

- **Zeinab Rezaeifar**
- **Lecturer in Cyber Security**
- **Zeinab.Rezaeifar@uwe.ac.uk**
- **5 January 2023**

ACE CSE TRAINING THE TEACHERS

Why Cybersecurity is important

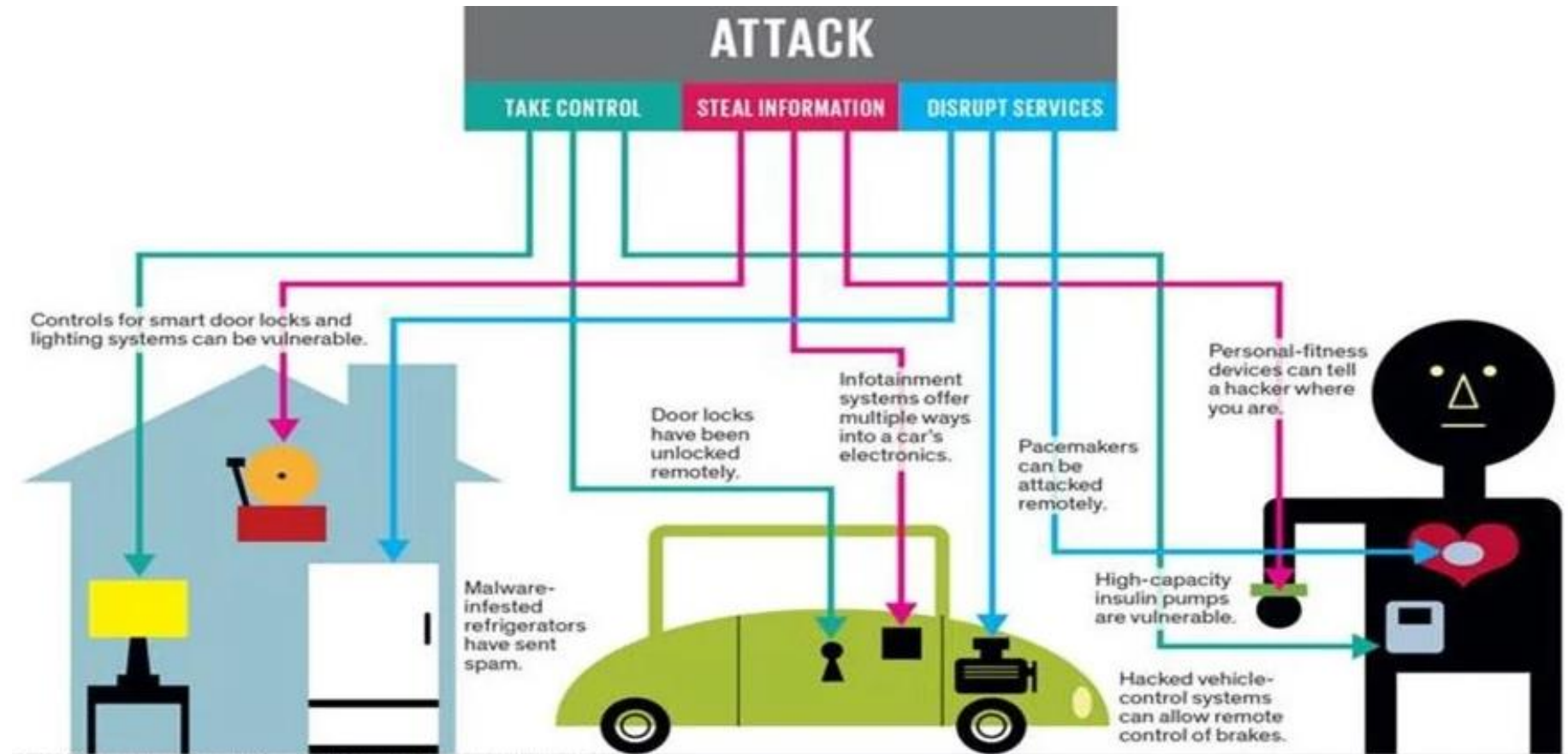
- Increasing cyber crime
 - Cyber crime reaches to £2 trillion in 2019 [1].
- Connecting everything to Internet
- Cost of Cyber Risks
 - It will be reached to £10.5 trillion by 2025 [2].
- Security of data



[1] [Why Cyber security is Important to you \[Especially in 2022\] \(simplilearn.com\)](https://www.simplilearn.com)

[2] [Cybercrime To Cost The World \\$10.5 Trillion Annually By 2025 \(cybersecurityventures.com\)](https://www.cybersecurityventures.com)

Why Computer Network is important in Cybersecurity




<http://spectrum.ieee.org/img/03Internetf2-1424374486017.jpg>

A person wearing a dark hoodie is shown from the chest down, sitting at a desk and typing on a keyboard. The background is dark with a network of glowing red lines and nodes, suggesting a digital or cyber environment. The overall tone is serious and technical.

Cyber Threat Map

[Cyber Threat](#)



Intended Outcome Learning

- Make computer network concepts more sensible
- Exercise some practical activities regarding computer network
- Exercise some network attacks
- Discuss and share some ideas to how students can be motivated and engaged regarding these concepts

Overview of the Sessions

Session 1

- How the network works with real life examples
- Practice some activity regarding sending and receiving packets
- Practice some network concept using Raspberry Pi

Session 2

- Look at computer network layers and protocols
- Look at the SSH protocol
- How security misconfiguration can cause an attack
- Look at brute force attacks in the network

Session 3

- Check how firewalls work
- Practice some commands to understand how firewalls work

Timetable

Time	Description
9 AM to 10:15 AM	Session1: Send and receiving packet
10:15 AM to 10:30 AM	Coffee break
10:30 AM to 12:15 PM	Session2: SSH and brute force attacks
12:15 PM to 1 PM	Lunch break
1 PM to 2 PM	Session3: Firewall
2 PM to 2: 15 PM	Coffee break
2:15 to 3 PM	Discussion



in association with
**National Cyber
Security Centre**



Department for
Digital, Culture,
Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

Session 1

- How the network works with real life examples
- Practice some activity regarding sending and receiving packets
- Practice some network concept using Raspberry Pi

What is Network

- A group of people or things that are interacted with each other
- Exchange information

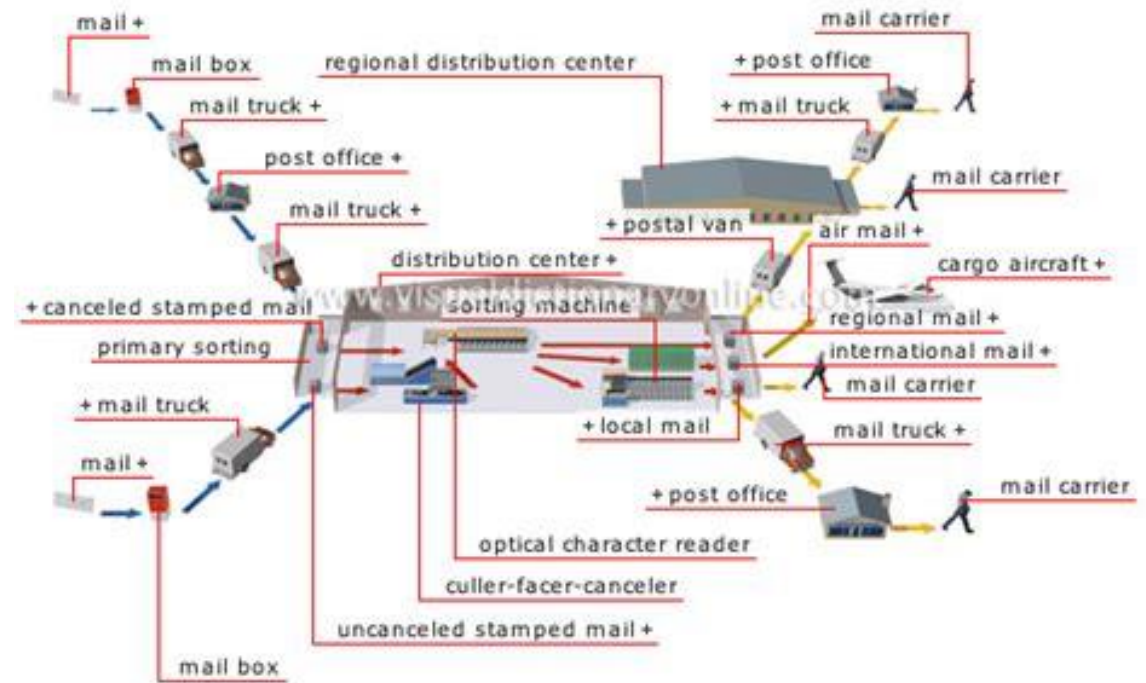


Internet vs Network

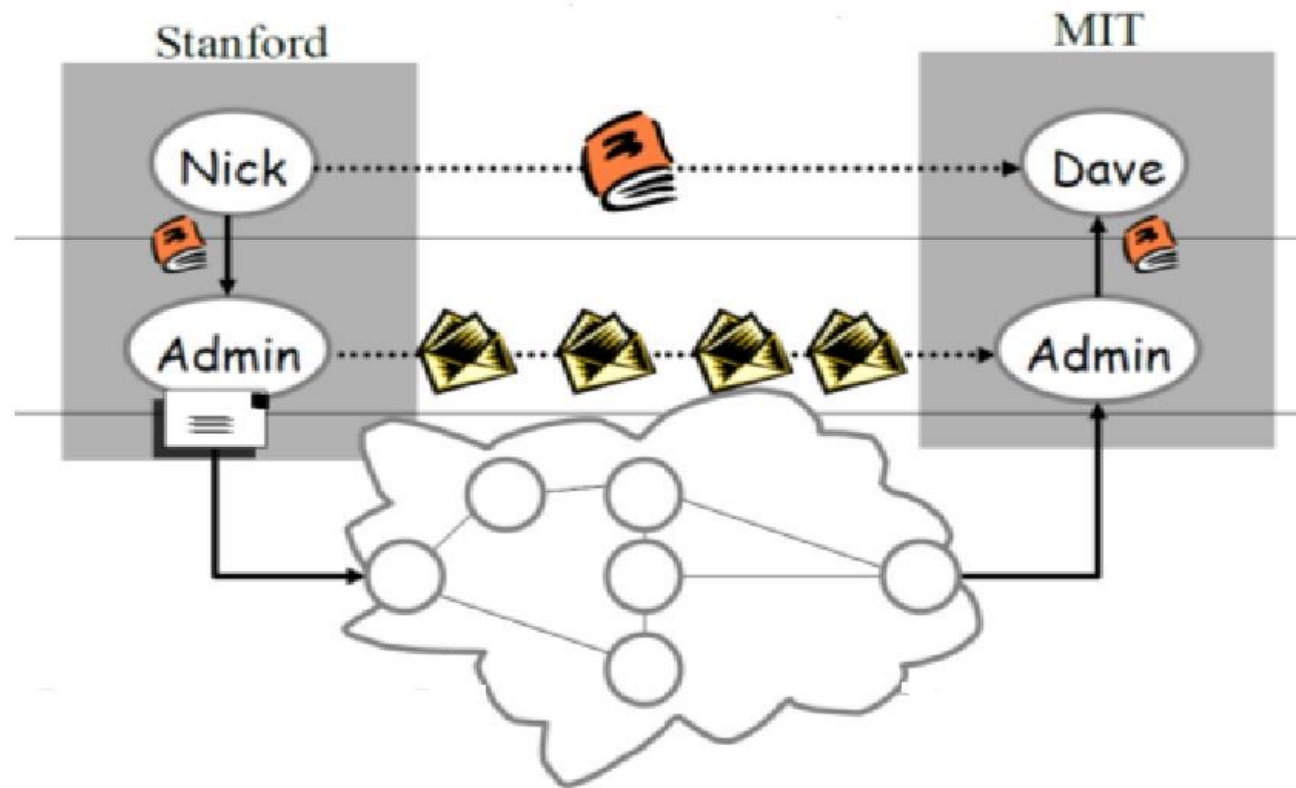
- The Internet is a big network that consists of many small networks
- The first Internet was the ARPANET project in the late 1960s by United States Defence department
- The Internet as we know today was invented by Tim Berners-Lee in 1989 by the creation of the World Wide Web (WWW)
- While small networks are called private networks, the networks that connected these small networks are called public network or Internet

Postal network

- Deliver different items like letters and packages
- Sender and receiver are identified by postal address (such as name house, Steet, city and country)
- The letter may pass through several mail trucks and mail distribution centre to reach its destination

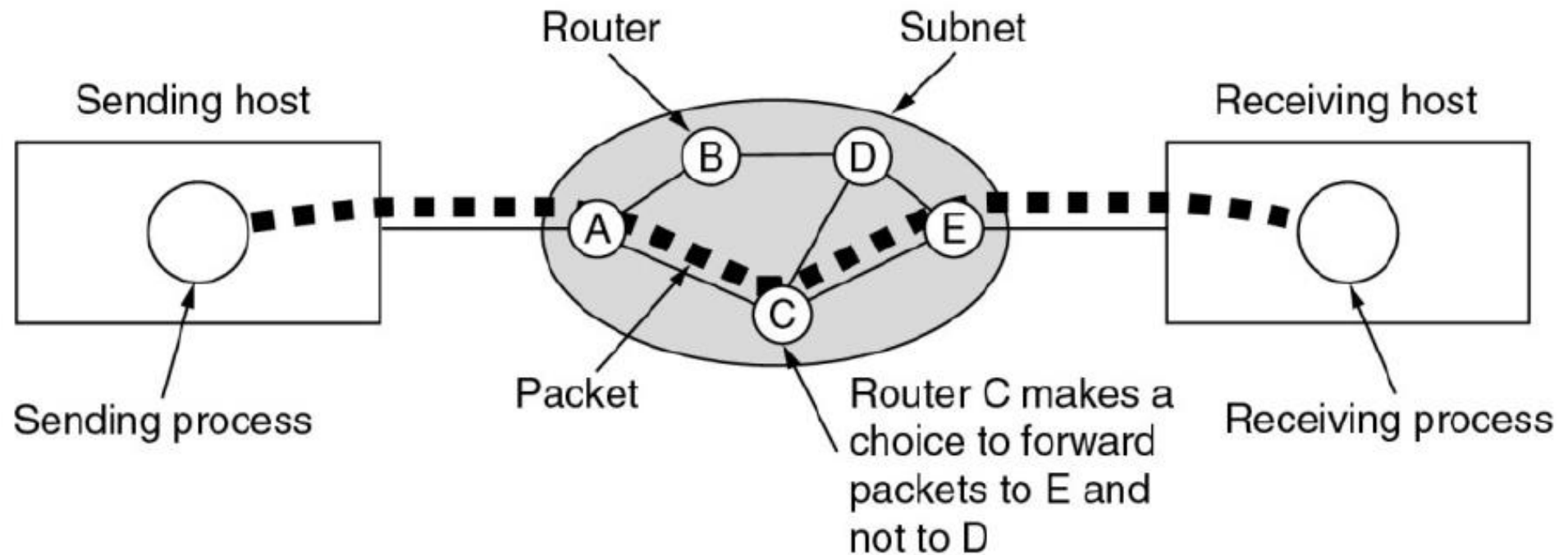


Introduction to postal system



A STREAM OF PACKETS FROM SENDER TO RECEIVER

- The packet in the network may pass from different routers to reach its destination



A Practical Example: Sending a Letter

- Send the letter inside the envelope
 - How to packet goes from a sender to a receive
- Send the letter inside the box with a locker
 - The importance of the encryption

Identifying devices on a network

- Internet Protocol (IP) address
 - Logical address to find location of a device and it can change in different networks-like your id in each school will be different
 - Similar to our home address in the postal network
- A Media Access Control (MAC) address
 - Physical address to send data to the right device through physical communication links. MAC address is unique and does not change-like your name which does not change in different schools
 - Similar to our names in the postal network

How to find your IP address

- Type ifconfig command in the terminal to find IP address

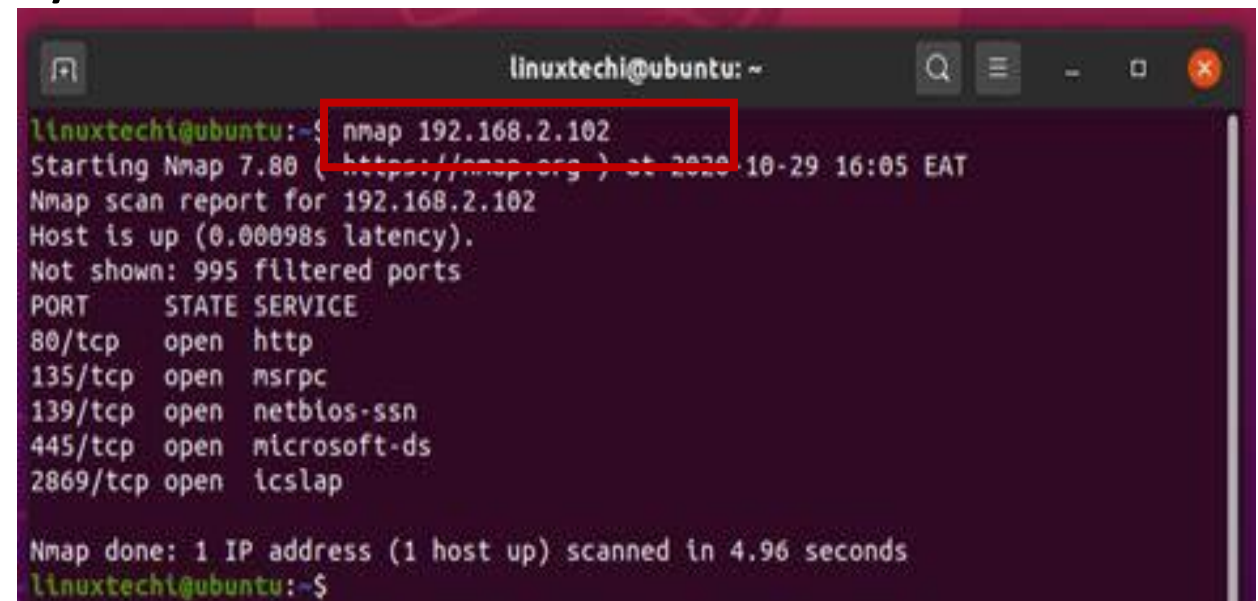
```
[01/03/23]STUDENT_ID-uwe@192.168.93.128: ~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:a2:84:b9:d9 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.93.128 netmask 255.255.255.0 broadcast 192.168.93.255
    inet6 fe80::4c3a:5b10:1c8f:be6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:46:e9:89 txqueuelen 1000 (Ethernet)
    RX packets 243 bytes 272531 (272.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 149 bytes 15620 (15.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 171 bytes 13845 (13.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
```


Network Mapper (Nmap)

- It is a network scanner tool
- It is used to discover host, service and operating system on a computer network by sending packets and analysing the responses
- It is used to detect vulnerability in the network
- Different method of scan
 - Nmap -sT [IP address]

A terminal window titled 'linuxtechi@ubuntu: ~' showing the execution of the command 'nmap 192.168.2.102'. The output displays the Nmap scan report for the target IP, including the host's status and a list of open ports with their corresponding services. The command 'nmap 192.168.2.102' is highlighted with a red box.

```
linuxtechi@ubuntu:~$ nmap 192.168.2.102
Starting Nmap 7.80 (https://nmap.org) at 2020-10-29 16:05 EAT
Nmap scan report for 192.168.2.102
Host is up (0.00098s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  iclslap

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
linuxtechi@ubuntu:~$
```

[Nmap - Wikipedia](#)

[20 Awesome Nmap Command Examples in Linux - linuxhowto.net](#)

[Nmap Commands | Best Nmap Commands to Scan Network \(educba.com\)](#)



in association with
**National Cyber
Security Centre**



Department for
Digital, Culture,
Media & Sport

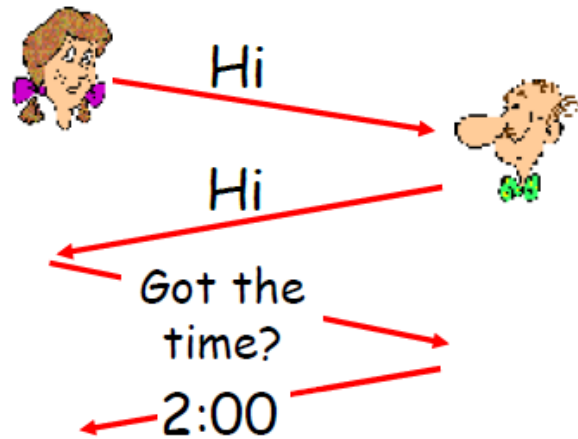
Academic Centre of Excellence in **Cyber Security Education**

Session2

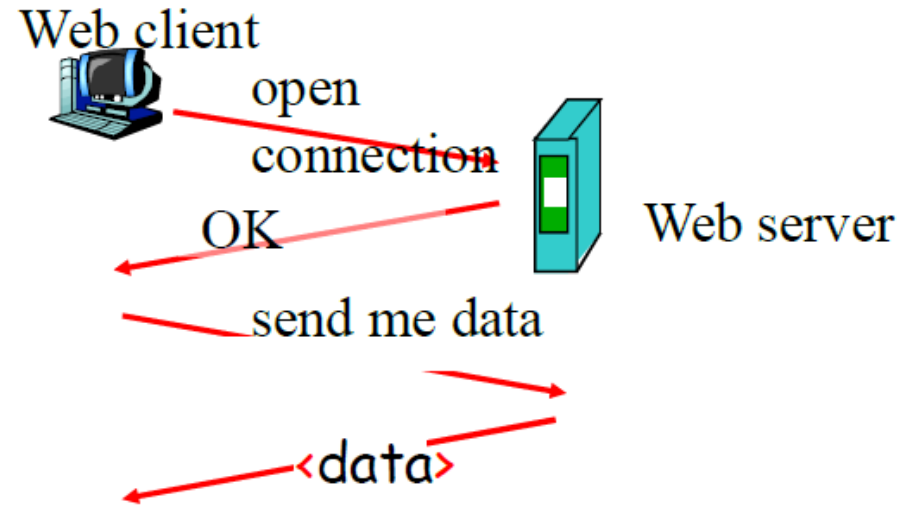
- Look at computer network layers and protocols
- Look at the SSH protocol
- How security misconfiguration can cause an attack
- Look at brute force attacks in the network

Computer Protocol Vs Human Protocol

Human Protocol



Computer Protocol



time
↓

Ping Command

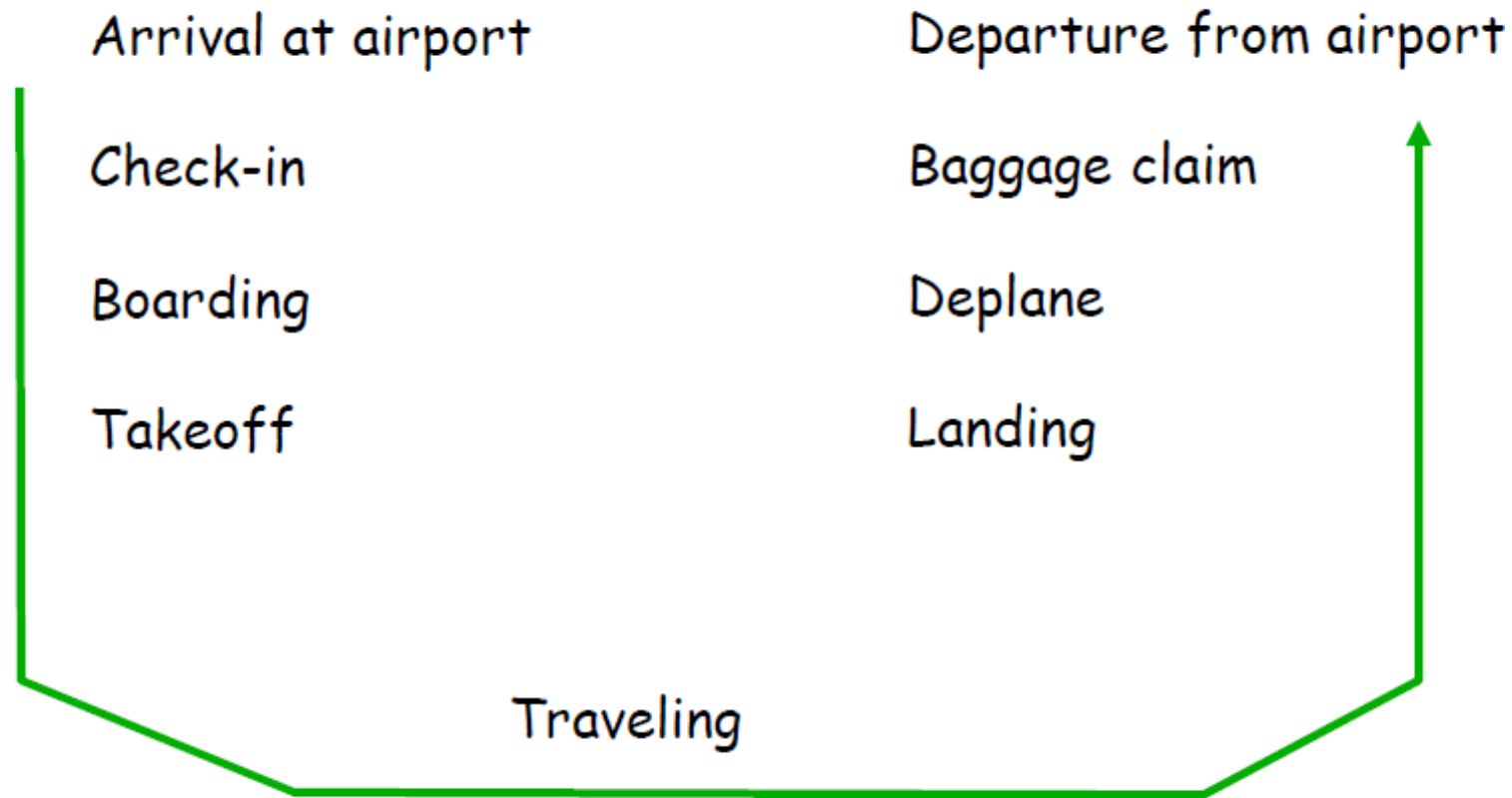
- Ping command is used to check the reachability to a host
- Ping uses Internet Control Message Protocol (ICMP) to find connection between devices

```
[01/03/23]STUDENT_ID-uwe@192.168.93.128: $ ping 192.168.45.24
PING 192.168.45.24 (192.168.45.24) 56(84) bytes of data:
64 bytes from 192.168.45.24: icmp_seq=1 ttl=128 time=98.5 ms
64 bytes from 192.168.45.24: icmp_seq=2 ttl=128 time=7.52 ms
64 bytes from 192.168.45.24: icmp_seq=3 ttl=128 time=46.4 ms
64 bytes from 192.168.45.24: icmp_seq=4 ttl=128 time=11.4 ms
64 bytes from 192.168.45.24: icmp_seq=5 ttl=128 time=87.2 ms
64 bytes from 192.168.45.24: icmp_seq=6 ttl=128 time=103 ms
64 bytes from 192.168.45.24: icmp_seq=7 ttl=128 time=7.35 ms
64 bytes from 192.168.45.24: icmp_seq=8 ttl=128 time=8.71 ms
64 bytes from 192.168.45.24: icmp_seq=9 ttl=128 time=143 ms
64 bytes from 192.168.45.24: icmp_seq=10 ttl=128 time=10.8 ms
64 bytes from 192.168.45.24: icmp_seq=11 ttl=128 time=9.35 ms
█
```

Layers

- To do a complex work, it splits to different level
- The networks are organized to different level or layers
- Each layer work provide service to upper layer
- However, each layer does not need to know how the process will be done with previous layer

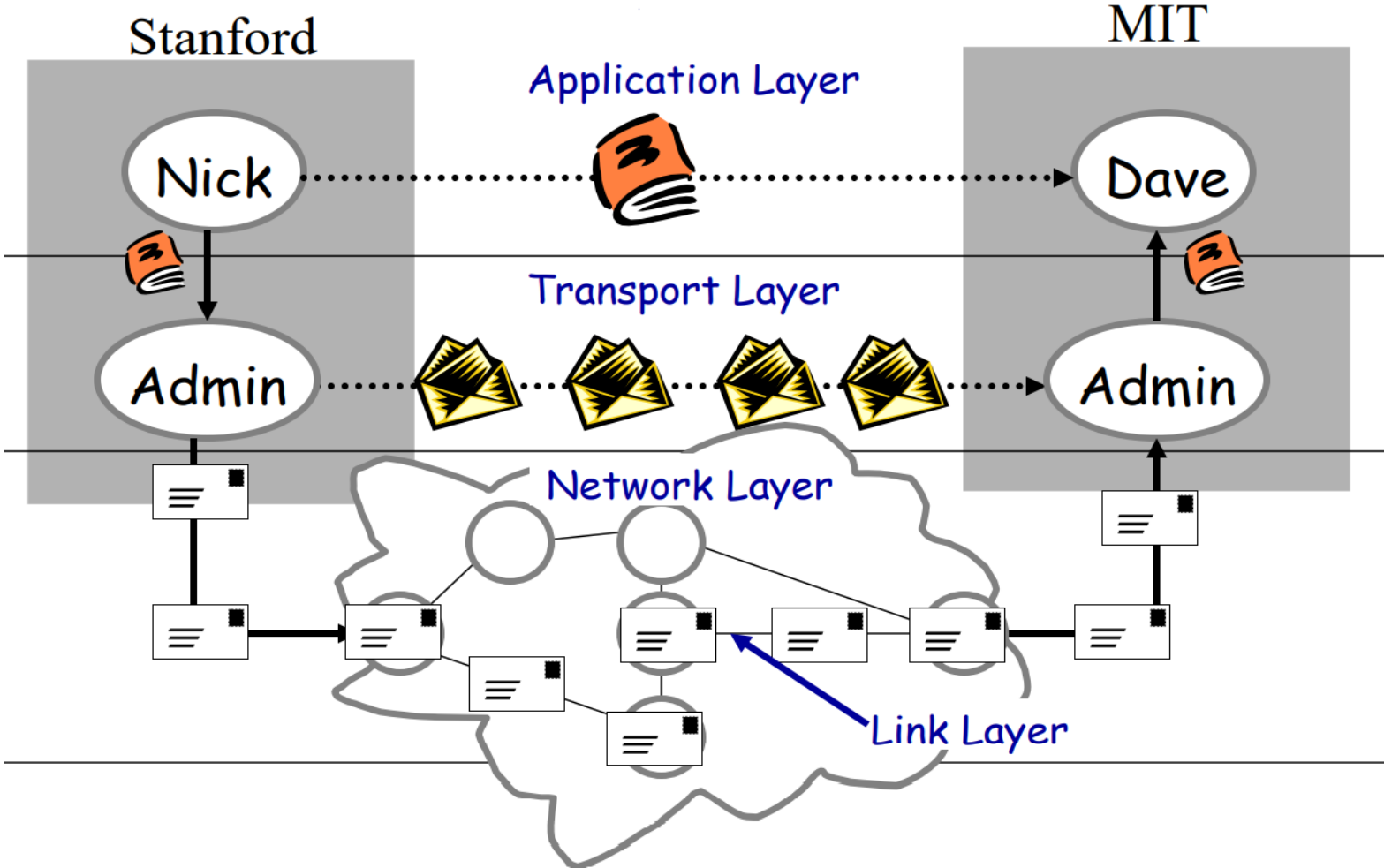
Solve air line problem using layering



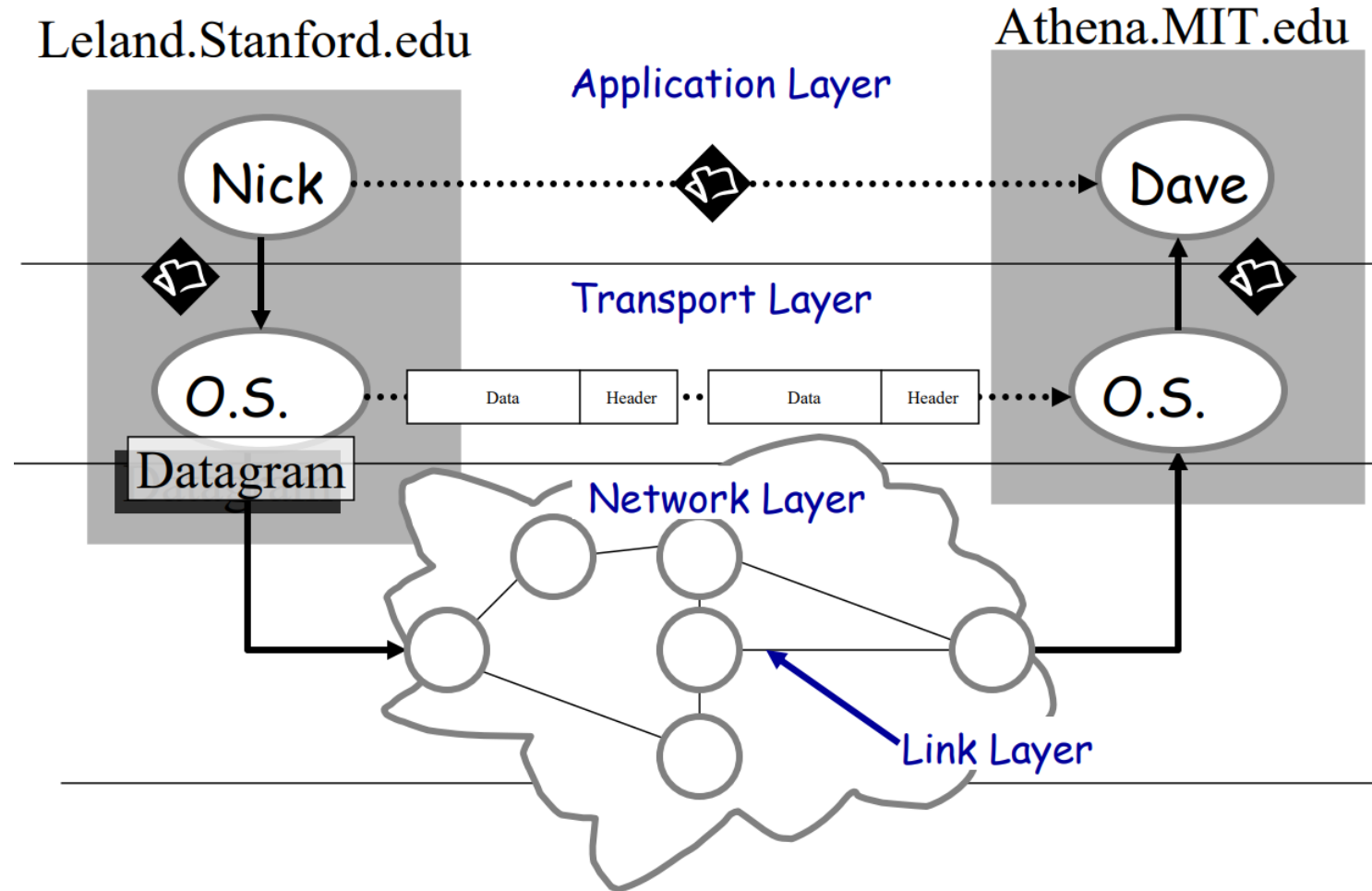
Network architecture

- A set of layers and protocols called network architecture
- We have two famous network architecture :
 - OSI (Open Source Interconnection) model (7 layers)
 - TCP/IP (Transmission Control Protocol/ Internet Protocol) architecture (Internet)

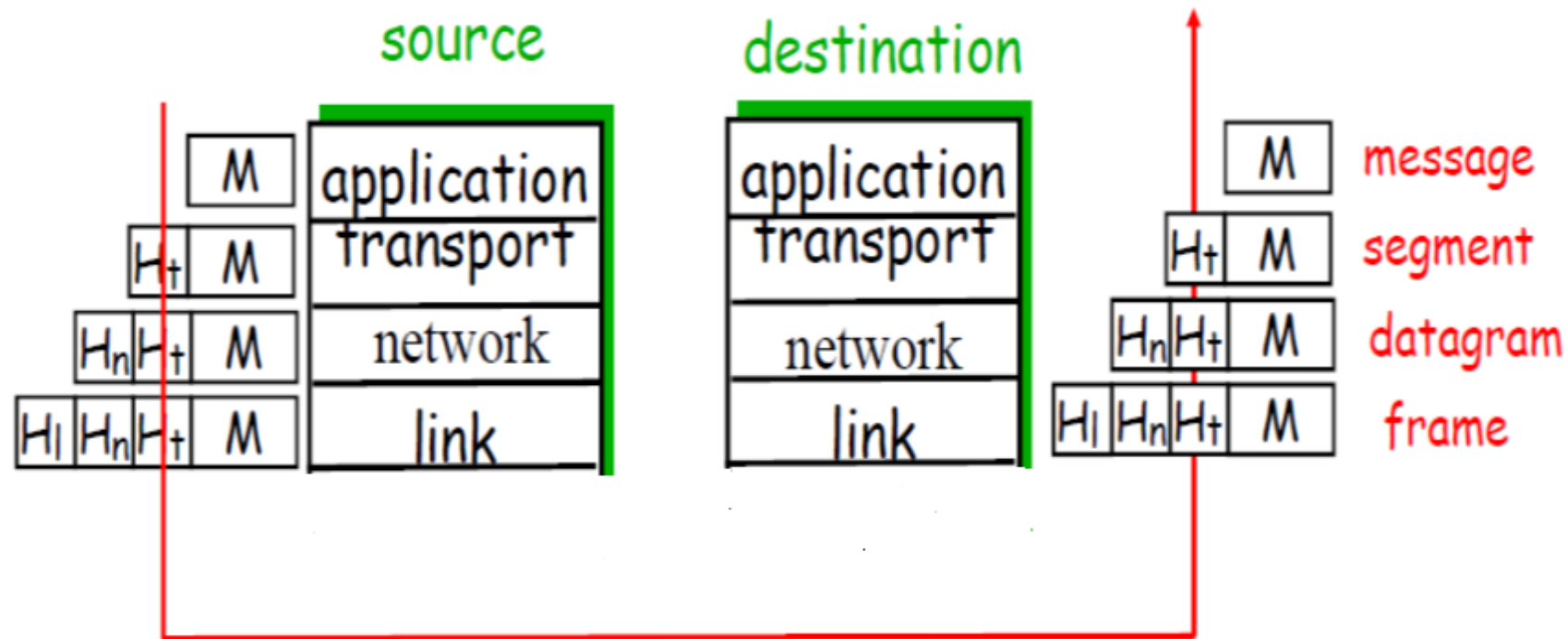
Mail System VS Internet Infrastructure



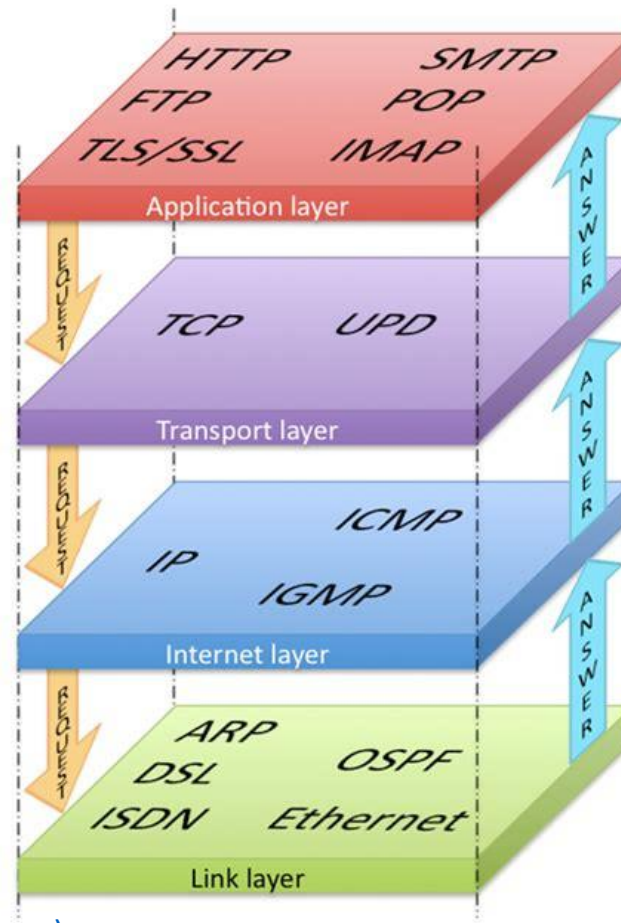
Mail System VS Internet Infrastructure



Internet Stack compare to airline traveling



TCP/IP Stack (Internet Protocol)



[What is the TCP/IP Stack \(smartbuildingsacademy.com\)](http://smartbuildingsacademy.com)

[Network Protocols - ARP, FTP, SMTP, HTTP, SSL, TLS, HTTPS, DNS, DHCP - Networking Fundamentals - L6 - YouTube](#)

SSH Protocol

- It is referred as Secure Shell protocol
- It is a protocol to securely access one computer from another computer
- To use SSH protocol and access the remote machine try the following command in the terminal
 - `ssh remote_username@<ip address of remote_host>`
 - If a password is set we then enter that user's password, which acts as a method of verification

Password attacks

- It is a common attack that attacker by uncovering your password can access your valuable information
 - Password spry : try common password or default password
 - Dictionary attacks: try a common list of passwords
 - Brute force attack: try all combination of letters, numbers and symbols

Breaking passwords

- To each of the following passport Give 1 to 4 number where 1 is easiest and 4 is hardest to break the password
 - Km1m 3
 - Password 1
 - ML@p1* 4
 - 3trawbery 2

Hydra

- Hydra is a tool for many operating system such as Kali linux to lunch bruteforce attack on login credentials
- Hydra has a option for attacking login on different protocols such as ssh
- You can use “wordlists” and pass it to hydra to test different password and find login credential

```
hydra -l kali -P /usr/share/wordlists/fasttrack.txt <ip.address> ssh -s <target port> -V
```



User

Password



Gold Award



in association with
**National Cyber
Security Centre**



Department for
Digital, Culture,
Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

Session 3

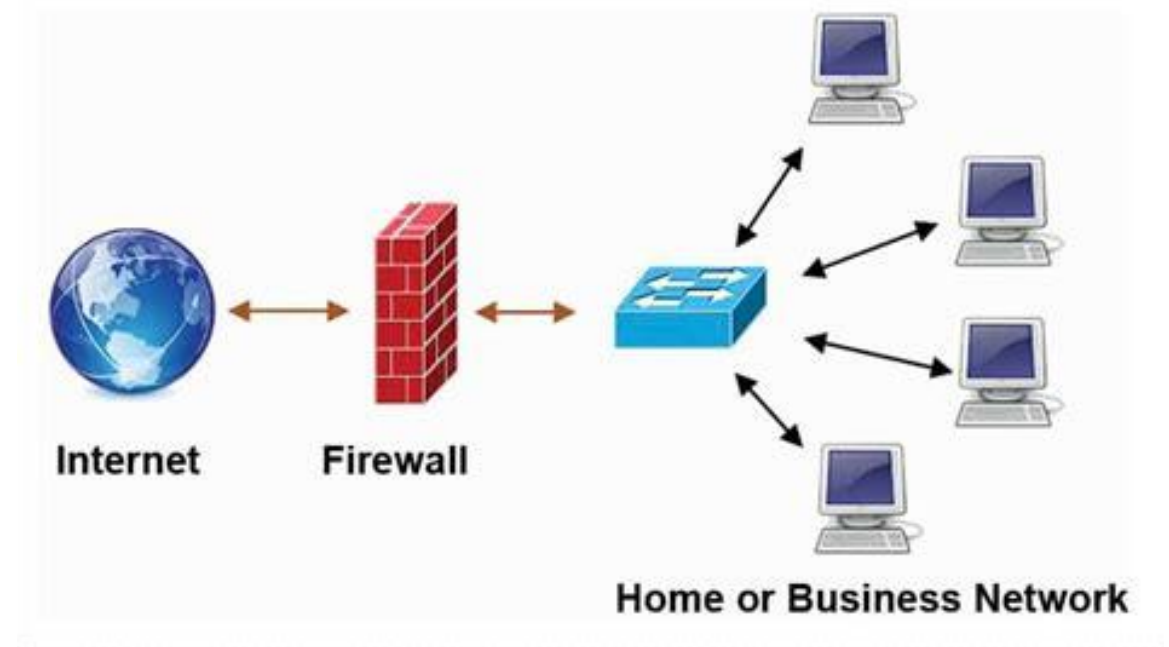
- Check how firewalls work
- Practice some commands to understand how firewalls work



Use a fire door to stop spreading fire to other side

What is firewall

- It is a network security system to protect your device from unwanted traffic
- Control incoming and outgoing traffics based on predetermined security rules
- It also prevents or limits illegal accesses to private networks
- The firewall can be hardware like the server or software that operates inside your computer



Some interesting links regarding firewall

- How to turn on firewall on [Windows](#) and [Mac](#)
- [What is a Firewall? – YouTube](#)
- Firewall game : [permission impossible](#)

IPTables firewall

- Firewall makes barrier between untrustworthy and trustworthy networks
- creates rules to control incoming and outgoing traffic to your computer or trustworthy network
- By using IPTables command we define a set of rules to control, allow or block incoming or outgoing network traffics.

[The Beginner's Guide to IPTables \(Linux Firewall\) Commands \(tecmint.com\)](https://www.tecmint.com/the-beginners-guide-to-iptables-linux-firewall-commands/)