Tri Pham - 8060220

Professor Szekely, D.

PROG8165 - Web Design & Development

26 Jan 2018

Investigation into OSI and TCP/IP and other protocols

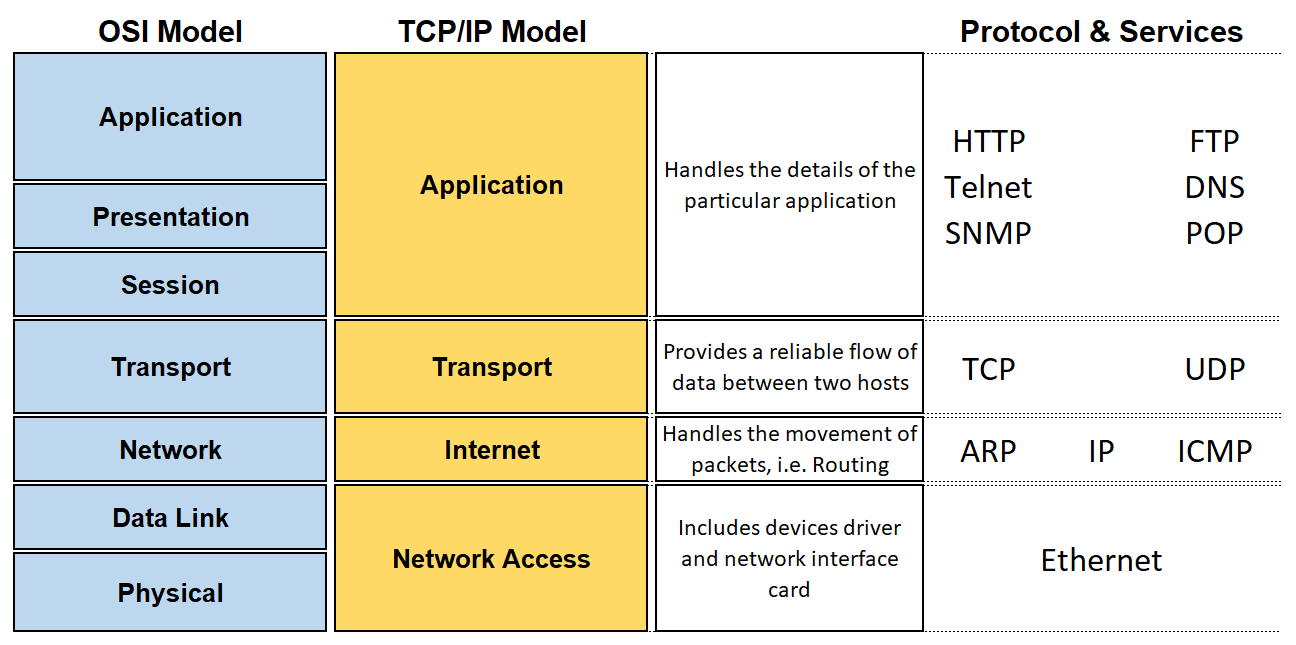
1. **Using Diagrams/written text do a comparative analysis between the OSI model and the TCP/IP model.** 
   1. **Key Differences between TCP/IP and OSI Model**

|  |  |
| --- | --- |
| **OSI (Open System Interconnection)** | **TCP/IP (Transmission Control Protocol / Internet Protocol)** |
| It has 7 layers | It has 4 layers |
| It follows vertical approach | It follows horizontal approach |
| It is a theoretical approach | It is developed for Internet |
| It is a reference model | It is the implementation of OSI model |
| It is stricter boundaries | It is not strictly defined. |
| It has separate session and presentation layers | It combines the session and presentation in the application layer. |
| Model was developed before the development of protocol | Protocol was developed first and then then model developed |
| It is independent protocol | It is dependent protocol |

* 1. **Key similarities between TCP/IP and OSI Model**

1. Both model shares a similar architecture, that means they are constructed with layers.
2. They share the common application layer
3. They have comparable transport and network layers.

Below diagram shows the sharing protocol and services between two models



1. **Describe using diagrams/written text the Transmission Control Protocol in detail, i.e. the use of ports, the TCP header, checksum, etc.**

#### **TCP**

The Transmission Control Protocol (TCP) is a protocol working between application and IP. TCP and IP are the first defined protocols and the main components to create a TCP/IP suite. TCP’s job is to identify errors while transferring IP data and to request re-send and re-arrange, and to help controlling traffic in internet. When receiving data, TCP will put packets in the right order and transfer them to the application. Hence, TCP is called a “reliable” protocol and connection-oriented. And this makes TCP working slowly and not suitable in the applications which require immediate transferring such as VoIP.

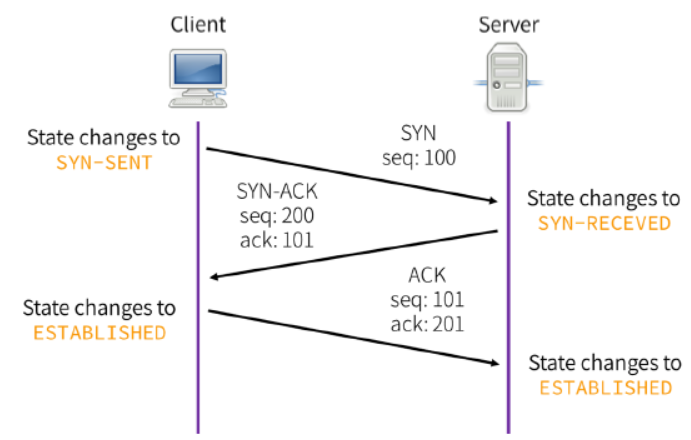
* 1. **Basic Protocol Operation**

TCP connections have three phases:

1. Connection establishment
2. Data transfer
3. Connection termination
   * 1. **Connection Establishment**

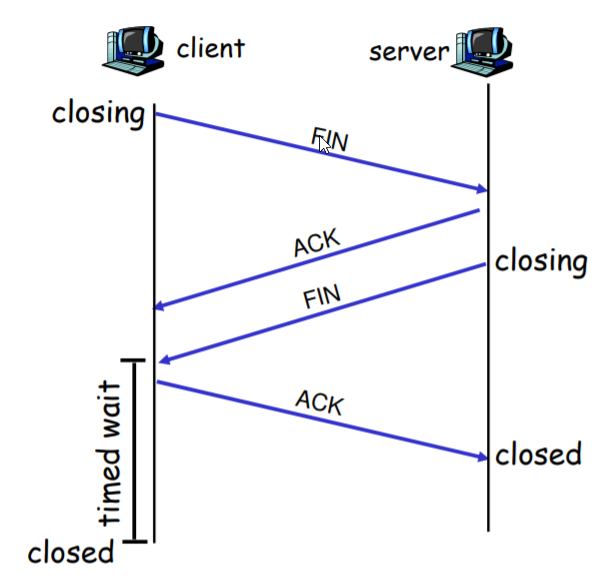
To establish a connection, TCP uses a 3-way handshake.

1. The client sends a SYN (synchronize) packet to the server, which has a random sequence number.
2. The server sends back a SYN‐ACK packet, containing a random sequence number and an ACK number acknowledging the client’s sequence number.
3. The client sends an ACK number to the server, acknowledging the server’s sequence number.
4. The sequence numbers on both ends are synchronized. Both ends can now send and receive data independently.



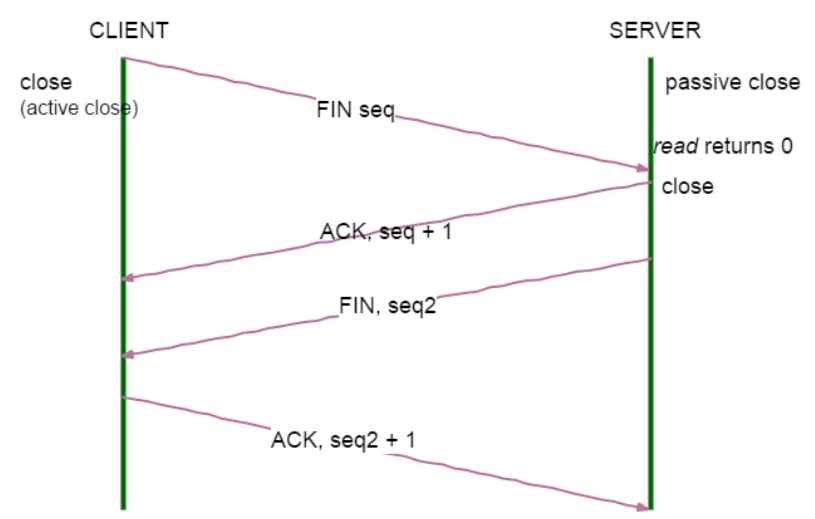
* 1. **Data transfer**

1. Client sends TCP FIN to server
2. Server receives FIN and responds ACK. Then it closes connection and sends FIN
3. Client receives FIN and responds ACK.
4. Server receives ACK, closes connection.



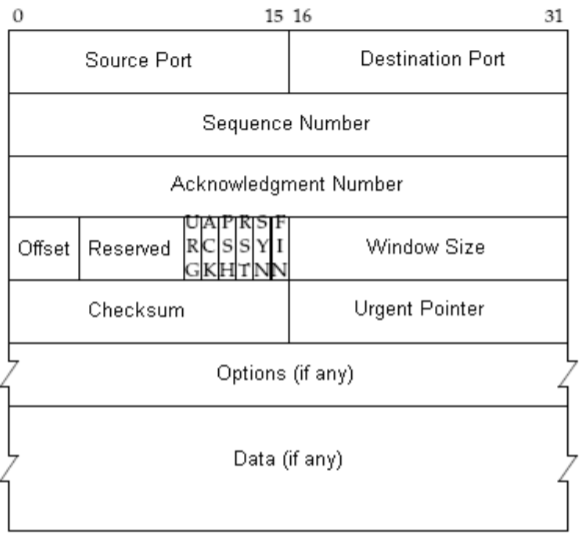
* 1. **Connection Termination**

1. One side, either client or server, calls close, and goes into active close and sends a FIN segment to the other side.
2. After receiving FIN, the other side goes into passive close. Reception of FIN is also acknowledged by TCP, after any data that may already have been queued, like an EOF (by the one in active close).
3. After some time, the side that receives the EOF will close its socket, and TCP sends another FIN.
4. The other side acknowledges the final FIN.



* 1. **TCP Packet Structure**

A TCP packet consists of two sections, header and data. All fields may not be used in every transmission. A flag field is used to indicate the type of transmission the packet represents and how the packet should be interpreted.



The header consists of these fields:

• **Source port (16 bits)**: is the address of source application.

• **Destination port (16 bits)**: is the address of destination application.

• **Sequence number (32 bits)**: is number of the first byte of segment when SYN bit is set to 1. If SYN bit is set to 1 then sequence number is the Initial Sequence Number (ISN) and the first data byte would be ISN + 1. TCP manages transferred bytes on a TCP connection through this field.

• **Acknowledgement number (32 bits)**: is the number of the next segment which client is expecting and it also shows good signal after server responds to client.

• **Data offset**: The size of the TCP header, it is also the offset from the start of the TCP packet to the data portion.

• **Reserved**: Reserved for future use, should be set to zero.

• **Flags** (also known as control bits): contains 6 1-bit flags:

- URG: Urgent pointer field is significant.

- ACK: Acknowledgement field is significant.

- PSH: Push function.

- RST: Reset the connection.

- SYN: Synchronize sequence numbers.

- FIN: No more data from sender.

• **Window**: The number of bytes the sender is willing to receive starting from the acknowledgement field value.

• **Checksum**: used for error-checking of the header and data.

1. **Describe using diagrams/written text the Internet Protocol in detail, i.e. Subnets, IP header, IP Addressing, etc.**

## **The Internet Protocol (IP)**

IP stands for Internet Protocol which covers about IP address and transferring data to the proper place.

## **What is an IP address?**

An IP address (internet protocol address) is a numerical representation that uniquely identifies a specific termination on the network (computer, router, printer…).

IP address is usually displayed in dotted-decimal format, with 4 numbers separated by periods, such as 192.168.123.132.

There are 3 ways to express an IP address:

* Decimal type: 130.57.30.56100
* Binary type: 10000010.00111001.00011110.00111000
* Hex type: 82 39 1E 38

An IP address includes two parts: Node Address (first part of an IP address) and Network address (last part of an IP address)

Network address is an unique number to identify a network. Node address is an unique number to specify a computer in a network.

For example:

192.168.123. Network  
 .132 Host

-or-

192.168.123.0 network address.  
 0.0.0.132 host address.

#### **Subnet Masks**

The subnet mask is to separate a big network into smaller multiple networks for reorganization and security purposes.

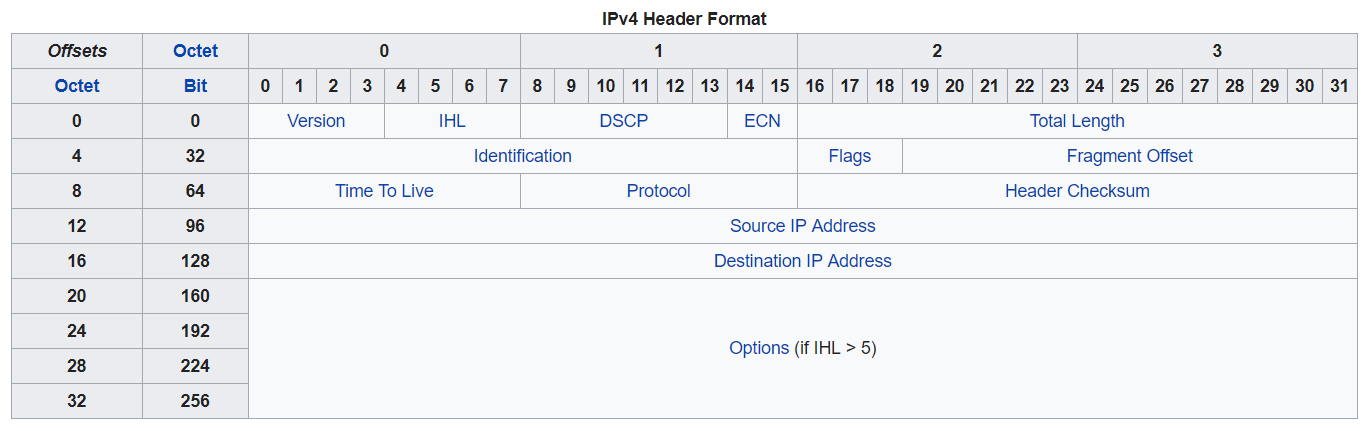
The bits of the subnet mask are defined as follows:

* All bits that correspond to the network ID are set to 1.
* All bits that correspond to the host ID are set to 0.

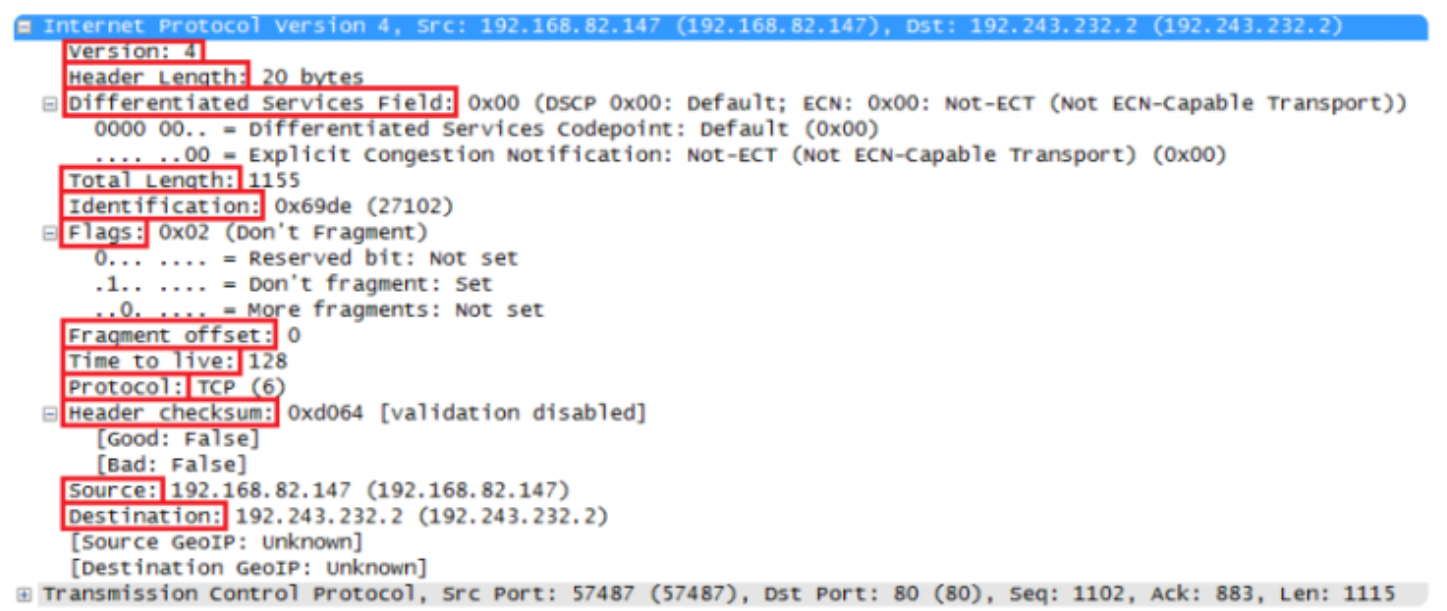
Subnet masks are specified based on classes of IP addresses:

|  |  |  |
| --- | --- | --- |
| Address Class | Subnet mask (bits) | Subnet mask |
| A | 11111111 00000000 00000000 00000000 | 255.0.0.0 |
| B | 11111111 11111111 00000000 00000000 | 255.255.0.0 |
| C | 11111111 11111111 11111111 00000000 | 255.255.255.0 |

#### **IP Header**



For example:



* **Version**: indicates version of IP protocol: IPv4 (0100) or IPv6 (0110). If it is IPv4 then value is 4.
* **Header length**: shows the length of IP header. Minimum value is 20 bytes and maximum value is 60 bytes.
* **Differentiated Services Code Point (DSCP)**: Originally defined as the Type of service (ToS) field. This indicates how to handle data and priority of IP packet.
* **Total** **length**: defines the entire packet size in bytes. Minimum size is 20 bytes and maximum size is 65535 bytes.
* **Identification**: If IP packet is fragmented then the fragments of a single packet will use the same 16 bits identification to identify which IP packet that they belong to.
* **IP Flag**: these 3 bits are used to identify fragments:
  + Bit 0 is always zero.
  + Bit 1 is called as DF (Don’t Fragment):
    - * DF = 1: The packet is fragmented, there are more than one fragment.
      * DF = 0: The packet is not fragmented.
  + Bit 2 is called as MF (More Fragment) bit:
    - * MF = 0: This is the last fragment.
      * MF = 1: This is not the last fragment, there are more segments coming.
* Fragment Offset: indicates the location of fragments of the first fragmented packet.
* Time to live: when the datagram arrives at a router, its TTL field will decrease by one. When the TTL field equals zero, the router discards the packet and typically sends an ICMP Time Exceeded message to the sender. TTL has 8 bits so the value is 255.
* Protocol: Indicates protocol in the data portion, such as TCP or UDP.
* Header checksum: is used for error-checking of the header. When a packet arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If the values do not match, the router discards the packet
* Source address: address of sender.
* Destination address: address of receiver.
* IP option: The options field is not often used.

1. **Examine the different Protocols that are used in various layers of the models (UDP, ARP, SMTP, HTTP, PPP etc.) pick at least 10 different ones and using simple diagrams/written text describe these succinctly, no more than one to three sentences each.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Application layer** | | | |
|  | Protocol | Common Port | Description |
|  | HTTP | 80 | Hypertext Transfer Protocol is often called the protocol of the Internet.  HTTP received this designation because most Internet traffic is based on HTTP.  When a user requests a Web resource, it is requested using HTTP. |
|  | SMTP | 25 | Simple Mail Transfer Protocol is a standard electronic-mail protocol that handles the sending of mail from one SMTP to another SMTP server. |
|  | FTP | 20, 21 | The **File Transfer Protocol** is used to connect to remote computers, list shared files, and either upload or download files between local and remote computers. |
|  | POP3 | 110 | Post Office Protocol 3 is used for electronic messaging across the Internet.  POP3 is a protocol that involves both a server and a client.  A POP3 server receives an e-mail message and holds it for the user. |
| **Transport layer** | | | |
|  | Protocol | Description t | |
|  | TCP | Transmission Control Protocol uses a reliable delivery system to deliver layer 4 segments to the destination. This would be analogous to using a certified, priority, or next-day service with the Indian Speed Post Service. | |
|  | UDP | UDP uses a best-effort delivery system, like how first class and lower postal services of the Indian Postal Service work. With a first-class letter (post card), you place the destination address and put it in your mailbox, and hope that it arrives at the destination. | |
| **Network layer** | | | |
|  | Protocol | Description | |
|  | ARP | The Address Resolution Protocol (ARP) is an Internet layer protocol that helps TCP/IP network components find other devices in the same broadcast domain. | |
|  | IPX/SPX | Internetwork Packet Exchange/Sequenced Packet Exchange developed by Novell and is used primarily on networks that use the Novell NetWare network operating system.  The IPX and SPX protocols provide services like those offered by IP and TCP.  Like IP, IPX is a connectionless network layer protocol. | |
| **Data link layer** | | | |
|  | Protocol | Description | |
|  | FDDI | Fiber Distributed Data Interface, shares many of the same features as token ring, such as a token passing, and the continuous network loop configuration. | |
|  | PPP | The Point-to-Point Protocol (PPP) is used to establish a direct connection between two nodes.  It connects two routers directly without any host or any other networking device in between.  It can provide connection authentication, transmission encryption and compression. | |
| **Physical layer** | | | |
|  | Protocol | Description | |
|  | ISDN | Integrated Services Digital Network adapters can be used to send voice, data, audio, or video over standard telephone cabling. | |
|  | Modems | Modems can be external, connected to the computers serial port by an RS-232 cable or internal in one of the computers expansion slots.  Modems connect to the phone line using standard telephone RJ-11 connectors. | |

Works cited

“Similarities between OSI Reference and TCP/IP Reference Model”, <https://www.studytonight.com/computer-networks/comparison-osi-tcp-model.php>

“What Are The Similarities Between Osi And Tcp/ip Model”

<https://triptofrence.wordpress.com/2017/06/02/what-are-the-similarities-between-osi-and-tcpip-model/>

Fujitsu, “The TCP/IP Protocol Suite”, December 20, 2006 http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf>

“Communication Networks/TCP and UDP Protocols”, Wikibooks, 8 September 2017

<https://en.wikibooks.org/wiki/Communication\_Networks/TCP\_and\_UDP\_Protocols>

“IP Address”

<https://www.paessler.com/it-explained/ip-address>

HIMANSHU ARORA , “IP Protocol Header Fundamentals Explained with Diagrams”, MARCH 26, 2012

<https://www.thegeekstuff.com/2012/03/ip-protocol-header/>

“Types Of Network Protocols Explained With Functions”, 22 December 2017

<https://www.computernetworkingnotes.com/networking-tutorials/types-of-network-protocols-explained-with-functions.html>