TCP/IP REFERENCE MODEL

TCP/IP Model:

The U.S. Department of Defense (DOD) created the TCP/IP reference model because it wanted a network that could survive any conditions

Application Layer:

The application layer handles high-level protocols, representation, encoding, and dialog control. The TCP/IP protocol suite combines all application related issues into one layer. It ensures that the data is properly packaged before it is passed on to the next layer. TCP/IP includes Internet and transport layer specifications such as IP and TCP as well as specifications for common applications. TCP/IP has protocols to support file transfer, e-mail, and remote login, in addition to the following:

- **File Transfer Protocol (FTP)** – FTP is a reliable, connection-oriented service that uses TCP to transfer files between systems that support FTP. It supports bi-directional binary file and ASCII file transfers.
- **Trivial File Transfer Protocol (TFTP)** – TFTP is a connectionless service that uses the User Datagram Protocol (UDP). TFTP is used on the router to transfer configuration files and Cisco IOS images, and to transfer files between systems that support TFTP. It is useful in some LANs because it operates faster than FTP in a stable environment.
- **Network File System (NFS)** – NFS is a distributed file system protocol suite developed by Sun Microsystems that allows file access to a remote storage device such as a hard disk across a network.
- **Simple Mail Transfer Protocol (SMTP)** – SMTP administers the transmission of e-mail over computer networks. It does not provide support for transmission of data other than plain text.
- **Telnet** – Telnet provides the capability to remotely access another computer. It enables a user to log into an Internet host and execute commands. A Telnet client is referred to as a local host. A Telnet server is referred to as a remote host.
- **Simple Network Management Protocol (SNMP)** – SNMP is a protocol that provides a way to monitor and control network devices. SNMP is also used to manage configurations, statistics, performance, and security.
- **Domain Name System (DNS)** – DNS is a system used on the Internet to translate domain names and publicly advertised network nodes into IP addresses.

Transport Layer:

The transport layer provides a logical connection between a source host and a destination host. Transport protocols segment and reassemble data sent by upper-layer applications into the same data stream, or logical connection, between end points.

- Creates packet from bytes stream received from the application layer.
- Uses port number to create process to process communication.

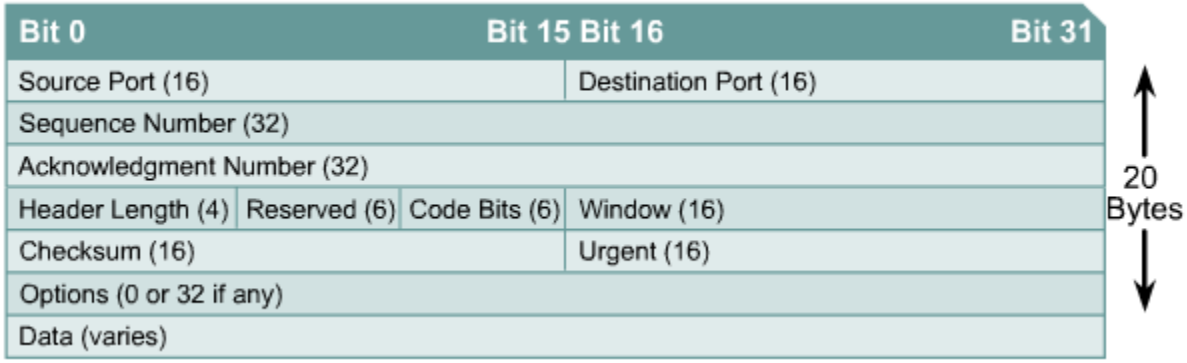
- Uses a sliding window protocol to achieve flow control.
- Uses acknowledgement packet, timeout and retransmission to achieve error control.

The primary duty of the transport layer is to provide end-to-end control and reliability as data travels through this cloud. This is accomplished through the use of sliding windows, sequence numbers, and acknowledgments. The transport layer also defines end-to-end connectivity between host applications. Transport layer protocols include TCP and UDP.

TCP is a connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. In a connection-oriented environment, a connection is established between both ends before the transfer of information can begin. TCP breaks messages into segments, reassembles them at the destination, and resends anything that is not received. TCP supplies a virtual circuit between end-user applications.

TCP Header Format:

TCP uses only a single type of protocol data unit, called a **TCP segment**. The header is shown in Figure . Because one header must serve to perform all protocol mechanisms, it is rather large, with a minimum length of 20 octets.



The following protocols use TCP:

- FTP
- HTTP
- SMTP
- Telnet

The following are the definitions of the fields in the TCP segment:

- **Source port** – Number of the port that sends data
- **Destination port** – Number of the port that receives data
- **Sequence number** – Number used to ensure the data arrives in the correct order
- **Acknowledgment number** – Next expected TCP octet
- **HLEN** – Number of 32-bit words in the header
- **Reserved** – Set to zero
- **Code bits** – Control functions, such as setup and termination of a session
- **Window** – Number of octets that the sender will accept
- **Checksum** – Calculated checksum of the header and data fields
- **Urgent pointer** – Indicates the end of the urgent data

- **Option** – One option currently defined, maximum TCP segment size
- **Data** – Upper-layer protocol data

Code Bits or Flags (6 bits).

- URG: Urgent pointer field significant.
- ACK: Acknowledgment field significant.
- PSH: Push function.
- RST: Reset the connection.
- SYN: Synchronize the sequence numbers.
- FIN: No more data from sender.

UDP (User Datagram Protocol):

UDP is the connectionless transport protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without guaranteed delivery. It relies on higher-layer protocols to handle errors and retransmit data.

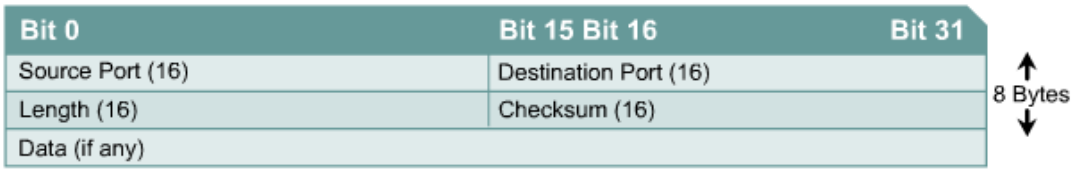


Fig: UDP Datagram

UDP does not use windows or ACKs. Reliability is provided by application layer protocols. UDP is designed for applications that do not need to put sequences of segments together.

The following protocols use UDP:

- TFTP
- SNMP
- DHCP
- DNS

The following are the definitions of the fields in the UDP segment:

- **Source port** – Number of the port that sends data
- **Destination port** – Number of the port that receives data
- **Length** – Number of bytes in header and data
- **Checksum** – Calculated checksum of the header and data fields
- **Data** – Upper-layer protocol data

TCP vs UDP:

S.no	TCP - Transmission Control Protocol	UDP - User Datagram Protocol
1	connection-oriented, reliable (virtual circuit)	connectionless, unreliable, does not check message delivery
2	Divides outgoing messages into segments	sends “datagrams”
3	reassembles messages at the destination	does not reassemble incoming messages
4	re-sends anything not received	Does-not acknowledge.

5	provides flow control	provides no flow control
6	more overhead than UDP (less efficient)	low overhead - faster than TCP
7	Examples:HTTP, NFS, SMTP	Eg. VOIP,DNS,TFTP

Internet Layer:

The purpose of the Internet layer is to select the best path through the network for packets to travel. The main protocol that functions at this layer is IP. Best path determination and packet switching occur at this layer.

The following protocols operate at the TCP/IP Internet layer:

- IP provides connectionless, best-effort delivery routing of packets. IP is not concerned with the content of the packets but looks for a path to the destination.
- Internet Control Message Protocol (ICMP) provides control and messaging capabilities.
- Address Resolution Protocol (ARP) determines the data link layer address, or MAC address, for known IP addresses.
- Reverse Address Resolution Protocol (RARP) determines the IP address for a known MAC address.

IP performs the following operations:

- Defines a packet and an addressing scheme
- Transfers data between the Internet layer and network access layer
- Routes packets to remote hosts

Network Access Layer:

The network access layer allows an IP packet to make a physical link to the network media. It includes the LAN and WAN technology details and all the details contained in the OSI physical and data link layers.

Drivers for software applications, modem cards, and other devices operate at the network access layer. The network access layer defines the procedures used to interface with the network hardware and access the transmission medium. Modem protocol standards such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) provide network access through a modem connection. Many protocols are required to determine the hardware, software, and transmission-medium specifications at this layer. This can lead to confusion for users. Most of the recognizable protocols operate at the transport and Internet layers of the TCP/IP model.

Network access layer protocols also map IP addresses to physical hardware addresses and encapsulate IP packets into frames. The network access layer defines the physical media connection based on the hardware type and network interface.

Source : http://dayaramb.files.wordpress.com/2011/03/computer-network-notes-pu.pdf