NETWORK VIRTUALIZATION TO IMPROVE QUALITY OF SERVICE OF INTERACTIVE VIDEO TRANSMISSION

by

Kathy Nguyen

A Thesis Submitted to the Faculty of the

COLLEGE OF OPTICAL SCIENCES

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the College of Optical Sciences

THE UNIVERSITY OF ARIZONA

2015

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at the University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

SIGNED: Kathy Nguyen

APPROVAL BY THESIS DIRECTOR

This thesis has been approved on the date shown below:

______________________	05/08/2015
Alan Kost	Date
Professor of Optical Sciences	

Acknowledgments

I would like to thank my advisor, Alan Kost, who was so patient and encouraging during this thesis. He challenged me to think more technically and critically, which will be invaluable throughout my engineering career. Thank you to my thesis committee, Professor Khanh Kieu and Professor Robert A. Norwood, for taking time out your busy schedules to support the final step of my graduate studies. Thank you to Arthur Chen, who provided programming help and snacks. I would also like to thank my family and friends for the positive energy. Yay!!!

Table of Contents

List of Figures

Abstract

Quality of Service (QoS) of interactive video transmission determines the overall performance and quality of video viewed and experienced from both sending and receiving users. Interactive video is highly sensitive to jitter, or variable delay. Jitter is caused by suboptimal queuing management, processing delays, and network path changes. These factors are highly volatile due to intermittent network congestion and differing packet processing rates in the network queue. Network virtualization is proposed as a way of decreasing jitter during interactive video transmission. Virtualization works by combining network hardware and software resources with network functionality into a software-based virtual environment. As part of this thesis, a Gaussian random-number generator was used to investigate simulated packet transmission with errors on a dual fiber network path that employed network virtualization. We found that the overall jitter remained within the acceptable range for interactive video transmission, highlighting the role of network virtualization in improved QoS for interactive video transmission.

Chapter 1: Introduction

Optical fiber networks are the essential communication infrastructure for businesses, military, education, and residences. The spike in multimedia devices requiring Internet connection has caused an unprecedented demand in bandwidth and network footprints. Businesses and education no longer rely on just desktop computers and laptops; they now rely on smart phones, tablets, and virtual meetings. In addition to businesses and universities leasing fiber lines, private residences want optical fibers to replace copper cable. Carriers and service providers are scrambling to keep pace with demand, but struggle to expand and deliver networks in a timely fashion. Furthermore, there is high demand commercially available optical fiber networks and infrastructure that can be customized to satisfy regional needs.

Leasing a fiber line between two locations is expensive, especially if the locations are off-net; off-net locations are sites outside of a service provider's fiber network. If an Internet service provider foresees a future need in a specific region and the customer is willing to pay and wait for construction, then service providers will install more backbone cable, expanding their footprint. But, in many cases, limited external infrastructure and city permit regulations prolong construction time, while increasing construction expenses. In addition, some cities only allow field engineers to maintain and construct fiber in tunnels for a few hours a day, with further restrictions in certain locations, such as tunnels underneath railway tracks. Moreover, there is nationwide moratorium on construction during holiday season. For these reasons, if a customer is looking for an affordable and timely solution to their bandwidth needs, then the most time and cost efficient option is leasing fiber (or copper) cable from a third party.

Universities may need less bandwidth during summer months and holidays, while consumers and online retailers need more bandwidth and reliability during holidays. Professional sports associations need upgraded and reliable Internet service for championship tournaments. Consumer networks are stagnant once annual contracts are signed; however, their bandwidth needs and reliability constantly change. Service providers can heavily fine consumers for changing, downgrading, or upgrading their leased fiber-line contracts before the term-of-service ends. Additionally, service providers are slow to upgrade current equipment or invest in new equipment and hardware. As a result, consumers and service providers are not keeping pace with demand and customization of leased fiber lines.

Given the growth and continuous demand for Internet connection and service, reliability is key for universities, businesses, and the public. The reliability of real-time applications, such as interactive video, is sensitive to momentary bandwidth scarcity and network congestion. In telecommunications, quality of service (QoS) describes the overall performance or quality specification of a communications channel or system. By monitoring system performance parameters, QoS data can qualitatively and quantitatively describe how packets move through a fiber optic network. QoS parameters in a fiber network are based on target values desired by those sending information and the lowest quality acceptable thresholds agreed upon by the transmitting and receiving parties.

Service providers tend to resist upgrades to infrastructure that would support cutting-end telecommunications technologies, they are reluctant to overhaul and change current and long term contracts and equipment supporting millions of live-traffic fiber lines. Customers are locked in to stagnant contracts with service providers, who implement incremental changes and maintenance updates. Consequently, drastic physical changes in current Internet architecture and hardware are very unlikely [1]. A transition from traditional optical fiber network and hardware components to a hybrid of heterogeneous network architectures cohabitating with shared physical infrastructure would segue to telecommunications advancement. Network virtualization separates the roles of traditional Internet service providers into two entities: infrastructure providers and virtual service providers. Infrastructure providers manage physical infrastructure and virtual service providers create virtual networks by aggregating multiple resources from infrastructure providers offering end-to-end services [2]. Current service providers manage and implement all physical and end-to-end services. Network virtualization allows clients and businesses to dynamically manage and change their services without contract restrictions or hindering QoS. It encourages a more adaptive change to Internet services without compromising QoS due to the overhaul of current infrastructure.

Chapter 2: Background

2.1 Internet Birth and Growth

In 1958, the United States Department of Defense created the Advanced Research Projects Agency (ARPA) to initiate a research program investigating communication technology and techniques. This program was designed around the ideas of robustness, reliability, and redundancy, such that communication continues in the event of a nuclear war. The Advanced Research Projects Agency Network (ARPANET) focused on and succeeded in becoming the first large-scale packet-switched network. ARPANET functioned on the concept of each node storing a copy of the packet until it was received at the next node. ARPANET nodes also required that each node use identical processors, which are called Interface Message Processors (IMPs) to form a subnet. IMPs were connected to each other via phone lines [3]. In an ARPANET layout, messages sent from host sites are sent to IMPs, and then finally sent to its designated host site.

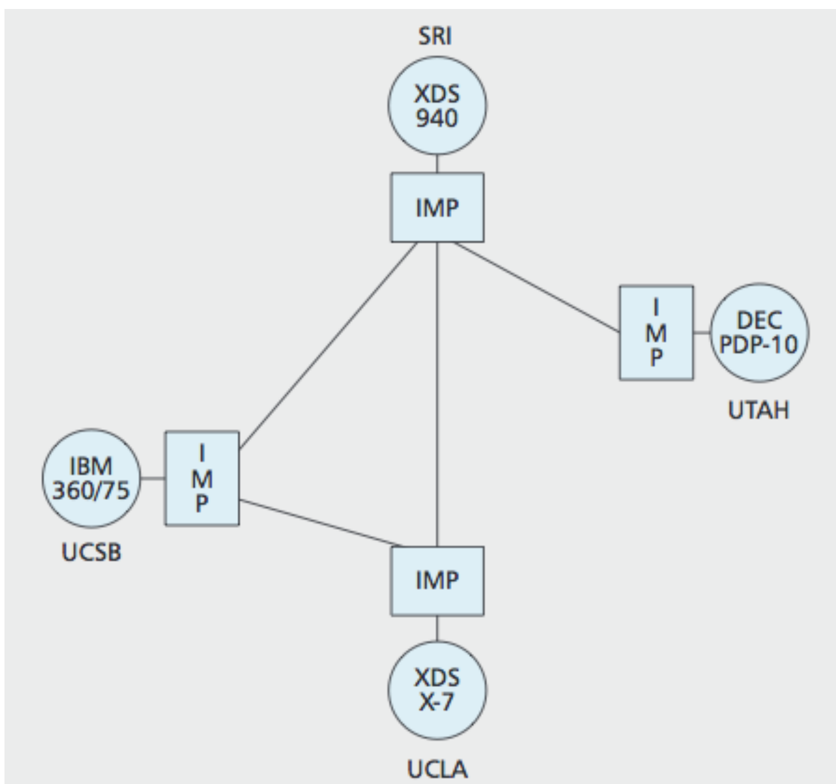

Figure 1: The initial four-node ARPANET in 1969 [4]

The first site to receive an IMP was the University of California, Los Angeles (UCLA). The second site to receive an IMP was Stanford Research Institute (SRI), followed by University of California, Santa Barbara (UCSB), and finally University of Utah. The four nodes were selected due to their ability to provide specialized network services and support. Professor Leonard Kleinrock of UCLA was renowned in queuing theory; respectively, he became one of the first computer scientists to develop and advance ARPANET. On October 29, 1969, Professor Kleinrock and a programmer at UCLA setup data transmission to Bill Duvall at SRI. The goal was to transmit the message 'login' from the UCLA SDS Sigma 7 Host computer to SRI SDS 940 Host computer across ARPANET. They succeeded in transmitting the 'l' and then the 'o,' before the system crashed. As a result, the first host-to-host message transmitted over ARPANET was "lo". About an hour later, after recovering from the system crash, the entire message "login" was transmitted [4].

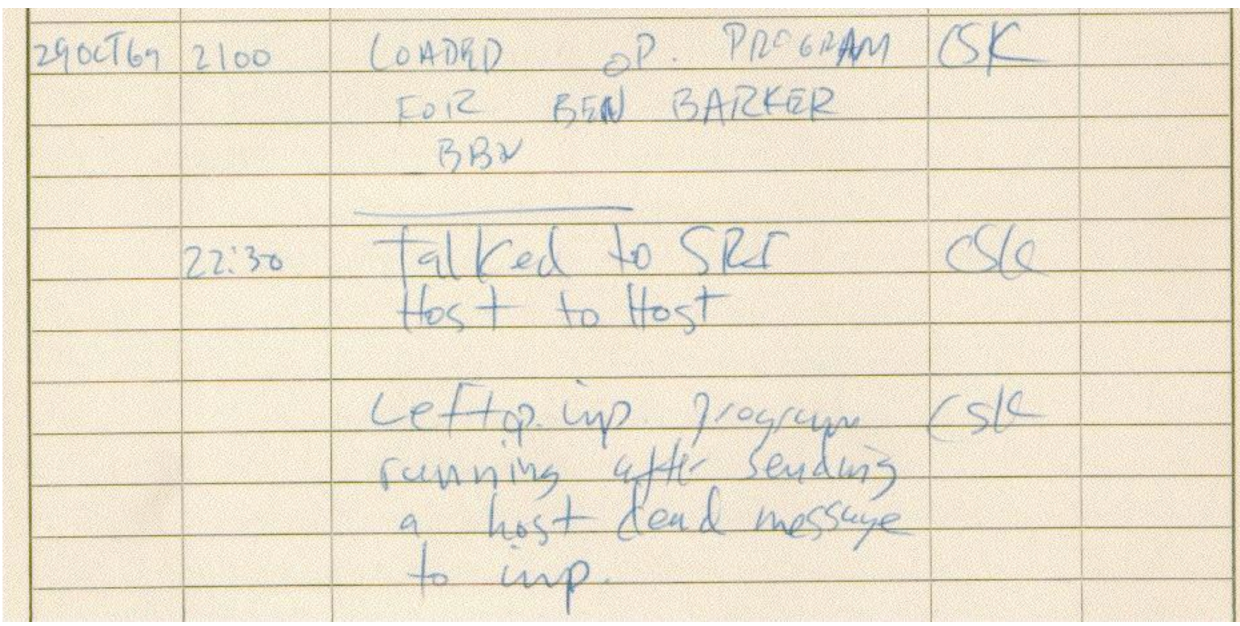

Figure 2: The original IMP log showing the first message transmission on the Internet [4]

Since the successful implementation of ARPANET, related communication technologies emerged, eventually evolving into the Internet. From ARPANET to dial-up to broadband service, the demand for Internet connection exponentially grew. According to the United States Census Bureau, "Computer and Internet Use in the United States: Population Characteristics", in 1984, zero United States households had Internet access and 8.2 percent of households owned a computer. Technology swiftly developed, creating more opportunities for computer integration into daily life. Computer application, capability, and affordability birthed the dot-com boom. The dot-com boom statistically showed in the 1997 United States Census that 36.6 percent of households owned a computer and 18 percent of households had Internet access. The number of households owning computers with Internet access continued to dramatically increase. In 2011, 75.6 percent of households owned at least one computer and 71.7 percent had access to the Internet [5]. Graphical data from the May 2013 United States Census showed rapid growth during the dot-com boom between 1997 and 2000. Computer ownership and connectivity peaked between 2009 and 2011. Although computer ownership peaked, the demand for connectivity expanded given novel technology markets utilizing Internet connectivity such as gaming consoles, tablets, and smart phones.

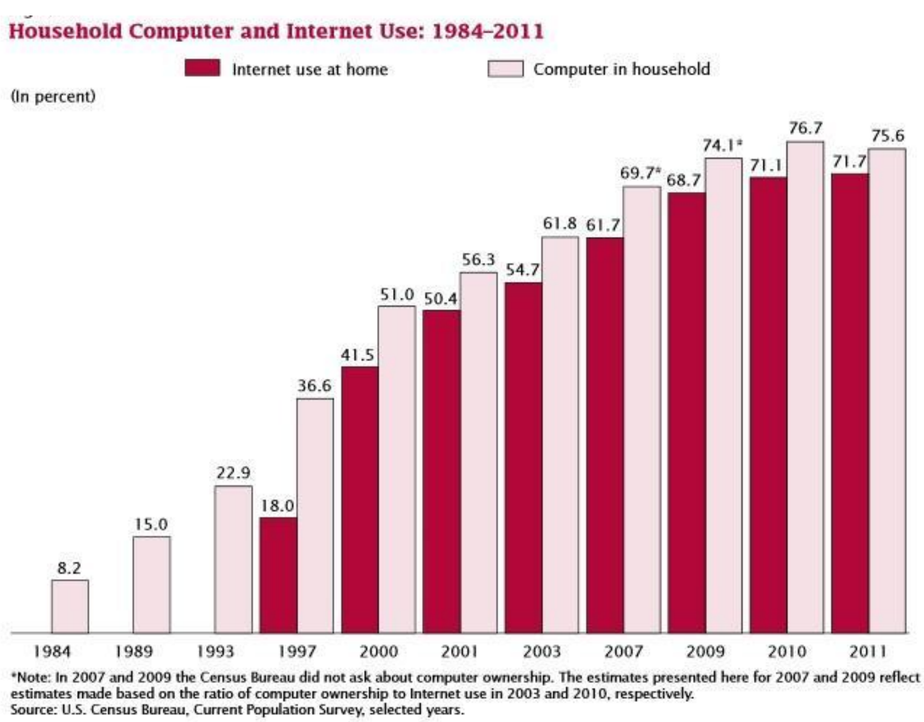

Figure 3: Household computer and Internet use in the United States [5]

2.2 Optical Fiber Networks

Innovative technology markets resulted in greater need and demand for Internet connectivity. These needs and demands opened doors to planning, constructing, and expanding physical network infrastructure. The size and makeup of the network and the distance between nodes depends upon consumer needs, as well as, capital investment in a region by local service providers. The arrangement of network elements, such as fiber or coaxial cables, equipment, and nodes is termed *physical network topology*. There are several different types of network topologies, with the four most common being: linear, ring, hub, and mesh.

The simplest topology is linear, also known as point-to-point. In a linear topology, there is a single direct link between two adjacent nodes. This topology is flexible and easily connects to additional nodes to extend the network. Construction of a linear topology is straightforward compared to other topologies; however, if there is a break anywhere in the cable or fiber line, then the entire network shuts down. Ring topology is designed such that each device is linked to two devices or nodes. In this network, information is transmitted unidirectional and is not dependent on a single control site. Bandwidth of the fiber ring is shared between all locations. Similar to linear topology, if there is a break in the fiber line, there is a total network outage.

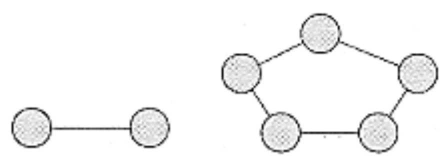

Figure 4: Linear and ring topology [6]

The hub, or star, topology is designed with each node or location connecting to a central network location. Data sent from one location passes through the hub before arriving at its destination, but each location does not communicate with other sites within the network. The advantage of the hub topology is that if one location experiences an outage, the remaining locations are unaffected. Additionally, if one location requires troubleshooting, maintenance, or equipment updates, the entire network is still in service. However, if equipment at the hub fails or experiences an outage, the entire network loses connectivity.

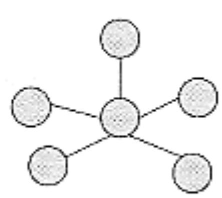

Figure 5: Hub topology [6]

Mesh topology is the most complex and expensive network to construct and deliver. In this setup, each node or location is interconnected with one another. Each node has to not only send and receive its own data, but it must also serve as a relay for other nodes. This network is expensive to deliver and difficult to troubleshoot due to redundant connections at each location. One advantage of this setup is that if one location experiences an outage, the other locations are not affected; the traffic at the failed node is redirected by the other nodes. The mesh topology is more common in wireless networks since such networks do not need physical infrastructure other than an access point.

Due to network redundancy, mesh topology is expensive; consequently, a partial mesh topology is preferred. Partial mesh topology is less expensive to implement and maintain since it benefits from lower redundancy in connectivity than a full mesh topology. In this instance, certain nodes are highly connected, while other nodes have a low degree of connectivity.

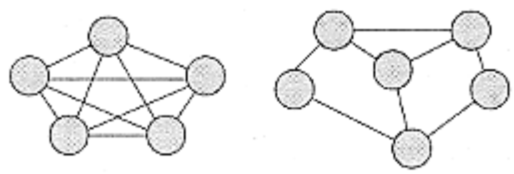

Figure 6: Full mesh and partial mesh topology [6]

Given the multitude of physical network topologies, constructing a network can be challenging. Networks signed and delivered to customers within a one-day turnover are those utilizing pre-existing cable owned or leased by a network provider. In this instance, field engineers merely plug in jumpers at the nodes and termination sites. Complicated network construction occurs when a network provider does not have a fiber footprint in a specific region and or if their backbone cables are completely exhausted. If a network provider chooses to not extend their fiber footprint or the customer requires immediate turnover, network providers may elect to lease 3rd party fiber.

A few issues typically arise when leasing 3rd party fiber. One issue is the type of fiber available in a specific region. In several locations where optical fiber is available, leasing from another network provider is straightforward. If a customer wants service in an area where network providers have not installed optical fiber, the customer can lease pre-existing copper cable; therefore, their network would comprise of hybrid fiber and copper cables. Copper cable has very limited bandwidth capacity because it was initially designed to transmit analog phone signals. In the early 1980s, copper cable could support 10 Mbps Ethernet. Transmission rates have improved; as of today, copper cable can support up to 1000 Mbps of Ethernet [7]. Fiber optic capacity surpasses copper cable capacity. Multi-mode fiber (MMF) generally transmits at up to 1 Gbps, but the range of transmission only over a few kilometers distance. MMF operates at 850 nm and 1310 nm. Single-mode fiber (SMF) transmits at high bit rates ranging from 1 Gbps to 100 Gbps with fiber distances spanning from 40 km to 30,000 km [8]. Amplifier and repeater hardware is spaced approximately every 40-80 km. SMF operates at 1310 and 1550 nm [9]. Another key issue is the equipment at the handoff or termination sites. Different cables require specific connectors to connect and terminate in the hardware. Copper cable requires twisted-pair or registered jack (RJ)-style connectors. Fiber cable typically uses standard connector (SC) optical connectors. Other common connectors are: Lucent connectors (LC), Fiber Jack, fiber connectors (FC), and straight terminus (ST) [10]. Data transmission that changes from fiber to copper requires a fiber media converter.

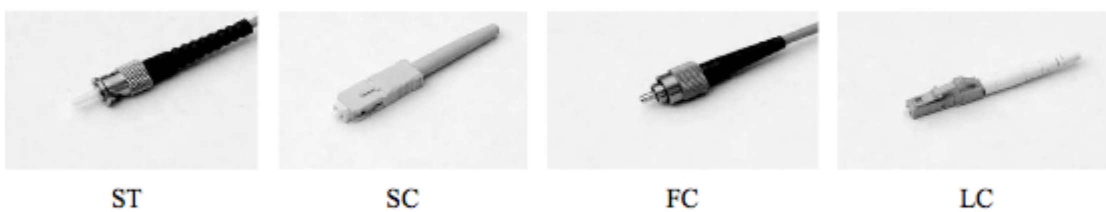

Figure 7: Different common types of connectors [10]

A fiber media converter is a device that functions as a transceiver by converting electronic signal from copper cabling into light signals in fiber optic cabling. There are other media converters that cater specifically to fiber-to-fiber conversion, such as converting from MMF to SMF or between different wavelengths in wave division multiplexing (WDM). Fiber media converters are viable options when network providers do not have a fiber network in a specific region or there is simply not enough time to construct and extend a network. Using a fiber media converter is also an inexpensive choice for clients who cannot afford fiber optic cables or perhaps are not ready to construct, lease, or upgrade to optical fiber lines; this allows clients to gradually transition from copper to fiber. One disadvantage of having a fiber media converter is introducing additional signal loss to the optical power loss budget. The connectors between the fiber line and the copper line contribute to a connector loss; connector loss is dependent upon the fiber and connector type. Connector losses are typically 0.15 to 0.30 dB

[10]. Another disadvantage is the limited range over which these converters optimally function. A common media converter is the Cisco 1000BASE Gigabit Interface Converter (GBIC) series, which plugs directly into several Cisco Ethernet ports. The Cisco GBIC models function at 1 km, 10 km, and even 100 km; however these can be expensive to lease and purchase and are also sensitive to temperature changes. An affordable model is the Cisco 1000BASE-T GBIC model, which uses a standard RJ-45 connector that operates up to 100 m [11]. If a network provider and client choose to install new fiber backbone in a new region, rather than utilizing copper cable, the network provider needs to consider how environmental concerns delay or halt construction.

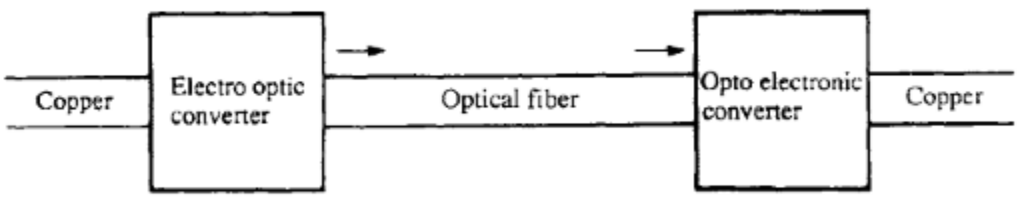

Figure 8: Construction of a hybrid fiber-copper network [7]

Environmental challenges occurred in California when the Plumas Sierra Rural Electric Cooperative (PSREC) applied to the Broadband Technology Opportunities Program (BTOP) grant to propose building, operating, and maintaining a 183 mile fiber optic network in Northeastern California and Northwestern Nevada. The proposed network would provide connection to one Nevada county and three California counties: Washoe, Plumas, Sierra, and Lassen County. Given the scale of this project, construction engineers had to follow regulations in accordance with the California Environmental Quality Act. A few of the Environmental Protection Measures included preventing greenhouse gases by encouraging carpooling to construction sites, limit idling construction equipment, and utilizing biofuels. In terms of biological protection, the PSREC were mindful of swallows nesting on bridges where conduit would be attached. Bank swallow nesting season begins in February and concludes in October. If the birds begin nesting before construction, construction workers can remove the swallow nests with hand tools or high pressure water. Following manual nest removal, netting is hung on the bridges to prevent further swallow nesting. In the instance that a bird-of-prey or special-status bird, such as the sandhill crane nests, is present on the construction site, a qualified biologist conducts nest clearance surveys to determine whether construction activity should be restricted around active nests, or if construction should cease until the young have fledged the nest or nesting attempt fails. Nesting surveys and nesting attempts follow their own timeline

[12]. The state of California has its own terms of construction restrictions and accessibility. Not only are there state specific environmental codes, there are permits regarding construction times and regulations that vary from city to city.

Expanding and building a fiber network is painstakingly slow given city specific regulations. One consistent construction regulation is holiday moratorium. Due to increased pedestrian and vehicle traffic, from November through early January, cities enforce construction moratorium, in which field engineers and construction workers cannot bore or trench into the city streets. When holiday moratorium is not in effect, some cities have street paving moratorium that does not allow fiber cable installation if the streets were recently repaved. For example, in San Francisco, California, the city does not allow fiber installation in downtown streets that were paved within the past 5 years due to the high volume of pedestrians and vehicles. In less populated parts of San Francisco where street paving moratorium is not applicable, the city allows fiber cable installation, but the service provider must have permits to construct. To access a permit, the entire route must be engineered and designed to show which streets are affected by construction. The city might approve of the route feasibility depending on the locations of utility ducts. Additionally, the time frame in which a permit is approved can take months, given the intricacies of public utilities and interdepartmental processes. If San Francisco approves the construction permit, the service provider can commence construction on days and hours specified on the permit. Characteristic to this city, construction hours are between midnight and 5 AM. In addition to the limited construction hours, the service provider must also repave the entire street following the completion of fiber installation [13]. City regulations and permits can hinder fiber network construction and installation, however more obstacles arise when building fiber in public transportation pathways.

Public transportation, such as buses and trains, provide connectivity so riders can access the Internet during commutes and leisure travel. In order to provide connectivity in underground train systems, fiber runs along the tracks and tunnels. Given that trains pass through several cities, field engineers must acquire permits from each city affected by fiber construction and maintenance; again permit processes and requirements vary from city to city. Moreover, the railway track owners regulate construction and accessibility permits, so additional permits must be acquired. In Northern California, the main train system in the San Francisco Bay Area is Bay Area Rapid Transit (BART), which spans 104 miles through 9 districts and 3 major counties. In 2008, BART serviced nearly 400,000 riders daily; since then, the number of daily commuters has increased [14]. Because of its large geographic footprint, BART has its own right-of-way (ROW). As a result, access permits are required to enter any BART owned tunnels and tracks and a BART inspector must be present during all construction. Obtaining accessibility permits are both expensive and cumbersome given the slow approval process by BART board of directors, who also charge additional administrative fees for major projects. Additionally, BART owns and traverses several underground tunnels. When installing or maintaining fiber in BART tunnels, field engineers are limited to the hours of midnight to 4 AM. If fiber construction occurs along BART tunnels or tracks crossing any Union Pacific Railroad (UPRR) ROW, another permit must be obtained from UPRR [15]. When installing fiber passing through UPRR owned tracks, not only are permits required by both the city and UPRR, they both regulate of how fiber is installed.

Fiber is installed underneath railway tracks. Construction and maintenance underneath tracks is regulated both by the city and the governing railway; as a result, both parties require permits. In the Bay Area, the main tracks are typically owned and governed by several companies, such as: UPRR, BART, CalTrain, and, Sonoma-Marin Area Rail Transit (SMART). Each of these governing railway companies has different boring and trenching regulations to build underneath tracks. Internet service providers, such as Zayo Group, have their own standards for boring, too. Zayo instructs field engineers that the bore depth must be at least 60 inches below the base of the railroad or 60 inches below paralleling drainage ditches [16]. Sagebrush Cable Engineer states that installing fiber under tracks is not difficult as long as the bore depth is 12 inches or more. When boring at depths less than 12 inches, the entire fiber backbone is carefully structured in a steel pipe, then jacked and bored to the railway crossing. Boring less than 12 inch depths is less than ideal and more expensive, however, it is necessary when there are distance and utility restrictions. Given standards implemented by service providers, cities also have their own standards, superseding telecommunication company standards. In San Francisco, the city does not allow boring for fiber installation; San Francisco allows only trenching which is a more expensive and time consuming method [15]. Given the difficulties of installing fiber, such as trenching and boring standards, and permit accessibility, building a fiber network is a laborious process that takes months and even years to fully implement. Because of city inconsistencies, the federal government generated a plan to unify fiber installation.

In March 2010, the Federal Communications Commission (FCC) proposed, *Connecting America: The National Broadband Plan*. In order to improve Internet access in the United States, this plan was created to act as a template for the booming broadband industry to address the following: design policies to ensure competition between network providers, allocate government-used and government-allocated infrastructure, and update broadband policies and standards necessary for government branches to function. One idea *The National Broadband Plan* recommends is for Congress to enact a "dig once" legislation such that all future federally funded projects along sewers, rails, pipelines, bridges, and all government owned structures, can coordinate construction. Because installing conduit is 75 percent of the total cost of fiber deployment, the FCC states that a substantial amount of money can be saved if conduit installation is coordinated with other infrastructure projects that require street digging [17]. In reality, the feasibility of coordinating multiple projects from different utility branches, such as water, gas, and roadways, can be painstaking and unpredictable. The process of obtaining permits from all the correct departments and ensuring the timely approval process for all utility branches wishing to simultaneously dig seems unrealistic. According to the United States Department of Transportation, Federal Highway Administration (USDOT-FHWA), very few states have implemented the "dig once" policies while other cities have no issue with multiple excavations as long as they can benefit from street reparations and maintenance. In 2013, USDOT-FHA surveyed five states to discuss the highway ROW. None of these five states mandated "dig once" or "joint use" policies; "joint use" means broadband utilities install fiber in the same trenches and conduit [18].

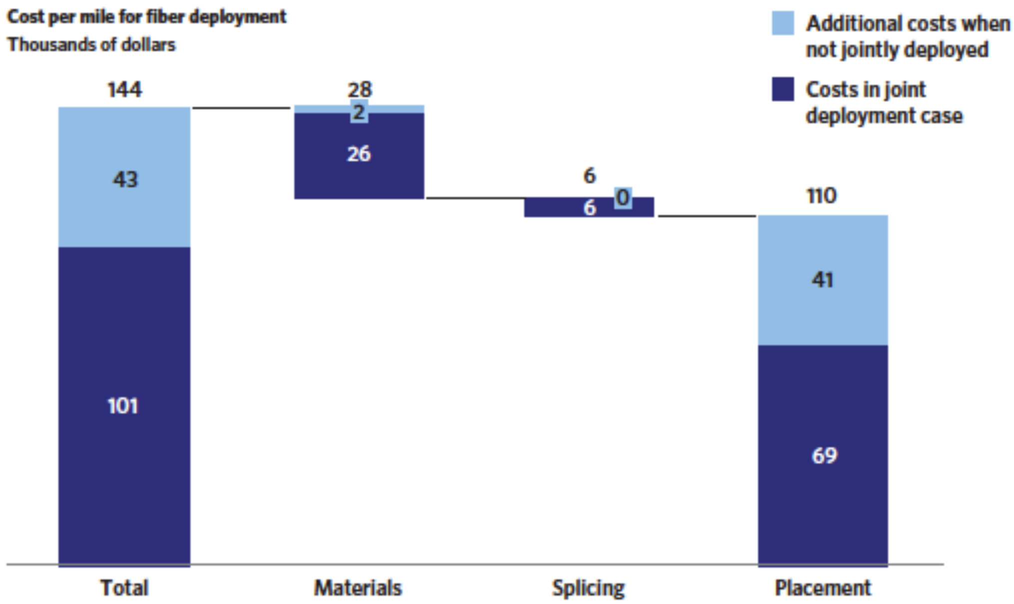

Figure 9: Joint deployment can reduce the cost of fiber deployment [17]

Additionally, the FCC estimates for implementing parts of *The National Broadband Plan*, put the cost anywhere from $12 billion to $24 billion [17]. PSREC received a $13 million grant through this plan to install 183 fiber miles [12]. This minor grant represents one of hundreds funded by *The National Broadband Plan*. Implementation costs do not include future maintenance and infrastructure upgrades. The FCC did not propose a long term solution in its plans; instead, they proclaim the United States should establish long term sustainable and adequate funding mechanisms to pay for future operations, maintenance, and upgrades [17]. Given impediments pertaining to conduit installation and maintenance, another issue arises from the service provider and the user's viewpoint regarding how data is transmitted and experienced.

2.3 Quality of Service

If fiber and hardware construction and installation are perfectly executed, then Internet service providers and consumers would not raise concerns regarding how data and information is transmitted across the network. On the contrary, perfectly delivered infrastructure does not guarantee what packets experience as they traverse networks. QoS describes the overall performance or quality specification of a communications channel or system. It describes how packets travel from the sender to receiver locations; how packets travel varies upon the application. The International Telecommunication Union (ITU) and European Telecommunications Standard Institute (ETSI) distinguish four particular definitions composing QoS standards: QoS requirements of the customer, QoS offered by the provider, QoS achieved by the provider, and QoS perceived by the customer. Their strategy, benchmarking, service deployment costs, and other factors influence QoS offered by service providers. However, the most important feedback from the service provider's perspective is the QoS perceived by the customer [19]. Service providers and customers must compromise on QoS standards best suited for specific applications, such as interactive video transmission.

To achieve end-to-end QoS on the Internet, there are two major frameworks that are considered the principal architectures for providing Internet QoS: Integrated services (IntServ) and Differentiated Services (DiffServ). IntServ is a per-flow based QoS framework with dynamic resource reservation. Its fundamental philosophy is that routers need to reserve resources in order to provide quantifiable QoS for specific traffic flows. Algorithms and protocols are programmed into routers to reserve network resources. The sender sends a message to the receiver specifying characteristics of the traffic. As the message propagates toward the receiver(s), each router along the network records path characteristics, such as available bandwidth. When the receiver receives the message, in return, the receiver sends a message on the exact same path to request intermediate routers to either accept or reject the message. If the request is accepted, link bandwidth and buffer space are allocated for the flow and the flow-specific state information is stored in the routers. The challenge of IntServ per-flow based framework arises in the Internet backbone, where hundreds of thousands of flows may be present. This may be difficult to manage because a router may need to maintain a separate queue for each flow. IntServ is more suitable for applications requiring high-bandwidth flows.

In contrast to IntServ, DiffServ is a per-aggregate-class based service discrimination that uses packet tagging. Packet tagging uses bits in the packet header to mark a packet for preferential treatment. Before a packet enters a DiffServ domain, it is marked by the end-host of the first-hop router according to the service quality the packet requires and is entitled to receive. Within the DiffServ domain, each router only needs to look at the marked header to decide the proper treatment for the packet. DiffServ QoS emphasizes "best effort" packet forwarding and can guarantee a peak rate service, which is optimized for regular traffic patterns and offers small or no queuing delay [21]. IntServ and DiffServ qualitatively describe two QoS architectural frameworks. QoS standards can be expressed quantitatively by a few parameters, such as bandwidth, packet loss, delay, and jitter.

Bandwidth determines an application's maximum throughput and end-to-end delay. It shows the bit rate available to transfer data for an application or target throughput that may be achieved [19]. For video transmission, fiber networks require a minimum bandwidth of 64 Kbps. Video is encoded differently depending upon the quality of the JPEG frame. High definition television, which is encoded by MPEG-1 or MPEG-2 standards, requires a minimum bandwidth of 20 Mbps [20].

Encoding	*Bandwidth*	*Resolution*	*Standard*
H.261	64 Kbps–2 Mbps	177×144	QCIF (conference)
		352×288	CIF (VHS quality)
M-JPEG	3–8 Mbps	352×288	CIF (VHS quality)
	15-25 Mbps	720×486	CCIR601 (PAL)
	60–100 Mbps	1920×1080	HDTV
MPEG-1	1.2–3 Mbps	352×288	CIF (VHS quality)
	5–10 Mbps	720×486	CCIR601 (PAL)
	20–40 Mbps	1920×1080	HDTV
MPEG-2 (H.262)	1–2 Mbps	352×288	CIF (VHS quality)
	4–5 Mbps	720×486	CCIR601 (PAL)
	8–10 Mbps	960×576	EDT
	20–30 Mbps	1920×1080	HDTV

Figure 10: Bandwidth requirements for video of varying quality [20]

Packet loss is defined as the ratio of the number of undelivered packets to sent ones. Packets are lost for two reasons: damage in transit or dropping when the network is congested. Loss due to damage is rare; this usually accounts for less than 1% of all packet loss. Therefore, packet loss is often an indication of network congestion. Most applications can recover from packet loss via redundancy and retransmission, but this would cause a drastic spike in jitter. Losses above 5% generally lead to poor effective throughput. If a packet containing a video frame is not delivered before its scheduled play out time, and the frame cannot be displayed accordingly, then the overall quality of video degrades. Media applications for streaming video require a fixed bandwidth to prevent packet loss, although some applications can adapt to changing network conditions. Video applications have software encoders that can adjust frame rate, image size, and quality. Traditionally, packets are dropped when the buffer and queue is full; buffer is space in the network designed to store short term data bursts rather than be continuously occupied. Typically, arriving packets or packets that have been in queue the longest are dropped. To avoid packet loss, a queue management algorithm is activated such that the router controls and schedules how higher priority packets exit and when and how many packets are dropped [21].

Delay is time elapsed for packets to travel from the start to the end location. Delay can be measured end-to-end or with regard to particular network elements. Cisco QoS requires one-way delay for interactive video should not exceed 150 ms [29]. *Delay jitter* is defined as the variations in IP packet transfer delay [19]. Real-time applications, such as video conferencing, are sensitive to transmission delay and delay jitter, so they usually require guaranteed high-capacity bandwidth. Under ideal conditions, all packets should undergo the same delay. However, due to queuing management, processing time variations in nodes, and even route changes, packets experience jitter [22]. The effects of delay jitter can be ameliorated with delay buffering. Delay buffering can compensate for delay jitter at the expense of delay. Transmitted frames are buffered in memory by the receiver, allowing each frame to be played out with constant delay, which achieves a steadier stream. Unfortunately, added latency from buffering disturbs interactive video applications [23]. For example, applications, such as video conferencing, can withstand delay jitter up to 30 ms, however delay buffering is not an option due to real-time nature of these applications [24].

Another type of jitter is random jitter. Random jitter is a random process described commonly by a Gaussian distribution since most noise sources have Gaussian profiles. The causes of random jitter are generally due to thermal and flicker noise. Electron scattering causes thermal noise when electrons move through a conducting medium and collide with silicon atoms or impurities in the glass lattice structure. Higher temperatures result in greater atomic vibrations and increased chances of collisions. Flicker noise, or inverse-frequency (1/f) noise, is caused by random capture and emission of carriers from oxide interface traps affecting carrier density in a transistor [25]. To improve the quantitative parameters of interactive video transmission across a network, we employ network virtualization.

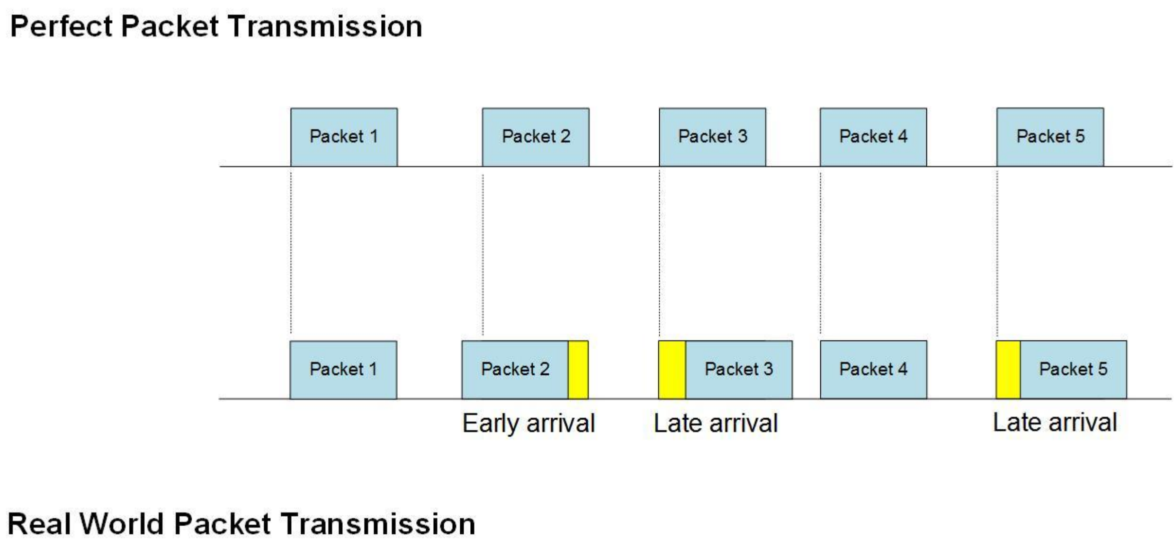

Figure 11: Packet arrival at the receiver with and without jitter

2.4 Network Virtualization

Network virtualization works by combining network hardware and software resources with network functionality into a software-based virtual environment. The virtualized environment is a subset of the underlying physical network resources; accordingly, it is a complete network abstracted in software. It separates services from infrastructure such that network resources are allocated across multiple providers and customers. The service separation changes the roles of traditional Internet providers into infrastructure providers, who manage physical infrastructure, and virtual service providers, who create and aggregate virtual networks by aggregating resources from infrastructure providers. With the separated roles, it provides an abstraction between the user and physical resources, so users have the illusion of direct interaction with physical resources. Network virtualization enables independent programmability of virtual networks, so a virtual network is no longer based on IP or a specific network architecture [26]. Without virtualization, alterations to Internet architecture are restricted to incremental updates and deployment of new network technologies is difficult to implement.

Virtualization allows infrastructure providers to deploy and manage the underlying physical network resources within the network virtualization environment. They construct, operate, and maintain the physical infrastructure, while access to the physical infrastructure is made available to different virtual service providers through a programmable interface; end users do not have access to this interface [1].

Virtual service providers lease resources from data carriers and network facility providers to create virtual networks and deploy customized protocols by programming the allocated network resources to offer end-to-end services to users. Virtual service providers can freely implement arbitrary network topology, routing and forwarding functionalities, and customized control protocols independent of the underlying physical network and other coexisting virtual networks. They can also create virtual sub-networks to partition their resources; these sub-networks can then be leased to other virtual service providers. With the separation of infrastructure and service providers, end users in a virtual network can choose from a wide range of services given the existence of multiple virtual network environments and child networks [2].

A virtual network environment is a collection of virtual nodes connected together by virtual links to form a virtual topology. Link virtualization permits the transport of multiple separate virtual links over a shared physical link. They can span over one or more physical links. Virtual links can be identified explicitly by a tag and also identified implicitly by a time slot or wavelength [1]. One or multiple virtual links can terminate in the same virtual node.

Physical nodes terminate one or multiple physical links, which may in turn carry multiple virtual links. Correspondingly, a virtual node terminates one or more virtual links. Furthermore, virtual nodes are based on isolation and partitioning of hardware resources. Physical resources of a node are partitioned into slices and each slice is allocated to a virtual node according to a set of user requirements [26]. Virtualizing nodes and links enables the creation of virtual networks, functionally equivalent to a physical network.

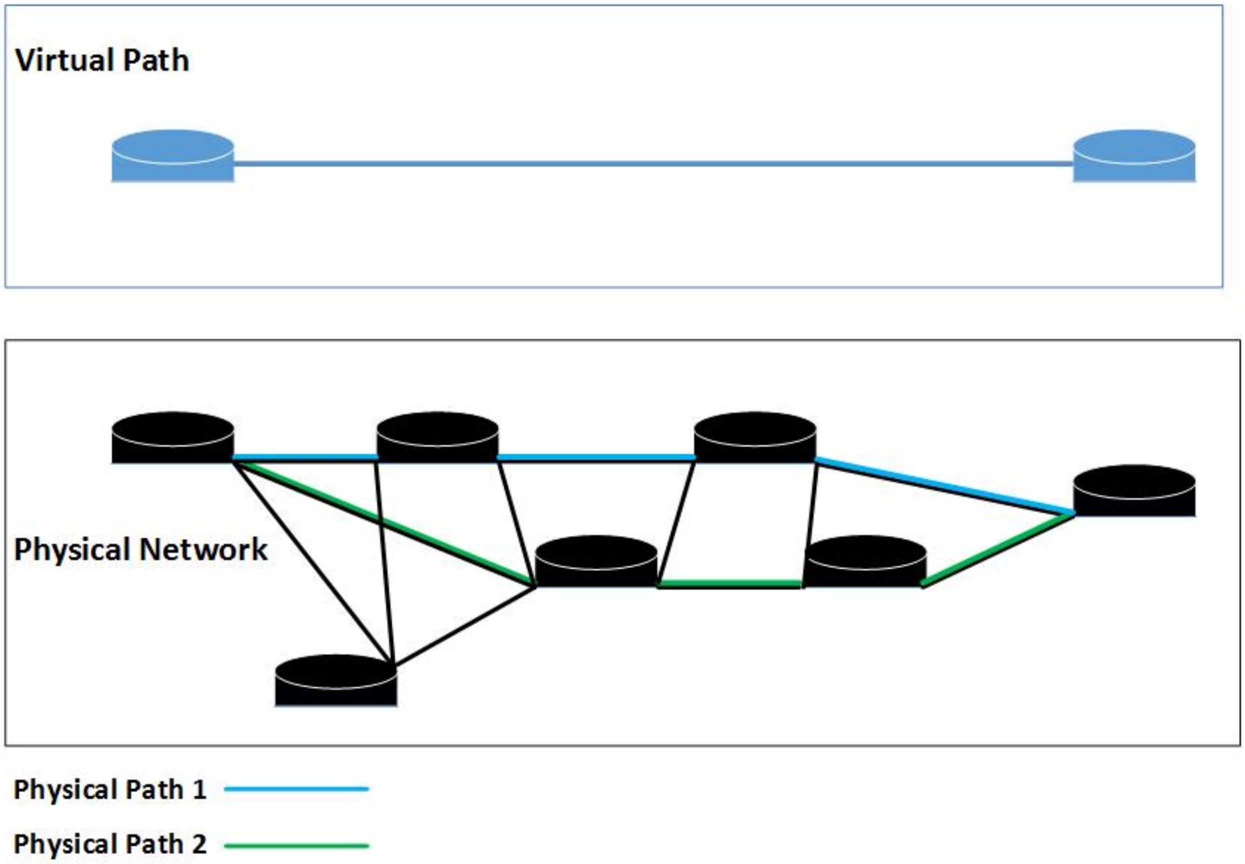

Figure 12: Network virtualization model

Chapter 3: Methodology

3.1 Parameters

Interactive video transmission is highly sensitive to jitter. Jitter is random in nature due to unpredictable queuing management, processing time variations, and even route changes. Queuing management and processing time variations occur at intermediate nodes and routers. The randomness of jitter negatively affects QoS of interactive video transmission. In the absence of jitter, video frames can be played as they are received, resulting in smooth playback. If a frame arrives late due to jitter, the user sees a frozen image of the most recently delivered frame, until the tardy frame arrives. The tardy frame is played to preserve the timing of the subsequent frame.

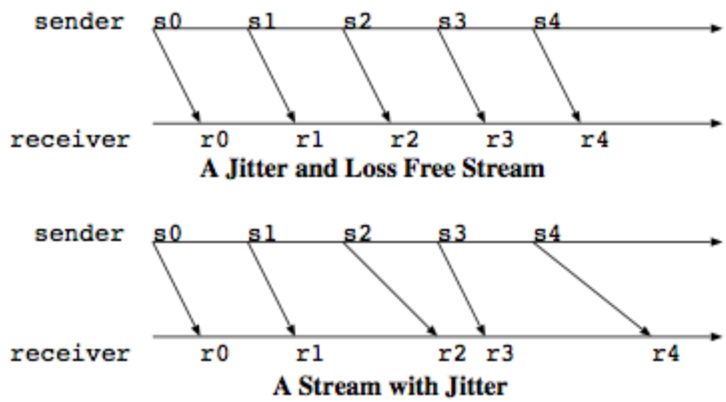

Figure 13: The figure models video packets transmitted from sender to receiver with and without jitter. In the presence of jitter, packet arrival at the receiver varies [27].

For quality interactive video transmission, Cisco standards state jitter should not exceed 30 ms. Cisco standards are stricter than jitter standards from the ITU, given that ITU states jitter should not exceed 50 ms. ITU also states that the jitter is calculated from the upper and lower bounds of delay according to,

$$Delay_{upper} = Delay_{mean} + Jitter_{upper}$$

The upper bound delay can be obtained by summing the mean delay and the maximum or upper bound jitter. As a result, the upper bound delay is 150 ms, which correlates to Cisco's one-way delay requirement. With this range of values for upper bound delay and jitter, ITU states that 99.9% of packets transmitted will meet acceptable transmission values [28].

The sizes of the packets within a frame vary based upon how much information is contained in a video frame. A high definition video frame may require 100 IP packets, although

40 to 60 packet-size is more common. We have chosen to simulate an interactive video transmission simulation that is not high definition, with an average packet number per frame chosen at 50 packets [29]. A normal user perceives no more than 25 frames per second [30], so a packet transmission of 1,000 packets is a bit less than one second of video, while a 75,000 packet transmission is one minute of video.

Given that jitter is random in nature, a Gaussian random number generator is used to represent the different packet delays. A Gaussian profile for the noise is a good representation for the random errors injected during the simulation because the Central Limit Theorem states that when the output of a random system consists of the sum of a number of independent and identically random variables, the resulting distribution tends to the Gaussian distribution as the number of variables increases [31].

$$Z_n = \frac{1}{n}\sum_{i=1}^{n}\frac{X_i - \mu}{\sigma}, \qquad n = 1, 2, 3, \ldots$$

where $\mu = \mu_1 + \mu_n$

$\sigma^2 = \sigma_1^2 + \ldots.\sigma_n^2$

$$\lim_{n\to\infty} P[Z_n \le z] = \int_{-\infty}^{z} \frac{1}{(2\pi)^{1/2}} e^{-y^2/2} 2\, dy$$

Figure 14: Formula for the Central Limit Theorem. Assume $X_1, X_2, \ldots, X_n$ is a sequence of independent, identically distributed random variables with mean μ and variance σ^2. Z_n converges, in distribution, to a standard Gaussian distribution with mean μ and variance σ^2. The Gaussian approximation works well for n>20 or so [31].

3.2 Simulation

To demonstrate that network virtualization improves QoS, a Gaussian distributed random number generator simulated packet transmission on two separate fiber paths to the same destination. Two different random generators represent two different fiber paths. Each of these virtual fiber paths simultaneously and separately transmit 1,000 packets with randomly chosen delays; as mentioned above, this represents less than one second of interactive video. This method is repeated, except with the simulator sending 75,000 packets on each path, representing one minute of interactive video. Cisco and ITU QoS standards state that delay should not exceed 150 ms. ITU also states that the acceptable mean delay is 100 ms [24]. To show improved jitter via network virtualization, a delay standard deviation, or jitter, is chosen at 40 ms, which exceeds acceptable jitter standards for interactive video. If a jitter value less than

30 ms is chosen, then the simulation would merely simulate packet transmission within acceptable jitter ranges. For higher quality video transmission, a combination of ITU and Cisco standards is chosen for the simulation. The Cisco standard for jitter is chosen over the ITU standard and the ITU mean delay is chosen over the Cisco delay. Therefore, the packets are transmitted on their respective paths with a mean delay of 100 ms and a standard deviation of 40 ms. At the destination, packets arriving with values of delay nearest to the mean delay were placed in the distribution.

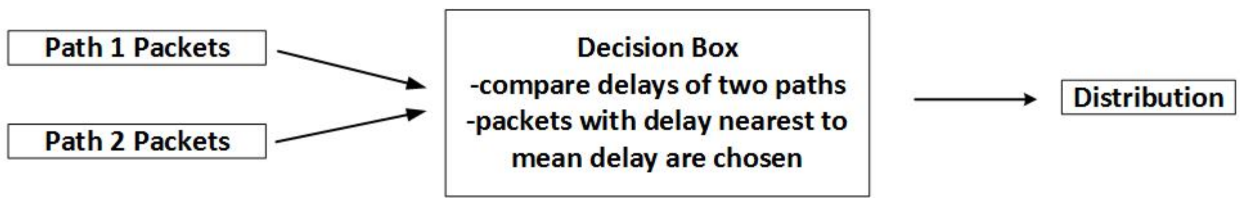

Figure 15: Packet transmission simulation

3.3 Results

Packets from both virtual links arrive at the destination with varying delays; moreover, the packet arriving with the least jitter is placed in the distribution, which represents queue for video. We find that when 1,000 packets are transmitted to the end user, the overall jitter is 23.27 ms, which is below the delay variation chosen in the simulation. When 75,000 packets are transmitted to the end user, the overall jitter is found to be 24.11 ms. The resulting jitter in both simulations is acceptable for quality interactive video display.

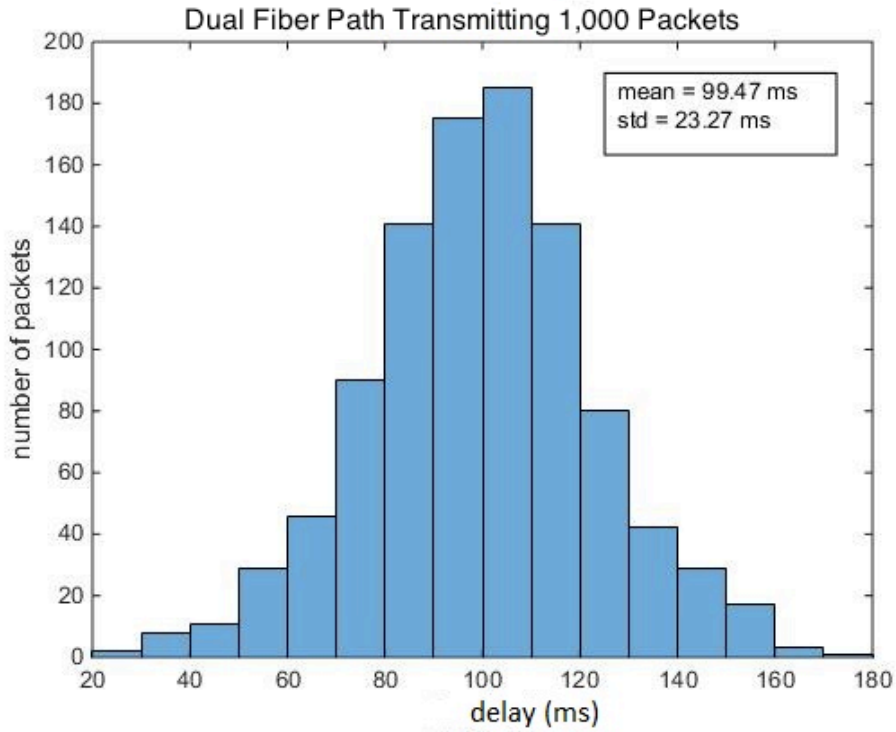

Figure 16: Histogram of dual fiber paths transmitting 1,000 packets across a network

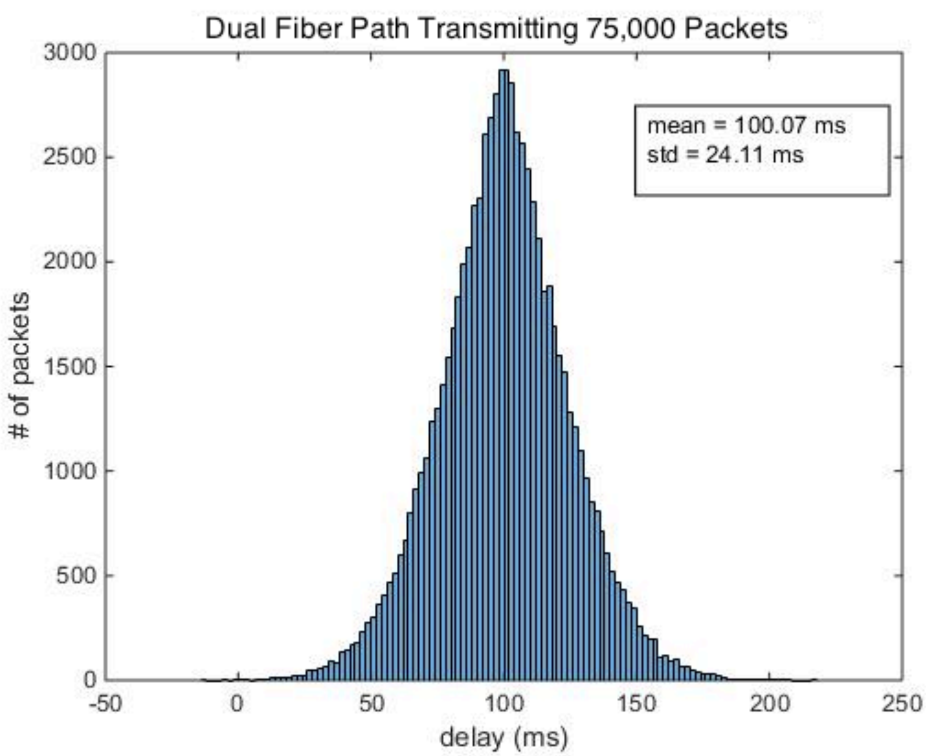

Figure 17: Histogram of dual fiber paths transmitting 75,000 packets across a network

Chapter 4: Conclusion

Fiber optic cables have transformed how data is being transmitted, affecting the consumer demand for network applications, such as social media, and Internet-enabled technologies, such as smart phones and tablets. Since the birth of ARPANET, the Internet has inspired new technologies, giving rise to numerous markets for networked hardware, which will culminate in the Internet of Things, a world in which every device is connected to the Internet. Consequently, fiber optic cable infrastructure has been installed globally. Fiber optic cable is more durable, reliable, and has more features than copper cable. With the growing demand for Internet connection and fiber optic cabling, service providers cannot keep pace with demands for fiber network expansion. Fiber optic networks are more complicated and tedious to design and construct. Extending fiber optic networks has proven problematic with rules and regulations specific to each state, city, and utility; hence Internet service providers cannot expand fiber optic networks at a pace commensurate with demand.

The demand for expanded fiber optic networks also correlates with a demand for improved QoS. QoS describes the overall performance of a network. QoS standards dictate and describe what data packets experience as they traverse a network. Different applications have different QoS requirements, such as acceptable jitter limits for interactive video. Network virtualization can improve the QoS of interactive video transmission. Network virtualization is the ability to combine hardware and software network resources with network functionality in a software-based virtual network. The virtualized network can be customized to any topology or customized protocol the customer chooses. With the flexibility in resource management afforded by network virtualization, QoS for interactive video is expected to improve. In this thesis, we used a Gaussian random-number generator to simulate packet transmission on dual virtual paths in order to investigate jitter. As expected, the addition of a second virtual path allowed the video jitter to decrease to acceptable Cisco standards.

To further improve QoS in this simulation, the same dual path simulation is repeated with packets on each path is transmitted at different delays and jitter. This would better represent different path lengths and number of intermediate nodes.

We also propose a third virtual path to be added to transmit the same interactive video used in the current simulation. In addition to the DiffServ QoS architecture, the service providers could transmit packets across a *virtual load balancer* through redundant links to avoid network congestion. If there is network congestion, the load balancer would redistribute and forward packets to paths with more capacity.

Another way to improve QoS of interactive video transmission using network virtualization is by transmitting packets on different servers. In a virtualized environment, the exact same virtual paths can exist in separate virtual environments, which are managed by different service providers. When the packets are transmitted to locations outside of their local area network, they traverse through different networks provided and managed by different service providers. Provided that network congestion and jitter factors are independent of each environment, a separate service provider on the same or similar virtual path can improve QoS of interactive video transmission by providing redundant virtual links, as proposed above, or virtual paths that contain fewer intermediate nodes between them and the end user. This improvement may be implemented using Software-Defined Networking, which can be programmed to automate the choices of the appropriate virtual networks outside of the local area network.

References

1. Chowdhury, NM Mosharaf Kabir, and Raouf Boutaba. “A survey of network virtualization.” *Computer Networks* 54.5 (2010): 862-876.
2. Chowdhury, NM Mosharaf Kabir, and Raouf Boutaba. "Network virtualization: state of the art and research challenges." *Communications Magazine, IEEE* 47.7 (2009): 20-26.
3. Hauben, Michael. "History of ARPANET." *Retrieved* 23 (2010): 13.
4. Kleinrock, Leonard. "An early history of the internet [History of Communications]." *Communications Magazine, IEEE* 48.8 (2010): 26-36.
5. File, Thom. “Computer and Internet use in the United States.” U.S. Department of Commerce Economics and Statistics Administration. U.S. Census Bureau. Current Population Survey Reports, Washington, D.C (2013), pp. P20-569
6. Mazda, Xerxes and F.F. Mazda. *Focal Dictionary of Telecommunications, Focal Press*. London: Routledge, 1999.
7. Elliott, Barry J. and M. Gilmore. *Fiber Optics Cabling.* Oxford: Butterworth-Heinemann, 2002. (pp. 7-9, and 19)
8. Kumar, Shiva and M. J. Deen. *Fiber Optic Communications: Fundamentals and Application.* Chichester, West Sussex, United Kingdom: Wiley, 2014. (pp. 68)
9. Christian, N. L. and L. K. Passauer. *Fiber Optic Component Design, Fabrication, Testing Operation, Reliability and Maintainability*. William Andrew Publishing/Noyes, 1989. (pp. 64-65)
10. Thyagarajan, K. and A. Ghatak. *Fiber Optic Essentials*. John Wiley & Sons, Inc., Hoboken, NJ, USA, 2007. (pp. 3)
11. “Cisco Gigabit Interface Converter.” Cisco Transceiver Modules. June 2010. Web. 24 March 2015.
12. Plumas Sierra Rural Electric Cooperative Mid-Mile Fiber Project. “National Environmental Policy Act Environmental Assessment ARRA Award: NT10 BIX 5570125.” U.S. Department of Commerce National Telecommunications and Information Administration. June 2011. (pp. 80, 241, 267)
13. Chris M. Simmons. Zayo Group OSP Construction Manager. Personal Interview. 26 February. 2014.
14. Bay Area Regional Transit. *2008 BART Station Profile Study*. BART Marketing and Research Department. 2008. (pp. 195)

15. Bob Durflinger. Sagebrush Cable Engineering-Operation/Project Manager. Personal Interview. 28 February. 14.
16. Zayo Business Development Team. “Outside Plant Manual.” Zayo Group. July 2013. Print. (pp. 82)
17. Federal Communications Commission. *Connecting America: The National Broadband Plan*. March 2010. (pp. 9, 114, 130, 136, 319)
18. United States Department of Transportation, Federal Highway Administration. *Executive Order: Accelerating Broadband Infrastructure Deployment, Best Approaches of Broadband Deployment in Highway Rights of Way Summary Paper*. Office of Policy and Government Affairs. May 2013. (pp. 7, 26)
19. Gozdecki, Janusz, Andrzej Jajszczyk, and Rafal Stankiewicz. "Quality of service terminology in IP networks." *Communications Magazine, IEEE* 41.3 (2003): 153-159.
20. Jha, Sanjay and M. Hassan. *Engineering Internet QoS.* Boston : Artech House, 2002. (pp. 7-8)
21. Zhao, Weibin, David Olshefski, and Henning G. Schulzrinne. "Internet quality of service: An overview." (2000).
22. Rizo-Dominguez, L., et al. "Jitter in IP networks: a cauchy approach." *Communications Letters, IEEE* 14.2 (2010): 190-192.
23. Claypool, Mark, and Jonathan Tanner. "The effects of jitter on the perceptual quality of video." *Proceedings of the seventh ACM international conference on Multimedia (Part 2)*. ACM, 1999.
24. Szigeit, Tim and C. Hattingh. End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs. Cisco Press, Indianapolis, November 2005.
25. Kuo, Andy. T. Farahmand, N. Ou, S. Tabatabaei, and A. Ivanov. Jitter Models and Measurement Methods for High-Speed Serial Interconnects. Test Conference, 2004. Proceedings. ITC, 2004. International. IEEE.
26. Carapinha, Jorge, and Javier Jiménez. "Network virtualization: a view from the bottom." *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*. ACM, 2009.
27. Claypool, Mark, and Jonathan Tanner. "The effects of jitter on the perceptual quality of video." *Proceedings of the seventh ACM international conference on Multimedia (Part 2)*. ACM, 1999.
28. Recommendation, I. T. U. T. "Network performance objectives for IP-based services." *ITU-T Recommendation Y* 1541 (2011).

29. Szigeit, Tim., K. McMenamy, R. Saville, and A. Glowacki. Cisco TelePresence Fundamentals. Cisco Press, Indianapolis, May 2009.
30. McCarthy, John D., M. Angela Sasse, and Dimitrios Miras. "Sharp or smooth?: comparing the effects of quantization vs. frame rate for streamed video."*Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2004.
31. Jeruchim, Michel C., P. Balaban, and K. S. Shanmugan. Simulation of Communication Systems: Modeling, Methodologies, and Techniques. Second Edition. Kluwer Academic Publishers. New York. 2000. pp. 320