IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 9, Issue 2 Ver. VI (Mar – Apr. 2014), PP 50-65
www.iosrjournals.org

Evaluate Signals Transmission over Internet Protocol Networks

Issa Obaid ALorf

Abstract: *The last decade has seen an explosion in the use of the Internet. Many more people are logging on the Internet, and Internet access has also spread to areas that have never had a telephone connection before. This growth in number of people accessing the Internet and the geographical spread has served to act as an impetus to the development of new applications on the Internet. The increased reliance on the Internet for a wide range of functionalities has given rise to the phenomenon of convergence. Convergence is the phenomenon of deploying various services, especially multimedia services, over traditional networks. Convergence is blocked by many problems that are caused by the inherent nature of the network expected to support these services. This research attempts to examine the state of integration of multimedia signals and their transmission over IP networks.*

Table of Contents

I. Introduction

A wide variety of new applications have been developed to work over the Internet. Modern information and communications tasks are all increasingly becoming reliant on the Internet. From banking to

entertainment, people are turning to the Internet more than ever before. This has led to increased traffic and functionality requirements of the Internet.

1.1 Convergence

The Internet traverses many different types of networks, physical and virtual, from underwater cables and dedicated ATM links to radio and satellite networks. However, the 'last mile' of the Internet is almost invariably the PSTN – the Public Switched Telephone Network. It is only a small minority of end users may not use the PSTN and connect to the Internet through other means such as fibre optic and wireless networks. Hence all the different types of communication packets, voice, video and data on the Internet have to travel through the PSTN to reach the end user. This is called convergence.

The PSTN is an ageing, analog network that provides users with dedicated end to end circuit connections for a session. The PSTN was designed for making telephone calls, and this dedication connection for a session is ideal for telephone calls. However, with increasing convergence, traffic on the PSTN is no longer mainly made up of telephone calls. More and more Internet communications packets are travelling through the PSTN network, due to increasing variety of services offered through the Internet, such as telephony, video calls, Internet television, etc.

Some of the services that a converged network may offer are the combination of wireless local area networks and cellular data networks to offer very high data rate capabilities (Salkintzis et al ,2002), video on demand (Lohan et al, 2002), real-time video streaming (Wu et al, 2001),

1.2 Economic Incentive for Convergence

It can be said that the single most compelling factor that drives convergence is convenience. Because the PSTN network is already a well-established infrastructure, it is more often than not easier to use the physical infrastructure of a network that has already been established. Installing new physical network infrastructure is often very costly. Hence there is a strong economic incentive for convergence. However, the pace of convergence is being greatly hindered by basic engineering trade-offs that exist because of the nature of convergence, which is essentially the act of forcing one type of traffic on the physical infrastructure of a network that was not designed to handle that type of traffic.

1.3 Aims and Objectives

Current research on the topic of convergence is vast. Many different methods have been proposed to solve the whole range of problems that arise due to convergence. However, to date, there has been no single or group of solutions that have proven to be sufficiently effective.

Thus, the main objective of this work is:

i. To attempt to examine state of integration of multimedia signals and their transmission over IP networks.
ii. To critically evaluate the state of convergence in terms of its success to date in order to be able to derive a hypothesis about the future of convergence.

In order achieve the aims described above firstly the work will examine current network topologies that are involved in convergence. This will include an examination of the characteristics of the different types of networks that the Internet traverses. This will help set the scene in order to understand the types of problems caused by convergence. This is followed by a discussion of the support for convergence in the new Internet Protocol (IP) standard, IPv6. Chapter four then examines convergence of VoIP (the Voice Over IP) Protocol, one of the most widely used multimedia protocols. Chapter five examines future convergence technologies and chapter six presents a critical evaluation of the state of convergence, with a conclusion that indicates further areas of research.

II. Network Topologies

This chapter discusses the topologies of the different types of networks in use today. Networks are composed of the hardware infrastructure, and the software that enables the communications. For example, in a wired network, the hardware consists of the copper coaxial cable, the connectors and other hardware in the network such as routers, and the software, such as the protocol that is used to transmit data.

A dedicated link is one where there are only two points in the network, and information travels only in one direction at a time (Harris, 2007). Such a connection requires much less overhead to transport information than more complex networks with a number of nodes. This is because the larger number of nodes a network has, the greater the number of paths from the source to the destination node. The transmission of information in this case requires management to ensure that the information originating from a source in a network finds, travels to,

and arrives at its destination using at least an acceptable path. The information in a network can travel from one node to another in two ways, through packet switching or circuit switching.

2.1 Packet Switching

Packet switching is the type of management of the transmission of information in a network where the information that has to be transferred from source to destination is broken down into small 'packets'. These packets are each loaded with information about the source, the destination and any other relevant details and then sent over the network individually.

Packet switching in practise can be of three different types, packet, frame and cell switching. Cell switching is when the information in broken up into chunks of fixed length. The 'chunks' are called cells. Frame and packet switching both break up information into chunks of variable length. The difference arises from the different method of implementation of the transmission. Packets and frames exist in different layers of the network – packets exist in Layer 3, the Network Layer, and frames exist in Layer 2, the Data Link Layer of the OSI network model. The Data Link Layer employs the Ethernet protocol to transmit frames, and the Network Layer employs the Internet Protocol to transmit packets. Furthermore, packets can be encapsulated into one or more frames, depending on the maximum size constraint dictated by the network, called the Maximum Transmission Unit.

The transmission units in a network (packet, frame or cell) need not travel by the same route even if their source and destination nodes are the same. The actual route they take depends on various factors such as the network management protocol that routes the packets (called routing protocol), the amount of other traffic in the network, etc. The decisions about which route to send a packet through can be dynamic, predetermined before the packet begins its journey, or made on the spot as the packet arrives at each node. Various different algorithms are used to achieve optimal routing, such as statistical time-division multiplexing which analyses the network statistics to determine the best possible route for a packet in that network.

The packets that form part of the same message are numbered, and therefore the receiving node is able to re-order the packets in their sequence as they arrive. This reassembling allows the receiving node to obtain the original message.

(Harris,2007, Kozierok, 2005 and Kenyon, 2002).

2.2 Circuit Switching

Circuit switching is quite different from packet switching; in circuit switching, a connection is set up whenever information has to be transferred from a source node to a destination node. This connection is called a circuit, from which the name circuit switching is derived. When a circuit is in operation, then the information can only travel through the circuit, or connection, from the source node to the destination node and cannot take any alternative path. A number of circuits may be in operation simultaneously in a network, and the network always holds information about the circuits that are in operations. Circuits can be set up as needed or can be permanent ones. Setting up a circuit involves the allocation of physical resources to the circuit, and hence the network requires and holds information about all the circuits in the network.

Although theoretically a circuit is a dedicated connection between two nodes, another type of circuit exists in large trunk connections. Here two or more circuits use the same set of physical resources that facilitate the large trunk connection using multiplexing. Multiplexing allocates small time slices to each circuit sharing the trunk connection. Traffic is then interleaved on the circuit (Kenyon, 2002).

The PSTN network is perhaps the most common circuit switched network. In the PSTN, when a person dials a number he is attempting to set up a circuit; if he gets through (the phone rings, or the person picks up) then the circuit is set up. The circuit is in operation throughout the duration of the call, and is broken when the call is ended. The route from the source to destination (caller to callee) may vary each time a call is made, even though the source and destination are the same. The choice of route is affected by many factors such as network bandwidth, route availability, etc. Circuit switching originated in the telephone network.

(Kozierok, 2005, Kenyon, 2002, Braun, 1997).

2.3 Transport Protocols

The transport layer of the OSI models has several protocols that are responsible for breaking up information into chunks, adding the required information (such as source and destination information) onto each chunk, and ensuring the delivery of these chunks without any errors. The protocols in this layer are the foundation of the Internet, and are therefore fundamental in determining the types of services that can be supported by the Internet. Among the protocols that are used for data transmission are TCP, IP, UDP, etc. Some of these are described below.

2.3.1 TCP – Transport Control Protocol

TCP is a reliable, connection-oriented, byte-oriented transport protocol. It is a full-duplex protocol, which means that each TCP connection supports a pair of byte-streams, one flowing in each direction. TCP also implements flow control, which means that there is a control on the speed with which packets are transmitted from source to destination; the control of speed ensures that the destination node's buffer does not overrun, and that each packet that arrives at the destination node is received properly. TCP also ensures that that the sender does not transmit too many packets at a time and create congestion in the network. TCP is an end-to-end, connection-oriented protocol, because when data is to be sent using TCP, a connection is established. The mechanism by which TCP establishes a connection is as follows:

i. The originator who wishes to send some information initiates a connection by sending a packet with the SYN bit set. This tells the receiver that the originator wishes to set up a connection.
ii. If the receiver is able/willing to reciprocate, then the receiver sends a packet to the originator with the SYN and ACK bits set. This amounts to telling the originator that the originator's request has been received, and can be accommodated.
iii. The originator then acknowledges receipt of this message with a packet with only the ACK bit set. Once the receiver receives this packet, the connection is set up. This mechanism is called the three way handshake. Once the connection is established, data packets can be sent.

(Hardy et al, 2002)

Fig 2.1 shows the format of the header of a TCP packet.

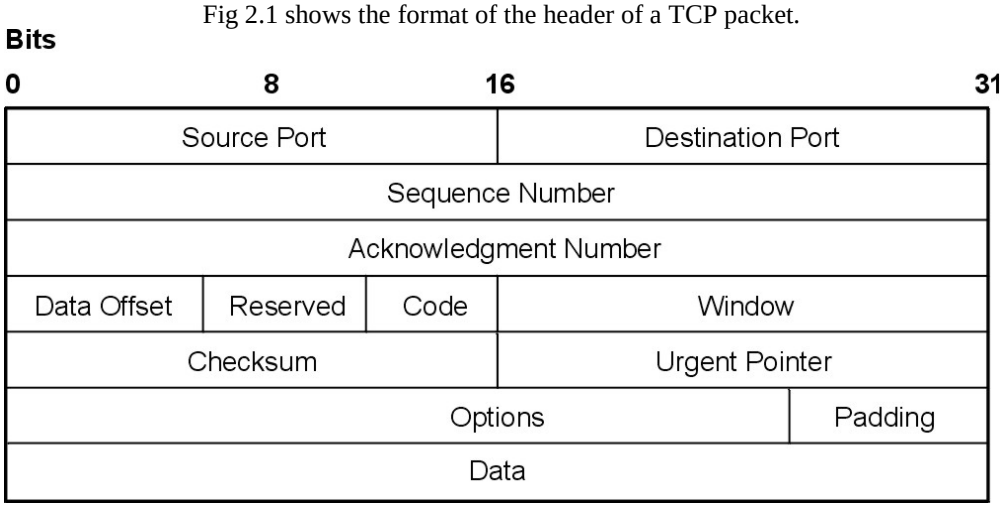

Figure 2.1 – TCP packet header (NCSA, n.d)

2.3.2 IP – Internet Protocol

The Internet Protocol, is a connectionless protocol. This protocol is described in detail in the next chapter and hence will not be dealt with here.

2.3.3 UDP – User Datagram Protocol

The UDP is a simple, connectionless protocol with little overhead. It provides unreliable data delivery. UDP packets may be lost, arrive out of order or be duplicated. As it is a connectionless protocol, each packet from a group of packets may take different routes to reach the destination even though the entire group have the same source and destination. The unreliable nature of the UDP protocol makes it unsuitable for services that have strict delivery constraints, such as voice communications. However, the small overhead makes UDP very desirable for other types of applications such as IP multicasting. Fig 2.2 shows the structure of a UDP packet.

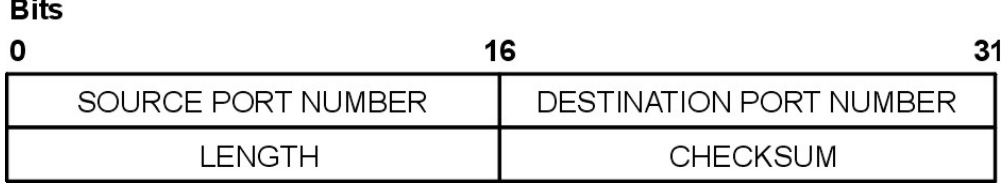

Fig 2.2 – UDP packet (NCSA, n.d.)

(Hallberg, 2005)

2.3.4 RTP/RTCP – Real Time Protocol and Real Time Control Protocol

The RTP is one of the specific protocols designed to support multimedia communications on the Internet. It can support real time unicast and multicast network applications such as audio and video streaming. It was developed by the IETF. The RTP protocol uses the underlying User Datagram Protocol (UDP) to manage multiple connections between two entities and to check for data integrity (checksum). RTP does not have any provision for ensuring or monitoring quality of service.

The RTCP is a control protocol, used to monitor data communications. It uses the same protocols as RTP. From time to time it sends control packets to all the nodes in a session in order to give a feedback on the data quality distribution, feedback used to keep control of the active codecs, advertise the number of session participants, and transmit other session control information (Minoli and Minoli, 2002).

Although these two protocols are called 'real time', they are constrained by the packet switched nature of the network. This means that there will invariably be some delay in practise (Schulzrinne et al, 1996). Fig. 2.3 shows the structure of the RTP packet.

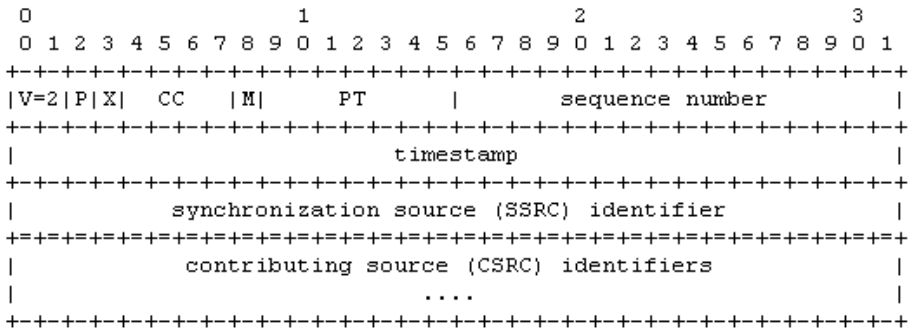

Fig. 2.3 – RTP packet (Schulzrinne et al, 1996)

2.3.5 SRTP – The Secure Real Time Transport Protocol

The SRTP is a specific implementation of the RTP that is designed to provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP). These additional features are facilitated by an additional encrypted section on the RTP packet which holds the encryption information. The originator and receiver in SRTP maintain cryptographic state information, called the cryptographic context. A key that is used throughout a session is used for encryption. A master key is used as the source from which the session keys are derived in a cryptographically secure way (Baugher et al, 2004).

2.4 Networks and Network Technologies

This section takes a look at the networks that are in use today, and the different network technologies that are relevant to convergence.

2.4.1 PSTN – Public Switched Telephone Network

The PSTN is the network to which every telephone in the world is connected. The majority of this network is built up of copper cables, but parts of the PSTN network have slowly been replaced with other types of digital networks. However, the final local loop, which is the part of the network that serves the individual nodes are still made up of copper wires. The local loop connects the individual telephones to the local exchange. Conceptually, the network is composed of a number of sub-networks, which are differentiated by its own unique set of codes (unique sequence of numbers). The entire PSTN network in a country is one sub-network, hence any nodes outside this network has to use the country code to specify access to this network. The country code for calling each country is unique, for example that of UK is 44, for Sweden is 41, for Singapore, 65 etc. Within the large sub-network of a country, there are many other sub-networks which generally serve a specific geographic region. Each region has a unique identifying code, and each telephone has a unique identifying number. Each telephone within the region can be accessed by a telephone outside the sub-network by using the unique code to access the regional sub-network prefixed before the unique identifying number for the destination telephone. For example, within the UK, there are a number of regions. If these regions are given the names A, B, C, etc. then a telephone in region A that wishes to call a telephone in region B prefixes the destination telephone number's unique identifying code with the code for region B. Two telephones which are in the same regional sub-network need not use the regional prefix code. The unique identifying numbers (addresses) for each telephone can therefore be either relative or absolute. Relative addresses may hold only the

unique identifying number, or have the regional prefix code; absolute addresses have all the unique identifying codes of all the sub-networks that the telephone belongs to. The PSTN network employs circuit switching (Harris, 2007).

2.4.2 ISDN – Integrated Services Digital Network

The ISDN is a communications protocol that works on the PSTN. This protocol offers digital telephony and data transport services over the analog PSTN. ISDN digitises communications over the telephone network, and this facilitates voice, data, text, graphics, and various other multimedia data to be transmitted over the copper wires of the PSTN. As the local loop of the PSTN is more often than not analog, the analog to digital or digital to analog conversion is done at the local exchange, beyond which the characteristics of the network change. ISDN is important from the point of convergence because it is the protocol that facilitates digital communication over an analog network. It facilitates a digital point to point circuit switched connection with full duplex communication and error handling (Harris, 2007). The ISDN protocol at the local telephone exchanges is what facilitates of new telephony facilities such as call waiting, caller id, speed dialling, etc. (Cisco, 2009).

2.4.3 SS7, C7 (Signalling System No.7)

The SS7 or C7 as it is otherwise known, s a global standard for telecommunications defined by the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T). The SS7 protocol facilitates the following facilities in the PSTN network:

i. Basic call setup, management, and tear down
ii. Wireless services such as personal communications services (PCS), wireless roaming, and mobile subscriber authentication
iii. Local number portability (LNP)
iv. Enhanced call features such as call forwarding, calling party name/number display, and three-way calling

(Performance Technologies Ltd, 2009)

2.4.4 PBX – Private Branch Exchange

The PBX is a private telephone switch that is located in a company's property. It supports all the functions of a local telephone exchange, but is private. It serves a large number of telephones all of which often belong to a single private entity. PBXs generally have a dedicated connection to the local exchange and control switching for both analog and digital signals.

2.4.5 DSL/ADSL – Digital Subscriber Line

DSL is a technology that allows the end user to have access to high-bandwidth, high-speed Internet over the copper wires of the PSTN network. DSL technology allows the transmission of data and voice signals simultaneously over the copper wires. It provides an 'always on' connection to the Internet. The implementation of DSL, although using the same PSTN network, requires different equipment at both the service provider's local exchange and the end user's connection point, and hence is not available everywhere (Harris, 2007). DSL achieves higher data transfer rates by using more of the available bandwidth spectrum. This is particularly important as it facilitates convergence, enabling continuous transmission of streaming video, audio and graphic-rich information (NexusNet, n.d.). ADSL (Asymmetric Digital Subscriber Line) is a particular implementation of DSL that is very widely used. ADSL is asymmetric, in that most of its bandwidth is allocated for downstream transmission of data, with only a small portion of bandwidth allocated for for upstream or user-interaction messages. This helps maximise the perceived speed of the connection, as the majority of user interaction with the Internet is downstream.

2.4.6 Internet

Kozierok (2005) states that the Internet is currently the largest network in the world. The Internet is made up of a huge number of computers around the world that are interconnected. It began as a small research network by a US defence organisation, but has since grown to span the whole world. The Internet is made up of all the protocols that facilitate the communication between computers over the PSTN network, and various other networks such as fibre optic networks, wireless networks, private local area networks, etc. Various protocols at various layers are used to facilitate communication on the Internet. The network layer protocols that are used in the Internet have been discussed in Section 2.3. Some of the application layer protocols that are used on the Internet are HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), etc. The World Wide Web is part of the Internet. It is a collection of websites, with information that is presented using the Hypertext Markup Language (HTML) in order to allow web browsers access to this information. The websites are hosted on

servers, which are computers connected to the Internet and have their own unique IP (Internet Protocol) address. In order to access a website, the user types in a URL (Uniform Resource Locator, or website address) into the browser. The browser sends the URL to a DNS server. The DNS server is a domain name server which maintains a list of URLs and their IP addresses. There are 13 DNS servers in the world, and collectively they store the IP addresses of all the unique domain names, or website addresses of all the websites in the world. If one DNS server does not have the IP address for a URL the search net is broadened to the other DNS servers. The browser thus obtains the IP address of the website from the DNS server, and the browser sends a HTTP request to this IP address. The server at the IP address responds by sending back a HTML page which is rendered by the browser. Hence it can be seen that the WWW is a special feature of the Internet, which allows the user to access website servers without having to remember the IP address of the server.

Lobovitz et al (n.d.) explain that the nature of the Internet, where it may takes tens of minutes to reach a consistent view of the network topology after a fault is major problem for convergence. The Internet takes many minutes to update its routing tables especially after a fault; this creates delayed convergence, where end-to-end Internet paths will experience temporary loss of connectivity. This is not a problem for the traditional Internet services such as the WWW (the user just needs to try again), but it creates a big problem for multimedia services such as telephony and streaming applications.

III. IPv6

3.1 Problems with IPv4

The version of Internet Protocol (IP) that is most widely in use today is the IP version 4, called IPv4. It was developed in the 1970s to facilitate data transmission over the then new network, the Internet. Hence the features supported by IPv4 reflect the requirements at the time. Because the network was a closed network, there was no necessity for security; because the network was very limited in scope, there was also no necessity for quality of service measures (Hagen, 2006). However, the explosive growth of the Internet has meant that today much more is required of the protocol. The explosive growth of the Internet also meant that another problem with IPv4, the lack of sufficient address space became a pressing problem. Because IPv4 was not envisaged to support a network with such a large number of nodes, it allocated limited space for the addresses of nodes. The increasing number of devices logging on to the Internet, from computers to mobile phones and other household devices meant that there would be too many devices and too little unique addresses for each of them. All these considerations prompted the development of a new version of the Internet Protocol, called IPv6.

3.2 Evolution of IPv6 – New Features Supported

IP supports many other protocols such as the UDP (User datagram protocol), TCP (Transmission Control Protocol), RTP (realtime protocol), RTSP (Real time streaming protocol), SDP (session description protocol), RTCP (Real time transport control protocol), etc. Each of these protocols was developed along the way when the need for the particular feature arose. Hagen (2006) details some of the new features that are supported by IPv6:

i. Extended address space – The space allocated for IP addresses is enlarged from 32 bits in IPv4 to 128 bits in IPv6. It also allows for hierarchical structuring of the address space, and facilitates the optimisation of global routing.
ii. Autoconfiguration – IPv6 supports stateless autoconfiguration. This means that when a device requests for an IPv6 address, it actually asks for its network prefix; the router then gives the network prefix to the device, which then autoconfigures itself for one or more global valid IP addresses. It uses information from its MAC address or a private random number to obtain a unique IP address.
iii. Simplified header format – The IPv6 header has a fixed length, 40 bytes, and is simpler than the IPv4 header. This results in reduced overheads for processing.
iv. Improved support for options and extensions – IPV6 carries options in its extension headers, allowing for this overhead to be dropped if they are not needed; this speeds up processing times when the options are not present.

3.2 IPv6

The Internet Protocol, is a connectionless protocol. This means that unlike a connection-oriented protocol, no connection is established. Packets are simply sent on their way to the destination code. Hence it is clear that IP does not guarantee reliable delivery of packets. Packets will therefore most likely arrive at the destination out of order, duplicated or not at all. Hence IP packets are often encapsulated in higher level protocols that provide reliability, such as TCP.

Each IP packet holds the source and destination address. Each packet can also take up a different route to reach the destination, even though two or more packets in the network may have the same source and destination. This means that routing is done at the packet level.

IP also supports fragmentation; this means that each packet can be broken down into two or more packets by the protocol. Das (n.d.) describes the architecture of IPv6 in detail. IPv6 addresses are broadly classified into three categories, unicast addresses (an identifier for a single interface), multicast addresses (an identifier for a group/set of interfaces that may belong to the different nodes) and anycast addresses (identifiers for a set of interfaces that may belong to the different nodes). From the point of view of convergence, IPv6 is a very important because it implements quality of service measures which are highly necessary for acceptable multimedia services. IPv6 ensures quality of service by classifying and marking packets to ensure certain set standards of delivery. Practically, this means that depending on the type of data being carried by the packet, the packet can be assigned different levels of priority. Voice data can be assigned a higher priority than normal data packets, and data from real-time applications can be assigned even higher priorities. This makes the transmission of packets containing multimedia data more reliable.

IPv6 mandatorily supports IPsec, thus facilitating security. It also supports mobile IPv6, which supports route optimisation. Figure 3.1 below shows the different architecture of the IPv4 header and IPv6 header.

The fields present in an IPv6 header are:

i. Version – version of the protocol
ii. Traffic Class – Holds information about the priorities of the IPv6 packets.
iii. Flow Label – used to label sequences of packets that require the same treatment for more efficient processing on routers
iv. Payload length – Length of data carried. The data comes immediately after the header.
v. Next header – Contains a protocol number or a value for an extension header
vi. Hop Limit – the number of hops. Decremented by one by every router. This ensures that the IPv6 packet does not take more than a specified number of hops.
vii. Source Address – the IP address of the source
viii. Destination Address – The IP address of the destination node

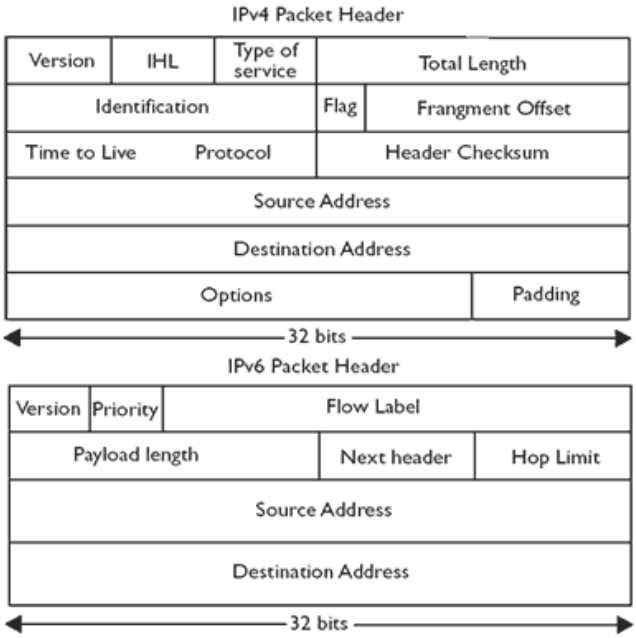

Fig 3.1 – IPv4 and Ipv6 packets (Mun and Lee, 2005.)

Loshin (2004) describes some of the practical problems faced by IPv6. Firstly, he explains that although IPv6 is capable of supporting a large number of devices on the Internet, the Internet backbones themselves are not capable of supporting a similarly large number of devices. He asserts that if such a large number of devices (of the order supported by IPv6) log on the Internet, this will cause a meltdown of the routing table. Hence IPv6 is only part of the solution to that limits the number of devices on the Internet. Secondly, Loshin also questions the need for such a large number of devices. Thirdly, there is the problem of adoption. In areas where IPv4 already meets all the needs of the users, there is no immediate need to switch over to IPv6.

IV. VoIP, or Voice over Internet Protocol

4.1 Introduction

VoIP is one of the most important protocols in convergence, because it allows the Internet Protocol to support voice services, and also some types of data and video services. VoIP can also work over the ATM (Asynchronous Transfer Mode) network. VoIP greatly facilitates convergence because it offers many

opportunities for the integration of voice services with data and video services, and also manages to provide significant cost savings. This is because VoIP allows electronic traffic to be carried over the same physical cabling and device (the computer) that handles the normal data communications over the Internet protocol.
Ahuja and Ensor (2004) examine the rapid expansion of VOIP technology and services. They find that the growth of VOIP is spurred by the dual benefits of decreasing costs and increasing revenues. VoIP allows service providers to reduce the cost of traditional services and also offer new multimedia services simultaneously. As VoIP uses the PSTN network infrastructure, the service providers are relieved of the necessity of installing expensive physical network infrastructure to provide new multimedia services. In fact, this means that the service providers can use the same hardware, and offer new services simply through the employment of new software. In other words, they can set up new revenue streams without substantial investment. Some of the new services that are offered by service providers using VoIP are click-to-dial services which allow users to control telephone calls from Web browsers, new media integration such as multimedia conference services, etc. The success of VoIP in facilitating convergence can be seen not only on the traditional PSTN network, but also in wireless and other wired networks (such as local area networks). IP networks are relatively inexpensive to use. This makes it even more attractive for the service providers to try to offer new services on the existing network, thus avoiding expensive investment in new infrastructure (Davidson, 2006, Khasnabish, 2003 and Johnson, 2004).

4.2 VoIP Quality of Service and Problems

VoIP works by digitising voice and transmitting it as a stream of packets over the Internet Protocol. Each individual packet is thus allowed to find the most efficient route to the destination. However, this also means that the packets thus sent will arrive at the destination out of sequence, at different times, and may possibly get lost on the way. Chong and Matthews (2004) explain how voice calls are made in this environment, stating that the end device (typically a computer) reassembles all these packets back in the correct order. The quality of a VoIP service therefore depends on many factors such as the amount of traffic in the network (which determines how long packets take to reach, are they able to take the most efficient route, are they lost etc.) as well as the efficiency of the end device in buffering the arriving packets and speed with which it can reorder the packets, etc. In practise, the quality of service is a major stumbling block in the path of effective VoIP implementations. This is because VoIP applications are competing with the telephony services offered by the circuit switched PSTN network. Circuit switched networks by nature of the dedicated connection they offer, can provide a high quality of service. Packet switched networks like the Internet on the other hand can only provide a lower quality of service. Bates (2000) lists some of the quality of service requirements for IP telephony, described below:

i. Variations of port definitions, or prioritisation of port interfaces based on application
ii. Dedicated paths for high bandwidth applications
iii. RSVP protocol

The new Internet Protocol, IPv6 attempts to address some of the quality of service problems of VOIP.
As VoIP is one of the key technologies that facilitates convergence, the success of convergence is strongly tied to the success of VoIP. VoIP must be robust and must be able to support a variety of features in order for it to succeed. This is borne out by Markopolou et al's (2002) assertion that in order for the Internet to constitute an attractive alternative to the PSTN, it must be able to provide high quality VOIP services. The quality of VoIP services over the Internet is measured by collecting delay and loss measurements between two different points, using appropriate voice quality measures. Such measurements are however not 100% accurate, as the different measurement facilities themselves, such as the probes introduce variances in the system. Markopolou et al (2002) state that the the quality of VoIP over the Internet backbones are very important because the quality of VoIP service on the backbones have an significant effect on the total quality of the VoIP service. Most VoIP services are facilitated by part of the transmission taking place on the switched telephone network in the local area and Internet backbones for the long haul. The fact that a large number of the backbone paths performed poorly for VoIP traffic, due to high delay and large delay variability (Markopolou et al, 2002) shows that the Internet backbones can be said to be a major obstacle in the path of convergence. Absolute delays and delay variability are much more important to voice traffic than they are to data traffic. Absolute delays are unacceptable for voice communications - a person cannot wait for 2 minutes after speaking to hear what the person on the other end replied; delay variability is also a problem because it makes it difficult for the VoIP software to predict the delay and make the necessary adjustments to ensure that voice communications flow smoothly. Markopolou et al's (2002) study found that the amount of delay and delay variability was so great that they would be totally unsuitable for telephony use in business conversations. Even paths with low delay and low delay variability occasionally experience long periods of loss that are disastrous for voice conversations.

Other problems that prevent more widespread adoption of VoIP are reliability, availability, scalability, service life, regulatory issues, etc (Chong and Matthews, 2004). Goode (2002) states that from an engineering point of view, a trade off between delay and efficient use of bandwidth must be made in a VOIP application. This is because VoIP services rely on the use of codecs (coder-decoders) which convert analog voice (sound) to digital data, and then break this data into packets that can be transmitted over the network. At the other end, the codecs must work to convert this information in digital packets back to analog sound. This process of conversion and breaking into packets consumes time, and creates a delay. Codecs can also be very complex, to ensure high fidelity, i.e. high sound quality is maintained. The higher the quality of the sound, the more complex the codec, and the longer it takes for the digitisation to be done, and consequently the greater the delay. Packets must however be ready without delay in order to take advantage of gaps in traffic as they arise, and thus use the available bandwidth efficiently. This shows that there is a trade off between delay and efficient use of available bandwidth. In practise, an acceptable level of delay must be set, which takes into account the available bandwidth, and the required voice service quality (Li et al, 2000).

Zheng et al (2001) state that delay jitter is also an important quality of service parameter for real-time services because delay jitters cause a significant deterioration in the quality of service for real-time traffic. Transient queuing effects can make it difficult to estimate delay jitter. Zheng et al (2001) conducted a study which showed that when the traffic load, traffic burstiness and the average ON (OFF) state length increase, the jitter behaviour significantly worsens. This means that the delay jitter between the speech samples may influence the service quality. Consequently, it can be said that VoIP capacity is highly sensitive to delay budget, and a small relaxation of delay budget can lead to more than 50% of capacity improvement.

4.3 VoIP over other Networks

There has been a significant amount of research into the deployment of VoIP over other networks (apart from the PSTN). Some of the other networks on which VoIP services have been deployed are wireless networks such as wireless local area networks, 3G networks, etc.

4.3.1 VoIP over WLAN (Wireless Local Area Network)

WLANs are increasingly being adopted especially in urban areas. WLANs are attractive because they facilitate roaming due to the lack of a wired connection to the network. Mobile devices are also catering for this demand, with new services that offer wireless access to the Internet. WLANs are also able to provide for a perpetual Internet connection, and today have acceptable levels of security. The increasing proliferation of WLANs means that it is also desirable to offer VoIP services over WLANs. VOIP services are provided over wireless networks by the implementation of VOIP protocols over the standard wireless network protocol, 802.11. Garg and Keppes (2003) examine the problems specific to the implementation of VoIP over 802.11. Some of the VOIP protocols have been customised for wireless networks. SIP (Session Initiation Protocol), for example, has been implemented as WiSIP, to deliver various telephony features over WiFi and WiMax networks (Kelly and Peterson, 2005).

However, there are two major difficulties that hinder the smooth implementation of VoIP services of a WLAN – low VoIP capacity in these networks and unacceptable levels of performance especially when the network is busy with traffic from other applications (Wang et al, 2005). One of the main problems are the lack of bandwidth, and hence the protocol overheads alone take up too much bandwidth. This means that only a few sessions can be supported simultaneously, creating a bottleneck. Wang et al (2005) however suggest a simple solution to the problem of coexistence of VoIP and other TCP traffic that only requires changes to the medium-access control (MAC) protocol at the access point.

The quality of VoIP service over a 3G WLAN is also beset with similar problems. The performance degrades significantly with the increase in number of VoIP connections, indicating that there is a maximum limit of the number of sessions that can be reasonably supported without too much degradation in quality of service. Moreover, the quality of service is also negatively affected by the mobility of the terminals; the greater the mobility, the poorer the performance (Rajavelsamy et al, 2005). Terminal mobility creates extra overhead in the network, and this indicates that there is problem with the coexistence of VoIP traffic and other network traffic, when the other network traffic increases.

4.3.2 VoIP over HSDPA

Rittenhouse and Zheng (2005) examine the use of VOIP over HSDPA. They find that HSDPA and other packet shared channel based system are promising choices for future data services, but they are not ready for immediate deployment of VoIP services. These networks need to be carefully engineered in order to support real-time delay-sensitive applications like telephony and streaming multimedia.

4.4 VOIP technologies

In practise, VoIP services are implemented with the help of a group of technologies that implement the necessary conditions for transmitting voice data over IP. Examples of these technologies are are SIP (Session Initiation Protocol), RTP (Realtime Transport Protocol), H.323, etc. These are described in the following sections.

4.4.1 Signalling over IP (SIGTRAN, Signal Transport Technology and SCTP)

SIGTRAN is actually an IETF task force that is dedicated to the development of signal transport technology. They specify a group of protocols that have been developed to provide reliable datagram communication over SS7 and ISDN. SIGTRAN protocols are important from the point of view of convergence because they provide the tools necessary for bridging the existing SS7 signaling network to the VoIP networks. Current SIGTRAN protocols are as follows:

i. SCTP - Stream Control Transmission Protocol, is an IP transport protocol designed for transporting signalling information over an IP network. It provides a transaction oriented data transmission facility in the network.
ii. UA - Common Signalling User Adaptation Layers (UAs)
iii. TUA - SS7 TCAP-User Adaptation Layer (TUA)
iv. SUA - SS7 SCCP-User Adaptation Layer (SUA) - Signalling Connection Control Part, facilitates routing, flow control, error correction, etc. in SS7
v. ISUA - SS7 ISUP-User Adaptation Layer (ISUA)
vi. M3UA - SS7 MTP3-User Adaptation Layer (M3UA) facilitates the implementation of SS7 user parts over IP.
vii. M2UA - SS7 MTP2-User Adaptation Layer (M2UA)
viii. M2PA - SS7 MTP2-User Peer-to-Peer Adaptation Layer (M2PA)
ix. IUA - ISDN-User Adaptation Layer (IUA)
x. TALI - Tekelec's Transport Adapter Layer Interface (TALI)
xi. SS7/IP - Miscellaneous SS7 over IP

(OpenSS7.org, 2006, Tuexen, 2008)

4.4.2 Speech Data Compression

The function of codecs has been briefly described in previous sections. Codes digitise analog voice into digital information and break them into chunks suitable for transmission by IP packets. The digitisation is however more complex in practise. Raw voice data when converted to a digital format, is relatively large. Hence various methods of compression are applied in order to reduce the size of the information that has to be transmitted and to prevent VoIP applications from hogging the bandwidth. Among the different digital audio compression techniques that are used are different types of sampling. Examples of these are ADPCM (adaptive differential pulse code modulation), APCM (adaptive pulse code modulation), etc. (Wylie, 1995). The different types of compression each have their own advantages and drawbacks; for example, compression can be lossless, where the quality of audio content is maintained at 100% (an accurate representation of the analog sound), or it can be lossy, where there is an acceptable level of deterioration or change in the digital sound. A trade off exists, between the quality of the sound and the size of the information.

Liu and Mouchtaris (2000) explains the importance of H.323, stating that is the key protocol that allowed the interoperability of VoIP products and moved the industry away from the initial proprietary solutions. Although it still has several limitations, these can be addressed using the concept of gateway decomposition. This protocol can also co-exist with other protocols such as H.248, and SIP which are increasingly being used for implementing VoIP services.

4.4.3 VoIP Security and H.323

One of the major practical considerations in deploying VoIP services is the security of the data being transmitted. Telephonic conversations, be it over the PSTN or over the Internet, should have an acceptable level of security such that they are not easily eavesdropped. Security of voice data transmissions over IP is one of the main problems in the path of convergence. IP packets by nature are very easy to 'sniff'. This means that it is very easy for a third party to capture and read the information in an IP packet, because the information is not encrypted in any manner. The H.323 protocol facilitates security of VoIP data, by providing authentication, integrity, privacy and non-repudiation. Authentication ensures that the originator's and receiver's identities are verified. Integrity is ensuring the integrity of the data in the packet that is transmitted, i.e. ensuring that the data in the packet received by the receiver is indeed the data as it has been sent by the originator. This amounts to assuring that that data has not been changed or tampered in any way by unauthorised entities along the way.

Non-repudiation is protection against false denials. This means that any VOIP data that is sent cannot be repudiated, i.e. once the originators identity has been verified and the session set up, the two ends of the session cannot deny their participation in the session (Pabrai, 2004).
In order to protect the privacy of VOIP data, the data in the IP packets must be encrypted. Sniffing is rendered useless if the data in the IP packets are encrypted. H.323 facilitates the encryption and decryption of data in VOIP packets (Goode, 2002).

4.4.4 SIP (Session Initiation Protocol)

The SIP is a control protocol that is used for controlling the setting up and breaking down of a session. It is similar to HTTP, in that it can signal the start and end of a session to the originator and receiver. SIP is also used to transmit other types of control information such as the type of the call, or session, for example, audio, video, a shared application, codec type, size of packets, etc. SIP does not specify an IP address, but specifies a logical destination. For example, the address could be an email or a telephone number. SIP also provides other features such as notification of changes in status such as a person coming online, email arrives, etc. (Goode, 2002).
Dalgic and Fang (n.d.) compare the two protocols, SIP and H.323. Both these protocols provide mechanisms for call establishment and teardown, call control and supplementary services, and capability exchange. They find that in terms of functionality and services that can be supported, H.323 version 2 and SIP are very similar. Supplementary services in H.323 are defined in much more detail, and therefore fewer interoperability issues are expected among its implementations. H.323 also ensures that there is compatibility among its different versions. Both the protocols have similar support for quality of service. SIP has a few advantages over H.323, in that it is more flexible, and therefore it is easier to add new features to SIP; it is also easier to implement and debug.

V. Future Convergence Technologies

This chapter attempts to examine the future of convergence technology. Some of the most prominent convergence technologies are discussed in detail in the following sections.

5.1 NGN (Next Generation Networks)

NGN is the used to denote the network that will exist once all the changes that are planned and/or currently in development have been successfully implemented. The term NGN is used for the network that is suitable for converged traffic will eventually take shape. It is envisaged that NGN will be able to support various technology domains that span from user premises to the core network. Mohapatra and Mortensen (n.d.) describe that the NGN would be composed of different segments, that are as follows:

i. Premises network—This is the network used by end users. End users can be individual home uses or business customers. Business customers may already have their own local area networks complete with physical network infrastructure, and therefore connect to the NGN using LAN protocols. The current increasing popularity of wireless networks indicates that home customers of the future may mostly use WiFi networks, and hence the NGN gateway will support many home networking technologies such as Ethernet, home phone line (Home Phoneline Networking Alliance [HPNA]), and universal serial bus (USB). Business entities are envisaged to connect through a customer-premises equipment (CPE) router to the provider's network.
ii. Access network—The access network is the service provider's network that comes right up to the premises network. It gives an ultra fast broadband connection in last mile. Various access technologies, including DSL, fiber-to-the-node (FTTN), fiber-to-the-home (FTTH) and also WiMAX technology will be used to connect to the end users.
iii. Aggregation network—The aggregation network, also called the metropolitan network, provides traffic aggregation from the access network and connection to the core IP/MPLS network.
iv. Core network – the NGN network is envisaged to have an MPLS–based IP network in core. Although there are many problems with an IP network that stand in the way of convergence, Mohapatra and Mortensen opine that the significant advances in IP combined with its inherent advantages makes IP remain as the best solution for convergence. The NGN network will also be expected to integrate with existing technology and protocols such as ATM.

Fig 5.1 shows the architectural view of a Next Generation Network.

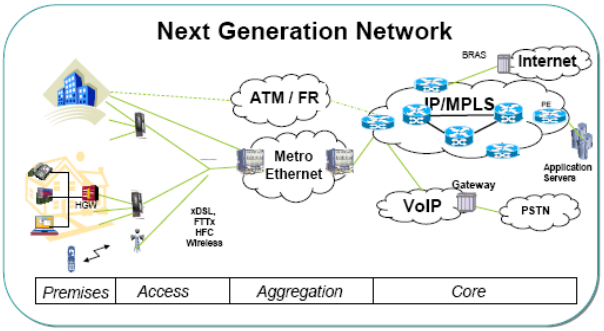

Fig. 5.1 – Architectural view of NGN network (Mohapatra and Mortensen, n.d.)

5.2 MPLS

Multiprotocol Label Switching (MPLS) is intended to be a technology that can support all the protocols in use today. It has been termed as the 'mother of all protocols'. It is envisaged to be scalable, and aims to eliminate dependence on data link layer technology. MPLS is expected to work on both packet switched and circuit switched networks. MPLS has been touted as the solution to IP QoS, gigabit forwarding, network scaling, and traffic engineering. MPLS adds the ability to forward packets over arbitrary non-shortest paths, and emulate high-speed "tunnels" between IP-only domains-capabilities critical to service providers (Armitage, 2002). MPLS forwards packets based on labels in order to implement a high performance packet forwarding engine. Routing is made to be separate from packet forwarding, and this facilitates the implementation of varied routing services (Viswanathan et al, 1998).

5.3 IMS (IP Multimedia Subsystem)

Chen et al (2006) describe IMS as "*a set of specifications that describes the Next Generation Networking (NGN) architecture for implementing IP based telephony and multimedia services"*. It is envisaged to facilitate the convergence of of voice, video, data and mobile network technology over an IP-based infrastructure. It is composed of a set of specifications that describes the NGN architecture required for implementing IP based telephony and multimedia services. Some of the salient features of IMS are:

i. It provides a standardised platform and reusable components. This allows the service providers to be able to easily adopt different services created by different providers and integrate two or more services. This creates an open market.
ii. IMS provides multimedia services with Quality of Service. This means that the technology will be able to guarantee levels of network bandwidth during transmission.
iii. IMS allows all services to be available irrespective of the users' location.

Figure 5.2 shows the architecture of the IMS network.

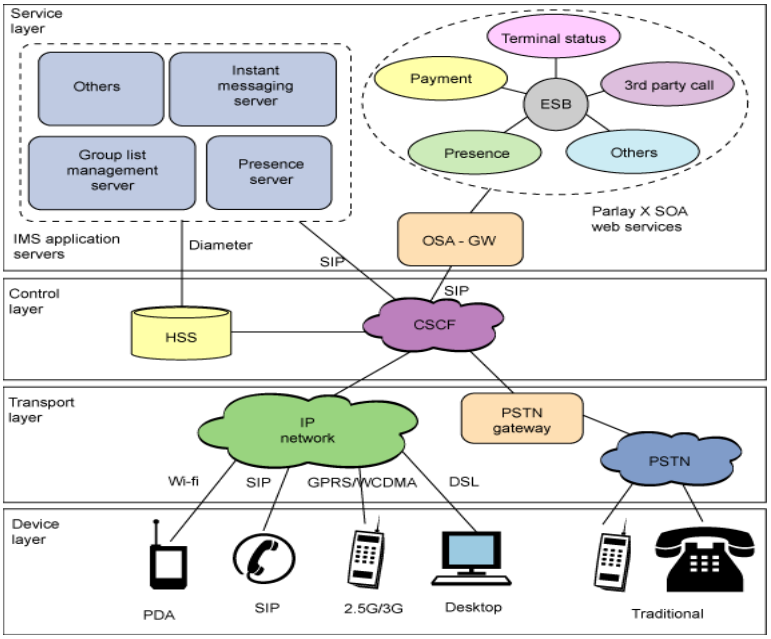

Fig 5.2 – Architecture of the IMS network (Chen et al, 2006.)

Camarillo and Garcia-Martin (2004) describe the various services that are delivered by IMS. They are:

i. IP Multimedia Sessions – IMS provides for IP Multimedia sessions over a packet switched networks.
ii. Quality of Service – IMS allows operators to control the quality of service that an end user gets.
iii. Interworking – IMS allows interworking between different types of networks, such as the circuit switched network, the PSTN and cellular networks.
iv. Roaming – IMS facilitates user roaming, without any interruption to the services that are provided.
v. Service Control – IMS allows network operators to impose policies on the services delivered to the user. These controls can be imposed on individual users as well as to all the users in the network.
vi. Rapid Service Creation – IMS standardises service capabilities instead of services. This allows service providers to rapidly offer new services.
vii. Multiple Access – IMS allows access through other networks, such as WLANs, ADSL, HFC (Hybrid Fibre Coax), etc.

Some of the protocols that are used in IMS are Session Control Protocol, the AAA protocol, etc.

5.4 Triple Play

The provision of three services, high speed Internet access, digital television, and telephone services over a single network is often termed as triple play. It is commonly used to denote the business use of the network, and does not indicate the provision of any of the technological features. Virgin may be one of the pioneering companies to offer triple play in certain areas. Virgin's fibre optic network that connects customers to its services, especially is newly cabled areas such as in Warrington in Cheshire is exemplary – it is able to provide high speed broadband (upto 50 mbps), with digital tv and telephony services over the same fibre optic network (Williams, 2008).

5.5 FTTx (Fibre to the X)

FTTx is the general term that is used to denote the network that is implemented using fibre optic cables, instead of the usual copper cables. Fibre optic networks are very expensive to install, but they are cheap to maintain. They also have many other advantages over copper cables, such as consuming less energy, being more secure, etc. Virgin is one of the companies in the UK that has made substantial investments in installing fibre optic network infrastructure. Several terms are used to denote the different levels of fibre optic network. They are:

i. FTTP (Fibre to the premises) - the fibre optic cabling infrastructure extends to the last mile, i.e. individual home customers connect directly to a fibre optic cabled network
ii. FTTC (fibre to the kerb)
iii. FTTB (fibre to the building).

Each of these different types of fibre optic networks indicate varying amounts of copper cabling in the network (Fibre to Home Council, n.d.)

VI. Critical Evaluation and Conclusion

6.1 Convergence – Solutions and The Future

Consumers today increasingly demand varied functionality, and expect these to be delivered on demand. The industry is responding by developing new services that cater for this need. It is becoming increasingly clear that different types of services, such as television, phone and Internet will all have to be served up on the same network, and is called convergence. The implementation of new services has been hampered by the lack of support from PSTN, the ageing dinosaur that was originally built for a different purpose. However, it is not possible to build an entire replica of the PSTN from scratch to support convergence, simply because of resource and cost limitations. Instead of making the best of the existing network, however, solutions for convergence have worked in two different ways. One, parts of the network that can be replaced has already been, currently is, or will be replaced. Examples of this are the inclusion of satellite networks were possible, the inclusion of fibre optic networks, etc. Two, solutions to facilitate better transmission of multimedia data over the existing network have been developed. This includes the development of new network protocols that provide for the additional features required by multimedia services, new network architectures, etc.

It is clear that there isn't a single solution that will facilitate total convergence in the future. Which solution becomes successful is partly determined by the robustness and efficiency of the solution itself, and partly by external factors such as existing network infrastructure, cost considerations, etc. For example, in a highly developed city like London which is already well-cabled, it does not make practical or economic sense to go about digging the underground copper cables and replacing them with fibre optic cables; on the other hand, in areas that have low copper cable density, it may make sense to install fibre optic cables. In large and unpopulated areas such as desert areas, it may not make practical or economic sense to lay underground cables;

wireless network solutions would be the way to go here. The fact that much of the populated regions in the world are already cabled to support the PSTN network makes it an unalienable part of the future of convergence simply for practical reasons, even though it may natively not be suitable for the transmission of digital multimedia information. Similarly, in terms of technology solutions, different groups of technologies may be suitable depending on the type and density of multimedia application that is required, the network environment, etc.

Some of the solutions developed to date such as VoIP and related protocols have been relatively very successful. Some of the solutions that have been proposed, such as NGN , MPLS, etc. are still very much in their infancy, and ambitious to say the least. Whether these technologies will ever mature and contribute to convergence remains to be seen.

6.2 Further Areas of Research

The demand for converged services is very high; today people expect to be able to make calls, watch tv and other streaming applications, surf the Internet, etc. all on one device. Televisions increasingly are providing for the functionality of surfing the Internet; so are mobile phones. People are increasing watching television programmes on their over the Internet. Hence just as the devices people use are becoming multifunctional, the network that is used also has to become multi-functional.

Current research in the area of convergence is very active; new solutions are being developed to allow the new features to be offered, straddling the old network. A prime example of this is the intelligent network (IN) which is a framework to decouple service logic from switching nodes and make it easily accessible from other nodes within the network. IN therefore supports both types of transport, uses existing infrastructure, reuses existing network services and offers new services (Chiang et al, 2000). One of the areas of significant demand within research in convergence is the provision of support for quality of service. Although IPv6 attempted to provide support for quality of service for converged networks, there are still some features that are lacking. Quality of service at different levels, such as at the Application Layer and Network Layer is also required. Security is also another major consideration. Although some solutions such as H.323 and some of the wireless protocols have paid attention to implementing sufficient security measures, much more remains to be done to ensure that security is achieved as a whole. Roy and Das (2004) show how research in this area can also be interdisciplinary. In short, it can be said that because of the varied type and high number of solutions that are being used to achieve convergence, the potential for research in this area is rich and will remain so for some time.

References

[1]. Ahuja, S.R. & Ensor, R., 2004. VoIP: What is it Good for? *Queue*, 2(6), 48-55.
[2]. Armitage, G., 2000. MPLS: the magic behind the myths [multiprotocol label switching]. *Communications Magazine, IEEE*, 38(1), 124-131.
[3]. Bates, R.J., 2000. Voice-over IP (VOIP), *McGrawHill.*
[4]. Baugher, M. Et al, 2004. The Secure Real Time Transport Protocol (SRTP). *IETF*. Available online at http://www.ietf.org/rfc/rfc3711.txt - last accessed Apr 2009)
[5]. Braun, T., 1997. Internet Protocols for Multimedia Communications, Part II: Resource Reservation, Transport, and Application Protocols. *IEEE MultiMedia*, 4(4), 74-82.
[6]. Camarillo, G. & García-Martín, M.A., 2004. The 3G IP multimedia subsystem (IMS), *Wiley.*
[7]. Chen, R., et al, 2006. Introduction to IP Multimedia Subsystem (IMS), Part 1. *IBM*. (Available online at http://www.ibm.com/developerworks/webservices/library/ws-soa-ipmultisub1/ - last accessed Apr 2009)
[8]. Cisco, 2009. Integrated Services Digital Network (ISDN) Overview. (Available online at http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ISDN.html - last accessed Apr 2009)
[9]. Chong, H.M. & Matthews, H.S., 2004. Comparative analysis of traditional telephone and voice-over-Internet protocol (VoIP) systems. In *Electronics and the Environment, 2004. Conference Record. 2004 IEEE International Symposium on*. pp. 106-111.
[10]. Dalgic, I. & Fang, H., n.d. Comparison of H. 323 and SIP for IP Telephony Signaling. In *Proc. of Photonics East*. (Available online at http://www.isdnsimulator.com/white_papers/dalg_comparison.pdf - last accessed Apr 2009)
[11]. Das, K., IPv6.com - IPv6 and the Next Generation Internet. Available at: http://www.ipv6.com/articles/general/ipv6-the-next-generation-internet.htm [Accessed February 12, 2009].
[12]. Davidson, J. et al., 2006. Voice Over IP Fundamentals, *CISCO Press*
[13]. Fiber to the Home Council. Available at: http://www.ftthcouncil.org/ - last accessed Apr 2009.
[14]. Garg, S. & Kappes, M., 2003. Can I add a VoIP call? In *IEEE International Conference on Communications, 2003. ICC'03*.
[15]. Goode, B., 2002. Voice over internet protocol (VoIP). *Proceedings of the IEEE*, 90(9), 1495-1517.
[16]. Hagen, S., 2006. IPv6 essentials, *O'Reilly*
[17]. Hardy, D., Malléus, G. & Méreur, J., 2002. Networks, *De Boeck Universite*
[18]. Hallberg, B., 2005. *Networking*: A Beginner's Guide. *McGraw Hill Professional*
[19]. Harris, S., 2007. CISSP All-in-one Exam Guide, *McGraw Hill*
[20]. Johnson, C.R. et al., 2004. VoIP reliability: a service provider's perspective. *IEEE Communications Magazine*, 42(7), 48-54.
[21]. Kelly, T.V. & Peterson, D., 2005. VoIP For Dummies, *For Dummies*
[22]. Kenyon, T., 2002. Data Networks. *Digital Press.*
[23]. Khasnabish, B., 2003. Implementing Voice Over IP, *Wiley.*
[24]. Kozierok, C.M., 2005. The TCP/IP Guide, *No Starch Press*

[25]. Li, B. et al., 2000. QoS enabled voice support in the next generation Internet: issues, existing approaches and challenges. *Communications Magazine, IEEE*, 38(4), 54-61.

[26]. Liu, H. & Mouchtaris, P., 2000. Voice over IP signaling: H. 323 and beyond. *IEEE Communications Magazine*, 38(10), 142-148.

[27]. Lobovitz, C., Ahuja, A. And Bose, A., n.d. Delayed Internet Routing Convergence. (Available online at http://exodus.cs.ccu.edu.tw/~cjwu/BGP/convergence.pdf - last accessed Apr 2006).

[28]. Lohan, F. et al., 2002. Integrated system for multimedia delivery over broadband ip networks. *IEEE transactions on consumer electronics*, 48(3), 564-574.

[29]. Loshin, P., 2004. IPv6, *Morgan Kaufmann*

[30]. Markopoulou, A.P., Tobagi, F.A. & Karam, M.J., 2002. Assessment of VoIP quality over Internet backbones. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*.

[31]. Minoli, D. & Minoli, E., 2002. *Delivering voice over IP networks*, Wiley.

[32]. Mohapatra, S.K. & Mortensen, M.H., A Solution Framework for Next-Generation Network Planning.

[33]. Mun, Y. & Lee, H.K., 2005. Understanding IPv6, *Springer*

[34]. NCSA, System Management Guide: Communications and Networks - TCP/IP Protocols. Available at: http://www.ncsa.uiuc.edu/UserInfo/Resources/Hardware/IBMp690/IBM/usr/share/man/info/en_US/a_doc_lib/aixbman/commadmn/tcp_protocols.htm [Accessed February 12, 2009].

[35]. NexusNet, n.d. What is DSL and ADSL. (Available online at http://www.nexusnet.com.au/knowledge/dsl.htm - last accessed Apr 2009)

[36]. Pabrai, U., 2004. The Challenge of VoIP Security. (Available at: http://www.certmag.com/read.php?in=957 – last accessed Apr 2009).

[37]. OpenSS7.org, 2006. Signalling Transport (Available online at http://www.openss7.org/sigtran.html- last accessed Apr 2009)

[38]. Pentikoussis, K., n.d. Can TCP be the transport protocol of the 21st century? (Available online at http://www.acm.org/crossroads/xrds7-2/tcp21.html - last accessed Apr 2009).

[39]. Rajavelsamy, R. et al., 2005. Performance evaluation of VoIP over 3G-WLAN interworking system. In *Wireless Communications and Networking Conference, 2005 IEEE*.

[40]. Rittenhouse, G. & Zheng, H., 2005. Providing VOIP service in UMTS-HSDPA with frame aggregation. In *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on*.

[41]. Roy, A. & Das, S.K., 2004. QM 2 RP: a QoS-based mobile multicast routing protocol using multi-objective genetic algorithm. *Wireless Networks*, 10(3), 271-286.

[42]. Schulzrinne, H, et al, 1996. RTP: A Transport Protocol for Real Time Applications. *IETF*. (Available online at http://www.ietf.org/rfc/rfc1889.txt - last accessed Apr 2009)

[43]. Salkintzis, A.K., Fors, C. & Pazhyannur, R., 2002. WLAN-GPRS integration for next-generation mobile data networks. *IEEE Wireless Communications*, 9(5), 112-124.

[44]. Tuexen, M., 2008. SCTP SIGTRAN and SS7 (Available at: http://www.cacetech.com/SHARKFEST.08/T1-12_Tuexen_SCTP_SIGTRAN%20and%20SS7.pdf last accessed Apr 2009)

[45]. Viswanathan, A. et al., 1998. Evolution of multiprotocol label switching. *Communications Magazine, IEEE*, 36(5), 165-173.

[46]. Wu, D. et al., 2001. Streaming video over the internet: Approaches and directions. *IEEE*

[47]. Williams, C., 2008. Warrington first to get Virgin Media 50Mb/s • The Register. (Available at: http://www.theregister.co.uk/2008/11/14/warrington_vm_trial/ - last accessed Apr 2009).

[48]. Wylie, F., 1995. Digital audio data compression. *Electronics & Communication Engineering Journal*, 7(1), 5-10.

[49]. Zheng, L., Zhang, L. & Xu, D., 2001. Characteristics of network delay and delay jitter and its effect onvoice over IP (VoIP). In *Communications, 2001. ICC 2001. IEEE International Conference on*.