Chapter 1

TCP/IP Protocol Suite:

What is a Protocol ?

A protocol is a set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another.

What is a Protocol Suite ?

A protocol suite is a collection of protocols that are designed to work together.

Before TCP/IP became the de-facto standard other protocol suites like IPX and SPX were common (Novell).

Protocol Stacks

It is possible to write a single protocol that takes data from one computer application and sends it to an application on another computer.- A Single stack Protocol

The problem with this approach is that it very inflexible, as any changes require changing the entire application and protocol software.

The approach used in networking is to create layered protocol stacks.

Each level of the stack performs a particular function and communicates with the levels above and below it.

The OSI and TCP/IP Networking Models

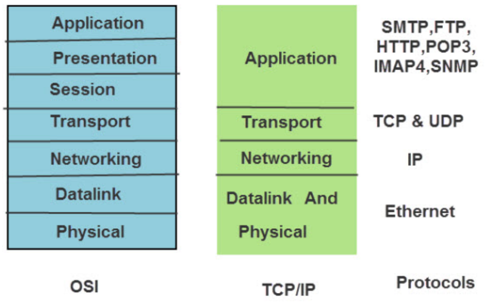
It is important to understand that this model provides for a conceptual framework, and no modern protocols implement this model fully.

The TCP/IP protocol suite uses a 4 layer model.

Note: The OSI model is an idealised networking model, whereas the TCP/IP model is a practical implementation.

The diagram shows how the TCP/IP and OSI models compare

OSI & TCP/IP Protocol-Stacks and Protocols



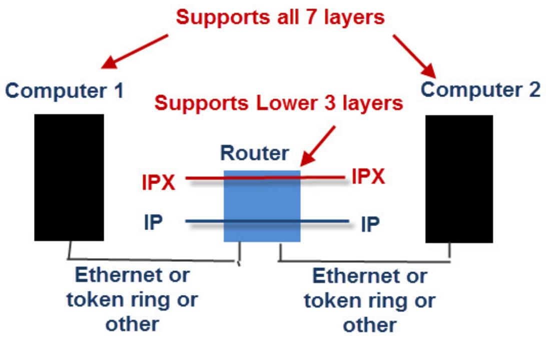
End to End Connections- Routers,Switches and OSI

When two computers communicate across a network the data must travel through various items of networking equipment.

You will often hear the terms level 2 and level 3 equipment used. These terms refer to the OSI levels of the protocol stack that the device operates at.

A router for example works at the networking layer and is a level 3 device.

A switch operates at the Ethernet level and is a level 2 device.



End To End Connections and OSI

Because a router operates at the networking layer it doesn't need to support the upper layer application protocols like HTTP,FTP etc.

The router works on network address which are part of the networking protocol (IP or IPX).

A router can route many different protocols at the same time, but it doesn't do protocol conversion.

An IP packet coming in will be an IP packet going out and an IPX packet coming in will be an IPX packet going out.

To do protocol conversion you will need a Gateway.

Likewise a switch doesn't have level 3,4,5,6 or 7 protocol stacks as it doesn't need them, and so it doesn't care about the routing protocol IP,IPX etc or the application FTP,HTTP etc that passes through it.

Because the switch operates at level 2 (data link layer) it only needs to understand the MAC addresses that are part of the Ethernet protocol.

Internet Protocol (IP)

Internet Protocol (IP) – a set of rules that dictate how data should be delivered over the public network (Internet). Often works in conjunction with the transmission control protocol (TCP), which divides traffic into packets for efficient transport through the Internet; together they are referred to as TCP/IP.

For example, when an email (using the simple mail transfer protocol – SMTP) is sent from an email server, the TCP layer in that server will divide the message up into multiple packets, number them and then forward them to the IP layer for transport. At the IP layer, each packet will be transported to the destination email server. While each packet is going to the same place, the route they take to get there may be different. When it arrives, the IP layer hands it back to the TCP layer, which reassembles the packets into the message and hands it to the email application, where it shows up in the Inbox.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a Media Access Control or MAC address.

The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol (IP) in use today, an IP address is 32-bits long, but MAC addresses are 48-bits long.

Reverse Address Resolution Protocol (RARP)

RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address

Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

RARP is available for Ethernet, Fiber Distributed-Data Interface, and token ring LANs.

Internet Control Message Protocol (ICMP)

Since IP does not have a inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.
e.g. the requested service is not available or that a host or router could not be reached.

Internet Group Management Protocol (IGMP)

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

Using the Open Systems Interconnection (OSI) communication model, IGMP is part of the Network layer. IGMP is formally described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2236.

UDP (User Datagram Protocol)

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss-tolerating connections between applications on the internet. Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. But there are important differences between the two.

Where UDP enables process-to-process communication, TCP supports host-to-host communication. TCP sends individual packets and is considered a reliable transport medium; UDP sends messages, called datagrams, and is considered a best-effort mode of communications.

In addition, where TCP provides error and flow control, no such mechanisms are supported in UDP. UDP is considered a connectionless protocol because it doesn't require a virtual circuit to be established before any data transfer occurs.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. TCP has emerged as the dominant protocol used for the bulk of internet connectivity due to its ability to break large data sets into individual packets, check for and resend lost packets, and reassemble packets in the correct sequence. But these additional services come at a cost in terms of additional data overhead and delays called latency.

In contrast, UDP just sends the packets, which means that it has much lower bandwidth overhead and latency. With UDP, packets may take different paths between sender and receiver and, as a result, some packets may be lost or received out of order.

TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control and -- because it is meant to provide error-free data transmission -- handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the transport layer, and parts of Layer 5, the session layer.

TCP is used for organizing data in a way that ensures the secure transmission between the server and client. It guarantees the integrity of data sent over the network, regardless of the amount. For this reason, it is used to transmit data from other higher-level protocols that require all transmitted data to arrive. Examples include:

- Secure Shell (SSH), File Transfer Protocol (FTP), Telnet: For peer-to-peer file sharing, and, in Telnet's case, logging into another user's computer to access a file.
- Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP): For sending and receiving email
- HTTP: For web access

SCTP (Stream Control Transmission Protocol)

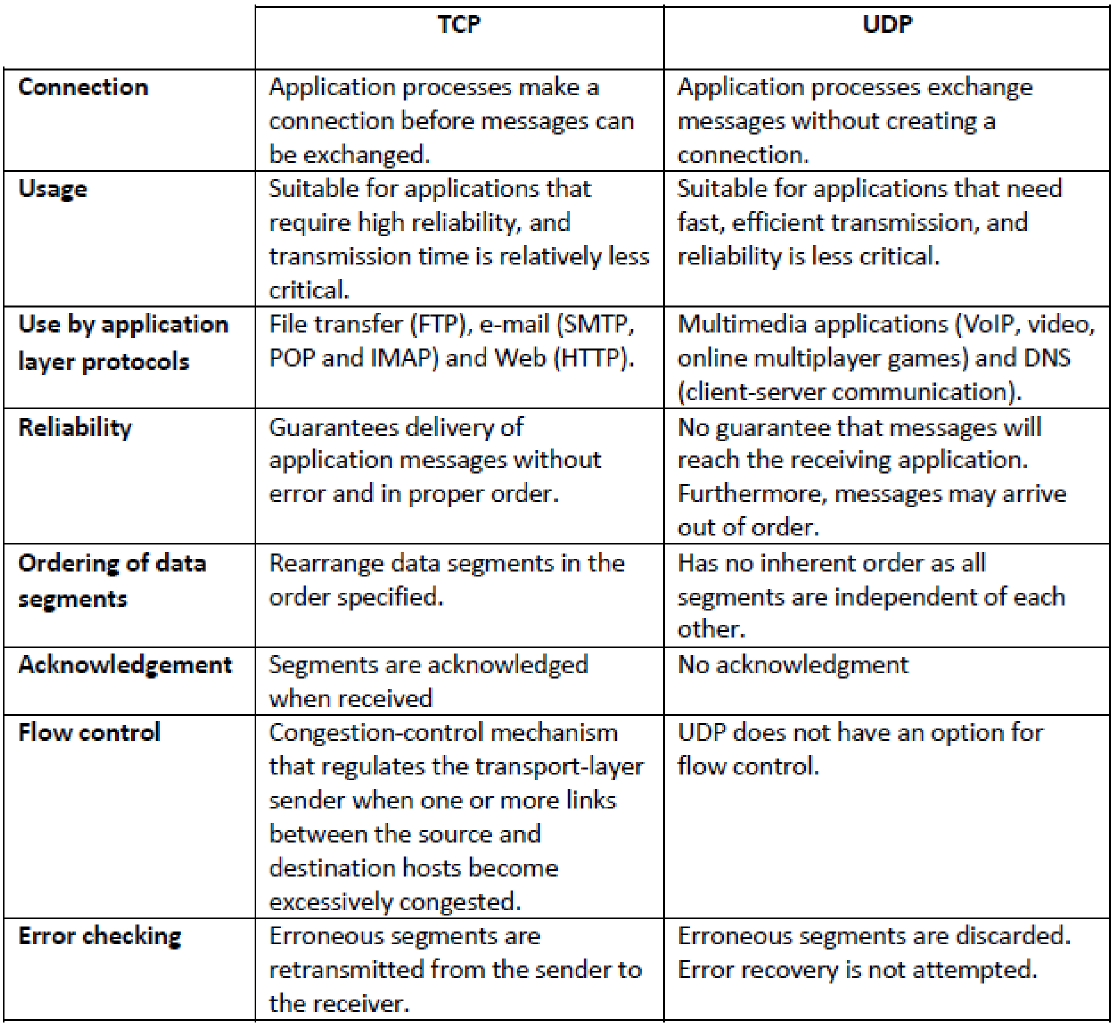
SCTP (Stream Control Transmission Protocol) is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network. Sometimes referred to as "next generation TCP" (Transmission Control Protocol) - or TCPng, SCTP is designed to make it easier to support a telephone connection over the Internet (and specifically to support the telephone system's Signaling System 7 - SS7 - on an Internet connection). A telephone connection requires that signaling information (which controls the connection) be sent along with voice and other data at the same time. SCTP also is intended to make it easier to manage connections over a wireless network and to manage the transmission of multimedia data.

Like TCP, SCTP manages "reliable transport" (ensuring the complete arrival of data units that are sent over the network) over the Internet's basically connectionless Internet Protocol (IP), the protocol responsible for moving the data but not for managing whether all the data arrives. Unlike TCP, SCTP ensures the complete concurrent transmission of several streams of data (in units called messages) between connected end points. SCTP also supports multihoming, which means that a connected end point can have alternate IP addresses associated with it in order to route around network failure or changing conditions.

Apple Talk

AppleTalk is a set of local area network communication protocols originally created for Apple computers. An AppleTalk network can support up to 32 devices and data can be exchanged at a speed of 230.4 kilobits per second (Kbps). Devices can be as much as 1,000 feet apart. AppleTalk's Datagram Delivery Protocol corresponds closely to the Network layer of the Open Systems Interconnection (OSI) communication model.

TABLE 1: COMPARISON OF UDP AND TCP



	TCP	UDP
Connection	Application processes make a connection before messages can be exchanged.	Application processes exchange messages without creating a connection.
Usage	Suitable for applications that require high reliability, and transmission time is relatively less critical.	Suitable for applications that need fast, efficient transmission, and reliability is less critical.
Use by application layer protocols	File transfer (FTP), e-mail (SMTP, POP and IMAP) and Web (HTTP).	Multimedia applications (VoIP, video, online multiplayer games) and DNS (client-server communication).
Reliability	Guarantees delivery of application messages without error and in proper order.	No guarantee that messages will reach the receiving application. Furthermore, messages may arrive out of order.
Ordering of data segments	Rearrange data segments in the order specified.	Has no inherent order as all segments are independent of each other.
Acknowledgement	Segments are acknowledged when received	No acknowledgment
Flow control	Congestion-control mechanism that regulates the transport-layer sender when one or more links between the source and destination hosts become excessively congested.	UDP does not have an option for flow control.
Error checking	Erroneous segments are retransmitted from the sender to the receiver.	Erroneous segments are discarded. Error recovery is not attempted.

Subnetting

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). Subnetting helps to reduce the network traffic and conceals network complexity. Subnetting is essential when a single network number has to be allocated over numerous segments of a local area network (LAN).

Subnets were initially designed for solving the shortage of IP addresses over the Internet.

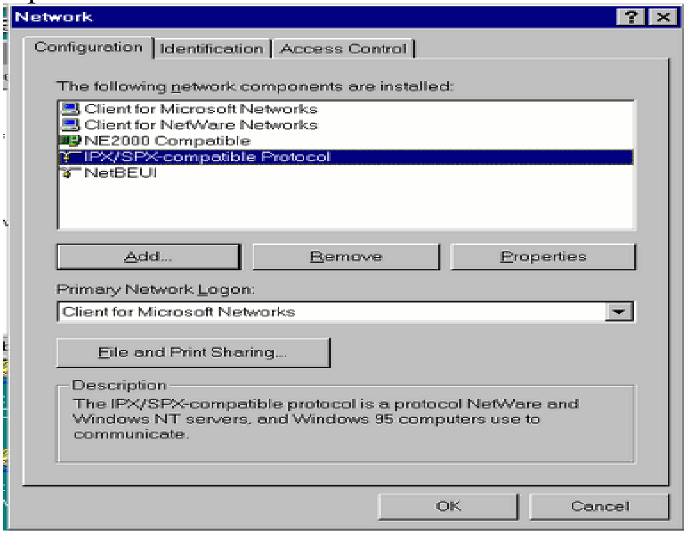
Supernetting

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

IPX/SPX – Compatible Protocol

IPX/SPX stands for Internetwork Packet Exchange/Sequenced Packet Exchange is a set of network protocols that provide packet switching and sequencing for small and large networks, used initially on networks using the Novell NetWare operating systems. Shortly after, they became widely used on networks deploying Microsoft Windows LANs, as they replaced NetWare LANs.



The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- NE2000 Compatible
- IPX/SPX-compatible Protocol
- NetBEUI

Primary Network Logon: Client for Microsoft Networks

Description

The IPX/SPX-compatible protocol is a protocol NetWare and Windows NT servers, and Windows 95 computers use to communicate.

IPX works at layer 3 of the Open Systems Interconnection (OSI) model and SPX works at layer 4.

Microsoft’s version of the Novell NetWare IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protocol for Microsoft Windows 95, Windows 98, and Windows 2000 is called IPX/SPX-Compatible Protocol.

IPX/SPX-Compatible Protocol supports the 32-bit Windows Sockets 1.1 and NetBIOS over Internetwork Packet Exchange (IPX) programming interfaces.