UNIVERSITY OF WESTMINSTER

Networks Fundamentals and security

6COSC019W- Cyber Security

Dr Ayman El Hajjar

January 30, 2024

School of Computer Science and Engineering
University of Westminster

OUTLINE

Introduction to Networking

- What is a Network?
  - Set of technologies that connects computers
  - Allows communication and collaboration between users
  - Collection of computers and devices connected together
- The uses of a network
  - Simultaneous access to data
  - Shared Resources
  - Personal communication
  - Easier data backup
- Main types of Networks
  - Wide Area Network (WAN): Connect systems over a large geographic area
  - Local Area Network (LAN) : Provide network connectivity for computers located in the same geographic area

Networking Layering models

THE OSI REFERENCE MODEL

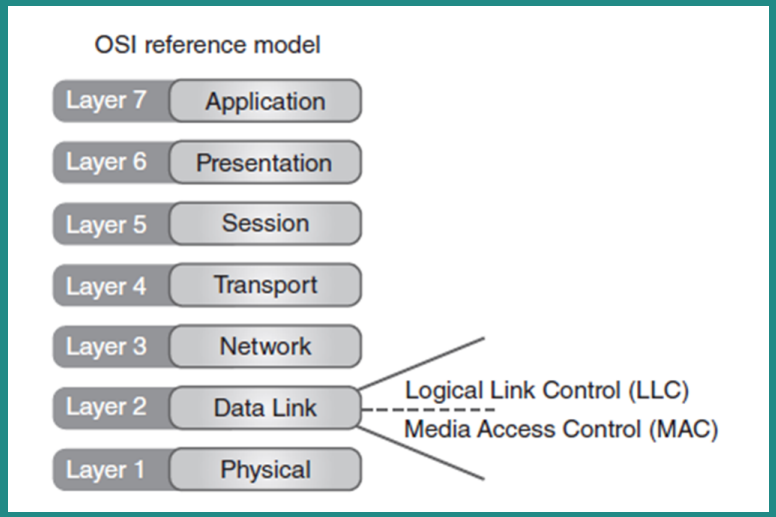


Figure 1: The OSI reference Model

❑ The OSI Reference Model is used mainly in today's networking environment as both a reference model and an effective means of teaching distributed communication.

❑ OSI layers are also referred to by number (7 is the Application Layer, and 1 is the Physical Layer.)

❑ Each layer interacts with the layer above it and the layer below it.

❑ The OSI Reference Model is also implemented in two areas: hardware and software. The bottom two layers are implemented in hardware, and the top five are implemented through software.

OSI LAYERS

Application layer

- The Application layer is responsible for interacting with end users applications. Is the point at which application software accesses network services and the is formatted in a format related to the application

Presentation layer

- The Presentation Layer responsible for the coding of data. The Presentation Layer includes file formats and character representations. From a security perspective, encryption generally takes place at the Presentation Layer.

OSI LAYERS

Session layer

- The Session Layer is responsible for maintaining communication sessions between computers. The Session Layer creates, maintains, and disconnects communications that take place between processes over the network.

Transport layer

- The Transport Layer is responsible for breaking data into packets and properly transmitting it over the network. Flow control and error checking take place at the Transport Layer.

Network layer

- The Network Layer is responsible for the logical implementation of the network. In TCP/ IP networking, logical addressing takes the familiar form of IP addresses.

OSI LAYERS

Data Link layer

- The Data Link Layer is responsible for framing data received from the Network Layer and preparing it for transmission over the Physical Layer such as the physical addressing, controls the access to the physical medium, and detecting and correcting errors that may occur during transmission

Physical layer

- The Physical Layer is responsible for the physical operation of the network. The Physical Layer must translate the binary ones and zeros of computer language into the language of the transport medium.

TCP/IP MODEL

TCP/IP layers	
Application Layer	Provides applications with standardized data exchange. At the application layer, the payload is the actual application data.
	It combines three layers of functions of OSI- Application, presentation and session layers
Transport Layer	Responsible for maintaining end-to-end communications across the network.
	It represents the Transport layer in OSI
Network Layer	The network layer, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries.
	It represents the Network layer in OSI
Data link Layer	The data link layer, also known as the network interface layer or physical layer, consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network.
	It combines two layers functions of OSI- Data Link and Physical layers

Figure 2: TCP/IP model

INTERNET PACKET ENCAPSULATION

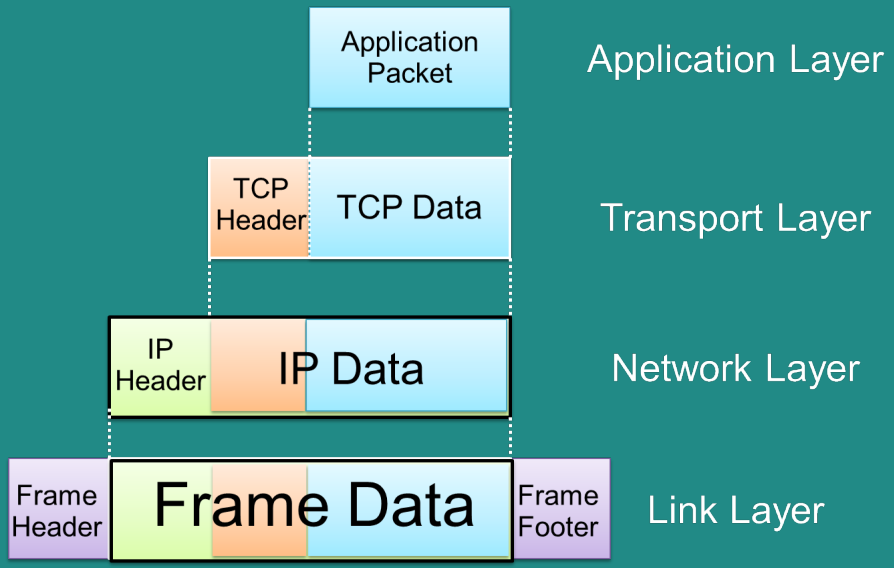


Figure 3: What we add at each layer

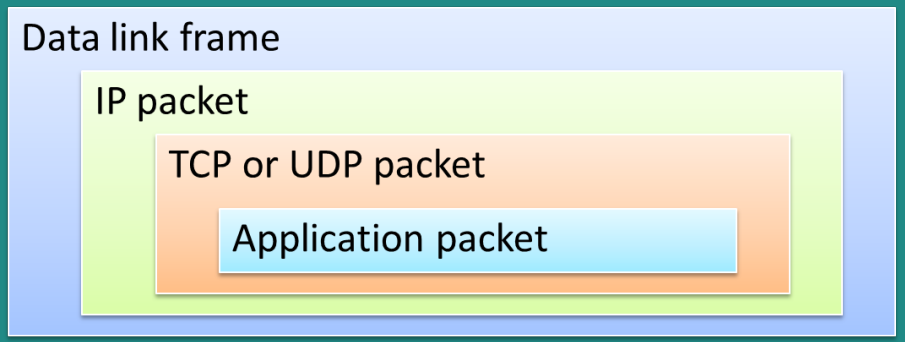
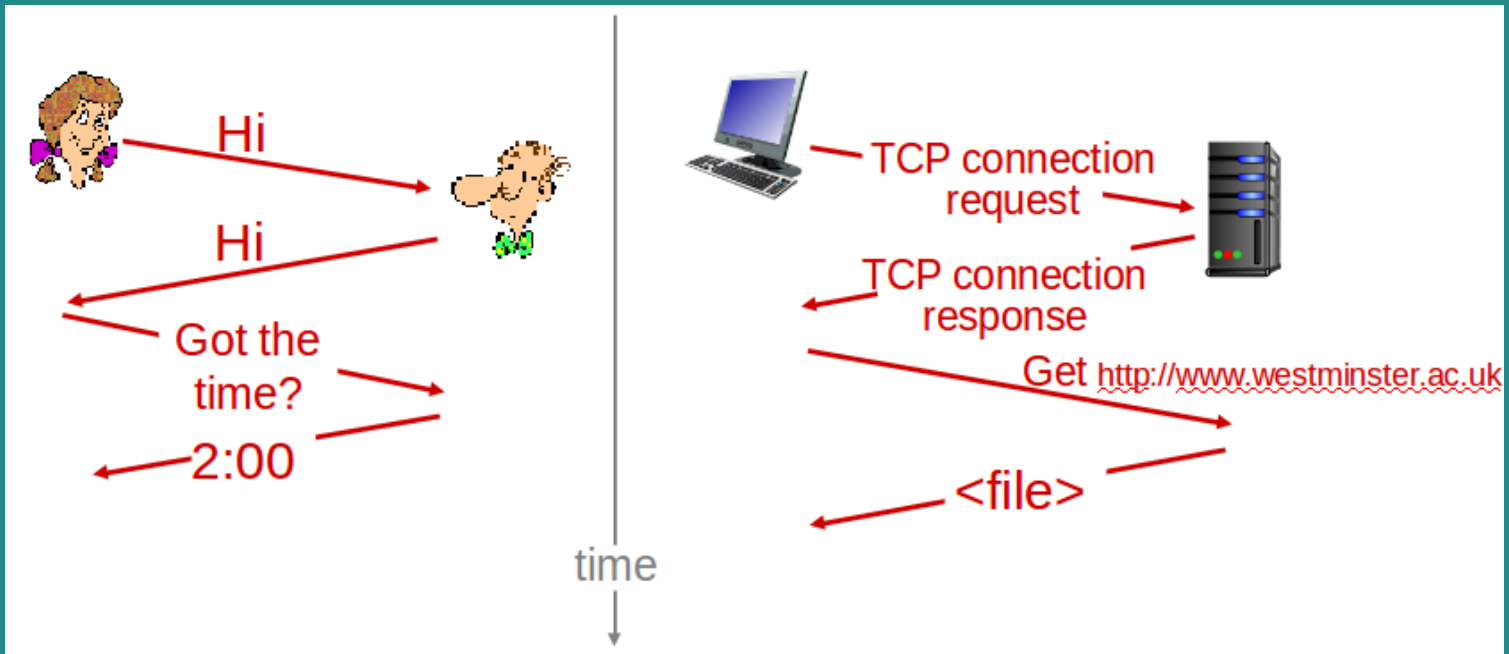


Figure 4: Encapsulated contents

WHAT IS A PROTOCOL?

Protocol

- A protocol is a set of rules and formats that govern the communication between communicating peers.
  - set of valid messages
  - meaning of each message
- A human protocol and a computer network protocol



PROTOCOLS

- A protocol defines the rules for communication between computers
- Protocols are broadly classified as connectionless and connection oriented
- Connectionless protocol
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (UDP)
- Connection-oriented protocol
  - Provides a reliable connection stream between two nodes
  - Consists of set up, transmission, and tear down phases
  - Creates virtual circuit-switched network
  - E.g., transmission control protocol (TCP)

Packets Contents

1. Control information for the packet: **header** and **footer or Trailer**
   - Headers are added at the beginning of the packet. They contain information about the about the packet, such as its origin and destination IP addresses, type of protocol, the sequence number and acknowledgment
   - Footers are placed at the end of the packet. They contain information such as error-checking data and the timestamp.
2. Data: **payload**

ENCAPSULATION

- A network protocol N1 can use the services of another network protocol N2
  - A packet p1 of N1 is encapsulated into a packet p2 of N2
  - The payload of p2 is p1
  - The control information of p2 is derived from that of p1

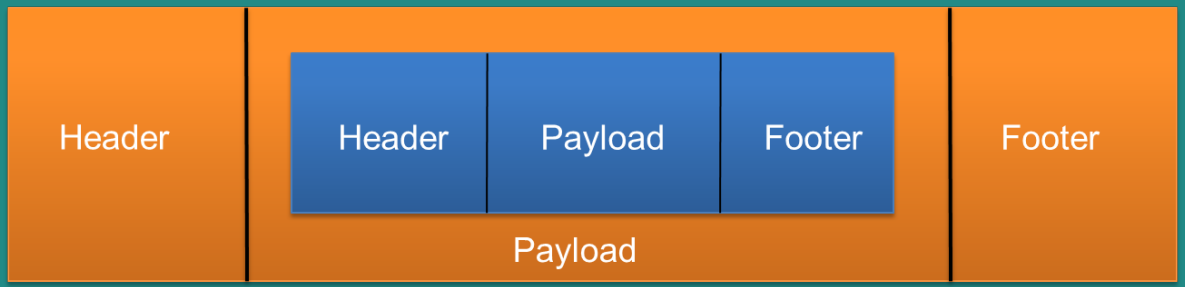
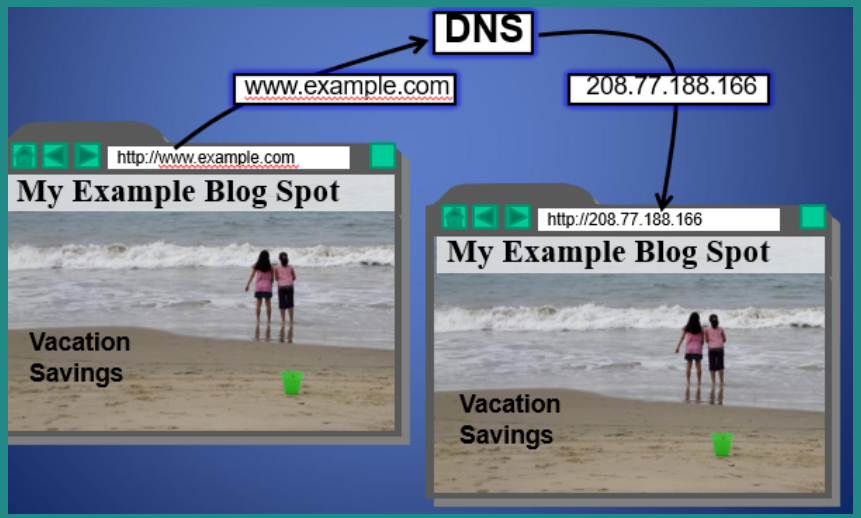


Figure 5: Network packets Encapsulation

Protocols in different layers

DOMAIN NAME SYSTEM

- **The domain name system (DNS)** is an application-layer protocol for mapping domain names to IP addresses
- DNS provides a distributed database over the internet that stores various **resource records**, including:
  - Address (A) record: IP address associated with a host name
  - **Mail exchange**(MX) record: mail server of a domain
  - **Name server** (NS) record: authoritative server for a domain

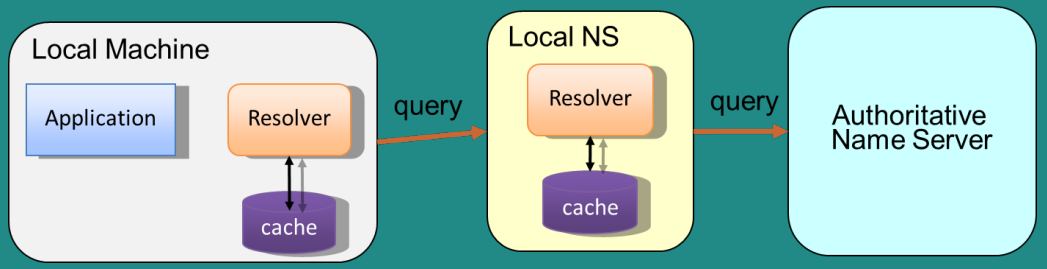


DNS Caching

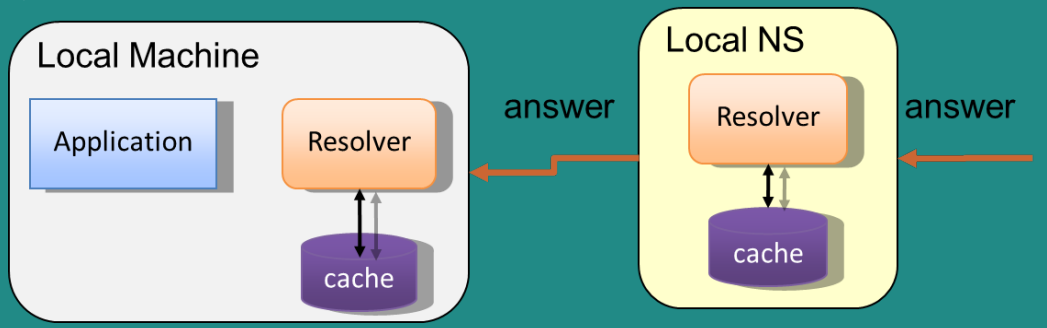
- There would be too much network traffic if a path in the DNS tree would be traversed for each query
  - Root zone would be rapidly overloaded
- DNS servers cache results for a specified amount of time
  - Specified by ANS reply's time-to-live field
- Some operating systems maintain DNS caches
  - Windows: **ipconfig /displaydns**
  - Linux: If you are on Ubuntu , it is possible to kill the cache file and create it again.
    - **sudo killall -USR1 systemd-resolved**
    - **sudo journalctl -u systemd-resolved > /cachemydns.txt**
    - **less cachemydns.txt**
- Associated privacy issues
- DNS queries are typically issued over UDP on port 53
  - 16-bit request identifier in payload

DNS CACHING

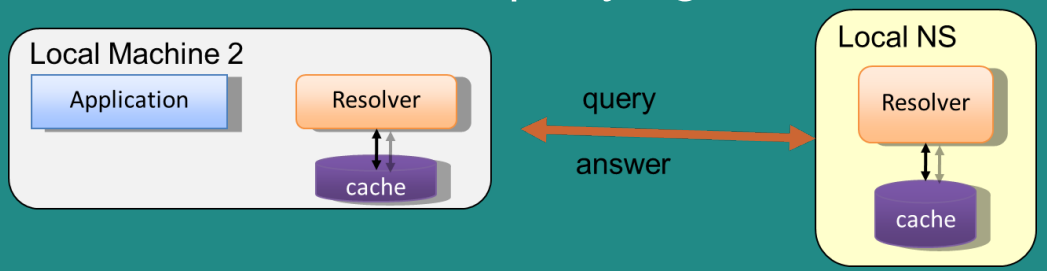
1 ❑ query yourdomain.org



2 ❑ receive reply and cache at local NS and host



3 ❑ use cached results rather than querying the ANS



TRANSPORT LAYER: USER DATAGRAM PROTOCOL (UDP)

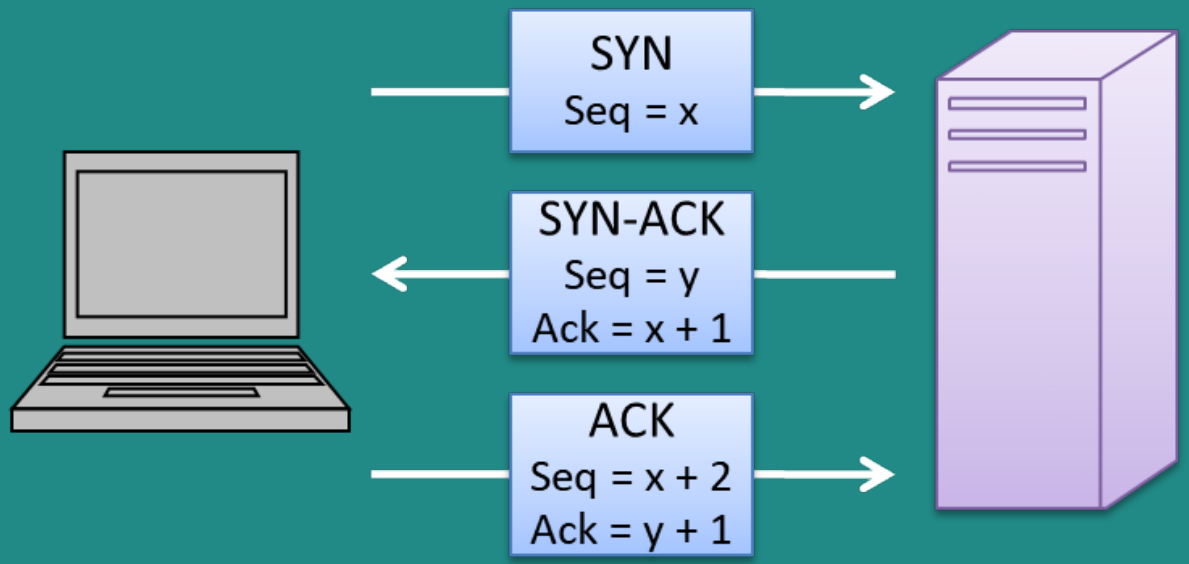
- Lightweight and connectionless
- Small packet sizes (60% less than TCP), in header size UDP (8 bytes) & TCP (20 bytes)
- No connection to create and maintain
- More control over when data is sent
- Does not compensate for loss of packet
- Does not deliver or guarantee packet delivery in order
- Does not check if network is busy

Transport Layer: Transmission Control Protocol (TCP)

- Reliable and connection-based
  - Sequence numbers, timeouts, and retransmissions protect against loss and reordering.
  - Sequence numbers: loss, reordering, duplication.
  - Timeouts: loss.
  - Retransmission: loss
- TCP packets have a header section with a flags field
- Consider 4 of the possible flags
  - SYN (Synchronise)
  - ACK (Acknowledge)
  - FIN (Finished)
  - RST (Reset)

TRANSPORT LAYER: TCP PACKETS

- Three way handshake TCP packets exchange
  - ☞ To initiate a TCP connection the initiating system sends a SYN packet to the destination.
  - ☞ Destination sends an ACK to acknowledge the receipt of the first packet (a combined SYN/ACK packet).
  - ☞ The first system sends an ACK packet to acknowledge receipt of the SYN/ACK
  - ☞ Data Transfer can then begin!



IP ADDRESSING

IPv4 addresses

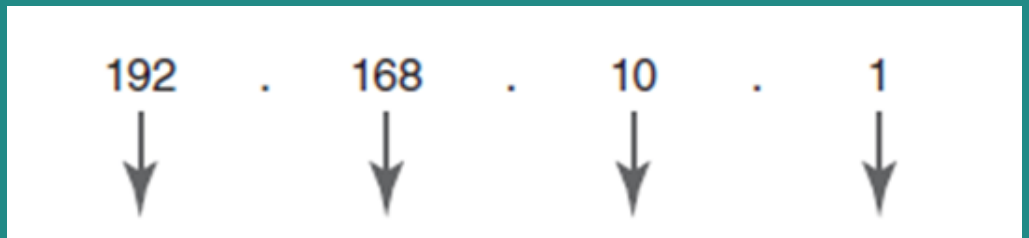
- Four-byte (32-bit) addresses that uniquely identify every device on the network
- Still the most common

IPv6 addresses

- Are 128 bits long
- Provide more unique device addresses
- Are more secure

IPv4 Addressing

- 32 bits Binary address
- Divided into 4 part, separated by a . of 8 binary each.
- Each 8 binary digits are converted to Decimal. Hence is called Dotted Decimal.
- Each IP represents the Network address and the host address
- For example, the IP address in this figure tell us the following:
  - 192.168.10.0 is the Network Address
  - 192.168.10.255 is the Broadcast address
  - Hosts can have any IP between 192.168.10.1 to 192.168.10.254
  - This is called a Class C IP address. In class C- the network part is the three first dots. The host part is only the last decimal number of the IP.



IP Addressing- Dynamic

Dynamic Host Configuration Protocol (DHCP)

- DHCP is used within a network to simplify the configuration of each user's computer

To obtain, renew or refresh a DHCP IP address dynamically you can use (as administrator):

In windows: **ipconfig /registerdns**
In Linux: **sudo dhclient**

THE LAB DHCP SCENARIO

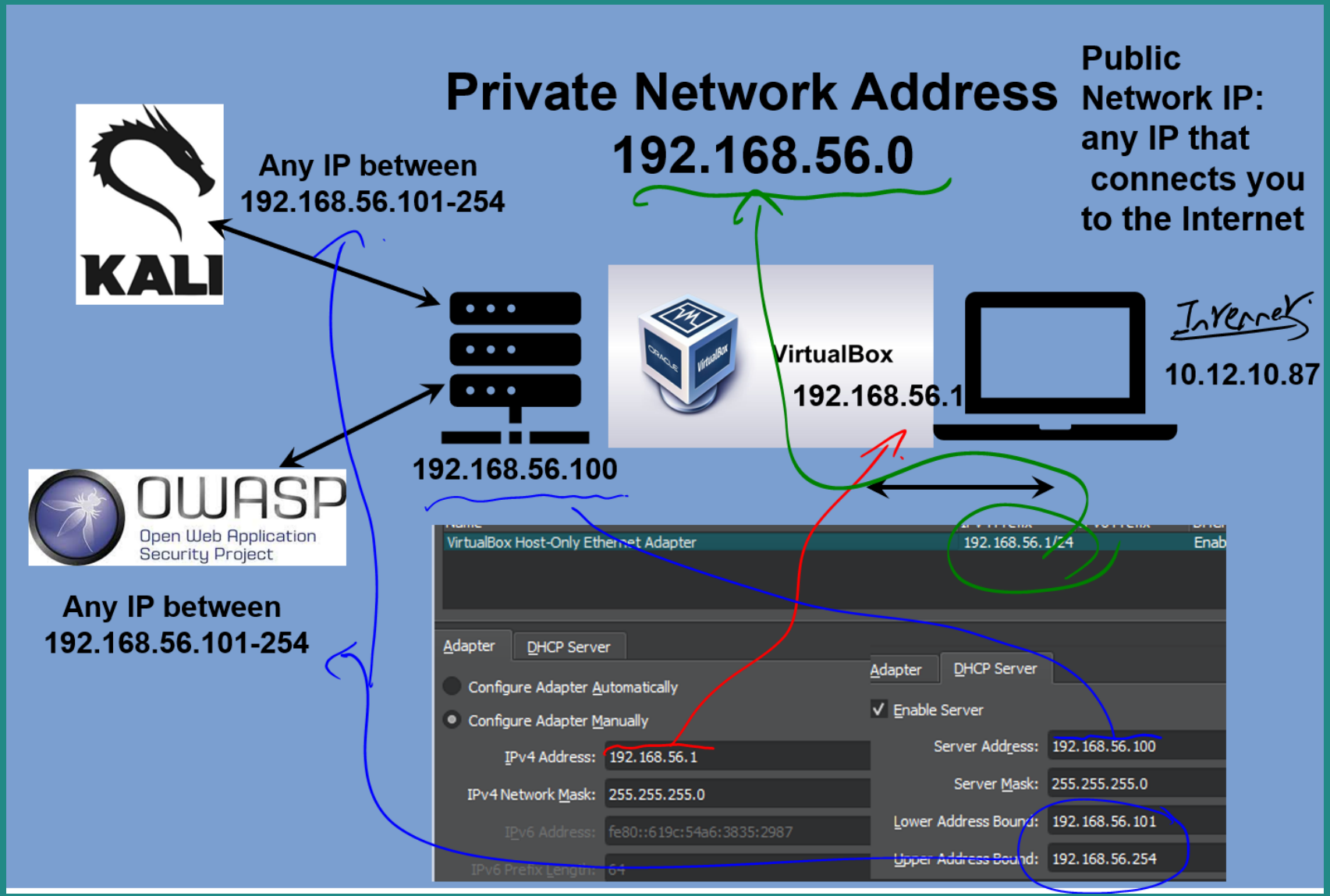


Figure 7: A DHCP Class C Network Example: The lab scenario

MAC Address

- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- On windows you can use **getmac** to obtain the MAC address of your machine. It is also listed when you type **ipconfig**.
- On Linux, you can see your MAC adddress when you type **ip addr**. it will be labelled by link/ether

ADDRESS RESOLUTION PROTOCOL (ARP)

- The **address resolution protocol (ARP)** connects the network layer to the data layer by converting IP addresses to MAC addresses
- ARP works by **broadcasting** requests and caching responses for future use
- The protocol begins with a computer broadcasting a message of the form
  - who has <IP address1> tell <IP address2>
- When the machine with **IP address1** or an ARP server receives this message, its broadcasts the response
  - <IP address1> belongs to <MAC address>
- The Linux and Windows command **arp a** displays the ARP table:

```
C:\Users\ayman>arp -a

Interface: 192.168.56.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.56.105        08-00-27-53-0c-ba     dynamic
  192.168.56.111        08-00-27-5f-19-98     dynamic
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
```

NETWORK INTERFACE

- Although network interfaces are not particularly protocols and they are physical devices, they determine which network interface card the system will use. They are considered both Physical layer and Data link layer interface as they also give the MAC address of the interface.
- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames
- Each network interface gets the frames intended for it
- A hacker/pen-tester will conduct traffic sniffing by configuring the network interface to read all frames (promiscuous mode, sometimes called Monitor mode)

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 2- Networking Foundations, CEH v11 Certified Ethical Hacker Study Guide
  - Chapter 5, Network and telecommunications, Fundamentals of Information Systems Security
  - Chapter 19 Introduction, CyBOK, The Cyber Security Body of Knowledge