Network Basics and Security

Lesson 8

KEY CONCEPTS

■ Network ■ Wired Network ■ Wireless Network ■ Computer Security ■ Network Security ■ Internet Security ■ Network Protocol ■ IP Address ■ Nodes and Hosts ■ Protocols ■ Data Packets ■ Domain Name

Learning Objectives

To understand:

- The concept of network and computer security
- And get acquainted with different types of network
- And gather an understanding of how networks operate along with relevant networking models
- The common threats to network security
- Measures to protect against attacks to network

Lesson Outline

- Computer and Network Security: An Introduction
- Intranets
- Extranets
- Internet
- Networking concepts OSI models TCP/IP model
- Ports
- Secure protocols
- Common network attacks
- Network Devices Hubs
- Bridges
- Switch
- Security Devices
- Firewall
- Lesson Round-Up
- Glossary
- Test Yourself
- List of Further Readings

INTRODUCTION

In today's technologically driven world, computers are used to network and connect on a daily basis throughout organizations, businesses, schools, government institutions and authorities. The importance of network and security can be understood by way of the following example:

In a multinational corporation having corporate offices around the world, employees are dependent upon computers to connect with clients, hold meetings and execute projects. In order to connect the huge workforce, such corporations have networks which host multiple servers at the same time. The workstations of the employees may have varied types of operating systems, hardware, software configuration, IP protocols and the employees using them may have different levels of awareness regarding cyberspace. Considering that thousands of employee workstations are connected to the internet, such a company network can become a potential target of cyber-attacks.

In this Lesson, an attempt has been made to trace the basic concepts of network and network security.

NETWORK SECURITY

A computer network is a group of two or more devices/computers connected to one another for efficient exchange of information. Networks are connected through networking devices like computer, switches, routers, modems, etc. These networking devices may be connected through wires (for example, cables) resulting in a wired network or through wireless media (for example, air) resulting in a wireless network.

It is important to note that data on a network is transmitted for communication in the form of packets, which are nothing but small chunks of data[1].

Network Security refers to the protective measures undertaken by an organization or individual to secure its network systems and data from unauthorized access and attacks by hackers. The basic aim of any network security system is to safeguard the accessibility, accuracy and confidentiality of sensitive data.

The importance of network security can be understood by way of the following example: Most businesses have moved to an electronic mode where transactions are conducted online and goods are sold through company owned websites or e-commerce websites. In order to facilitate such operations on the internet, it is important to safeguard company resources and information, as any unauthorized attack can leak sensitive company and customer information into the public domain. Even a minor security threat has the potential to disrupt the company's efficiency and reputation in the market.

Network security seeks to protect data in order to ensure and maintain the following[2]:

Data confidentiality: Assures that the data does not fall in the hands of unauthorized users.

Privacy: Assures that individuals are able to decide what data belonging to them may be disclosed, to whom it is disclosed and the extent of disclosure.

Data Integrity: Assures that the data remains in its intended form, subject to modification only in authorized manner.

System Integrity: Assures that systems perform their intended function, unhampered by any external manipulation.

Availability: Assures that data available on the system is readily accessible and not denied to authorized users.

1 Computer Networks, Available at: https://ncert.nic.in/textbook/pdf/lecs110.pdf.
2 William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Publication Ltd. 2017, England.

Objectives of Network Security

It must be noted that a secure network is one which is able to:

a. Control the physical access to the network.

b. Prevent any accidental deletion, modification or tampering of data.

c. Detect and prevent internal network security breaches.

d. Detect and prevent external network attacks.

INTRANETS

It refers to a private network within organizations for ensuring secure data sharing and communication among all the employees[3]. It enables the organization to safely transmit sensitive and confidential data. The term 'intra' means 'inside'. Therefore, it can be said that intranet centralises the digital workplace of an organisation, so that documents, projects, databases, etc. can be shared securely within the organization[4]. Intranet is used by departments and all employees of a company.

Intranet enables the organization to not only benefit from time and cost savings but also increases the productivity and efficiency of workforce, by making the information available on a real time basis. Intranet also serves as a tool to facilitate easy communication between the workforce.

EXTRANETS

It refers to a private network existing within an organization which uses the internet to connect with people outside the organization, like customers and suppliers. This network is controlled in a manner that allows customers, third parties or partners to access specific information only without providing them with access to entire network[5].

Extranet is used by business partners, suppliers and customers for collaboration with the company[6]. Benefits of extranet include flexibility, reduced time in processing of orders, timely updation of information and reduction of errors.

INTERNET

A worldwide network of inter-connected computers, servers, phones, and electronic devices is referred to as the internet. These devices communicate with one another using the transmission control protocol (TCP) standard to allow for the quick exchange of data and files as well as other services[7].

Internet is a global hub of computer networks which enables a user at one computer system/workstation to not only interact but also share and receive data and resources from any other user working on any other system/ workstation[8].

The internet is widely used for purposes of communication, transmission of information and sharing of resources across devices on a network. Whenever a user tries to visit a website, a request is made by protocol to the server, which is a collection of web pages. The server in turn, looks for the exact webpage and delivers the same to the user's computer/device, resulting into an 'end-to-end' user experience[9].

3 Difference between Intranet and Extranet, Available at: https://byjus.com/gate/difference-between-intranet-and-extranet/.
4 Ibid.
5 Supra, Note 2.
6 Ibid.
7 Chiradeep BasuMallick, What Is the Internet: Meaning, Working and Types, SPICEWORKS, (February 22, 2022); Available at: https://www.spiceworks.com/tech/networking/articles/what-is-the-internet/.
8 Ibid.
9 Ibid

NETWORKING CONCEPTS

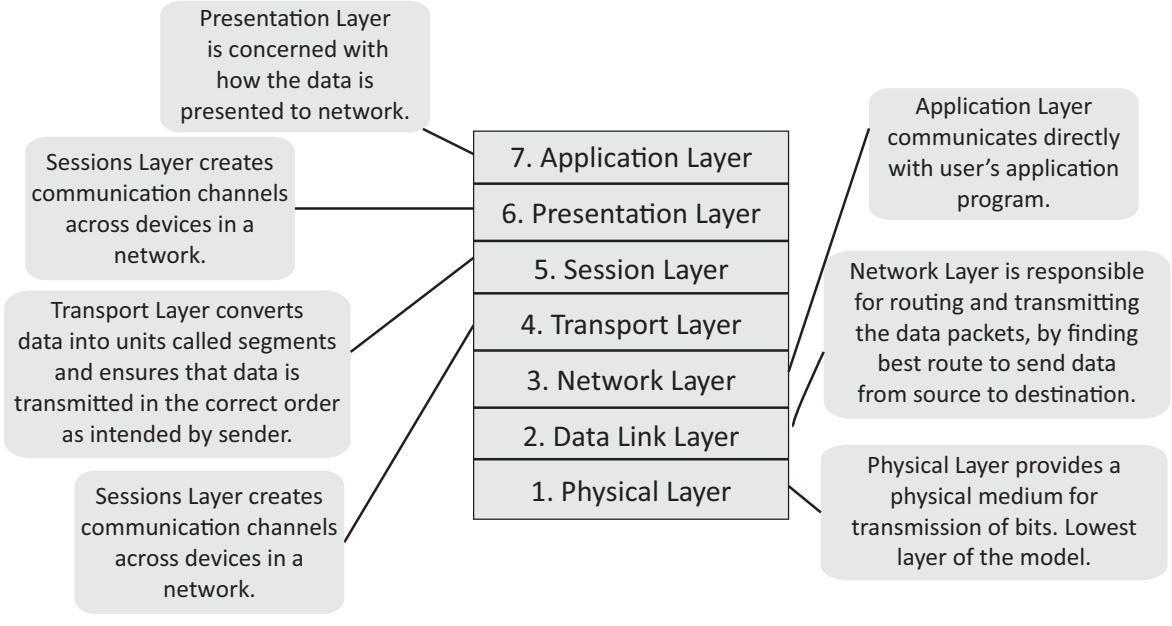
OSI model

Open Systems Interconnection (OSI) model is reference framework created by the International Standards Organization to foster an understanding of how technologies and devices interact with each other on a network. This model consists of different layers which work together to move data around a network[10]. The different layers of OSI Network will be discussed as follows:

- **Physical Layer:** This is the lowest layer in OSI model and is concerned with physical aspect of data transmission. Here, information is contained in the form of bits, which is transmitted to network notes. The transmission takes place through optical fibre, metallic cable, wireless radio wave, etc.
- **Data Link Layer:** This layer breaks the data into smaller units called frames and adds a header and trailer to each frame. The header contains a destination address to which the frame is transferred. This layer ensures that data is transferred from node to node without any error.
- **Network Layer:** This layer determines the best route to transmit the data packet to its destination and this function is known as 'routing'. The Network Layer also places the IP addresses of sender and receiver on header of each frame.
- **Transport Layer:** This layer takes data from higher levels of OSI model and breaks the same into 'segments', which are then sent to lower layers of the model for data transmission.[11] It also undertakes sequencing of data so that it is received and reassembled in correct order at the destination.
- **Session Layer:** This layer is responsible for establishing, maintaining and terminating connections between networked devices[12]. It initiates a session and ensures that the session remains active while data is being transmitted. After successful transmission, this layer closes the session. It also establishes checkpoints, from where date transfer can be resumed in case of interruption during any session.
- **Presentation Layer:** This layer is responsible for ensuring how data is presented to the network. It undertakes three primary operations, namely Translation, Compression and Encryption. Translation is done to convert data in form which can be understood by differently configurated computers. Compression is done to reduce the size of data so that it can be transferred in a speedier manner. Encryption involves encoding the data to protect it from getting tampered.
- **Application Layer:** This layer works as an interface to provide network services to the end user[13]. The network applications produce data which is then transmitted over a network[14]. This layer allows network applications to access the network and display information to the user.

10 Computer Network, Available at: https://mrcet.com/downloads/digital_notes/CSE/III%20Year/COMPUTER%20NETWORKS%20NOTES.pdf.
11 Resource Material on Computer Networks, Available at: https://mrcet.com/downloads/digital_notes/CSE/III%20Year/COMPUTER%20NETWORKS%20NOTES.pdf.
12 Ibid.
13 OSI Model, Available At: https://www.javatpoint.com/osi-model.
14 Layers of OSI Model, Available at: https://www.geeksforgeeks.org/layers-of-osi-model/.

Please Note: This Model is only used for reference purposes and the current model being used on the internet is TCP/IP model.

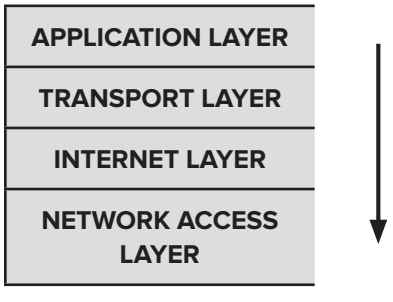


TCP/IP model (the Internet Protocol Suite)

The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a set of protocols that make up the network layer of the internet.[15] TCP/IP model is an inter-networking solution which was initially developed for communication within a limited network but later on turned out to be the standard protocol for unsecured communication over the internet.

It is interesting to note that Advanced Research Projects Administration Network, i.e., APRANET (1975) was actually the earliest version of TCP/IP model. However, in 1983, the name was changed when the model turned into an open standard that could be used on any network.[16]

The TCP/IP model consists of the following layers, where data moves from top to bottom:



The Internet Protocol Suite

i. **Application Layer:** This is the top most layer that acts as an interface through which applications and programs communicate with the user. Commonly used protocols in this layer have been discussed below:

15 Kartik Menon, The best guide to understand what is TCP/IP model, (February 26, 2023), Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model.
16 Supra, Note 18.

- **HTTP:** The Hyper Text Transfer Protocol (HTTP) is the foundation of data exchange over the World Wide Web as it makes data (be it in the form of files, images, sound clips, etc) easily accessible to the user through hyperlinks. HTTP further specifies how data requests by the user will be processed by sending it to the appropriate server, which in turn will send respond to such request[17].
- **SMTP:** Simple Mail Transfer Protocol (SMTP) is entrusted with the task of sending and receiving electronic mails[18].
- **FTP**: File Transfer Protocol (FTP) is concerned with transfer of files over a network[19].

ii. **Transport Layer:** This layer is concerned with packaging of data into smaller packets and segments so that they can be transmitted over the network. This layer also creates a communication channel between the sender and receiver device for an error-free transmission of data without any hindrance.

Some of the protocols used in transport layer are:

- **TCP:** Transmission Control Protocol (TCP) is the protocol which establishes a connection between the source and destination system and further ensures proper movement of segments over communication channel.[20]
- **UDP:** User Diagram Protocol (UDP) is mainly responsible for detection of errors during transmission of data over the network[21].

iii. **Internet Layer:** This layer is responsible for routing the data during transmission by pointing out the path which the data packets will use for transmission. This layer also helps in identification of data over the network by providing IP addresses to the system.

The protocols used in this layer are discussed below:

- **IP:** Internet Protocol (IP) is the most important protocol in internet layer, as it is responsible for sending data packets across a network from the source to destination.
- **ARP:** Address Resolution Protocol (ARP) uses the IP address to locate the physical address of the host[22].
- **IGMP:** Internet Group Management Protocol (IGMP) is used for data transmission to a group of networks[23].

iv. **Network Access/Interface Layer:** This layer is concerned with physical aspect of data transmission in raw form, i.e. binary format, through physical communication modes over a network[24]. This layer makes use of protocols like ethernet cables, fibre links and token rings.

---

17 HTTP overview, Available At: https://www.tutorialspoint.com/http/http_overview.htm.
18 Ujjwal Abhishek, TCP/IP Reference Model I Computer Networks, Available At: https://workat.tech/core-cs/tutorial/tcp-ip-reference-model-in-computer-networks-4c9jodl67ax5.
19 Ibid.
20 Kartik Menon, The best guide to understand what is TCP/IP model, (February 26, 2023), Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model.
21 Ibid.
22 Supra, Note 21.
23 Ibid.
24 Supra, Note 23.

PORTS

Ports are network points allotted to specific process or service, where connections begin and end[25]. Ports are managed by a computer's operating system[26].

Ports helps to make network connections more efficient and flawless. At any particular point of time, a computer may receive and send varied kind of data over the same network connection. In this scenario, ports help the computer to sieve through the data traffic and directs the computer what to do with the data.

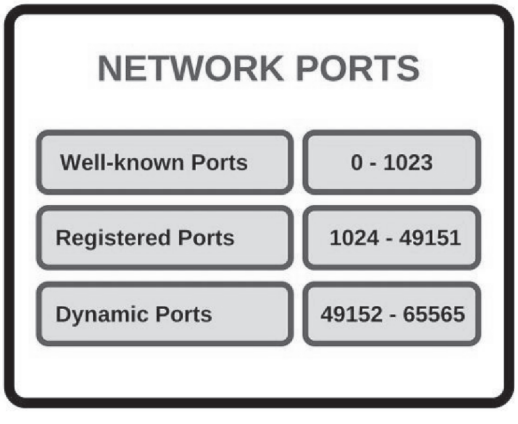
Ports can be both physical as well as virtual. Physical ports serve as connection points from where external devices can be connected to the computer. Virtual ports are connection points that allows data to freely flow between a program and the computer or over the internet[27].

In simple terms, port is an address which is assigned to every application running on a computer which utilises the internet for communication[28]. Port helps to transmit data between a computer application and computer network[29].

Every process or service (which is run by an application) is connected to a separate port. Every port has a port number which helps to identify which application is running on a device. Sometimes, this number is automatically assigned to the application running on the computer by the operating system[30].

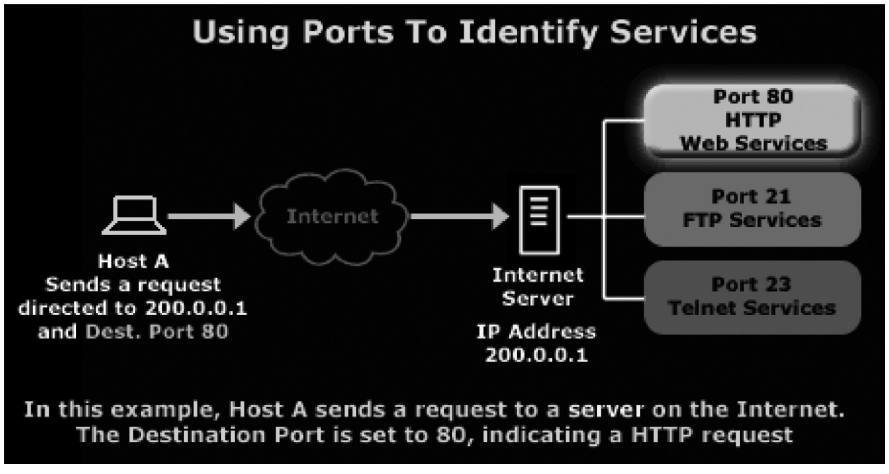
In a network, port numbers fall in the range between 0 to 65535[31]. The range of Port Numbers are as follows:

- Well known/System ports (falling in the range between 0 to 1023) are associated with common applications and services such as FTP, HTTP and SMTP[32]. For example, port number 80 is used with HTTP, whereas FTP uses port number 20 and 21.
- Registered Ports (falling in the range between 1024-49151) are assigned for specific use on application to Internet Assigned Numbers Authority[33].
- Dynamic Ports (falling in range between 49152-65565), which are also called Unassigned or Ephemeral Ports, are utilised for any type of service[34].



25 *What is a Port?, CLOUDFARE, Available at: https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/.*
26 *Ibid.*
27 *What is a Network Port?, TUTORIALS POINT, Available at: https://www.tutorialspoint.com/what-is-network-port.*
28 *What is a Port? SCALER TOPICS, Available at: https://www.scaler.com/topics/computer-network/what-is-port/.*
29 *Ibid.*
30 *Ibid.*
31 *Ibid.*
32 *Supra, Note 30.*
33 *What is a Port? SCALER TOPICS, Available at: https://www.scaler.com/topics/computer-network/what-is-port/.*
34 *Supra, Note 36.*

Ports are concerned with Transport Layer of the Internet Protocol Suite or TCP/IP model. Only protocols like the Transmission Control Protocol (TCP) or User Diagram Protocol (UDP) found in the Transport Layer are able to indicate the exact port to which a data packet is required to be sent.



SECURE PROTOCOLS

The communication protocols which are structured to transmit data between two connection points in a secure and encrypted form are called secure protocols. Such protocols aim to preserve the security, integrity and authenticity of data during communication through network channels, including the internet. Such protocols prevent unauthorized access to data in a network.

Secure Protocols usually make use of cryptography and encryption techniques to secure and encrypt data, which can only be decrypted by using special algorithm, logical key, formula or a combination of them[35]. This means if data falls into the hands of any third party, it will be unreadable and of no use, unless it is duly decrypted.

Commonly used secure protocols are Secure Sockets Layer (SSL), Secure File Transfer Protocol (SFTP) and Transport Layer Security (TLS).

SSL Protocol is designed to facilitate secure data transfer between a web browser and a web server, while guarding the confidentiality and authenticity of information. It is very popular as most web browsers support SSL protocol. It is found between the application layer and transport layer.

TLS Protocol generates a master key for encryption of data using a pseudo-random algorithm[36]. The encrypted data is then transmitted from the client to server, ensuring data protection. It encrypts communication between web browser and web server (for example- a web browser loading a website)[37].

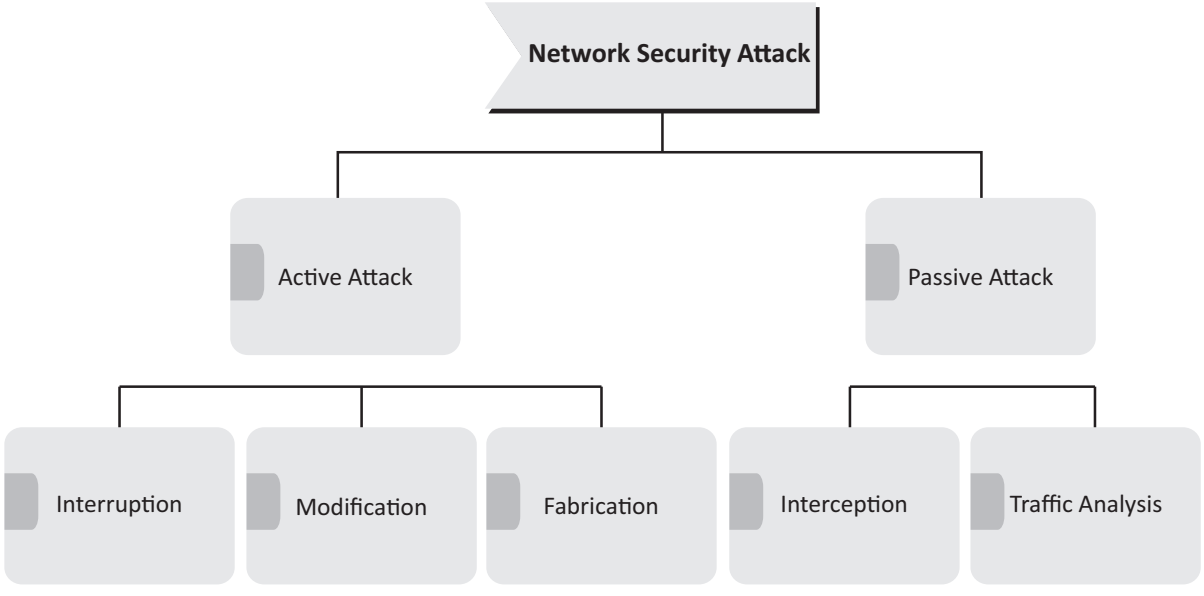
Other secure protocols are also used, apart from SSL and TLS. For example, FTPS which stands for File Transfer Protocol Secure helps in secure transmission of files over the internet.

Secure Protocols are essential to protect the safety and security of sensitive data which may be shared over the internet. Nowadays, increased number of transactions are conducted online, which involves sharing of OTPs (One-Time Passwords), debit and credit card details, UPI number, bank account details, etc. In order to safeguard such information and protect against falling prey to cybercrimes, secure protocols protect security and privacy of such sensitive data.

35 Margaret Rouse, Network Security Protocols, Available at: https://www.techopedia.com/definition/29036/network-security-protocols.
36 Types of Internet Security Protocols, GEEKS FOR GEEKS, (September 27, 2021), Available at: https://www.geeksforgeeks.org/types-of-internet-security-protocols/.
37 What is Transport Layer Security, CLOUDFLARE, Available at: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

COMMON NETWORK ATTACKS

Network security attacks can be classified under different heads as follows:



Passive Attack: It involves intrusion in the form of monitoring by an attacker, with the goal of "reading data on the network"[38]. Through this attack, an attempt is made by third party/attacker to obtain confidential information which is being transmitted. More often than not, neither the sender, nor the receiver is aware that the data security has been breached and data has been read by an attacker as such attacks do not involve any alteration of data.

Passive Attacks are of two types; Interception and Traffic Analysis. ***Interception*** involves reading of contents of any message, file, email, etc which may be sent across a network and extracting the information contained in the message. Interception may be avoided by having encryption protection in place. ***Traffic Analysis*** involves monitoring of traffic which is moving across a data network, which on careful analysis may reveal information like size, frequency and number of messages and the source and destination of such messages[39].

Active Attack: It involves active intrusion by an attacker, with the goal of "writing data onto the network"[40]. Attacker in such situations can seriously tamper with the data being transmitted across a communication network by:

a. Deleting the data sent;

38 Network Security Tutorial by APNIC, Available at: https://training.apnic.net/wp-content/uploads/sites/2/2016/12/TSEC01.pdf.
39 Available at : https://archive.mu.ac.in/myweb_test/MCA%20study%20material/M.C.A.(Sem%20-%20IV)%20Paper%20-%20III%20-%20%20Network%20Security.pdf.
40 Supra, Note 42.

b. Intercepting messages sent on the network and substituting the same with his own messages, where parties are fooled into believing that they are talking to each other when they are actually talking to the attacker (Man-in-the-middle);

c. Modification of data;

d. Playback of data from another connection[41].

Active attacks are of three types:

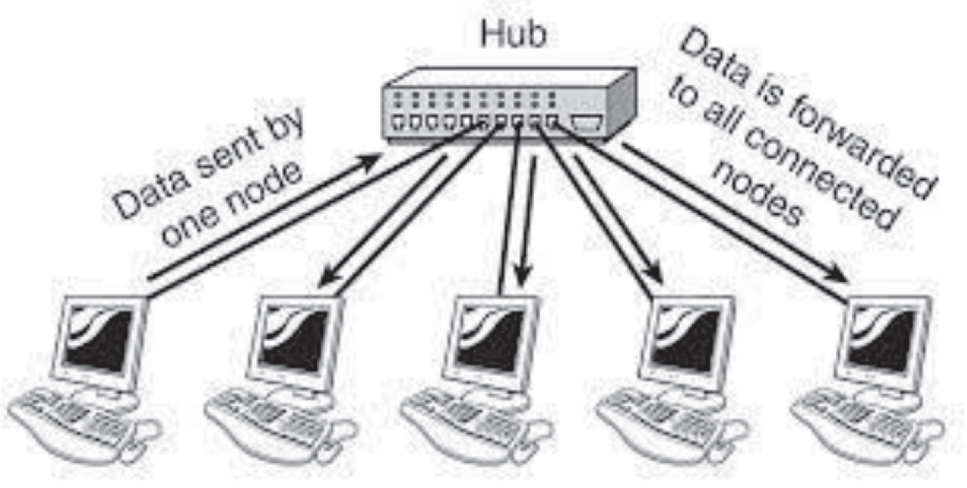
- ***Interruption:*** In this type of attack, the attacker masquerades as a different person and hamper with the communication network. For example, a hacker may impersonate himself as a Manager of a factory and send a message on his behalf to all the workers, frivolously announcing a ten-day paid holiday. Such type of security breaches will not only harm the reputation of the factory but also lead to business losses.
- ***Modification:*** In this attack, the original message is altered or modified by the attacker to produce an undesirable effect. For example, message to the effect that "Raju has been promoted" may be modified to mean "Raju has been demoted".
- ***Fabrication:*** The 'Denial of Service' attacks falls under this category, where an attacker attempts to affect the use of network facilities by seriously disrupting a network by disabling it or overloading it so as to degrade performance[42]. Timely detection is the key to prevent active attacks.

NETWORK DEVICES HUBS

Network devices are physical devices which allow communication between hardware on a computer network[43]. Examples of network devices include routers, gateways, bridge, switch, hubs, etc.

A hub refers to a networking device which is used for connection of multiple devices on a network[44]. Hubs are generally used in Local Area Networks (LAN). A hub consists of many ports, which are in turn connected to computer systems which are connected to the network.

41 Available at: https://archive.mu.ac.in/myweb_test/MCA%20study%20material/M.C.A.(Sem%20-%20IV)%20Paper%20-%20III%20-%20%20Network%20Security.pdf
42 Notes on Network Security, Available at: https://www.vssut.ac.in/lecture_notes/lecture1428550736.pdf.
43 Network Devices, February 21, 2023, Available at: https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/.
44 What are hub and switch in a computer network?, TUTORIALS POINT, Available at: https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network.



Hubs are not able to differentiate between data packets. Therefore, any information or data which is shared with a hub through a port, is in turn transmitted to every other port connected to the hub. This means data is sent to all the connected devices on a network. A major limitation of a hub is that if data is received from two different devices at the same time, it may lead to a collision.

BRIDGES

A bridge can be defined as a device which connects smaller sub-networks in order to create a single, bigger network[45]. This function of a bridge of consolidating a single network from multiple sub-networks is called *'network bridging'*[46]. Bridges are used to create one extended LAN from multiple LANs. Bridges are found in the data link layer of the OSI model.

The following types of bridges are found in a computer network:

a. **Transparent Bridges:** Transparent bridges connect numerous network segments to other bridges in order to make routing choices[47].

b. **Translational Bridges:** When switching from one kind of networking system to another, translational links are employed. They can link various networks, including Ethernet and Token ring networks[48].

c. **Source Routing Bridges:** A source routing bridge chooses the best path between two server hosts[49].

SWITCH

A switch is a network device which is used to connect multiple computers or devices on a network. On receiving data, a switch identifies the destination from data packet and locates where exactly to send the packet. Unlike a hub, a switch sends data only to the designated nod and does not send the data to all devices on a network. A switch drops signals when it receives data which is corrupted in any manner. In such a case, a switch makes a request to the sender to resend the data packet. Switches are commonly used in homes and offices to create network connections to access the internet, smart TVs, etc.

45 Jaya Sharma, What is a Bridge in a computer network?, March 3, 2023, Available at: https://www.shiksha.com/online-courses/articles/bridge-in-computer-network/.
46 Ibid.
47 Jaya Sharma, What is a Bridge in a computer network?, March 3, 2023, Available at: https://www.shiksha.com/online-courses/articles/bridge-in-computer-network/.
48 Ibid.
49 Ibid.

Difference between a Switch and a Hub[50]:

Switch	*Hub*
Concerned with data link layer of OSI model.	Concerned with physical layer of OSI model.
Data is transmitted to only destination node.	Data is transmitted to all nodes.
Since they are associated with network software, they are 'active' devices.	Since they are not associated with any software, they are 'passive' devices.

SECURITY DEVICES

Network Security refers to the practice of safeguarding the network from any unauthorized access or external risks. The devices used by network administrators to safeguard their network are called network security devices.

Network Security devices are typically physical or virtualised hardware appliances, with vendor specific software installed. Seldom, organizations build their own network security device using custom software and commodity server hardware. For a specific type of equipment, one strategy may be more cost-effective than the other depending on your company's specific needs.[51]

With the spike in cloud computing, some devices that would be traditionally hosted on a local network, are instead provided by a third party. Businesses commonly host security applications used to protect web applications and email communications in the cloud, especially if the websites and email services themselves are cloud-hosted.

Types of Network Security Devices:

- ***Active Devices:*** Such devices block the surplus or unwanted traffic on a network. For example, firewalls, anti-virus scanning devices, content filtering devices, etc.
- ***Passive Devices:*** Such devices are concerned with identification and reporting of intrusion on a network. For example, intrusion detection devices.
- ***Preventive Devices:*** Such devices prevent potential security attacks by scanning, detecting and identifying breaches of security on a network.
- ***Unified Threat Management:*** These devices provide one-stop security solutions for all network problems. For example: Firewalls, web caching, etc.

Authentication Applications: These applications authenticate the identity of the sender of data to ensure that the communication has been sent by the intended sender and not an imposter/hacker, before providing access to a network. Data may be authenticated in the following manner:

- ***Peer Entity Authentication:*** It assures and reaffirms the identity of the entity involved in the communication.
- ***Data Origin Authentication:*** It verifies whether the source disclosed by the sender is the same as the actual source of data.

50 What are hub and switch in a computer network?, TUTORIALS POINT, Available at: https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network.
51 Available at: https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/.

- ***Access Control:*** It prevents unauthorized use of data by controlling the access to the data by specifying under what conditions the data may be accessed, who may access the data, etc.
- ***Data Confidentiality:*** It assures that the privacy of the data has been protected against unauthorized access.
- ***Data Integrity:*** It assures that the data has not been tampered or compromised and its original form has not been altered.

Other security mechanisms:

- ***Encipherment:*** This technique is employed to hide the data in order to protect its authenticity and confidentiality. Data may be enciphered by both cryptography as well as encipherment.
- ***Digital Signature:*** Under this mechanism, the sender put his digital signature on the data which is then verified by the receiver. A digital signature authenticates that the data has originated from the sender.
- ***Traffic Padding:*** This mechanism inserts extra bits into the data stream which is being transmitted, so that any attempt to analyse the traffic is frustrated[52].
- ***Network Access Control:*** This technique controls the level of access granted to a network by placing password protections, firewalls, etc.
- ***Notarization:*** This mechanism involves the use of a trusted third party in the process of data exchange.

FIREWALL

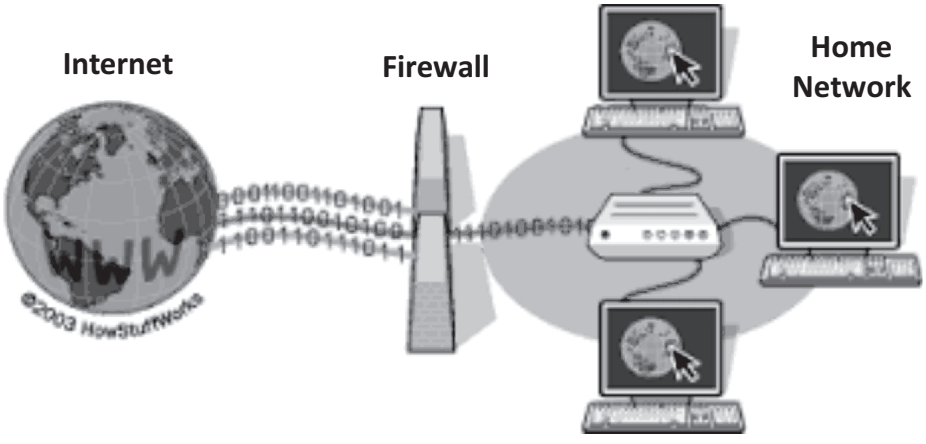
A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. Appositely, it is a barrier that stands between a private internal network and the open Internet at its most basic level. Firewalls exclude unwanted and undesirable network traffic from entering the organization's systems. Depending on the organization's firewall policy, the firewall may completely disallow some traffic or all traffic, or it may perform a verification on some or all of the traffic.[53]

Primarily, it is an essential component of any security design since it gives your network security device control over host level defences, eliminating the need for guesswork. With the help of an integrated intrusion prevention system (IPS), firewalls, and especially Next Generation Firewalls, concentrate on thwarting malware and application-layer attacks. These Next Generation Firewalls can react swiftly and seamlessly to detect and respond to external attacks across the entire network. They can implement policies to better protect your network and do speedy analyses to find intrusive or dubious activities, like malware, and stop it.

Firewalls can carry out fast assessments to detect intrusive or suspect behaviour, such as malware, and can be configured to act on previously specified policies to further safeguard a network. Network can be configured with precise policies to allow or prohibit incoming and outgoing traffic by using a firewall as security infrastructure.

52 Types of Security Mechanism, (September 10, 2020), GEEKS FOR GEEKS, Available at: https://www.geeksforgeeks.org/types-of-security-mechanism/.

53 Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.



The various types of Firewalls have been enlisted below:

- ***Packet Filtering***: A small amount of data is analysed and distributed according to the filter's standards.
- ***Proxy Service***: Network security system that protects while filtering messages at the application layer.
- ***Stateful Inspection****:* Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- ***Next Generation Firewall***: Deep packet inspection Firewall with application-level inspection.

LESSON ROUND-UP

- A network can be defined as a group of two or more computers or electronic devices which are connected together for the efficient exchange of information and resources.
- Computer networks are typically categorised as LAN (Local Area Network), MAN (Metro Area Network), and WAN (Wide Area Network) based on the geographic region covered and data transfer rate.
- Each device in a communication network that can receive, generate, store, or send data to network routes is referred to as a node.
- Network Security refers to the level of protective measures undertaken to secure data during transmission.
- Network security protects data to ensure its confidentiality, integrity and privacy.
- The unique number which identifies a computer or device or network on the internet is called Internet Protocol (IP) Address.
- Port is an address which is assigned to every application running on a computer which utilises the internet for communication.
- Secure Protocols usually make use of cryptography and encryption techniques to secure and encrypt data.
- Passive Attacks and Active Attacks are the common network attacks.
- The devices used by network administrators to safeguard their network are called network security devices. For example, Unified Threat Management, Encipherment, Digital Signature, etc.

GLOSSARY

Network: A network can be defined as a group of two or more computers or electronic devices which are connected together for the efficient exchange of information and resources.

Wired Network: It refers to a network where devices are connected through cables to switches, which are in turn connected to network router for accessing the internet.

Wireless Network: It refers to a network where devices are connected through radio waves to an access point, which is in turn connected to a router, for accessing the external network.

Security: In simple words, it refers to the state of being safe or free from danger. However, in terms of computer science, security refers to the level to which a program or device is safe from unauthorized use.

Computer Security: It refers to protection of computer systems through tools, measures and techniques, in order to protect data and evade hackers, data theft or unauthorized use.

Network Security: It refers to the level of protective measures undertaken to secure data during transmission.

Internet Security: It refers to the level of protective measures undertaken to secure activities conducted over the internet.

Network Protocol: Protocols enables transmission of data between various devices on the same network and allows internal devises on a network to communicate irrespective of differences in their internal configuration, structure or design.

IP Address: The unique number which identifies a computer or device or network on the internet is called Internet Protocol (IP) Address. When a computer connects to the internet through internet service provider (ISP), this IP address enables the identification and location of the computer device. IP address may affect the kind of information that you may receive over the internet.

Nodes and Hosts: A node is a term which is used to refer to any computer or device which is connected to a network. A host refers to any device having an IP address which requests or provides networking resources to other hosts or nodes connected to a network.

Protocols: Protocols enables transmission of data between various devices on the same network and allows internal devises on a network to communicate irrespective of differences in their internal configuration, structure or design.

Suppose, a computer which uses IP Protocol may not be able to communicate with a computer which does not use the same protocol. This is where standardized protocols help to establish communication by serving as a common language for computers.

Data Packets: Data which is transmitted through the internet is organised into smaller chunks, called data packets. The Computer/device is able to understand the final output of data sent via data packets, with help of protocols.

Domain Name: A domain name refers to the address of a website which a user types into the web browser. Domain name allows a user to connect to the server that hosts a website's data and services, in the absence of an IP address.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What is meant by network security? What are the goals of network security?
2. What is the difference between intranet and extranet?
3. Discuss the different types of active attacks.
4. Explain the Internet Suite Protocol.
5. Differentiate between a hub and a switch.
6. Write short notes on: (a) Firewalls, (b) Security Devices, (c) Internet and (d) Protocols.
7. What is the use of a bridge in a network connection?
8. Explain different types of network security devices.

LIST OF FURTHER READINGS

- Network Security Tutorial by APNIC, Available at: https://training.apnic.net/wpcontent/uploads/sites/2/2016/12/TSEC01.pdf
- William Stallings, "Cryptography and Network Security- Principles and Practice", Seventh Edition, Pearson, Delhi
- Cryptography and Network Security – by Atul Kahate – TMH
- Data Communications and Networking- by Behourz A Forouzan
- Cyber Security Operations Handbook – by J.W. Rittiaghouse and William M.Hancok – Elseviers.