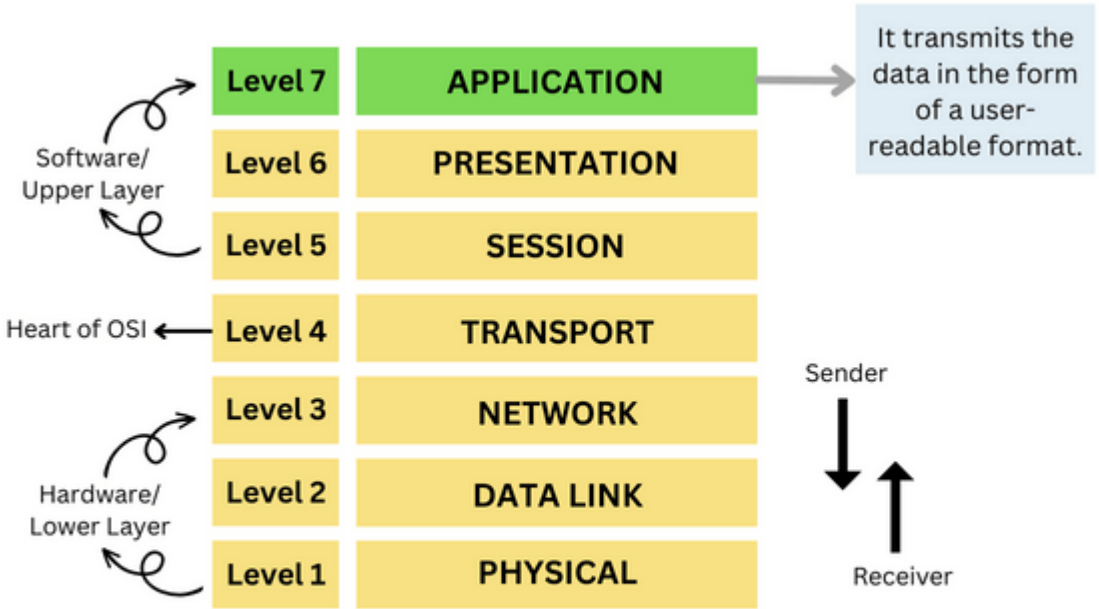
UNIT-V

Application Layer in OSI Model

The application layer is the last and 7th layer from the bottom of the OSI model. It is a layer through which the end user can communicate directly with the software. The application layer transmits the data in the form of a user-readable format. It provides many services to the user. It transfers data to the presentation layer. Furthermore, it either provides services to the presentation layer or takes services from the presentation layer.

Not only that, but it is the responsibility of the application layer that the communication between two hosts is taken place smoothly without any disturbance. The application layer ensures that the required media is available on both hosts. It determines which protocol is to be used while communicating between the hosts.

It delivers the standard interface that applications can use to transmit and obtain information to communicate with each other over the network. The application layer includes different protocols that are used in email communication, file transfer, web browsing, and more. These protocols deliver a standardized method for applications to convey messages to each other.



The OSI Model: Application Layer

Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	Hypertext Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

Functions of the application layer in the OSI model

- The application layer determines the communication partner to whom data will be transmitted.
- This layer specifies the availability of resources, i.e., it checks whether adequate network resources are available or not.
- This layer delivers protocols that are accountable for creating seamless transmission between applications.
- This layer serves as an interface between user applications and the network.
- This layer delivers directory services, which means it permits access to any sort of data from a distributed database.
- This layer delivers several facilities to the users for multiple email forwarding and storage facilities.
- This layer lets users log into a remote host and access any type of application.
- This layer lets the user access the files in the remote host.
- This layer provides email services.
- This layer provides file transfer access and management.
- This layer communicates with the operating system and guarantees that data is saved properly.
- This layer enables users to communicate with other software applications.

Protocols of the application layer in the OSI model:

- ***SMTP:*** It is an abbreviation for Simple Mail Transfer Protocol which is a TCP/IP protocol used to organize email. With the use of this protocol, data is sent from one email address to another. It is accountable for the transmission of email messages over the Internet. It is a valid protocol for ensuring the delivery of email messages. It also provides security for email transmission by supporting authentication mechanisms.

One of the most popular application layer protocols for network services is electronic mail (e-mail). The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP).

SMTP transfers messages from senders' mail servers to the recipients' mail servers using TCP connections. In SMTP, users are based on e-mail addresses. SMTP provides services for mail exchange between users on the same or different computers.

Following the client/server model:

  - SMTP has two sides: a client-side, which executes on a sender's mail server, and a server-side, which executes on the recipient's mail server.
  - Both the client and server sides of SMTP run on every mail server.
  - When a mail server sends mail (to other mail servers), it acts as an SMTP client.
  - When a mail server receives mail (from other mail servers), it acts as an SMTP server.

- ***HTTP:*** It is an abbreviation for Hypertext Transfer Protocol that allows users to access Internet data. It is accountable for the conversation between the client and the web server. When a user requests data, the browser transmits an HTTP request to a server hosting the data. The server replies with an HTTP response, which holds the requested data or an error notification if the data is not found or cannot be accessed.
- ***FTP:*** It is the short form for File Transfer Protocol which is used to send files between server and client using the internet. It uses a client-server model, where the client requests a file, and the server responds with the requested file. It uses TCP to share data as TCP delivers error-free transmission of data.

  FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another. FTP differs from other client-server applications because it establishes 2 connections between hosts. Two connections are Data Connection and Control Connection.

  Data Connection uses PORT 20, and control connection uses PORT 21. FTP is built on a client-server architecture and uses separate control and data connections between the

client and the server. One connection is used for data transfer, the other for control information (commands and responses). The FTP is data reliably and efficiently.

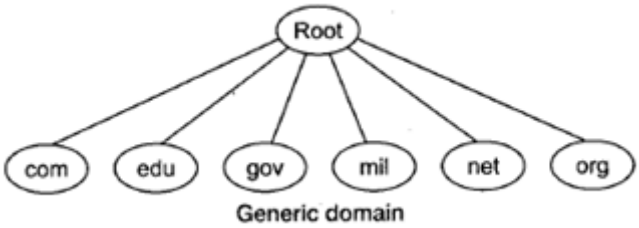
- ***TFTP:*** It is the short form for Trivial File Transfer Protocol. It is a User Datagram Protocol (UDP) based protocol, which means it is unreliable and connectionless. It transmits all commands and data over a single UDP port. It is used when a lightweight and fast file transfer protocol is required. It is uncomplicated to use and configure.
- ***DNS:*** It is the short form for Domain Name System that translates human-readable domain names into IP addresses so that web browsers can comprehend what a user desires to access on the Internet.

  In Domain Name System (DNS), TCP/IP protocol uses the IP address that uniquely identifies a host's connection to the Internet to identify an entity. DNS is a hierarchical system based on a distributed database that uses a hierarchy of Name Servers to resolve Internet host names into the corresponding IP addresses required for packet routing by issuing a DNS query to a name server.

  DNS in the Internet: DNS is a protocol that can be used on different platforms.

  Domain name space is divided into three categories.

  Generic Domain: The generic domain defines registered hosts according to their generic behavior. Each node in the tree defines a domain which is an index to the domain name space database.



Generic domain

- ***SNMP:*** It is an abbreviation for Simple Network Management Protocol used for managing and monitoring network devices and systems. Using this protocol, network administrators gather data about network performance, identify and troubleshoot problems, and remotely configure network tools.
- ***TELNET:*** TELNET is an application layer protocol in which a client-server application allows a user to log onto a remote machine and lets the user access any application program on a remote computer. TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.

On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine. TELNET is a protocol that provides a general, bi-directional, eight-bit byte-oriented communications facility. Many application protocols are built upon the TELNET protocol. Telnet services are used on PORT 23.

- ***DHCP:*** DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.

- ***POP(Post Office Protocol)*** is also called the POP3 protocol. This is a protocol used by a mail server in conjunction with SMTP to receive and holds mail for hosts.POP3 mail server receives e-mails and filters them into the appropriate user folders.
- When a user connects to the mail server to retrieve his mail, the messages are downloaded from the mail server to the user's hard disk.

Conclusion:

- In this article, you have studied the Application Layer in OSI Model. It is the 7th layer in the OSI model which provides communication to end-user applications. The primary role of this layer is to support interoperability between applications on different devices on a network.
- You have learned about the functions of the application layer, such as file transfer, email services, directory services, and remote login.
- You have gained knowledge of several protocols of the application layer, such as Simple Mail Transfer Protocol (SMTP), Telecommunication Network (TELNET), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), and Simple Network Management Protocol (SNMP).

Overview of Services

Service	Type	Direction
DNS	UDP	Out
HTTP/HTTPS	TCP	Out
FTP	TCP/UDP	Out
TELNET	TCP/UDP	Out
POP3	TCP	Out
SMTP	TCP	Out
IRCU	TCP/UDP	Out
IDENT	TCP	In
Private File Service	TCP/UDP	In/Out
NNTP	TCP/UDP	Out
NTP	TCP/UDP	Out
Remote Desktop	TCP/UDP	In/Out

Application Layer Protocol Examples

Examples of application layer protocols include the X.400 Message Handling Service Protocol allowing email transfer between compatible systems.

- The Simple Network Management Protocol (SNTP) provides remote host management.
- Use the Hypertext Transfer Protocol (HTTP) for message or text communications.
- To accept and store mail for hosts, a mail server employs the POP (Post Office Protocol) protocol in conjunction with SMTP.

Network Security

Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

What is Network Security?

All the measures used to safeguard a computer network's integrity and the data on it are collectively referred to as network security. Network security is crucial because it protects sensitive data from online threats and guarantees the network's dependability. Multiple security measures are used in successful network security plans to shield users and organizations from malware and online threats like distributed denial of service.

Computers, servers, wireless networks, and other associated devices make up a network. Many of these gadgets are open to possible intruders. Utilizing a range of hardware and software tools on a network or as software as a service is necessary for network security. As networks get increasingly complicated and businesses rely more on their networks and data to operate, security becomes more crucial. As threat actors develop new ways to target these more complex networks, security techniques must change.

Security is typically described as everyone's duty since every user on the network represents a potential vulnerability in that network, regardless of the exact method or business security plan.

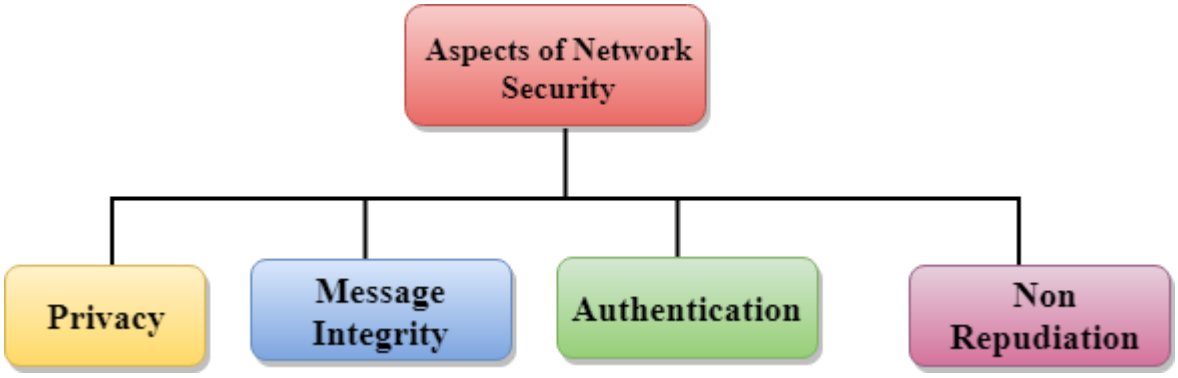
Advantages of Network Security

- Network security is essential for safeguarding client data and information, maintaining the security of shared data, guaranteeing dependable network performance, and defending against online attacks.

- An effective network security solution lowers overhead costs and protects businesses from significant losses brought on by a data breach or other security event.
- Ensuring appropriate access to systems, applications, and data facilitates company operations and customer service.

Aspects of Network Security

Following are the desirable properties to achieve secure communication:



- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
- **End-point authentication:** Authentication means that the receiver is sure of the sender?s identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

How is Network Security Implemented?

Hardware and software technologies are used in conjunction to ensure network security. Network security's main objective is to stop unauthorized access to or communication inside a network.

A security officer or team decides upon an organization's network security plans and policies to assist the organization in meeting security requirements. These security guidelines must be followed by everyone using the network. Data can be compromised anywhere in the network where an authorized user could access it, whether by a violent actor or by a negligent or mistaken user.

In the modern environment, no method can guarantee complete security. However, measures may be taken to protect data when it is sent across an unprotected network or the internet. The most popular method is cryptography.

Encrypting plain-text data using cryptography makes it more difficult to decipher and understand. Today, a variety of cryptographic algorithms are accessible, as follows:

1. Secret Key Cryptography:

The sender and the receiver share one secret key. The data is encrypted at the sender's end using this secret key. Data is encrypted before being transferred to the recipient via a public network. The recipient may readily decipher the encrypted data packets because they are both aware of and possess the Secret Key.

The Data Encryption Standard (DES) is an illustration of secret key encryption. It is challenging to administer Secret Key encryption since each computer on the network needs a unique key.

2. Public Key Cryptography

Each user in this encryption scheme has a unique Secret Key that is not kept in the common domain. The secret key is kept from the public. Every user has a unique but public key in addition to a secret key. Senders encrypt the data using a public key that is always made available to the public. Using the user's personal Secret Key, he can quickly decode the encrypted data once he receives it. Rivest-Shamir-Adleman (RSA), a kind of public key encryption, is an illustration.

3. Message Digest

In this approach, a hash value is computed and delivered in place of actual data. The second end user generates its hash value and contrasts it with the most recent one. It is approved if both hash values match; otherwise, it is refused.

Message Digest example using MD5 hashing. It is mostly utilized in authentication processes when server passwords are compared against user passwords.

Tools and Software for Network Security

Network to network, and with time, there are changes in the security tools and rules available. Strong security frequently requires various strategies, sometimes known as layered security or defence, to provide organizations with the most feasible security controls. The following are some examples of frequently used tools and software for network security:

1. Firewalls

Web pages, pop-ups, and other service entry and departure decisions are made by firewalls, which are guardian services or devices. Depending on the needs, these firewalls utilize a preset set of rules to help block or allow traffic. Depending on the requirements of the system, firewalls might be either software- or hardware-based, or both.

2. Access Control

Access control enables businesses to stop unauthorized people and devices from connecting to a specific network and to stop prospective attackers from accessing sensitive data. This limits network access to users who are authorized to utilize the specified resources.

3. Virtual Private Networks (VPN)

In most cases, a VPN encrypts the communication between an endpoint device and a network via the internet. Additionally, VPN enables experts to verify the connection between the network and the device. As a consequence, an online tunnel that is encrypted and safe is created.

4. Intrusion Prevention Systems

Intrusion prevention systems scan network traffic to identify and stop assaults. This is accomplished by connecting network activity with databases of attack methods that experts are familiar with.

5. Wireless Security

In comparison to wireless networks, wired networks could be more secure. It would help if you had control over the computers and people who may access the network of your business. It would help if you had wireless security, especially in light of the fact that fraudsters are increasingly extorting people for their private information.

6. Application Security

Applications' weak points may be tracked down and secured using a combination of software, hardware, and processes, which makes it harder for hackers to access your network.

7. Behavioural Analysis

You need to have a solid understanding of the typical behaviour of your network if you want to be able to spot abnormalities and different network breaches as they happen. Different behavioural analytics solutions are available that may quickly identify unusual activity.

Problems with Network Security

There are several difficulties in maintaining network security, such as the following:

- **Changing attack techniques on networks:** The rapidity at which cyberattacks develop presents the largest challenge to network security. As technology advances, threat actors and their techniques are continuously changing. For instance, emerging technologies like blockchain have given rise to new malware assaults like cryptojacking. Network security defence tactics must thus change to counter these fresh dangers.
- **User compliance:** Every network user is accountable for security, as was previously stated. It may be challenging for organizations to make sure that everyone is following the best practices for network security while also adapting those tactics to deal with the most recent threats.
- **Mobile and remote access:** As more businesses implement BYOD policies, there will be a larger and more complicated network of devices for organizations to secure. Additionally, remote work is becoming common. Given that users are more likely to access business networks over a personal or public network, wireless security is now even more crucial.
- **Partners from outside parties:** A company's network is frequently accessed by cloud service providers, managed security service providers, and security product suppliers, creating additional potential security flaws.

Best Tools for Network Security

The following is a list of some of the security software, hardware, and tools required to guarantee that the network is, in fact, secure:

1. Wireshark
2. Nessus
3. Snort
4. Netcat
5. Metasploit
6. Aircrack
7. BackTrack
8. Cain and Abel

Attack against Network Security

Cybercriminals' malicious attempts to undermine a network's security are known as network security attacks. These assaults are the main causes of the critical need for network security. These assaults on the network infrastructure must be stopped via network security. Let's find out more about these types of assaults so you can determine how to stop them.

Attack Types in Network Security

The following list includes a few of the several network security attack types:

1. Virus

It is a malicious file that may be downloaded, and after a user has opened it, it begins to overwrite the computer's code with a new set of codes. The system files on the computer will become corrupt as the infection spreads, which may cause the files on other computer systems in the network to become corrupt as well.

2. Malware

It is one of the swiftest, most severe, and worst attack methods that aid in gaining unauthorized access to a system or network of systems. The majority of malware is self-replicating, which means that once it infects one system, it may quickly infect all other computers linked to the network through the internet. Malware can corrupt any external device that is plugged into the system.