

# ***Voice over Internet Protocol (VoIP): The “Killer” Application?***

Written for Mind Commerce by: P.J. Louis, July, 2004

[PJLouis@MindCommerce.com](mailto:PJLouis@MindCommerce.com)

Voice over IP (VoIP) is considered by many to be the “killer app” of the next generation network. The business benefits of VoIP deployment are: reduced long distance costs, lower network costs, and more enhanced services – Voice over IP is just one of the services. The technical benefits of VoIP deployment are: less bandwidth for more calls, more efficient use of network resources, and distributed network intelligence.



Research Consulting Training  
Technical Writing

---

[www.MindCommerce.com](http://www.MindCommerce.com)

## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Network Signaling</b> .....	<b>4</b>
The OSI Model.....	5
TCP/IP Model.....	7
Network Layer.....	9
Transport Layer .....	10
Application Layer.....	11
TCP/IP Protocol Architecture .....	12
<b>Philosophical Differences between the Internet and Non-Internet Worlds .....</b>	<b>14</b>
<b>Customer Demands of Voice Today versus National Security .....</b>	<b>15</b>
<b>Adaptive/Dynamic Routing</b> .....	<b>16</b>
<b>Quality of Service</b> .....	<b>16</b>
Availability.....	17
Mean Time between Failure (MTBF) .....	17
Reliability .....	18
Transaction Delay .....	18
Security .....	19
Bandwidth.....	20
Information Loss.....	21
<b>VoIP Market</b> .....	<b>21</b>
<b>About The Author</b> .....	<b>22</b>
<b>VoIP Research, Training and Consulting</b> .....	<b>23</b>

## Introduction

Voice over IP (VoIP) is considered by many to be the “killer app” of the next generation network. The next generation network will be Internet Protocol (IP) based. Depending on your definition of the next generation network, it could mean VoIP over wireless or VoIP over wireline networks. In reality it does not matter.

VoIP is voice over an Internet Protocol (IP) based network. All networks will be supporting IP. There are two ways of looking at VoIP: regulatory/business and technical. We are going to address the technology. The regulatory and business perspective will provide a framework by which VoIP will be provided. However, the regulatory and business view is far too complex to discuss in a white paper.

Before we leap into what VoIP is, engineers need to understand voice. As a service, voice is a basic necessity. Despite the preponderance of email, people prefer to talk to one another rather than email one another. Declining minutes of use in the wireline network is due to the existence of wireless communications and email. As a mass market service, voice is the basic service of all services. Without voice a telecommunications service provider is not meeting the needs of all of its customers. If one looked at every Internet Service Provider (ISP) today you would find that all of them are working towards providing voice.

The Internet was not originally designed to carry audio communications. In fact the Internet protocol could not meet the exacting requirements of the voice service customer. Furthermore, there were many engineers involved in the Internet who did not believe the Internet had to provide voice in a manner equal in quality to that of the circuit switched network. The lack of business and the need to make money changed all of that. Market realities in the end dictate how technology will be provided. Voice is the most sought after service across the entire telecommunications marketplace. Despite the various data tools and services available, people need to communicate verbally. Once an ISP is capable of providing voice it will be able to take advantage of its position as an information services provider to the user and provide all services (including voice) to the user.

At one time, VoIP was provided as a best effort service just as other Internet services had been. The Internet Protocol is a “best effort” protocol. The focus on the moving of data in the Internet world is on flexibility in interconnection not the reliability of the data at the destination point. Until recently the only thing that the Internet had guaranteed is that a “best effort” would be made to ensure the data arrived intact. This is probably not a fair statement to make today. The Internet community is working at meeting the needs of voice.

Is VoIP commercially viable today? The answer is technically yes and technically no. VoIP does work. There are regulatory, business, and implementation issues related to VoIP that need to be addressed. However, if past experience means anything all of these issues will be addressed simultaneously while VoIP is being aggressively sold.

As I had indicated the focus on voice as opposed to other data services is simple to understand. Voice is the application that appeals to the mass market. The revenue generated by the mass market is what is needed to get IP deployed. By itself, IP has enormous benefits. However, to the mass market the benefits of IP all boil down to a single idea; meeting the lowest common denominator for service needs and that common denominator is voice. IP networks have been around for years but until voice became a viable commercial service the investment community treated IP as a high-end technology meant for the lab. In fact until the market environment changed enough to warrant investors to spend money on deploying IP, VoIP was considered just voice over a packet data network. Until the revenue opportunities all but disappeared because of the “dot-bomb” explosion, the investment community ignored IP. Without any new opportunities VoIP and IP suddenly became popular in 2003. To understand VoIP we need to understand IP.

In general there are business and technical benefits to deploying an IP network. The business benefits are:

- Reduced long distance costs
- Lower network costs
- More enhanced services – Voice over IP is just one of the services.

The technical benefits are:

- Less bandwidth for more calls
- More efficient use of network resources
- Distributed network intelligence

In order to understand the aforementioned benefits we need to understand how IP works.

## **Network Signaling**

The network signaling protocol of the Internet is TCP/IP. The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite was originally used for and still is used for the internetworking of Local Area Networks (LANs). All of the signaling protocols used in the Internet are part of the TCP/IP protocol suite. The TCP/IP protocol suite was developed as a result of work first begun by the United States Department of Defense’s Advanced Research Project Agency (ARPA) in 1957. ARPA’s objective was to develop science and

technology in response to the military threat posed by the Soviet Union (at that time). ARPA was later changed to DARPA. The Cold War had initiated a technology effort that would eventually cause the most sweeping change in communication since the invention of the telegraph.

The TCP/IP protocol suite is composed of multiple protocols. The TCP/IP protocol suite is layered; more so than Signaling System 7 (SS7) or even ATM. TCP and IP are just two of the protocols in the suite of Internet protocols. The term TCP/IP refers to this family of protocols.

The TCP/IP protocol suite's multiple layers facilitate future development of new Internet protocols. Whether or not this was by design is not relevant for this discussion, however, it is fortunate that the suite was architected by the Internet Engineering Task Force (IETF) in this manner for it has enabled software engineers across the globe to find new applications for the Internet.

As I had noted, the protocol architecture of TCP/IP was designed for use by the United States military. Given its roots, the protocol suite is capable of interconnecting multiple pieces of equipment from multiple vendors. There are four layers to the TCP/IP protocol suite. The layers are:

- Physical/Link
- Network
- Transport
- Application

The layers correspond to the layers described in the Open Systems Interconnection (OSI) model. The OSI model was created by the International Organization for Standardization (ISO) for use in a computing environment. When communication is desired among computers from different manufacturers/vendors, the software development effort can be very difficult. Different vendors use different data formats and data exchange protocols that do not allow computers to communicate with one another.

The OSI model is an engineering model that breaks everything down into very simple and discrete tasks or layers. The OSI model serves as a framework for all telecommunications signaling protocol development.

## **The OSI Model**

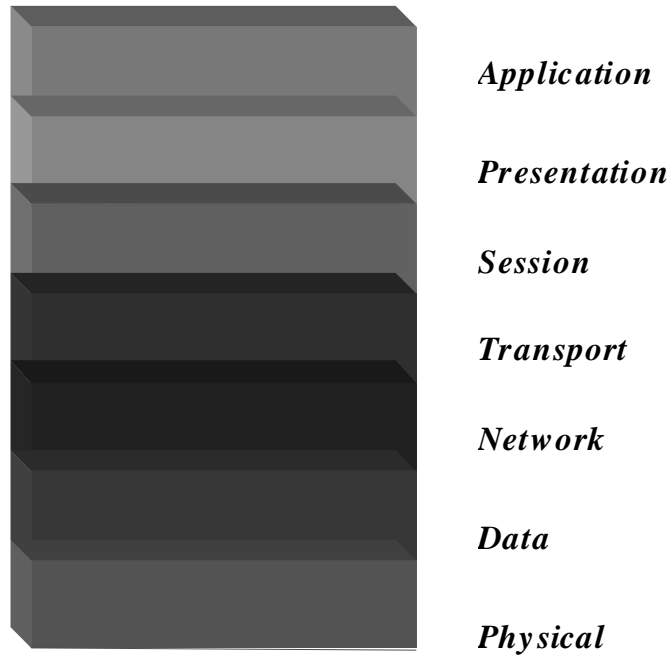
The OSI model consists of seven layers. The communication functions are broken down into a hierarchical set of layers. Each layer performs a related subset of the functions required to communicate with another system. Each layer relies on the next lower layer to perform more primitive functions and to conceal the details of those functions. It provides services to the next higher layer. The layers are defined in such a manner so that changes in one layer do not require

changes in the other layers. By partitioning the communication functions into layers, the complexity of the protocol becomes manageable.

The following is a description of the layered architecture starting from the bottom of the stack.

- Physical - Concerned with transmission of unstructured bit stream over the physical link. It invokes such parameters as signal voltage swing and bit duration. It deals with the mechanical, electrical, procedural characteristics to establish, maintain and deactivate the physical link.
- Data Link - Provides for the reliable transfer of data across the physical link. It sends blocks of data (frames) with the necessary synchronization, error control, flow control, and other overhead information.
- Network - Provides upper layers with independence from the data transmission and switching technologies used to connect systems. It is responsible for establishing, maintaining and terminating connections.
- Transport - Provides reliable, transparent transfer of data between end points. It provides end-to-end error recovery and flow control.
- Session - Provides the control structure for communication between applications. It establishes, manages and terminates connections (sessions) between cooperating applications.
- Presentation - Performs generally useful transformations on data to provide a standardized application interface and to provide common communications services. It provides services such as encryption, text compression and reformatting.
- Application - Provides services to the users of the OSI environment. It provides services for FTP, transaction server, network management, end users services, etc.

The following diagram, Figure 1, illustrates the OSI model. Notice that the following model is a picture of a stack of layers. The foundation layer is the Physical layer. Every other layer is built on top of the Physical and each other. You can see how these layers are interdependent upon each other.

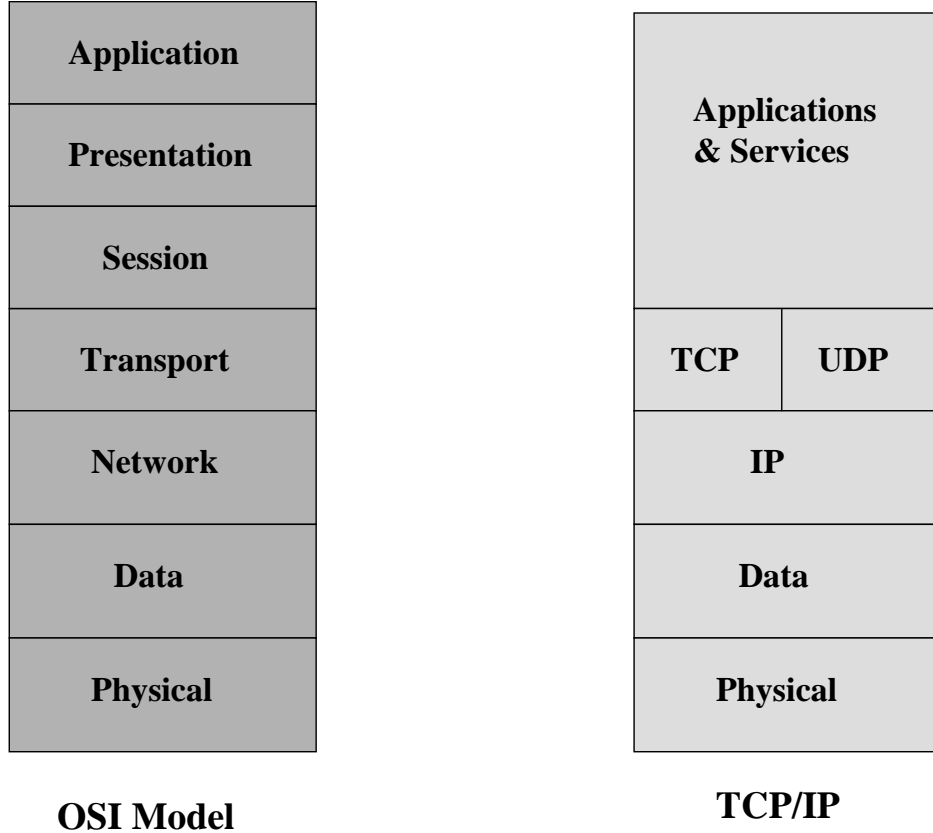


## OSI Model

Figure 1

### TCP/IP Model

When one overlays the TCP/IP protocol model over the OSI model we can draw direct correlations between the two models. The TCP/IP protocol architecture is principally described as a 4 layer model. Figure 2 is an illustration of the TCP/IP model as compared to the OSI model. The layers of the TCP/IP model are described below:



## Model Comparison

**Figure 2**

- Physical/Data Link layer (as it corresponds to the OSI model's Physical Layer and Data Layer) also known by laymen as the Network Interface layer manages and routes the exchange of data between the network device and the network. The data or information referred to includes header information/overhead information.
- Network layer (as it corresponds to the OSI model) also known as the Internet layer. This layer is responsible for managing the Internet Protocol (IP). The Internet Protocol provides the Internet addressing for routing. The IP is a connectionless protocol that provides datagram service. A datagram is a method of transmitting information. The datagram is broken up into sections and is transmitted in packets across the network. More information on this layer follows

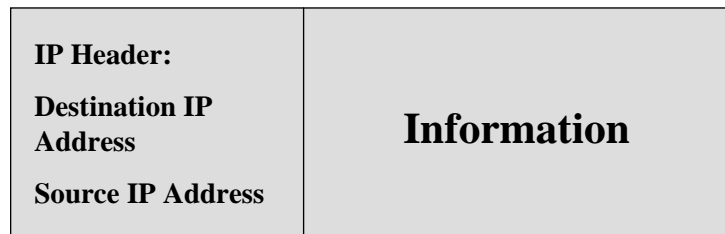
- Transport layer, which corresponds to the same Transport layer in the OSI model, transports the data. The Transmission Control Protocol (TCP) is run at the Transport layer. More information on this layer follows.
- Application layer is responsible for managing all services. This layer corresponds to the Session, presentation, and Application layers of the OSI model.

Up until recently, the bulk of the capabilities behind the power of the Internet lie in the Network and Transport Layers. However, with the advent of applications such as location-based services the Application Layer has reached the same level of importance. A location-based service would be “directed advertising”. Directed advertising is when the wireless handset communicates with the network and the handset receives relevant local advertising and sales coupons. The Application Layer will grow even further with the advent of wireless-based personal banking transactions. Therefore additional detail is provided in the following sections.

### **Network Layer**

The Network layer is also known as the Internet layer or the Internet Protocol layer. This layer supports connectionless datagram routing. Each datagram is routed along an independent path. The unfortunate thing is that the Internet Protocol does not guarantee delivery or even in-sequence delivery of the datagrams. A datagram typically is comprised of header information and the information packet itself. The header information is comprised of the packet’s destination address and its source address.

In general the problem with packet switching is that there is no way of guaranteeing the arrival of all the datagrams. Furthermore, packet switching does not even guarantee the information that is delivered can even be assembled in the correct order. The Internet Protocol is a packet switching protocol. Figure 3 is an illustration of a datagram.



## **IP Datagram**

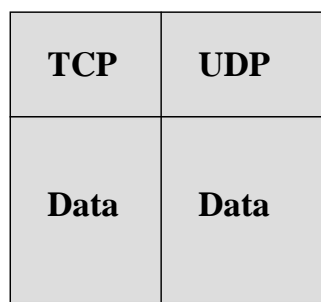
**Figure 3**

### **Transport Layer**

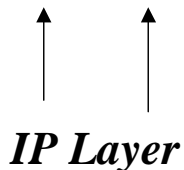
The Transport layer in the TCP/IP suite is comprised of two protocols; the TCP and the UDP. TCP stands for Transmission Control Protocol. UDP stands for User Datagram Protocol.

The TCP (Transmission Control Protocol) performs the transport layer functions of the Internet Protocol. The TCP is designed to provide for data connection services to support applications. The TCP contains parameters to ensure reliable and error free delivery of datagrams. The TCP also ensures that the datagrams are delivered without missing packets and in sequence. Let us say that an application sends a file to the TCP. The TCP adds a header to the datagram. The datagram is now called a segment. The TCP will receive incoming data from the IP layer then it will determine which application is suppose to receive the segment.

The UDP (User Datagram Protocol) is a connectionless function that is normally used by database lookup applications. The UDP supports stand alone messages like a simple query. Figure 4 is a depiction of the Transport layer.



*The IP layer will transit data to the appropriate Transport layer sub-layer.*



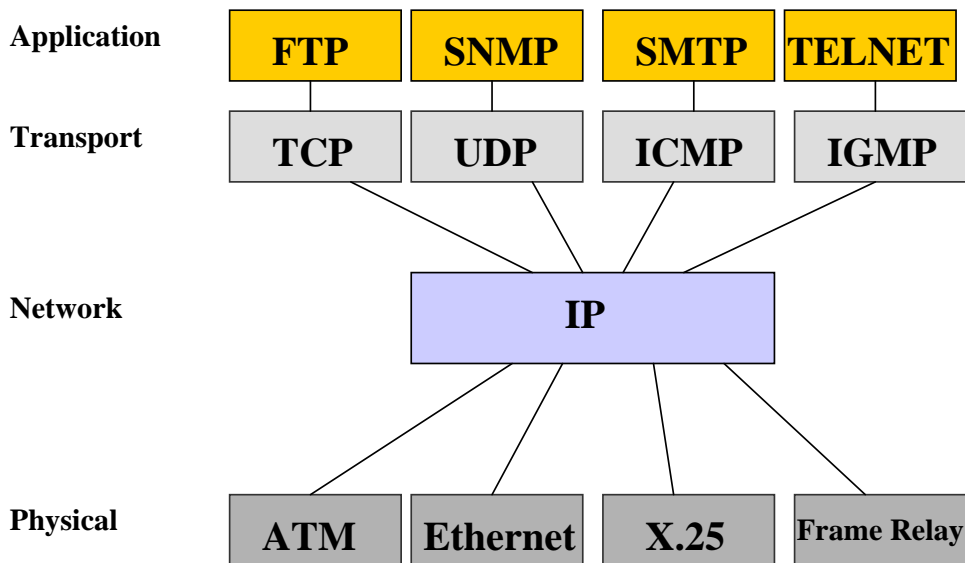
**Figure 4: Transport Layer**

**Application Layer**

The Application Layer is typically ignored. This layer rides on top of the Network and Transport Layers and is typically considered a fairly non-intelligent and non-robust layer. This type of view is not unfair. Until recently the only real applications were email, web shopping, and research (information gathering). However, the Application Layer is the layer that generates the revenue and the interest from the investment community.

I predict that in the next year applications such as wireless banking transactions and wireless gaming will become major drivers for new investment in the Internet. Voice over IP will ensure long-term mass-market acceptance but it will not be the only driver for wide-scale acceptance of the Internet.

I have noted over the years that I believe that Internet acceptance is based on layers of opportunities that appeal to millions of people. Each opportunity enables the Internet industry to build a critical mass of consumers who eventually will use the Internet to communicate and transact business for nearly every aspect of their lives. It is this critical mass of people with diverse interests that will cause the Internet to become a mass-market utility just the way the old wireline telephone had become and once was. Figure 5 illustrates the Application Layer.



**Figure 5: Application Layer**

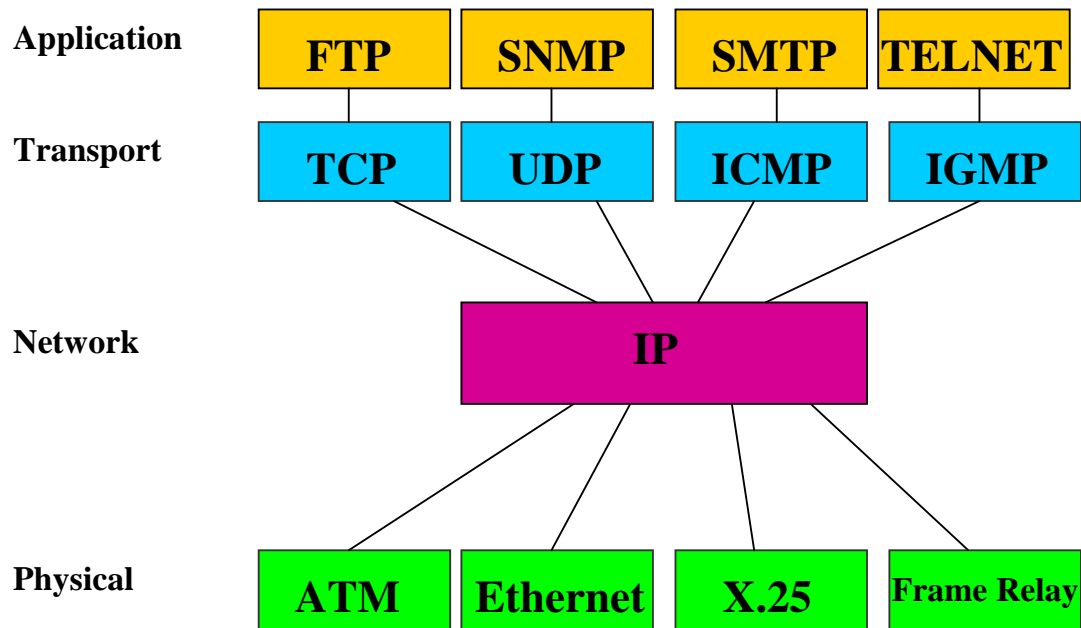
## **TCP/IP Protocol Architecture**

The TCP/IP protocol suite is comprised of a number of protocols that supports a variety of functions such as applications and network management. The following is a list of dominant and popular members of the TCP/IP protocol suite.

- FTP – FTP is the abbreviation for File Transfer Protocol. FTP supports the transfer of files between computers that remote from each other.
- SMTP – SMTP stands for Simple Message Transfer Protocol. SMTP supports electronic mail transmission and reception.
- SNMP – SNMP (Simple Network Management Protocol) supports network management.
- TCP – TCP is the Transmission Control Protocol
- UDP – The UDP (User Datagram Protocol) is normally bundled with the IP. UDP supports connectionless transmission.
- ICMP – The ICMP (Internet Control Message Protocol) supports diagnostic functions.

- IGMP – The IGMP (Internet Group Management Protocol) supports group management on a router.
- Routing Information Protocol (RIP) is a popular routing protocol in use today.

The above protocols are all part of the TCP/IP protocol suite. The following diagram highlights how these protocols are layered together in a way that allows them to complement one another. See Figure 5.



**Figure 5: The TCP/IP Protocol: Layered with Multiple Protocols**

The TCP/IP protocol suite was designed to interconnect dissimilar network elements and networks together. In other words, one could be looking at a series of local area networks (LANs) or wide area networks (WANs) interconnected together. To the wireline or wireless telecommunications engineer it would look a like a jumble of networks hobbled together. The fact is that TCP/IP enabled the interconnection of private networks, which ultimately led to the Internet. Early in the life of the TCP/IP protocol suite, these private networks had been stand-alone networks that performed a variety of different tasks; ranging from academic to business functions. The beauty of TCP/IP was its ability to enable this jumble of networks to speak to one another. The physical translation of the protocol architecture is the series of hosts and routers used to

bring the Internet to life. The router, like the tandem in the voice telecommunications world, is the central piece of switching equipment in enabling the interconnection of these dissimilar networks.

## **Philosophical Differences between the Internet and Non-Internet Worlds**

The Internet once stressed flexibility not reliability. However, with the advent of VoIP that has changed. In a traditional telecommunications environment, which encompasses the wireline and wireless carriers, the stress is on reliability and that is because of the demands and expectations of the customer. Voice is a real-time service.

Reliability is a subjective measure of dependability. Reliability is one of those soft touchy feely word that mean different things to different people. : Reliability is very different than either Availability or MTBF. Reliability is a measure of performance or dependability while the system is operational. Reliability is a subjective measure that takes into account Availability, MTBF, and consistent quality of product. Reliability is a subjective measurement because how much weight one places over one measurement over another is dependent on the person.

Due to the stress on reliability, the wireline and wireless carriers maintain an exhaustive set of operating and technical requirements, which govern what can be interconnected into their networks. During the early 1990s, a large wireline carrier suffered a massive network failure affecting multiple states and resulting in a loss of service for several hours. In the traditional telecommunications environment, if a piece of equipment does not meet specific operating and technical standards then that piece of equipment will be prohibited from use in the network. The traditional telecommunications environment relies heavily on NEBS. NEBS, which is the acronym for Network Equipment Building Systems, is managed by Telcordia, formerly Bellcore.

The Internet, however, stresses flexibility, therefore, the need for stringent standards does not exist. The Internet players' concentration on flexibility has allowed multiple equipment vendors to manufacturer a variety of computers, host, routers, storage devices, laptop computers, software utilities, network management tools, etc., without having to account for national standards of performance. If an Internet company's product does not satisfy the marketplace it usually goes out of business.

When one looks at how the Internet is configured with multiple network types and multiple configurations, it is difficult not to be amazed at the Internet's ability to adapt.

The Internet Protocol was designed to be a "best effort" protocol. The focus on the moving of data in the Internet world is on flexibility in interconnection

not the reliability of the data at the destination point. In other words, the only thing that the Internet will guarantee is that a “best effort” will be made to ensure the data arrives intact. Many “Internet bred” telecommunications pundits bask in the Internet’s ability to enable the communication of so many different devices quickly. However, these same industry pundits discount the voice telecommunications experts need to ensure data integrity (bit error rates on the order of 1 in every billion) as overkill. In the world of banking, making claims of anything less than 1 bit error in every billion bits is suicidal. Many of the current Internet players are the early pioneers so the view of the world is technology focused, however, one should remember the focus is on the customer not the technology. In the world of service provisioning consistent and uninterrupted service is a sign of excellent service.

As I see it voice is considered to be a basic necessity, which I have expounded for many years. The mass market is where “Wall Street” wants to see a product make its mark, investors only care about making money in the shortest amount of time possible, the average user wants to use as few devices as possible, and the average user still thinks voice is all important.

## **Customer Demands of Voice Today versus National Security**

The original intent of the Internet (inter-network), as defined by the Department of Defense, had been to support telecommunications needs of the government and the military. The original concept of the Internet was made sense especially during the Cold War. From a national security perspective the Internet still makes sense. One cannot depend solely on the wireline and wireless carriers for telecommunications needs.

Alternative arrangements are simply prudent steps to take. Conceptually, the Internet has not changed its requirements or capabilities. The Internet is capable of supporting:

- A multitude of computers, hosts, routers, and other devices, made by multiple vendors.
- Support network growth without regard to end-to-end planning.
- Support network growth without affecting the (public) Internet.
- Support the implementation and deployment of all types of subscriber based applications without affecting the various network interconnected to the Internet.
- Support operational flexibility. Maintain operation regardless of the network health/status of any interconnected networks.

- Support backward and forward compatibility. This means more than just simple network growth. The ability to maintain communications between network types regardless of the software or hardware versions in place is an enormous benefit to the users of the Internet.
- Adaptive/Dynamic Routing – This is an important capability during these times of national security.

## **Adaptive/Dynamic Routing**

Adaptive/dynamic routing refers to the Internet Protocol's ability to determine the best path of transmission in real time. In other words as the datagrams are traversing the network in a multitude of paths, every network router is making a decision (in real time) as to the next best intermediate destination of the datagram. This means that any physical change in any one of the many intermediate networks would not have any affect on the datagram. In other words a change in any one of the networks would simply have the affect of causing the datagram to take a different route. This capability to real time adapt routes is a fantastic capability that serves to increase the flexibility and usefulness of IP.

## **Quality of Service**

Quality of service (QoS) is a perception. In the case of the telecommunications industry, which the Internet is a part of, perception means customer perception. QoS is subjective. However, QoS can be measured using qualitative tools. From a customer perspective, QoS involves the following subjective needs:

- Does the service meet the customer's needs?
- Is the service easy to use?

QoS can be defined as the standard of measurement used to determine whether or not the service provider is providing the service in a manner that meets the expectations of the customer. Despite the subjective nature of QoS, there are objective ways of establishing QoS levels. QoS is typically measured from the network standpoint. Measuring QoS from network perspective is far easier than attempting too guarantee performance from a terminal device. Terminal devices are not normally provided by a service provider and therefore

the service provider should not be held to a standard of performance that involves terminal performance. QoS is an objective and subjective measurement focused on the customer yet based in the network. QoS parameters can be divided into the following categories:

- Availability
- Mean Time Between Failure (MTBF)
- Reliability
- Delay – both perceived and measured
- Security
- Bandwidth
- Information Loss – bit error rate; video and audio

The aforementioned parameters measure specific things or levels of performance. Individually, the parameters mean nothing to a customer. However, when one views the parameters in total the result is some overall perceived level of performance. QoS affects all players in the Internet business; ASPs, content providers, e-commerce and m-commerce providers, etc. The reality is that users of e-commerce sites and m-commerce sites expect availability of a site 24 hours a day, 365 days per year. The following is an explanation of what the parameters mean.

### **Availability**

Availability is the amount of time a system (computer, network, etc.) is available for processing transactions. The way to measure availability is by taking the ratio of the total time a system is capable of being used during a given time period (the industry norm is one year). Therefore availability of a website or some system providing an application would be measured as some number of hours over the total number of hours in a year. The result is typically presented as a percentage. The normal objective of all system operators is 99.9999% availability. An availability of 99.9999% means that the system is only unavailable for 31.536 seconds per year. Most telecommunications companies can reasonably expect an availability of 99.97%, which translates into a yearly unavailability of 2.628 hours.

### **Mean Time between Failure (MTBF)**

Mean Time between Failure (MTBF) is the average time a manufacturer estimates a failure will occur in a piece of equipment. Individual components of a system have MTBFs that are different than other system components. There are

overall system MTBFs. These system MTBFs need to be qualified as total system outage. The time period given for a MTBF should be on the order of several months or years.

The MTBF will impact system overall system maintenance costs, which eventually impacts cost of service to the customers and then finally profit margins.

## **Reliability**

Reliability is very different than either Availability or MTBF. Reliability is a measure of performance or dependability while the system is operational. Reliability is a subjective measure that takes into account Availability, MTBF, and consistent quality of product. Reliability is a subjective measurement because how much weight one places over one measurement over another is dependent on the person.

## **Transaction Delay**

If a customer perceives that a particular web transaction or even making a telephone call takes too long to complete, then the company must determine what that perceived human limit is. Human factors engineering has always been a component of telecommunications network design. The human ear/customer perceives a delay within a range of 250 milliseconds to 500 milliseconds. After the user has entered the last digit, a telephone call may take as long as 3 full seconds to complete (the calling party hears ringing). However, a user that hears a delay in receiving dial tone longer than 500 milliseconds will perceive a problem with telephone service. A user is double clicking on icons to enter a website and it takes nearly a minute to actually see the next web page. However, in this case because the user has either experienced delays this long or even longer, the user does not perceive there is a problem. The delays I have described are perception based but are indeed valid transaction delays that customers encounter.

There are measured network delays that can affect the quality of service. These delays are in information transmission and packet data assemblage. These kinds of delays are information delay variations. Packet data is not an ideal way of supporting real time applications like voice conversations or video streaming. The delay variations must have defined limits set for each application so that there is no perceived degradation in quality of service. The delay variation limit may be 50 milliseconds. This would mean that the application being supported must have all of the data transported across the network within a 50 millisecond window. This window would require that the beginning of a web page and the end of a web page reach the destination all within a 50 millisecond time period. The fact is that there is no industry standard governing the way in which web pages are presented.

The initial transmission of voice over a packet network requires a sufficient number of voice samples be collected before the voice package is placed inside a data packet and then launched. The Internet Protocol (IP) data packet will place about 20 voice samples inside a packet. Voice is sampled at a rate of one every 1/8000 seconds; voice is sampled at this rate in a digital wireline network. The math is very simple. A normal packet is approximately 600 bytes in length. A voice sample is generated at a rate of one every 125 microseconds. A packet delay would therefore equate to 125 microseconds X 600 bytes = 75,000 microseconds. In reality the IP packet can vary in length, up to 64,000 bytes. When you look at the way packets are routed one will recall that the packets are typically buffered at the destination end until sufficient number of packets are assembled for final presentation. In other words the delays can add up.

The problem with the Internet is that most have come to expect delays. This is an unfortunate circumstance for this leaves many users with the perception that the Internet just can't do it all. In reality, the industry has worked to meet the high consumer perceived standards of excellence by overcoming technical barriers and setting high operating standards. Transaction delays and latency in general may be tolerated for web surfing but they are not tolerated or considered acceptable for plain old voice services.

Transaction delays can be due to limited bandwidth transmission facilities or inefficient and poorly designed websites.

The potential for latency in VoIP packets can be mitigated via network interconnection agreements. The reality is that carriers interconnect their networks to specific carriers. The limited number of points of network interconnect means the carrier will likely use one carrier for TDM-based long distance and one carrier for packet data. With a limited number of paths to follow, latency becomes less of an issue.

## **Security**

No telecommunications network is totally secure from fraud, computer viruses, and privacy threats. There use to be an axiom that the wireline network lived by: "The telephone network is inherently secure". This old saying was touted before the days of the computer virus but even then it was not true. Wire tapping and telephone bugging has been around for decades. The "bad guys" might not have been able to listen in on a phone conversation by tapping into a line while atop a telephone pole but the "good guys" could tap into your phone lines from the switching center. Therefore, from a certain perspective the telephone is inherently secure.

The information networks today are using a variety of methods to secure the network. These methods entail:

- Anti-viral software
- Passwords
- Encrypted transactions
- Network validation procedures
- User identification authentication procedures
- Fire Walls

Security as a QoS parameter is an important one that is constantly being threatened by the hackers and criminals of the world. It is an unfortunate state of affairs that over a thousand new computer viruses are being discovered month. These viruses threaten the personal security of the user as well as the security of the nation. A website that is not secure form unauthorized access invites trouble.

Security is even a bigger threat now to the Internet than it was a few years ago. The proliferation of ASPs has created a series of new opportunities for the hacker and criminal to wreak havoc on the network. Today, ASPs have to pass a variety of requirements before an ISP will even consider connecting their network to the ASPs database.

E-commerce and m-commerce sites interact with users gathering data such as credit card information, home addresses, and home telephone numbers. All information that today when entered into most commerce sites is preceded with the statement: "You are entering a website that this provider cannot guarantee is secure from privacy threats". There would be more users if the e-commerce and m-commerce sites had a way of ensuring end-to-end security.

## **Bandwidth**

The more bandwidth available for transmission the faster the download and upload speeds for data. The biggest complaint from Internet users is "slow speed". The fact is that most ISPs have access to homes over twisted pair local loop telephone wire, which can only reliably support transmission speeds of up to 57,600 bits per second.

The lack of bandwidth has affected users' perception of a large number of websites that support video and audio applications. As a result of the lack of bandwidth, users' cannot or will not bother accessing websites that provide high quality video and audio content. The larger the bandwidth, the greater the volume of data, that can be transmitted per second. Voice and video require network access that supports real time applications. Network access refers to the modem, the local network and the long distance network. The application will be limited by the lowest bandwidth device used in the network.

## **Information Loss**

Information loss is defined as missing bits within an information stream. This could be a large multi-mega bit size file that is missing some information due to noise over the transmission facility, some flaw at a network node, or even a node failure. Packet networks could suffer a network node yet not lose all of the data because most of the data would be transiting the network via a different path. The network has no way of knowing it contributed to a loss of information. The destination end would have to request the information file be re-sent.

Information loss parameters could be set where a transmission node or facility would have an operating standard to comply with. The banking industry uses a standard of  $1 \times 10^{-9}$  bit error rate, which means that for every 1,000,000,000 bits of data one can lose 1bit of data. There should always be a standard of operations quality for a network element or facility.

The impact of data loss will vary from file to file and application to application. In a perfect world one would desire not to lose any data, however, this is not a perfect world and therefore one will lose data despite operations standards. Transmitting the lost data would be possible in a text file. Some applications can recover from data loss and a re-transmission request would enable a user to recover lost data. These applications could be a video or audio application. The application itself cannot recover if the missing bits were sent; however, a re-transmission request would enable the application to be re-sent in its entirety.

The potential for information loss increases with the number of parties now involved with the provisioning of an Internet based service. Imagine the loss of information due to multiple network elements embedded within multiple Internet companies.

## **VoIP Market**

The VoIP market is poised for explosive growth. The number of terminal devices that can handle a VoIP call have increased dramatically in number and have come down in price. VoIP is in reach of the average consumer. However, the average consumer needs an incentive to want to switch from circuit-switched voice to VoIP. In order to gain wide scale acceptance in the business community, the business community needs to find a way of finding more value out of an IP network.

The solution is probably one that requires bundling of services. Service bundling is an old concept. Bundling is a very simple concept; people want as much for their money as possible. Consumers and businesses want many layers of value for the money they spend on telecom services. Bundling in the case of IP means bundled voice, data, and video.

Since the days of ISDN (Integrated Services Digital Network) circa 1976, the telecom industry has been seeking to combine voice, data, and video on a single set of transmission wires to a single terminal. Of course in 1976 no one had heard of the Internet but there was a vision of a network that would enable people to transact business of some kind using a network.

The term “killer app” is overused. What is good for one person is not good for another. The service that creates enough interest in a mass number of people usually ends up being crowned the “killer app”. For years pundits called email the killer app. For a period of time it was the “killer app”, but email soon became a “free-bee” or a “flat fee service”. Voice will be the next “killer app but it will be one that is bundled with others. Today, there are providers of voice. VoIP is not going to sell unless there is a financial imperative and personal benefit to the consumer. In today’s economic environment this situation will call for bundling. People want as much for their money as possible. The mass-market consumer is always looking for a deal.

The technology and critical mass of consumer/user devices have grown and evolved to the point at which bundled VoIP, video, and Internet is not only possible but also cost effective. The recent economic collapse and slow recovery of the telecom industry is forcing the industry and Wall Street moneymakers to put product out into the marketplace at reasonable costs. The first bundled voice services will most likely be sold as audio and video conference services.

However, despite the onset of VoIP, there will be operational support system challenges and marketing challenges. These challenges are being addressed by the industry today.

## About The Author



**P.J. Louis**

P.J. Louis is a 25-year veteran of the telecommunications industry. He had been chief of technical staff for Network Engineering in the old New York Telephone Company (formerly NYNEX and now known as Verizon Communications),

managing senior engineer in Bell Communications Research (Bellcore), Director for Technology in NextWave Wireless, Vice President of Product Management and Marketing for TruePosition, and most recently a Managing Director in FTI Financial Consulting's and PricewaterhouseCoopers' corporate restructuring divisions. He is a former wireless standards chairperson for the Telecommunications Industry Association (TIA). While in standards, P.J. had participated in the development of IS-41 Revisions A, B, and C, the early incarnations of wireless intelligent networking, PCS standards, and early definitions of 3G. While in NYNEX he had been involved in the planning and deployment of the first digital switches, ISDN, Frame Relay, and SS7. He had been Bellcore's subject-matter-expert for wireless/wireline network interconnection and signaling. His knowledge and experience in switching and signaling begins with the Step-By-Step (SxS) switch and continues into the softswitch era.

P.J. has served on the editorial advisory board of Cellular Integration. He is a contributor to Cellular Networking Perspectives. He holds a BSEE from Columbia University and a MS in Management from Polytechnic University of NY. He is a senior member of the IEEE and a former officer of the IEEE's Communications Society – NY Section. He holds membership in the Association of Old Crows and the Radio Club of America.

P.J. has authored four books for McGraw-Hill Publishing; "Telecommunications Internetworking", "M-Commerce Crash Course", "Broadband Crash Course", and "Telecom Management Crash Course". P.J. has recently completed a new book for Mind Commerce; entitled "Telecom and IT Financial Handbook".

P.J. is currently engaged in the development of new business opportunities in the United States and overseas. He is a partner in Beacon Communications, LLC (a regulatory consulting firm) and a partner in TEX Management, LLC (a telecommunications executive management firm).

The author may be reached at [PJLouis@MindCommerce.com](mailto:PJLouis@MindCommerce.com)

## **VoIP Research, Training and Consulting**

For VoIP research, training and consulting, see Mind Commerce ([www.MindCommerce.com](http://www.MindCommerce.com)) or contact us at [VoIP@MindCommerce.com](mailto:VoIP@MindCommerce.com).



Research Consulting Training Technical Writing

[www.MindCommerce.com](http://www.MindCommerce.com)

**Mind Commerce®**

## **Custom Research Services**

Do you have a need for special research into a particular area but don't have the time and/or resources for specific project?

Mind Commerce offers independent and customized research as well as [Consulting and Training Services](#). We will research, evaluate, and report findings and recommendations based on your unique requirements for various projects such as:

- Market Research
- Competitive Analysis
- Technical Assessment

Mind Commerce also offers various [Writing Services](#) including technical and/or marketing white paper development

## **Research Services on Request**

For special research requests  
email us at [Research@MindCommerce.com](mailto:Research@MindCommerce.com)

Mind Commerce also accepts Request for Proposal (RFP) for special assignment

[RFP@MindCommerce.com](mailto:RFP@MindCommerce.com)

## **Special Corporate/Agency Discounts**

Your company may be eligible for a discount

When ordering *Mind Commerce Research Services*

Mind Commerce will accept corporate Purchase Orders (PO)

Contact us to inquire about our [special corporate discounts](#)