necessary both to the business operations and needs of the residents of a city. A large city without an airport would suffer greatly. Any individual airline or private business does not typically have the resources to build and operate an airport that could serve the needs of a large city, nor would they be able to offer an adequate number of routes and services to satisfy the needs of the city. It would be extremely wasteful and costly if each airline were to purchase land, build terminals, build runways, operate traffic control systems, etc. Instead, it makes sense for a city to invest in the building and operations of an airport. Several airlines can then make use of the same runways, terminals, and other systems as coordinated by the municipally owned airport. The result is that competition is encouraged and there is great economic benefit to the city because of greater availability of flights, lower prices, and increased economic activity. [Lin 2006]

Similarly, an open access network can allow multiple service providers to operate and compete, while operating on a municipally owned and operated network. With the high costs

associated with building a fiber network, it is extremely cost prohibitive for any fiber network provider to over-build a network in the area of a competing fiber network provider. However, service providers who would otherwise be unwilling to compete in a given market because of the huge upfront infrastructure costs, would be able to compete by avoiding the upfront costs of building their own network by using the open access municipal network.

In July of 2009, the FCC commissioned the Harvard University's Berkman Center for Internet and Society to conduct a study about broadband deployment and usage throughout the world. Their research examined the affect of open access network policies on various countries that are considered to be leaders in broadband adoption.

> Our most surprising and significant finding is that "open access" policies—unbundling, bitstream access, collocation requirements, wholesaling, and/or functional separation—are almost universally understood as having played a core role in the first generation transition to broadband in most of the high performing countries; that they now play a core role in planning for the next generation transition; and that the positive impact of such policies is strongly supported by the evidence of the first generation broadband transition.

In the statement above, the first generation transition refers to the transition from dial up to broadband services, with the next generation transition begin the migration to higher speed broadband in the range of 40-50 Mbps or more per connection.

> The theory underlying open access is that the more competitive consumer broadband markets that emerge from this more competitive environment will deliver higher capacity, at lower prices, to more of the population. The competing theory, that underlies the FCC's decision early in this decade not to impose open access for broadband infrastructure, is that forcing incumbents to lease their network to competitors will undermine that industry's incentives to invest in higher capacity networks to begin with, and without that investment, the desired outcomes will not materialize. [Berkman 2009]

The theory that prevails in the study is that the lack of open access requirements in the United States has caused it to fall behind relative to other countries that have adopted open access policies. The study itself is evidence that the FCC is reconsidering its policies regarding open

access and looking for greater justification to impose open access requirements in the United States.

2.5 Network Segmentation

Simply having a fiber network in place with the adequate bandwidth to support services does not guarantee that services on that network will work properly. In fact, unless carefully designed controls are put in place, the services on a network are most likely to fail. One aspect of network design that must be considered is that of network segmentation. Network segmentation is the idea of dividing up a network logically into smaller pieces. This research is concerned with large municipal networks that may involve tens of thousands, hundreds of thousands, or even millions of network nodes. Common Ethernet and Internet Protocol (IP) networking have limitations that would cause problems for having so many nodes on a network.

Internet Protocol uses broadcast traffic to identify other devices and for automatic configuration of devices or Dynamic Host Configuration Protocol (DHCP). Broadcast traffic spans the entire network segment arriving at every device within that segment. As the number of network devices increases on a single network segment, the amount of broadcast traffic at each node receives increases resulting in unwanted network congestion. As each device receives this traffic, it must process it which can result in a negative performance if too much unnecessary traffic is received. Cisco Systems notes that in a controlled environment, they have observed that a network with 100 broadcasts per second will have measurable system degradation. [Cisco Systems 2006] This is just one vulnerability of a large network involving thousands or more customers. Therefore, it is necessary to carefully design mechanisms that protect the services delivered to each individual customer.

2.6 Traffic Prioritization

The network operator must ensure that the various types of traffic are prioritized appropriately on the network to avoid data loss for critical services at the expense of less critical services. For example, a single Ethernet frame lost in a voice conversation may be noticed as audible noise or a momentary loss of sound. A lost Ethernet frame of video service may cause freezing of the video image or corruption of the image. However, a lost Ethernet frame of Internet data will probably be re-sent and not be noticed at all by the end user. Therefore, it is important to separate the different types of traffic and to prioritize them according to their requirements. This type of prioritization is known as Quality of Service (QoS). QoS can be implemented using several different methods. The IEEE 802.1p standard (published as part of the IEEE 802.1D standard) specifies that the Ethernet address frame may include a VLAN (Virtual Local Area Network) tag that specifies a priority value. An Ethernet frame with a VLAN specified may take the following structure.

Table 1 - Structure of Ethernet Packet

# of Bytes	6	6	2	4	46-1500
Description	Destination MAC	Source MAC	Type	VLAN Tag	Data

The VLAN tag portion of an Ethernet frame has the following structure:

Table 2 - Structure of VLAN Tag

# of Bits	3	1	12	16
Description	Priority	CFI	ID	Ethernet Type/Length

The Priority field, or Class of Service (CoS), can contain any value 0-7. This value can be used by layer-2 switches to prioritize, rate limit, and queue traffic. [IEEE 802.1D standard]

These CoS priorities can be used to distinguish different services and ensure that they operate properly. The following diagram shows a scenario involving DSL connections where Virtual Circuits (VC) are used to separate services from customer premises to the DSL termination (GE DSLAM) where it interfaces with Ethernet equipment. Then at the Ethernet equipment the ports are 802.1Q encapsulated. This encapsulation may include the CoS priority being set which will enable upstream aggregation switches to ensure proper QoS.

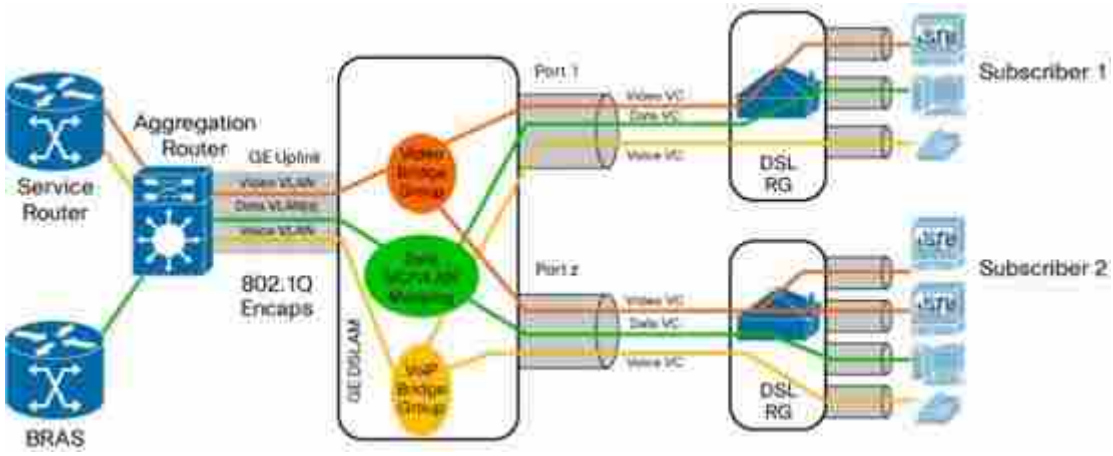


Figure 3 - Aggregation and Access Example [Cisco Systems - Optimizing Video 2006]

Diffserv is another method for providing QoS. A Cisco whitepaper titled, "Diffserv – The Scalable End-to-end Quality of Service Model" suggests a combination of Diffserv and IntServ mechanisms for providing QoS [Cisco Systems – Diffserv 2006] Diffserv mechanisms classify flows and set precedence bits in the IP packet header. These values are then used throughout the network to prioritize packet forwarding and in the case of congestion, may drop packets with a lower priority. IntServ is another method of QoS that functions differently than

Diffserv in that it specifies traffic requirements and signals the reservation of the transmission path before the traffic is sent. The conclusion of this whitepaper is not a single approach to QoS but rather that all aspects of the network must be aware of a QoS design and participate at various levels and with various methods.

2.7 MPLS

Multiprotocol Label Switching (MPLS) is increasingly becoming the preferred mechanism for providing redundancy, traffic engineering, and virtual circuit functionalities for Metropolitan Area Networks. A Metropolitan Area Network is defined as a network that extends beyond the distances of a Local Area Network (LAN) but is contained within the same Metropolitan area (approximately 120km). Almost all FTTH networks fall into this category. However, a FTTH network is type of MAN that is focused on connecting very high percentage of the premises in its coverage area as opposed to typical MANs that may be business-focused, connecting only those premises requiring dedicated circuits and other functionalities provided by the MPLS protocol. While the requirements for a FTTH deployment may not require it, having MPLS functionality gives the FTTH network the flexibility to provide advanced business class services including traffic engineering, classes of service (CoS), virtual private networks (VPNs), virtual leased lines (VLLs), and virtual private LAN services (VPLS), which can be far more profitable than typical residential type connections. [Tan 2004]

2.8 Access Layer Topology

The decision of whether to deploy a Homerun, GPON, or an Active-Ethernet based network must be made early in the process of designing a FTTH network. Any of these designs

are technically capable of delivering next-generation services in an open-access environment, but each has its own advantages and disadvantages. It is not the intent of this research to determine which is better than the other, and this will not be addressed in detail because only Active-Ethernet networks were included in the case studies of this research. However, any community considering a FTTH network should understand the various topology types and choose the one that best fits their needs.

In an Occam Networks whitepaper entitled "Fiber Drivers in Today's Access Networks," there is a cost analysis of the various network topologies for FTTH. The first, most basic topology is to simply run a dedicated fiber to each home from the central office. This topology requires significantly more fiber than other approaches. The construction work is nearly the same, and the costs of aggregation cabinets or huts are eliminated. For high density areas, the costs are actually less than for Active Ethernet, and not significantly greater than those of GPON. For medium and low density areas, the costs can be significantly higher. Another major limitation with this design is that for medium and lower density areas, the very long lengths of fiber cable expose the network to longer spans that are vulnerable to fiber cuts, without any redundancy.

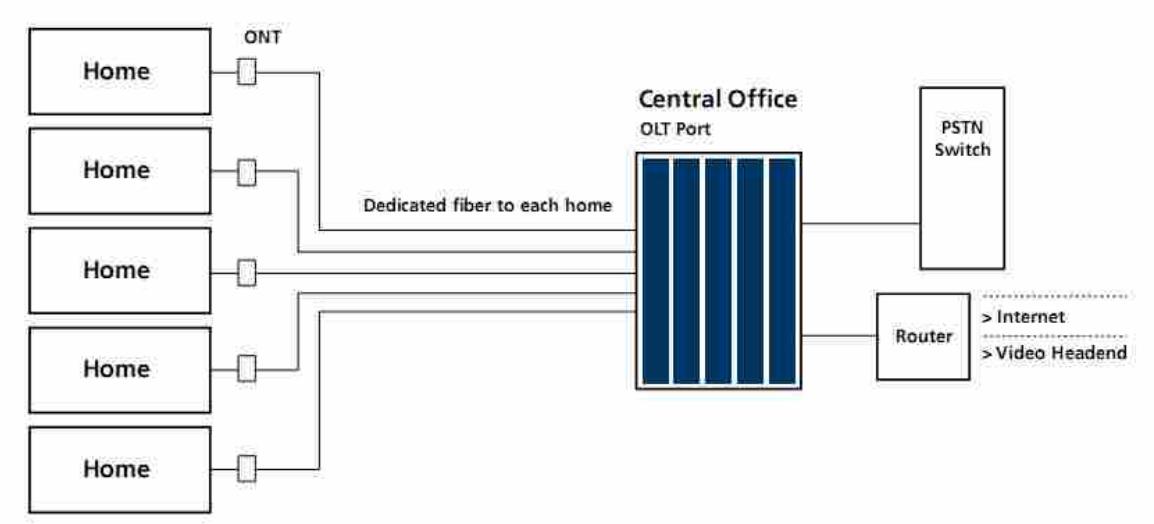


Figure 4 - Home Run Fiber Architecture [Occam 2005]

The next topology considered in the Occam whitepaper is Active Ethernet Star topology. Both the UTOPIA networks and the iProvo network implemented forms of Active Ethernet Star in their networks. This design provides for redundancy out to the customer aggregation sites (cabinets or huts). It also significantly reduces the amount of fiber needed that ties back to the central office. However, each cabinet or hut has the burden of maintaining active electronics which require electricity and cooling.

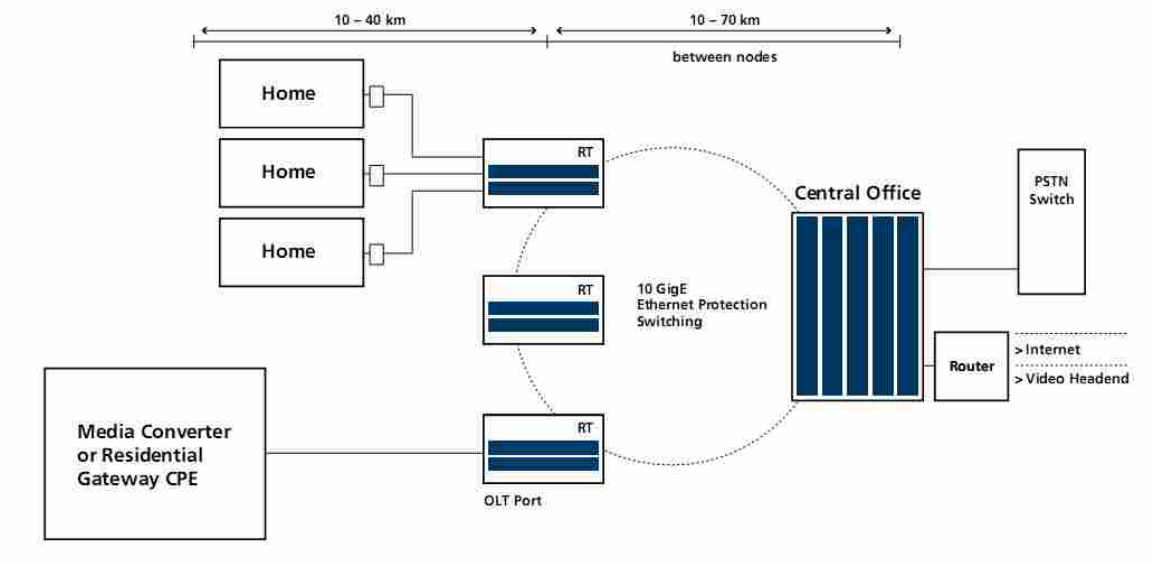


Figure 5 – Active Ethernet FTTH Topology [Occam 2005]

The third topology type discussed in the whitepaper is PON. This topology uses passive optical splitters at the access layer where the customer connections are aggregated. This allows for smaller, lower cost cabinets that do not require active electronics or cooling. However, its disadvantages include a lack of redundancy from the splitters back to the central office. It is also less flexible for adding additional customers or changing the design of the access layer network once it has been deployed. Also, the bandwidth available from each Optical Line Terminal (OLT) is shared among all of the customers in an area and relies on oversubscription to deliver bandwidth competitive to a 100 Mbps Active Ethernet topology.

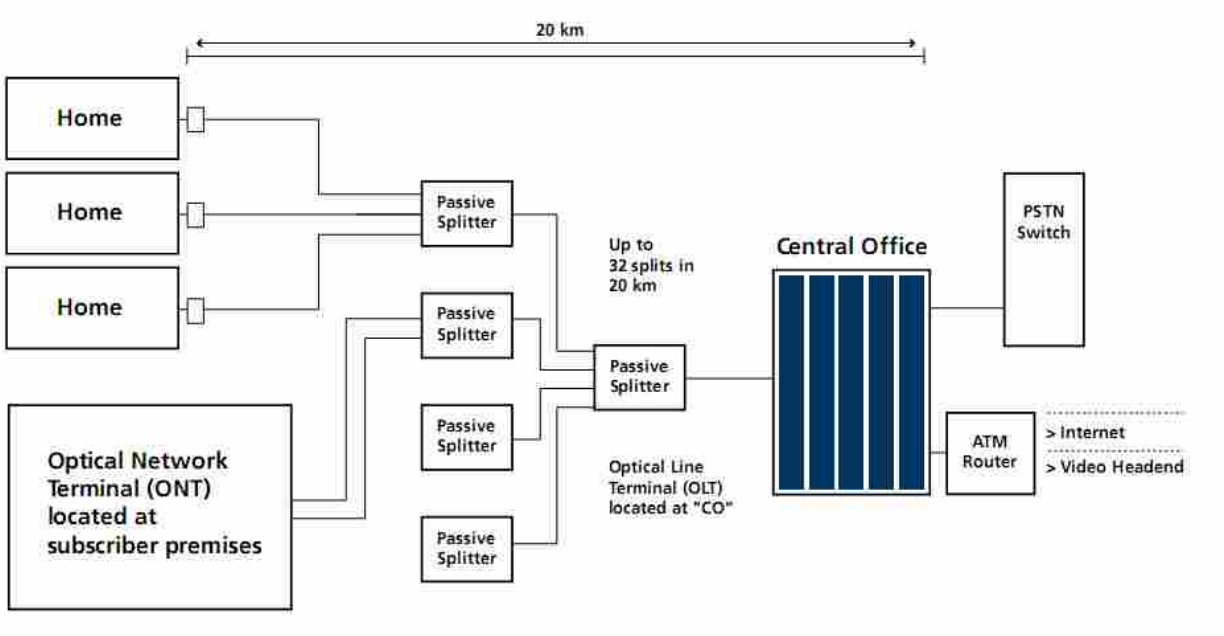


Figure 6 - PON FTTH Topology [Occam, 2005]

For urban deployments, the costs are relatively similar for any of the various topologies. However, as the deployment becomes more rural, the costs for Active Ethernet Star and PON become very similar whereas a Home Run deployment quickly becomes cost prohibitive.

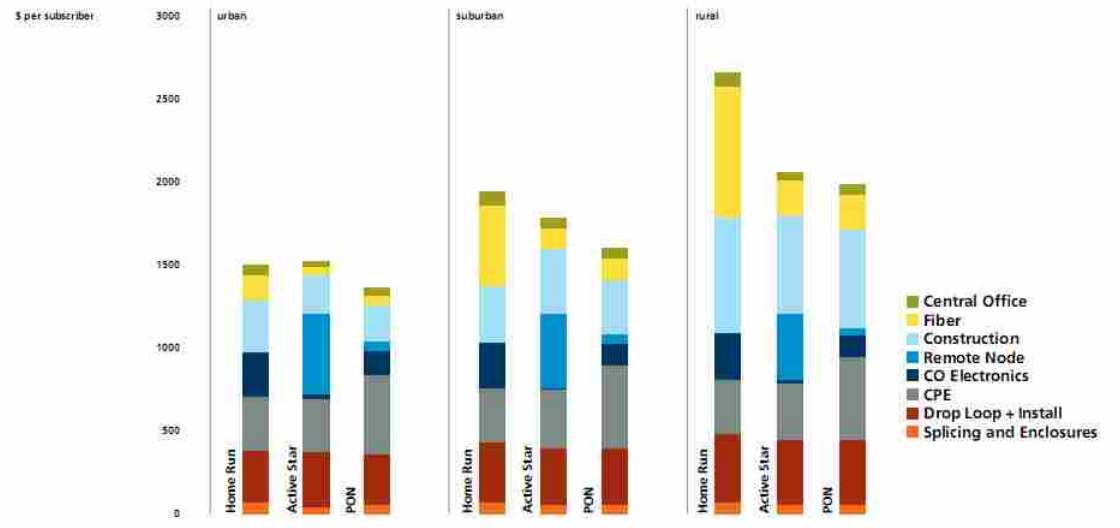


Figure 7 - Installation Costs for Different Topologies [Occam, 2005]

The figure above shows the overall relative costs for the various topology types. The UTOPIA and iProvo networks are primarily suburban type areas, with a small mix of urban and rural areas. Therefore, the analysis of those networks will fall primarily within the cost structure identified above as suburban.

2.9 Trends

Today's telecommunications providers typically offer any combination of data (Internet), video, and telephone services. While the types of services have not significantly changed in the past ten years, the requirements of each individual service have changed significantly.

	2000	2004	2008
Typical Data Requirements	56k dial-up modem to 128k DSL	4-8 Mbps broadband	20–30 Mbps broadband
Broadcast TV Requirements	40 channels analog 2 TVs per home	150 channels digital 3.8 Mbps per TV 2 TVs per home	250 channels digital 10–20 Mbps per HDTV 3 TVs per home
On-Demand Requirements	None	Music downloads/ online gaming	Music downloads/ online gaming HD Video On Demand (10-20 Mbps per subscriber) Place Shifting Holographic
Bandwidth Requirements per Home	128k + Cable TV	10-20 Mbps	100-120 Mbps

Figure 8 - Changing Requirements for Triple-play Over Time [Occam 2005]

The trends of the figure above suggest that today's services require 100-120 Mbps of total bandwidth per home. While no specific prediction is given for periods beyond 2008, the trend suggests that significantly more bandwidth may be required to each home in the future.

In addition to its analysis of open access benefits, the 2009 study from the Harvard University's Berkman Center for Internet and Society also analyzes trends of broadband infrastructure from several countries. Japan, considered to be the world leader in broadband technology, speed, and price, is also ahead of other countries in its adoption of FTTH availability. The following figure shows how fiber in Japan has actually overtaken the next most popular broadband technology (DSL) and continues to grow at a rapid pace.

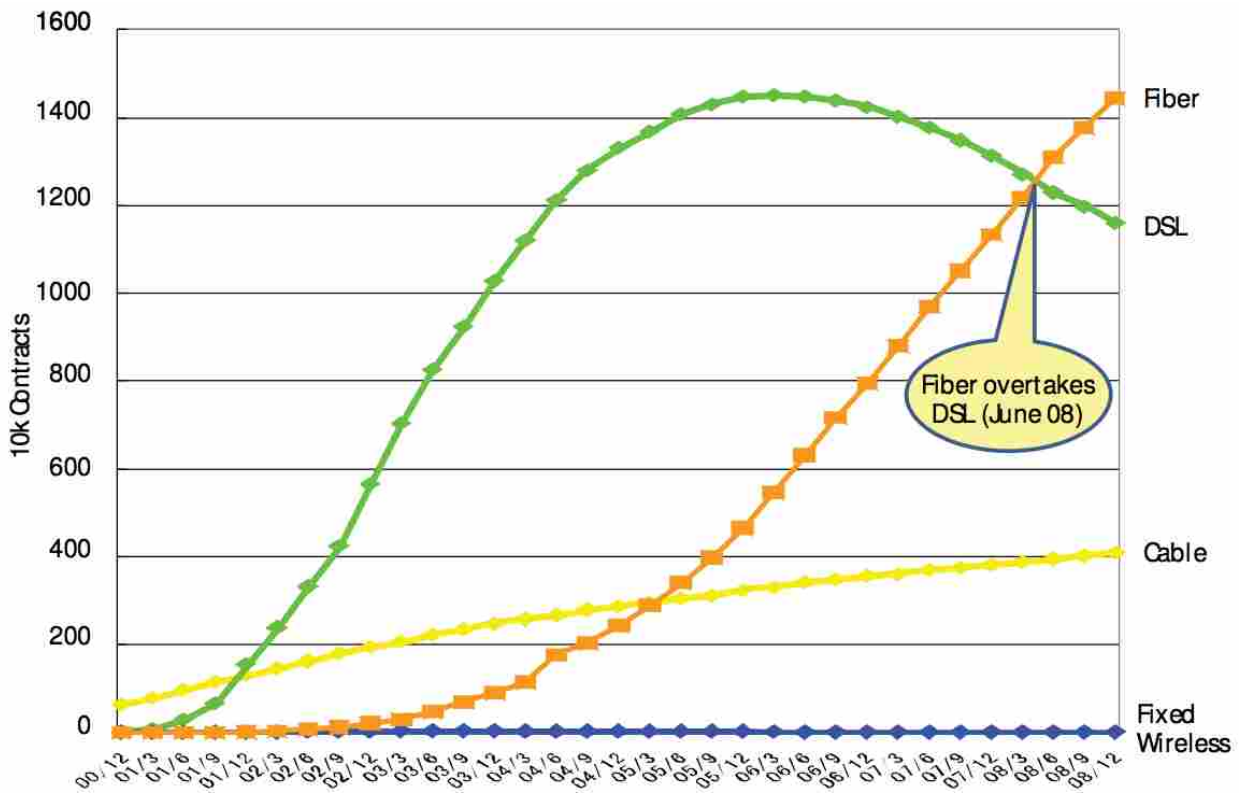


Figure 9 - Japan Market Share by Technology [Berkman 2009]

2.10 Review of Literature Conclusions

Telecommunications requirements are increasing at a rapid pace. Incumbent providers in the United States insist that they are keeping up with consumer demand. However, other countries have demonstrated that consumers desire and consume more bandwidth when it is available. The most common connectivity types in the United States are DSL, cable, and wireless. These infrastructure types may be adequate for the current market, but will not be able to keep up with increasing consumer demands. Fiber connectivity is the only infrastructure type that is known to be capable of supporting long-term telecommunications requirements.

Whether it is subsidized or mandated by government, it also seems that open access may someday become the standard for the telecommunications industry. Existing research suggests the likelihood of the increase of open access fiber networks. While there is much research regarding the technologies and justification of open access fiber networks, very little information is available regarding the actual implementation of this type of network. The two examples of open access networks being researched (UTOPIA and iProvo), took different approaches to many aspects of their designs and each faced various technical and operational struggles. Being some of the first to build this type of network, there was little reference material regarding how to design their networks. For this reason, this research will collect information from their experiences and decisions to make recommendations for future open access fiber networks.

3 RESEARCH

3.1 Introduction

The iProvo and UTOPIA networks were both built to provide open-access, FTTH connectivity throughout their communities. However, there are many differences in how the two networks approached the same objective. The following is a collection of information from both networks on how they approached the various aspects of designing an open-access FTTH network.

3.2 Physical Infrastructure

The most costly and time-consuming parts of a FTTH project are the materials and labor to get the fiber built throughout the city and to each individual premises. Provo City and UTOPIA both used public easements and ran their fiber lines in parallel to other telecommunications lines. For distribution rings, these typically run along utility poles below the electrical service lines. However, the fiber that runs through each neighborhood to each premises is installed with whatever mix of overhead (utility pole attached) or underground (through existing or new conduit) methods are most appropriate for the area. This part of the design must always be engineered specifically for the neighborhood in question. However, several aspects of the design can be based on the requirements related to the size of the footprint, support systems, electronics, and available resources.

3.2.1 Network Footprint

During the early stages of their projects, both the iProvo and UTOPIA networks had to determine their own strategies for the construction of a network footprint. The network footprint, in this context, refers to the area served by a single aggregation point (cabinet or hut). The iProvo project began with a demonstration project where they installed various products to determine which were preferable. They began with a neighborhood in the Grandview neighborhood in the northeast part of Provo City. They installed cabinets to house the electronics and Uninterruptible Power Supplies (UPSs). From the cabinet location, the fiber was built out across utility poles and conduits throughout the surrounding neighborhood. Each of these cabinets houses four 24-port access switches, providing services for up to 96 customers. The cabinets included standard 19 inch spaced railings for mounting network devices, rack-mount UPS, and fiber splice trays. A small air conditioner is mounted in the door of each cabinet.

Figure 10 – iProvo Demonstration Area Cabinet

Provo City's demonstration project design proved to be difficult to work with for several reasons. The cabinets lacked adequate space for proper fiber management and provided little insulation from weather. This design also lacked space for redundant air conditioners or UPSs. The operating time in the case of a power outage only lasted a few hours. It also could not be easily accessed during severe weather conditions because of the risk of exposing the electronics to water, wind, dirt, etc. After the difficulties it faced with the cabinets it used in its demonstration project, Provo City determined that a larger, hut-based design would be preferable. For the rest of the city, Provo City designed larger footprints that include approximately 1500 homes each. The huts are larger walk-in structures that fit full-size server cabinets.

Figure 11 - iProvo Hut

Provo was divided into 24 footprint areas, each with its own hut. These huts connect the fiber rings that are built throughout the city and house all of the necessary electronics and support systems for their corresponding footprint.

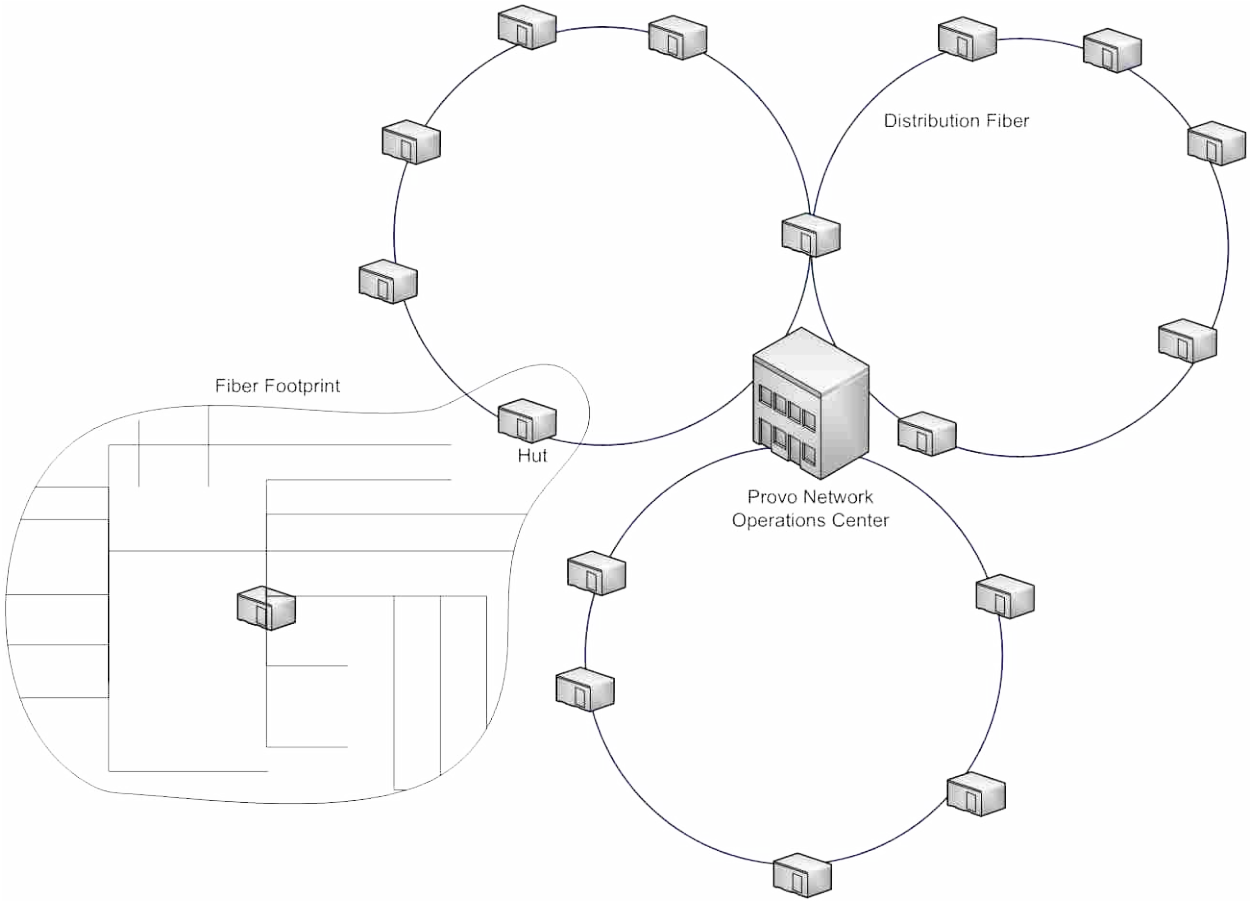


Figure 12 - iProvo Conceptual Diagram

In addition to connecting the various parts of a city to a central network, the UTOPIA network had the additional complexity of connecting several cities together. To do this, UTOPIA acquired multiple long spans of fiber to provide its core fiber rings.

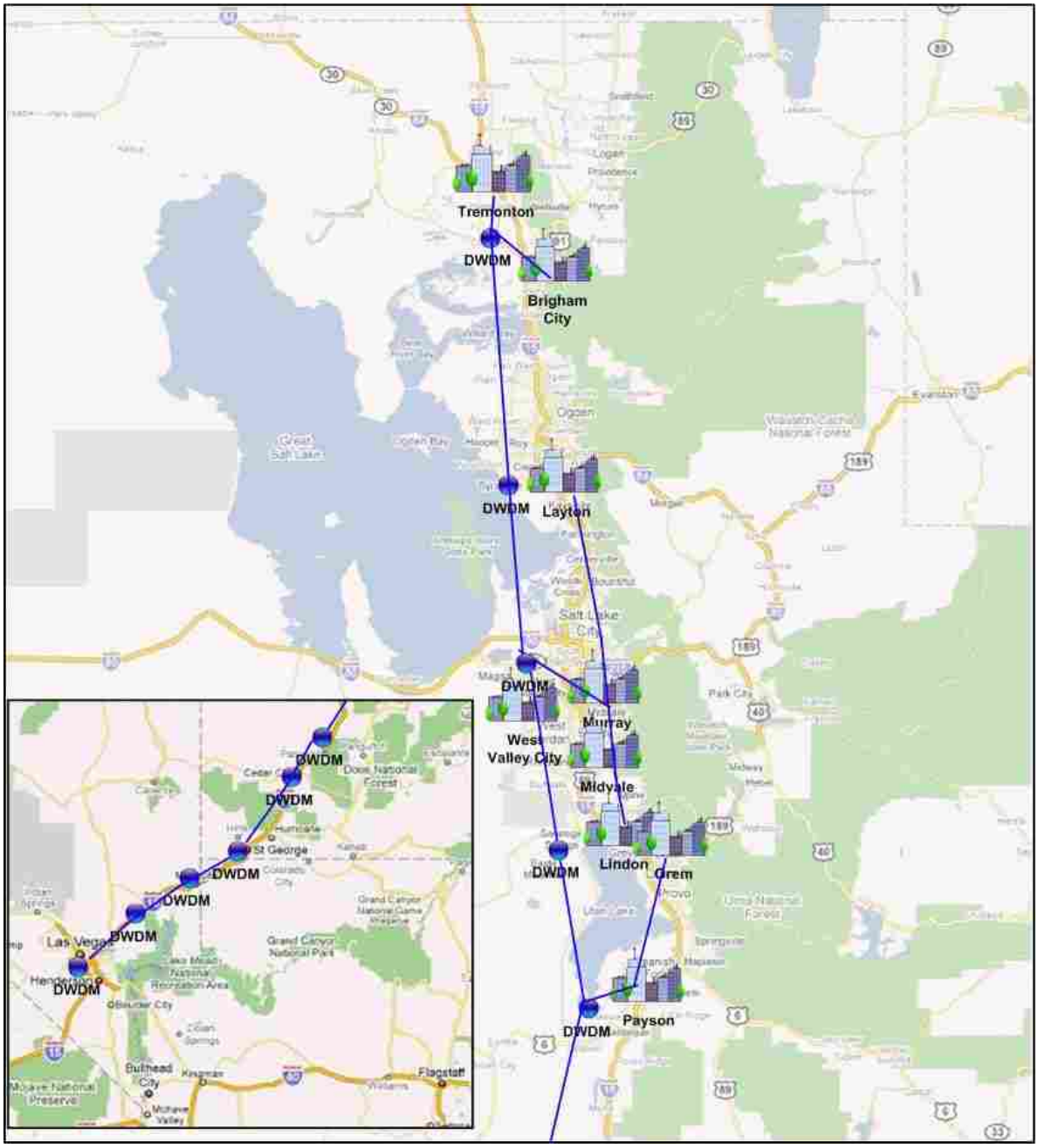


Figure 13 - UTOPIA Fiber Network Map

The Core fiber rings that provide the backbone of the UTOPIA network are terminated in one or two huts per city (depending on the size of the city). From these huts, distribution fiber rings are built to connect several cabinet locations. From each cabinet location, the fiber is

constructed throughout the footprint past about 1000 customers. In some cases, the hut locations also serve as the cabinet for the immediately surrounding area.

The UTOPIA cabinets are larger cabinets that house electronics adequate for about 500 customers. When a cabinet location is built, the site is prepared for three cabinets. Only two are initially installed with one housing the fiber management, and the other housing the electronics for the first 500 connections. If the capacity of the electronics cabinet is exceeded, then a third cabinet is installed to support an additional 500 connections.

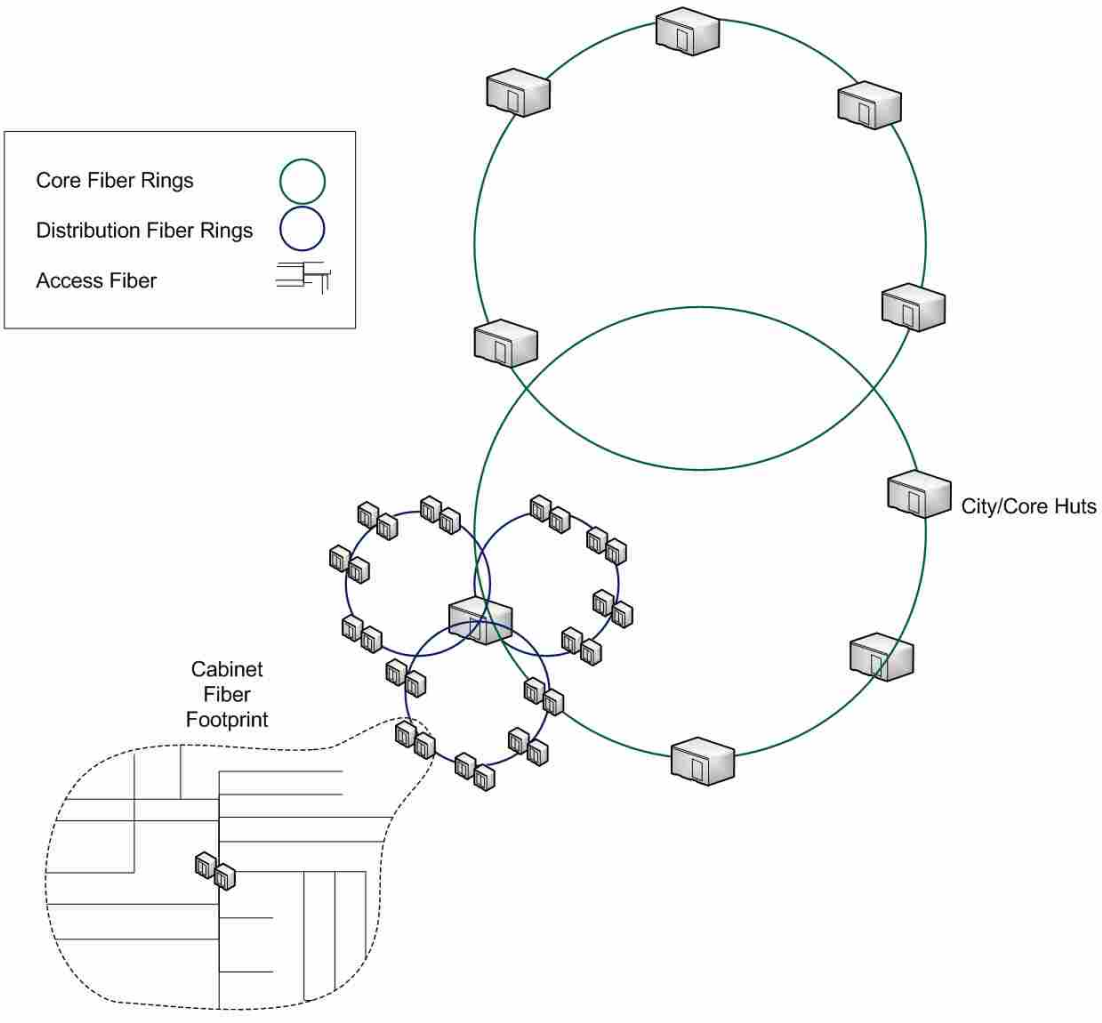


Figure 14 - UTOPIA Conceptual Design Diagram

The following is a drawing showing an example of a UTOPIA footprint. Footprints are designed to access the targeted number of homes per footprint at the lowest cost. The example below shows a major road on the west side of the footprint, and a canal on the east side. Crossing either of these types of obstacles can be costly, so the borders of the footprints are designed around these obstacles when possible.

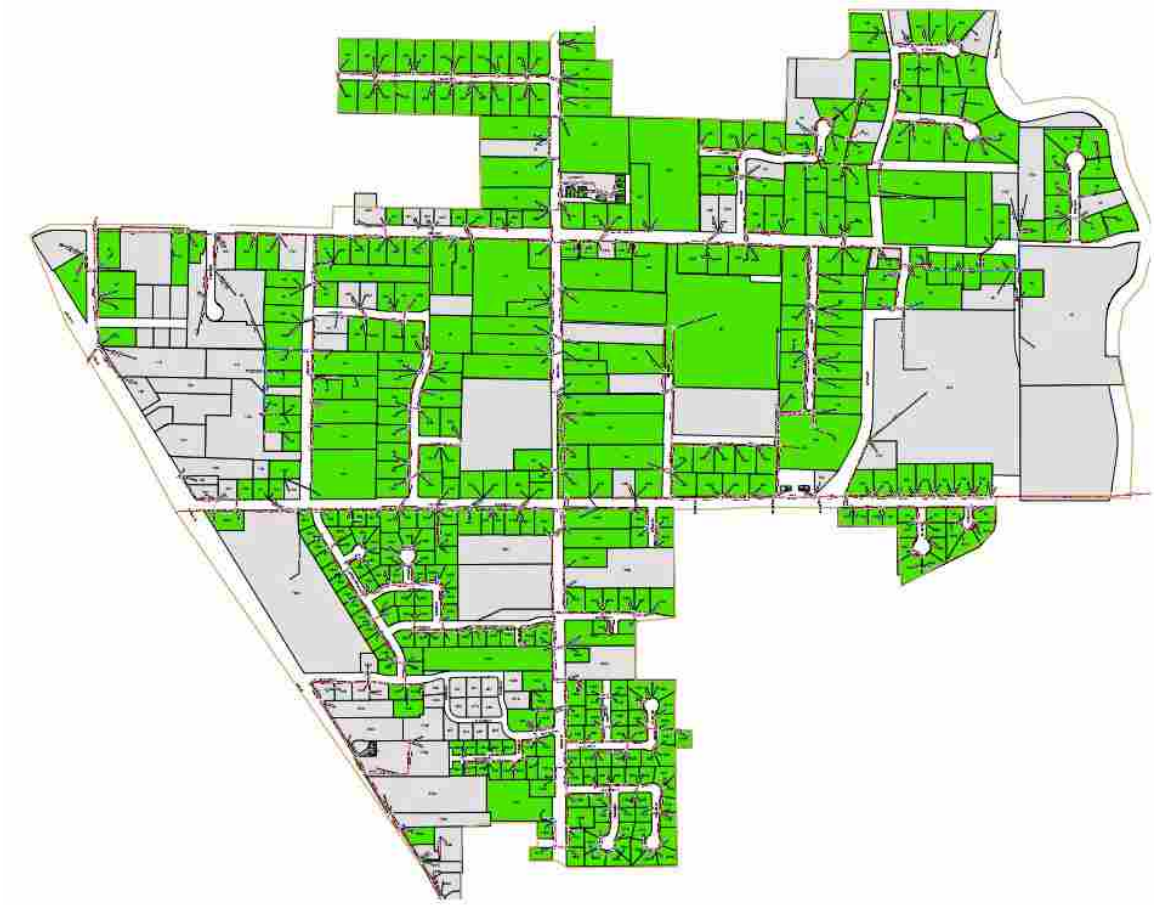


Figure 15 - Example UTOPIA Footprint [Map provided by UTOPIA]

3.2.2 Redundancy

Redundancy is a critical aspect of the design of a fiber network. Fiber networks are relatively robust in nature. However, fiber cuts or damage are fairly common for any widespread

fiber network. Fiber cuts or damage are often caused by back hoes or other construction equipment that encounter fiber while digging. This can happen from improper staking identification of utility lines, lack of staking notification, or just careless construction work. Severe weather, vandalism, and traffic accidents involving utility poles are also fairly common causes of fiber cuts or damage. Fiber repair work is very costly and time consuming. Therefore, the placement of the fiber must be designed with redundancy in mind. In both the UTOPIA and iProvo networks, this is accomplished by building the distribution fiber in as rings throughout areas of each city. A large enough fiber bundle is installed to provide connections in each direction of the ring, for each site that the distribution ring passes. This provides physical path diversity for every access level device.

3.2.3 Support Systems

One of the disadvantages of Active Ethernet based networks is the need to house active electronics. Several support systems need to be in place to allow the operation of the access level network equipment housed in each hut or cabinet.

3.2.3.1 Uninterruptable Power Supplies

An Uninterruptable Power Supply (UPS) is needed in the cabinets and huts to prevent outages in the case of a power failure. iProvo and UTOPIA took different approaches to this requirement. iProvo's design utilized fewer, larger hut locations. A natural gas powered backup generator was installed at each hut. Therefore, the UPS requirement for the iProvo network only required that UPSs have the capacity to keep the equipment running for a few minutes while the generators start up and stabilize. iProvo does not utilize redundant UPS systems or redundant

power supplies for its distribution or access switches. In this scenario, the UPS becomes a critical single point of failure, and on several occasions, has been the cause of network outages.

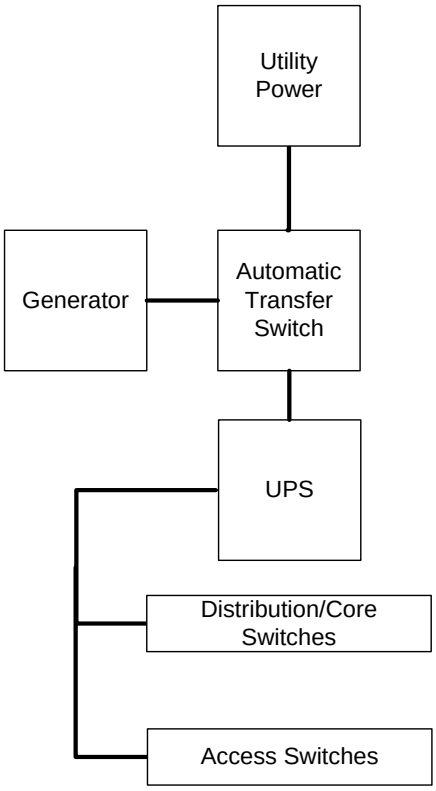


Figure 16 - iProvo Hut UPS Design

The UTOPIA network uses smaller cabinets without backup generators. Therefore, the UPSs in the UTOPIA network need to have adequate capacity to power the equipment for several hours, until a technician with a generator can arrive, connect, and start up a portable generator. Generally, these UPSs have capacity to run for at least 4 hours.

In the earlier phases of its project, UTOPIA installed a single UPS in each cabinet and used access switches that had dual power supplies. In the case of a power failure, one of the two

power supplies in the network equipment would shut down, but the other power supply connected to the UPS would continue to operate on UPS power.

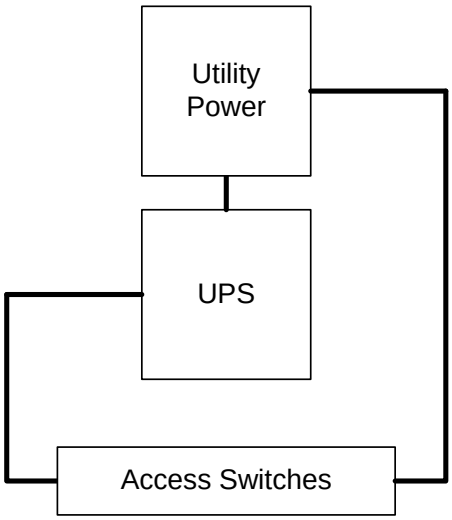


Figure 17 - UTOPIA Cabinet UPS Design – Early Phase

In later phases of the project, UTOPIA installed dual UPSs in each cabinet. This was primarily because of the history that they have had with a high frequency of UPS failures. Because of this, it was determined that it was a worthwhile expenditure to install redundant UPSs in future cabinet deployments. Since that time, UTOPIA has migrated to higher speed network equipment that supports optional redundant power supplies. However, because of the very low failure rate of these power supplies, and the relatively low impact of affecting only 24 customers each, UTOPIA decided not to install redundant power supplies in each network device. UTOPIA now installs power strips with built in automatic transfer switches so that the single power supply devices can still benefit from the dual UPS configuration.

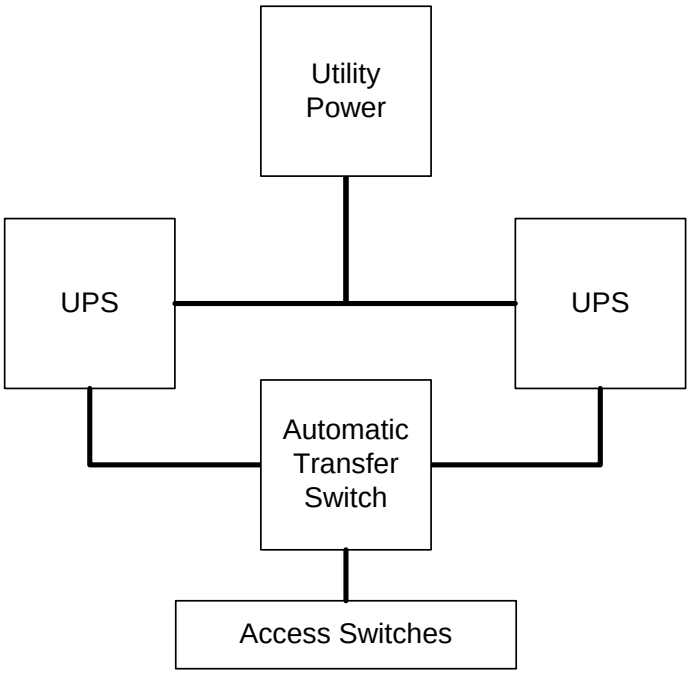


Figure 18 - UTOPIA Cabinet UPS Design – Current

The UTOPIA huts are larger and house more equipment than cabinets. They are also more critical to the operation of the network. Therefore, they are equipped with generators so that they can operate continuously in the case of a power outage.

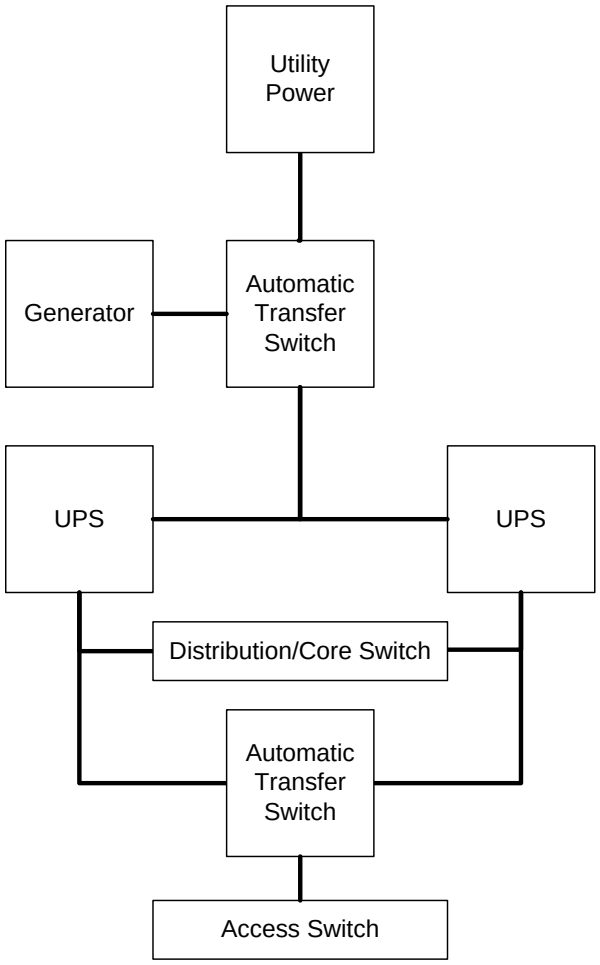


Figure 19 - UTOPIA Hut UPS Design

3.2.3.2 Backup Generators

The iProvo network uses natural gas generators at each hut location. These generators have the capacity to run all of the electronics and support systems of the hut. The benefit of using gas generators is that they can be connected directly to natural gas lines and operate indefinitely in the case of a power outage.

The UTOPIA network does not have on-site generators at its cabinet locations. Instead, UTOPIA has several large generators on trailers that technicians can quickly hitch to a UTOPIA vehicle, and then take out to a cabinet location in need of power before the UPS in the cabinet

fails. The capacity of the UPSs at the cabinets provide power for several hours giving adequate time for technicians to arrive. However, because of the inconvenience and non-scalability of this model, UTOPIA is currently considering designs to implement smaller generators at each of its cabinet locations instead of large capacity UPSs.

UTOPIA hut locations each have an on-site diesel generator that provides backup power. UTOPIA uses diesel tank-based generators that need occasional maintenance to ensure that the fuel has not deteriorated and that fuel levels are adequate.

Both the UTOPIA network and iProvo network decided that one backup generator per site was necessary. Backup generators are rarely used and must be tested regularly to ensure that they will operate properly in the case of a power outage.

3.2.3.3 Cooling

One of the disadvantages of an active-Ethernet network compared to other FTTH architectures is that active electronics are required at all aggregation points. These devices produce a significant amount of heat and must be maintained at reasonably cool temperatures. A failure in air conditioning can quickly result in overheating and damage to electronics, as well as an extended outage of services. Because of the critical nature of proper cooling, redundant air conditioners are used in both the iProvo network and UTOPIA networks at both hut and cabinets locations. iProvo and UTOPIA huts basically have the same air-conditioning design for their huts. Two wall-mount air-conditioners are installed at each hut and operate independently of each other. Each unit has the capacity to cool the entire hut. One unit is set at a higher temperature than the other so that it only operates in the case of a failure. In this configuration, identifying a failed air conditioner is simple because the backup air conditioner only operates

when the primary has failed. The primary and secondary roles can also be easily reversed in order to verify correct operation of both units.

The design of the UTOPIA cabinets uses UPS units that do not have the instantaneous capacity to power air conditioners. The UTOPIA cabinet UPSs are Alpha Technologies FXM 2000 units. These devices can provide 2000 Watts of power which is enough for the network electronics, but not for the combination of air conditioning and network electronics. Therefore, the air conditioners are connected only to utility power and in the case of a power outage, the cabinet will quickly heat up. To prevent the overheating of the electronics in this situation, a pair of heat exchangers are installed in the front doors of each cabinet. One of these exchangers brings outside air into the cabinet, and the other vents inside air out.

Recently, several network equipment manufacturers have released temperature extended devices that can operate in extreme temperatures without the need for air-conditioning or heating. For example, the Alcatel-Lucent OS-6555 is an active Ethernet switch capable of providing fiber port aggregation, and has an operating temperature of -40ºC to +75ºC (-40ºF to +167ºF).

Figure 20 - Alcatel OS-6855 Temperature Hardened Switch [Image by Alcatel-Lucent]

Temperature extended optics are also required for an installation without air-conditioning. These devices, and similar devices from other manufacturers, are significantly more expensive than traditional devices. However, if the costs for these devices continue to fall, there will likely be a

point where it becomes economical to eliminate the requirement for air-conditioning in distribution cabinets and/or huts.

3.3 Layer 2 Network Design

There are several possible ways to design the logical flow of traffic through an open—access fiber network. Both UTOPIA and iProvo have taken what can be considered a Layer 2 approach for the design of their networks. Layer 2 refers to the Data Link Layer of the OSI model.

Table 3 - OSI Model Examples

Layer	Name	Examples
7	Application	HTTP, DNS, FTP
6	Presentation	SSL, MIME
5	Session	SAP, NetBIOS
4	Transport	TCP, UDP, PPTP
3	Network	IP, IGMP, ICMP
2	Data Link	ARP, Frame Relay
1	Physical	Ethernet, SONET, PON

This approach allows all of the mechanisms of higher layers of the OSI model to be controlled and managed by service providers on the network. By primarily using only Layer 2 mechanisms, the open access network can provide the needed connectivity while allowing the service providers the greatest flexibility in their implementations. It also makes the open access network transparent to the service provider and to the end-customer.

3.3.1 Layer 2 Advantages

There are several possible ways to deliver services in an open access fiber network. However compared to other design approaches, a Layer 2 approach offers several distinct advantages.

3.3.1.1 Speed

Layer 2 devices generally do not do as much processing and packet inspection as Layer 3 routers do, and therefore are often much faster at passing traffic. In both the UTOPIA and iProvo networks, customer traffic traverses the network and arrives at the service provider equipment without ever encountering a Layer 3 device. The result of this is that the open access portion of the network introduces very little network latency. Typically, the latency on the UTOPIA network is less than 3ms between the customer and their service provider.

3.3.1.2 Simplicity

By only using Layer 2 transport mechanisms for customer services, the open access network can avoid having to manage the customer IP addressing of the network. All that is required of a new installation for the open access network operator is to configure the appropriate VLANs and rate limits onto customer facing ports for the services that the customer has signed up for. For the UTOPIA and iProvo networks, service provisioning is handled by the Network Operations Center staff, usually by running a network script or by configuring the demarcation device manually.

.

3.3.1.3 Flexibility

The Layer 2 model allows greater flexibility for service providers. They are free to choose any IP addressing schema that they choose, even those that may overlap other service providers on the open access network. Service providers may need to very granularly provide public IP addresses to some customers and private IP addresses to others. Some service providers use tunneling protocols such as PPoE (Point to Point over Ethernet) to provide dedicated circuits back to the service provider router for each customer. Other providers use IP flow based rate limiting and traffic shaping. By participating only at Layer 2, the open access network needs no interaction with the service provider to allow them to implement any of these features for their customers.

3.3.2 Disadvantages

Despite several advantages of using only Layer 2 mechanisms, there are also vulnerabilities to this approach.

3.3.2.1 Network Loops

Layer 2 networks are vulnerable to network loops. Loops can occur when two customer facing ports are bridged together through another switch, access point, or any device that may send customer destined traffic back into the network. The result of a loop is that all traffic going out a customer facing port re-enters the network back on that port, or possibly another port. Depending on the nature of the loop, this can causes incorrect entries in the MAC address tables of the network switches which cause traffic to flow through the wrong path, loop around in the network causing a traffic storm, or to become stranded and dropped without reaching its

destination. To the customer, this appears as slow data speeds, dropped phone calls, scrambled video, or a service outage.

One way to mitigate this limitation is limit the number of MAC addresses that are allowed to communicate on a given customer-facing port, which effectively blocks traffic from a loop or additional devices beyond the limit. This prevents the flooding of downstream traffic back up into the network. However, if this feature is implemented, any customers with multiple devices must also install a router between their devices and the network. This aggregates the traffic from their devices and allows their devices to appear as one device on the fiber network staying complaint with the one-MAC limit. Both the iProvo and UTOPIA networks have considered implementing this option but did not because of the incremental cost of having to provide routers to every customer and having to support those routers. This type of limit is commonly used on DSL and Cable networks.

Another way to mitigate the vulnerability of loops on the network is to block any customer-to-customer traffic. The UTOPIA network is configured to block traffic between customers unless the traffic traverses the service provider's router (i.e. they are on different IP subnets). Loops are unable to traverse through a router, so this model does provide some protection between customers. However, the loop traffic can still affect the MAC address tables of the upstream switches, so static configuration of the service provider MAC addresses on the service provider facing ports of the network switches is also required for this method to work properly.

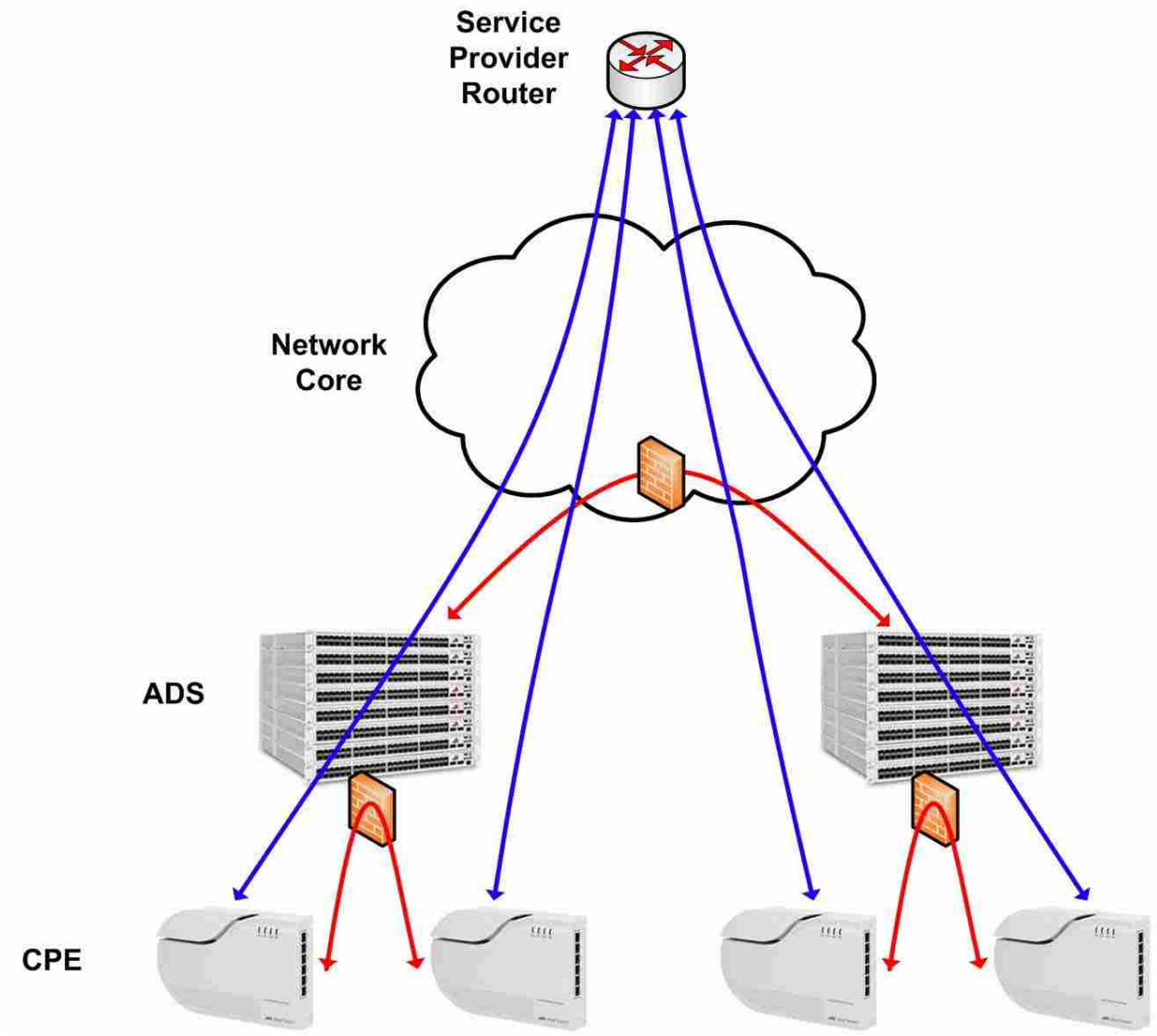


Figure 21 - UTOPIA Customer-to-Customer Traffic Blocking

This diagram shows the flow of traffic between the Customer Premises Equipment (CPE) and their service provider. Traffic is blocked (red paths) between customers both at the Access Distribution Switches (ADSs) and in the network core. However, every customer can communicate with their service provider (blue paths). See Appendix A for information about how this is configured on the UTOPIA network.

The iProvo network does allow communication directly between customers without traversing a service provider router. To mitigate loops, iProvo has implemented network device scanning that checks for movement of MAC addresses. In most cases when a MAC address moves frequently from one portion of the network to another, it is likely that a loop has occurred. By detecting this behavior, iProvo technicians can identify the source of the problem and disable the offending customer port.

3.3.3 Layer 3/4 Vulnerabilities

Some Layer 3 and Layer 4 protocols have inherent vulnerabilities that may affect customers below a point in the network where the service provider has protections in place to prevent it. For example, in most cases, a service provider will provide DHCP (Dynamic Host Configuration Protocol) services to customer devices on the network. DHCP is a protocol that distributes IP address, gateway, subnet, and other information to clients when they connect to the network. However, DHCP suffers from the vulnerability that it does not authenticate against the server, and may therefore receive DHCP settings from rogue DHCP servers that responds to its request. In a typical Layer 2 network, any rogue DHCP server (such as a wireless router plugged in with the client facing port connected to the open access network), may send out incorrect DHCP settings. This effectively breaks other customers in that segment of the network who receive those false settings instead of the DHCP response from the service provider.

While it is expected that the service providers will provide some protection from the Internet with its own firewalls and access control lists, attacks between users on the same subnet would still be possible without the ability of the service provider to intervene. In order to resolve this and other Layer 3/4 vulnerabilities, many switch manufacturers implement some Layer 3/4

protocol filtering. This allows the open access network to block DHCP server responses from customer facing ports. UTOPIA and iProvo use this capability to block several protocols, including upstream DHCP server responses. The methods of loop prevention mentioned in section 3.3.2.1 are also effective at protecting against some Layer 3/4 vulnerabilities.

3.4 Service Delivery Requirements

For an open access network to operate properly, the requirements of each service must be included in the design. It would be far simpler to just provide a "bit pipe" to each customer regardless of the services that they receive. However, various services can easily interfere with each other if protections are not in place.

For example, a triple-play customer on a 100 Mbps FTTH network may have voice, video, and data services. Suppose that a customer is running a bandwidth intensive file-sharing application (i.e. Bittorrent, Aries, eDonkey), using two High-Definition DVRs, and using their phone service. Without service-based controls in place, the file-sharing application could easily reach 50 Mbps or more. High-Definition MPEG-2 streams use about 15-20 Mbps each and each DVR may receive up to 3 streams (max 60Mbps per DVR). Phone service can require up to 100 kbps per active phone call. This situation could potentially require up to about 170 Mbps. Obviously, this would exceed the limits of a 100 Mbps link to the home. Without service differentiation in place, the CPE would randomly drop packets from all services. The result of this to a customer would be dropped phone calls, unwatchable video, and an unstable internet connection. Therefore, it is necessary to differentiate and prioritize the various services on the network to ensure a good experience for the customer given the limits of the network.

3.4.1 Management

Network Management is not a service that the customer subscribes to or is even aware may exist on the network. However, it is usually considered to be the most important service. This is the service that the network operator uses to configure, monitor, and troubleshoot the network devices. Regardless of what services or events may be present on the network, it is most important that the network operator maintain access to the network devices so that events and problems that may occur can be fixed. Therefore, it is necessary to give the network management service top priority. Without this, any customer services that overwhelm a link could potentially prevent the network operator from fixing or troubleshooting the problem remotely. On the UTOPIA and iProvo networks, the following are performed on this service level:

- Provisioning of network devices to provide customer services
- Monitoring of device status
- Collection of statistics from devices for purposes of bandwidth management and trending
- Collection of Simple Network Management Protocol (SNMP) traps
    - Temperature alarms
    - Battery failure alarms
    - Power status alarms
    - Network Topology changes
- Backup system monitoring (generators, air conditioning, fire suppression)
- Security video feeds

The bandwidth requirements of these services on the 100 Mbps link to the home is negligible, but the priority must be configured to ensure that those services remain available even if network links become saturated.

3.4.2 Voice Services

Voice (telephone) service is generally the least bandwidth intensive and highest priority service that an end customer experiences. This is because it is considered to be a critical service that must always be available. It is also very intolerant of loss or delay. Both the iProvo and UTOPIA networks prioritize voice traffic over any other service traffic. Rate limits are also set that allow at least 64 kbps per phone line. Depending on the encoding algorithm and compression used by the service provider, the actual requirements may be lower.

Table 4 - Common VOIP Codecs

Codec	Bitrate (kbps)	Description
G.711	64	Common, low compression, low processor requirements
G.722	48/56/64	Adapts to network congestion
G.723.1	5.3/6.3	High Compression, processor intensive
G.726	16, 24, 32, 40	Updated version of G.723
G.729	8	Licensed codec, error tolerant

The table above shows some common VOIP encoding algorithms and the bit rate required by each.

Other than providing appropriate rate limiting and prioritization, the iProvo and UTOPIA networks are not involved in providing phone services. However, it is important to understand how these systems work for integration and troubleshooting purposes. The following is a

conceptual diagram that shows how a service provider interconnects and provides VOIP services.

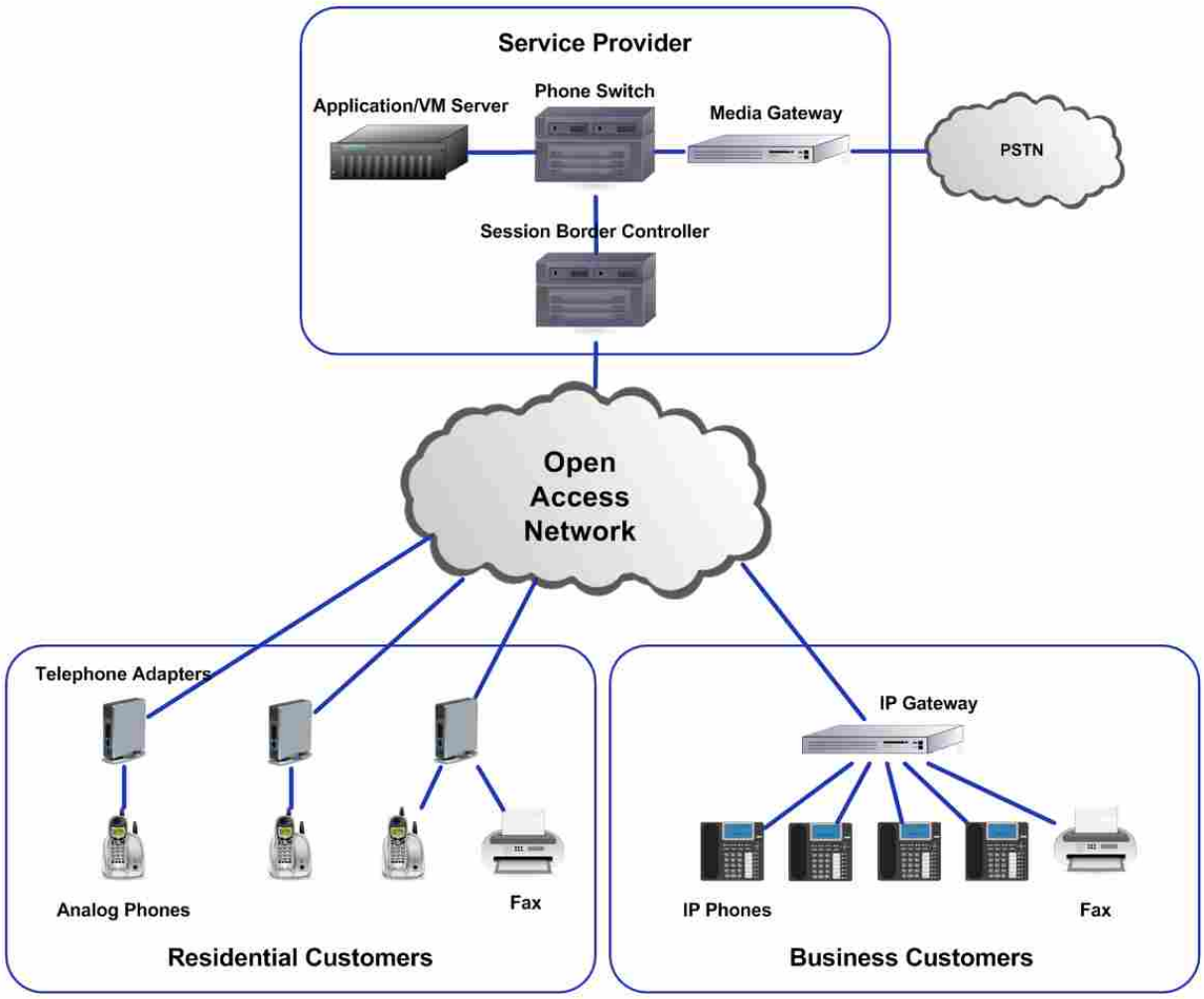


Figure 22 - Conceptual Diagram of VOIP Services on Open Access Network

Because of the large up-front costs required for a service provider to provide VOIP services, it has been common for iProvo and UTOPIA service providers to re-sell each other's VOIP services, or to purchase VOIP services from other third party providers.

3.4.3 Video Services

In an ideal fully open-access environment, the network operator would not be involved with the acquisition or delivery of IPTV services other than doing some network configuration to facilitate it working properly on the network. However, the up-front costs of creating an IPTV system are very high, and existing IPTV providers are very rare. Early in their projects, both iProvo and UTOPIA realized that they would need to act as IPTV service operators to ensure that IPTV services were available in their networks. Restrictions from the Utah Municipal Cable Television and Public Telecommunications Services Act do not allow municipalities to provide retail cable TV services in the state of Utah, so iProvo and UTOPIA act as IPTV operators and partner with their service providers to bill the retail side of it. The model is similar to a DirecTV video service provided by Qwest.

3.4.3.1 Headend Design

The first step in providing video services is to obtain a source of video content. Any system that plans to offer video services will likely need to install and maintain their own video headend. A video headend is a facility that houses various equipment required for the reception and signal conversion of video signals for use in video distribution networks. Content providers (i.e. Disney, Turner Broadcasting, MTV Networks) distribute their signals via C-band transmission (4-8 GHz) which require large satellite dish antennas (3-5 meter). These dishes are installed and aimed at the various satellites needed to supply feeds for the planned channel lineup. Several online tools are available to aid in the aiming angle of each satellite.

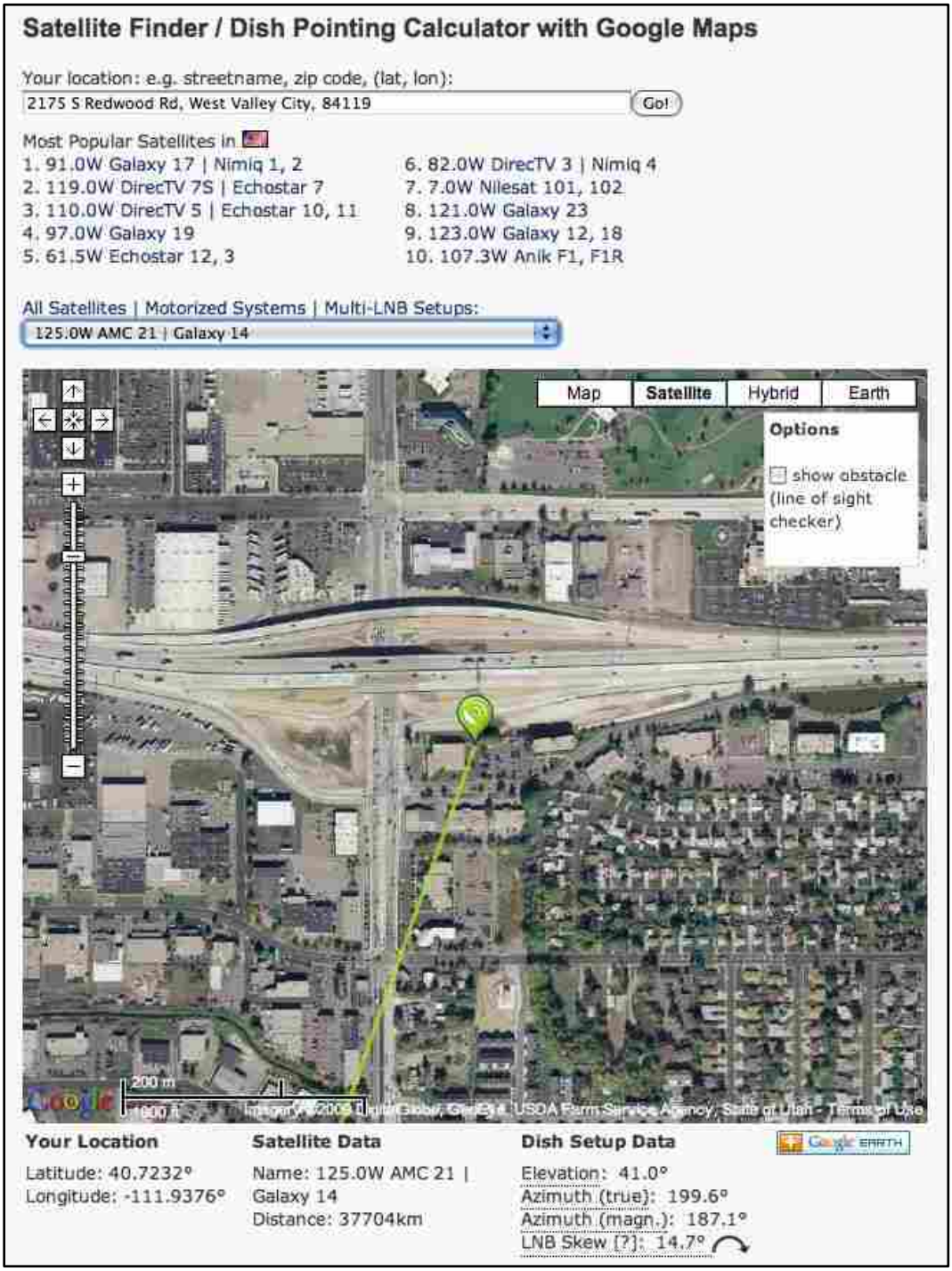


Figure 23 - Satellite Finder / Dish Pointing Calculator from Dishpointer.com

Once the dish is aimed in roughly the correct angle, a satellite signal meter is usually used to fine-tune the angle and elevation of the dish to get the best signal possible.

Each satellite signal is received at the dish with an LNB (Low Noise Block) that converts the signal to a lower frequency that can be sent over coaxial cable to the satellite receiver. The satellite receivers decrypt the signals and output the streams as an ASI (Asynchronous Serial Interface). Each ASI may include several video streams multiplexed together. At this point, it is fairly common to place ad-insertion equipment that uses cue tones to trigger local advertisements. Then, any combination of video transcoding, bit rate grooming, encryption, and IP encapsulation may be used, depending on the requirements of the system, before it is then injected into network as a multicast IP stream. A middleware system is used to provide set top box software, account provisioning, channel management, billing, electronic program guide information, and Video on Demand (VOD) integration.

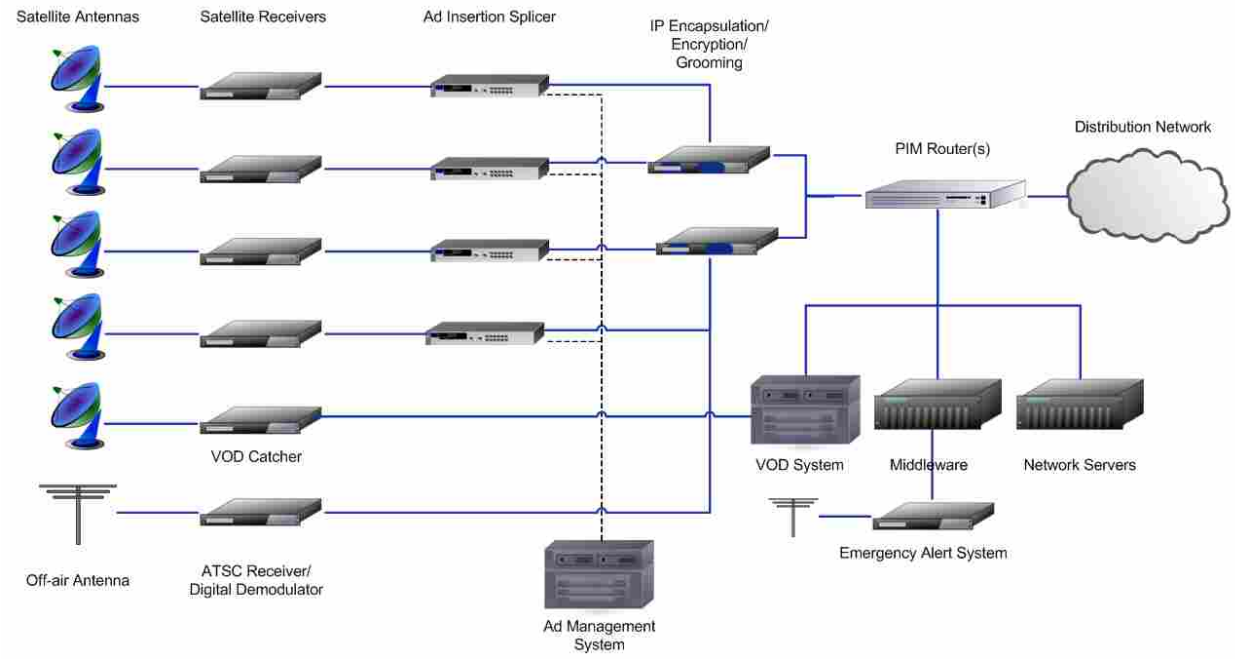


Figure 24 - Example IPTV Headend Configuration

Provo City acquired and installed a Simulsat dish when it was upgrading the Provo Cable system for the iProvo FTTH project. A Simulsat dish is a large dish that can receive signals from several satellites simultaneously. Provo also used a video aggregation provider (Comcast HITS) to reduce the number of satellite receivers and antennas needed. Video aggregation providers are systems that downlink a large number of signals, transcode the signals, and multiplex them together before sending them back up to fewer satellites. This allows headends to receive more channels with fewer satellite antennas and fewer receivers, reducing the upfront costs of deploying a video system significantly. With its Simulsat dish and a few standard dishes, Provo was able to receive all of the necessary channels for its lineup. They converted these signals to fiber at the site of their dish antennas and transported to signals to the Provo Network Operations Center building that housed the rest of the headend equipment (off-air antennas, satellite receivers, encryption system, middleware, VOD system, etc).

UTOPIA originally chose not to build a headend, but opted instead to enter into an agreement with Provo City where Provo City would provide video transport services and deliver video content to the UTOPIA network. UTOPIA acquired its own Middleware and VOD systems, but used the feeds from the Provo system. When Provo City sold the iProvo network to Broadweave Networks in 2008, Provo City terminated its agreement with UTOPIA and UTOPIA was forced to pursue other options. UTOPIA then chose to implement its own headend using aggregated services from Avail-TVN combined with direct reception for some content providers that were not available through Avail-TVN. UTOPIA also installed its own antennas and demodulation equipment to receive signals for the local off-air broadcast channels. With these systems in place, UTOPIA was able to independently launch its own IPTV service.

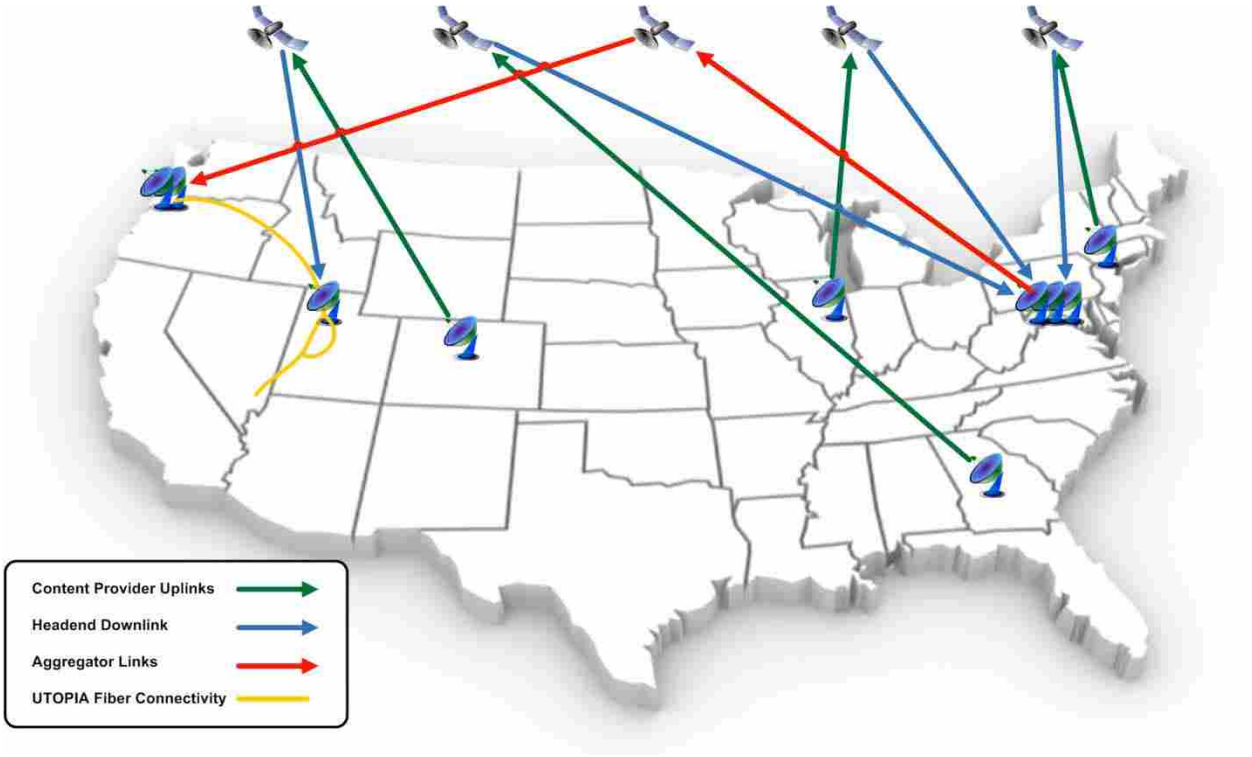


Figure 25 - Conceptual Diagram of Satellite Signal Distribution to the UTOPIA Network

The figure above shows a conceptual overview of how various signals from different content providers are uplinked and received by the UTOPIA network. It also shows an aggregation system that downlinks from several providers and sends the aggregated content back up to satellite for use by headends as an alternative to direct feeds.

3.4.3.2 Video Distribution

There are two common methods for distributing video services in a FTTH network. Most GPON networks overlay an analog cable signal or a Digital QAM (Quadrature Amplitude Modulation) digital cable signal at a different wavelength of light (typically 1550nm) that is combined with the wavelength used for data (typically 1310nm and 1490nm) before it leaves the central office. As the signal arrives at the home, the ONT converts this signal to a coaxial

connector that can use the home's existing coaxial cabling for distributing video to TVs and set top boxes. This approach has the advantage of being able to provide video service without having to run new CAT5E lines to each TV location as well as not requiring a set top box for each TV. However, content providers are increasingly requiring that their channels be encrypted as they are sent to the customer premises. To be able to view encrypted channels, there must be a set top box to decrypt and decode each video channel.

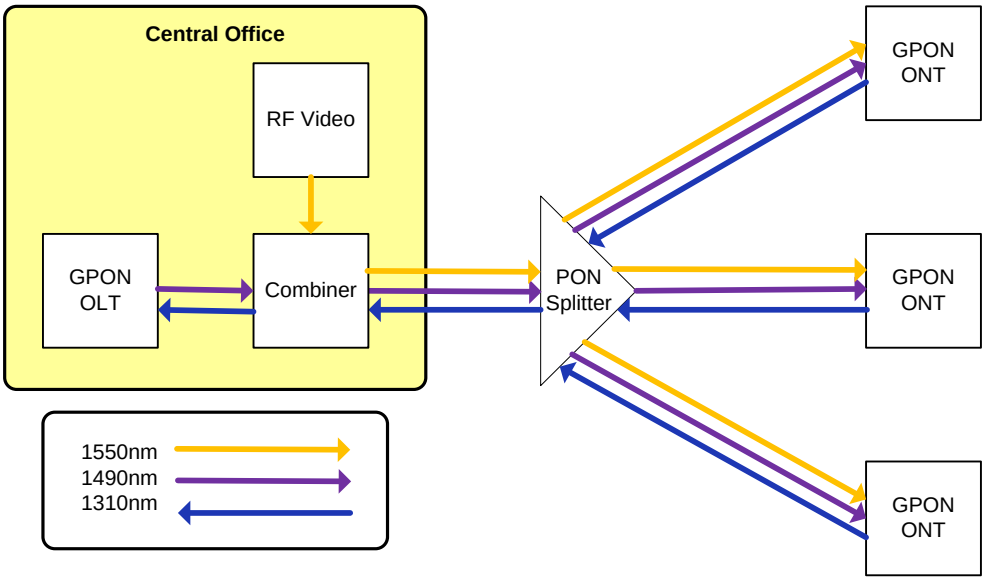


Figure 26 - GPON Network with RF Video Overlay

Provo and UTOPIA chose to utilize the Ethernet network to deliver all services including IPTV. Video on these networks is sent as multicast UDP traffic. The design of how video is delivered to the customer will be discussed in more detail later in this chapter. However, the result is that only those streams (channels) that a customer is viewing traverse the 100 Mbps link to the home. Initially, this limitation seemed to be of little significance because each standard definition channel only required 2-4 Mbps of throughput. However, as High-Definition channels

were added, the 100 Mbps limitation became much more serious. The typical High-Definition MPEG-2 channel requires 12-20 Mbps of throughput. Therefore, while accounting for overhead and other services, this only allows for a maximum of four High-Definition channels to be received in a home simultaneously. The high definition channels in the UTOPIA network are a mix of MPEG-4 and MPEG-2 channels. The MPEG-4 high definition channels usually require 8-12 Mbps each. However, UTOPIA must plan for a worst case scenario when setting installation standards and therefore has to limit installations to set top boxes that use a total of 4 HD streams per household. IPTV service is given a QoS priority below management and voice services, but above all other services. Management and voice services use very little bandwidth, allowing the IPTV service to use nearly all of the 100 Mbps available when needed.

3.4.3.3 Internet Group Management Protocol (IGMP) Snooping

A critical aspect in the design of IPTV is the implementation of IGMP snooping. In general, the open access network does not participate at OSI network layers higher than layer 2. However, it is necessary that the open access participate in the delivery of IPTV services. The aggregation of video services from an IPTV video provider can easily exceed 1 Gbps. Typically, video streams for IPTV are sent in multicast format. A network with only OSI layer 2 functionality will treat this traffic as broadcast traffic and all active streams will flood every part of the network. This would obviously be a problem as it would easily exceed the capacity of the 100 Mbps links to each home.

IGMP snooping is a process where layer 2 switches analyze IGMP messages (join and leave messages) to populate an internal state table that tracks where active members of the multicast groups reside. The multicast streams are blocked from links that do not contain active

members of that multicast group. In this scenario, multicast group members are set top boxes that have tuned to a given TV channel (multicast stream). As the set top box is tuned to a channel, the set top box sends an IGMP join message and when it changes away from a channel, it sends an IGMP leave message for that stream. The result of this is that only those video streams that are being watched on a given connection, are sent to that connection. Both the iProvo network and UTOPIA enabled IGMP snooping throughout their networks in order to allow efficient routing of video through their networks. Every end-user connection would be overwhelmed with unwanted multicast traffic if this were not implemented.

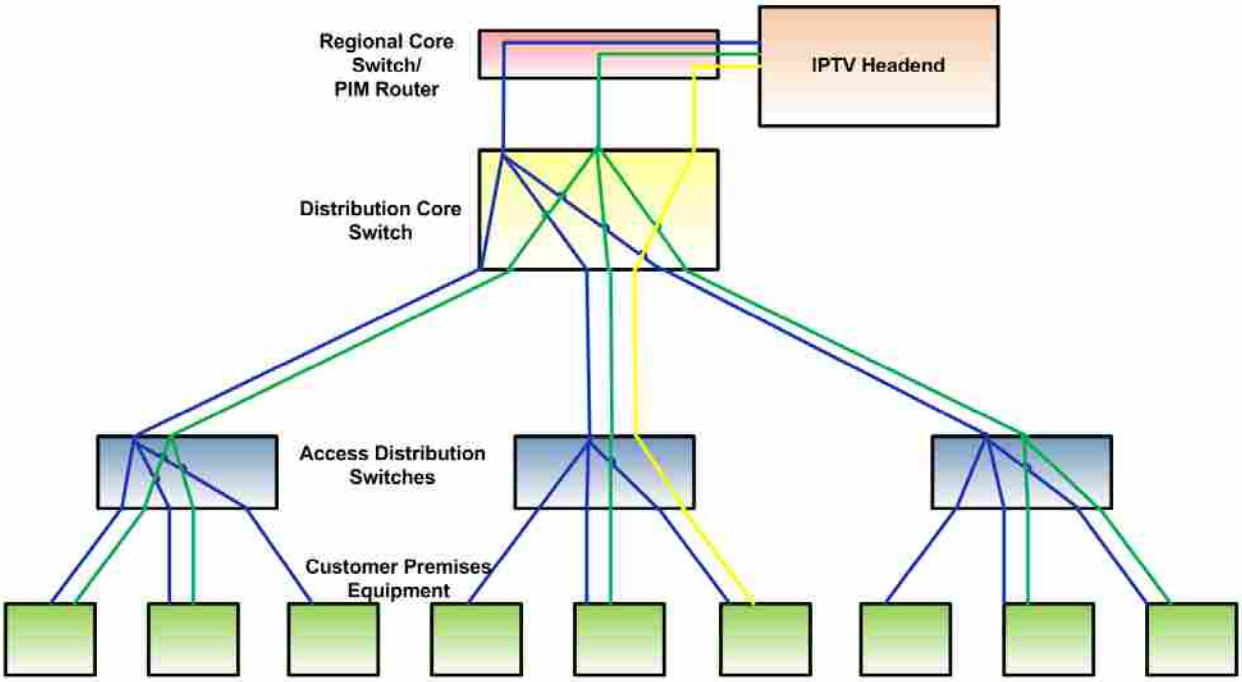


Figure 27 - IGMP Snooping Example

In the figure above, IGMP snooping is enabled on the Distribution/Core Switches and Access Distribution Switches. The blue path represents a popular program being watched by every end customer in the system. The stream exists only once on any link in the network. The

green path represents a somewhat popular channel being watched by at least one customer below each Access Distribution Switch. The yellow path represents an unpopular channel being watched by only one customer. The benefit of multicast video is that only one copy of each stream is sent along any path in the network. The benefit of enabling IGMP snooping is that video bandwidth can be conserved wherever a given channel is not required by the end customers.

3.4.4 Data Services

Data services (including Internet connectivity) on the UTOPIA and iProvo networks are given the lowest priority of the "triple-play" services. Most data traffic leaves the local network and accesses devices and servers on the Internet. The reliability of a connection on the Internet is generally unknown. Internet applications are designed with this in mind and are very tolerant of loss and delay. Therefore, data connections operate well under this type of prioritization.

Data is, in general, the simplest of the triple-play services to provide. The basic design of a data service consists only of a router, DHCP servers, DNS servers, and an upstream bandwidth provider. However, behavior of the data services is also the most variable. Unlike voice and video traffic that consists only of protocols and streams under the control of the service provider, data services consists of any type of traffic that can be generated by a computer or network device. Most of the efforts in providing a reliable data service involve protecting the service from its users. Traffic shaping, IP filters, intrusion prevention systems, firewalls, and other methods are frequently used to protect and ensure a reliable data service for end customers. Data services for both the iProvo and UTOPIA networks are managed entirely by the service providers on the network with little involvement from the open access network operator.

3.4.5 Transparent LAN Service

Transparent LAN Service (TLS) refers to providing private network connectivity between two or more sites while hiding the devices and network operations to connect those sites. In contrast to data services, TLS does not generally include any sort of connectivity to the Internet. It acts as a private and secure circuit between customer sites.

The most simple, but costly, method to provide TLS services is to provide a dedicated fiber, or "dark fiber". This allows the locations on either end of the fiber to take advantage of the full available bandwidth of the fiber and to control all aspects of the signaling on the fiber. Customers using this type of a connection can use any speed of signaling or even send multiple wavelengths of light across the fiber. However, this approach also places the responsibility and costs of network devices and optic modules on the customer. There are few customers on the iProvo and UTOPIA networks that are willing to pay the premium for this type of connection. From the network operator's perspective, this can be a very profitable service. Fiber bundles come with set quantities of fiber which means that there is typically left over fiber from what was required in the network design. Once the fiber strands needed for the FTTH deployment are used, any remaining unused fiber can be leased out. Also, fiber links can be reclaimed as needed for this purpose if existing links are upgraded to higher speed or multiple wavelength connections.

By far, the most common method of providing TLS services on the iProvo and UTOPIA networks is to simply provide a unique VLAN that terminates at the various customer locations. This is also the least expensive solution because it doesn't require dedicated fiber, and beyond what is required for a typical installation, only requires configuration of network devices to provide the needed path for that VLAN.

In some cases, usually for larger organizations, the customer requirements may require the use of several VLANs. These VLANs may also be specific VLANs that are in use on the open-access network for other purposes, creating a conflict. For these cases, the UTOPIA network provides TLS services using QinQ VLAN tagging. QinQ is the name of an amendment to the 802.1Q standard that allows multiple levels of VLAN values in Ethernet frame headers. QinQ VLAN tagging provides this service by accepting VLAN tagged traffic from the customer port, and encapsulating it further into a second (or outer) VLAN tagged header. At the other end of a QinQ connection, the outer VLAN tag is stripped from the customer traffic and the customer's traffic egresses the port with only its original VLAN tag in place. This gives the customer the ability to use any combination of VLANs at all of its locations on the networks without specific VLAN coordination with the network operator. The common CPE for the UTOPIA network does not have the capability of adding a second VLAN tag. Therefore, UTOPIA installs a different device to support these types of customers. Currently the device of choice for this is an Alcatel-Lucent LS-6212. See Appendix C for an example of QinQ configuration on the UTOPIA network.

3.4.6 Quality of Service

Quality of Service (QoS) refers to the various mechanisms used to prioritize and manage flow of various types of traffic in a network. QoS configuration is typically an ongoing effort by any network to fine-tune rules, priorities, rate limits, traffic shaping, and other mechanisms to ensure that services perform as required. QoS mechanisms are highly dependent on the specific features available on the hardware being used. In the iProvo network, the CPE did not have any rate-limiting ability. Therefore, this was configured at the first aggregation device (ADS) above

it on a per-VLAN basis. In the UTOPIA network, per-port rate limits are configured on the data ports of each CPE. The differences in QoS approaches between these two networks is more likely because of the specific device limitations than from differences in QoS policy. See Appendix D for details about the QoS configuration of these networks.

3.5 Design Details

For the purpose of providing open access fiber network connectivity, there is no single correct way to design a network. However, by examining the various design details of the iProvo and UTOPIA networks, comparisons can be made that will help with the formulation of "best practices" other networks may benefit from. This analysis will describe the designs of these networks using a Core->Distribution->Access model. The Core portion of this model represents the most central part of the network where all customer connections and services are aggregated and interconnected with service providers. The Distribution portion of this model represents the part of the network that extends services out to the various geographic areas of the network. The Access portion of this model represents the final point of aggregation where all individual customer connections are received. The CPE portion of the network will also be included in this discussion which acts as an extension of the Access network, terminating the Access ports at each customer premises and providing a demarcation point.

3.5.1 Core

The iProvo network Core aggregates all of the physical areas of the network as well as the various services and service provider handoffs. The core is located within a few racks of equipment at the central Provo Network Operations Center building. The core consists of many

World Wide Packets LE-427 devices interconnected to provide adequate aggregation capabilities. They also used World Wide Packets LE-3700's (rebranded Enterasys ER-16s) routers to provide layer-3 routing in the core.

Figure 28 - Provo Network Core and Headend

Redundancy in the iProvo network core is provided using Rapid Spanning Tree Protocol (RSTP) which provides automatic failover and loop prevention. All of the links in the iProvo network core are GigE interfaces. To provide adequate bandwidth to aggregate all of the areas of the network, several GigE links are aggregated together (up to four per link). This gives the network a 4 Gbps core capacity at its most aggregated point.

UTOPIA approached the design of its core with a more geographically diverse approach. The UTOPIA network serves many cities, most of which are along the Wasatch front. Instead of focusing on a central core location, UTOPIA placed portions of its core in four different locations throughout the Wasatch front. This way, any fiber cut, power failure, or other outage at a site would not affect the rest of the network. The core devices are physically connected in a ring topology so that any one failure will not disrupt connectivity for the rest of the core network.

The UTOPIA network is designed with greater core capacity so that it can serve hundreds of thousands of customers. All of the core devices are Alcatel-Lucent 7450 ESS-12 devices and are interconnected with each other with 10 GigE interfaces. These devices have capacity for many more 10 GigE connections as the network grows. They are also upgradeable to 40 GbE and 100 GbE (still in development) as those interfaces become available.

The UTOPIA network core uses MPLS protocol for redundancy. MPLS allows the configuration of multiple paths for redundancy and/or load balancing. Failures to one path are quickly resolved (typically 50ms or less) by re-routing traffic via a different path. The fast re-route feature of MPLS enables fast convergence time by creating a temporary bypass tunnel for traffic to continue flowing towards its destination while MPLS signaling changes the entire path to its secondary path. MPLS also allows for having the flexibility of many paths from any device to another without concern for loops or other topology related problems. See Appendix F for detailed configuration details for MPLS configuration on the Alcatel-Lucent ESS 7450 platform.

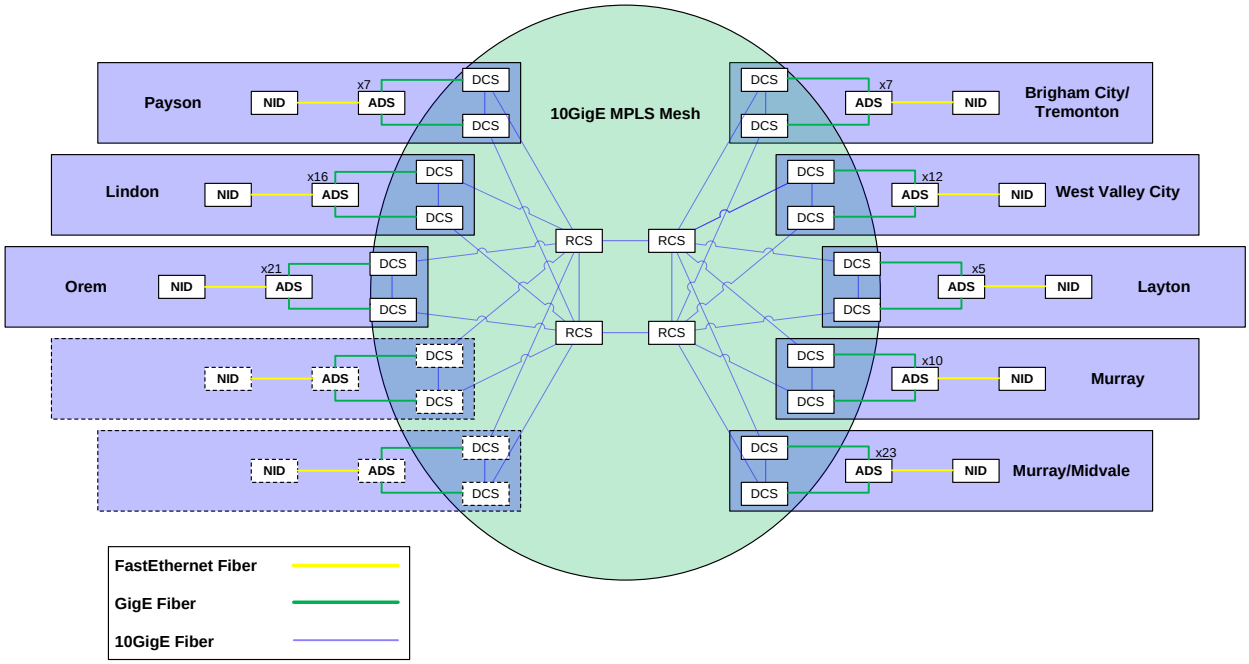


Figure 29 - UTOPIA Core/Distribution/Access Connectivity

The figure above shows the physical connectivity of the core, distribution, and access portions of the network. Devices are named corresponding to those portions of the network as Regional Core Switches (RCSs), Distribution Core Switches (DCSs), and Access Distribution Switches (ADSs). Only the RCSs and DCSs participate in the UTOPIA MPLS network.

3.5.2 Distribution

At the distribution layer of the network, the iProvo network uses a pair of 16 port GigE switches (World Wide Packets LE-427s) to connect back to the core. Each LE-427 is fed from different physical paths through the city back to the network core in order to provide fiber path redundancy.

Like the core of the network, the iProvo network distribution devices use RSTP for redundancy. All of the devices in each iProvo network hut (distribution and access) are

configured to be part of the RSTP domain. Rings are intentionally built so that the RSTP sets certain ports to blocking state in its default operating state. When there is a fiber break, device failure, or transceiver failure, RSTP enables the ports that were in blocking state, and connectivity is restored.

One weakness of this approach for redundancy is that IGMP snooping does not interact directly with RSTP. Therefore, when there is an RSTP topology change, the IGMP tables may become inaccurate according to the multicast groups that have been joined by hosts in that part of the network. The effect of this is that depending on the differences in the IGMP tables before the topology event, and what they should be after the event, a video outage of several minutes may occur whenever there is a RSTP topology change. The duration of the outage typically lasts until the next IGMP general query is received from the upstream router.

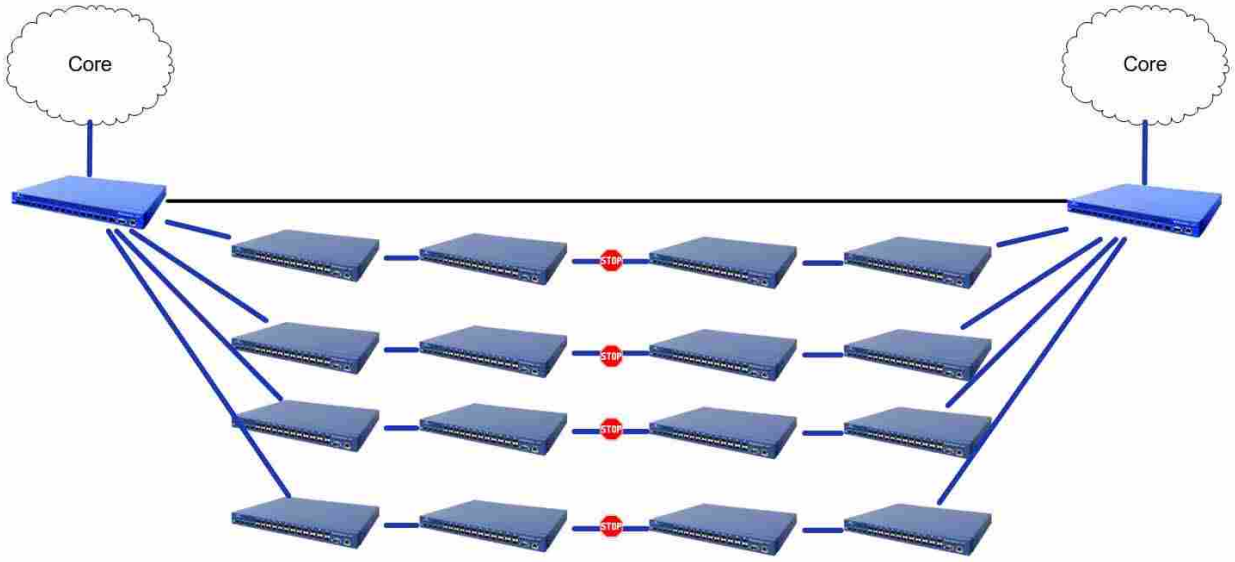


Figure 30 - iProvo Distribution and Access Design

In the UTOPIA network, a pair of Alcatel-Lucent 7450 ESS-7 devices are installed in each city area and are used to aggregate all of the connections from the cabinets. Each DCS

connects to a different RCS on a diverse fiber path. The DCSs participate in the MPLS configuration with the RCSs, which provides redundancy and traffic engineering abilities. IGMP snooping instances are configured within each VPLS service. Because the redundancy and routing of VPLS is managed by the underlying MPLS configuration, topology changes do not affect the accuracy of the IGMP tables relative to the downstream multicast group memberships.

3.5.3 Access

The Access switches for the iProvo network are World Wide Packets LE-327 devices. Each LE-327 provides 24 SFP ports for connecting the CPEs in each home or business. These devices are connected to the Distribution layer LE-427s in a ring configuration so that STP can enable a backup path in the case of a failure in any part of the ring. The LE-327s also have the same IGMP snooping vulnerability as the LE-427s that IGMP snooping does not participate in the STP topology changes, and can therefore cause outages until its IGMP tables are corrected from the next query cycle.

ADSs used in the UTOPIA network are either Riverstone 8600s or Alcatel-Lucent OS-6400-U24 devices, depending on the area. Neither of these devices are MPLS capable. Therefore, a different mechanism must be used to provide redundancy between the Access and Distribution layers. The current method is to use a multi-chassis link aggregation group (LAG). A multi-chassis LAG allows ports on multiple devices to participate in a single logical link to a downstream device. The physical ports can be assigned priorities and set in active or standby mode. By doing this, the uplink from every ADS can be tied to two DCSs, with automatic failover from on to the other, if the link of the primary port is lost.

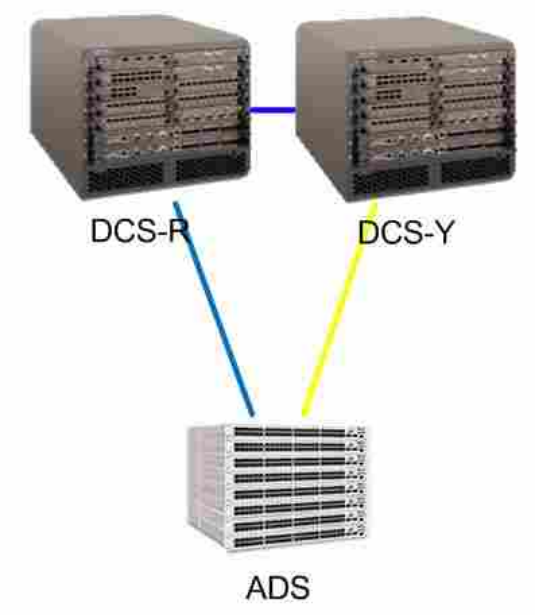


Figure 31 - UTOPIA DCS to ADS Redundancy

Similar to the IGMP snooping issues caused by RSTP topology changes on the iProvo network, this part of the UTOPIA network is also subject to short outages related to IGMP table inconsistencies. In this case, IGMP snooping running on the DCSs runs independently of this redundancy mechanism, so the IGMP table state of the backup DCS will likely not match multicast group memberships of the ADS immediately after a topology change, potentially causing a video outage that lasts until the next query interval.

Fortunately, device and link failures between the Distribution and Access layers of these networks are rare, so the vulnerability of a video service interruption of a few minutes in the case of a topology changes is considered by both networks to be an acceptable risk in their designs.

3.5.4 Customer Premises Equipment

At the Access layer of the network (where the handoff to the customer occurs), The iProvo network most commonly uses a World Wide Packets LE-46 device as the CPE. This

device has a 100 Mbps fiber uplink port to connect it to the distribution network. It has 5 customer facing 100 Mbps ports and 2 Plain Old Telephone Service (POTS) ports. Typically, the first port is configured for data services, and the rest for video services. This configuration is customizable, but is the most common configuration. For phone service, a phone line can be plugged into each of the 2 POTS ports using the VOIP adapter built into the CPE. Alternatively, one of the customer facing 100 Mbps ports can be configured to support an external telephone adapter (TA) such as a Linksys PAP2.

Figure 32 - World Wide Packets LE-46 [Image from World Wide Packets]

UTOPIA most commonly uses an Allied Telesis IMG606BD. The uplink is a fixed 100Mbps SMF bi-directional optic. This device has 6 customer facing 100 Mbps ports. Typically, the first port is configured for data services, ports 2-5 are configured for video service, and port 6 is configured for voice service. The IMG606BD does not have an internal VOIP adapter. UTOPIA initially installed models that did have built in VOIP adapters, but migrated away from them due to the difficulty of standardizing firmware, configurations, and management of multiple service providers having to interoperate with the CPE and their various phone switches.

Figure 33 - Allied Telesis iMG606BD [Image from Allied Telesis]

Both networks considered using hardened CPEs (weather proof) in a secure enclosure, installed at a relatively standard location (near electrical utility boxes). This would allow for physical access to the CPE without coordination from the customer, better physical security for the CPE, and a convenient location for tying into Advanced Metering Infrastructure (AMI) systems. Unfortunately, such hardened portals are very costly. Instead, for the sake of reducing costs for the project, the iProvo and UTOPIA networks opted for non-hardened CPEs that would be installed indoors. This carries with it the advantage that the CPE can be installed in a more central location which makes in-house wiring more manageable. However, it does mean that it is more vulnerable to customer service interruptions (i.e. disconnected power), less standardized installations, and greater difficulty in accessing the device physically.

Each CPE must also have a UPS to provide backup power in the case of a power outage. Voice services are considered to be a “life-line” service and are expected to be available in the case of a power outage. Several manufacturers offer UPS devices specifically targeted at the FTTH market. The base model is generally a model that has a 12 volt battery rated at 7.2AH. The UTOPIA CPE (Allied Telesis iMG606BD) draws 6 watts at 12 volts under normal use. At perfect efficiency, this would yield over 14 hours of backup time. However, the UTOPIA CPE does not include a telephone adapter. In the case that a Linksys PAP2 model telephone adapter (commonly used by UTOPIA service providers) is used, the backup time will be significantly

less. The Linksys PAP2 consumes 5 watts at 5 volts. Therefore, a 7.2AH battery with both a UTOPIA CPE and a Linksys PAP2 connected to it will yield about 4.8 hours of backup time. In practical use, the backup time can be expected to be closer to four hours, which is considered to be acceptable by UTOPIA and its service providers. There is no official standard for how long batteries are required to last for FTTH networks, and UTOPIA has accepted 4 hours as the requirement simply based on the common capacity of UPSs and the draw of common FTTH electronics.

3.6 Service Provider Coordination

For an open access network to be successful, it is vital that the service providers on that network be able to operate as efficiently as they would if they were operating their own network. In the early stages of the UTOPIA and iProvo networks, there was very little visibility into the network by service providers. Troubleshooting almost always required a telephone call to the Network Operations Center (NOC) to verify connectivity and collect other useful information. Out of both a desire to streamline their processes and to decrease the number of calls to the NOC, several features and tools were developed to allow service providers to operate more efficiently in an open access environment.

3.6.1 DHCP Option 82

DHCP Option 82 attaches information from the relay agent (aggregation switch above the CPE) to each DHCP request. This information contains the MAC address of the aggregation switch, as well as the physical port number that the DHCP request was received on. By itself, this information is useless to the service provider. However, the open access network operator

can identify the customers individually using this information and make that available to the service providers. This enables service providers to use DHCP Option 82 information to provision services and track each customer individually without direct access to the network municipal network devices. For example, a service provider would be able to create DHCP scopes for every neighborhood or city of the network by placing match statements in the DHCP configuration for the relay agent MAC address. They could also use this functionality to permanently assign IP addresses to specific customers using DHCP.

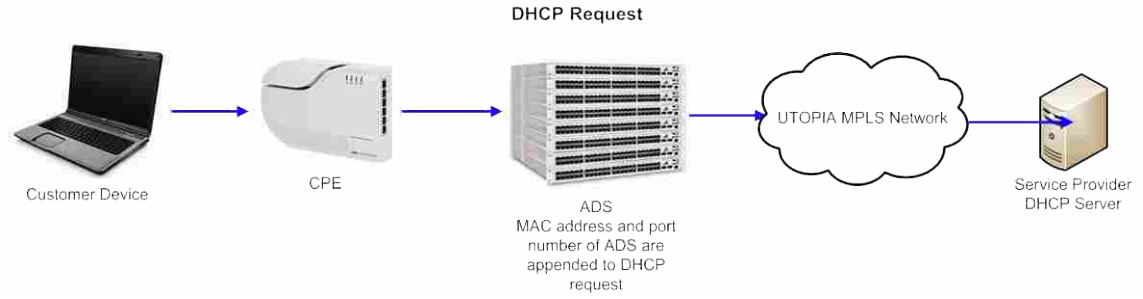


Figure 34 - DHCP Option 82 Request

3.6.2 Access to Information

Another feature that both networks implemented was a view-only interface for the demarcation device. The current UTOPIA interface provides the following information:

- Link status of all ports
- MAC address table of customer facing ports
- MAC address table of network facing ports
- Configured VLANS
- Configured rate limits
- Approximate throughput rate

- Port error counters
- Maximum Transmit Unit (MTU) setting
- Port Negotiation
- Uptime

This information is made available to service providers through a web based tool developed by UTOPIA staff and is known as AP View.

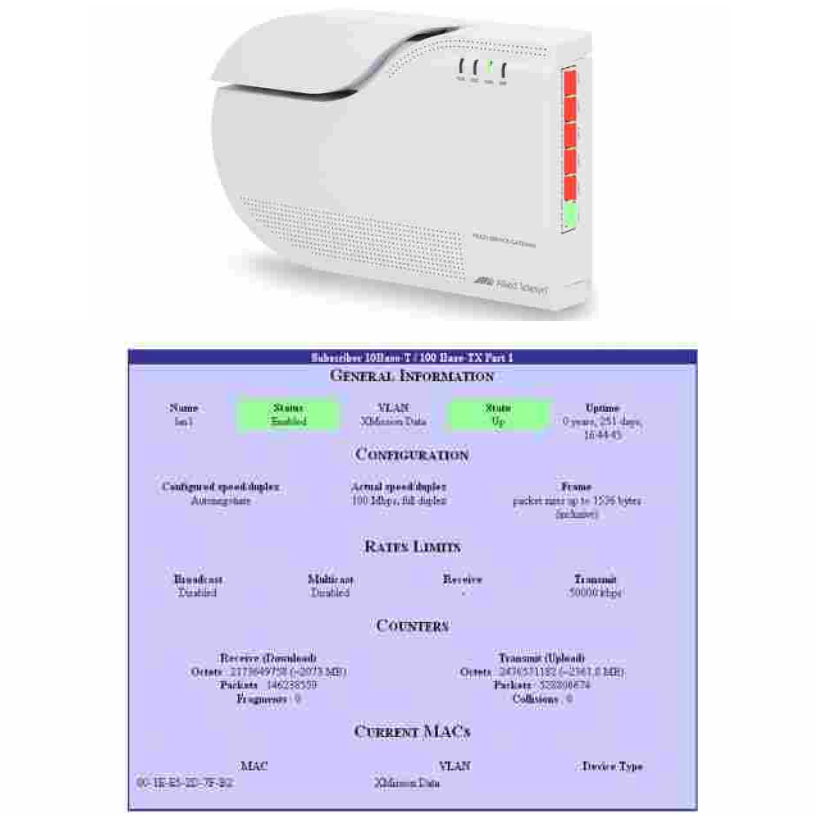


Figure 35 - UTOPIA AP View Interface

While not yet implemented, it is planned to add additional capabilities to the AP View tool that could allow service providers to immediately deactivate ports, activate ports, change VLAN assignments, change rate limits and other functions.

3.7 Monitoring

Both the iProvo and UTOPIA networks have implemented various forms of monitoring. They both have Network Operations Centers (NOCs) that are staffed 24/7 so that any emergency situations or serious outages can be dealt with, tracked, and escalated as soon as they are observed. Field technicians and engineers are also available on an on-call basis to respond to any network emergencies.

3.7.1 Network Monitoring System (NMS)

The NOC technicians and engineers at both iProvo and UTOPIA use an NMS to track and alert staff about network changes and outages. An NMS is a system that monitors network devices by polling and recording performance and status information. NMSs will also collect various statistics used for trending, link utilization, and Service Level Agreement (SLA) reports. Several commercial and open-source systems are available to provide this functionality. Both iProvo and UTOPIA use OpenNMS (http://www.opennms.org) as their primary monitoring system.

Figure 36 – UTOPIA OpenNMS Dashboard Screen

Provo also uses WhatsUpGold (http://whatsupgold.com) as a backup monitoring system and for visual modeling of the network.

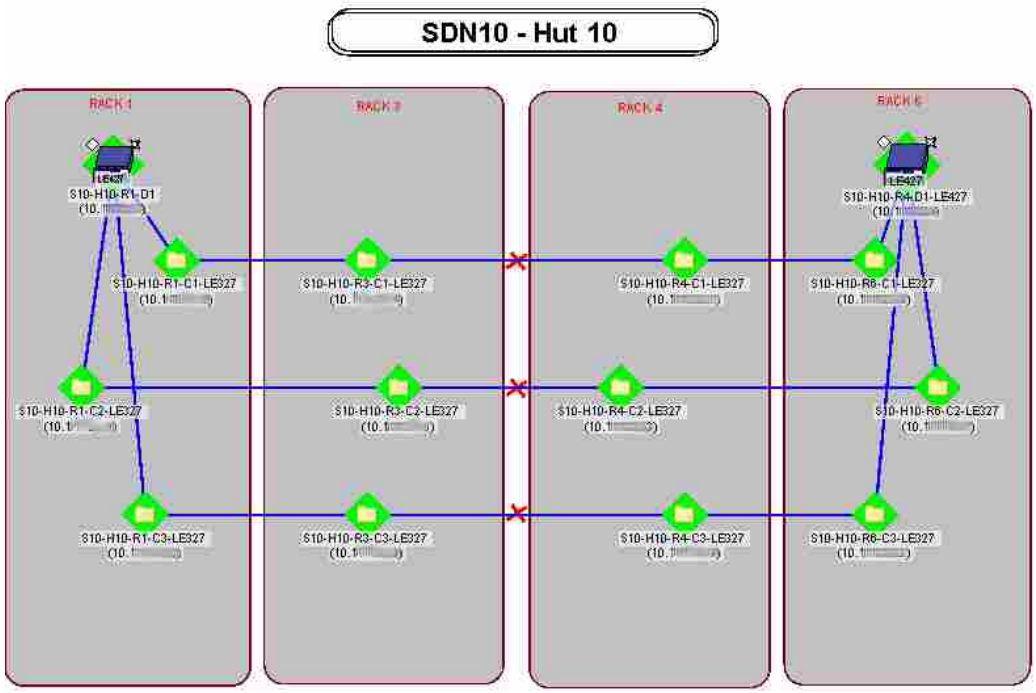


Figure 37 - iProvo WhatsUp Gold View of a Hut

UTOPIA has also implemented a backup monitoring system based on Zenoss Core and is working to implement it as their primary NMS.

Figure 38 - UTOPIA Zenoss Core Dashboard Screen

3.7.2 Core/Distribution/Access Monitoring

The network core, distribution, and access devices of the iProvo and UTOPIA networks are redundant, so typical ICMP (Ping) monitoring of each core device is not adequate. In the case of a link failure, all devices remain reachable by ICMP, and customer services are not seriously affected. However, any single failure of a link or redundant system makes the system vulnerable in the case of a second simultaneous failure. To detect any fiber cuts, optical transceiver failure, or support system failures that may not actually be causing an outage, the Core and Distribution devices are configured to send SNMP traps to the NMS when there is a

physical port change or other status change. The NOC receives a notification when SNMP traps are received by the NMS and can then investigate the cause so that backup links or other redundant systems can be repaired before a second failure occurs. The following are some examples of SNMP traps that are tracked and escalated to the engineering or field services groups to resolve:

- Port Link State Change
- High Temperature
- Port Error Count
- Power Supply Failure or Status Change
- Device Reboot
- RSTP or Label Switched Path (LSP) topology change
- Switch Fabric Failure
- Fan Failure
- Management Card Failure

3.7.3 CPE Monitoring

The typical CPE used in FTTH is capable of providing information about the condition of service at the hand-off point. The iProvo NMS actively monitors every CPE device and alerts on outages or battery status changes. The UTOPIA NMS monitors the CPEs for all non-standard residential type customers and alerts on outages. By actively monitoring CPEs in the network, the network operator can pro-actively respond to outages or other issues that may occur to individual customers

3.7.4 Bandwidth Monitoring

Both the UTOPIA and iProvo network closely monitor bandwidth use on the networks. Many times, problems are identified just by looking at bandwidth trends. Bandwidth trends are very repetitive and therefore any change can usually be attributed to some sort of network event.

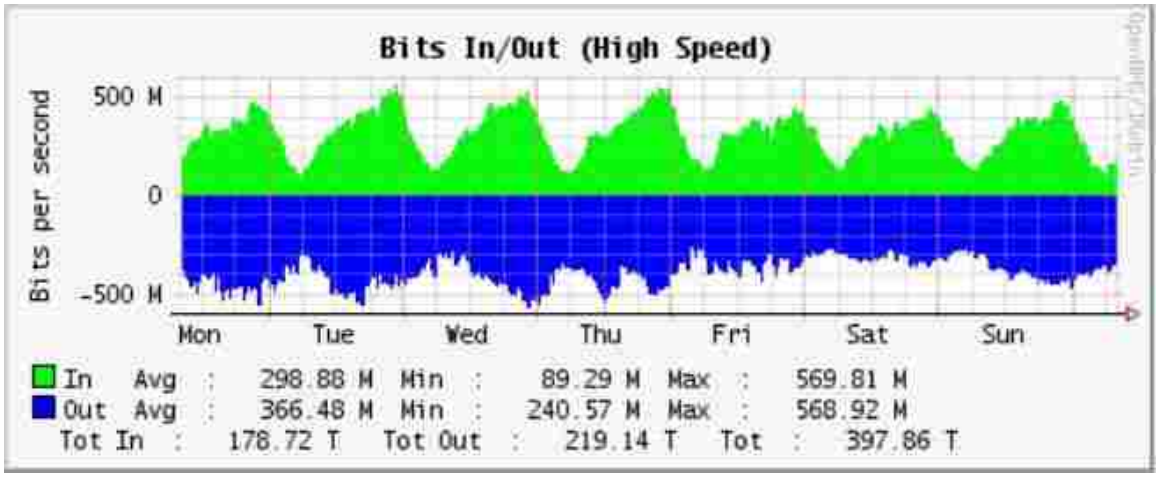


Figure 39 - Example Bandwidth Graph for Residential Data Service

The example above shows a residential data service interconnect port that represents several thousand customers. The trend shows fairly constant patterns day to day, with peak usage in the late evening, and the minimum usage in the early morning, with some irregularity in the weekend

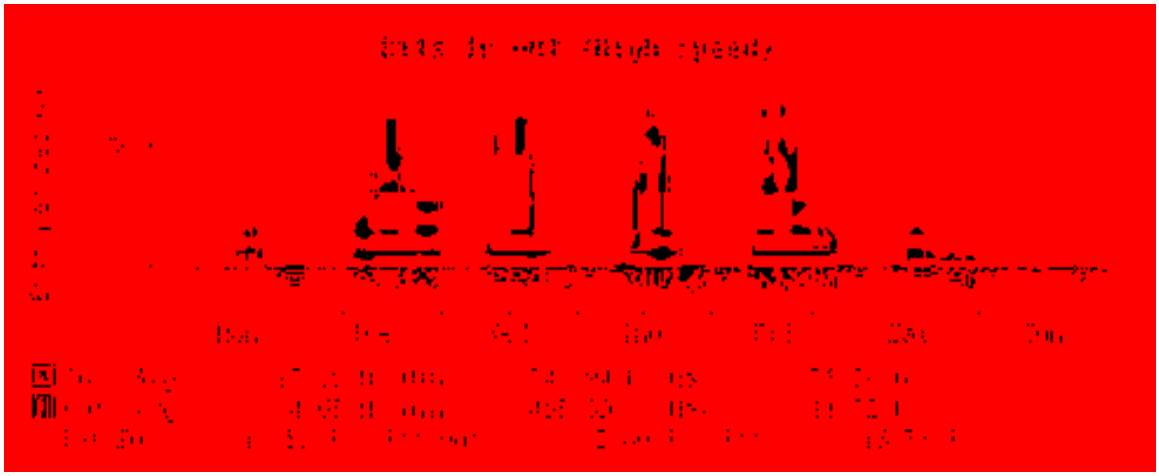


Figure 40 - Example Bandwidth Graph for Business Data Service

This example shows a business data service representing a few hundred business customers. The trend above shows a fairly constant pattern day to day, with very little use during the weekend. The peaks occur in the middle of the day, with the minimum usage in the early morning. This trend follows what would be expected for business data services, except for the Monday period. However, on this week, Monday was a holiday which explains the lower than expected bandwidth usage. If that weren't the case, there would be reason for concern and an issue may be raised with the service provider and network engineers to troubleshoot the variance.

3.7.5 Logging

Logging is an important tool for troubleshooting issues. On the UTOPIA and iProvo networks, there are frequently device or link issues that quickly resolve themselves. It can be difficult to troubleshoot these events, or even notice them, if they do not trigger alarms in the NMS. Proper logging allows engineers and NOC staff to find and troubleshoot problems that otherwise do not trigger alerts by the NMS. The UTOPIA network collects syslog messages from

all of the network devices for this purpose. Syslog is a standard messaging protocol for reporting and receiving log messages. UTOPIA uses a syslogd service running on a FreeBSD server. The following is an example from the UTOPIA syslog system.

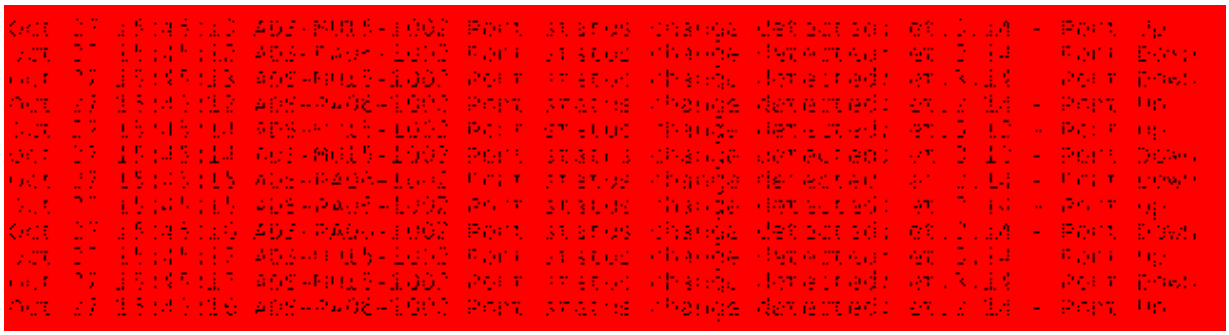


Figure 41 – UTOPIA Syslog Example

In this example, there are recurring port status changes on two ports on the network. These are ports that are not normally monitored and do not trigger alarms. However, the syslog messages indicate that they are repeatedly going up and down, suggesting a failure of the fiber, or optical transceiver for that link.

Another form of logging is accomplished by using authentication systems. UTOPIA uses Terminal Access Controller Access-Control System (TACACS) for user authentication into network devices. The TACACS system authenticates and logs every command issued by user. This enables the network operator staff `to identify when, what, and by whom any network configuration changes were made.

3.7.6 Physical Security

The network itself can be a valuable tool to enable various types of physical security. There are IP-enabled devices for almost every aspect of physical security (cameras, door sensors,

card scanners, and other security devices). Both the iProvo and UTOPIA networks use IP cameras to monitor physical access to the various sites. As well as being a very effective tool for internal use, having such a system in place is also an effective demonstration of the power of the network.

Figure 42 - Aviosys 9070-IR [Image from Aviosys]

The IP camera shown above is an IP enabled, high definition (1280x720 resolution) outdoor camera with infrared night vision capabilities. This camera outputs an MPEG-4 video stream at up to 4 Mbps. By installing cameras like these at each hut location, the network operator can easily record when employees enter the huts and identify them.

UTOPIA uses the open-source software Zoneminder (http://zoneminder.com) to manage the video recording and motion events from the various cameras they have installed. Zoneminder can also monitor sensor ports on IP cameras that have them, which can be used to monitor door sensors, motion sensors, or systems that can be tied to a digital sensor.

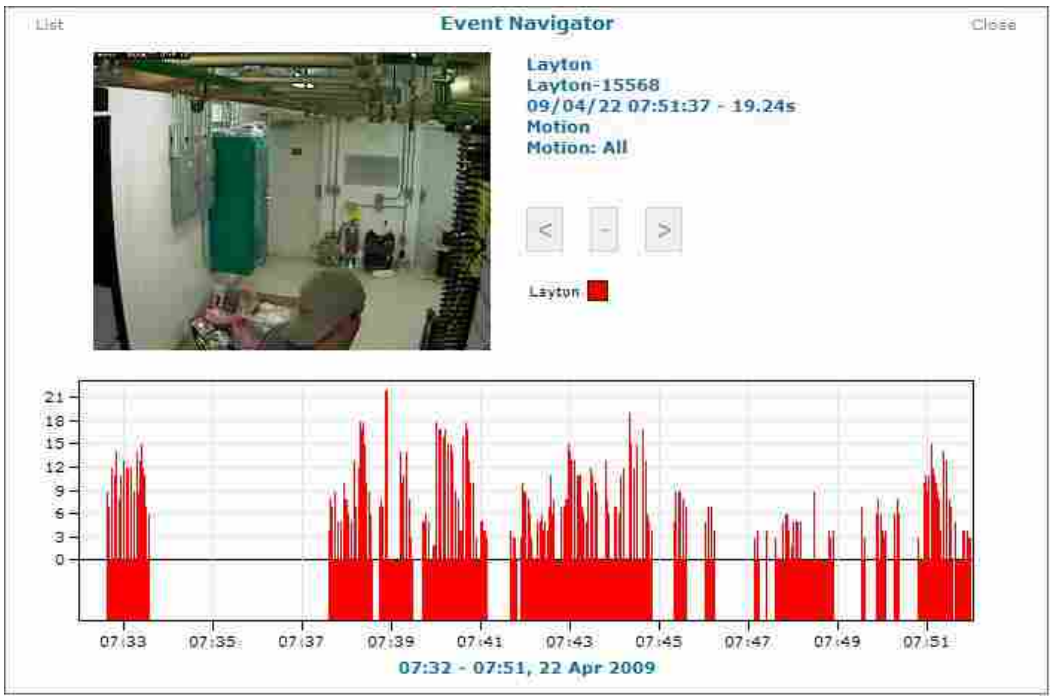


Figure 43 - Zoneminder Timeline View

Figure 44 - Zoneminder Montage View

3.8 Research Conclusions

It would be nearly impossible to collect and analyze every detail of a FTTH network operation. However, the information collected in this research is aimed at providing useful information that will aid in the decision making process for other FTTH networks as they consider architectures, systems, equipment, and operational requirements for an open access fiber network. The UTOPIA and iProvo networks have had financial difficulties, but they have been technical successes. They have brought advanced telecommunications to their customers and promoted more competition in their markets. It is hoped that the recommendations that can be made based on their experiences and deployments will be of great value to others who are considering their own open access fiber networks.

4 CONCLUSIONS

The intent of this research is to provide a set of recommendations and "best practices" for open access FTTH networks. It is expected that any open access FTTH network will need to conduct a feasibility study and business case for their project. It is hoped that these recommendations will play a vital role in the design and decision process of these networks. However, it is expected that some of these recommendations may not be followed due to the need to compromise between an ideal design, and the need to make the costs of the network fit within the financial constraints of the project. Therefore, these recommendations are not meant as definitive solutions for all open access fiber networks, but rather as suggestions to be considered when planning and designing an open access fiber network.

4.1 Physical Infrastructure

Typically the design of the physical infrastructure for a fiber network is outsourced to an engineering firm. It is assumed that the engineering firm will follow standards for fiber network design. However, based on this research, there are several additional recommendations or requirements that should be used in the design process.

4.1.1 Hut Design

Both the iProvo and UTOPIA projects began their projects with cabinet-based designs. This initially seemed to be the most cost effective way to deploy a large-scale fiber network.

However, both projects have either migrated (Provo) or are in the process of migrating (UTOPIA) to a hut-based design. Several aspects of the hut-design make it a preferable alternative to cabinets.

- Better insulation from external temperatures
- Additional space for more electronics
- Easier to access during inclement weather
- Fewer/larger network nodes makes technician time more efficient
- Larger, more reliable, more efficient air conditioning
- Larger, more reliable, more efficient UPS
- Fewer sites allow more advanced access and security systems to be installed
- Cleaner environment for electronics
- Less prone to vandalism

The recommendation of this research is that in most cases, the use of huts is preferable over cabinets. In general the costs are nearly the same for suburban type deployments, but there are many benefits of huts over cabinets. However, areas that are more rural would require greater fiber construction costs for a hut based design, so there is a threshold where cabinets become far more economical than huts. For fully urbanized areas, cabinets may also be preferable because of the difficulty and cost of obtaining locations to house huts.

4.1.2 Footprint Size

Obviously, each city or community being designed for a FTTH network should consider factors that may influence the size of the footprint (i.e. population density, easement access). However, from the experiences of the iProvo and UTOPIA networks, the preferred design is to

implement larger fiber footprints that include approximately 2500-3500 premises. It becomes increasingly difficult to manage fibers as the number of fibers per site increases beyond this, and cost of fiber grows exponentially as the footprint size gets larger. 2500-3500 is roughly the amount of fibers that can easily be managed (with supporting electronics) in the space of a typical hut structure.

4.1.3 Support Systems

The support systems for an open access fiber network should meet the following requirements.

- At least two air conditioners should be installed at every hut or cabinet, each with capacity for the entire hut or cabinet.
- At least two UPSs should be installed at every hut or cabinet, each with capacity for the entire hut or cabinet.
- Generators should be installed at all hut and cabinet locations.
- Natural gas fueled generators should be used except for where natural gas lines are not available.
- Support systems should be regularly tested.
- Support systems should be monitored either by IP sensor devices or SNMP management interfaces.

4.2 Layer 2 Design

Most large networks implement various levels of layer 3 routing throughout their networks. However, in order to provide network transparency and service provider flexibility for

an open access network, it is preferred to use layer 2 mechanisms to provide connectivity between service providers and their customers. Some of the advantages of this design are as follows:

- Greater speed – very low latency with 0 router hops
- Simplicity of configuration for the network operator
- Greater flexibility of services for service providers

4.3 Services

In an ideal scenario, the open access network provider is not directly involved in the services on its network. The network operator would simply provide transport for the services ordered by the various service providers on the network. It is recommended by this research, that if there is adequate competition on the open access network among its service providers, the network operator should act only as a wholesale transport provider. However, as demonstrated by iProvo and UTOPIA operating IPTV systems, it may be necessary to provide services in a wholesale/retail partnership if the service providers lack the resources to provide triple-play services on their own.

4.3.1 QoS

The actual QoS values and configuration will vary from system to system. However, open access fiber networks will likely adopt QoS policies that are relatively similar. It is a recommendation of this research that the open access fiber operator configure and implement a QoS policy that resembles the following:

Table 5 – QoS Policy Example

Priority	Name	Description
1	Management	Traffic to access and configure network devices - This includes Telnet, SSH, HTTP, SNMP, and ICMP polling.
2	Voice	Traffic for VOIP phone lines
3	Video	Multicast UDP IPTV traffic
4	TLS	Transparent LAN Service
5	Management Data	Various uses for the network operator that are high bandwidth, low priority, such as IP Cameras, Slingboxes, etc
6	Gold Data	Internet traffic for Businesses
7	Silver Data	Internet traffic for Residential Customers
8	Bronze Data	Internet traffic for complimentary services, such as public WiFi at parks, libraries, etc.

This table assumes that eight queues are available on the network hardware. If fewer are available, then the top 4 should be used with the rest of the services sharing the lowest priority queue.

4.3.2 Core/Distribution/Access

The ideal design for the Core, Distribution, and Access layers of the network would be to use all MPLS capable devices so that aspects of redundancy and service provisioning could be

handled within a single mechanism. This would eliminate issues of IGMP snooping states being inaccurate in the case of topology changes, as well as having to deal with the complexity of translating VLANs to VPLS services as services traverse between MPLS and non-MPLS enabled parts of the network. However, the costs for MPLS enabled devices can be significantly higher than for traditional Ethernet switching hardware. It is expected that over time, MPLS functionality will become more widely available in lower priced network hardware, and that at some point, MPLS itself will not be a financial obstacle.

Therefore, the recommendation from this research is that an open access fiber network design should use MPLS-based design for the entire Core, Distribution, and Access layers of the network, except where it is not financially reasonable to do so. At least two diverse fiber paths should connect each Core, Distribution, and Access device. The network devices in these layers should be fully redundant either by using pairs of separate devices, or using devices that have built in redundancy (multiple power supplies, switch fabrics, processors, etc). All support systems for these layers of the network should also be redundant (air conditioners, UPSs, etc).

The Core, Distribution, and Access devices should also support the following features:

- Redundant Power Supplies
- Redundant Switch Fabrics
- Redundant Control Modules/Processors
- MPLS/VPLS Support (where financially reasonable)
- 10 GigE interfaces (Core/Distribution)
- Support for generic manufacturer transceivers
- Support for single fiber bidirectional optical transceivers (Access)
- 19” Rack mountable

- Network Equipment Building System (NEBS) level 3 complaint
- 802.1p Class of Service
- 802.1Q VLAN Tagging (full range)
- IGMP Snooping v1/v2/v3
- 802.1ad-2005 for QinQ functionality
- SNMP v2c/v3 for NMS integration
- Up to 9000 byte jumbo frame support
- Telnet/SSH management access
- TACACS and Radius authentication supports
- DHCP Option 82 (Access only)
- Spanning Tree Protocol support (per VLAN and/or per VPLS)

4.3.3 CPE

For the purposes of physical access and standardization of installation, an outdoor hardened CPE is preferred. However, internal CPEs are generally far more economical. Despite this preference, it is expected that many FTTH deployments will continue to use indoor CPEs due to the cost savings. This decision must be considered by each FTTH deployment to determine the best option based on their feasibility study.

Therefore, the recommendation of this research is that outdoor hardened CPEs are preferable, but indoor CPEs may be used when financially necessary. The CPE should be installed with a UPS that will last 4 hours or more. There is no official standard for the duration of backup batteries, but commonly available hardware is typically designed around a 4 hour backup time. The CPE must also support the following features:

- 100 Mbps or greater SFP uplink port that supports single fiber bidirectional optics
- At least 6 customer facing 100 Mbps ports (1-Data, 1-Voice, 4-Video)
- 12V Power Input for Telco-type UPS integration
- Wall Mountable
- External sensor connectivity for monitoring UPS battery status, and UPS power source
- Per-port egress and ingress rate limiting
- 802.1p Class of Service with at least 4 priority queues
- 802.1Q VLAN Tagging (full range)
- IGMP Snooping v1/v2
- 802.1ad-2005 for QinQ functionality
- SNMP v2c/v3 for NMS integration
- Up to 9000 byte jumbo frame support
- Telnet/SSH management access
- TACACS and Radius authentication support
- Spanning Tree Protocol support
- Layer 2 filtering capabilities

Other features that should be considered, but may be cost prohibitive or unnecessary depending on the specific deployment, include the following:

- Time-domain reflectometer (TDR) for finding CAT5E cable faults
- Mocha or HPNA interfaces for using existing coaxial cabling
- Diagnostics capable uplink port and optics that report optical light levels
- Additional fiber capable port for stacking or ring configurations

- MPEG analyzer for troubleshooting video streams
- Port mirroring capabilities
- VOIP client with POTS ports
- Zigbee interface for operation with utility devices or home automation
- Casing that allows separate access for end customers and network technicians

4.4 Monitoring

An NMS must be used by the open access network provider to ensure proper operation and quick resolution to emergencies or outages. A 24/7 Network Operations Center should be used for larger networks to ensure proper response and reporting of all network events. The following should be monitored and create alarms when they change state:

- Port Link State Change
- High Temperature
- Port Error Count Increments
- Power Supply Failure or Status Change
- Device Reboot
- RSTP or Label Switched Path (LSP) topology change
- Switch Fabric Failure
- Fan Failure
- Management Card Failure
- High Bandwidth Thresholds

4.5 Conclusion

In the near future, it is expected that all telecommunications provider networks will by choice, or by government mandate, become open access in nature. Building and operating open access fiber networks is a very complicated and expensive endeavor. This research provides communities, municipalities, or other groups interested in designing and building open access FTTH networks with information and recommendations that will allow them to benefit from the experiences of the iProvo and UTOPIA networks.

REFERENCES

Adamski, D., “Broadband Stimulus Policy in Europe and the US: A Comparative Review,” 2009, Media Law & Policy Volume 18 Number 2, available from http://www.nyls.edu/user_files/1/3/4/30/84/187/245/Adamski,%20SPRING%202009,%2018%20MEDIA%20L.%20&%20POL’Y.pdf

Carlson, S., “A Historical, Economic, and Legal Analysis of Municipal Ownership of the Information Highway,” Rutgers Computer & Technology Law Journal, 25, 1, 54-55 (1999)

Chalon, D.; Durand, Y.; Richard, B., "An Overview of Automatic Network Configuration for IPv4 Applicances," HPL-2001-235, 2001, available from http://www.hpl.hp.com/techreports/2001/HPL-2001-235.pdf

Cherry, S., "A broadband utopia," Spectrum, IEEE , vol.43, no.5pp. 48- 54, May 2006

Cisco Systems, "DHCP Option 82 Support for Routed Bridge Encapsulation," available from http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrbeo82.pdf

Cisco Systems, “Optimizing Video Transport in Your IP Triple Play Network,” Cisco Systems Whitepapers, 2006, available from http://www.cisco.com/en/US/prod/collateral/routers/ps368/prod_white_paper0900aecd80478c12.pdf

Cisco Systems, “Diffserv - The Scalable End-to-End QoS Model,” Cisco Systems Whitepapers, 2006, available from http://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.pdf

Cisco Systems, "Virtual LAN Security Best Practices," Cisco Systems Application Note, 2002, available from http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf

D'Antonio, S.; D'Arienzo, M.; Pescape, A.; Ventre, G., "An architecture for automatic configuration of integrated networks," Network Operations and Management

Symposium, 2004. NOMS 2004. IEEE/IFIP , vol.1, no.pp. 351- 364 Vol.1, 19-23 April 2004

De Ghein, L., "MPLS Fundamentals", November 21, 2006, Cisco Press, available from http://proquest.safaribooksonline.com.erl.lib.byu.edu/1587051974

Dynamic City, "OSPN"; available from http://www.dynamiccity.com/city/ospn.html

Green, P.E., "Fiber to the home: the next big broadband thing," Communications Magazine, IEEE , vol.42, no.9pp. 100- 106, Sept. 2004

Lemay, R., “No NBN winner: Govt goes FTTH alone”, April 2009, ZDNet Australia, available from http://www.zdnet.com.au/news/communications/soa/No-NBN-winner-Govt-goes-FTTH-alone/0,130061791,339295839,00.htm

Lin, C., "Broadband optical access networks and fiber-to-the-home : systems technologies and deployment strategies", 2006, Chichester, England ; Hoboken, NJ : John Wiley, c2006.

Luo Rui; Ning Ti-gang; Li Tang-jun; Cai Li-bo; Qiu Feng; Jian Shui-sheng; Xu Jing-jing, "FTTH - a promising broadband technology," Communications, Circuits and Systems, 2005. Proceedings. 2005 International Conference on , vol.1, no.pp. 609- 612 Vol. 1, 27-30 May 2005

Moerman, K.; Fishburn, J.; Lasserre, M.; Ginsburg, D. Communications Magazine, IEEE, Vol.43, Iss.11, Nov. 2005 Pages: 142- 150

Occam Networks, "FTTx: Selecting the Best Architecture for the Access Network", May 2005, available from http://www.occamnetworks.com/pdf/WP_FTTX_FINAL.pdf

Provo General Information Website, available from http://www.iprovo.net/modules/xoopsfaq/index.php?cat_id=1#q4

Riverstone Networks, "FTTP Shootout - Active Ethernet vs. PON," Riverstone Networks Whitepapers, available from http://www.riverstonenet.com/pdf/pon_vs_active_ethernet.pdf

Technology Futures Inc., "Forecasts for Higher Bandwidth Broadband Services," available from http://www.tmcnet.com/tmcnet/articles/2005/broadband-ip-video-higher-bandwidth-forecast-technology-futures-vanston.htm

United States. Congress. Senate. Committee on Commerce, Science, and Transportation., "State and local issues and municipal networks", February 14, 2006, available from http://purl.access.gpo.gov/GPO/LPS76144

“Utah Municipal Cable Television and Public Telecommunications Services Act”, available from http://le.utah.gov/~code/TITLE10/10_0C.htm

World Wide Packets, "Choosing the Right Network Access Architecture," available from http://www.wwp.com/technology/white-papers/EthernetvPON-WhitePaper.pdf

World Wide Packets, "Introduction: The Expanding Role of Ethernet," available from http://www.wwp.com/technology/white-papers/CarrierEthernet-WhitePaper.pdf

APPENDIX A. BLOCKING OF CUSTOMER-TO-CUSTOMER TRAFFIC ON THE UTOPIA NETWORK

As discussed in Section 3.3.2.1, the UTOPIA network prevents network loops and any direct customer-to-customer traffic on the network. Several layers of configuration are required to enable this functionality. Typically, service providers interconnect to the UTOPIA network at devices known as Regional Core Switches (RCSs). The following is the configuration of a Virtual Private LAN Service (VPLS) which provides the connectivity from a service provider to the various Distribution Core Switches (DCSs). The configuration of a VPLS is dependent on Switched Data Paths (SDPs) being configured. Examples of SDP configuration can be found in Appendix C.

```
vpls 832 customer 1 create
      fdb-table-size 10000
      local-age 86400
      stp
          shutdown
      exit
      sap 9/2/15:832 create
      exit
      mesh-sdp 111:832 create
      exit
      mesh-sdp 112:832 create
      exit
      mesh-sdp 113:832 create
      exit
      mesh-sdp 114:832 create
      exit
      mesh-sdp 115:832 create
      exit
      mesh-sdp 116:832 create
      exit
      mesh-sdp 117:832 create
      exit
      mesh-sdp 118:832 create
      exit
      mesh-sdp 119:832 create
```

```
        exit
        mesh-sdp 120:832 create
        exit
        mesh-sdp 121:832 create
        exit
        mesh-sdp 122:832 create
        exit
        mesh-sdp 123:832 create
        exit
        mesh-sdp 124:832 create
        exit
        mesh-sdp 125:832 create
        exit
        mesh-sdp 126:832 create
        exit
        mesh-sdp 127:832 create
        exit
        mesh-sdp 128:832 create
        exit
        mesh-sdp 129:832 create
        exit
        mesh-sdp 130:832 create
        exit
        mesh-sdp 131:832 create
        exit
        mesh-sdp 133:832 create
        exit
        mesh-sdp 5911:832 create
        exit
        mesh-sdp 5912:832 create
        exit
        mesh-sdp 5913:832 create
        exit
        no shutdown
    exit
```

In this example, a Mesh SDP is configured to each DCS in the network. Traffic received from each DCS's Mesh SDP is not forwarded to other Mesh SDPs. However, it is forwarded to any SAPs. In this example, a SAP is configured on physical port 9/2/15. This physical port serves as an interconnect to a service provider for this service. The ":832" indicates that the port is configured as a 802.1Q tagged port, and therefore, traffic on this port is sent to the service provider as tagged traffic on VLAN 832. This enables a single interconnect port to act as a service provider interconnect for several services with each separated by VLAN number. The

customer-to-customer traffic is blocked by virtue of the Alcatel-Lucent implementation of VPLS that specifies that traffic from Mesh SDPs are not forwarded on to other Mesh SDPs.

At the DCS level, things are somewhat different. The VPLS service only points back to a few RCS devices via a Mesh SDP where a service provider interconnect may exist. However, all of the downstream Access Distribution Switches (ADSs) connect into the VPLS service via a Service Access Port (SAP). In this case, the SAP is a Link Aggregation Group (LAG), which is a group of physical ports that act as a single port. This is used in this situation to provide link redundancy to the ADS. The difficulty here is that traffic from SAPs typically is forwarded to other SAPs. This would allow direct customer-to-customer communication on the network. Therefore, split-horizon is used to prevent this. A split horizon group is created, and the SAPs are all configured to be a member of the group. According to the split horizon algorithm, traffic will not be forwarded between members of the same split horizon group, thus blocking any customer-to-customer traffic. Forwarding can also be managed at a more granular level by configuring multiple split horizon groups, but for the purposes of blocking customer-to-customer traffic, a single group is required.

```
vpls 832 customer 1 create
      fdb-table-size 10000
      split-horizon-group "P2MP-832" create
      exit
      stp
          shutdown
      exit
      sap lag-1:832 split-horizon-group "P2MP-832" create
      exit
      sap lag-2:832 split-horizon-group "P2MP-832" create
      exit
      sap lag-3:832 split-horizon-group "P2MP-832" create
      exit
      sap lag-4:832 split-horizon-group "P2MP-832" create
      exit
      sap lag-5:832 split-horizon-group "P2MP-832" create
      exit
      sap lag-6:832 split-horizon-group "P2MP-832" create
```

```
        exit
        sap lag-7:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-8:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-9:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-10:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-11:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-12:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-13:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-14:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-15:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-16:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-17:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-18:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-19:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-20:832 split-horizon-group "P2MP-832" create
        exit
        sap lag-23:832 split-horizon-group "P2MP-832" create
        exit
        mesh-sdp 5911:832 create
        exit
        mesh-sdp 5912:832 create
        exit
        mesh-sdp 5913:832 create
        exit
        no shutdown
    exit
```

The ADSs themselves must also be configured differently to block customer-to-customer traffic on their customer facing ports. The Alcatel-Lucent Omniswitch platform does this using its port-mapping function. The following is an example of port-mapping configuration on an Alcatel-Lucent OS6400-U24.

```
port mapping 1
port mapping 1 user-port 1/3
port mapping 1 user-port 1/4
port mapping 1 user-port 1/5
port mapping 1 user-port 1/6
```

```
port mapping 1 user-port 1/7
port mapping 1 user-port 1/8
port mapping 1 user-port 1/9
port mapping 1 user-port 1/10
port mapping 1 user-port 1/11
port mapping 1 user-port 1/12
port mapping 1 user-port 1/13
port mapping 1 user-port 1/14
port mapping 1 user-port 1/15
port mapping 1 user-port 1/16
port mapping 1 user-port 1/17
port mapping 1 user-port 1/18
port mapping 1 user-port 1/19
port mapping 1 user-port 1/20
port mapping 1 user-port 1/21
port mapping 1 user-port 1/22
port mapping 1 user-port 1/23
port mapping 1 user-port 2/1
port mapping 1 user-port 2/2
port mapping 1 user-port 2/3
port mapping 1 user-port 2/4
port mapping 1 user-port 2/5
port mapping 1 user-port 2/6
port mapping 1 user-port 2/7
port mapping 1 user-port 2/8
port mapping 1 user-port 2/9
port mapping 1 user-port 2/10
port mapping 1 user-port 2/11
port mapping 1 user-port 2/12
port mapping 1 user-port 2/13
port mapping 1 user-port 2/14
port mapping 1 user-port 2/15
port mapping 1 user-port 2/16
port mapping 1 user-port 2/17
port mapping 1 user-port 2/18
port mapping 1 user-port 2/19
port mapping 1 user-port 2/20
port mapping 1 user-port 2/21
port mapping 1 user-port 2/22
port mapping 1 user-port 2/23
port mapping 1 network-port linkagg 1
port mapping 1 enable
```

In the example above ports 1/24 and 2/24 are members of the link aggregation named “linkagg1” and serve as the uplink ports into the network. Ports 1/1 and 1/2 are excluded from the port mapping because they are used as utility ports for other network devices. Typically, switch stacks in the UTOPIA network include up to 8 devices and therefore the port-mapping may be configured through port 8/24.

APPENDIX B. UTOPIA REDUNDANCY CONFIGURATION

As discussed in section 3.4, redundancy in the core and distribution devices of the UTOPIA network is provided by MPLS. However, the ADSs do not support MPLS. Therefore, a different method for redundancy must be provided. UTOPIA does this with multi-chassis LAG configuration. This method allows ports from multiple DCS devices to participate in a single aggregation port, with one acting as a primary port, and the other as a standby port. The configuration is accomplished as follows:

First, we will assume that the underlying configuration is complete, including the slot, blade, and port configuration (see Appendix C for details). The ports on the DCSs facing the ADS are then configured to be part of a new LAG as follows:

```
lag 1
    description "TO-Some-ADS"
    mode access
    encap-type dot1q
    port 1/2/1 priority 10
    lacp active administrative-key 101
    no shutdown
exit
```

The lower “priority 10” setting is what makes this the primary port of the multichassis LAG. A higher value designates ports that will stay in standby mode if the lower priority port is active. In the UTOPIA network, the setting of “priority 20” is used for the backup DCS. The lag then needs to be configured to be part of a multichassis configuration.

```
redundancy
    multi-chassis
        peer 10.51.22.23 create
            source-address 10.51.22.24
            mc-lag
```

```
                lag 1 lacp-key 1 system-id 00:00:00:01:02:01 system-
                priority 100
                no shutdown
                exit
            no shutdown
            exit
        exit
    exit
```

This is configured on both DCSs, except for the peer and source-addresses being swapped. This example is on a DCS with IP address 10.51.22.24 with the other DCS having the IP address 10.51.22.23. Once this configuration is in place, then the ADSs also need to be configured for the LAG. The following is the configuration necessary on a Riverstone 8600 acting as an ADS in this configuration:

```
smarttrunk create st.1 protocol lacp
lacp set aggregator st.1 port-type gigabit-ethernet actor-key 1
partner-key 1
lacp set port gi.15.1 port-key 1 enable partner-key 1 timeout short
lacp set port gi.15.2 port-key 1 enable partner-key 1 timeout short
```

In this example, ports gi.15.1 and gi.15.2 are the two uplink ports that connect to the two DCSs.

An Alcatel-Lucent OS6400-U24 acting as an ADS in this configuration is configured as follows:

```
lacp linkagg 1 size 2 admin state enable
lacp linkagg 1 actor admin key 101
lacp linkagg 1 partner admin key 1
lacp agg 1/24 actor admin key 101
lacp agg 1/24 partner admin key 1
lacp agg 1/24 partner admin state active
lacp agg 2/24 actor admin key 101
lacp agg 2/24 partner admin key 1
lacp agg 2/24 partner admin state active
```

In this example, ports 1/24 and 2/24 are the two uplink ports that connect to the two DCSs.

APPENDIX C. WORKING ALCATEL-LUCENT OS-LS-6212 CONFIGURATION WITH QINQ VLAN TAGGING

The Alcatel-Lucent OS-LS-6212 is the device currently used in the UTOPIA network to provide QinQ Transparent LAN Services (TLS). QinQ refers to the double-tagging of Ethernet frames so that a customer may use the entire range of VLANs within a TLS. An example working configuration for QinQ is included below (edited for security reasons):

```
interface ethernet e1
description Customer1-QinQ-TLS
exit
interface ethernet e2
description Customer2-QinQ-TLS
exit
interface ethernet g2
description UpLink
exit
interface range ethernet e(1-2)
switchport mode customer
exit
interface ethernet g2
switchport mode trunk
exit
vlan database
vlan 1299,2132,2163
exit
interface ethernet g2
switchport trunk allowed vlan add 1299
exit
interface ethernet g2
switchport trunk allowed vlan add 2132
exit
interface ethernet e1
switchport customer vlan 2132
exit
interface ethernet g2
switchport trunk allowed vlan add 2163
exit
interface ethernet e2
switchport customer vlan 2163
exit
ip igmp snooping
interface vlan 1299
ip address 10.196.25.23 255.255.255.0
```

```
exit
ip default-gateway 10.196.25.1
hostname QinQ-Demarc
aaa authentication enable default none
aaa authentication login default tacacs line
snmp-server location SP-Location
snmp-server contact UtopiaEngineering
snmp-server community xxxxxxxxx ro 10.196.25.12 view Default
snmp-server host 10.96.0.10 xxxxxxxxx traps 2
tacacs-server host 172.16.10.13 key xxxxxxxxx
clock timezone -7 zone MST
clock summer-time recurring usa zone utc
clock source sntp
sntp client poll timer 120
sntp unicast client enable
sntp unicast client poll
sntp server 172.16.66.232
```

In this example, ports e1 and e2 each terminate a different TLS. Traffic that ingresses these ports is double-tagged with VLAN 2132 and 2163 respectively. A similar configuration on the other end of each TLS will strip these outer tags, allowing traffic from any VLAN to traverse the network between the TLS endpoints. The network operator only needs to configure the outer-tag VLAN through the core and distribution network devices that interconnect the TLS endpoint devices.

APPENDIX D. QOS EXAMPLES FROM IPROVO AND UTOPIA

In both the iProvo and UTOPIA networks, the majority of the QoS configuration takes place at the first aggregation device above the Customer Premises Equipment (CPE). In the UTOPIA network, this is typically a Riverstone 8600 and more recently some Alcatel-Lucent OS-6400's. The following is an excerpt from QoS configuration of a Riverstone 8600 .

```
qos set l2 name HIGH-250-4 priority high dest-mac any vlan 250 in-port-
list st.1 ignore-ingress-802.1p
qos set l2 name LOW-550-1 priority low dest-mac any vlan 550 in-port-
list st.1 ignore-ingress-802.1p
qos set l2 name LOW-650-0 priority low dest-mac any vlan 650 in-port-
list st.1 ignore-ingress-802.1p
qos set l2 name HIGH-950-5 priority high dest-mac any vlan 950 in-port-
list st.1 ignore-ingress-802.1p
qos set l2 name HIGH-1298-4 priority control dest-mac any vlan 1298 in-
port-list st.1 ignore-ingress-802.1p
qos set l2 name HIGH-250-4 priority high dest-mac any vlan 250 in-port-
list et.*.* ignore-ingress-802.1p
qos set l2 name LOW-550-1 priority low dest-mac any vlan 550 in-port-
list et.*.* ignore-ingress-802.1p
qos set l2 name LOW-650-0 priority low dest-mac any vlan 650 in-port-
list et.*.* ignore-ingress-802.1p
qos set l2 name HIGH-950-5 priority high dest-mac any vlan 950 in-port-
list et.*.* ignore-ingress-802.1p
qos set l2 name HIGH-1298-4 priority control dest-mac any vlan 1298 in-
port-list et.*.* ignore-ingress-802.1p
```

This configuration (modified for security purposes) sets different priority levels for different VLANs. In this example, VLAN 250 is used for video services (high priority), VLAN 550 and 650 are used for data services (low priority), VLAN 950 is used for voice services (high priority), and VLAN 1298 is used for device management purposes (control priority).

The priorities can also be set as numbers which correspond to the following textual values:

- 0 or 1 = Low
- 2 or 3 = Medium
- 4 or 5 = High
- 6 or 7 = Control

The “ignore-ingress-802.1p” setting configures the switch to apply the QoS setting regardless of what value is set in the 802.1p or CoS field in the Ethernet frame header. If this is not specified in the configuration, the switch will apply forwarding priority based on the CoS value in the incoming Ethernet frame header.

The iProvo network devices are configured somewhat differently to provide this type of functionality. The CPE devices have limited rate-limiting capabilities, so the QoS configuration of their access aggregation devices includes both traffic prioritization and rate-limiting.

```
      flow service-level create port 1 slid 1 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 1 slid 26 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 2 slid 2 cir 5056 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 2 slid 27 cir 256 pir 2560 priority 7
size min name SPVoiceSDN4
      flow service-level create port 3 slid 3 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 3 slid 28 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 4 slid 4 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 4 slid 29 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 5 slid 5 cir 512 pir 7040 priority 2
size large name SPDataSDN4
      flow service-level create port 5 slid 30 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 6 slid 6 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 6 slid 31 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 7 slid 7 cir 512 pir 15040 priority 2
size large name SPDataSDN4
```

```
      flow service-level create port 7 slid 32 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 8 slid 8 cir 512 pir 5056 priority 2
size large name SPDataSDN4
      flow service-level create port 8 slid 33 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 9 slid 9 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 9 slid 34 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 10 slid 10 cir 512 pir 2048 priority 2
size large name SPDataSDN4
      flow service-level create port 10 slid 35 cir 256 pir 512 priority 2
size min name SPVoice500k
      flow service-level create port 11 slid 11 cir 512 pir 2048 priority 2
size large name SPDataSDN4
      flow service-level create port 11 slid 36 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 12 slid 12 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 12 slid 37 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 13 slid 13 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 13 slid 38 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 14 slid 14 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 14 slid 39 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 15 slid 15 cir 512 pir 15040 priority 2
size large name SPDataSDN4
      flow service-level create port 15 slid 40 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 16 slid 16 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 16 slid 41 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 17 slid 17 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 17 slid 42 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 18 slid 18 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 18 slid 43 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 19 slid 19 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 19 slid 44 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 20 slid 20 cir 512 pir 15104 priority 2
size large name SPDataSDN4
      flow service-level create port 20 slid 45 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 21 slid 21 cir 512 pir 10048 priority 2
size large name SPDataSDN4
```

```
      flow service-level create port 21 slid 46 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 22 slid 22 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 22 slid 47 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 23 slid 23 cir 512 pir 15040 priority 2
size large name SPDataSDN4
      flow service-level create port 23 slid 48 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 24 slid 24 cir 512 pir 10048 priority 2
size large name SPDataSDN4
      flow service-level create port 24 slid 49 cir 256 pir 384 priority 7
size min name SPVoiceSDN4
      flow service-level create port 25 slid 25 cir 512 pir 10048 priority 2
name SPDataSDN4High
      flow service-level create port 25 slid 51 cir 512 pir 7104 priority 2
name SPDataSDN4Mid
      flow service-level create port 25 slid 52 cir 128 pir 512 priority 2
name SPDataSDN4Low
      flow service-level create port 25 slid 55 cir 1024 pir 1024 priority 5
size min name VideoSDN1-Up
      flow service-level create port 25 slid 56 cir 384 pir 10240 priority 7
size min name Voice-Up
      flow service-level create port 25 slid 57 cir 512 pir 2048 priority 2
name SPData2Mbps
      flow service-level create port 25 slid 58 cir 256 pir 512 priority 2
name SPVoice500k
      flow service-level create port 25 slid 59 cir 512 pir 2560 priority 2
name customvoice2500
      flow service-level create port 25 slid 61 cir 512 pir 15040 priority 2
size large name Data-15Mb
      flow service-level create port 25 slid 62 cir 512 pir 5056 priority 2
size large name Data-5Mb
      flow service-level create port 25 slid 63 cir 5056 pir 10048 priority 2
size large name Data-10/5Mb
      flow service-level create port 25 slid 64 cir 512 pir 2048 priority 7
size min name DataS4-2MB
      flow service-level create port 26 slid 50 cir 5952 pir 48000 priority 2
name SPDataSDN4
      !


      flow service-mapping create vlan 858 src-port 1 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 2 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 3 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 4 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 5 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 6 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 7 dst-port 25 slid 56
statistics-mode drop
```

```
      flow service-mapping create vlan 858 src-port 8 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 9 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 10 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 11 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 12 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 13 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 14 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 15 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 16 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 17 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 18 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 19 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 20 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 21 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 22 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 23 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 858 src-port 24 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 1 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 2 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 3 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 4 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 5 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 6 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 7 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 8 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 9 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 10 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 11 dst-port 25 slid 56
statistics-mode drop
```

```
      flow service-mapping create vlan 958 src-port 12 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 13 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 14 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 15 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 16 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 17 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 18 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 19 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 20 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 21 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 22 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 23 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 958 src-port 24 dst-port 25 slid 56
statistics-mode drop
      flow service-mapping create vlan 1099 src-port 1 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 2 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 3 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 4 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 5 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 6 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 7 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 8 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 9 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 10 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 11 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 12 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 13 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 14 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 15 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 16 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 17 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 18 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 19 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 20 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 21 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 22 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 23 dst-port 25 slid 55
      flow service-mapping create vlan 1099 src-port 24 dst-port 25 slid 55
      flow service-mapping create vlan 2158 dst-port 26 slid 50
      flow service-mapping create vlan 2158 src-port 11 dst-port 25 slid 57
      flow service-mapping create vlan 2158 src-port 25 dst-port 11 slid 11
      flow service-mapping create vlan 2858 src-port 1 dst-port 25 slid 25
      flow service-mapping create vlan 2858 src-port 3 dst-port 25 slid 25
      flow service-mapping create vlan 2858 src-port 4 dst-port 25 slid 25
      flow service-mapping create vlan 2858 src-port 5 dst-port 25 slid 25
```

```
flow service-mapping create vlan 2858 src-port 7 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 9 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 10 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 11 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 12 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 13 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 14 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 15 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 16 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 17 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 19 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 20 dst-port 25 slid 61
flow service-mapping create vlan 2858 src-port 21 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 22 dst-port 25 slid 25
flow service-mapping create vlan 2858 src-port 23 dst-port 25 slid 61
flow service-mapping create vlan 2858 src-port 24 dst-port 25 slid 64
flow service-mapping create vlan 2858 src-port 25 dst-port 1 slid 1
flow service-mapping create vlan 2858 src-port 25 dst-port 3 slid 3
flow service-mapping create vlan 2858 src-port 25 dst-port 4 slid 4
flow service-mapping create vlan 2858 src-port 25 dst-port 5 slid 5
flow service-mapping create vlan 2858 src-port 25 dst-port 7 slid 7
flow service-mapping create vlan 2858 src-port 25 dst-port 9 slid 9
flow service-mapping create vlan 2858 src-port 25 dst-port 10 slid 10
flow service-mapping create vlan 2858 src-port 25 dst-port 11 slid 11
flow service-mapping create vlan 2858 src-port 25 dst-port 12 slid 12
flow service-mapping create vlan 2858 src-port 25 dst-port 13 slid 13
flow service-mapping create vlan 2858 src-port 25 dst-port 14 slid 14
flow service-mapping create vlan 2858 src-port 25 dst-port 15 slid 15
flow service-mapping create vlan 2858 src-port 25 dst-port 16 slid 16
flow service-mapping create vlan 2858 src-port 25 dst-port 17 slid 17
flow service-mapping create vlan 2858 src-port 25 dst-port 19 slid 19
flow service-mapping create vlan 2858 src-port 25 dst-port 20 slid 20
flow service-mapping create vlan 2858 src-port 25 dst-port 21 slid 21
flow service-mapping create vlan 2858 src-port 25 dst-port 22 slid 22
flow service-mapping create vlan 2858 src-port 25 dst-port 23 slid 23
flow service-mapping create vlan 2858 src-port 25 dst-port 24 slid 24
flow service-mapping create vlan 2958 src-port 2 dst-port 25 slid 63
flow service-mapping create vlan 2958 src-port 6 dst-port 25 slid 25
flow service-mapping create vlan 2958 src-port 7 dst-port 25 slid 25
flow service-mapping create vlan 2958 src-port 8 dst-port 25 slid 62
flow service-mapping create vlan 2958 src-port 18 dst-port 25 slid 25
flow service-mapping create vlan 2958 src-port 23 dst-port 25 slid 25
flow service-mapping create vlan 2958 src-port 24 dst-port 25 slid 25
flow service-mapping create vlan 2958 src-port 25 dst-port 2 slid 2
flow service-mapping create vlan 2958 src-port 25 dst-port 6 slid 6
flow service-mapping create vlan 2958 src-port 25 dst-port 7 slid 7
flow service-mapping create vlan 2958 src-port 25 dst-port 8 slid 8
flow service-mapping create vlan 2958 src-port 25 dst-port 18 slid 18
flow service-mapping create vlan 2958 src-port 25 dst-port 23 slid 23
flow service-mapping create vlan 2958 src-port 25 dst-port 24 slid 24
```

This example from a World Wide Packets LE-327 includes the two parts of configuring QoS on these devices. The first part is to create various service levels defined as an association

of physical port, service level identifier (slid), committed information rate (cir), peak information rate (pir), priority level (priority), buffer size (size), and a label (name). The service level identifier is an arbitrary number used in other commands to identify the specific service level. The committed information rate is the amount of throughput guaranteed to be available for that service level. The peak information rate is the maximum throughput allowed for traffic within the service level. The priority level identifies which traffic takes priority when there is congestion or when the peak information rate is reached.

Priority	**Name**	**Description**
Undefined	Management	This priority includes traffic to access and configure the network devices. This includes Telnet, SSH, HTTP, SNMP, ICMP directed at the
2	Data	Internet traffic for Residential Customers
5	Video	Multicast UDP IPTV traffic
7	Voice	Voice traffic using VOIP

The buffer size portion of the service level creation statement defines how much traffic is buffered into memory before being discarded when the peak information rate is exceeded.

The second part of this configuration creates service-mappings that apply the rules of a service-level to a VLAN, source port (src-port), and destination port (dst-port). These switches have a limitation in that they can only support 99 service-mappings. Therefore, iProvo chose to only apply QoS settings for the upload direction for voice and video services.

The Alcatel-Lucent OS-6400 platform is currently used for newer UTOPIA areas and supports several queuing methods. They are defined as follows:

- Strict Priority – Higher priority queues are always services before lower priority queues.

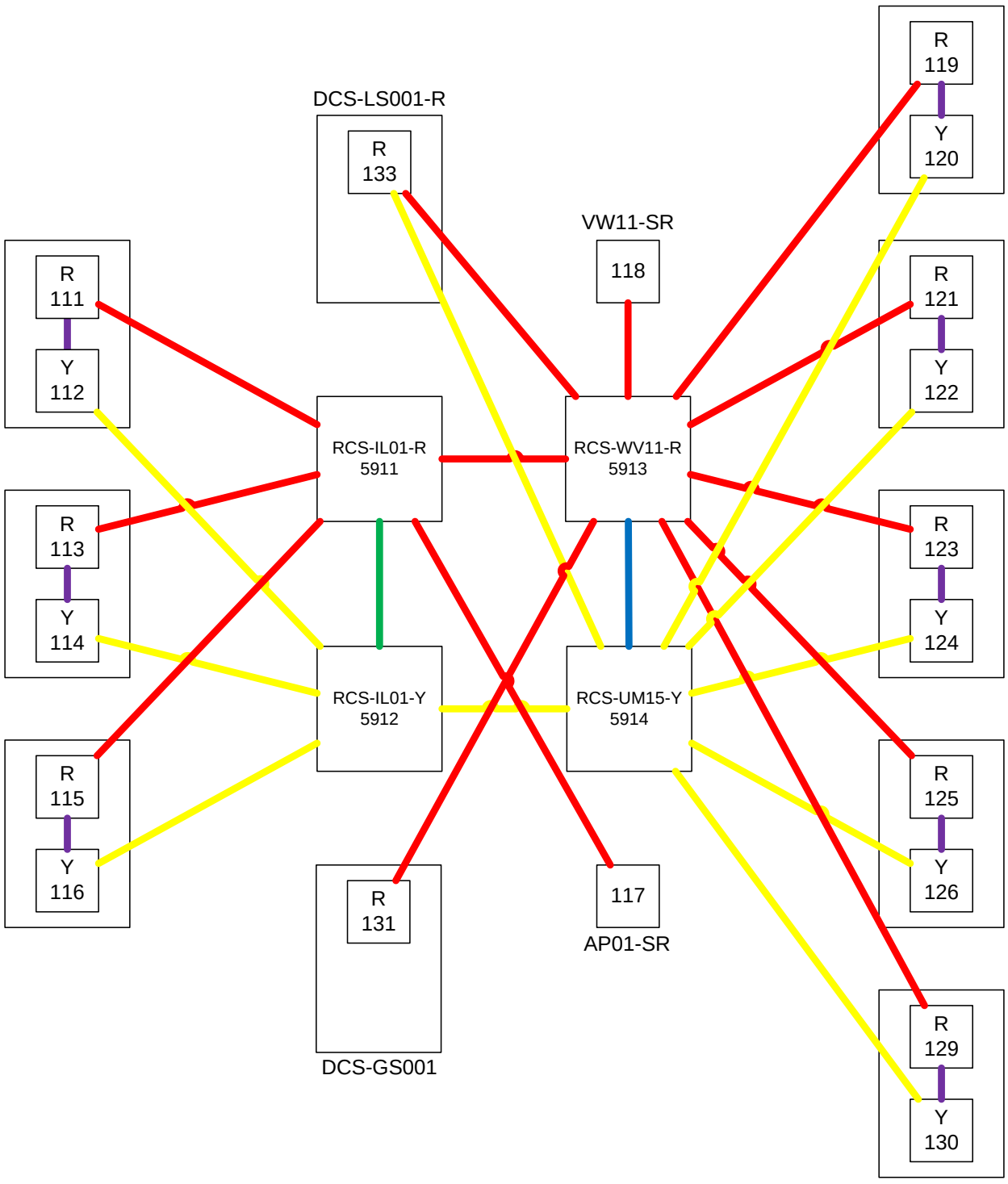
- WRR—All queues participate in a weighted round robin scheme. Traffic is serviced from each queue based on the weight of the queue.
- Priority-WRR—A type of WRR scheme that combines Strict-Priority queues (zero weight) and WRR queues (non-zero weight).
- DRR—All queues participate in a deficit round robin scheme. Traffic is serviced from each queue based on the weight of the queue.

These options give even more granular control of how QoS can be implemented in addition to the previous examples of rate limiting and prioritization. The default setting is WRR. However, UTOPIA has opted to apply Strict Priority in its network to ensure that lower priority services can not unexpectedly affect higher priority services.

APPENDIX E. WORKING ALCATEL-LUCENT ESS-12 7450 MPLS CONFIGURATION

The following is a diagram and working configuration file for an Alcatel-Lucent 7450 from the UTOPIA network. All passwords, hashes, IP addresses, customer names, and other confidential information has either been modified or removed for security purposes. Several portions of configuration that are repetitive have also been removed to shorten the length of the configuration file. Much of the configuration related to QoS settings and short descriptions of each section are also included

The following diagram shows the MPLS network with its MPLS interfaces identified by color. These colors correspond to the MPLS administrative group color designations that allow for primary and secondary path traffic engineering. The numbers on each device correspond to the switched data path (SDP) identifier referenced in the SDP configuration section below.


DCS-LS001-R
R
133
VW11-SR
118
R
119
Y
120
R
111
Y
112
R
121
Y
122
RCS-IL01-R
5911
RCS-WV11-R
5913
R
113
Y
114
R
123
Y
124
RCS-IL01-Y
5912
RCS-UM15-Y
5914
R
115
Y
116
R
125
Y
126
R
131
117
AP01-SR
DCS-GS001
R
129
Y
130

The configuration begins with general configuration options for the system name, time server, and timezone settings.

```
-----------------------------------------------
#-------------------------------------------------
echo "System Configuration"
#-------------------------------------------------
    system
        name "RCS-IL01-Y"
        snmp
            packet-size 9216
        exit
        login-control
            idle-timeout 120
        exit
        time
            ntp
                server 172.16.3.33
                no shutdown
            exit
            sntp
                shutdown
            exit
            dst-zone MDT
                start second sunday march 02:00
                end first sunday november 02:00
            exit
            zone MST
        exit
        thresholds
            rmon
            exit
        exit
    exit
```

This section specifies login and security related parameters. In this example a Terminal Access Controller Access-Control System (TACACS) is used which maintains a list of users, passwords, and access rights which can be centrally managed. It also sets the SNMP authentication parameters used by the NMS.

```
#-------------------------------------------------
echo "System Security Configuration"
#-------------------------------------------------
    system
        security
            telnet-server
            ftp-server
            tacplus
```

```
                    accounting
                    authorization
                    timeout 1
                    server 1 address 172.16.3.33 secret
"MfKCpBBbbFpa.aQkBeFh0haG6Gq732Sh" hash2
                exit
                user "admin"
                    password "1.ig98PBBBBiwsWBBBBB" hash2
                    access console ftp
                    console
                        member "administrative"
                    exit
                exitutopiareplace
                user "utopiareplace"
                    password "WR2bBBBBBBjUQVFIxwXoww.2avah" hash2
                    access snmp
                    snmp
                        authentication hash md5
918ffc493abcde12347f28601bb3eca privacy des 1c5de38592837591283a28920bfd8007
                        group "utopiareplace"
                    exit
                exit
                snmp
                    access group "utopiareplace" security-model usm
security-level privacy read "iso" write "iso" notify "iso"
                    community "utopiareplace" r version both
                exit
                per-peer-queuing
            exit
        exit
```

This section specifies log destinations and SNMP trap destinations.

```
    #-------------------------------------------------
    echo "Log Configuration"
    #-------------------------------------------------
        log
            syslog 1
                description "SP02"
                address 172.16.3.33
            exit
            snmp-trap-group 2
                description "Send traps to OpenNMS"
                trap-target "OpenNMS" address 10.233.233.10 snmpv2c notify-
community "utopiareplace"
                trap-target "Zenoss" address 10.233.233.53 snmpv2c notify-
community "utopiareplace"
            exit
            log-id 1
                description "Syslog to PS02"
                time-format local
                from main
                to syslog 1
            exit
            log-id 2
```

```
            description "SNMP traps to OpenNMS"
            from main security change
            to snmp 1024
        exit
    exit
#--------------------------------------------------
echo "System Security Cpm Hw Filters Configuration"
#--------------------------------------------------
    system
        security
        exit
    exit
```

This section specifies the types of Input/Output Modules (IOMs) and the cards that are installed in them. For example, “iom-20g-b” refers to a IOM that has 20 Gbps of backplane capacity. An M2-10gb-xfp refers to a Media Dependent Adapter (MDA) with two, 10 GigE XFP ports on it, which can be centrally managed.

```
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom-20g-b
        mda 1
            mda-type m20-1gb-sfp
        exit
    exit
    card 7
        card-type iom-20g-b
        mda 1
            mda-type m2-10gb-xfp
        exit
    exit
    card 8
        card-type iom-20g-b
        mda 1
            mda-type m1-10gb-xfp
        exit
        mda 2
            mda-type m1-10gb-xfp
        exit
    exit
    card 9
        card-type iom-20g-b
        mda 1
            mda-type m1-10gb-xfp
        exit
        mda 2
            mda-type m1-10gb-xfp
        exit
    exit
```

```
    card 10
        card-type iom-20g-b
        mda 1
            mda-type m1-10gb-xfp
        exit
        mda 2
            mda-type m1-10gb-xfp
        exit
    exit
```

This section specifies the configuration of the physical ports on the device. Most are configured as Ethernet ports with the mode as access, and “dot1q” encapsulation type. This configuration allows 802.1Q VLAN encapsulated frames to pass in and out on these ports, which is typical of any service provider interconnect ports. Auto-negotiation is enabled on some ports and disabled on others. Unfortunately, not all devices interoperate properly in regards to auto-negotiation despite it being part of the 802.3 standard. Therefore, in some instances, it may be necessary to disable it. In the example below, it is disabled on several service provider interconnect ports.

```
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 1/1/1
        description "SP1-Interconnect"
        ethernet
            mode access
            encap-type dot1q
        exit
        no shutdown
    exit
    port 1/1/2
        description "SP2-Interconnect"
        ethernet
            mode access
            encap-type dot1q
        exit
        no shutdown
    exit
    port 1/1/3
        description "SP3-Interconnect"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
```

```
port 1/1/4
    shutdown
    description "SP4_Interconnect Old"
    ethernet
        mode access
        encap-type dot1q
        no autonegotiate
    exit
exit
port 1/1/5
    description "SP4-Customer1-Temp"
    ethernet
        mode access
    exit
    no shutdown
exit
port 1/1/6
    description "SP5 Interconnect"
    ethernet
        mode access
        encap-type dot1q
        mtu 9212
    exit
    no shutdown
exit
port 1/1/7
    description "SP6 Interconnect"
    ethernet
        mode access
        encap-type dot1q
    exit
    no shutdown
exit
port 1/1/8
    description "TO-RCS-IL01-R"
    ethernet
        mode access
    exit
    no shutdown
exit
port 1/1/9
    description "TO-IL001-MGT"
    ethernet
        mode access
        encap-type dot1q
    exit
    no shutdown
exit
port 1/1/10
    description "TO-OMNI-11"
    ethernet
        mode access
        encap-type dot1q
    exit
    no shutdown
exit
port 1/1/11
```

```
        description "SP4_Interconnect_New"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/12
        description "RO21-PIM"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/13
        description "RO21-PIM"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/14
        description "SP7-Interconnect"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/15
        description "TO-PAS-IL01-02-5-1"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/16
        description "TO-PIM-IL01-02-2-1"
        ethernet
            mode access
            encap-type dot1q
            no autonegotiate
        exit
        no shutdown
    exit
    port 1/1/17
        description "TO-PIM-IL01-02-4-1"
        ethernet
            mode access
```

```
        encap-type dot1q
        no autonegotiate
    exit
    no shutdown
exit
port 1/1/18
    description "TO-PIM-IL01-02-6-1"
    ethernet
        mode access
        encap-type dot1q
        no autonegotiate
    exit
    no shutdown
exit
port 1/1/19
    description "SP5-Test"
    ethernet
        mode access
    exit
    no shutdown
exit
port 1/1/20
    description "SomeCity-Interconnect"
    ethernet
        mode access
        encap-type dot1q
        mtu 9212
    exit
    no shutdown
exit
port 7/1/1
    shutdown
    ethernet
    exit
exit
port 7/1/2
    shutdown
    ethernet
    exit
exit
port 8/1/1
    ethernet
    exit
    no shutdown
exit
port 8/2/1
    description "TO-RCS-IL01-R"
    ethernet
    exit
    no shutdown
exit
port 9/1/1
    description "TO-DCS-AP01-Y"
    ethernet
    exit
    no shutdown
exit
```

```
    port 9/2/1
        shutdown
        ethernet
        exit
    exit
    port 10/1/1
        description "TO-RCS-UM15-Y"
        ethernet
        exit
        no shutdown
    exit
    port 10/2/1
        ethernet
        exit
        no shutdown
    exit
```

This section is not used by UTOPIA and is in default state.

```
#--------------------------------------------------
echo "System Sync-If-Timing Configuration"
#--------------------------------------------------
    system
        sync-if-timing
            begin
            ref1
                shutdown
            exit
            ref2
                shutdown
            exit
            bits
                shutdown
            exit
            commit
        exit
    exit
```

This section shows an aggregation port that consists of two physical ports. This allows the logical port to remain in operation if one of the ports goes down as well as allowing the logical port to use aggregated amount of bandwidth provided by the member ports.

```
#--------------------------------------------------
echo "LAG Configuration"
#--------------------------------------------------
  lag 102
        description "RO21-PIM"
        mode access
        encap-type dot1q
        port 1/1/12
```

```
            port 1/1/13
            no shutdown
        exit
```

This section creates QoS rules that can be applied to Service Access Ports (SAPs). In this example, QoS is initially configured in this section, but not yet applied in the SAP configuration sections.

```
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        sap-ingress 10 create
            queue 1 create
            exit
            queue 11 multipoint create
            exit
        exit
        sap-ingress 11 create
            queue 1 create
            exit
            queue 11 multipoint create
            exit
            default-fc "l2"
        exit
        sap-ingress 12 create
            queue 1 create
            exit
            queue 11 multipoint create
            exit
            default-fc "af"
        exit
        sap-ingress 13 create
            queue 1 create
            exit
            queue 11 multipoint create
            exit
            default-fc "l1"
        exit
        sap-ingress 14 create
            queue 1 create
            exit
            queue 11 multipoint create
            exit
            default-fc "h2"
        exit
        sap-ingress 15 create
            queue 1 create
            exit
            queue 11 multipoint create
            exit
            default-fc "ef"
```

```
            exit
            sap-ingress 16 create
                queue 1 create
                exit
                queue 11 multipoint create
                exit
                default-fc "h1"
            exit
            sap-ingress 17 create
                queue 1 create
                exit
                queue 11 multipoint create
                exit
                default-fc "nc"
            exit
        exit
```

This section allows traffic filters. Most of the rules used in the UTOPIA network have been removed for security reasons, but one example is included below that targets several individual MAC addresses to be blocked.

```
#--------------------------------------------------
echo "Filter Configuration"
#--------------------------------------------------
    filter
        mac-filter 12490 create
            default-action forward
            description "Block MACs"
            entry 1 create
                match
                    src-mac 00:00:77:9d:1d:22 ff:ff:ff:ff:ff:ff
                exit
                action drop
            exit
            entry 2 create
                match
                    src-mac 00:0f:1f:6f:6c:b1 ff:ff:ff:ff:ff:ff
                exit
                action drop
            exit
            entry 3 create
                match
                    src-mac 00:14:22:10:be:c8 ff:ff:ff:ff:ff:ff
                exit
                action drop
            exit
        exit
    exit
#--------------------------------------------------
echo "Management Router Configuration"
#--------------------------------------------------
    router management
```

```
    exit
```

This section is the configuration of the router interfaces that face other Alcatel-Lucent 7450 devices.

```
#------------------------------------------------
echo "Router (Network Side) Configuration"
#------------------------------------------------
    router
        interface "TO-DCS-IL01-Y"
            address 10.22.0.10/30
            port 10/2/1
        exit
        interface "TO-DCS-RO21-Y"
            address 10.22.0.26/30
            port 8/1/1
        exit
        interface "TO-DCS-AP01-Y"
            address 10.22.0.38/30
            port 9/1/1
        exit
        interface "TO-RCS-IL01-R"
            address 10.22.0.14/30
            port 8/2/1
        exit
        interface "TO-RCS-UM15-Y"
            address 10.22.0.157/30
            port 10/1/1
        exit
        interface "system"
            address 10.11.255.12/32
        exit
        router-id 10.11.255.12
#------------------------------------------------
echo "Static Route Configuration"
#------------------------------------------------
        static-route 0.0.0.0/0 next-hop 10.3.0.1
```

This section enables Open Shortest Path First (OSPF) routing on the interfaces configured above.

```
#------------------------------------------------
echo "OSPFv2 Configuration"
#------------------------------------------------
        ospf
            asbr
            traffic-engineering
            export "ExportStatic"
            area 0.0.0.0
                interface "system"
                exit
```

```
            interface "TO-DCS-IL01-Y"
                interface-type point-to-point
            exit
            interface "TO-RCS-UM15-Y"
                interface-type point-to-point
            exit
            interface "TO-DCS-RO21-Y"
                interface-type point-to-point
            exit
            interface "TO-DCS-AP01-Y"
                interface-type point-to-point
            exit
            interface "TO-RCS-IL01-R"
                interface-type point-to-point
            exit
        exit
    exit
```

This section assigns color names to different MPLS groups. This allows Label Switched Paths (LSPs) to be assigned certain interfaces to use for primary and secondary use.

```
#------------------------------------------------
echo "MPLS Configuration"
#------------------------------------------------
    mpls
        admin-group "blue" 8
        admin-group "green" 10
        admin-group "magenta" 3
        admin-group "red" 1
        admin-group "yellow" 4
        interface "system"
        exit
        interface "TO-DCS-IL01-Y"
            admin-group "yellow"
        exit
        interface "TO-RCS-UM15-Y"
            admin-group "yellow"
        exit
        interface "TO-DCS-RO21-Y"
            admin-group "yellow"
        exit
        interface "TO-DCS-AP01-Y"
            admin-group "yellow"
        exit
        interface "TO-RCS-IL01-R"
            admin-group "green"
        exit
        path "TO-RCS-IL01-R-P"
            no shutdown
        exit
        path "TO-RCS-IL01-R-S"
            no shutdown
        exit
```

```
path "TO-DCS-IL01-R-P"
    no shutdown
exit
path "TO-DCS-IL01-R-S"
    no shutdown
exit
path "TO-DCS-IL01-Y-P"
    no shutdown
exit
path "TO-DCS-IL01-Y-S"
    no shutdown
exit
path "TO-DCS-RO21-R-P"
    no shutdown
exit
path "TO-DCS-RO21-R-S"
    no shutdown
exit
path "TO-DCS-RO21-Y-P"
    no shutdown
exit
path "TO-DCS-RO21-Y-S"
    no shutdown
exit
path "TO-DCS-AP01-R-P"
    no shutdown
exit
path "TO-DCS-AP01-R-S"
    no shutdown
exit
path "TO-DCS-AP01-Y-P"
    no shutdown
exit
path "TO-DCS-AP01-Y-S"
    no shutdown
exit
path "TO-DCS-VW11-R-P"
    no shutdown
exit
path "TO-DCS-VW11-R-S"
    no shutdown
exit
path "TO-DCS-VW11-Y-P"
    no shutdown
exit
path "TO-DCS-VW11-Y-S"
    no shutdown
exit
path "TO-DCS-UM01-R-P"
    no shutdown
exit
path "TO-DCS-UM01-R-S"
    no shutdown
exit
path "TO-DCS-UM01-Y-P"
    no shutdown
exit
```

```
path "TO-DCS-UM01-Y-S"
    no shutdown
exit
path "TO-DCS-UM15-R-P"
    no shutdown
exit
path "TO-DCS-UM15-R-S"
    no shutdown
exit
path "TO-DCS-UM15-Y-P"
    no shutdown
exit
path "TO-DCS-UM15-Y-S"
    no shutdown
exit
path "TO-DCS-AL09-R-P"
    no shutdown
exit
path "TO-DCS-AL09-R-S"
    no shutdown
exit
path "TO-DCS-AL09-Y-P"
    no shutdown
exit
path "TO-DCS-AL09-Y-S"
    no shutdown
exit
path "TO-DCS-VC03-R-P"
    no shutdown
exit
path "TO-DCS-VC03-R-S"
    no shutdown
exit
path "TO-DCS-VC03-Y-P"
    no shutdown
exit
path "TO-DCS-VC03-Y-S"
    no shutdown
exit
path "TO-DCS-CB04-R-P"
    no shutdown
exit
path "TO-DCS-CB04-R-S"
    no shutdown
exit
path "TO-DCS-CB04-Y-P"
    no shutdown
exit
path "TO-DCS-CB04-Y-S"
    no shutdown
exit
path "TO-MDCS-UM15-R-P"
    no shutdown
exit
path "TO-MDCS-UM15-R-S"
    no shutdown
exit
```

```
path "TO-MDCS-UM15-Y-P"
    no shutdown
exit
path "TO-MDCS-UM15-Y-S"
    no shutdown
exit
path "TO-MDCS-LS01-Y-P"
    no shutdown
exit
path "TO-MDCS-LS01-Y-S"
    no shutdown
exit
path "TO-RDCS-IL01-R-P"
    no shutdown
exit
path "TO-RDCS-IL01-R-S"
    no shutdown
exit
path "TO-RDCS-IL01-Y-P"
    no shutdown
exit
path "TO-RDCS-IL01-Y-S"
    no shutdown
exit
path "TO-RCS-UM15-Y-P"
    no shutdown
exit
path "TO-RCS-UM15-Y-S"
    no shutdown
exit
path "TO-DCS-GS01-R-P"
    no shutdown
exit
path "TO-DCS-GS01-R-S"
    no shutdown
exit
path "TO-RCS-VW11-R-P"
    no shutdown
exit
path "TO-RCS-VW11-R-S"
    no shutdown
exit
path "TO-DCS-SomePoP-R-P"
    no shutdown
exit
path "TO-DCS-SomePoP-R-S"
    no shutdown
exit
path "TO-DCS-SomePoP-Y-P"
    no shutdown
exit
path "TO-DCS-SomePoP-Y-S"
    no shutdown
exit
```

Each LSP is configured here with the groups of MPLS interfaces to use for its primary and secondary paths. Any one physical outage in an area of the network should only be able to affect either the primary or secondary path, but not both.

```
lsp "TO-RCS-IL01-R"
    to 10.11.255.11
    cspf
    adspec
    primary "TO-RCS-IL01-R-P"
        adaptive
        include "green"
        exclude "blue"
        exclude "magenta"
        exclude "red"
        exclude "yellow"
    exit
    secondary "TO-RCS-IL01-R-S"
        standby
        adaptive
        include "blue"
        include "red"
        include "yellow"
        exclude "green"
        exclude "magenta"
    exit
    no shutdown
exit
lsp "TO-DCS-IL01-R"
    to 10.11.0.11
    cspf
    adspec
    primary "TO-DCS-IL01-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "red"
    exit
    secondary "TO-DCS-IL01-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-IL01-Y"
    to 10.11.0.12
```

```
        cspf
        adspec
        primary "TO-DCS-IL01-Y-P"
            adaptive
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "magenta"
            exclude "red"
        exit
        secondary "TO-DCS-IL01-Y-S"
            standby
            adaptive
            include "green"
            include "magenta"
            include "red"
            exclude "blue"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-DCS-RO21-R"
        to 10.11.0.13
        cspf
        adspec
        primary "TO-DCS-RO21-R-P"
            adaptive
            include "magenta"
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "red"
        exit
        secondary "TO-DCS-RO21-R-S"
            standby
            adaptive
            include "green"
            include "red"
            exclude "blue"
            exclude "magenta"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-DCS-RO21-Y"
        to 10.11.0.14
        cspf
        adspec
        primary "TO-DCS-RO21-Y-P"
            adaptive
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "magenta"
            exclude "red"
        exit
        secondary "TO-DCS-RO21-Y-S"
```

```
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-AP01-R"
    to 10.11.0.15
    cspf
    adspec
    primary "TO-DCS-AP01-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "red"
    exit
    secondary "TO-DCS-AP01-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-AP01-Y"
    to 10.11.0.16
    cspf
    adspec
    primary "TO-DCS-AP01-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-DCS-AP01-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-RDCS-IL01-R"
```

```
        to 10.11.0.17
        cspf
        adspec
        primary "TO-RDCS-IL01-R-P"
            adaptive
            include "magenta"
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "red"
        exit
        secondary "TO-RDCS-IL01-R-S"
            standby
            adaptive
            include "green"
            include "red"
            exclude "blue"
            exclude "magenta"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-RDCS-IL01-Y"
        to 10.11.0.18
        cspf
        adspec
        primary "TO-RDCS-IL01-Y-P"
            adaptive
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "magenta"
            exclude "red"
        exit
        secondary "TO-RDCS-IL01-Y-S"
            standby
            adaptive
            include "green"
            include "magenta"
            include "red"
            exclude "blue"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-DCS-VW11-R"
        to 10.11.0.19
        cspf
        adspec
        primary "TO-DCS-VW11-R-P"
            adaptive
            include "magenta"
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "red"
        exit
```

```
    secondary "TO-DCS-VW11-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-VW11-Y"
    to 10.11.0.20
    cspf
    adspec
    primary "TO-DCS-VW11-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-DCS-VW11-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-UM01-R"
    to 10.11.0.21
    cspf
    adspec
    primary "TO-DCS-UM01-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "red"
    exit
    secondary "TO-DCS-UM01-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
```

```
lsp "TO-DCS-UM01-Y"
    to 10.11.0.22
    cspf
    adspec
    primary "TO-DCS-UM01-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-DCS-UM01-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-UM15-R"
    to 10.11.0.23
    cspf
    adspec
    primary "TO-DCS-UM15-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "red"
    exit
    secondary "TO-DCS-UM15-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-UM15-Y"
    to 10.11.0.24
    cspf
    adspec
    primary "TO-DCS-UM15-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
```

```
    exit
    secondary "TO-DCS-UM15-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-AL09-R"
    to 10.11.0.25
    cspf
    adspec
    primary "TO-DCS-AL09-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "red"
    exit
    secondary "TO-DCS-AL09-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-AL09-Y"
    to 10.11.0.26
    cspf
    adspec
    primary "TO-DCS-AL09-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-DCS-AL09-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
```

```
exit
lsp "TO-DCS-VC03-R"
    to 10.11.0.27
    cspf
    adspec
    primary "TO-DCS-VC03-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "red"
    exit
    secondary "TO-DCS-VC03-R-S"
        standby
        adaptive
        include "green"
        include "red"
        exclude "blue"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-VC03-Y"
    to 10.11.0.28
    cspf
    adspec
    primary "TO-DCS-VC03-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-DCS-VC03-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-CB04-R"
    to 10.11.0.29
    cspf
    adspec
    primary "TO-DCS-CB04-R-P"
        adaptive
        include "magenta"
        include "yellow"
        exclude "blue"
        exclude "green"
```

```
            exclude "red"
        exit
        secondary "TO-DCS-CB04-R-S"
            standby
            adaptive
            include "green"
            include "red"
            exclude "blue"
            exclude "magenta"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-DCS-CB04-Y"
        to 10.11.0.30
        cspf
        adspec
        primary "TO-DCS-CB04-Y-P"
            adaptive
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "magenta"
            exclude "red"
        exit
        secondary "TO-DCS-CB04-Y-S"
            standby
            adaptive
            include "green"
            include "magenta"
            include "red"
            exclude "blue"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-MDCS-LS01-Y"
        to 10.11.0.32
        cspf
        adspec
        primary "TO-MDCS-LS01-Y-P"
            adaptive
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "magenta"
            exclude "red"
        exit
        secondary "TO-MDCS-LS01-Y-S"
            standby
            adaptive
            include "green"
            include "magenta"
            include "red"
            exclude "blue"
            exclude "yellow"
        exit
```

```
    no shutdown
exit
lsp "TO-MDCS-UM15-Y"
    to 10.11.0.34
    cspf
    adspec
    primary "TO-MDCS-UM15-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-MDCS-UM15-Y-S"
        standby
        adaptive
        include "green"
        include "magenta"
        include "red"
        exclude "blue"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "fast-reroute"
    shutdown
exit
lsp "TO-RCS-UM15-Y"
    to 10.11.255.14
    cspf
    adspec
    primary "TO-RCS-UM15-Y-P"
        adaptive
        include "yellow"
        exclude "blue"
        exclude "green"
        exclude "magenta"
        exclude "red"
    exit
    secondary "TO-RCS-UM15-Y-S"
        adaptive
        include "blue"
        include "green"
        include "red"
        exclude "magenta"
        exclude "yellow"
    exit
    no shutdown
exit
lsp "TO-DCS-GS01-R"
    to 10.11.0.31
    cspf
    adspec
    primary "TO-DCS-GS01-R-P"
        adaptive
        include "green"
```

```
            include "red"
            exclude "blue"
            exclude "magenta"
            exclude "yellow"
        exit
        no shutdown
    exit
    lsp "TO-RCS-VW11-R"
        to 10.11.255.13
        cspf
        adspec
        primary "TO-RCS-VW11-R-P"
            adaptive
            include "green"
            include "red"
            exclude "blue"
            exclude "magenta"
            exclude "yellow"
        exit
        secondary "TO-RCS-VW11-R-S"
            standby
            adaptive
            include "blue"
            include "yellow"
            exclude "green"
            exclude "magenta"
            exclude "red"
        exit
        no shutdown
    exit
    lsp "TO-DCS-SomePoP-R"
        to 10.11.0.33
        cspf
        adspec
        primary "TO-DCS-SomePoP-R-P"
            adaptive
            include "green"
            include "red"
            exclude "blue"
            exclude "magenta"
            exclude "yellow"
        exit
        secondary "TO-DCS-SomePoP-R-S"
            standby
            adaptive
            include "magenta"
            include "yellow"
            exclude "blue"
            exclude "green"
            exclude "red"
        exit
        no shutdown
    exit
    no shutdown
exit
```

This section enables Reservation Protocol – Traffic Extenstions (RSVP-TE).

```
#--------------------------------------------------
echo "RSVP Configuration"
#--------------------------------------------------
        rsvp
            interface "system"
            exit
            interface "TO-DCS-IL01-Y"
            exit
            interface "TO-RCS-UM15-Y"
            exit
            interface "TO-DCS-RO21-Y"
            exit
            interface "TO-DCS-AP01-Y"
            exit
            interface "TO-RCS-IL01-R"
            exit
            no shutdown
        exit
#--------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------
        ldp
            interface-parameters
            exit
            targeted-session
            exit
        exit
    exit
```

This section is where the Switched Data Paths (SDPs) are configured. The SDP represents the logical path between any set of devices. The underlying LSP provides the physical path and redundancy that the SDP may traverse through the network.

```
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 create
            description "Default customer"
        exit
        customer 200 create
            description "Video Customer"
        exit
        sdp 111 mpls create
            description "SDP to DCS-IL01-R"
            far-end 10.11.0.111
            lsp "TO-DCS-IL01-R"
            keep-alive
```

```
        shutdown
    exit
    no shutdown
exit
sdp 112 mpls create
    description "SDP to DCS-IL01-Y"
    far-end 10.11.0.112
    lsp "TO-DCS-IL01-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 113 mpls create
    description "SDP to DCS-RO21-R"
    far-end 10.11.0.113
    lsp "TO-DCS-RO21-R"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 114 mpls create
    description "SDP to DCS-RO21-Y"
    far-end 10.11.0.114
    lsp "TO-DCS-RO21-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 115 mpls create
    description "SDP to DCS-AP01-R"
    far-end 10.11.0.115
    lsp "TO-DCS-AP01-R"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 116 mpls create
    description "SDP to DCS-AP01-Y"
    far-end 10.11.0.116
    lsp "TO-DCS-AP01-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 117 mpls create
    description "SDP to RDCS-IL01-R"
    far-end 10.11.0.117
    lsp "TO-RDCS-IL01-R"
    keep-alive
        shutdown
    exit
    no shutdown
```

```
exit
sdp 118 mpls create
    description "SDP to RDCS-IL01-Y"
    far-end 10.11.0.118
    lsp "TO-RDCS-IL01-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 119 mpls create
    description "SDP to DCS-VW11-R"
    far-end 10.11.0.119
    lsp "TO-DCS-VW11-R"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 120 mpls create
    description "SDP to DCS-VW11-Y"
    far-end 10.11.0.120
    lsp "TO-DCS-VW11-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 121 mpls create
    description "SDP to DCS-UM01-R"
    far-end 10.11.0.121
    lsp "TO-DCS-UM01-R"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 122 mpls create
    description "SDP to DCS-UM01-Y"
    far-end 10.11.0.122
    lsp "TO-DCS-UM01-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 123 mpls create
    description "SDP to DCS-UM15-R"
    far-end 10.11.0.123
    lsp "TO-DCS-UM15-R"
    keep-alive
        shutdown
    exit
    no shutdown
exit
sdp 124 mpls create
    description "SDP to DCS-UM15-Y"
```

```
        far-end 10.11.0.124
        lsp "TO-DCS-UM15-Y"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 125 mpls create
        description "SDP to DCS-AL09-R"
        far-end 10.11.0.125
        lsp "TO-DCS-AL09-R"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 126 mpls create
        description "SDP to DCS-AL09-Y"
        far-end 10.11.0.126
        lsp "TO-DCS-AL09-Y"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 127 mpls create
        description "SDP to DCS-VC03-R"
        far-end 10.11.0.127
        lsp "TO-DCS-VC03-R"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 128 mpls create
        description "SDP to DCS-VC03-Y"
        far-end 10.11.0.128
        lsp "TO-DCS-VC03-Y"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 129 mpls create
        description "SDP to DCS-CB04-R"
        far-end 10.11.0.129
        lsp "TO-DCS-CB04-R"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 130 mpls create
        description "SDP to DCS-CB04-Y"
        far-end 10.11.0.130
        lsp "TO-DCS-CB04-Y"
        keep-alive
```

```
            shutdown
        exit
        no shutdown
    exit
    sdp 131 mpls create
        description "SDP to DCS-GS01-R"
        far-end 10.11.0.131
        lsp "TO-DCS-GS01-R"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 132 mpls create
        description "SDP to MDCS-LS01-Y"
        far-end 10.11.0.132
        lsp "TO-MDCS-LS01-Y"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 133 mpls create
        description "SDP to DCS-SomePoP-R"
        far-end 10.11.0.133
        lsp "TO-DCS-SomePoP-R"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 134 mpls create
        description "SDP to MDCS-UM15-Y"
        far-end 10.11.0.134
        lsp "TO-MDCS-UM15-Y"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 5911 mpls create
        description "SDP to RCS-IL01-R"
        far-end 10.11.255.11
        lsp "TO-RCS-IL01-R"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 5913 mpls create
        description "SDP to RCS-VW11-R"
        far-end 10.11.255.13
        lsp "TO-RCS-VW11-R"
        keep-alive
            shutdown
        exit
        no shutdown
```

```
exit
sdp 5914 mpls create
    description "SDP to RCS-UM15-Y"
    far-end 10.11.255.14
    lsp "TO-RCS-UM15-Y"
    keep-alive
        shutdown
    exit
    no shutdown
exit
```

This section includes the creation and configuration of Virtual Private LAN Services (VPLSs). Each VPLS represents a service on the network. For example, VPLS 261 below is the configuration of some service provider's video service. It provides switching between the local LAG port (102), other core switches (via spoke-SDPs), and downstream switches (via mesh-SDPs). It also has IGMP snooping enabled to provide efficient forwarding of multicast streams.

```
vpls 261 customer 1 create
    stp
        shutdown
    exit
    igmp-snooping
        no shutdown
    exit
    sap lag-102:261 create
    exit
    spoke-sdp 112:261 create
    exit
    spoke-sdp 114:261 create
    exit
    spoke-sdp 116:261 create
    exit
    mesh-sdp 5911:261 create
    exit
    mesh-sdp 5913:261 create
    exit
    mesh-sdp 5914:261 create
    exit
    no shutdown
exit
vpls 290 customer 1 create
    stp
        shutdown
    exit
    sap 1/1/9:290 create
    exit
    sap lag-101:290 create
    exit
    no shutdown
exit
```

```
vpls 550 customer 1 create
    stp
        shutdown
    exit
    mesh-sdp 111:550 create
          ingress qos
    exit
    mesh-sdp 112:550 create
    exit
    mesh-sdp 113:550 create
    exit
    mesh-sdp 114:550 create
    exit
    mesh-sdp 115:550 create
    exit
    mesh-sdp 116:550 create
    exit
    mesh-sdp 117:550 create
    exit
    mesh-sdp 118:550 create
    exit
    mesh-sdp 119:550 create
    exit
    mesh-sdp 120:550 create
    exit
    mesh-sdp 121:550 create
    exit
    mesh-sdp 122:550 create
    exit
    mesh-sdp 123:550 create
    exit
    mesh-sdp 124:550 create
    exit
    mesh-sdp 125:550 create
    exit
    mesh-sdp 126:550 create
    exit
    mesh-sdp 127:550 create
    exit
    mesh-sdp 128:550 create
    exit
    mesh-sdp 129:550 create
    exit
    mesh-sdp 130:550 create
    exit
    mesh-sdp 131:550 create
    exit
    mesh-sdp 132:550 create
    exit
    mesh-sdp 133:550 create
    exit
    mesh-sdp 134:550 create
    exit
    no shutdown
exit
vpls 551 customer 1 create
    discard-unknown
```

```
fdb-table-size 10000
local-age 86400
stp
    shutdown
exit
sap 1/1/3:551 create
    description "TO-SP3"
    ingress
        filter mac 551
    exit
exit
mesh-sdp 111:551 create
exit
mesh-sdp 112:551 create
exit
mesh-sdp 113:551 create
exit
mesh-sdp 114:551 create
exit
mesh-sdp 115:551 create
exit
mesh-sdp 116:551 create
exit
mesh-sdp 117:551 create
exit
mesh-sdp 118:551 create
exit
mesh-sdp 119:551 create
exit
mesh-sdp 120:551 create
exit
mesh-sdp 121:551 create
exit
mesh-sdp 122:551 create
exit
mesh-sdp 123:551 create
exit
mesh-sdp 124:551 create
exit
mesh-sdp 125:551 create
exit
mesh-sdp 126:551 create
exit
mesh-sdp 127:551 create
exit
mesh-sdp 128:551 create
exit
mesh-sdp 129:551 create
exit
mesh-sdp 130:551 create
exit
mesh-sdp 131:551 create
exit
mesh-sdp 132:551 create
exit
mesh-sdp 133:551 create
exit
```

```
        mesh-sdp 134:551 create
        exit
        no shutdown
    exit
    vpls 902 customer 1 create
        stp
            shutdown
        exit
        sap 3/1/1:902 create
        exit
        mesh-sdp 111:902 create
        exit
        mesh-sdp 112:902 create
        exit
        mesh-sdp 113:902 create
        exit
        mesh-sdp 114:902 create
        exit
        mesh-sdp 115:902 create
        exit
        mesh-sdp 116:902 create
        exit
        mesh-sdp 117:902 create
        exit
        mesh-sdp 118:902 create
        exit
        mesh-sdp 119:902 create
        exit
        mesh-sdp 120:902 create
        exit
        mesh-sdp 121:902 create
        exit
        mesh-sdp 122:902 create
        exit
        mesh-sdp 123:902 create
        exit
        mesh-sdp 124:902 create
        exit
        mesh-sdp 125:902 create
        exit
        mesh-sdp 126:902 create
        exit
        mesh-sdp 127:902 create
        exit
        mesh-sdp 128:902 create
        exit
        mesh-sdp 129:902 create
        exit
        mesh-sdp 130:902 create
        exit
        mesh-sdp 131:902 create
        exit
        mesh-sdp 132:902 create
        exit
        mesh-sdp 133:902 create
        exit
        mesh-sdp 134:902 create
```

```
    exit
    no shutdown
exit
vpls 903 customer 1 create
    stp
        shutdown
    exit
    sap 3/1/1:903 create
    exit
    mesh-sdp 111:903 create
    exit
    mesh-sdp 112:903 create
    exit
    mesh-sdp 113:903 create
    exit
    mesh-sdp 114:903 create
    exit
    mesh-sdp 115:903 create
    exit
    mesh-sdp 116:903 create
    exit
    mesh-sdp 117:903 create
    exit
    mesh-sdp 118:903 create
    exit
    mesh-sdp 119:903 create
    exit
    mesh-sdp 120:903 create
    exit
    mesh-sdp 121:903 create
    exit
    mesh-sdp 122:903 create
    exit
    mesh-sdp 123:903 create
    exit
    mesh-sdp 124:903 create
    exit
    mesh-sdp 125:903 create
    exit
    mesh-sdp 126:903 create
    exit
    mesh-sdp 127:903 create
    exit
    mesh-sdp 128:903 create
    exit
    mesh-sdp 129:903 create
    exit
    mesh-sdp 130:903 create
    exit
    mesh-sdp 131:903 create
    exit
    mesh-sdp 132:903 create
    exit
    mesh-sdp 133:903 create
    exit
    mesh-sdp 134:903 create
    exit
```

```
    no shutdown
exit
vpls 1249 customer 1 create
    fdb-table-size 20000
    stp
        shutdown
    exit
    sap 1/1/6:1249 create
    exit
    sap 1/1/7:1249 create
    exit
    sap 1/1/9:1249 create
    exit
    sap 1/1/20:1249 create
    exit
    mesh-sdp 111:1249 create
    exit
    mesh-sdp 112:1249 create
    exit
    mesh-sdp 113:1249 create
    exit
    mesh-sdp 114:1249 create
    exit
    mesh-sdp 115:1249 create
    exit
    mesh-sdp 116:1249 create
    exit
    mesh-sdp 117:1249 create
    exit
    mesh-sdp 118:1249 create
    exit
    mesh-sdp 119:1249 create
    exit
    mesh-sdp 120:1249 create
    exit
    mesh-sdp 121:1249 create
    exit
    mesh-sdp 122:1249 create
    exit
    mesh-sdp 123:1249 create
    exit
    mesh-sdp 124:1249 create
    exit
    mesh-sdp 125:1249 create
    exit
    mesh-sdp 126:1249 create
    exit
    mesh-sdp 127:1249 create
    exit
    mesh-sdp 128:1249 create
    exit
    mesh-sdp 129:1249 create
    exit
    mesh-sdp 130:1249 create
    exit
    mesh-sdp 131:1249 create
    exit
```

```
        mesh-sdp 132:1249 create
        exit
        mesh-sdp 133:1249 create
        exit
        mesh-sdp 134:1249 create
        exit
        no shutdown
    exit
     vpls 2066 customer 1 create
        description "TLS-SP4-SomeNetwork1"
        stp
            shutdown
        exit
        sap 1/1/2:2066 create
        exit
        mesh-sdp 129:2066 create
        exit
        mesh-sdp 130:2066 create
        exit
        no shutdown
    exit
    vpls 2067 customer 1 create
        description "TLS-SP5-SomeNetwork2"
        service-mtu 5000
        stp
            shutdown
        exit
        sap 1/1/6:2067 create
        exit
        mesh-sdp 111:2067 create
        exit
        mesh-sdp 112:2067 create
        exit
        no shutdown
    exit
    vpls 2069 customer 1 create
        description "SP6 Demo TLS"
        stp
            shutdown
        exit
        sap 1/1/7:2069 create
        exit
        mesh-sdp 118:2069 create
        exit
        mesh-sdp 119:2069 create
        exit
        mesh-sdp 120:2069 create
        exit
        mesh-sdp 121:2069 create
        exit
        mesh-sdp 122:2069 create
        exit
        mesh-sdp 123:2069 create
        exit
        mesh-sdp 124:2069 create
        exit
        no shutdown
```

```
        exit
    exit
#-------------------------------------------------
echo "Router (Service Side) Configuration"
#-------------------------------------------------
    router
#-------------------------------------------------
echo "OSPFv2 Configuration"
#-------------------------------------------------
        ospf
        exit
#-------------------------------------------------
echo "Policy Configuration"
#-------------------------------------------------
        policy-options
            begin
            policy-statement "ExportStatic"
                entry 1
                    from
                        protocol static
                    exit
                    action accept
                    exit
                exit
            exit
            commit
        exit
    exit

#-------------------------------------------------
echo "System Time NTP Configuration"
#-------------------------------------------------
    system
        time
            ntp
            exit
        exit
    exit
-----------------------------------------------
```