Interaction of Layered Protocols in a Communication Network

u5539006, Peter Walker

1 Abstract

It can be difficult to understand complex layered protocols through textual descriptions, due to their theoretical nature. This report aims to enhance the reader's understanding of layered protocols in the OSI Model through diagrams to illustrate different sections of the communication process and how they interact in the context of loading a webpage.

Contents

2 Introduction

The Open Systems Interconnection (OSI) Model is used to model communication between different devices, using standard protocols (see Figure 1). It is split into seven abstract layers and each layer contributes some information to the communication process. Not all layers are extensively involved in all communication scenarios; the model instead aims to provide a structure to the process. Data moves down the layers in the model on the client as more information is

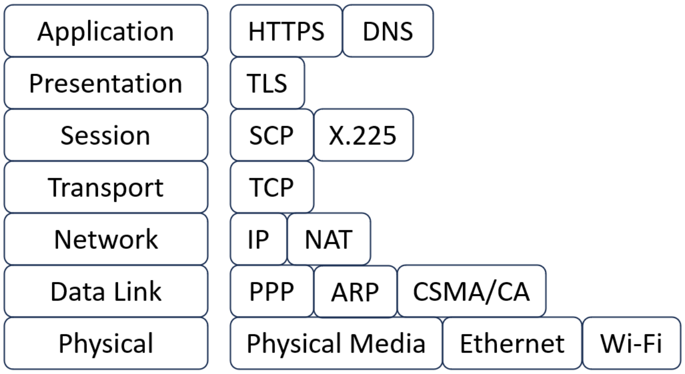


Figure 1: From left to right: the 7-layer OSI Model, and the protocols that may be involved in the loading of a webpage.

added at each layer (see Figure 2), and up the model on the receiving device. [1, 2]

3 OSI Model in Context

This section follows the application of the OSI Model when a user loads a webpage on a device.

3.1 Application

The protocols included in loading a webpage at the application layer are the Hyper-Text Transfer Protocol Secure (HTTPS) and Domain Name System (DNS).

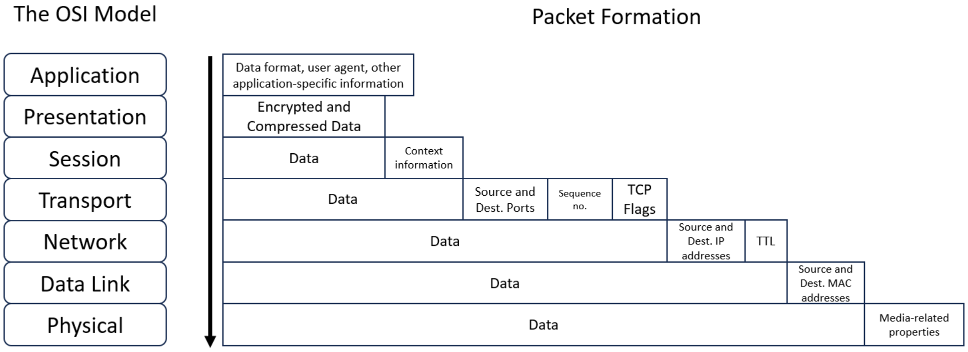


Figure 2: An overview of the data that is added at each layer of the OSI Model before the data is sent. [2]

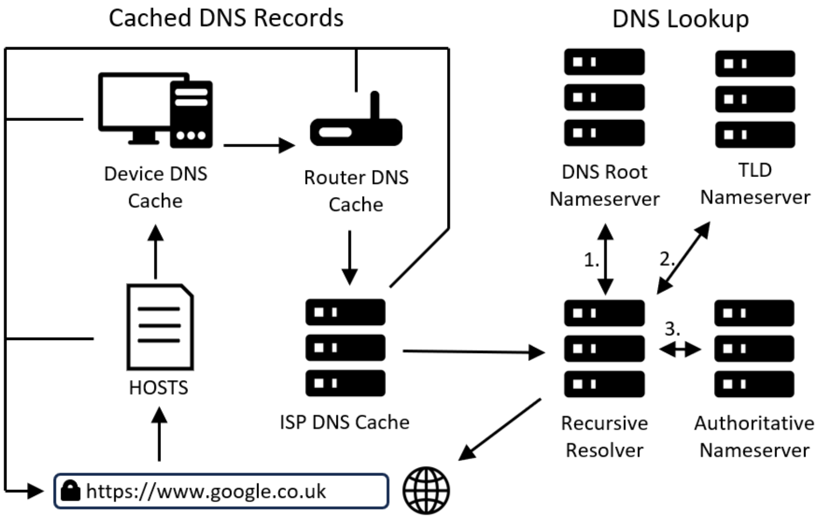


Figure 3: The process of finding the IP Address of the webserver for a given URL. [3]

HTTPS is a version of HTTP (the standard for loading webpages, but is insecure, that includes Transport Layer Security (TLS)). HTTPS formats the request for the webpage to send to the webserver, including data such as the HTTP version. DNS serves to format the Uniform Resource Locator (URL), that is visible to the user, into an IP (Internet Protocol) Address. If the IP Address cannot be found in one of the caches (device, router or ISP), it must be queried by a recursive resolver (see Figure 3). [3]

3.2 Presentation

The presentation layer of the OSI Model involves the compression and encryption of the application data. In this case, TLS is used and this encrypts the HTTP request (the data passed to this layer from the application layer). This is asymmetric encryption, and helps to stop man-in-the-middle attacks as any intercepted data cannot be read. This involves the client and the server establishing a Transport Control Protocol (TCP) connection and then undergoing a TLS handshake (see Figure 4). [4]

3.3 Session

This layer isn't really involved loading a webpage, since it only requires a single request, but would be used to have multiple virtual TCP connections within a single connection.

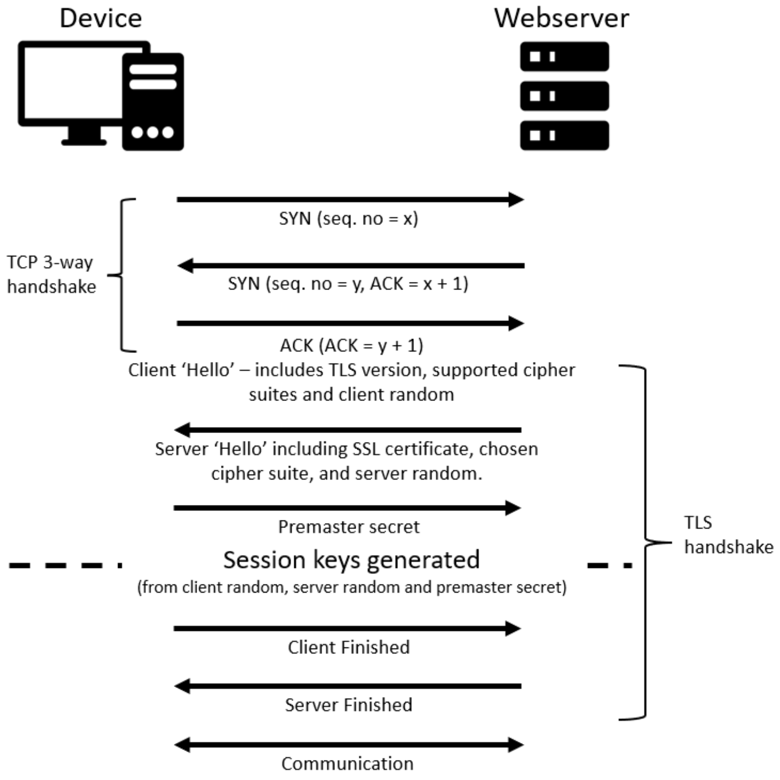

Device
Webserver
TCP 3-way handshake
SYN (seq. no = x)
SYN (seq. no = y, ACK = x + 1)
ACK (ACK = y + 1)
Client 'Hello' – includes TLS version, supported cipher suites and client random
Server 'Hello' including SSL certificate, chosen cipher suite, and server random.
Premaster secret
Session keys generated
(from client random, server random and premaster secret)
Client Finished
Server Finished
Communication
TLS handshake

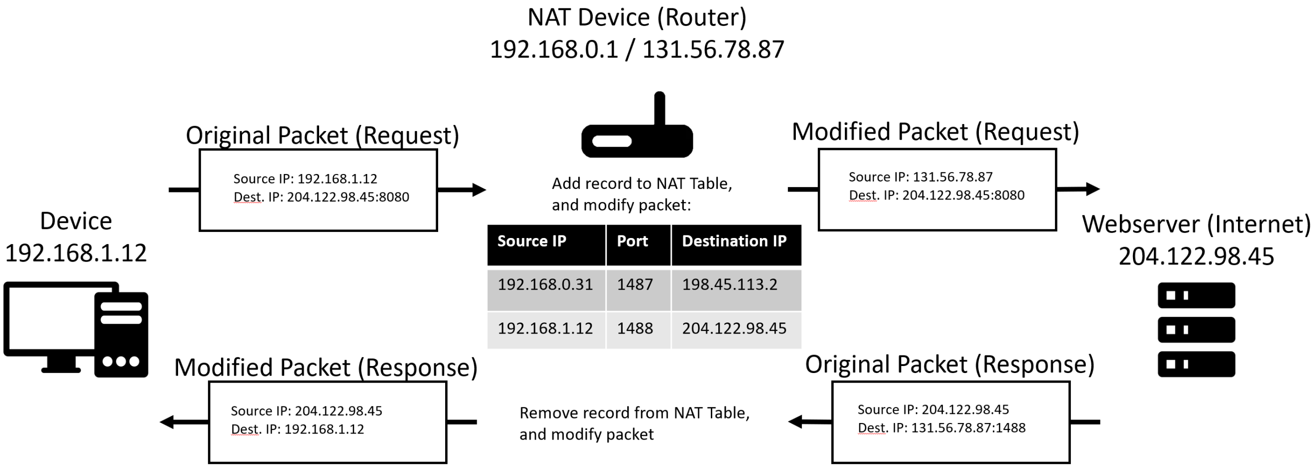
Figure 4: The flow of data in the handshake, involving the 3-way TCP handshake and the TLS handshake [4]

3.4 Transport

TCP is the protocol most widely-used in this layer, due to reliability features it contains, unlike User Datagram Protocol (UDP). This layer is where key information is added to the TCP segments (the data passed from all the upper layers) as TCP headers. They contain flags to identify the use of TCP, as well as source and destination port numbers, and the sequence number for each segment, so they can be reordered at the destination correctly.

3.5 Network

At the network layer, IP (either v4 or v6) and Network Address Translation (NAT) are used. IP adds the IP addresses of the source and destination devices to the packets as headers, that were obtained by DNS. NAT is used to translate private IP addresses (used on a Local Area Network (LAN)) to public IP



Source IP	Port	Destination IP
192.168.0.31	1487	198.45.113.2
192.168.1.12	1488	204.122.98.45

Figure 5: The process of sending and receiving a packet involving translating private and public IP addresses between LANs and the Internet. [5]

addresses for the Internet. This usually happens at the router (see Figure 5). [5] This is because private IP addresses are not routable on the Internet.

3.6 Data Link

In the data link layer, three protocols may be used: Point-to-Point Protocol (PPP), Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) and Address Resolution Protocol (ARP). ARP is used to translate the IP addresses attached in the packet to MAC addresses (unique identifiers for each Network Interface Card - these are required to have network access on a device). [8] PPP is no longer common, but is used by Internet Service Providers (ISPs) to provide dial-up access to the Internet to consumers. [7] Finally, CSMA/CA is a protocol used by devices sending packets on a network to prevent collisions of data that is routed to the same device (see Figure 6). This is achieved by utilising requests and responses between clients and the router to make sure the channel is available, or whether to wait before transmitting data. This allows the router to control the flow of packets from connected clients. [6]

3.7 Physical

The physical layer, the bottom layer, is concerned with the physical transportation of the bits that form the frame. This could involve protocols such as Ethernet and Wi-Fi, but also copper coaxial cable and fibre optics, depending on which devices are communicating. For copper coaxial cable or Ethernet, this layer would concern the frequency of voltage switches, and which voltage signified what string of bits. For fibre optics, this concerns the frequency of the light signals, and their duration. Wi-Fi would involve the frequency and channel of radio signals being sent.

4 Conclusion

The OSI Model contains seven abstract layers, all of which contribute some data or function to facilitate communication between devices. Not all the layers are useful in every scenario, but it provides an effective framework. Diagrams help to illustrate the intricacies of the layered protocols involved.

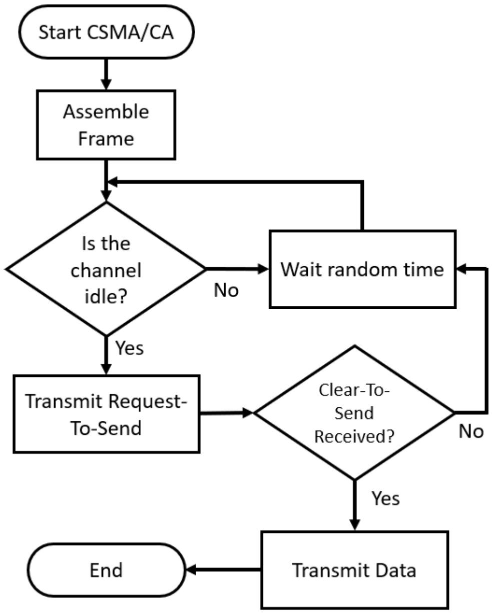


Figure 6: A flowchart representing the decisions involved when sending data to another device to avoid collisions [6]

References

[1] What is the OSI model? — Cloudflare. Available at: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/ (Accessed: 10 January 2024).

[2] Encapsulation in OSI and TCP/IP models (2022) — Study CCNA. Available at: https://study-ccna.com/encapsulation/ (Accessed: 10 January 2024).

[3] What is DNS? — How DNS works — Cloudflare. Available at: https://www.cloudflare.com/learning/dns/what-is-dns/ (Accessed: 10 January 2024).

[4] What happens in a TLS handshake? — SSL handshake — Cloudflare. Available at: https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/ (Accessed: 10 January 2024).

[5] What is Network Address Translation (nat)? (2022) — Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-address-translation-nat/ (Accessed: 10 January 2024).

[6] CSMA with collision avoidance (CSMA/CA) — Tutorialspoint. Available at: https://www.tutorialspoint.com/csma-with-collision-avoidance-csma-ca (Accessed: 10 January 2024).

[7] Froehlich, A. and Burke, J. What is PPP (point-to-point protocol) and how does it work? (2022) — TechTarget Available at: https://www.techtarget.com/searchnetworking/definition/PPP (Accessed: 10 January 2024).

[8] Address resolution protocol (ARP) — IBM. Available at: https://www.ibm.com/docs/en/zos-basic-skills?topic=3-address-resolution-protocol-arp (Accessed: 10 January 2024).