Internet: The Next Generation

Justin Fiore[1] and Patrick Graf[2]

Abstract *— The Internet today is the primary medium of global communication. Modern communication was set in motion by the invention of the telegraph in the early 1800's. As the years progressed, communication technology grew to meet the world's increasing needs. The Next Generation Internet is culmination of all previous technological advances and breakthroughs and will revolutionize communication as we know it. The Next Generation Internet consists of three major areas: hardware, software, and the Next Generation Internet Protocol. Current and future software applications require greater speed, reliability, and security than the Internet currently offers. These needs can be met by the implementation of higher speed networking media and Internet Protocol version 6 (IPv6). IPv6 offers layer 3 security and reliability that the current Internet (IPv4) does not. This extra security and reliability requires greater bandwidth, one reason optical networks are gradually replacing copper wire networks. Besides improving security and reliability, IPv6 will solve the IP address shortage facing IPv4. The address space that IPv6 allots enables every person on Earth to have several thousand IP's. As with any other development in society, the Internet cannot remain stagnant. The next generation Internet is upon us and the world must be ready to accept this revolutionary technology.*

Index Terms — Fiber Optics, IPv4, IPv6, Internet, OSI Layer 3.

INTRODUCTION

As we enter a new technological era, communication technologies have progressed rapidly. As a world community, we are now approaching the next great step in information technology known as the Next Generation Internet. This new form of communication has revolutionized our current Internet structure through the development of new Internet Protocol (IPv6) and the continually increasing capabilities of both optical and wireless networks, as well as the other hardware agents. While looking at the future of Internet technologies, one must first examine its beginnings.

History of the Internet

The Internet as we know it today traces its roots back to the early 1960's at the height of the Cold War. The first pure data network was developed under government supervision by the Advanced Research Projects Agency (ARPA). This agency was charged with the task of creating a data network that would connect military facilities and population centers in the event of a possible nuclear attack from the U.S.S.R. Due to the nature of this network, the design would differ greatly from the telephone infrastructure of the period. The telephone network was contingent upon call centers, which directed all communications along selected predetermined paths. Thus, strategically placed attacks could effectively bring down the whole telephone system. The new data network must remove all central dependences. If one node, a device on the network, is destroyed, each data packet within the data transfer must have the ability to find a new path to the destination. If some of the data was lost in transmission, the call would not be terminated like under the old system. Rather, partial communication could still take place and the transmission could still serve its purpose. With this goal in mind, construction of the Internet began.

The development of this data network was very important to the government. In order to expedite the design process, ARPA declassified the operation and requested help from universities around the nation. By the late 1960's a decentralized, nationwide data network, labeled ARPANET, was born. Every network structure, including the Internet, is composed of both a physical structure, which is addressed briefly above, and the logical (software) structure, network protocol. Originally, ARPANET used Network Control Program (NCP) protocol to transmit the data. However, in 1973, Transmission Control Protocol/Internet Protocol (TCP/IP) was developed. By the early 1990's, all systems connected to ARPANET had converted from NCP to TCP/IP, ensuring greater stability than the previous protocol had offered. With this new protocol in place, ARPANET became a more effective part of defense operations and was extremely important to the government. From these humble beginnings the Internet grew to encompass the data transport features and connectivity with which the average person is familiar today. [1]

Modern Uses of the Internet

Today, the Internet is used for much more than military communications, the purpose of its original design. It has destroyed the geographical barriers of worldwide communication and commerce. However, the current physical and logical structure of the Internet cannot handle the volume of use and stress placed upon it by current and future applications. As with any technological advancement, the Internet cannot remain stagnant, but rather, its physical and logical structures must continue to develop. Several

[1] Justin Fiore, University of Pittsburgh, Pittsburgh, PA 15213 jmf21@pitt.edu
[2] Patrick Graf, University of Pittsburgh, Pittsburgh, PA 15213 pag3@pitt.edu

global technological initiatives find their homes on the Internet and Next Generation Internet will greatly affect these enterprises. The most common example of Internet driven crusades is open-source programming. Programmers from different parts of the globe create and develop new applications together via the Internet. This atmosphere of cooperation improves the computing environment drastically by uniting the brightest programmers, regardless of location, in similar goals. The Internet also provides a medium in which inexperienced programmers may post their applications and programming code so that others may build upon and critique these works. The Internet is used for a variety of different reasons by a large spectrum of people. The Next Generation Internet technologies will further unite mankind and help the world achieve new heights of excellence.

CURRENT INTERNET STRUCTURE

The next generation technologies are currently in development but, as they are released to the public, they will greatly change the way we look at communication. However, until that time, the world will continue using the current Internet structure. In order to understand the future Internet, one must have some knowledge of Internet structure. The structure of the Internet can be explained best through use of the Open System Interconnection (OSI) Reference Model (Fig. 1). This diagram divides networking into seven distinct layers, each communicating with the layer above and below it. The Physical Layer (Layer 1) contains the signal transmission medium, the actual cables that the data travels over. The Data Link Layer (Layer 2) has two subdivisions, the Media Access Control (MAC) and the Logical Link Control (LLC). The MAC controls the communication between the physical medium and the hardware that actually transmits data over the cables, e.g. a Network Interface Card. The LLC communicates directly with the Network Layer (Layer 3). This third layer contains the logical addresses of the two computing devices, the data's origin and its destination, as well as the route the packet should take to arrive at the destination device. Layer 3 is where the routing or directing of the data transmission occurs. In this layer, the data is encapsulated within the Internet Protocol header. The Transport Layer (Layer 4) establishes a degree of reliable communication between the end users. Depending on the protocol, it is responsible for confirmation that the whole message was received and sends messages to the source requesting data packets that were corrupt in or missing from the transmission. The final layer we will address is the Application Layer (Layer 7) with which the user directly interacts. This is the only layer that most users see and are actively aware of.

After briefly discussing the most important facets of Internet structure, it is important to see how all aspects fit together. In this model, when User A transmits data to User B, the data flows through each of the layers. Each level adds its own header that contains information the layer will use on the receiving end of the transmission. Once the data and the headers arrive at the Physical Layer, the information, which is represented in bits, is converted into voltage fluctuations and transmitted across the physical wire (Physical Link). When the Physical Layer of User B receives these voltage pulses, it converts them back into bits and sends the data up through the seven layers. Each layer then takes the appropriate actions and transforms the data into material practical for the user. The Application Layer displays the recompiled data for User B. This is essentially the basis behind Internet traffic and how different computer users can communicate with each other.

OPEN SYSTEMS INTERCONNECTION MODEL

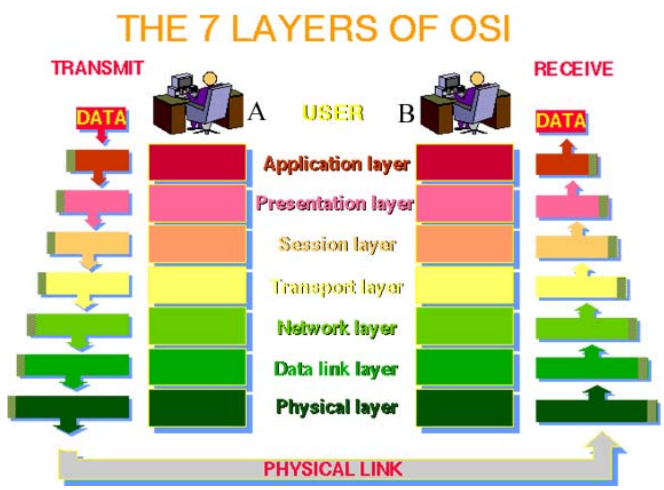

FIGURE 1 [2]

Physical Structure of the Internet

As we mentioned above, the physical layer and the physical link are the devices that transmit and carry out data transfers. Thus, these areas should bear special significance when considering today's Internet. The Internet incorporates several different physical technologies in order to smoothly transfer data. The backbone of the Internet is based on fiber optic technology. Fiber optics are universally considered a next generation technology but the speed of transfer makes it a necessary part of the current Internet also. Optical technology will be discussed in greater depth later in the paper under the next generation technology section.

Besides its optical backbone, the Internet has another primary constituent technology, the copper wiring that brings the World Wide Web to each home and office. Today, several forms of copper wiring are used to provide Internet access. "Cable Internet" is a link to a local or regional Internet Service Provider (ISP) via coaxial copper cable, the same cable that carries television signals. Many ISPs use this media because the infrastructure already exists in many areas. The television and data signals can be separated at user end of the cable and directed to each appropriate device. Another common connection to the Internet comes through Unshielded Twisted Pair (UTP) copper wire loops (Cat 3) using Digital Subscriber Line (DSL) technology that can share usage of the same UTP copper loops with existing plain old telephone service (POTS). However, the most common type of physical connectivity is the "dial-up" modem. This is similar to DSL in that it also uses existing telephone lines for data transference. The main differences between the two are transfer rate and coexistence with voice communication. DSL can broadcast simultaneously with voice communication on the same telephone line because it transmits at a different frequency than voice communications. This feature allows DSL to have an "Always-On" type of connection, similar to cable Internet. DSL also transmits more data than traditional Dial-Up because it uses modulation techniques to pack the data more efficiently. DSL has a bandwidth of 9 Mbps where Dial-Up only has a bandwidth of 56 Kbps, a speed over a thousand times slower. These forms of Internet are the most common versions of home access. [3]

Another class of Internet Access refers to network connections primarily used at business settings or on college campuses. Local Area Networks (LANs) offer high speed Internet access through the use of Category 5 (CAT 5) cables and are the primary example of network Internet connections. CAT 5 is a very practical medium for office networks because it is cheap and still capable of transmitting data expediently, reaching speeds of up to 100 Mbps. The other network Internet connection exists in Wireless Local Area Networks. This technology is still in its infancy, especially in the United States. It is usually considered to be a next generation technology and, as such, will be discussed in detail later in this paper. As applications use the Internet more frequently and intensively, the need for faster physical technologies is apparent.

Logical Structure of the Internet: The Internet Protocol

After addressing the physical structure of the Internet, we must also address the protocol behind all Internet activity. Internet Protocol Version 4 (IPv4) is the current standard Network Layer protocol of the Internet. However, it is unreliable and lacks built in security mechanisms. Anyone who intercepts IPv4 traffic can read the content unless a person makes a special effort to encrypt the information. Besides the security and reliability issues, IPv4 only uses a 32 bits name, an IP Address, to identify given logical device on a network. The address is represented in a dotted-decimal format using four octets of 8 bits each, e.g. 65.108.6.108. The number of IP Addresses provided by a 32-bit addressing system is not sufficient for the growing user base of the Internet. Finally, IPv4 has no current mechanism to handle network intensive applications efficiently. For example, Real Time video is a network application that requires great bandwidth and must be carried out in order to provide a live video stream. IPv4 would have a very hard time carrying out the tasks this application would require of it. Internet Protocol Version 6 (IPv6) solves many of the problems that IPv4 currently faces by increasing addressing space, adding security and reliability, and expanding functionality. [4]

NEXT GENERATION PHYSICAL TECHNOLOGIES

As time passes and technology improves, the Internet will continually improve, becoming faster, more reliable and secure. In order to successfully bring about great improvements, two distinct areas must develop and mature. These two areas are the IPv6 protocol, the logical force behind the new Internet, and the optical and wireless technologies, the physical structures behind the new Internet. In this section we will focus primarily on the physical nature of the new Internet and address IPv6 in a later section.

Optical technologies

In this new millennium, the world needs new technologies in order to accommodate the needs of the ever-growing number of people on the Internet. In order to address these concerns, faster, more efficient means of data transportation have been developed. This next generation networking technology is founded upon the principles of fiber optic communications. As addressed earlier, the backbone of the current Internet system is founded upon a fiber optic backbone. However, the today's Internet and local area networks still primarily use traditional wiring to connect users to the Internet and transfer data. Wiring has served its purpose well over the last century as the means of data transport but it has too many limitations to meet the world's need in the future. Wires, even those that are considered the best conductors, have transfer speed limitations because data is carried on electrons, charged particles that have mass associated with them. As data travels along this medium, it moves more slowly than the speed of light due to physical limitations and it can be corrupted by surrounding electromagnetic fields due to the negatively charged nature of electrons. Because of these shortcomings, our data transfer rate and reliability is severely impeded. [5]

With these limitations in mind, scientists and engineers developed a new form of data transfer known as fiber optics. Unlike wires, fiber optics attaches data to light beams and transmits, not along a metal wire, but along a glass fiber. The result of such a transmission is communication at the speed of light, a necessity for the networks of the 21st century. Fiber optic communication works by transmitting light into the end of a glass fiber at an angle greater than the critical angle of reflection so that the light will reflect within the fiber until it exits the other end at its destination. Besides just offering faster communication, fiber also offers greater data capacity. Unlike metal conductors, multiple data transmissions may take place on a single fiber by broadcasting data at different light (electromagnetic) frequencies. Wires require a dedicated line in order to transmit data from point A to point B. These are just some of the benefits optical communication has to offer. [5]

Although optical technology holds much promise for the future, several obstacles have only been solved recently in order to make it more economical to implement. The first obstacle was finding a transferring medium most suitable for data transfer on light beams. Such a material was found in silica sand, a very abundant planetary resource. Scientists discovered that this sand could be inexpensively turned into a silica glass that was suitable for data transfer. A second problem in development was signal degradation. Fiber optics were useful for short range transmission but, as the transfer distance increased, the signal weakened and became very ineffective. The first solution to this problem was amplification of the signal while it was in an electrical state. This was a costly procedure which involved converting a weak light signal to an electrical signal using a repeater, a photon to electron conversion unit, using an electrical amplifier to increase signal strength, and then converting the signal back to a light. This was a cumbersome process so experts in the field began development of all optical amplifiers, which increase signal strength while the data is still in the form of light. Two distinct optical amplification methods have been developed to address the problem. The first method is semiconductor amplification which sends the light beam between two semi-conducting materials, thus amplifying the light as it passes through. The second method of optical amplification is known as Erbium-doped fiber amplification. This process takes excited Erbium ions to uses their excess energy and to fuel the beam and increase transmission strength. With the resolution of these problems optical networks are ready and able to increase transfer speed and make the Next Generation Internet a truly great technology. [5]

Wireless Technologies

Optical networking is an essential part of the Next Generation Internet. However, another technology that has the prospect of changing the Internet as we know it is the wireless local area network (WLAN). Unlike the standard LAN and other hard-line connections to the current Internet, WLANs give the user a great boon, mobility. With this technology, employees of companies would be able to carry their laptops around company buildings and could have instant access to company resources and the Internet if they had to do work outside of their offices. Wireless LANs are considered a next generation technology that will greatly shape the future of the Internet and network systems.

WLANs are another technology of the future and, once the problems are worked out, they will be an integral part of communications technology. Wireless networking, as is apparent in the title, does not have a direct connection into the Internet. Rather it utilizes specific electromagnetic radiation frequencies, ranging from 900 Mhz to 2.4 Ghz, to transmit and receive data. Within a standard network that supports wireless technology, there are several wireless gateways to the network and Internet called access points through which all data travels. However, because the data is transmitted over radio signals, the guaranteed data transfer rate is only 2 Mbps, megabits per second, in the United States. Europe, on the other hand, has put more effort in developing WLANs than the United States. Because of these efforts, Europe has been able to achieve wireless transfer speeds of up to 24 Mbps, this being much faster than many wired LANs. As the United States follows the lead of its European counterparts, WLANs will contribute greatly to the effectiveness of the Next Generation Internet. [5]

However, with all the promise Wireless networking presents, one must remember their biggest downfall, their total lack of security. WLANs, unlike their hardwired counterparts, are very easy to break into and, thus, cause a company serious problems. Many companies today like the convenience wireless networks offer but do not think that they are worth the security risk. Several wireless network security measures have been developed over the past few years but all of them have been proven inept and easily circumvented. The most recent protection, Wired Equivalent Privacy (WEP), which was thought to be a valid, safe form of network protection, was proven inept by a team of scientists in 2001. This security problem is the major deterrent against corporations' widespread use of wireless networks. [6]

Although there is little security for wireless networks at the moment, several solutions are in development. New hardware that contains the new Advanced Encryption Standard chipset is being produced and eventually all wireless network users will have to purchase the improved hardware. Also, companies need to apply greater protections on the wireless access point, the spot through which all wireless network connections are routed to reach the network. [6]

This problem is a major deterrent to WLANs and have thus slowed their development in the United States. However, the problems involving security are already being solved and will hopefully pose no problems in the near future. Thus, wireless networking should still be pursued because its benefits far outweigh its problems and it will add a new dimension to the Internet that is fully present at the moment

NEXT GENERATION INTERNET PROTOCOL (IPV6)

IPv6 Header

IPV4 HEADER

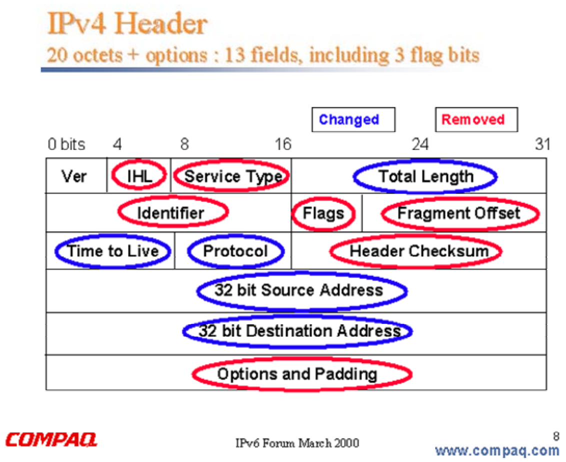

FIGURE 2 [7]

IPV6 HEADER

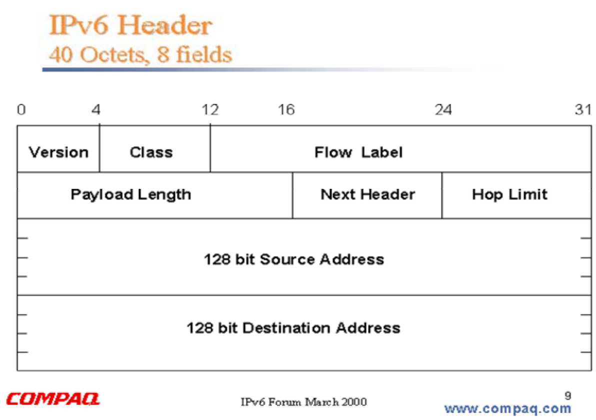

FIGURE 3 [8]

While physical technology is important, the driving force behind the Next Generation Internet movement is the IPv6 protocol. The defining characteristic of any network protocol is the header section. The IPv6 header resides in Layer 3 of the OSI model, alluded to earlier in the paper. This header provides information to Layer 3 devices about the source, destination, and handling of the packet. Packet routing occurs at Layer 3.

The IPv6 header, the basis of all Next Generation Internet travel, can be broken into several sections. The first row is divided into three distinct divisions. The Version field in the upper left hand corner tells the devices involved in the data transfer which version of the Internet Protocol the packet is using. Fig. 2 shows that the version field remains constant from IPv4 to IPv6. The second area called the Class field prioritizes the data packets that the header is sending. Based on the priority of the packet in relation to other similar groups, the router will treat packets differently. The third and final field of the first row is the Flow Label. A given transmission of data from one source to another is assigned a flow label number. When a router is processing a packet, it will look at the source address, the destination address, and the flow label. If it finds that it has already routed a packet with these credentials, it will simply send the packet along the same path as the previous packet with the matching credentials. This allows very quick routing of packets within a larger transmission because the router spends less time deciding on which interface to send the packet out. In addition, a flow can be given special treatment due to the class of the packet. This helps the prioritization of time sensitive traffic such as Real-Time video and audio streaming. Overall, flow labeling will expedite the routing process, consequently increasing network efficiency. [4][9]

After the elements of the first row have been scanned, the second row is examined. The first section, Payload Length, tells the devices involved how much data is being carried within the packet. This length does not include the Layer 3 header, but only counts the data or payload. The Next Header field, the second division of this row, allows the implementation of Extension Headers, one of the key improvements in IPv6. Extension Headers are not actually part of the IPv6 header but will be discussed at the end of this section. The Next Header field indicates whether there are any Extension Headers, and if so, what header follows next. By establishing extension headers, IPv6 maintains all the functions of IPv4 without storing all the options within the primary header. This method standardizes the IPv6 header length unlike the IPv4 header which varies in length based on the length of desired options. Now a router does not have to spend time calculating where the header begins and ends and, thus, this saved time increases overall network throughput. Finally, the Hop Limit field shares similarities with the Time to Live field in IPv4 by telling the router when to trash a packet. Each intermediate device that looks at the Layer 3 information subtracts one from the Hop Limit value. When the Hop Limit reaches zero, the packet is discarded thus preventing packets from endlessly traveling the Internet and causing needless congestion. [4][9]

Besides the fields previously discussed, the router also reads the logical addresses of the packet, the Source Address and Destination Address. The IPv6 and IPv4 addressing schemes are both designed in a hierarchical structure. However, the rapid growth of users on the current Internet has created a massive shortage of addresses. In addition to limiting the users that are directly connected to the Internet, such a shortage has caused the degradation of this hierarchical structure. The addresses in IPv6 use 128 bits instead of 32 bits and creates a plethora of available addresses. This will enable the expansion of the Internet for many years to come as well as reestablish the logical state of the addressing structure. Routers now will have to know less about their surroundings to route a packet effectively and thus will route more efficiently. This new efficiency cuts down on routing overhead on the network and consequently improves the performance of the Internet. Due to the number of improvements made in the development of the IPv6 header, the new Internet will ultimately be far superior to what we have now and can truly serve us in the future. [4][9]

IPv6 Extension Headers

Besides the IPv6 header itself, the other very important aspect of the next generation protocol is the extension header. As mentioned earlier, all data sent over the Internet today is encapsulated within an IPv4 header. However, IPv6 set up a new system of data organization under the form of extension headers, of which six are primary. The first main extension header is the Routing header, which designates all the locations a data packet must stop on its way to the final destination. This is one of the few parts of the IPv6 protocol that is examined at every stop on its transmission. Two other important extension headers refer primarily to imbedded security options. These are known as the Authentication header and the Encapsulating Security Payload header. These headers govern encryption settings, passwords and even set up a time counter to make sure the data is analyzed at the proper time by the correct machine. The fourth header is called the Hop to Hop Options header, which dictates tasks to be done at each individual stop. Like the Routing header, it is another extension header examined at every stop the data makes. The final two headers of importance are the Destination Options header and the Fragment header. The first of these headers contains special instructions that are read at the final destination. The fragment header, on the other hand governs how all the data is divided and sent as packets across the Internet. These IPv6 extension headers add a new dimension to Internet protocol that is not present in the IPv4 protocol. The way these headers were designed contributes greatly to the efficiency of the IPv6 protocol and will remedy many problems that plague the Internet today. [4]

TRANSITIONING TO IPV6

At the moment, IPv4 protocol is what is most commonly used by the world today. However, if the world will ever make the switch to IPv6, a gradual changeover must take place. The transition from IPv4 to IPv6 involves the coexistence of the two protocols. There are three main transitioning mechanisms that are currently being implemented: dual IP stacks, translation, and tunneling.

Dual IP Stacks

When posed with the problem of two devices, one or both of which may be using IPv6, communicating with each other, a relatively simple solution appears. Make any IPv6 device “speak” in both the IPv6 and IPv4 language. This is the concept behind the dual IP stack transition mechanism. In many implementations of IPv6, a client will have both an IPv4 and an IPv6 protocol stack at its disposal. Such a node would have two separate protocols operating at the network layer (Layer 3) of the OSI reference model. Thus, the levels above Layer 3 must also operate under different protocol structures.

How then does the node know which version of the Internet Protocol to use when transmitting and receiving data? When receiving a data packet the node will look at the Version field in the IP header, which tells the node which version of IP that packet is using. The procedure for transmitting is slightly different than receiving. When transmitting a data packet, there is not yet a Version field because the sender creates the IP header. To determine the proper version, the computer looks at the destination address. This analysis will determine whether it is a 128-bit address or a 32-bit address, sending it to the IPv6 stack or IPv4 stack respectively. [10][11]

The implementation of dual IP stacks presents a partial solution which introduces a possible problem. What if a node is only using IPv6? This can be dealt with by using protocol translation.

Translation

A translation mechanism is usually in the form of a network device such as a router or gateway. This device is fitted with dual IP stacks and allows for a local area network (LAN) to use only the IPv6 protocol. These networks are often called IPv6 islands. The device with the dual stacks is on the border of the network, controlling incoming and outgoing traffic. In addition to routing the traffic to the appropriate node, the device must translate between the IPv4 header and the IPv6 header. This translation occurs both ways. In a 6to4 translation, the router or gateway will convert the IPv6 header into an IPv4 header and then send the packet over an IPv4 network link. Because of the differences in the IP headers, many of the features of IPv6 such as flow labeling are lost in the translation process. Since the dual IP stacks create dual Transport and Application layers, the conversion must also traverse these layers. This results in not only a conversion of the IP header, but also the payload of the packet. In addition to the previous methods listed, a third technique for implementing IPv6 in an IPv4 world is tunneling. [11]

Tunneling

The tunneling of network traffic can help solve the problem encountered by IPv6 islands. Tunneling involves the encapsulation of an entire IPv6 packet within an IPv4 header allowing IPv6 packets to travel over IPv4 networks without experiencing the functionality loss of translation. With this technique, an IPv6 packet is sent to a tunnel endpoint across an IPv6 network. The tunnel endpoint then creates an IPv4 packet storing the IPv6 packet as its payload. This IPv4 packet is then sent over the IPv4 Internet until it reaches a tunnel endpoint that can communicate with the IPv6 destination node. This endpoint then removes the IPv4 encapsulation and sends the IPv6 packet along the IPv6 network until the packet reaches the intended destination. With this approach, no IPv6 functionality is used until the packet sheds its false IPv4 skin resumes its course over an IPv6 network. The only downside to using this tunneling mechanism exclusively is the difficulty experienced by an IPv6 node while attempting to find an appropriate tunnel endpoint. [10][11]

No single transitioning mechanism will solve the problems of IPv6-IPv4 interoperability. The combination of these techniques will pave the way to a new Internet, the IPv6 Internet. As with any other technology, improvements and innovations in the transition process will accelerate the convergence of IPv6. Compatibility with IPv4 is requisite of the success of the Next Generation Internet.

EVERYONE PUT ON A SMILING FACE

When one looks at the Next Generation Internet technologies, sustainability may be hard to address at first sight. There are no harmful environmental issues to address, one of the most definite areas of sustainability. However, at closer examination this issue clearly affects quality of life. This technology may not have as visible consequences of a medical breakthrough but it does make a person's life more comfortable. As more people go on the Internet to make purchases, set up their own web pages or just try to surf the net, web traffic increases beyond the capabilities of the current system. This could mean slower connection speeds, less reliability and even less Internet security. The development of next generation technologies services all these problems and makes all Internet users' lives a little easier and secure.

One may argue that the new Internet will not be much different than the current system and that this plays no part in quality of life. We would firmly disagree. How many times a day does a person sit at a computer waiting for a web site to load? As time passes, frustration builds and on occasion the person might actually lose his or her temper. With the development of fiber optic communication, waiting time would drastically decrease and the person would be in a much better and friendlier frame of mind. Also, fiber optics would greatly change the way people communicate via computer. Many people today spend a great deal of time "talking" to people using AOL instant messenger. Often times, typing may be tedious and one can not always convey the meaning he or she is trying to get across. With fiber optics and the increased Internet capabilities of IPv6 protocol, a person could hold a crystal clear conversation face to face over the computer. There would be fewer connection errors or transmitting problems. This would definitely improve everyone's life and have an overall positive effect.

Besides making every person's life easier, the new Internet would make each person's personal data and computer secure through the implementation of the IPv6 protocol. IPv6, unlike IPv4, has built in security mechanisms that protect any information sent over the web. This added security means that a person would not have to worry while sending personal information, such as credit card numbers, bank numbers and social security numbers, over the Internet. Also, due to the nature of this new Internet protocol, personal computers would be less susceptible to hacking. Security is one major benefit that IPv6 offers which no other Internet protocol has offered before.

However, as you have probably gleaned from this paper, this great new technology will eventually require the construction of an entirely new network infrastructure. Such a development will take many years to complete and cost millions upon millions of dollars. Although fiber optic equipment is dropping in price it is still a very costly technology. The conversion from wired networking systems to optical systems will be very costly and very many people are not ready to make the transition. However, as improvements on fiber optic systems are continually made and IPv6 gradually phases out the current Internet, prices will come down and more people will enter the new age. The eventual benefits of such a communications system are unfathomable and far outweigh the costs which are required to implement the new technology. We are very optimistic about what the future of the Internet has in store for us and are ready to witness yet another great technological advance.

CONCLUSION

As we stand today and look back through history, the accomplishments mankind has made in the realm of communications technology is astounding. No one would have foreseen the extent to which data transfer and communication have developed when the telegraph was first developed by Samuel Morse. However, every advance we made as a society has been built upon the work of those before us. Our current Internet can trace its roots back to first time a signal was sent over a telegraph. However, as a civilization we must look ahead and strive to greatness. The future is coming quickly and accompanying it is the next generation technology. The development of the new IPv6 protocol will replace the current IPv4 which is overtaxed and not up to challenge of supporting the ever-growing number of new technologies. Also, fiber optic data transfer will remove many bandwidth problems and increase the capabilities of the Internet beyond anything we can imagine. The Next Generation Internet is the future before us. Are you ready to accept it?

REFERENCES

[1] Izzo, Paul, Gigabit Networks: Standards and Schemes for Next-Generation Networking, New York: John Wiley & Sons, Inc., 2000.

[2] "Webopedia: The 7 Layers of the OSI Model" February 14, 2003 <http://www.webopedia.com/quick_ref/OSI_Layers.asp>

[3] "xDSL – Webopedia.com" February 14, 2003 <http://www.webopedia.com/TERM/x/xDSL.html>

[4] Miller, Mark A. Implementing IPv6, New York: M&T Books, 1998.

[5] Sadiku, Matthew N.O. Optical and Wireless Communications: Next Generation Networks, New York: CRC Press, 2002.

[6] Molta, Dave, "Wireless LANs reach the Last Hurdle", *Network Computing*, 13, No. 12, 10 Jun 2002, 38-43. Academic Search Elite

[7] "IPv4 Header." February 14, 2003 <http://www.ipv6forum.org/navbar/events/telluride00/presentations/yanickpouffary-compaq/sld008.htm>

[8] "IPv6 Header." February 14, 2003 <http://www.ipv6forum.org/navbar/events/telluride00/presentations/yanickpouffary-compaq/sld009.htm>

[9] Miller, Stewart S. IPv6, The Next Generation Internet Protocol, Boston, Massachusetts: Digital Press, 1998.

[10] Samad, M. et al, "Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version 4 (IPv4) Tunnel", *IEEE CNF*, 2002, 109-112. IEEExplore.

[11] Chang, Fangzhe and Waddington, Daniel G., "Realizing the Transition to IPv6", *IEEE Communications Magazine*, June 2002, 138-148. IEEExplore

ACKNOWLEDGMENTS

We would like to thank the Mr. Jeff Kissell and Mr. Doug Ripka, instructors in the Cisco Networking Academy, for providing a necessary networking background to write this paper.

We would also like to thank Dr. Stewart for providing a rudimentary background in electricity and Mr. Peter Scheetz (High School Physics Teacher) for providing a fundamental background in optical technology.

Lastly, Justin would like to thank his father, Stephen Fiore, for fueling his interest in electrical and computer engineering throughout his life.