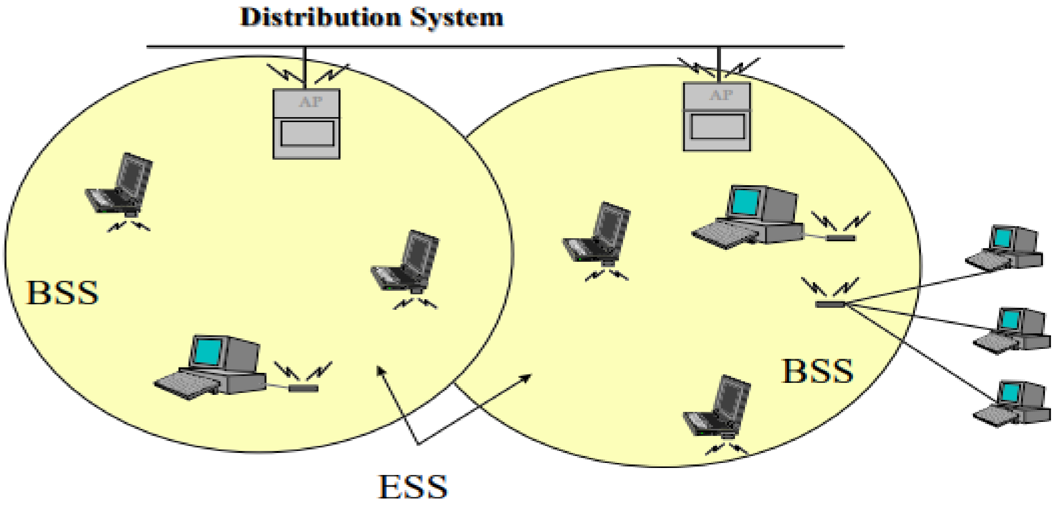
IE590 Information Engineering HW3

Q-1) Write a summary of the IEEE 802.11 protocol standard

The wireless local area network (WLAN) protocol, IEEE 802.11, and associated technologies, such as the 802.1X protocol and Wi-Fi Protected Access (WPA), allow secure high-speed wireless network access and mobile access to a network infrastructure. Until the recent development and wide adoption of IEEE 802.11b, also known as *Wi-Fi*, in order to obtain high-speed network access to your local area network (LAN) your network client needed to be physically connected to the LAN with some type of wiring.

802.11 Architecture

The 802.11 logical architecture contains several main components: station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS).
Some of the components of the 802.11 logical architecture map directly to hardware devices, such as STAs and wireless APs. The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The wireless AP functions as a bridge between the wireless STAs and the existing network backbone for network access.



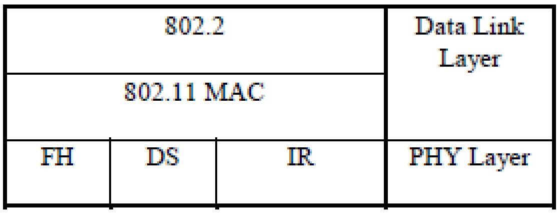
An ESS is a set of two or more wireless APs connected to the same wired network that defines a single logical network segment bounded by a router (also known as a *subnet*).

The APs of multiple BSSs are interconnected by the DS. This allows for mobility, because STAs can move from one BSS to another BSS. APs can be interconnected with or without wires; however, most of the time they are connected with wires. The DS is the logical component used to interconnect BSSs. The DS provides distribution services to allow for the roaming of STAs between BSSs.

IEEE 802.11 Layers Descriptions:

As any 802.x protocol covers the MAC and Physical layer, the standard currently defines a single MAC which interacts with 3 PHYs

- Frequency Hopping Spread Spectrum in the 2.4 GHz Band
- Direct Sequence Spread spectrum in the 2.4 GHz
- Infrared



802.2			Data Link Layer
802.11 MAC			
FH	DS	IR	PHY Layer

802.11 Protocols and Technologies:

The 802.11-related protocols and technologies are discussed in detail in the following section:

- **802.11.** The IEEE 802.11 wireless standard defines the specifications for the physical layer and the media access control (MAC) layer.

- **802.1X.** The IEEE 802.1X standard defines port-based, network access control used to provide authenticated network access for Ethernet networks.

- **Extensible Authentication Protocol (EAP) over LAN (EAPOL).** EAP is a Point-to-Point Protocol (PPP)-based authentication mechanism that was adapted for use on point-to-point local area network (LAN) segments.

- **Wired Equivalent Privacy (WEP).** WEP provides data confidentiality services by encrypting the data sent between wireless nodes.

- **Wi-Fi Protected Access (WPA).** WPA is an interim standard until the IEEE 802.11i standard is ratified. These standards, intended to be a replacement for the WEP standard, offer more robust methods of data encryption and network authentication.

Q2) Write a summary of TCP/IP and UDP protocol.

TCP/IP Protocol:

TCP/IP protocols map to a four-layer conceptual model known as the *DARPA model*, named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.

Below Figure 1.1 shows the TCP/IP protocol architecture.

(Source: https://technet.microsoft.com/en-us/library/cc958821.aspx)

Figure 1.1 shows the TCP/IP protocol architecture.

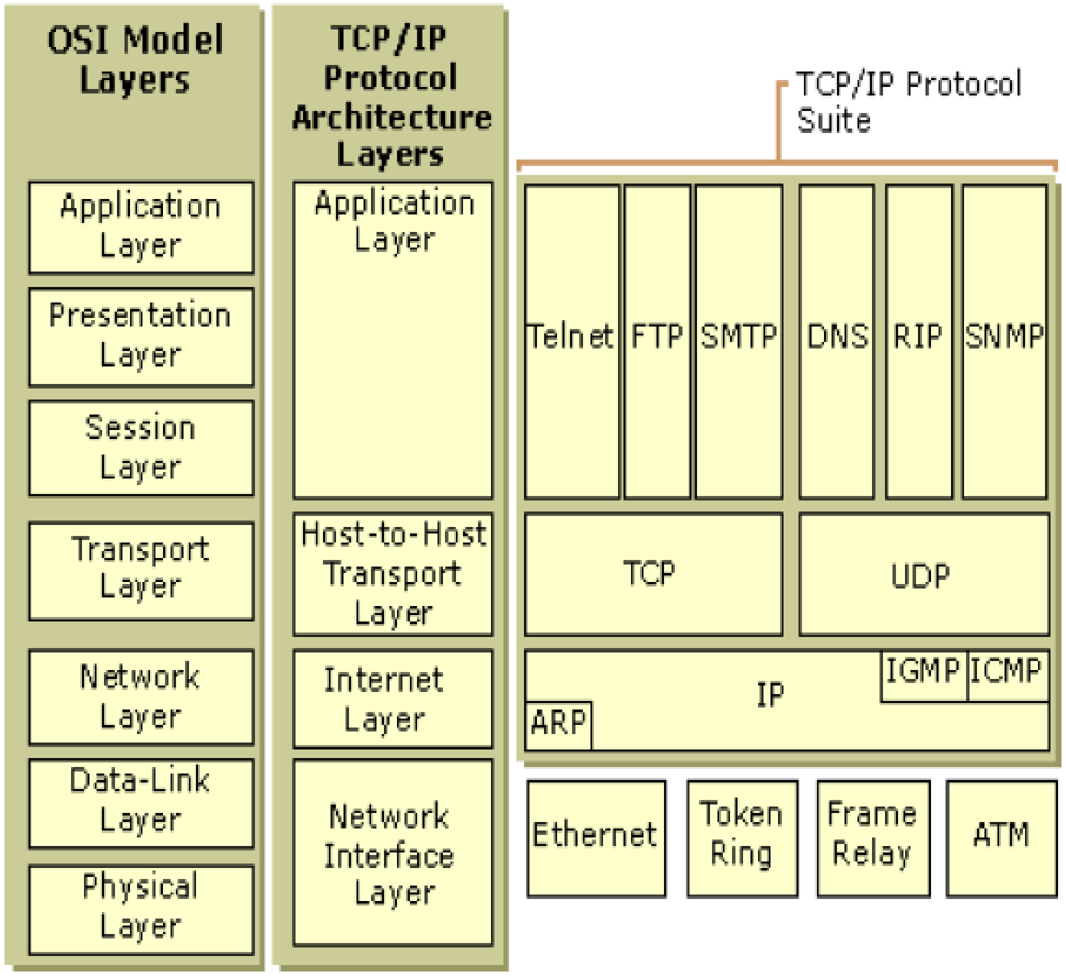


Figure 1.1 TCP/IP Protocol Architecture

1) Network Interface Layer

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium.

In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model. Note that the Internet layer does not take advantage of sequencing and acknowledgment services that might be present in the Data-Link layer. An unreliable Network Interface layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport layer.

2) Internet Layer

The *Internet layer* is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The *Internet Protocol* (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The *Address Resolution Protocol* (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The *Internet Control Message Protocol* (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The *Internet Group Management Protocol* (IGMP) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

3) Transport Layer

The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

4) Application Layer

The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (FTP) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

- The Domain Name System (DNS) is used to resolve a host name to an IP address.
- The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Examples of Application layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under Windows 2000.

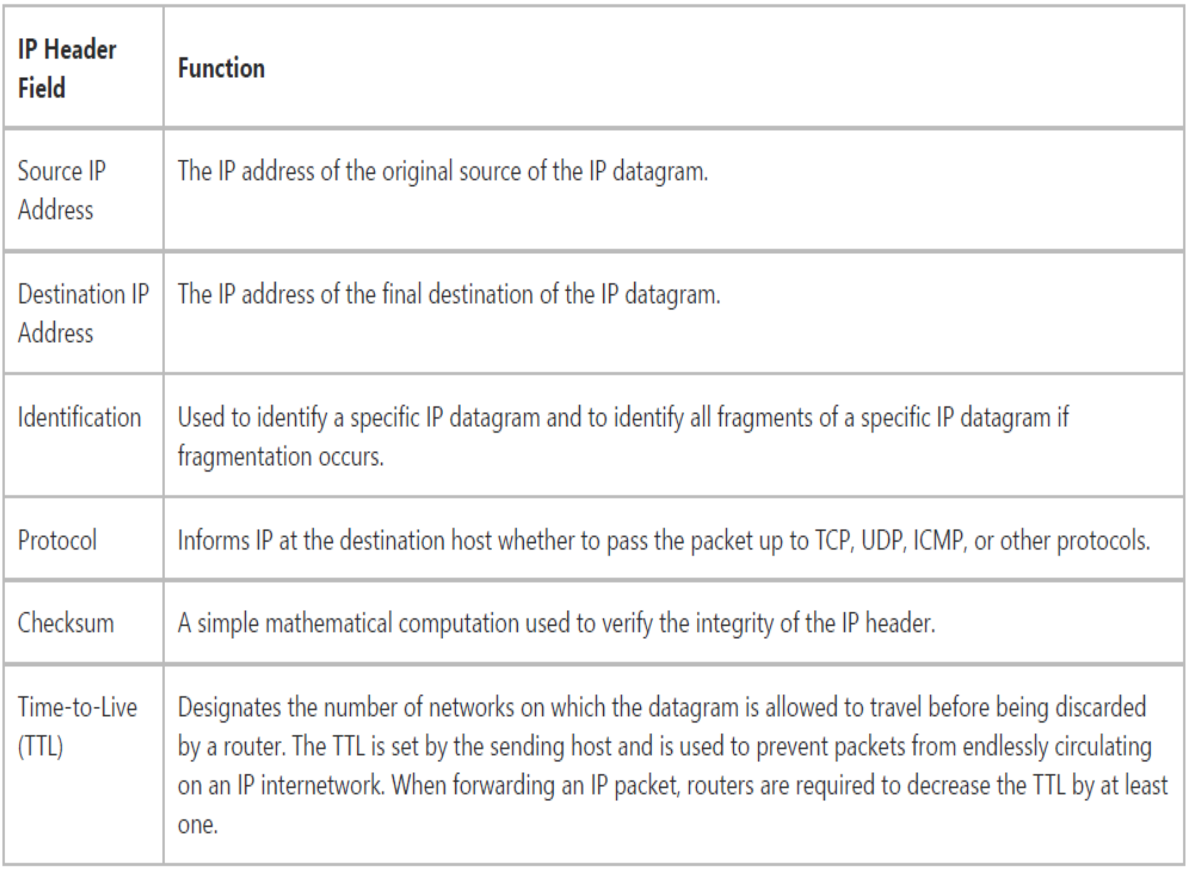
NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagrams, and name resolution.

Internet Protocols:

IP is a connectionless, unreliable datagram protocol primarily responsible for addressing and routing packets between hosts.

Connectionless means that a session is not established before exchanging data. Unreliable means that delivery is not guaranteed. IP always makes a "best effort" attempt to deliver a packet. An IP packet might be lost, delivered out of sequence, duplicated, or delayed. IP does not attempt to recover from these types of errors. The acknowledgment of packets delivered, and the recovery of lost packets is the responsibility of a higher-layer protocol, such as TCP. IP is defined in RFC 791.

An IP packet consists of an IP header and an IP payload. Below Table describes the key fields in the IP header.



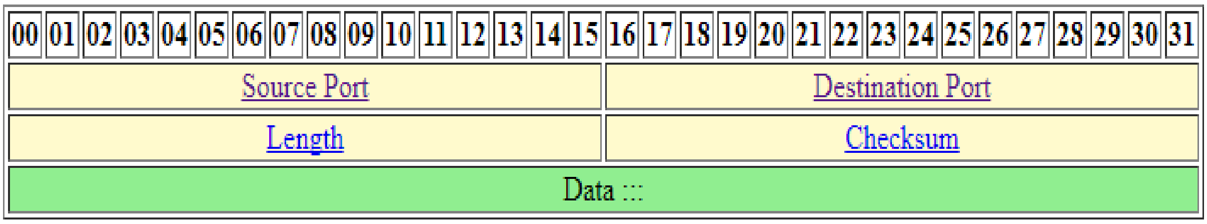
IP Header Field	Function
Source IP Address	The IP address of the original source of the IP datagram.
Destination IP Address	The IP address of the final destination of the IP datagram.
Identification	Used to identify a specific IP datagram and to identify all fragments of a specific IP datagram if fragmentation occurs.
Protocol	Informs IP at the destination host whether to pass the packet up to TCP, UDP, ICMP, or other protocols.
Checksum	A simple mathematical computation used to verify the integrity of the IP header.
Time-to-Live (TTL)	Designates the number of networks on which the datagram is allowed to travel before being discarded by a router. The TTL is set by the sending host and is used to prevent packets from endlessly circulating on an IP internetwork. When forwarding an IP packet, routers are required to decrease the TTL by at least one.

User Datagram Protocol(UDP)

The User Datagram Protocol offers only a minimal transport service -- non-guaranteed datagram delivery -- and gives applications direct access to the datagram service of the IP layer. UDP is used by applications that do not require the level of service of TCP or that wish to use communications services (e.g., multicast or broadcast delivery) not available from TCP.

UDP is almost a null protocol; the only services it provides over IP are check summing of data and multiplexing by port number. Therefore, an application program running over UDP must deal directly with end-to-end communication problems that a connection-oriented protocol would have handled -- e.g., retransmission for reliable delivery, packetization and reassembly, flow control, congestion avoidance, etc., when these are required. The complex coupling between IP and TCP will be mirrored in the coupling between UDP and many applications using UDP.

UDP header:



<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Source Port</td><td colspan="16">Destination Port</td></tr>
<tr><td colspan="16">Length</td><td colspan="16">Checksum</td></tr>
<tr><td colspan="32">Data :::</td></tr>
</table>

Source Port. 16 bits.
The port number of the sender. Cleared to zero if not used.

Destination Port. 16 bits.
The port this packet is addressed to.

Length. 16 bits.
The length in bytes of the UDP header and the encapsulated data. The minimum value for this field is 8.

Checksum. 16 bits.
Computed as the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded as needed with zero bytes at the end to make a multiple of two bytes. If the checksum is cleared to zero, then checksum is disabled. If the computed checksum is zero, then this field must be set to 0xFFFF.