The OSI Model and Network Protocols

Networks - FdSc Computer Technology

Word Count - 2574

CONTENTS

THE OSI MODEL AND NETWORK PROTOCOLS

THE INTERNET, PROTOCOLS AND HOW IT ALL CONNECTS – INTRODUCTION

> *"It would be difficult to overstate the importance of the OSI model. Virtually all networking vendors and users understand how important it is that network computing products adhere to and fully sully support the networking standards this model has generated." - Novell Network Primer* [19]

Network architecture provides only a conceptual framework for communications between computers. The model itself does not provide specific methods of communication. Actual communication is defined by various communication protocols.

In the following discussion we will look at the protocols at each layer of the OSI Reference Model and compare to the TCP/IP model.

In addition to the OSI network architecture model, there exists other network architecture models by many vendors, such as IBM SNA (Systems Network Architecture), Digital Equipment Corporation (DEC; now part of HP) DNA (Digital Network Architecture), Apple computer's AppleTalk, and Novell's NetWare.

We will look at how the adoption of the OSI model has affected the development of networking and considerations on where network architecture may be heading.

Protocols and Purpose

Protocol architecture is the layered structure of hardware and software that supports the exchange of data between systems and supports distributed applications e.g. email and file transfer. At each layer, one or more common protocols are applied in communication systems. Each provides rules for the exchange of data between systems.

Examples of the main set of protocols;

- **HTTP** - Hyper Text Transfer Protocol - Facilitates hypertext sending and receiving between browsers and servers. A set of rules for transferring sound, graphics, text, video and multimedia files. A user is indirectly accessing HTTP as soon as he/she opens a Web browser.
- **HTTPS** - Hyper Text Transfer Protocol Secure – Used to send or receive data securely on internet with the help of SSL (Secure Socket Layer). These are often used for payment or secure ecommerce on the web, such as online banking. Https encrypt the session or page with digital certificate i.e. HTTPS over SSL (Secure Socket Layer) - used by web browser.
- **POP** - Post Office Protocol (POP3) allows an email client to download an email from a server. It is simple i.e. download only. Its design assumes that the email client downloads all available email, deletes them and disconnects.
- **SMTP** – Simple Mail Transfer Protocol - used when email is delivered from a client, such as Outlook Express, to an email server or when email is delivered from one email server to another.
- **IMAP** - Internet Message Access Protocol - set of rules that allows a user to access email from a local server. Client/server protocol – email retrieved from a secure Internet server, user decides whether to download after reading its sender information and heading. Allows users to create folders, delete and purge messages off the Internet server and manipulate mailboxes. Users should be logged into their Internet server mailbox while using IMAP.
- **FTP** - File Transfer Protocol allows computers to exchange files over the Internet. FTP allows users to copy, move, rename and delete files, in addition to downloading programs or files.

Figure 1: Main Protocols

The most widely used being the TCP/IP protocol suites – used in concert with each other. An internet based protocol suite is the framework for developing a complete range of computer communications standards. Consisting of the following layers: physical, network, internet, transport and application. [1]

A Protocol ensures that devices talk to each other effectively. In the OSI Reference Model, a protocol is defined as a set of rules governing communication between entities, at the same layer. The Transmission Control Protocol (TCP) is responsible for specific set of functions on the TCP/IP networks. [2]

Internet Protocol (IP) is the principal set digital formats/rules for exchanging messages between computers across a single or a series of interconnected networks, using the Internet Protocol Suite. Messages are exchanged as datagrams, or data packets/packets.

The main task of IP is delivery of datagrams from the host to the destination host based on their addresses. IP includes methods and structures for putting tags within datagrams, this process is called encapsulation. [3]

IP[1] operates at the network layer of the OSI model. The Transmission Control Protocol (TCP) operates one level higher, at the transport layer. TCP manages connections between computers. Messages are carried (encapsulated) in IP datagrams. [4]

Both TCP and UDP are protocols used for sending packets of data — over the Internet.

TCP guarantees the recipient will receive packets in order by numbering them. The recipient acknowledges receipt to the sender. If the sender does not get a correct response, the packet is resent to ensure the recipient received them. Packets are checked for errors. TCP is about reliability. Packets sent with TCP are tracked so no data is lost or corrupted. [4] File downloads do not become corrupted even if there are network hiccups.

The User Datagram Protocol (UDP) serves the same role as the TCP but offers less features. In UDP and TCP, both are carried within IP packets, but the only UDP feature that is supported is the resending of any packets not received at the destination. UDP is a connectionless protocol; its main advantage is being faster for trivial network communication e.g. sending a web page to a client computer. Because UDP does not offer many error-checking or handling features, it should only be used when it is not important for data to be mangled between points and needs to be resent, or when an application has its own error-checking and error-handling functions. [4] "Quick UDP Internet Connections" (QUIC), which were proposed by Google in 2012 as a reliable protocol on top of UDP to reduce web page retrieval time. [5]

Both TCP and UDP support the concept of ports. E.g. Use ‘Port 80; used to send data between server’s/server machines to receive requests. [3]. UDP is used when speed is desirable and error correction not necessary. UDP is frequently used for live broadcasts and online games.

Another important protocol architecture is the Open Systems Interconnect (OSI) Model.

[1] Internet Protocol version 4 (IPv4) was the first major version of IP. This is the dominant protocol of the Internet. However, iPv6 is active and its deployment is increasing worldwide. [15]

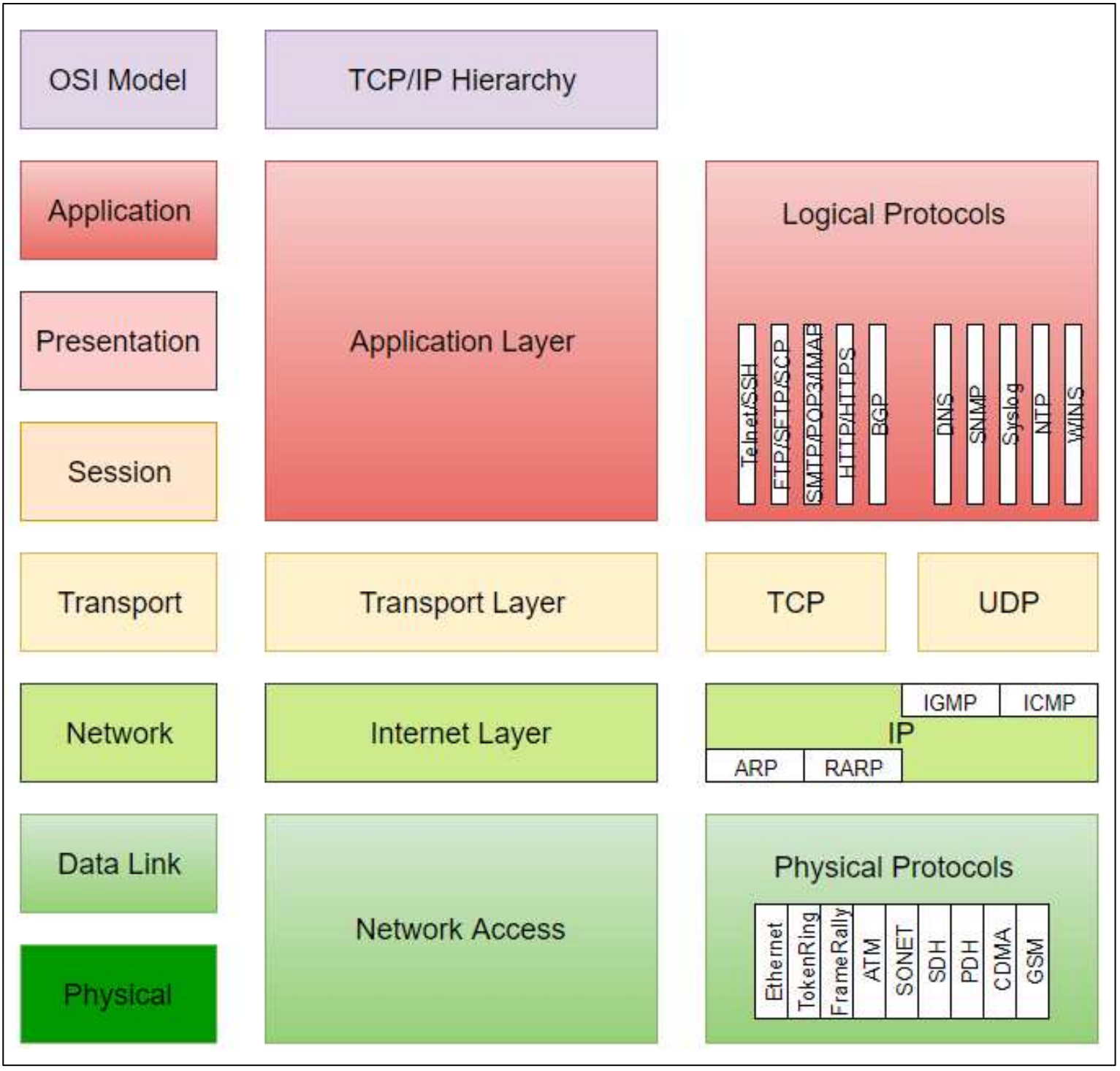

Figure 2: Protocols, OSI Model and TCP Comparison

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. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.

THE OSI 7-LAYER MODEL

OSI Reference Model, seven layers that define the stages data must go through to travel from one device to another. A 7-layer OSI product is supposed to perform the data conversion service between the network and the user application [6] . Each layer relies on services provided by a lower layer.

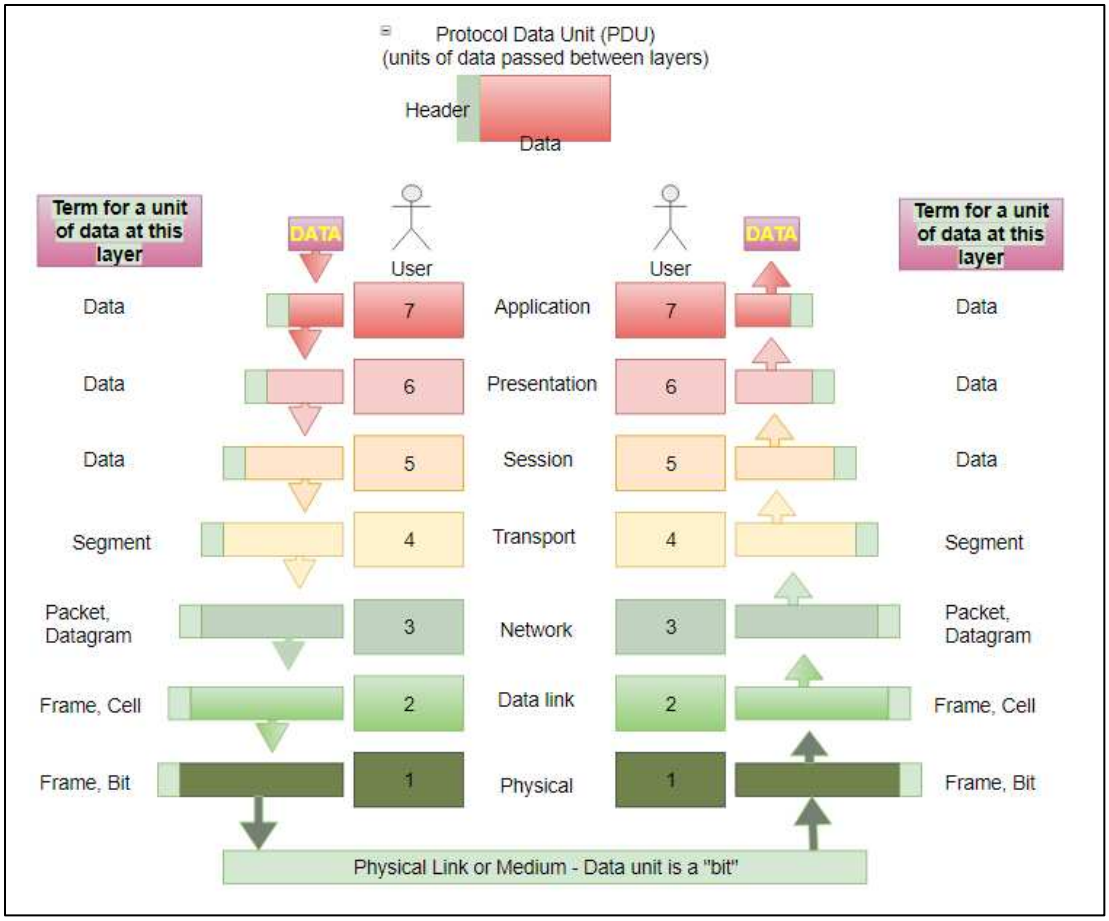

Figure 3: The OSI Model – PDU's

Each layer contains a Protocol Data Unit (PDU). PDU's are used for peer-to-peer contact between corresponding layers.

1, 2, 3. The top three layers - Application, Presentation and Session, handle data.

4 Data is segmented by the Transport layer.

5 Network layer places it into packets.

6 Data Link frames the packets for transmission.

7 Physical layer converts it into bits and sends it out over the transmission media.

The receiving computer reverses the process using the information contained in the PDU. [3]

Frame Component	Function
Header	Signifies the start of the frame and carries Layer 2 source and destination address information
Payload	Carries data from Layer 3, such as packets from the network layer containing user data
Trailer	Signifies the end of the frame and carries error-detection information in the form of a cyclic redundancy check (CRC)

Figure 4: Frame Components and Functions [8]

Layer 7: Application

This layer interacts with the operating system or application whenever the user chooses to transfer files, read messages or perform other activities.

The seventh and highest layer in the OSI is the application layer. Application protocols are defined at this layer, which implement specific user applications and other high-level functions. Since they are at the top of the stack, application protocols are the only ones that do not provide services to a higher layer; they make use of services provided by the layers below.

Firewalls - There is no simple answer to which OSI Level a Firewall belongs to. The level of protection firewalls provides and the way they offer that protection varies.

- Application-level gateway. Application level firewalls decide whether to drop a packet or send them through based on the application information (available in the packet). They do this by setting up various proxies on a single firewall for different applications. Both the client and the server connect to these proxies instead of connecting directly to each other. Therefore, these proxies drop any suspicious data or connections.

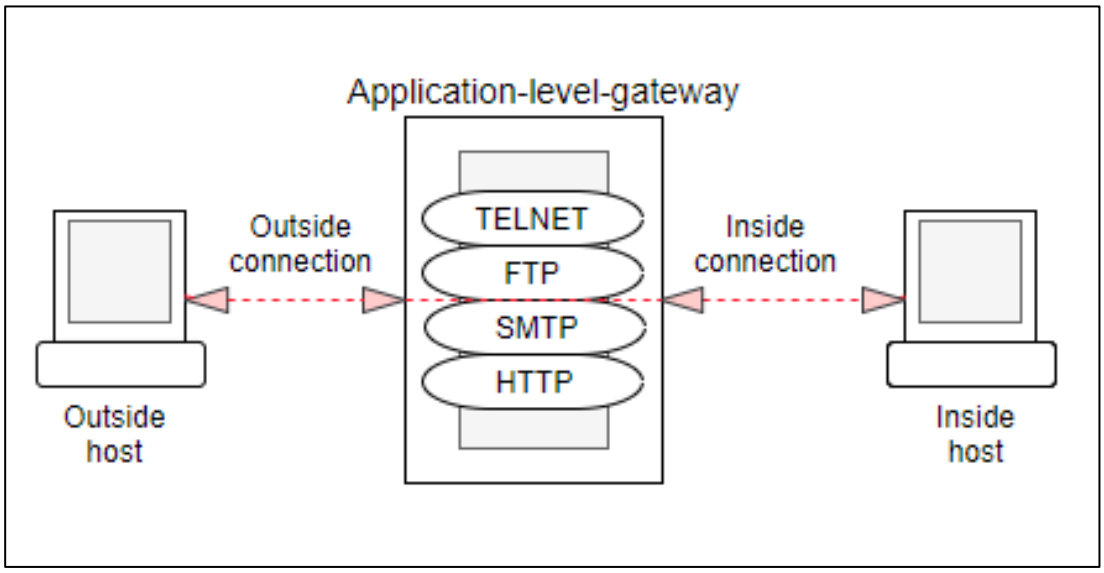

Figure 5: Application Level Gateway (Firewall)

Layer 6: Presentation

Takes the data provided by the Application layer and converts it into a standard format.

> ***Gateways*** – Operate at all seven layers of the OSI model; a protocol converter. A router by itself transforms, accepts and relays packets only access networks using similar protocols. A gateway can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP).

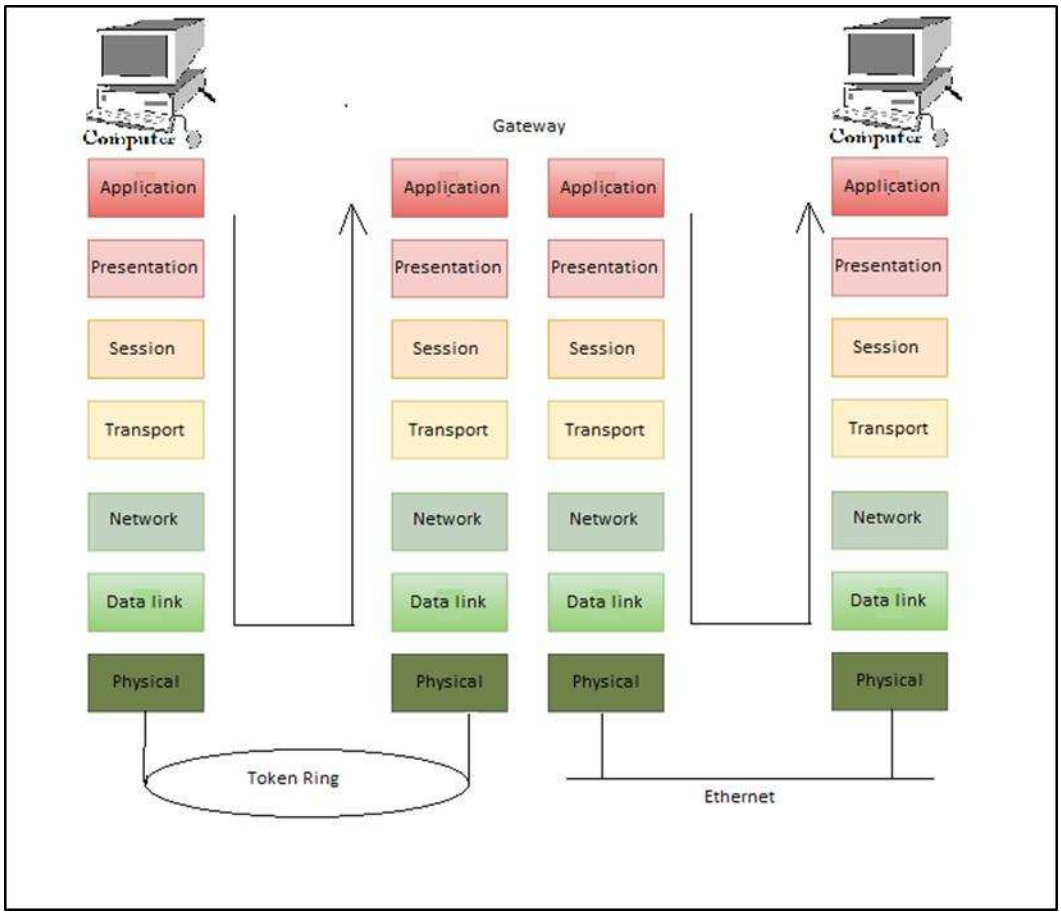

Figure 6: Gateway Data Flow

Layer 5: Session

Establishes, maintains and ends communication with the receiving device.

> *Firewall* - Circuit-level gateway. Monitors TCP handshaking (See Figure 7: TCP Handshaking Example) between the packets to determine if a requested session is legitimate. The information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway. Therefore, there is no way for a remote computer or a host to determine the internal private IP addresses of an organization.

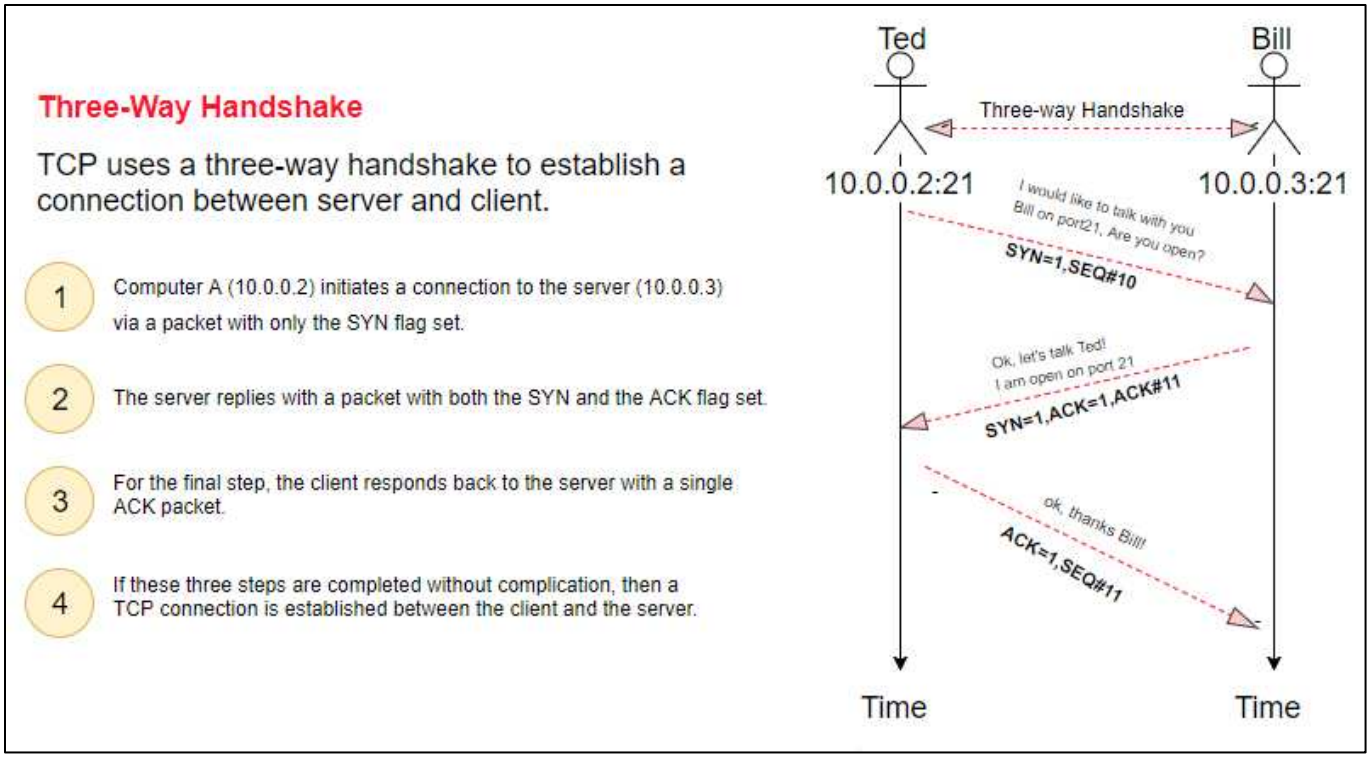

Figure 7: TCP Handshaking Example

Layer 4: Transport

This layer maintains flow control and provides for error checking and recovery of data between the devices. Flow control means that the Transport layer looks to see if data is coming from more than one application and integrates each application's data into a single stream for the physical network. Transport PDUs are typically called segments.

> *Operating System* -Application - Layer 3 – Network and Layer 4 - Transport
>
> A networking OS provides the Layer3 (IP/ARP) and Layer4 (TCP/UDP) functionality. Almost everything above that is provided by applications.

Layer 3: Network

The way that the data will be sent to the recipient device is determined in this layer. Logical protocols, routing and addressing are handled here.

> *Router* - Used to connect networks. The Internet consists of many interconnected routers. Using a network protocol, like TCP/IP, a router can intelligently move data from one network to another. [7]

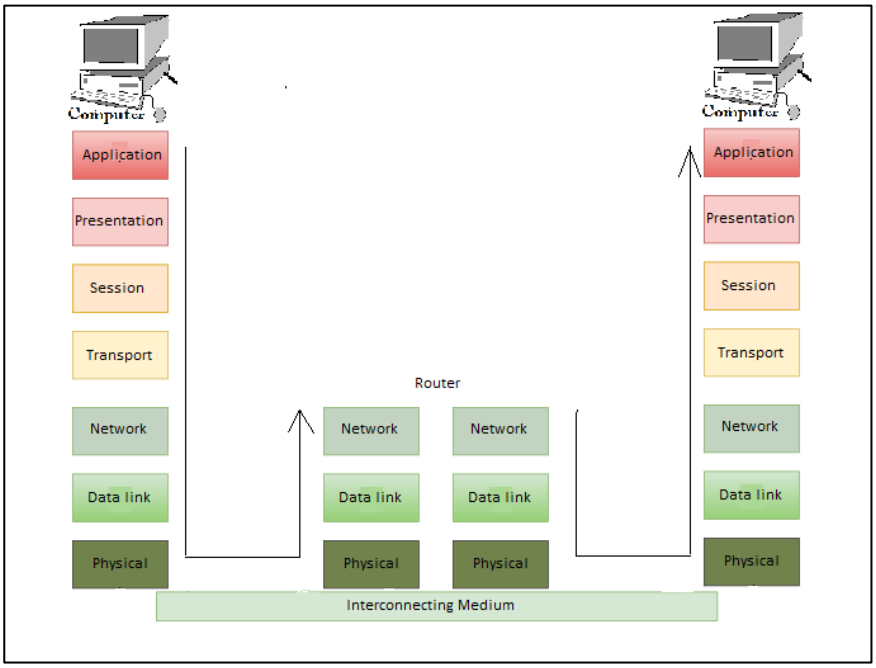

Figure 8: Router Data Flow

Upon receiving the Packet, the router has to follow three generic steps before it routes the packets.

1. Routing
2. Forwarding (switching)
3. Encapsulation

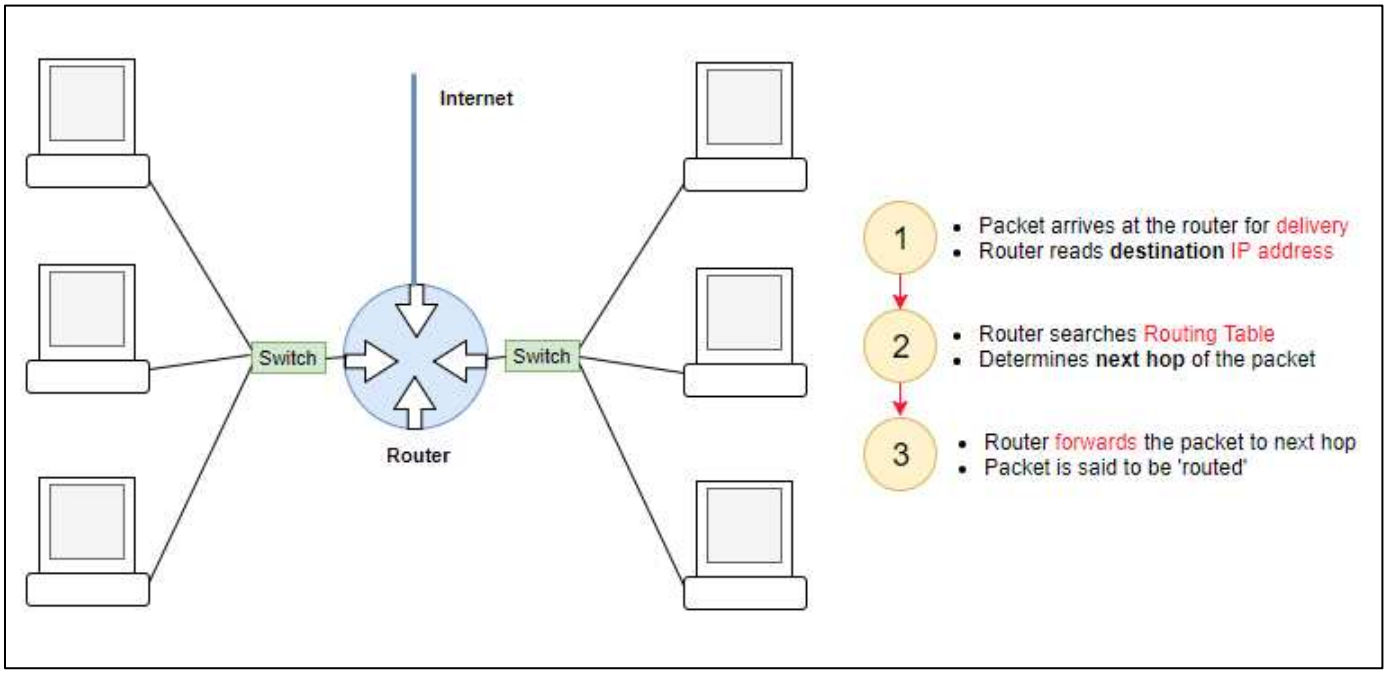

Figure 9: How a Router Works

- **Packet-filtering firewall** - Layer 3 – Network. Packet filtering, each packet passing through a firewall is compared to a set of rules before it can pass through. Either depending on the packet and the rule, it can be dropped, sent through or a message can be forwarded to the originator. The rules which determine which packets to be sent, and which not to be sent can be based on the source and destination IP address, source and destination port number or the protocol used. Packet filtering can also be done at the router level, providing an additional layer of security.

Layer 2: Data Link (also MAC Sublayer)

In this layer, the appropriate physical protocol is assigned to the data. The type of network and the packet sequencing is defined. MAC is responsible for deciding who sends next on a multi-access link.

Network Interface Card – Application - Layer 1 – Physical and Layer 2 – Data Link.

NIC allows the computers of a network to communicate as OSI layer 1 and layer 2 hardware devices. It also makes possible the physical contact with a network's resource or other medium. With NIC a low-level addressing structure with the use of MAC addresses becomes possible. It permits the computers users to establish a connection with each other by using cables to communicate wirelessly.

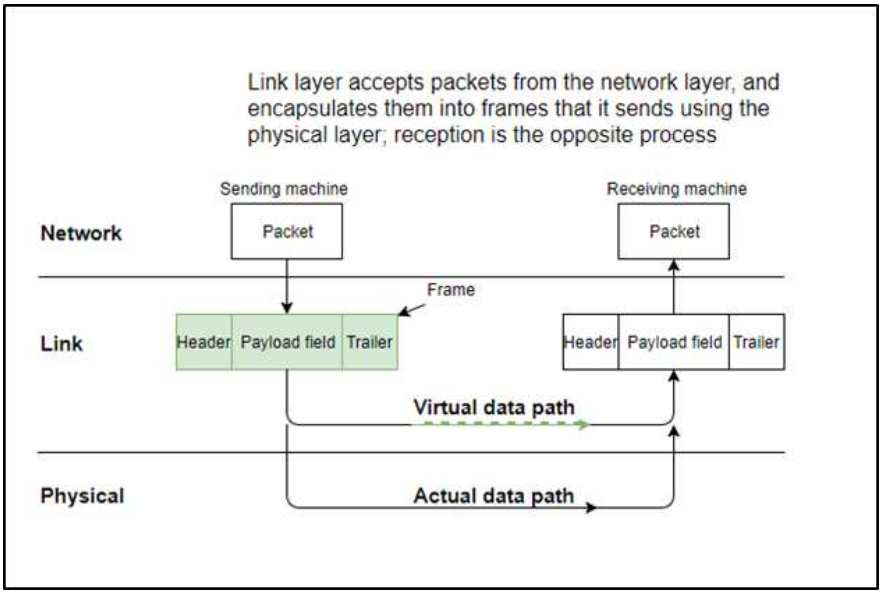

Figure 10: Data Link Layer – Dealing with Packets

Layer 1 - Physical

Lowest layer of the OSI Model; concerned with the transmission and reception of the unconstructed raw bit stream, over a physical medium [8].

This is the level of the actual hardware. It defines the physical characteristics of the network such as connections, voltage levels and timing. Also at this level, a Hub, which has the primary purpose to regenerate a signal.

Transmission Media

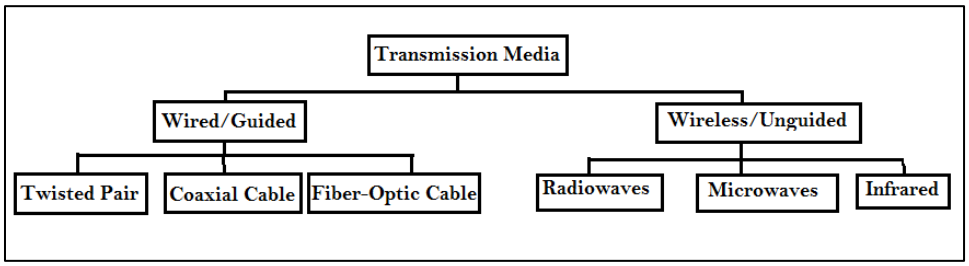

Figure 11: Transmission Media

OSI – How it Progressed, Unified and Molded Network Design

OSI is a standardized architecture often used to describe communication functions; now rarely implemented. A conceptual model, used most often in network design and engineering network solutions. (Stallings, 2011) [9] This is the view of some IT professionals; however, OSI has a deep history, periodically reviewed to stay in keep with current technologies. Working out the architecture defines a module structure that will facilitate evolution and change. (Day, 1995) [10]

Real-world networks conform to the OSI model, although differences exist between the theory and actual practice. [11] OSI still offers how to understand and visualize computer networks to each other.

The early successes of in the mid-1970's made it apparent that to utilize the full potential of computer networks, international standards were required. In 1977, the International Standards Organization (ISO) initiated work on OSI to add these requirements. The OSI is the highest level of abstraction in the scheme. [12]

In 1983, a group of major computer and telecommunication companies decided to get involved to establish a common reference model for which others could develop detailed interfaces, which in turn could become standards. The consequence led to the *adoption* of the OSI reference model as an international standard by the ISO, defining how messages should be transmitted between any two points in a network. The need for interconnectivity continued to drive the office automation strategies of major vendors into late 1980s. This gave users the freedom to choose equipment from the various vendors supporting the standards, as well as the flexibility to move from one generation of products to another without fear of redundancy. By publishing the interfaces and protocols of their open architectures, vendors encouraged third-party suppliers to develop specialized products for the networks, increasing the options available.

During this period users of IBM and other popular PCs were looking for ways to communicate with mainframe computers, either to access centralized data files or to utilize powerful host resources such as high-speed print facilities. Effort was going into the development of local networks to link microcomputers workstations and peripherals for resource sharing. Many general-purpose LANs and component suppliers that provided a range of LAN interconnection devices such as bridges, routers and gateways began to emerge. 3Com, Chipcom, Madge Networks, Sytek, and Ungermann-Bass were some of the leading firms in the emerging sub-fields.

In 1985, Ungermann-Bass also reached agreement with Microsoft to develop and market products compatible with the IBM PC network, which commercialized the first LAN technology; ARCnet, and observed the rapid movement of PC network software vendors away from proprietary protocols and software, moving toward the IBM and Microsoft standards. [6]

Transition to multi-vendor, multi-protocol solutions (1989–1992). Many users were moving from the mainframe-based networking environment to a distributed management environment. They wanted a more open environment where they could bring in the different network devices from a wide array of vendors. Besides the OSI model, Simple Network Management Protocol (SNMP) and the TCP/IP emerged as two influential alternatives. Given the surge of distributed computing, the wide area requirements for the local area network systems have begun to take on critical importance.

Switched Multi-Megabit Data Services (SMDS), Broadband Integrated Services Digital Networks (B-ISDN), frame relay, SONET, and Asynchronous Transfer Mode (ATM) were the technologies developed by the companies to facilitate and support such networking applications. The device bridges and routers interconnected LANs over all these broadband technologies. [13]

Considerations were being made in the 1990s to commercialize the Internet network and services because the Internet would be able to provide greater interoperability, higher transmission rates and an addressing scheme that accommodates global reach.

During the 1990's the mass population adopted the internet.

However, technology trends in computing are increasingly testing the limits of yesterday's networks - many that were 'good' for yesterday are not 'good enough' for tomorrow. Consumerization of IT, mobility, virtualization and cloud computing along with a massive increase in video traffic are putting rising demands on the network. [14]

In the future, rather than just focusing on how applications and devices connect to the network, we will have to look at the performance of the application on the network, adjust packet transfer rates and integrate virtualization into the network operating system.

The network of the future will be incredibly flexible and intelligent. Services will be consumed dynamically, and this will be made possible by and is completely dependent on, dynamic and flexible network services.

CONCLUSION

Forming an opinion, from researching the reasoning, development and real-world application of the OSI Reference Model over the last four decades, it has molded and defined network architecture. Both in bringing companies and organizations together to set standards. In doing so, OSI and protocols ensured they work together so their components are compatible. This fact alone would be a major factor in worldwide adoption of networking and the internet. Figuratively shaping of the 'always on' culture, we live in today.

Next-generation technologies require a next-generation network that is architected to deliver reliability, agility and performance.

REFERENCES

[1] H. Zimmerman, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications,* vol. 28, no. 4, pp. 425-, 1980.

[2] C. C. Kozierok, The TCP/IP Guide, Version 3, 2005.

[3] W. Stallings, "Protocol Architecture, TCP/IP, and Internet-Based Applications," in *Data and Computer Communications, Ninth Edition*, New Jersey, US, Pearson Education, 2011, pp. 61-81.

[4] B. A. Hallberg, Networking: A Beginner's Guide, Fifth Edition, New York, US: McGraw-Hill, 2010.

[5] G. Carlucci, L. De Cicco and S. Mascolo, "HTTP over UDP: An Experimental Investigation of QUIC," in *SAC '15 Proceedings of the 30th Annual ACM Symposium on Applied Computing*, Salamanca, Spain, 2015.

[6] K. Fong and J. Reinstedler, "Development of an OSI Application Layer Protocol Interface," *ACM SIGCOMM Computer Communication Review,* vol. 19, no. 3, pp. 21-57, 1989.

[7] P. Smith and J. Wei, "Hubs, Switches, And Routers," *http://web4.uwindsor.ca/,* vol. 15, no. 3, 2002.

[8] Microsoft, "The OSI Model's Seven Layers Defined and Functions Explained," 19 Apr 2017. [Online]. Available: https://support.microsoft.com/en-gb/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained. [Accessed 16 Jan 2018].

[9] W. Stallings, Data and Computer Communications, New Jersey, US: Pearson Education, 2011.

[10] J. Day, "The (un)revised OSI Reference Model," *ACM SIGCOMM Computer Communication Review,* vol. 25, no. 5, pp. 39-55, 1995.

[11] J. D. Day and H. Zimmerman, "The OSI Reference Model," *Proceedings of the IEEE,* vol. 71, no. 12, pp. 1334-1340, 1983.

[12] M. Addison-Wesley, "Telecommunications Networks: Protocols, Modelling and Analysis," Addison-Wesley Longman Publishing Co, Boston, MA, US, 1987.

[13] P.-H. Soh and E. B. Roberts, "Networks of innovators: a longitudinal perspective," *Elsevier Research Policy,* vol. 32, pp. 1569-1588, 2003.

[14] M. Gupta, "Networks of the Future," 2014. [Online]. Available: https://www.cisco.com/c/en_in/about/knowledge-network/networks-of-future.html. [Accessed 6 Feb 2018].

[15] J. Campbell, "Network Protocols Explained," http://www.ehow.com/about_6519116_network-protocols-explained.html?ref=Track2&utm_source=IACB2B.

[16] eTutorials.org, "OSI Model (As It Applies to LANs and the Interrelation Between Layers)," eTutorials.org, 2017. [Online]. Available: http://etutorials.org/Networking/Lan+switching+first-step/Chapter+3.+Local-

Area+Networking+Introduction/OSI+Model+As+It+Applies+to+LANs+and+the+Interrelation+Between+Layers/. [Accessed 23 Jan 2018].

[17] B. Sosinsky, Networking Bible, Indianapolis, US: Wiley Publishing, Inc, 2009.

[18] Study Tonight.com, "Computer Networks," [Online]. Available: https://www.studytonight.com/computer-networks/comparison-osi-tcp-model. [Accessed 2 Feb 2018].

[19] Novell.com, "Network Primer," 2015. [Online]. Available: https://www.novell.com/info/primer/primer.html. [Accessed 21 Jan 2018].