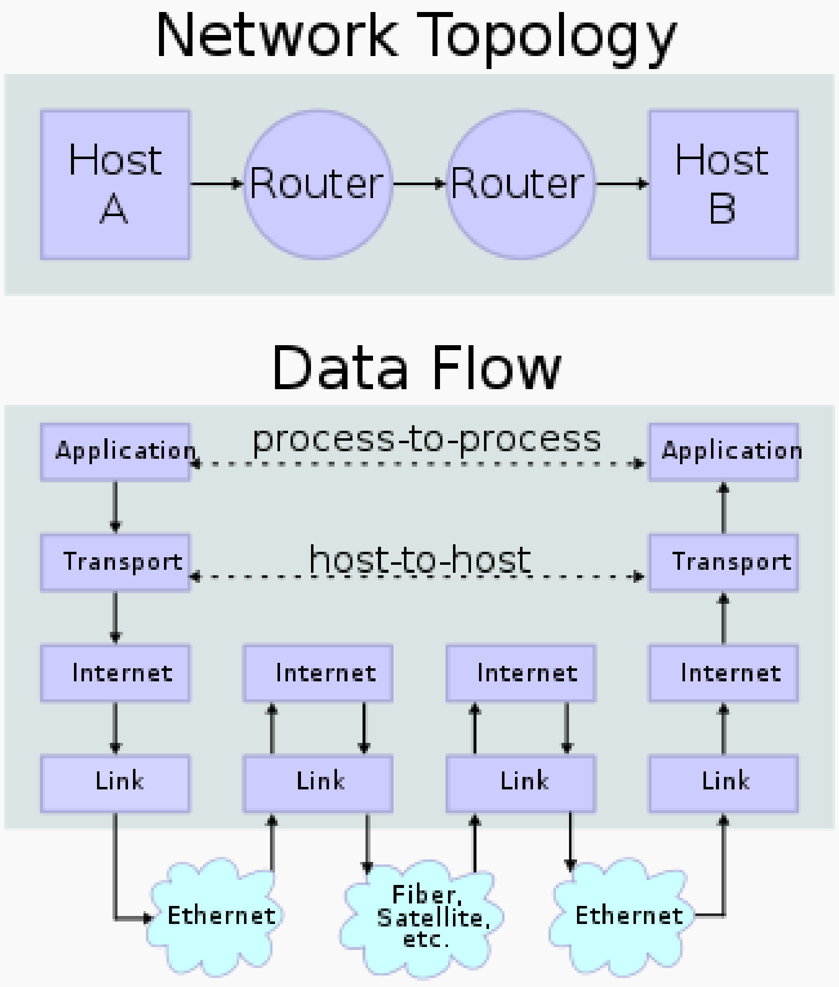
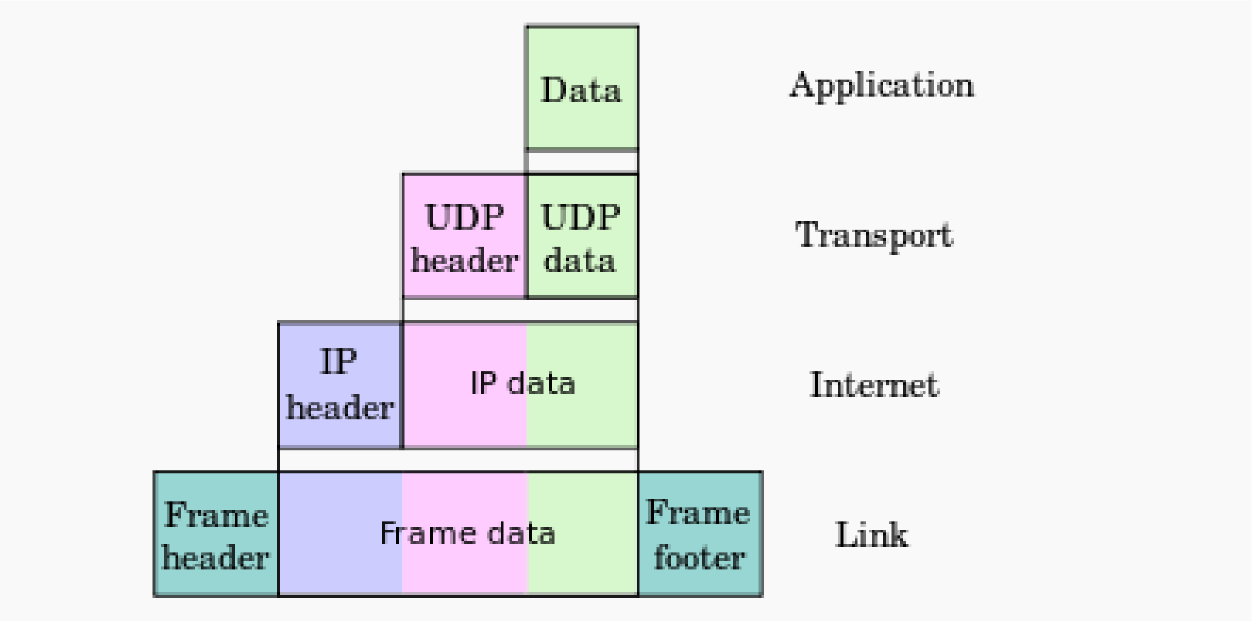
Brief Introduction to TCP/IP

- The **Internet protocol suite** is the computer networking model and set of communications protocols used on the Internet and similar computer networks.
- It is commonly known as**TCP/IP**, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP).



Two Internet hosts connected via two routers and the corresponding layers used at each hop. The application on each host executes read and write operations as if the processes were directly connected to each other by some kind of data pipe. Every other detail of the communication is hidden from each process. The underlying mechanisms that transmit data between the host computers are located in the lower protocol layers.



TCP/IP PROTOCOL SUITE

Communications between computers on a network is done through protocol suits. The most widely used and most widely available protocol suite is TCP/IP protocol suite. A protocol suit consists of a layered architecture where each layer depicts some functionality which can be carried out by a protocol. Each layer usually has more than one protocol options to carry out the responsibility that the layer adheres to. TCP/IP is normally considered to be a 4 layer system. The 4 layers are as follows :

1. Application layer
2. Transport layer
3. Network layer
4. Data link layer

1. Application layer

This is the top layer of TCP/IP protocol suite. This layer includes applications or processes that use transport layer protocols to deliver the data to destination computers.

At each layer there are certain protocol options to carry out the task designated to that particular layer. So, application layer also has various protocols that applications use to communicate with the second layer, the transport layer. Some of the popular application layer protocols are :

- HTTP (Hypertext transfer protocol)
- FTP (File transfer protocol)
- SMTP (Simple mail transfer protocol)
- SNMP (Simple network management protocol) etc

2. Transport Layer

This layer provides backbone to data flow between two hosts. This layer receives data from the application layer above it. There are many protocols that work at this layer but the two most commonly used protocols at transport layer are TCP and UDP.

TCP is used where a reliable connection is required while UDP is used in case of unreliable connections.

TCP divides the data(coming from the application layer) into proper sized chunks and then passes these chunks onto the network. It acknowledges received packets, waits for the acknowledgments of the packets it sent and sets timeout to resend the packets if acknowledgements are not received in time. The term 'reliable connection' is used where it is not desired to loose any information that is being transferred over the network through this connection. So, the protocol used for this type of connection must provide the mechanism to achieve this desired characteristic. For example, while downloading a file, it is not desired to loose any information(bytes) as it may lead to corruption of downloaded content.

UDP provides a comparatively simpler but unreliable service by sending packets from one host to another. UDP does not take any extra measures to ensure that the data sent is received by the target host or not. The term 'unreliable connection' are used where loss of some information does not hamper the task being fulfilled through this connection. For example while streaming a video, loss of few bytes of information due to some reason is acceptable as this does not harm the user experience much.

3. Network Layer

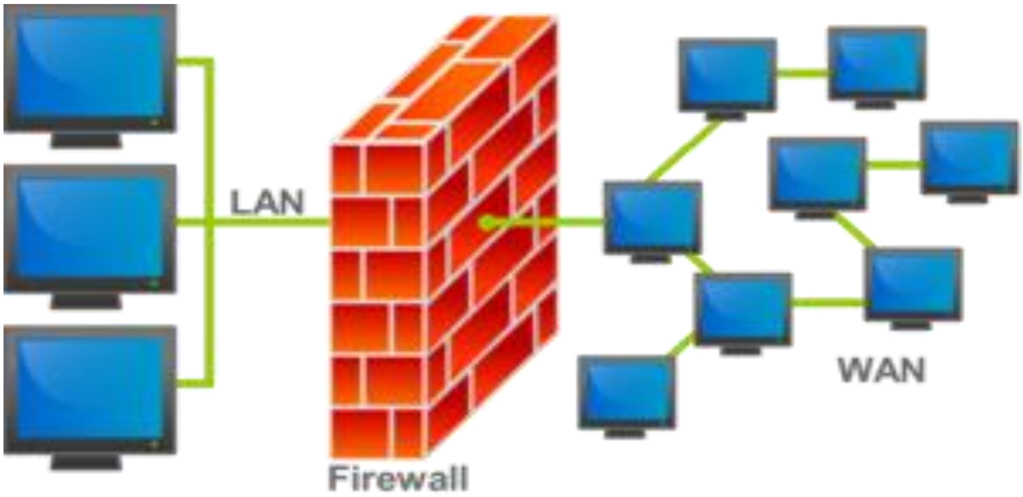
This layer is also known as Internet layer. The main purpose of this layer is to organize or handle the movement of data on network. By movement of data, we generally mean routing of data over the network. The main protocol used at this layer is IP. While ICMP(used by popular 'ping' command) and IGMP are also used at this layer.

4. Data Link Layer

This layer is also known as network interface layer. This layer normally consists of device drivers in the OS and the network interface card attached to the system. Both the device drivers and the network interface card take care of the communication details with the media being used to transfer the data over the network. In most of the cases, this media is in the form of cables. Some of the famous protocols that are used at this layer include ARP(Address resolution protocol), PPP(Point to point protocol) etc.

Firewall

- In computing, a **firewall** is a network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted.
- Firewalls exist both as a software solution and as a hardware appliance.



- There are different types of firewalls

Network layer or packet filters
Application-layer
Proxies

Network layer firewall

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply.

Application layer firewall

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

Proxy server

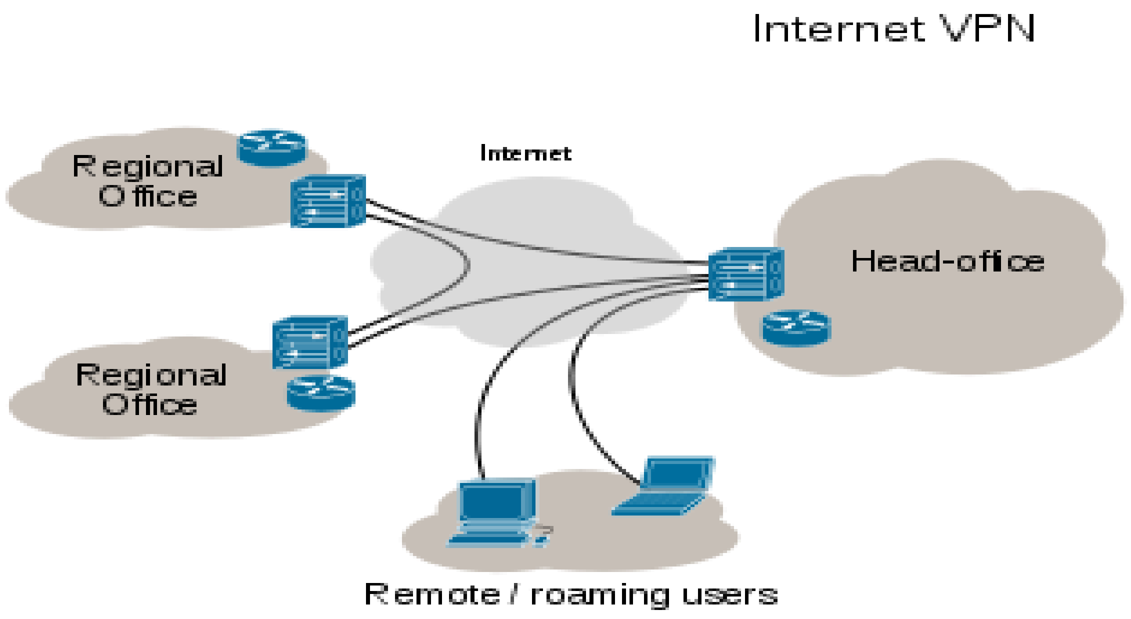
A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

Virtual Private Network.

A **virtual private network** (**VPN**) extends a private network across a public network, such as the Internet

It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.



A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.

A well-designed VPN provides a business with the following benefits:

- Extended connections across multiple geographic locations without using a leased line
- Improved security for exchanging data
- Flexibility for remote offices and employees to use the business intranet over an existing Internet connection as if they're directly connected to the network
- Savings in time and expense for employees to commute if they work from virtual workplaces
- Improved productivity for remote employees

Secure Transport Protocol

Two main secure Transport protocol

1. **S-HTTP**
2. **SSL**

S-HTTP

- **Secure Hypertext Transfer Protocol (S-HTTP)** is a little-used alternative to the HTTPS URI scheme for encrypting web communications carried over HTTP.
- Web browsers typically use HTTP to communicate with web servers, sending and receiving information without encrypting it.
- For sensitive transactions, such as Internet e-commerce or online access to financial accounts, the browser and server must encrypt this information.
- HTTPS and S-HTTP were both defined in the mid-1990s to address this need.
- S-HTTP encrypts only the served page data and submitted data like POST fields, leaving the initiation of the protocol unchanged. Because of this, S-HTTP could be used concurrently with HTTP (unsecured) on the same port, as the unencrypted header would determine whether the rest of the transmission is encrypted.

SSL

- **Secure Sockets Layer (SSL),** are cryptographic protocols designed to provide communication security over the Internet.
- SSL (Secure Sockets Layer) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- a protocol developed by Netscape for transmitting private documents via the Internet.
- SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message.
- EX. many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Secure Electronic payment protocol:

SETP

Secure Electronic Transaction protocol:

- **Secure Electronic Transaction (SET**) was a communications protocol standard for securing credit card transactions over insecure networks, specifically, the Internet**.**
- SET was developed by the SET Consortium, established in 1996 by VISA and MasterCard in cooperation with GTE, IBM, Microsoft,Netscape, SAIC, Terisa Systems, RSA, and VeriSign.
- SET allowed parties to identify themselves to each other and exchange information securely. Binding of identities was based on X.509certificates with several extensions.

To meet the business requirements, SET incorporates the following features:

- **Confidentiality of information**
- **Integrity of data**
- **Cardholder account authentication**
- **Merchant authentication**

A SET system includes the following participants:

- **Cardholder**
- **Merchant**
- **Issuer**
- **Acquirer**
- **Payment gateway**
- **Certification authority**

Certification for Authentication:-

- In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates.
- A digital certificate certifies the ownership of a public key by the named subject of the certificate.
- In this model of trust relationships, a CA is a trusted third party - trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.
- A CA issues digital certificates that contain a public key and the identity of the owner. The matching private key is not made available publicly, but kept secret by the end user who generated the key pair.
- The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate
- A certificate authority (CA) is an organization that stores public keys and their owners and every party in a communication trusts this organization (and knows its public key).
- When the user's web browser receives the public key from website it also receives a digital signature of the key (with some more information, in a so-called X.509 certificate)
- Website uses a public key that the certification authority certifies, a fake website can only use the same public key. Since the fake website does not know the corresponding private key, it cannot create the signature needed to verify its authenticity.

IP Security

- Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
- IPsec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*)
- Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks.
- IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite.

The IPsec suite is an open standard. IPsec uses the following protocols to perform various functions

- **Authentication Headers (AH)** provide connectionless integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- **Encapsulating Security Payloads (ESP)** provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.
- **Security Associations (SA)** provide the bundle of algorithms and data that provide the parameters necessary to AH and/or ESP operations.