OLD DOMINION UNIVERSITY

CYSE 301: CYBERSECURITY TECHNIQUES AND OPERATIONS

FALL 2017

Module I
Traffic Tracing and Analysis

Topic 1: Introduction of Network Architecture

1. Introduction

In this module, we are going to learn about the basic network structures and the way of simple network defense and countermeasures. As a network administrator, if we want to set up and maintain a simple functionality and security network, we are not only need to master the fundamental knowledge of the network but also need to operate and configure the network facility such as the switch, router and firewall in the field and track the trace of the package through the network to deeply understand how to do cyber defense from the very beginning. Also, as a network administrator, one essential ability is to capture and analyze network traffic. This can be important to identify the cause of bottleneck, determining who is responsible for certain intrusion.

2. Objective

The objective of this topic is to review the ISO (International Standard Organization) OSI (Open Systems Interconnection) reference model for computer communications basic network architecture before tracking and analysis the data traffic. A focus is placed on the analysis of protocols at different layers, network architectures, and networking systems performance analysis. The following subtopics will be addressed:

1. How to classify a computer network
2. What is network architecture

3. Computer Network

3.1 What is Computer Network

> *A computer network or data network is a digital telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media* [1].

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data [2].

In today's world, data communication is changing the way of business and another daily affair works. A network is connected by a set of devices (laptops, desktop and mobile phones) which are always mentioned as nodes. A node in the network can send and receive data generated by the other nodes in the network. And the link used to connect these nodes are called communication channels.

The best example of computer network is Internet, like the traditional telecommunication network the basic communication model can be expressed like below:

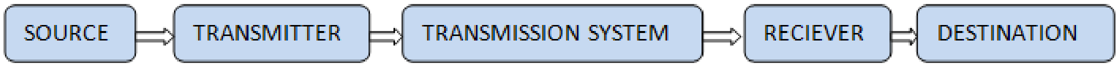


Figure 1

In this model of a communication network (Fig.1), source is the device generating data, like mobile phone, computers etc. The transmitter will transform and encode the data generated by source into a form to produce electromagnetic waves or signals. A transmission system can be a single transmission line or a complex network connecting source and destination. Receiver accepts the signal from the transmission system and converts it into a form that can be access by the destination device.

Data communication is a special case of communication, where the data is exchanged in the form of 0's and 1's. The transmission medium used is wire cable or wireless media. Here are the components of the data communication:

- **Message**: It is the information to be delivered.
- **Sender**: Sender is the person who is sending the message.
- **Receiver**: Receiver is the person to him the message is to be delivered.
- **Medium**: It is the medium through which message is to be sent for example modem.
- **Protocol**: These are some set of rules which govern data communication.

3.2 How to classify computer networks?

To classify computer networks, two dimensions stand out as important:

1. Transmission Technology

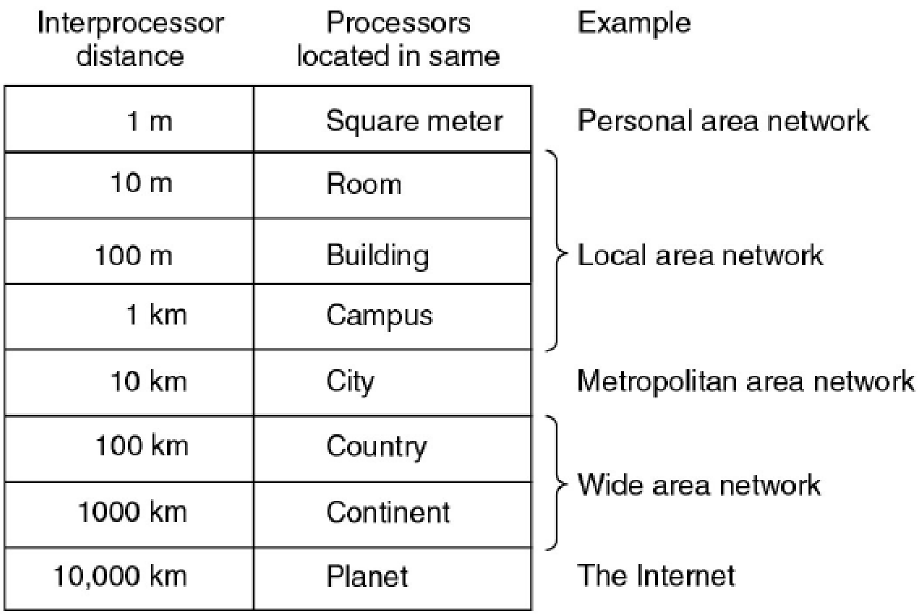
There are two types of transmission technology:

- Broadcast Networks (Multipoint Networks)
- Point-to-point Networks

Broadcast networks have a single communication channel that is shared by all the machines on the network and point-to-point network consist of many connections between individual pair of machines.

2. Scale

The network can be classified by the range of transmission.



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure 2

Local area networks, generally called LAN, are privately owned networks within a single building or campus of up a few KMs in size.

A wide area network, or WAN, spans a large geographical area, often a country or a continent. It is a collection of machines, called hosts, intended for running user programs. The hosts are connected by a communication subnet, which consists of two distinct components:

- Transmission lines
- Switching elements

The job of the subnet is to carry messages from host to host.

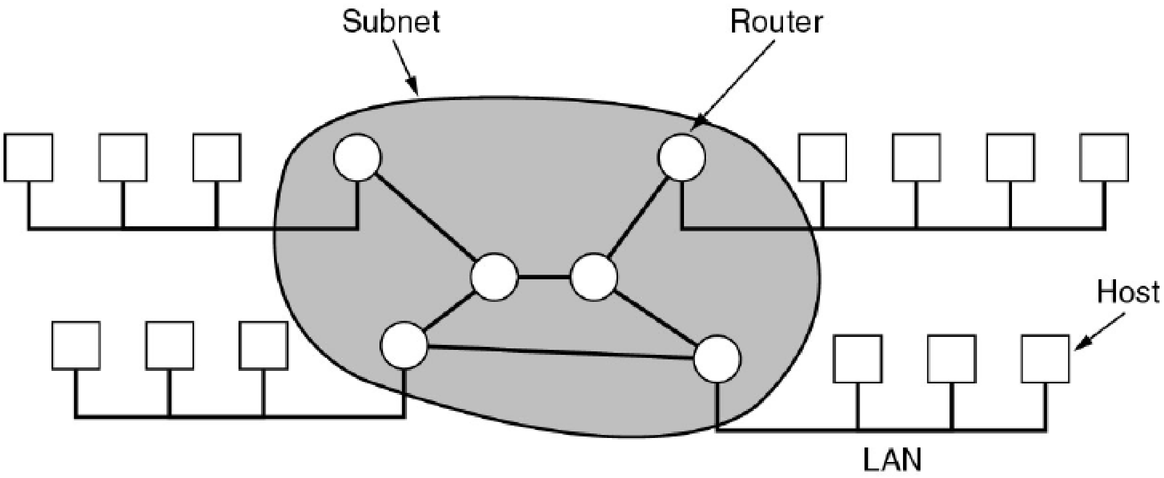


Figure 3 Relation between hosts on LANs and the subnet

And the following figure is a simple multiple hop communication and it will give you an example on how to deliver a packet from sending host to receiving host.

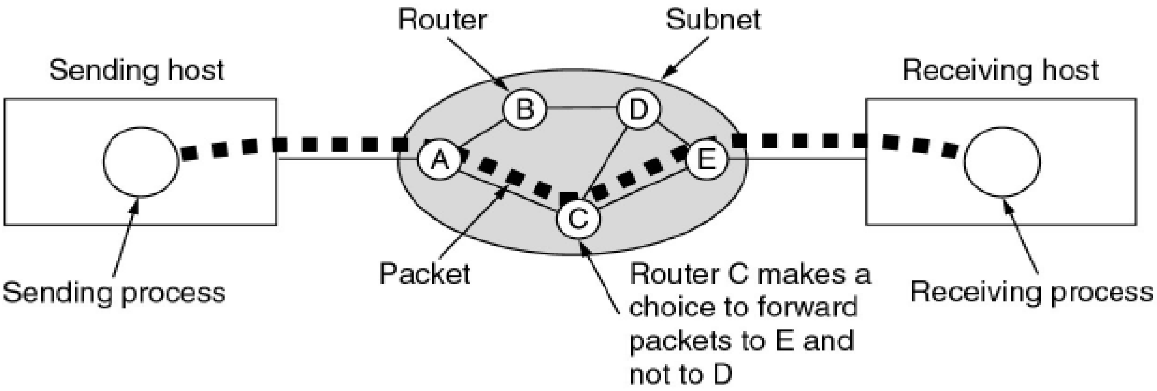


Figure 4 Packet Switched Subnet

In the Fig. 4 above, we know that a single packet is transmitted between different hops and reach its destination. That means on each node, the similar mechanism is implemented to process the data steam, which is called network architecture.

3.3 Introduction to network architecture

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The rules and conventions used by the corresponding peers are known as the layer *n* protocol, i.e., a ***protocol*** is an agreement between peers on how communication is proceeded. Between each pair of adjacent layers, there is an *interface*, which defines which primitive operations and services the lower layer provides to the upper one. And a list of protocols used by a certain system, one protocol per layer, is called a *protocol stack*.

Overall, a set of layers and protocols is called a ***network architecture***.

3.3.1 Design issues for the Layers.

1. Reliability
   - Error detection: how to deal with the situation if the packets is damaged.
   - Finding a working path through a network: multiple paths exists
2. Evolution of the network
   - Networks grow larger and new designs emerge that need to be connected to the existing network.
3. Resource allocation
   - Capacity of transmission
4. Different kinds of threats
   - Eavesdropping on communications

3.3.2 The Relationship of Services to Protocols

Services and protocols are distinct concepts. This distinction is so important that we emphasize it again here.

A *service* is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

A *protocol*, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocol are completely decoupled. This is a key concept that any network designer should understand well.

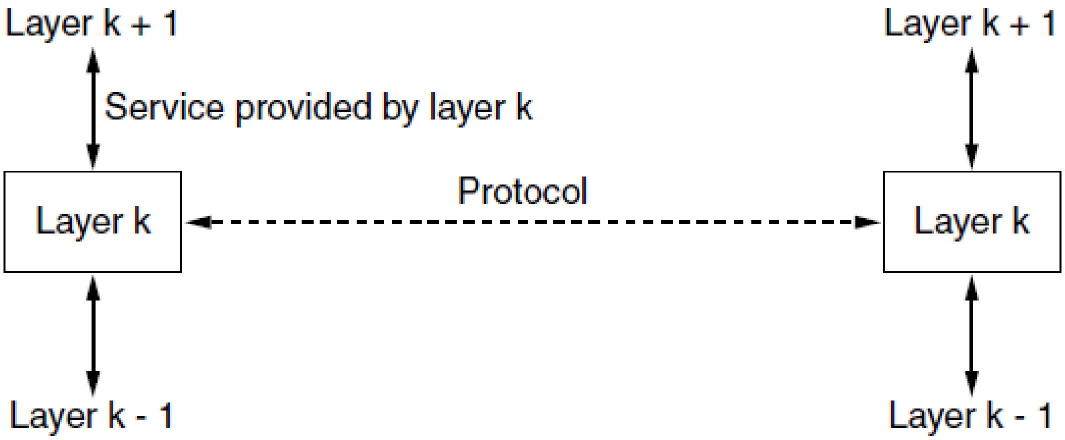


Figure 5 The relationship between a service and a protocol

,

3.3.3 The OSI Reference Model

The OSI model (minus the physical medium) is shown in Fig.6. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995 (Day, 1995). The model is called the ISO **OSI (Open Systems Interconnection)** Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. We will just call it the **OSI model** for short.

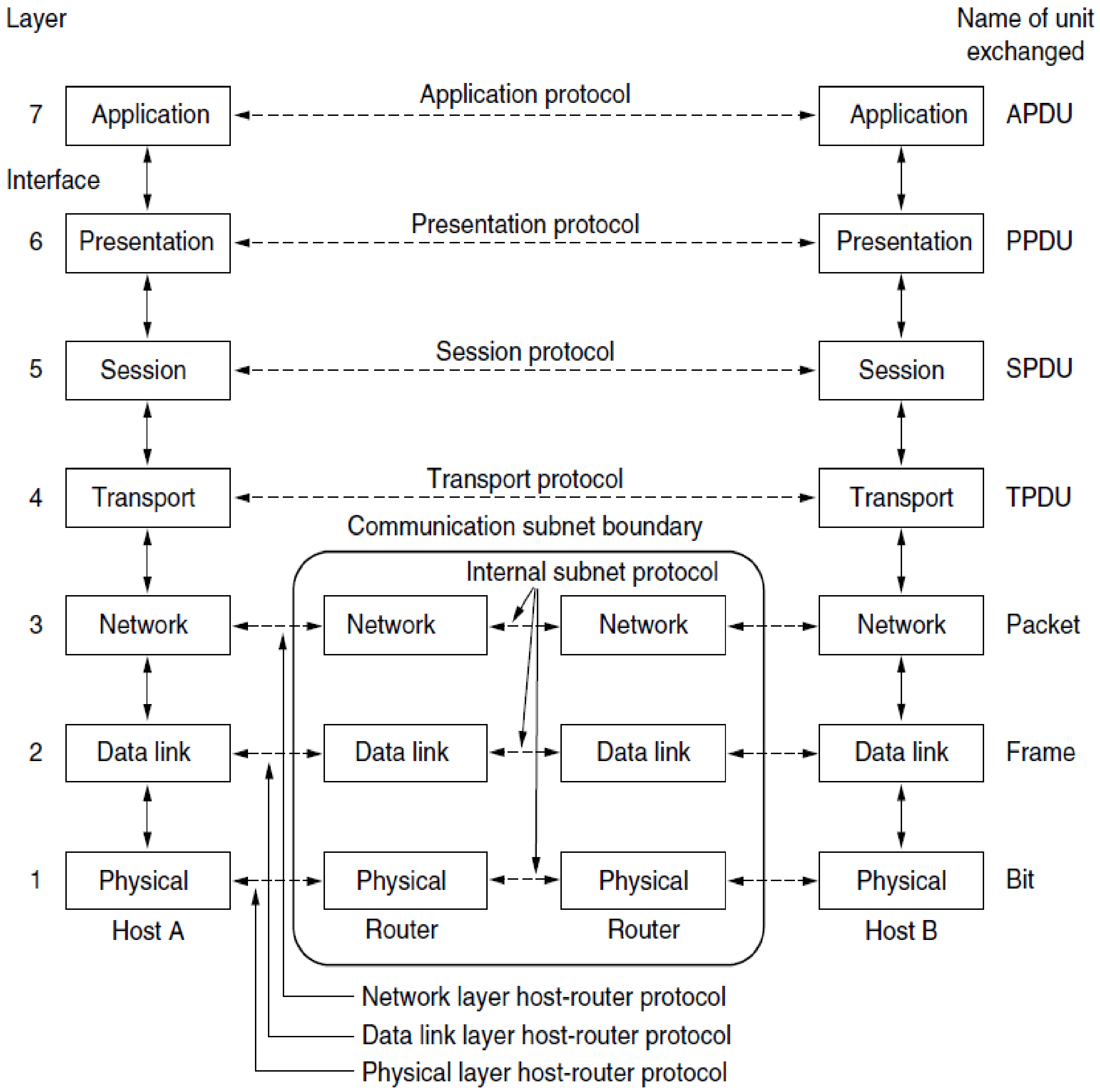


Figure 6 The OSI reference model.

And here is the description of each layer:

- **The Physical Layer**

OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

- **The Data Link Layer**

At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

- **The Network Layer**

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

- **The Transport Layer**

OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

The transport layer is a true **end-to-end layer**; it carries data all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers, each protocol is between a machine and its immediate neighbors, and not between the ultimate source and destination machines, which may be separated by many routers. The difference between layers 1 through 3, which are chained, and layers 4 through 7, which are end-to-end, is illustrated in Fig. 6.

- **The Session Layer**

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

- **The Presentation Layer**

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

- **The Application Layer**

OSI Model, Layer 7, supports ***application*** and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

3.3.4 The TCP/IP Reference Model

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.

And the following figure Fig.7 will illustrate the TCP/IP protocol architecture and different protocols running on different layers.

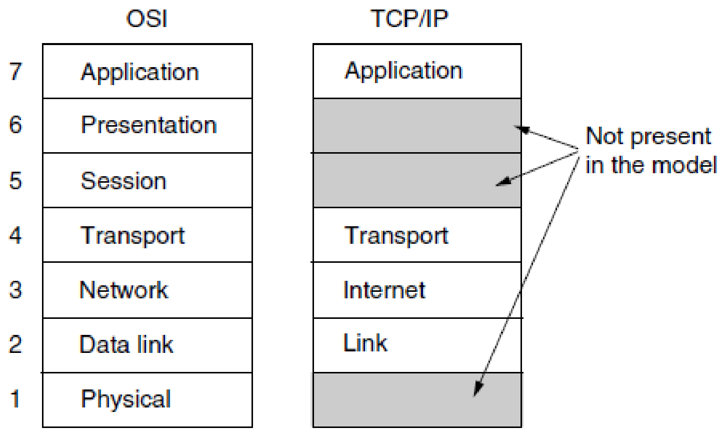
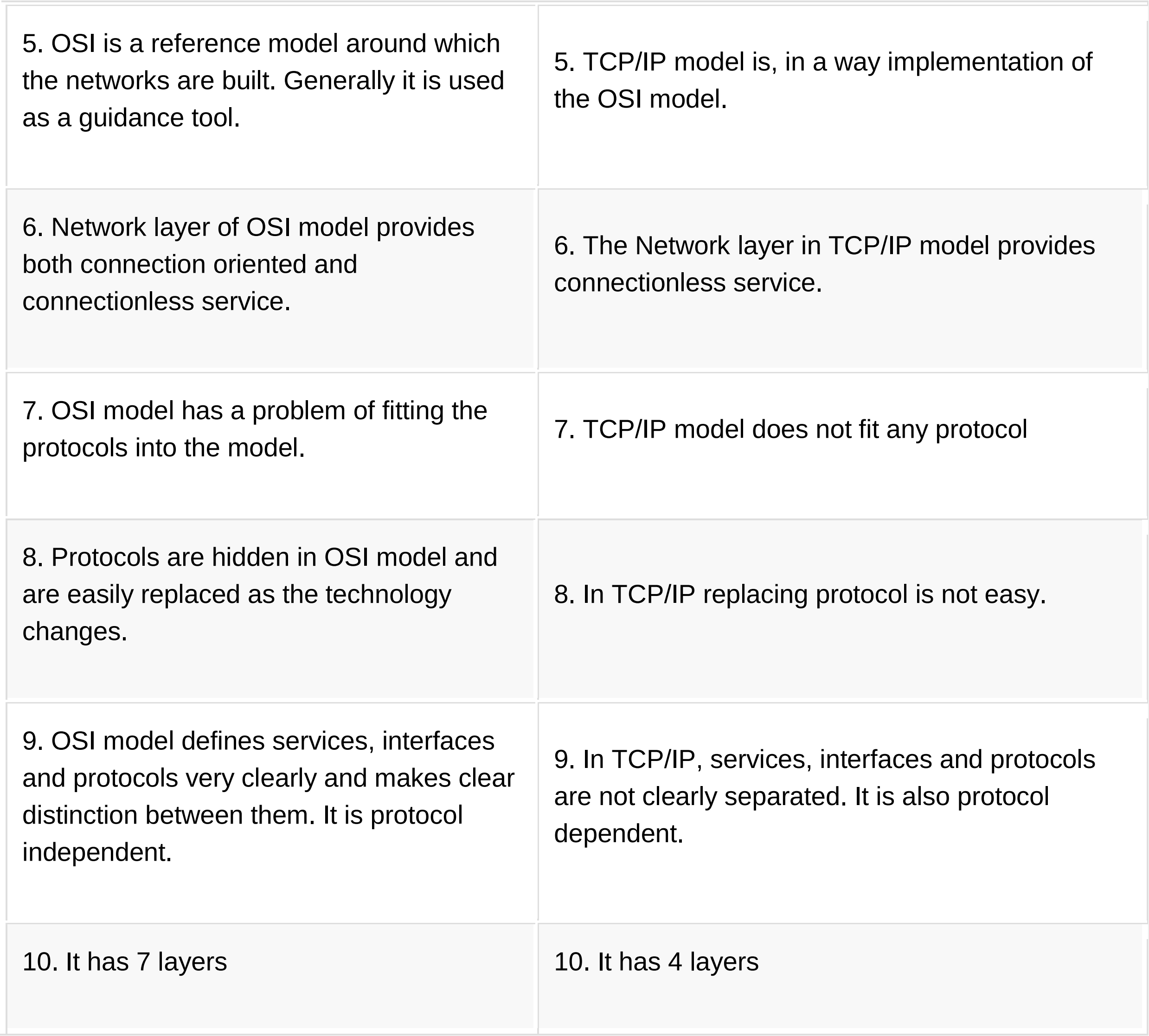


Figure 7 TCP/IP Protocol Architecture

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI **(Open System Interconnection)**	**TCP/IP** **(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.



5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

Reference

[1] https://en.wikipedia.org/wiki/Computer_network
[2] Computer Networks, 5e, A.S. Tanenbaum, ISBN: 0132126958, Prentice Hall