Basics of OSI and TCPIP Layers

Introduction:

This article outlines **OSI** layers and **TCPIP** basics required for RF and Wireless Engineers. The OSI (Open system Interconnection) is developed for defining seven layers which makes two different vendors systems communicate. TCPIP is used for internet applications mainly. The figure describes how TCPIP layers map to OSI layers.

OSI and TCPIP Basics:

OSI Layers	TCP/IP Protocol Layers	TCP/IP Protocol Suit			
Layer 7 Application	Application Layer	Telnet		DNS	
Layer 6 Presentation		FTP		RIP	
Layer 5 Session		SMTP		SNMP	
Layer 4 Transport	Host-to-Host Transport Layer	TCP		UDP	
Layer 3 Network	Internet Layer	ARP	IP	ICMP	
				IGMP	
Layer 2 Data Link	Network Interface Layer	ETHER NET	TOKEN Ring	ATM	FRAME Relay
Layer 1 Physical					

In OSI layer model, control is passed from one layer to the next, starting at the Layer 7, application layer in one station, proceeding to the succeeding bottom layer and so on till information reaches Layer 1.Then the information transmitted over the channel to the next station's Layer 1 and transmitted to succeeding layers till information delivered to Layer 7. Each Layer in the OSI model does the job for the previous layer and also adds prefixes information termed as "header". The data link layer adds suffixes called cyclic redundancy check as "trailer" which is used for error detection. The brief functionality of each OSI layer is mentioned below.

Application:
All the applications for user reside at this layer. It includes FTP, Telnet, e-mail etc.
Presentation:
It formats and encrypts data to be sent across a network. Its basic task is to make application layer and network layer talk to each other by processing the data. It provides independence to the application processes from differences in data representation by way of syntax conversion.
Session:
It Provides control mechanism to connect two applications running on different machines. It covers basic function to establish, to maintain and to release connections.
Transport:
It assures reliable data communication between two hosts. It is responsible for error recovery and flow control between two hosts. It also does multiplexing and de multiplexing functionalities for transmitting and receiving host respectively.
Network:
The main function is switching and routing of the packet. It adds logical addressing to do this. It also takes care of error handling, congestion control and packet sequencing.
Data Link:
It takes care of errors in the physical layer. It provides flow control and also does frame synchronization. ARQ is implemented to take care of retransmission in case of erroneous packets. In latest today's technologies it provides Medium Access Control functionality, hence known as MAC. MAC takes care of resource assignment to the end devices wanted to seek connection to the network for various applications (voice, data, etc.).
Physical:
It mainly takes care of bit stream transmission over physical medium (cable, air etc.). It provides the hardware means of sending and receiving data through cable or wireless medium. Some wireless standards viz. wlan, wimax, zigbee, LTE defines physical layer specifications which takes care of forward error correction and modulation-demodulation functionalities as well as making the information suitable to be transmitted. Following figure mentions logical structure of the layered protocols inside a computer on an internet. This figure is taken from RFC 1180 to describe the concept.

RFC1180 describes logical structure of protocols inside a typical internet enabled device as mentioned below.
Ethernet Cable--ENET Card--ARP/IP--TCP/UDP--Network Applications
As mentioned Ethernet cable is connected directly with Ethernet card which has upper layer ARP or IP. This has upper layer TCP or UDP and above all applications are running.
Every device has its own Ethernet address which is 6 bytes and listens for Ethernet frames with that destination address. An IP address is 4 bytes. Ethernet uses CSMA/CD. CSMA/CD means that all devices communicate on a single medium in which only one can transmit at a time and they can all receive simultaneously. If two devices try to transmit at the same instant, the transmit collision is detected and both devices wait a random period of time before trying to transmit again. An Ethernet frame contains the destination address, source address, type field, and data.

Let's understand how data flows from one host A and another host B. Let us assume host A is transmitting packet and Host B is receiving it.

- As mentioned above all the hosts receive the packets and each will compare destination address in the Ethernet header with its' own Ethernet or MAC address of 6 bytes and accept the same if it matches otherwise does not pay attention.

- Next it will check for type field(2 byte long), if it is 0x806 then the packet will be passed to ARP module and if it is 0x800 it will be passed to IP module. ARP module responds to hosts seeking for Ethernet address based on their logical (IP) address.
- After packet is received by IP layer it will decide where the packet need to be routed based on routing table and destination IP address embedded in received packet's IP header. IP header is usually 20 bytes.
- If the host is the final end system then IP module checks for protocol field
- (1 byte long) in the IP header. If it is 0x06 then the packet is passed to the TCP module and if it is 0x11 then the packet is passed to the UDP module.
- Above the TCP or UDP there is application layer, where so many applications will be usually running. Information to each application will be passed based on 'destination port number' field (16 bit long) embedded inside the TCP or UDP header. TCP utilizes 'sequence number field' (32 bit long) for reassembly of all the IP data grams received at irregular time instants in irregular orders. For example FTP has dedicated port address 23 and Telnet has dedicated port address 21, which is used to deliver the data to each.
  Organizations that influence the development of TCP-IP protocol stack are summarized below.

- Internet Architecture Board (IAB), www.iab.org/
- Internet Engineering Task Force (IETF), www.ietf.org/
- Internet Society, www.isoc.org/
- The Internet Corporation of Assigned Names and Numbers (ICANN), www.icann.org/
- Internet Research Task Force (IRTF), www.irtf.org/
- World Wide Web Consortium (W3C), www.w3.org/

References:

1. RFC 1180, A TCP IP Tutorial
2. RFC793, TCP
3. RFC826, ARP
4. RFC792,ICMP
5. RFC768,UDP