Network Security

tutorialspoint

SIMPLYEASYLEARNING

www.tutorialspoint.com

About the Tutorial

Network Security deals with all aspects related to the protection of the sensitive information assets existing on the network. It covers various mechanisms developed to provide fundamental security services for data communication.

This tutorial introduces you to several types of network vulnerabilities and attacks followed by the description of security measures employed against them. It describes the functioning of most common security protocols employed at different networking layers right from application to data link layer. After going through this tutorial, you will find yourself at an intermediate level of knowledge regarding network security.

Audience

This tutorial is prepared for beginners to help them understand the basics of network security. The ones who are keen on taking up career in the field of Information and Network security, this tutorial is extremely useful. For all other readers, this tutorial is a good learning material.

Prerequisites

We assume the reader has a basic understanding of computer networking and cryptography. Knowledge about communication protocols is a plus.

Disclaimer & Copyright

Table of Contents

1. Network Security — Overview

In this modern era, organizations greatly rely on computer networks to share information throughout the organization in an efficient and productive manner. Organizational computer networks are now becoming large and ubiquitous. Assuming that each staff member has a dedicated workstation, a large scale company would have few thousands workstations and many server on the network.

It is likely that these workstations may not be centrally managed, nor would they have perimeter protection. They may have a variety of operating systems, hardware, software, and protocols, with different level of cyber awareness among users. Now imagine, these thousands of workstations on company network are directly connected to the Internet. This sort of unsecured network becomes a target for an attack which holds valuable information and displays vulnerabilities.

In this chapter, we describe the major vulnerabilities of the network and significance of network security. In subsequent chapters, we will discuss the methods to achieve the same.

Physical Network

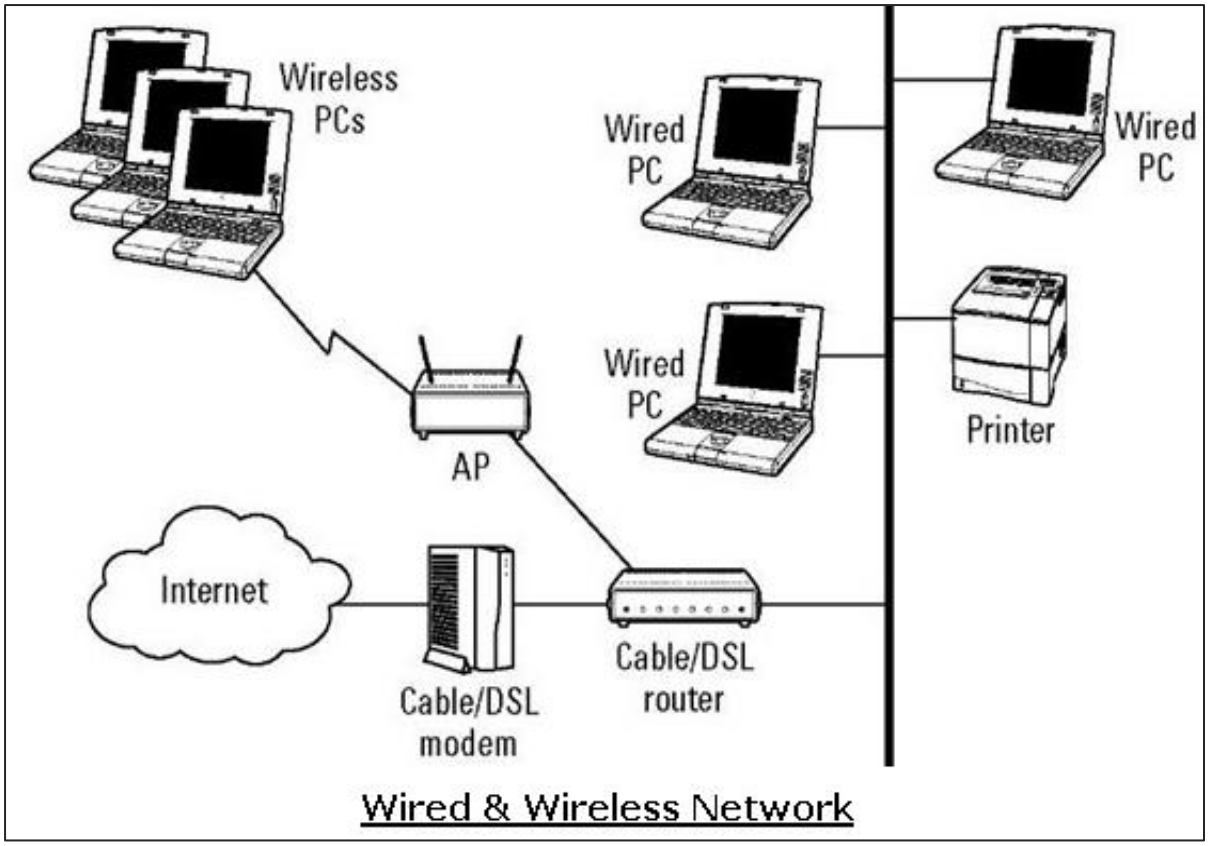
A network is defined as two or more computing devices connected together for sharing resources efficiently. Further, connecting two or more networks together is known as **internetworking**. Thus, the Internet is just an internetwork – a collection of interconnected networks.

For setting up its internal network, an organization has various options. It can use a wired network or a wireless network to connect all workstations. Nowadays, organizations are mostly using a combination of both wired and wireless networks.

Wired & Wireless Networks

In a wired network, devices are connected to each other using cables. Typically, wired networks are based on Ethernet protocol where devices are connected using the Unshielded Twisted Pair (UTP) cables to the different switches. These switches are further connected to the network router for accessing the Internet.

In wireless network, the device is connected to an access point through radio transmissions. The access points are further connected through cables to switch/router for external network access.



Wired & Wireless Network

Wireless networks have gained popularity due to the mobility offered by them. Mobile devices need not be tied to a cable and can roam freely within the wireless network range. This ensures efficient information sharing and boosts productivity.

Vulnerabilities & Attacks

The common vulnerability that exists in both wired and wireless networks is an "unauthorized access" to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection.

After accessing, an attacker can exploit this vulnerability to launch attacks such as:

- Sniffing the packet data to steal valuable information.
- Denial of service to legitimate users on a network by flooding the network medium with spurious packets.
- Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a 'man-in-the-middle' attack.

Network Protocol

Network Protocol is a set of rules that govern communications between devices connected on a network. They include mechanisms for making connections, as well as formatting rules for data packaging for messages sent and received.

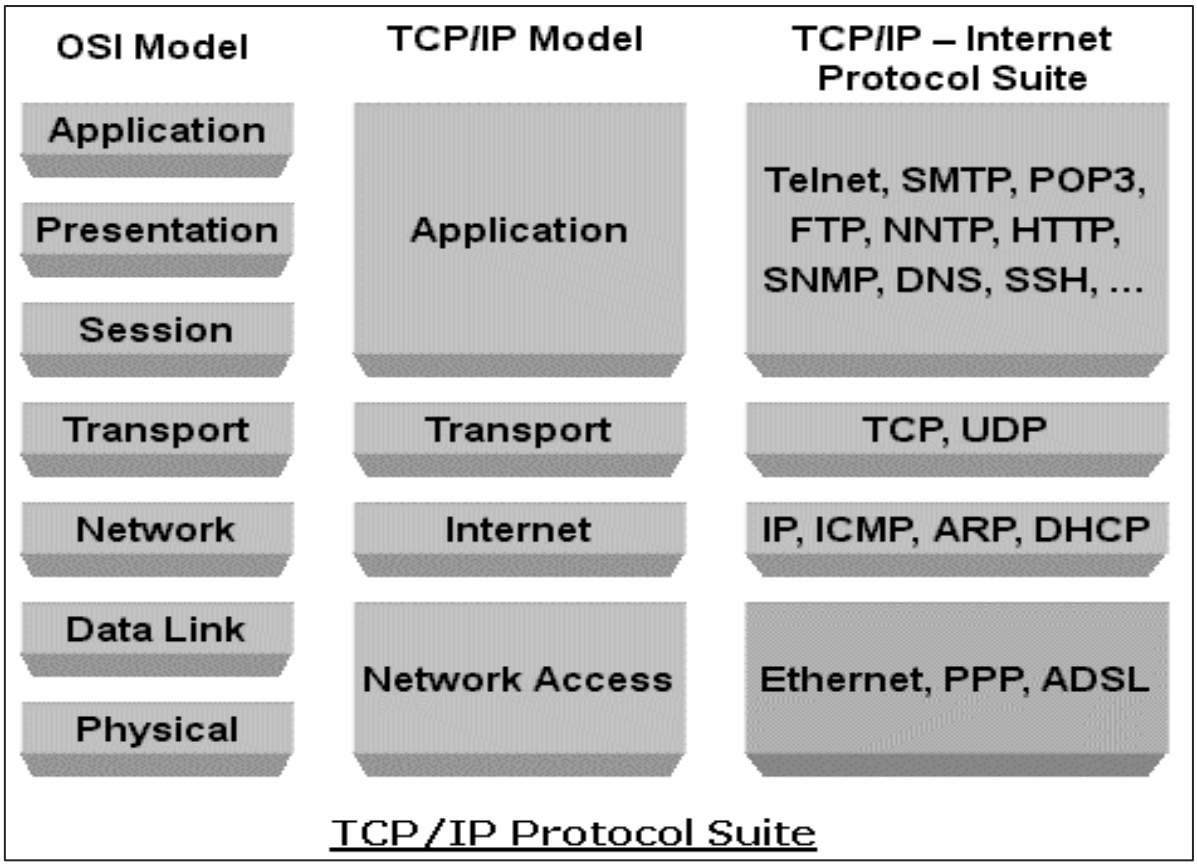
Several computer network protocols have been developed each designed for specific purposes. The popular and widely used protocols are TCP/IP with associated higher- and lower-level protocols.

TCP/IP Protocol

Transmission Control Protocol (TCP) and **Internet Protocol** (IP) are two distinct computer network protocols mostly used together. Due to their popularity and wide adoption, they are built in all operating systems of networked devices.

IP corresponds to the Network layer (Layer 3) whereas TCP corresponds to the Transport layer (Layer 4) in OSI. TCP/IP applies to network communications where the TCP transport is used to deliver data across IP networks.

TCP/IP protocols are commonly used with other protocols such as HTTP, FTP, SSH at application layer and Ethernet at the data link/physical layer.



TCP/IP protocol suite was created in 1980 as an internetworking solution with very little concern for security aspects.

It was developed for a communication in the limited trusted network. However, over a period, this protocol became the de-facto standard for the unsecured Internet communication.

Some of the common security vulnerabilities of TCP/IP protocol suits are:

- HTTP is an application layer protocol in TCP/IP suite used for transfer files that make up the web pages from the web servers. These transfers are done in plain

text and an intruder can easily read the data packets exchanged between the server and a client.

- Another HTTP vulnerability is a weak authentication between the client and the web server during the initializing of the session. This vulnerability can lead to a session hijacking attack where the attacker steals an HTTP session of the legitimate user.
- TCP protocol vulnerability is three-way handshake for connection establishment. An attacker can launch a denial of service attack "SYN-flooding" to exploit this vulnerability. He establishes lot of half-opened sessions by not completing handshake. This leads to server overloading and eventually a crash.
- IP layer is susceptible to many vulnerabilities. Through an IP protocol header modification, an attacker can launch an IP spoofing attack.

Apart from the above-mentioned, many other security vulnerabilities exist in the TCP/IP Protocol family in design as well in its implementation.

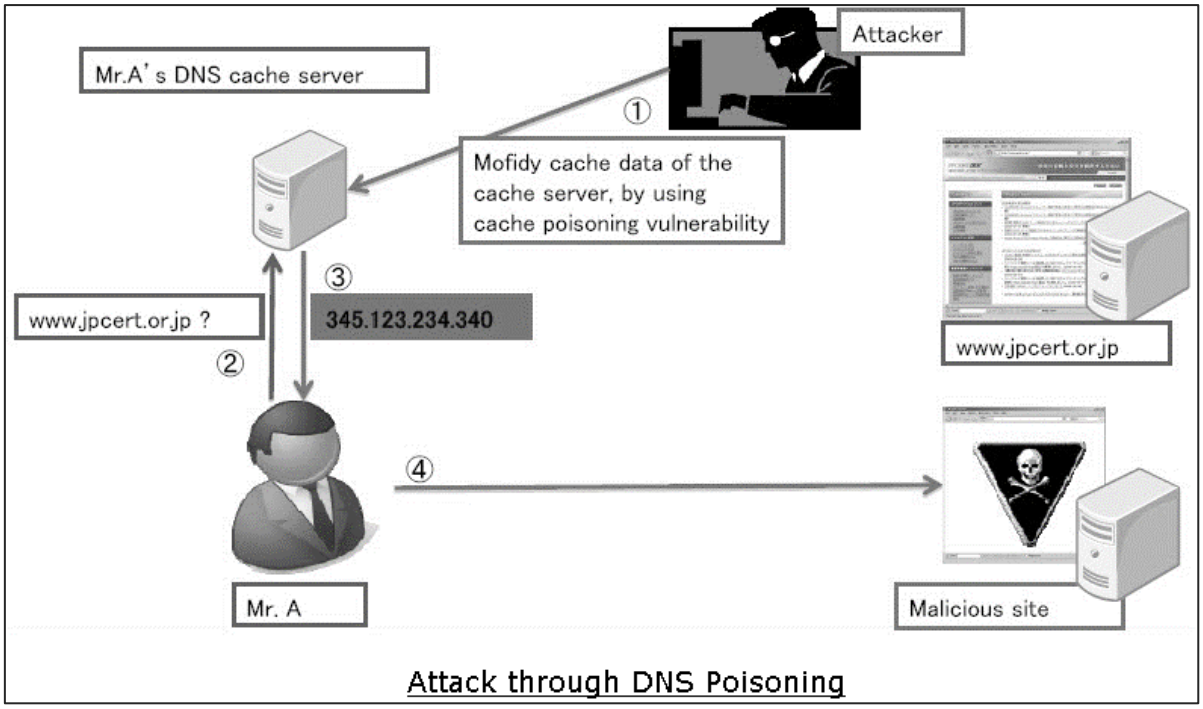
Incidentally, in TCP/IP based network communication, if one layer is hacked, the other layers do not become aware of the hack and the entire communication gets compromised. Hence, there is need to employ security controls at each layer to ensure foolproof security.

DNS Protocol

Domain Name System (DNS) is used to resolve host domain names to IP addresses. Network users depend on DNS functionality mainly during browsing the Internet by typing a URL in the web browser.

In an attack on DNS, an attacker's aim is to modify a legitimate DNS record so that it gets resolved to an incorrect IP address. It can direct all traffic for that IP to the wrong computer. An attacker can either exploit DNS protocol vulnerability or compromise the DNS server for materializing an attack.

DNS cache poisoning is an attack exploiting a vulnerability found in the DNS protocol. An attacker may poison the cache by forging a response to a recursive DNS query sent by a resolver to an authoritative server. Once, the cache of DNS resolver is poisoned, the host will get directed to a malicious website and may compromise credential information by communication to this site.



Attack through DNS Poisoning

ICMP Protocol

Internet Control Management Protocol (ICMP) is a basic network management protocol of the TCP/IP networks. It is used to send error and control messages regarding the status of networked devices.

ICMP is an integral part of the IP network implementation and thus is present in very network setup. ICMP has its own vulnerabilities and can be abused to launch an attack on a network.

The common attacks that can occur on a network due to ICMP vulnerabilities are:

- ICMP allows an attacker to carry out network reconnaissance to determine network topology and paths into the network. ICMP sweep involves discovering all host IP addresses which are alive in the entire target's network.
- Trace route is a popular ICMP utility that is used to map target networking by describing the path in real-time from the client to the remote host.
- An attacker can launch a denial of service attack using the ICMP vulnerability. This attack involves sending IPMP ping packets that exceeds 65,535 bytes to the target device. The target computer fails to handle this packet properly and can cause the operating system to crush.

Other protocols such as ARP, DHCP, SMTP, etc. also have their vulnerabilities that can be exploited by the attacker to compromise the network security. We will discuss some of these vulnerabilities in later chapters.

The least concern for the security aspect during design and implementation of protocols has turned into a main cause of threats to the network security.

Goals of Network Security

As discussed in earlier sections, there exists large number of vulnerabilities in the network. Thus, during transmission, data is highly vulnerable to attacks. An attacker can target the communication channel, obtain the data, and read the same or re-insert a false message to achieve his nefarious aims.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure.

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network.

The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as **CIA triangle**.

- **Confidentiality**. The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.
- **Integrity**. This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.
- **Availability**. The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

Achieving Network Security

Ensuring network security may appear to be very simple. The goals to be achieved seems to be straightforward. But in reality, the mechanisms used to achieve these goals are highly complex, and understanding them involves sound reasoning.

International Telecommunication Union (ITU), in its recommendation on security architecture X.800, has defined certain mechanisms to bring the standardization in methods to achieve network security. Some of these mechanisms are:

- **En-cipherment.** This mechanism provides data confidentiality services by transforming data into not-readable forms for the unauthorized persons. This mechanism uses encryption-decryption algorithm with secret keys.
- **Digital signatures.** This mechanism is the electronic equivalent of ordinary signatures in electronic data. It provides authenticity of the data.
- **Access control.** This mechanism is used to provide access control services. These mechanisms may use the identification and authentication of an entity to determine and enforce the access rights of the entity.

Having developed and identified various security mechanisms for achieving network security, it is essential to decide where to apply them; both physically (at what location) and logically (at what layer of an architecture such as TCP/IP).

Security Mechanisms at Networking Layers

Several security mechanisms have been developed in such a way that they can be developed at a specific layer of the OSI network layer model.

- **Security at Application Layer** – Security measures used at this layer are application specific. Different types of application would need separate security measures. In order to ensure application layer security, the applications need to be modified.

  It is considered that designing a cryptographically sound application protocol is very difficult and implementing it properly is even more challenging. Hence, application layer security mechanisms for protecting network communications are preferred to be only standards-based solutions that have been in use for some time.

  An example of application layer security protocol is Secure Multipurpose Internet Mail Extensions (S/MIME), which is commonly used to encrypt e-mail messages. DNSSEC is another protocol at this layer used for secure exchange of DNS query messages.

- **Security at Transport Layer –** Security measures at this layer can be used to protect the data in a single communication session between two hosts. The most common use for transport layer security protocols is protecting the HTTP and FTP session traffic. The Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the most common protocols used for this purpose.

- **Network Layer –** Security measures at this layer can be applied to all applications; thus, they are not application-specific. All network communications between two hosts or networks can be protected at this layer without modifying any application. In some environments, network layer security protocol such as Internet Protocol Security (IPsec) provides a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. However, security protocols at this layer provides less communication flexibility that may be required by some applications.

Incidentally, a security mechanism designed to operate at a higher layer cannot provide protection for data at lower layers, because the lower layers perform functions of which the higher layers are not aware. Hence, it may be necessary to deploy multiple security mechanisms for enhancing the network security.

In the following chapters of the tutorial, we will discuss the security mechanisms employed at different layers of OSI networking architecture for achieving network security.

2. Network Security — Application Layer Security

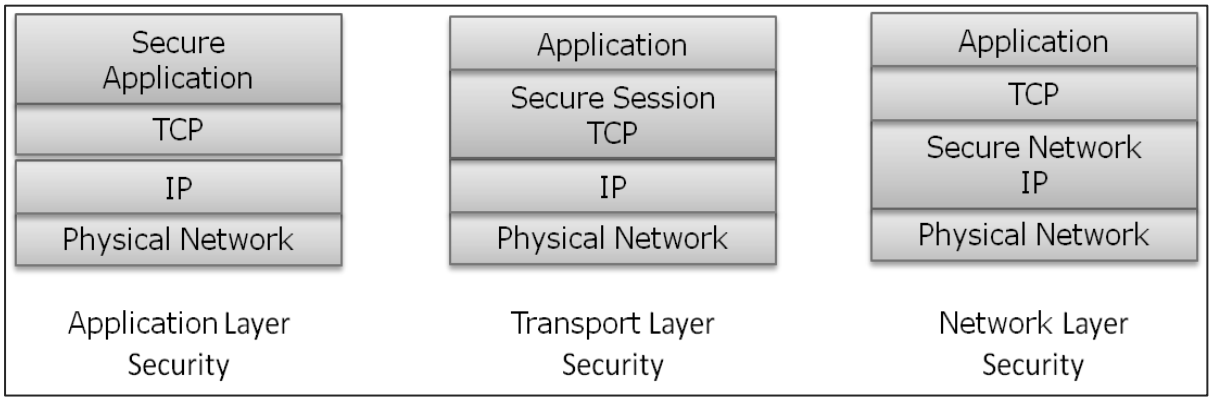
Various business services are now offered online though client-server applications. The most popular forms are web application and e-mail. In both applications, the client communicates to the designated server and obtains services.

While using a service from any server application, the client and server exchange a lot of information on the underlying intranet or Internet. We are aware of fact that these information transactions are vulnerable to various attacks.

Network security entails securing data against attacks while it is in transit on a network. To achieve this goal, many real-time security protocols have been designed. Such protocol needs to provide at least the following primary objectives:

- The parties can negotiate interactively to authenticate each other.
- Establish a secret session key before exchanging information on network.
- Exchange the information in encrypted form.

Interestingly, these protocols work at different layers of networking model. For example, S/MIME protocol works at Application layer, SSL protocol is developed to work at transport layer, and IPsec protocol works at Network layer.



In this chapter, we will discuss different processes for achieving security for e-mail communication and associated security protocols. The method for securing DNS is covered subsequently. In the later chapters, the protocols to achieve web security will be described.

E-mail Security

Nowadays, e-mail has become very widely used network application. Let's briefly discuss the e-mail infrastructure before proceeding to know about e-mail security protocols.

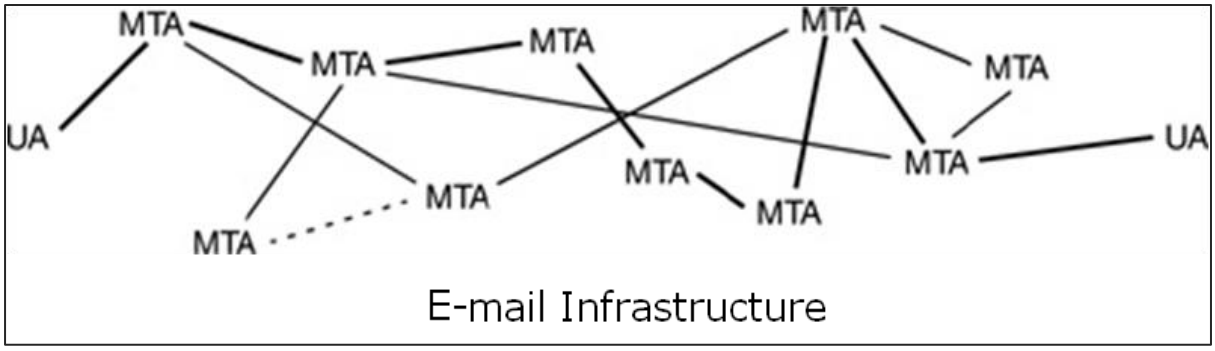
E-mail Infrastructure

The simplest way of sending an e-mail would be sending a message directly from the sender's machine to the recipient's machine. In this case, it is essential for both the machines to be running on the network simultaneously. However, this setup is impractical as users may occasionally connect their machines to the network.

Hence, the concept of setting up e-mail servers arrived. In this setup, the mail is sent to a mail server which is permanently available on the network. When the recipient's machine connects to the network, it reads the mail from the mail server.

In general, the e-mail infrastructure consists of a mesh of mail servers, also termed as **Message Transfer Agents** (MTAs) and client machines running an e-mail program comprising of User Agent (UA) and local MTA.

Typically, an e-mail message gets forwarded from its UA, goes through the mesh of MTAs and finally reaches the UA on the recipient's machine.



E-mail Infrastructure

The protocols used for e-mail are as follows:

- Simple mail Transfer Protocol (SMTP) used for forwarding e-mail messages.
- Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are used to retrieve the messages by recipient from the server.

MIME

Basic Internet e-mail standard was written in 1982 and it describes the format of e-mail message exchanged on the Internet. It mainly supports e-mail message written as text in basic Roman alphabet.

By 1992, the need was felt to improve the same. Hence, an additional standard *Multipurpose Internet Mail Extensions* (MIME) was defined. It is a set of extensions to the basic Internet E-mail standard. MIME provides an ability to send e-mail using characters other than those of the basic Roman alphabet such as Cyrillic alphabet (used in Russian), the Greek alphabet, or even the ideographic characters of Chinese.

Another need fulfilled by MIME is to send non-text contents, such as images or video clips. Due to this features, the MIME standard became widely adopted with SMTP for e-mail communication.

End of ebook preview

If you liked what you saw…

Buy it from our store @ **https://store.tutorialspoint.com**