S-5 (SLO-1) Public Switched Telephone Network

The Public Switched Telephone Network is understood as an aggregate of world's circuit switched telephone networks, used for providing public telecommunication. The PSTN networks are called POTS (Plain Old Telephone Systems). These networks are operated regionally, locally, nationally and inter-nationally using telephone lines, fiber optic cables, microwave transmission links or cellular communications.

PSTN consists of switches at centralized points on the network, which act as nodes for communication between any point and any other point on the network. All the types of Switching techniques discussed previously, such as circuit switching, packet switching and message switching are different modes of using PSTN.

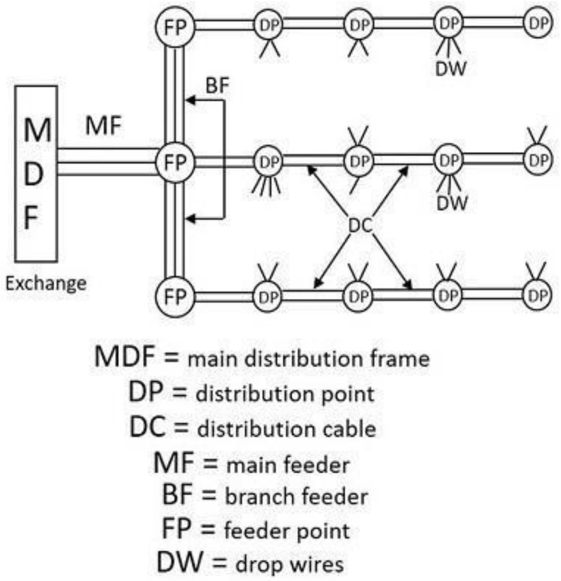
Properties of PSTN

- It is also known as Plain Old Telephone Service (POTS)
- It has evolved from the invention of telephone by Alexander Graham Bell.
- The individual networks can be owned by national government, regional government or private telephone operators.
- Its main objective is to transmit human voice in a recognizable form.
- It is an aggregation of circuit-switched networks of the world.
- Originally, it was an entirely analog network laid with copper cables and switches.
- Presently, most part of PSTN networks is digitized and comprises of a wide variety communicating devices.
- The present PSTNs comprises of copper telephone lines, fibre optic cables, communication satellites, microwave transmission links and undersea telephone lines. It is also linked to the cellular networks.
- The interconnection between the different parts of the telephone system is done by switching centres. This allows multiple telephone and cellular networks to communicate with each other.
- Present telephone systems are tightly coupled with WANs (wide area networks) and are used for both data and voice communications.
- The operation of PSTN networks follows the ITU-T standards

Subscriber Loop Systems

In a general telephone network, every subscriber has two dedicated lines connecting to the nearest switching exchange, which are called the Loop lines of that subscriber. The laying of lines to the subscriber premises from the exchange office is called Cabling. As it is difficult to run cables from each subscriber's premises to the exchange, large cables are used through which the drop wires (subscriber lines) are taken to a distribution point.

The drop wires are connected to wire pairs at the distribution point, in the cables. Such distribution cables from nearby geographical area are connected at a same feeder point where they connected to branch feeder cables which in turn, are connected to the main feeder cable. This whole process can be understood with the help of the following figure.



The subscriber cable pairs from the exchange will also terminate at MDF through main feeder cables that carry large number of wire pairs. These subscriber pairs and exchange pairs are interconnected at the MDF using jumpers, which makes MDF to provide flexible mechanism for reallocating cable pairs and subscriber numbers. This means a subscriber who shifts to a different location though in the same exchange area, can be allowed to use the same number using appropriate jumper, while his old drop wires can be used by another subscriber with a new number.

Switching Hierarchy and Routing

The next important system in this is the switching hierarchy and routing of the telephone lines. The interconnectivity of calls between different areas having different exchanges is done with the help of **trunk lines** between the exchanges. The group of trunk lines that are used to interconnect different exchanges are called the **Trunk Groups.**

In the process of interconnecting exchanges, there are three basic topologies, such as

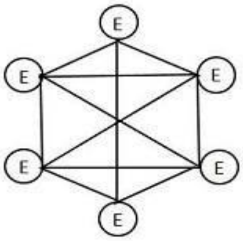
- Mesh Topology
- Star Topology

- Hierarchical

Mesh Topology

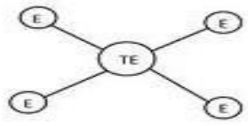
Mesh topology, as the name implies, is a fully connected network. The number of trunk groups in a mesh network is proportional to the square of the exchanges being interconnected. Hence, these mesh topologies are widely used in metropolitan areas where there is heavy traffic

The following figure shows how a mesh topology looks like.

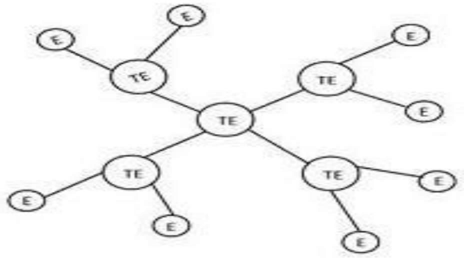


Star Topology

Star topology is connected in the shape of a star, which utilizes an intermediate exchange called a **tandem exchange** through which all other exchanges communicate. The figure given below shows the model of a star network. The star network is used when traffic levels are comparatively low. Many star networks can be used by interconnecting through additional tandem exchange, leading to a two-level star network as shown in the following figure.



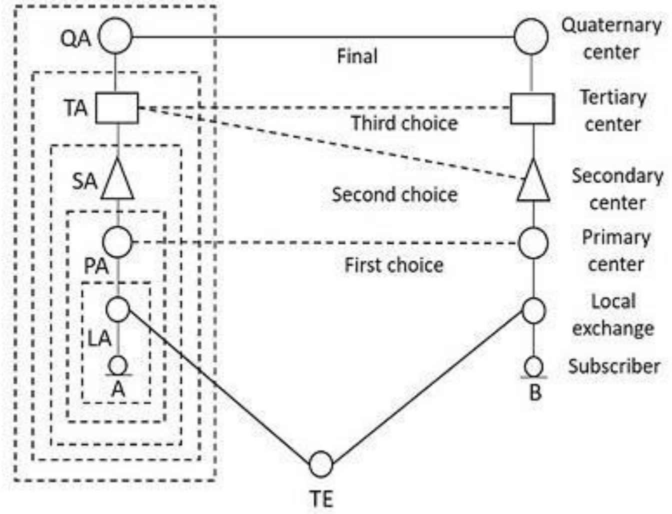
Star Topology



Two-level Star

Hierarchical

The hierarchical topology is used to handle heavy traffic with minimal number of trunk groups. The traffic flows through the **Final route** which is the highest level of hierarchy. If the traffic intensity between any pair of exchanges is high, direct trunk routes may be established between them as indicated by dashed lines in the figure given below. These direct trunk routes are **High Usage routes**. Wherever these high usage routes exist, the traffic flows through them. Here, the overflown traffic is routed along the hierarchical path. No overflow traffic is permitted from the final route.



To decide the routing on a particular connection, the following three methods are used –

- Right-through routing
- Own-exchange routing
- Computer-controlled routing

How Do PSTN Phone Lines Work?

Think of a Public Switched Telephone Network (PSTN) as a combination of telephone networks used worldwide, including telephone lines, fiber optic cables, switching centers, cellular networks, as well as satellites and cable systems. These help telephones communicate with each other.

Put simply, when you dial a phone number your call moves through the network to reach its destination – and two phones get connected. To fully understand how a **pots** actually works, consider what happens when you dial a number from your own phone.

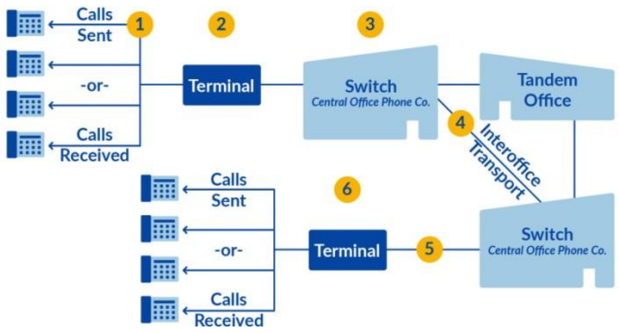
- ***Step #1 –*** Your telephone set converts sound waves into electrical signals. These signals are then transmitted to a terminal via a cable.
- ***Step #2 –*** The terminal collects the electrical signals and transmits these to

the central office (CO).

- ***Step #3 –*** The central office routes the calls in the form of electrical signals through fiber optic cable. The fiber optic conduit then carries these signals in the form of light pulses to their final destination.
- ***Step #4 –*** Your call is routed to a tandem office (a regional hub responsible for transmitting calls to distant central offices) or a central office (for local calls).
- ***Step #5 –*** When your call reaches the right office, the signal is converted back to an electrical signal and is then routed to a terminal.
- ***Step #6 –*** The terminal routes the call to the appropriate telephone number. Upon receiving the call, the telephone set converts the electrical signals back to sound waves.

This may sound complicated, but the thing to remember is that it takes a few seconds for your call to reach its destination. This process is facilitated by using fiber optic cables and a global network of switching centers.

Plain Old Telephone Service (POTS) Networking



PSTN – Understanding The Art of Switching

You could say that PSTNs are all about switching, which forms the backbone of traditional phone networks. When a call is made, switches create a wire circuit between two telephones, with this particular connection lasting as long as the duration of the call.

Now, let's have a look at each of the four types of switching which take place at different levels.

1. The Local Exchange

- A local exchange – which may consist of one or more exchanges – hooks up subscribers to a PSTN line. Also known as a central office or a switching exchange, a telephone exchange may have as many as 10,000 lines.
- All telephones are connected to the local exchange in a specific area. Interestingly, if you were to dial the number of your supplier located in the building next to yours, the call won't leave your local exchange and will be routed to the supplier as soon as it reaches the exchange.
- The exchange then identifies the number dialed so it can route the call

towards the correct end destination. This process works as follows:

- The first three digits of a phone number represent the exchange (the local switch), while the last four digits identify the individual subscriber within that exchange.
- This means that when you dial a number and it reaches your local exchange, your call is immediately linked to the subscriber without the need for any further routing.

2. The Tandem Office

Also known as a junction network, a tandem office serves a large geographical area comprising several local exchanges while managing switches between local exchanges.

Communication andTechnology

What are some examples of communication technology?
Imagine you are standing in the hallway at school talking to your friends. Are you using communication? Yes. Communication is sending, receiving, and responding to messages. Are you using communication **technology**? No. When you are talking face-to- face, you are not using communication technology.

However, if you communicate by using a written note, Instant Messaging (IM), or a cell phone, then you are using communication technology. **Communication technology** is the transfer of messages (information) among people and/or machines through the use of technology. This processing of information can help people make decisions, solve problems, and control machines.

The knowledge, skills, and tools that were the foundation of past and current communication technology are also the founda- tion for new technologies and improved ones.

The Systems Model

- ***How does communication fit the systems model?***

As you know, systems can be charted breaks systems into input, process, output, and feedback. This is the systems model.

Communication systems include all the inputs, processes, out- puts, and feedback associated with sending and receiving mes- sages (information). The message is the input. How the message is moved is the process. The reception of the message at the other end is the output. Feedback may relate to static or clarity

The Plain Old Telephone Service has many robust features, but when it comes to businesses, POTS tends not to be a good fit because choosing this option costs a lot in the long-run (and let's not forget that these services run on an old technology).

After all, the switching technology itself hasn't changed much since the last century. This is a potential drawback of PSTN phone networks as they don't allow you to transmit other data types.

What's more, this downside has led to a new and modern telephone service known as VoIP, which is proving to be nothing less than a game-changer in the telephone industry.

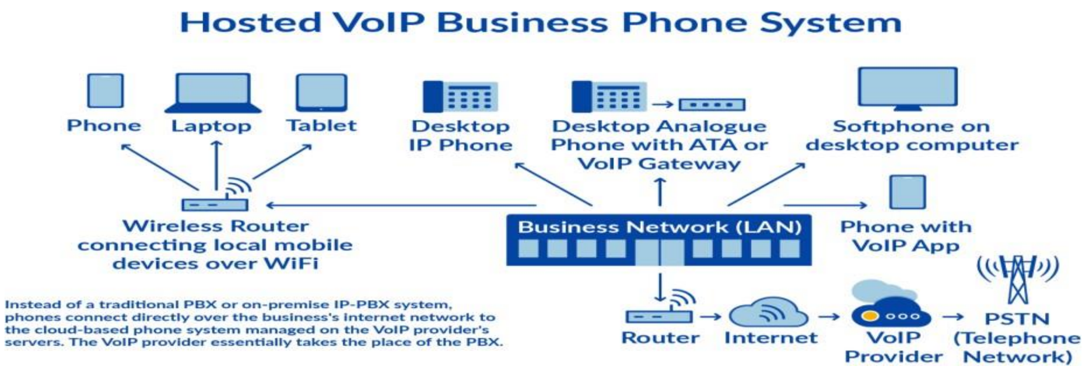
The Voice Over Internet Protocol (VoIP) is considered to be the best-known alternative to the PSTN system as it isn't just cost-effective but also has several other benefits that businesses (and consumers) love.

VoIP is the transmission of voice and other data over the internet protocol network. Your VoIP telephone set is connected to a DSL or a cable modem connecting you to the Internet

VoIP is and how it is different from PSTN.

What is VoIP?

Voice over IP (VoIP) is also known as IP telephony, broadband telephony, or internet telephony—but it means the same thing: your voice transmitted through the internet. The voice signal is converted into a digital signal and it then travels over the internet and reaches the destination



Hosted VoIP Business Phone System

Phone
Laptop
Tablet
Desktop IP Phone
Desktop Analogue Phone with ATA or VoIP Gateway
Softphone on desktop computer
Wireless Router connecting local mobile devices over WiFi
Business Network (LAN)
Phone with VoIP App
Router
Internet
VoIP Provider
PSTN (Telephone Network)

Instead of a traditional PBX or on-premise IP-PBX system, phones connect directly over the business's internet network to the cloud-based phone system managed on the VoIP provider's servers. The VoIP provider essentially takes the place of the PBX.

Unlike PSTN, VoIP uses the internet where you don't have to rely on a cable wire. There is no need for any exchange if you're making a VoIP to VoIP call. However, if you dial a PSTN number from your VoIP, your call will be transmitted through an exchange. It works for all types of calls, data transfers, and more.

So how does a VoIP phone network work, and how is it different from the traditional landlines?

The PSTN uses circuit switching (or switching) for connecting calls (as discussed above). **Business VoIP phone systems** use packet switching. This type of switching is more efficient than circuit switching because the data is sent and received as and when needed. A constant connection isn't maintained throughout the call duration.

Plus, VoIP doesn't use dedicated lines. Instead, the data packets use routers and the internet, and each data packet travels through the least congested and shortest path.

Why Do Businesses Prefer VoIP Over PSTN?

The differences discussed above provide a solid ground as to why businesses prefer VoIP, but there are other benefits that your business will derive from the shift.

Here are a few reasons why VoIP is a better option for your business on any given day.

- Cost Savings
- Better Customer Service
- Better Productivity
- Scalability

S-6 (SLO-1) Communication andTechnology

What are some examples of communication technology?

Imagine you are standing in the hallway at school talking to your friends. Are you using communication? Yes. Communication is sending, receiving, and responding to messages. Are you using communication technology? No. When you are talking face-to- face, you are not using communication technology.
However, if you communicate by using a written note, Instant Messaging (IM), or a cell phone, then you are using communication technology. Communication technology is the transfer of messages (information) among people and/or machines through the use of technology. This processing of information can help people make decisions, solve problems, and control machines. The knowledge, skills, and tools that were the foundation of past and current communication technology are also the foundation for new technologies and improved ones

The Systems Model

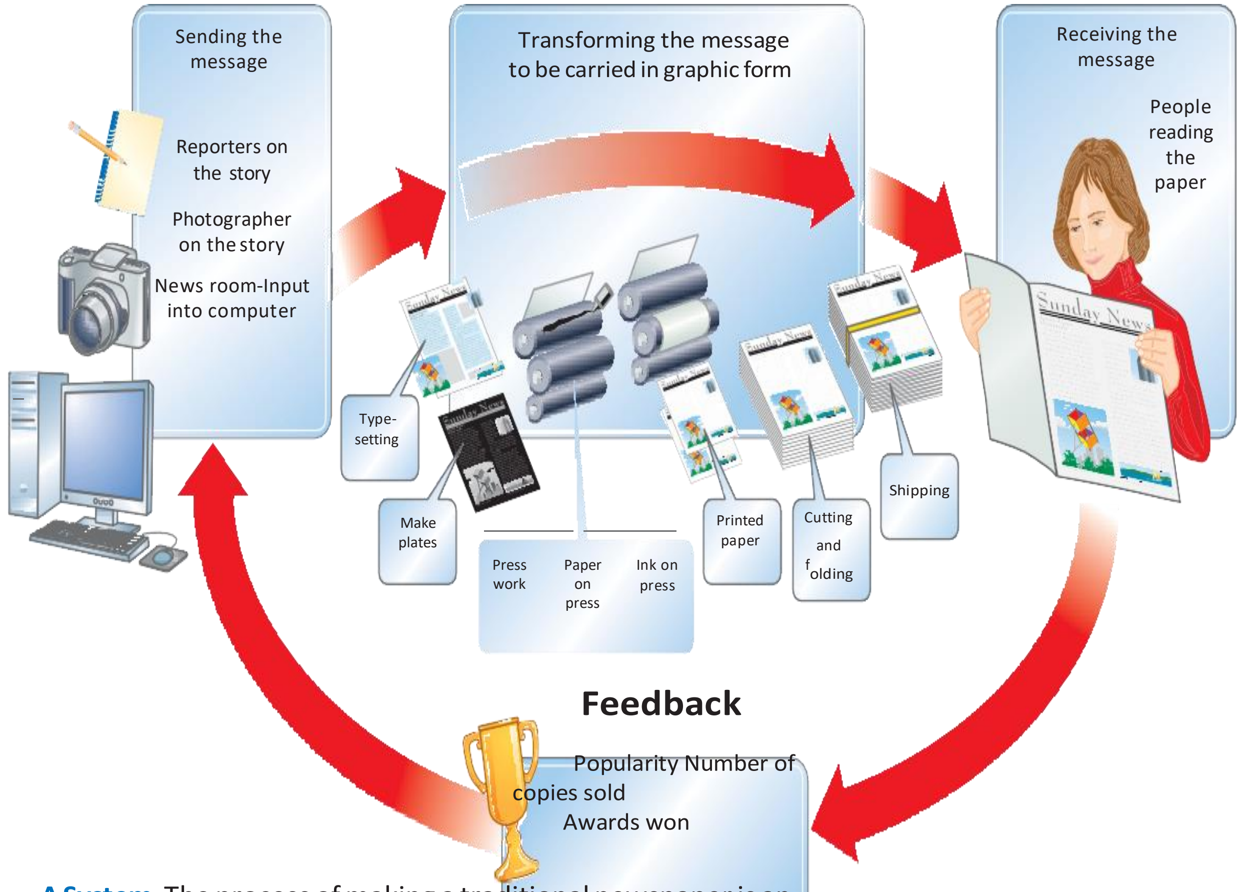
How does communication fit the systems model?

As you know, systems can be charted breaks systems into input, process, output, and feedback. This is the systems model.
Communication systems include all the inputs, processes, out- puts, and feedback associated with sending and receiving messages (information). The message is the input. How the message is moved is the process. The reception of the message at the other end is the output. Feedback may relate to static or clarity.

Real-World Systems

Suppose you write an article for the school newspaper about the computer lab. Your words, pictures, time you spend, and the computer you use are inputs. Putting the newspaper together and printing it are parts of the process. The primary output is the newspaper.

Communication System: A Newspaper Process.



A System The process of making a traditional newspaper is an example of a communication system. *Give some examples of inputs.*

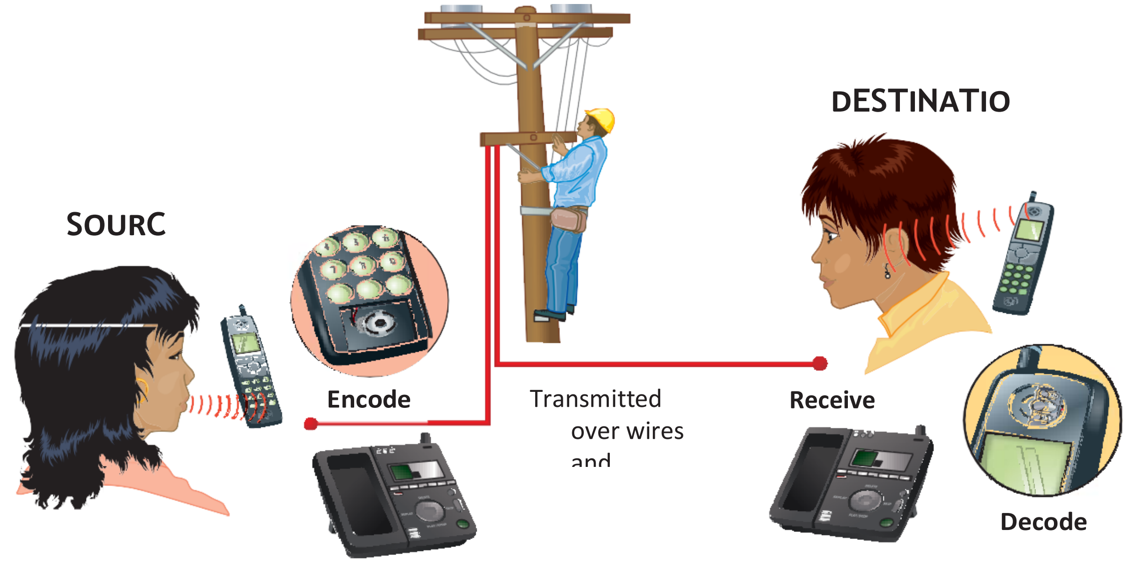
When you read a book or listen to an MP3 player, you are on the output end of the communication system, receiving the message. When you use a telephone, a computer, or a video camera, you are controlling both the input and output of the system. What parts of a system are you involved with when you play a video game, watch television, or type an e-mail or IM? Computers, iPods, and video recorders are communication systems that may contain the input, process, and output devices all in one unit.

Communication Subsystems

How would you use a decoder?

Communication systems usually include several subsystems that help transmit information. See Figure 9.2. The subsystems are made up of these elements: a source, an encoder, a transmitter, a receiver, a decoder, and a destination.
The source is the sender, which could be a person or a machine with a message to send. The encoder changes the message so that it can be transmitted. When you write a note, type on a computer keyboard, or talk into a telephone, you are encoding your mes- sage. Your message could be written on paper or be sent as an electronic signal.

The receiver of the message at the final destination could be a person or a machine. The



Systems within a System Most communication systems have several subsystems. *What are some examples of a destination?*

Message is then decoded, which means symbols on paper must be read or electronic impulses must be turned into information that a person or machine can understand.

Forms of Communication

What is one way to identify or group communication systems?

Although the different forms of communication may overlap, communication systems can be grouped by the way they carry messages. Let's look at some different ways that you can transmit a message, including biological communication, graphic commu- nication, wave communication, and telecommunication.

- Biological Communication
- Graphic Communication
- Wave Communication

Telecommunication

Communication over a distance is telecommunication. Today most telecommunication systems use electronic or optoelectronic devices. Have you ever used a telecommunication machine or device? You have if you have used a phone, television, or radio.

Satellites and Telecommunication

Satellites are also telecommunication devices. Satellites placed 22,300 miles above the earth and traveling at the same speed that Earth spins are in a "geosynchronous orbit." This means that the satellite always stays above the same part of the earth. Its lack of movement in relation to the ground could give the impression that the satellite was attached to Earth with a very long pole. When a satellite is in a geosynchronous orbit, it seems to move with the objects on the ground.

Uses of Satellites

Satellites can help produce maps, provide climate information, track weather patterns, and even observe what people are build- ing in other parts of the world. The United States has many spy satellites looking down on other countries as the satellites circle the earth. Some of these spy satellites can take detailed photos by using equipment similar to that used on the Hubble Space Telescope. It is possible for some satellites to see the details of an object that is smaller than a golf cart.

Modes ofCommunication

Evolving Modes of Communication

What progress have people made in their ability to communicate with each other?

Technology has given us new modes of communication. A mode is a way of doing something. Originally, "people-to-people" communication was the only mode. It is still the most basic mode of communication. Over time people have learned to create new and more powerful modes of communication. They gained the knowledge and skills needed to build complex communication devices and used the mode called "people-to-machines" communication. People also created graphic communication systems to transmit their messages using the printed word, which uses the mode called "machines-to-people" communication. Finally, people developed communication based on electrical signals that are sometimes used for the mode called "machines-to-machines" communication.

- People to People
- People to Machines
- Machines to People
- Machines to Machines

Impacts of Communication Technology

How has communication technology affected the world?
When people say the world is getting smaller, they mean tech- nology allows us to communicate instantly with almost anyone anywhere. Communication technology is neither good nor bad, but the use of its products and systems can have good and bad consequences. Political, social, cultural, economic, and environ- mental issues are influenced by communication technology.

- Political Impacts
- Social and Cultural Impacts
- Economic Impacts
- Environmental Impacts

S-7 (SLO-1) Standard Committees - ITU - International Telecommunication Union.

The International Telecommunication Union (ITU) is a specialized agency of the United Nations that is responsible for issues that concern information and communication technologies (ICT).

- The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world, and assists in the development and coordination of worldwide technical standards. The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.
- ITU also organizes worldwide and regional exhibitions and forums, such as ITU TELECOM WORLD, bringing together representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology.
- ITU is committed to connecting all the world's people – wherever they live and whatever their means. Through their work, they protect and support everyone's fundamental right to communicate. ITU membership reads like a Who's Who of the ICT sector, being unique among United Nations agencies in having both public and private sector membership. So in addition to the 193 Member States, ITU membership includes ICT regulators, many leading academic institutions and some 700 tech companies.
- In an increasingly interconnected world, ITU is the single global organization embracing all players in this dynamic and fast-growing sector.

The IETF mission includes:

1. Identifying and proposing solutions to pressing operational and technical problems in the Internet,

2. Specifying the development (or usage) of protocols and the near-term architecture solve such technical problems for the Internet,
3. Making recommendations to the IAB regarding standardization of protocols and protocol usage in the Internet,
4. Facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community.
5. Providing a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors, and network managers.

Steering group

The **Internet Engineering Steering Group** (**IESG**) is a body composed of the Internet Engineering Task Force (IETF) chair and area directors. It provides the final technical review of Internet standards and is responsible for day-to-day management of the IETF. It receives appeals of the decisions of the working groups, and the IESG makes the decision to progress documents in the standards track.

The chair of the IESG is the director of the General Area, who also serves as the overall IETF Chair. Members of the IESG include the two directors of each of the following areas:

- Applications Area (app)
- Internet Area (int)
- Operations & Network Management Area (ops)
- Routing Area (rtg)
- Real-time Applications and Infrastructure Area (rai)
- Security Area (sec)
- Transport and Services Area (tsv) – frequently also referred to as the "Transport Area"

Who’s Who in the International Standards World

- International Standards are needed so that products and systems developed in different parts of the world are interoperable and compatible with each other. The standards aim to ease out the technical differences and also to ensure product safety.
- The most prominent organization that lays down international standards is the ISO (International Standards Organization). Two other major organizations for technical standards are NIST (National Institute of Standards and Technology) and IEEE (Institute of Electrical and Electronics Engineers).

International Standards Organization (ISO)

ISO is an independent, voluntary, non-treaty, non-government standards organization. It issues standards of a vast number of subjects that may be proprietary, industrial or commercial in nature. Its members are national standards organizations of member countries. Some of its prominent members are BSI (British Standards Institution), ANSI (American National Standards Institute), AFNOR (Association Française de Normalisation), etc.

ISO has over 200 Technical Committees (TC), each of which defines the standards for a particular subject. Each TC has sub-committees (SC) which in turn has working groups (WG).

National Institute of Standards and Technology (NIST)

NIST is a metrology laboratory of the US Department of Commerce. It issues standards and organizes laboratory programs in the fields of nanoscience and technology, engineering, IT, material measurement, physical measurement and neutron research. It provides Standard Reference Materials to industry, academia, government and many other users. NIST publishes Handbook 44 each year.

Institute of Electrical and Electronics Engineers (IEEE)

IEEE is a professional association that aims for educational and technical advancement in the fields of electrical engineering, electronics engineering, computer engineering, telecommunications and other related disciplines. It has a standardization organization IEEE-SA (IEEE Standards Association) that develops standards in the technical fields. One of its most notable standards is the IEEE 802 group that is widely used for computer networking.

Network Standards

Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.
During data communication, a number of standards may be used simultaneously at the different layers. The commonly used standards at each layer are −

- **Application layer −** HTTP, HTML, POP, H.323, IMAP
- **Transport layer −** TCP, SPX
- **Network layer −**IP, IPX
- **Data link layer −** Ethernet IEEE 802.3, X.25, Frame Relay
- **Physical layer −**RS-232C (cable), V.92 (modem)

Types of Standards

Standards are of two types

- **De facto −** These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.
- **De jure −** These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

Standards Organizations

Some of the noted standards organizations are

- International Standards Organization (ISO)
- International Telecommunication Union (ITU)
- Institute of Electronics and Electrical Engineers (IEEE)
- American National Standards Institute (ANSI)
- Internet Research Task Force (IETF)
- Electronic Industries Association (EIA)

Communication Technologies – Introduction

Exchange of information through the use of speech, signs or symbols is called communication. When early humans started speaking, some 5,00,000 years ago, that was the first mode of communication. Before we dive into modern technologies that drive communication in contemporary world, we need to know how humans developed better communication techniques to share knowledge with each other

Some of the main functions of the ITU are :

- Allocates global use of radio spectrum
- Assigns satellite orbits through international cooperation
- Develops standards for networking technologies
- Strives to improve communications in developing and underdeveloped countries.
- Protects and supports communications and information exchange.

ITU has three main sectors

- **ITU-T:** It is the Telecommunications Standardization Sector. It defines the global as well as the local standards for Internet access, communications protocols, compression of voice and video, home networking and many other particulars of communications.
- **ITU-R:** It is the Radio-communications Sector. It coordinates the allocation and management of radio frequency spectrum and satellite orbits that aid in satellite enabled services like phone calls, television services, online maps and navigation.
- **ITU-D:** It is the Telecommunication Development Sector. It has programmes to develop ICT (Information and Communication Technologies) particularly in the developing and underdeveloped areas. It strives to bridge the "digital divide" between countries.

Membership to ITU is of two types

1) UN Members (countries and states) who join ITU as member states.
2) Private organizations who join ITU as Non-voting members. This includes –

- Telephone companies, e.g. AT&T, Vodafone
- Manufacturers of telecom equipments, e.g. Cisco, Nokia
- Vendors of computers, e.g. Microsoft, Toshiba

- Manufacturers of chips, e.g. Intel, Motorola

S-7 (SLO-2) Internet Engineering Task Force and MFA Forum

The **Internet Engineering Task Force** (**IETF**) is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP).[2] It has no formal membership roster or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors.

The IETF started out as an activity supported by the federal government of the United States, but since 1993 it has operated as a standards-development function under the auspices of the Internet Society, an international membership-based non-profit organization

The internet Engineering Task Force (IETF) is the protocol engineering, development, and standardization arm of the Internet Architecture Board (IAB). The IETF began in January 1986 as a forum for technical coordination by contractors for the U.S. Defense Advanced Projects Agency (DARPA), working on the ARPANET, U.S. Defense Data Network (DDN), and the Internet core gateway system. Since that time, the IETF has grown into a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet protocol architecture and the smooth operation of the Internet.

The IETF mission includes:

1. Identifying and proposing solutions to pressing operational and technical problems in the Internet,
2. Specifying the development (or usage) of protocols and the near-term architecture solve such technical problems for the Internet,
3. Making recommendations to the IAB regarding standardization of protocols and protocol usage in the Internet,
4. Facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community.
5. Providing a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors, and network managers.

MFA Forum Introduction

Originally three Forums: 9 Frame Relay Forum, founded in Spring 1991 9 ATM Forum, founded in Fall 1991 9 MPLS Forum, founded in Spring 2000

- FRF and MPLSF merged in April 2003 to form the MPLS & Frame Relay Alliance
- MFA Forum formed in July 2005 by merging the ATM Forum and the MPLS & FR Alliance

The merger

1. Consolidates the three forums in order to optimize the strengths of each in addressing next generation multi-protocol networks and their interworking.

2. Leverages the combined resources of the combined organizations to advance the recognition, acceptance, and implementation of packet technologies in the global networking communications industry.
3. Provides the industry with one point of contact for MPLS, FR, and ATM technologies 9 Maintains the body of specifications from the parent organizations

Mission

The MFA Forum’s mission is to enable users, enterprise customers, and carriers to make the leap from legacy technologies to next generation networking by defining & promoting the interfaces and capabilities for enterprise and carrier IP/MPLS networks and services, including core networks, access technologies, security and privacy, visibility and reporting, and QoS (Quality of Service).

SL-8 (SLo-1) Type-length-value

Within data communication protocols, **TLV** (*type-length-value* or *tag-length-value*) is an encoding scheme used for optional information element in a certain protocol. The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size. These fields are used as follows:

1. **Type** A binary code, often simply alphanumeric, which indicates the kind of field that this part of the message represents;
2. **Length** The size of the value field (typically in bytes);
3. **Value** Variable-sized series of bytes which contains data for this part of the message.

Some advantages of using a TLV representation data system solution are:

- TLV sequences are easily searched using generalized parsing functions;
- New message elements which are received at an older node can be safely skipped and the rest of the message can be parsed. This is similar to the way that unknown XML tags can be safely skipped;
- TLV elements can be placed in any order inside the message body;
- TLV elements are typically used in a binary format which makes parsing faster and the data smaller than in comparable text based protocols.

Generic TLV Format

- The generic format of a TLV is shown below:

Byte	Description
1	Tag (MSB)
2	Tag (LSB)

Byte	Description
3	Length (MSB)
4	Length (LSB)
5	Value[0] (Data)
:	:
:	Value[n]

Variable Size Encoding for Type (T) and Length (L)

(Both the text below and that in TLV encoding section are adopted from an earlier packet specification draft by Mark Step)
To minimize the overhead during early deployment and to allow flexibility of future protocol extensions to meet unforeseeable needs, both type (T) and length (L) take a variable size format. For implementation simplicity, both type and length take the same encoding format.

We define a variable-length encoding for numbers in NDN as follows:

- VAR-NUMBER-1 **=** %x00-FC
- VAR-NUMBER-3 **=** %xFD **2OCTET**
- VAR-NUMBER-5 **=** %xFE **4OCTET**
- VAR-NUMBER-9 **=** %xFF **8OCTET**

The first octet of the number either carries the actual number, or signals that a multi-octet encoding is present, as defined below:

- If the first octet is less than or equal to 252 (0xFC), the number is encoded in that octet.
- If the first octet is 253 (0xFD), the number is encoded in the following 2 octets, in network byte-order. This number must be greater than 252 (0xFC).
- If the first octet is 254 (0xFE), the number is encoded in the following 4 octets, in network byte-order. This number must be greater than 65535 (0xFFFF).
- If the first octet is 255 (0xFF), the number is encoded in the following 8 octets, in network byte-order. This number must be greater than 4294967295 (0xFFFFFFFF).

A number MUST be encoded in the shortest format. For example, the number 1024 is encoded as %xFD0400 in VAR-NUMBER-3 format, not %xFE00000400 in VAR-NUMBER-5 format.

NDN TLV Encoding
TLV encoding for NDN packets is defined as follows:

- NDN-TLV **=** TLV-TYPE TLV-LENGTH TLV-VALUE
- TLV-TYPE **=** VAR-NUMBER-1 **/** VAR-NUMBER-3 **/** VAR-NUMBER-5
- TLV-LENGTH **=** VAR-NUMBER-1 **/** VAR-NUMBER-3 **/** VAR-NUMBER-5 **/** VAR-NUMBER-9

- TLV-VALUE **= *OCTET**
- TLV-TYPE MUST be in the range **1-4294967295** (inclusive). Zero is reserved to indicate an invalid TLV element and MUST NOT appear on the wire. TLV-TYPE SHOULD be unique at all nested levels. Section TLV-TYPE number assignments of this document lists initial TLV-TYPE assignments.
- The **TLV-LENGTH** field indicates number of bytes that **TLV-VALUE** uses. It **does not** include number of bytes that **TLV-TYPE** and **TLV-LENGTH** fields themselves occupy. In particular, empty payload TLV will carry **TLV-LENGTH** equal to 0.
- This encoding offers a reasonable balance between compactness and flexibility. Most common, standardized TLV-TYPE numbers will be allocated from a small-integer number-space, and these common types will be able to use the compact, single-byte encoding.

Non-Negative Integer Encoding

A number of TLV elements in the NDN packet format take a non-negative integer as their TLV-VALUE, with the following definition:
NonNegativeInteger **= 1OCTET / 2OCTET / 4OCTET / 8OCTET**
The TLV-LENGTH of the TLV element enclosing a **NonNegativeInteger** MUST be either 1, 2, 4, or 8. Depending on the TLV-LENGTH, a **NonNegativeInteger** is encoded as follows:

- if the length is 1, the **NonNegativeInteger** is encoded in 1 octet;
- if the length is 2, the **NonNegativeInteger** is encoded in 2 octets, in network byte-order;
- if the length is 4, the **NonNegativeInteger** is encoded in 4 octets, in network byte-order;
- if the length is 8, the **NonNegativeInteger** is encoded in 8 octets, in network byte-order.

The following shows a few examples of TLVs that have a **NonNegativeInteger** as their value component in hexadecimal format (where **TT** represents the TLV-TYPE, followed by the TLV-LENGTH, and then the TLV-VALUE):

- => TT0100
- => TT0101
- 255   => TT01FF
- 256   => TT020100
- 65535 => TT02FFFF
- 65536 => TT0400010000

Considerations for Evolvability of TLV-Based Encoding

- To ensure that the TLV-based protocol can evolve over time without requiring flag days, the least significant bit of TLV-TYPE number (unless overridden by the specification of a particular network/library/application TLV element) is reserved to indicate whether that TLV element is "critical" or "non-critical". A compliant TLV format decoder should follow the order, quantity, and presence requirements of the recognized elements defined in the corresponding specification. At the same time, if the decoder encounters an unrecognized or out-of-order element, the behavior should be as follows:

- if the least significant bit of the element's TLV-TYPE number is **1**, abort decoding and report an error;
- if the least significant bit of the element's TLV-TYPE number is **0**, ignore the element and continue decoding;
- TLV-TYPE numbers 0-31 (inclusive) are "grandfathered" and are all designated as "critical" for the purposes of packet processing.
- **Note**
- A recognized element is considered out-of-order if it appears in the element order that violates a specification. For example, - when a specification defines a sequence {**F1 F2 F3**}, an element **F3** would be out-of-order in the sequence {**F1 F3 F2**}; - for {**F1 F2? F3**} specification (i.e., when **F2** is optional, **F2** would be out-of-order in the same sequence {**F1 F3 F2**}.

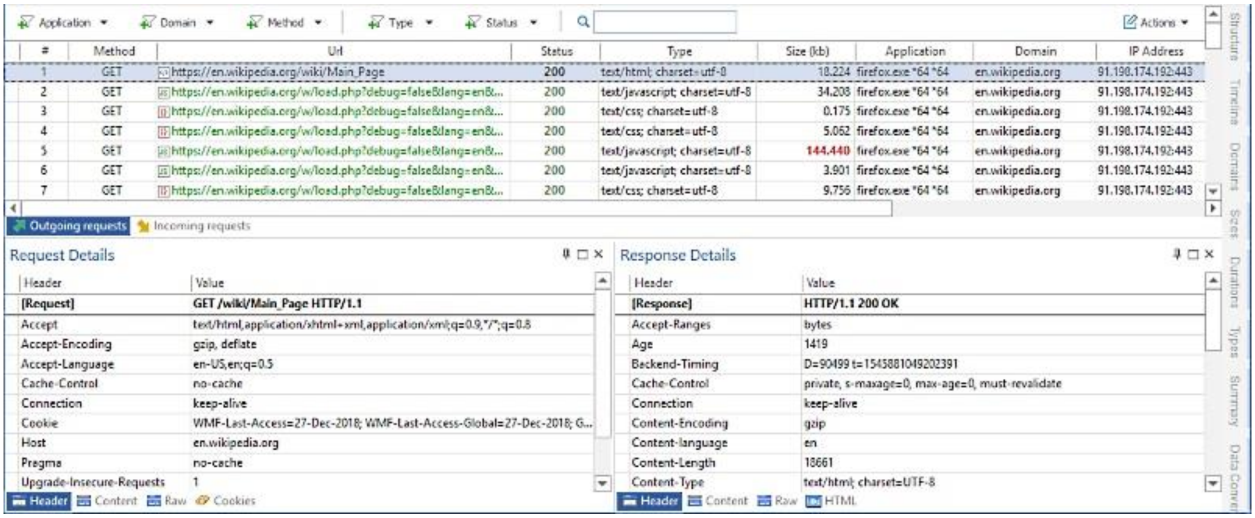
S-8 (SLO-2) Network Protocol Analyzer

Network Protocol Analyzer is a software tool used to capture and analyze the data traffic in a network. Network protocol analyzers can build the network's graphic map, generate alarms when the number of packets increases above a certain level or when it detects specific packet types in the network.

Developers may use network protocol analyzers for intercepting and analyzing the traffic from their applications, usually for HTTP protocol traffic.

Network Protocol Analyzer Main Functions.

The number of functions depends on maturity and complexity of the network protocol analyzer. But all packet sniffers and analyzers must be able to capture and analyze network packets and filter data. Some of them can display network utilization statistics, show usage and error rates, and alerts you to unusual actions. Bellow are to 10 main functions of a network protocol analyzer.



#	Method	Url	Status	Type	Size (kb)	Application	Domain	IP Address
1	GET	https://en.wikipedia.org/wiki/Main_Page	200	text/html; charset=utf-8	18.224	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443
2	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...	200	text/javascript; charset=utf-8	34.208	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443
3	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...	200	text/css; charset=utf-8	0.175	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443
4	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...	200	text/css; charset=utf-8	5.062	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443
5	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...	200	text/javascript; charset=utf-8	144.440	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443
6	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...	200	text/javascript; charset=utf-8	3.901	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443
7	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...	200	text/css; charset=utf-8	9.756	firefox.exe *64 *64	en.wikipedia.org	91.198.174.192:443

Request Details

Header	Value
[Request]	**GET /wiki/Main_Page HTTP/1.1**
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.5
Cache-Control	no-cache
Connection	keep-alive
Cookie	WMF-Last-Access=27-Dec-2018; WMF-Last-Access-Global=27-Dec-2018; G...
Host	en.wikipedia.org
Pregma	no-cache
Upgrade-Insecure-Requests	1

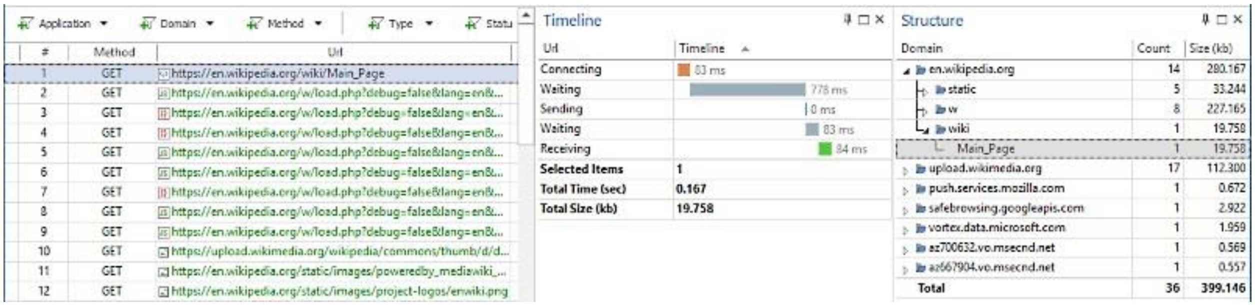
Response Details

Header	Value
[Response]	**HTTP/1.1 200 OK**
Accept-Ranges	bytes
Age	1419
Backend-Timing	D=90499 t=1545881049202391
Cache-Control	private, s-maxage=0, max-age=0, must-revalidate
Connection	keep-alive
Content-Encoding	gzip
Content-language	en
Content-Length	18661
Content-Type	text/html; charset=UTF-8

- Capture packets from LAN and WiFi adapters
- Advanced filtering
- Save data to a disk
- Create network maps
- Display error rates
- Display network utilization statistics
- Programmable alerts
- Unusual actions alerts
- Decode SSL packets
- Built-in HTTP protocol analyzer

Most network sniffers and analyzers work in a similar way and display nearly the same set of information. Simple network sniffers work by switching the network card into the so-called promiscuous mode, the more advanced ones intercept network traffic at the network driver level. This allows them to intercept and decode the SSL traffic as well by using the Man-in-the-middle technique.

HTTP Debugger is an example of a network protocol analyzer and sniffer for Windows that intercepts all of the network traffic at the driver level as well as it can decode the SSL traffic.



#	Method	Url
1	GET	https://en.wikipedia.org/wiki/Main_Page
2	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
3	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
4	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
5	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
6	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
7	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
8	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
9	GET	https://en.wikipedia.org/w/load.php?debug=false&lang=en&...
10	GET	https://upload.wikimedia.org/wikipedia/commons/thumb/d/d...
11	GET	https://en.wikipedia.org/static/images/poweredby_mediawiki_...
12	GET	https://en.wikipedia.org/static/images/project-logos/enwiki.png

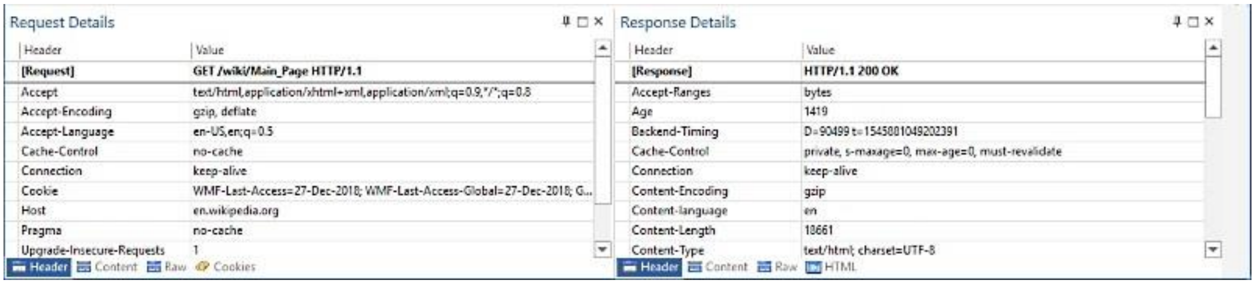
Timeline

Url	Timeline
Connecting	83 ms
Waiting	778 ms
Sending	0 ms
Waiting	83 ms
Receiving	84 ms
Selected Items	**1**
Total Time (sec)	**0.167**
Total Size (kb)	**19.758**

Structure

Domain	Count	Size (kb)
en.wikipedia.org	14	280.167
static	5	33.244
w	8	227.165
wiki	1	19.758
Main_Page	1	19.758
upload.wikimedia.org	17	112.300
push.services.mozilla.com	1	0.672
safebrowsing.googleapis.com	1	2.922
vortex.data.microsoft.com	1	1.959
az700632.vo.msecnd.net	1	0.569
az667904.vo.msecnd.net	1	0.557
Total	**36**	**399.146**

Most protocol analyzers can decode over three hundred different protocols. The more information presents the protocol analyzer, the less manual work you will have to do. A common problem for network protocol analyzers is the inability to accurately identify a protocol that is on a non-default port number, and this can be a problem in protecting against malicious hackers.



Request Details

Header	Value
[Request]	**GET /wiki/Main_Page HTTP/1.1**
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.5
Cache-Control	no-cache
Connection	keep-alive
Cookie	WMF-Last-Access=27-Dec-2018; WMF-Last-Access-Global=27-Dec-2018; G...
Host	en.wikipedia.org
Pragma	no-cache
Upgrade-Insecure-Requests	1

Response Details

Header	Value
[Response]	**HTTP/1.1 200 OK**
Accept-Ranges	bytes
Age	1419
Backend-Timing	D=90499 t=1545881049202391
Cache-Control	private, s-maxage=0, max-age=0, must-revalidate
Connection	keep-alive
Content-Encoding	gzip
Content-language	en
Content-Length	18661
Content-Type	text/html; charset=UTF-8

Network Monitoring

- Network protocol analyzers are often used to monitor the performance of the network. The protocol analyzer can display network utilization, number of collisions and number of defective frames.

The network protocol analyzer can be programmed to display alarms for a number of conditions; for example, a load level has been exceeded, an error level has been exceeded, a new workstation (new MAC address) has been added to the network, or detect packets with specific words or to certain destinations.

Data Collection and Analysis

Network protocol analyzers are usually used for collecting and analyzing captured data. The burst rate or the maximum rate at which the device can collect data without losing any information is an important characteristic of the network protocol analyzer.

Detect Defect Frames

Network interface cards can become faulty and begin transmitting packets with errors; for example, by specifying the packet data in the destination field and cause the network overload. Protocol analyzers can detect and notify about such defective cards, as well as can detect and warn about expired frames. A network protocol analyzer can detect broadcast packets and indicate which particular station sends these packets.

NETWORK ANALYZERS

Meaning and Features Network analyzers are also known as packet sniffer, protocol analyzers or packet analyzers. Network analyzers can be defined as computer programs or sometimes a hardware device which can listen to all the traffic flowing inside that network. In computer networks, information flows as raw binary data. However, these network analyzers can convert these raw binary data into human-readable format which helps to analyze the network. The legal use of network analyzer is to manage, troubleshoot and maintain network security by network administrators. However, network analyzers are used illegally too. Generally, the illegal use can be by a hacker who wants to gain unauthorized access and gather sensitive information and data from that network. Network analyzers can be tapped into many parts of the network, without the knowledge of IT administrator [16]. In Ethernet networks, Ethernet adapters are built with the feature called “filter”, which ignores any traffic not meant for it. However, network sniffing program puts the adapter into “promiscuous mode” and thus network adapters accept all frames even if the MAC address doesn’t match to its own. Hardware, capture filter, buffers, decoder etc. are the components of network sniffers. The network sniffing procedure is described below:

Collecting - It is the first task of network analyzers. In general, analyzers put the network interface card (NIC) into promiscuous mode. Thus, the NIC of that computer can listen to all the traffic in its network segment and captures all the raw binary data.

Converting - This process is carried out by decoder component of packet sniffers. In this second step, captured binary data from process one is converted into human readable form.

Analyzing - This is the last step of sniffing process. It is the step to perform protocol analysis. The protocols used in the network traffic can be viewed from the information gathered from second process. All the packets can be analyzed and explained from the viewpoint of protocols.

Who Uses Network Analysis? System administrators, network engineers, security engineers, system operators, and programmers all use network analyzers, which are invaluable tools for diagnosing and troubleshooting network problems, system configuration issues, and application difficulties. Historically, network analyzers were dedicated hardware devices that were expensive and difficult to use. However, new advances in technology have allowed for the development of software-based network analyzers, which make it more convenient and affordable for administrators to effectively troubleshoot a network. It also brings the capability of network analysis. The art of network analysis is a double-edged sword. While network, system, and security professionals use it for troubleshooting and monitoring the network, intruders use network analysis for harmful purposes.A network analyzer is a tool, and like all tools, it can be used for both good and bad purposes. A network analyzer is used for:

- ■ Converting the binary data in packets to readable format
- ■ Troubleshooting problems on the network
- ■ Analyzing the performance of a network to discover bottlenecks
- ■ Network intrusion detection
- ■ Logging network traffic for forensics and evidence
- ■ Analyzing the operations of applications
- ■ Discovering faulty network cards
- ■ Discovering the origin of virus outbreaks or Denial of Service (DoS) attacks
- ■ Detecting spyware
- ■ Network programming to debug in the development stage
- ■ Detecting a compromised computer
- ■ Validating compliance with company policy
- ■ As an educational resource when learning about protocols
- ■ Reverse-engineering protocols to write clients and supporting programs

Common Network Analyzers

- Wireshark
- WinDump
- Network General Sniffer
- Network General Sniffer
- EtherPeek
- Tcpdump
- Snoop
- Snort
- Dsniff
- Ettercap
- Analyzer
- Packetyzer
- MacSniffer

How Does It Work?

This section provides an overview of how sniffing takes place, and gives background information on how networks and protocols work. However, there are many other excellent resources available, including the most popular and undoubtedly one of the best written, Richard Stevens^‶TCP/IP Illustrated.