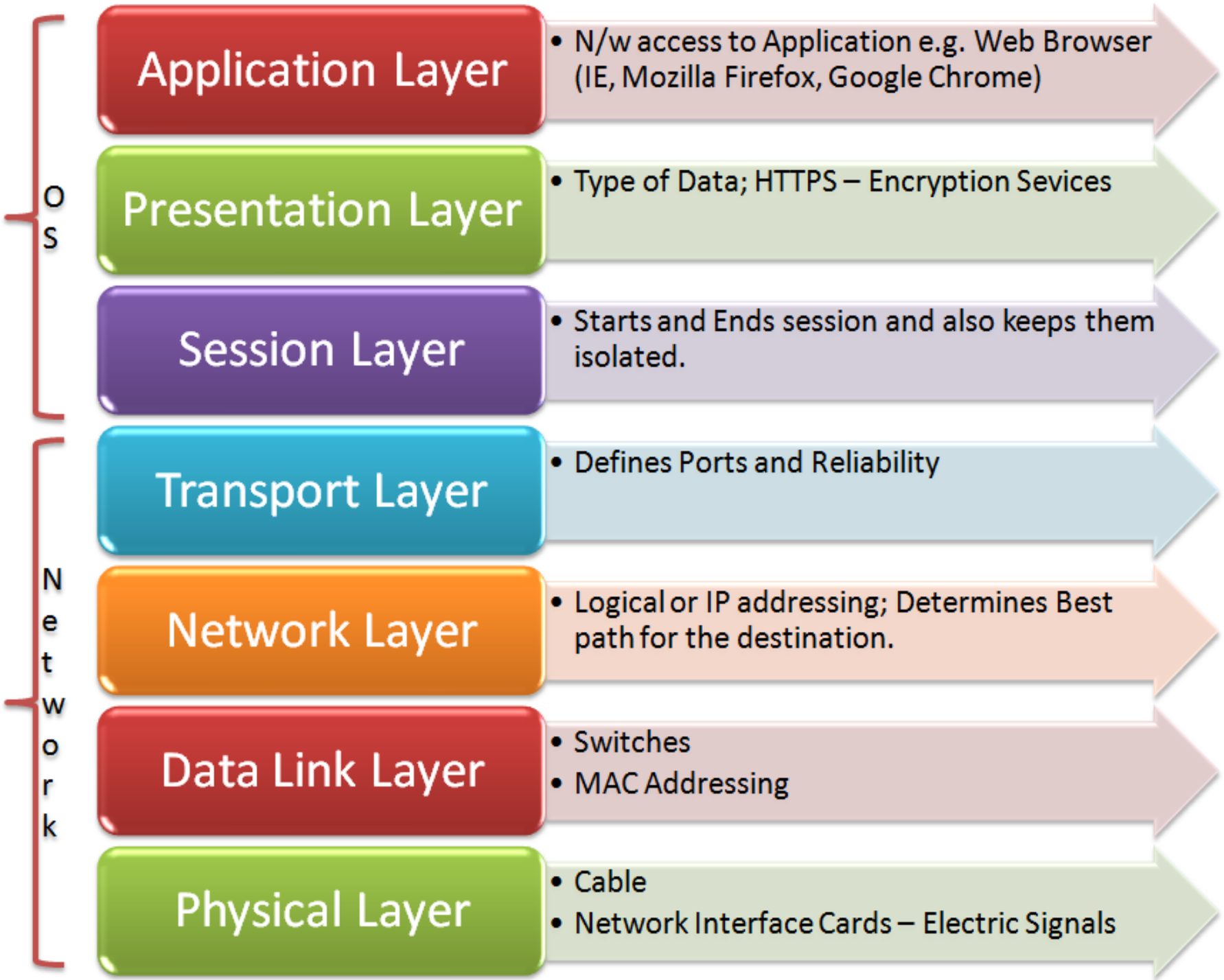
Network Infrastructure and Security

Sathish H Bowatta

OSI Model


OS
Application Layer
• N/w access to Application e.g. Web Browser (IE, Mozilla Firefox, Google Chrome)
Presentation Layer
• Type of Data; HTTPS – Encryption Sevices
Session Layer
• Starts and Ends session and also keeps them isolated.
Network
Transport Layer
• Defines Ports and Reliability
Network Layer
• Logical or IP addressing; Determines Best path for the destination.
Data Link Layer
• Switches
• MAC Addressing
Physical Layer
• Cable
• Network Interface Cards – Electric Signals

Changing Host Name

```
echo “newhostname” > /etc/hostname
```

Network Interfaces

Check all network interfaces

```
ifconfig -a
```

Detecting devices connected to PCI Bus

```
lspci
```

Controlling Network Manager

```
nmcli
```

```
nmcli device show device_name
```

Assigning an IP address

Assign temporary IP address for interface

```
ifconfig device_name down
ifconfig device_name 192.168.1.1 netmask 255.255.255.0 up
```

Assign multiple IP addresses to a interface

```
ifconfig device_name down
ifconfig device_name:1 192.168.1.1 netmask 255.255.255.0 up
ifconfig device_name:2 192.168.1.2 netmask 255.255.255.0 up
```

Assign static IP address for interface

```
vim /etc/network/interfaces

auto device_name

iface device_name inet static

    address 192.168.10.128

    network 192.168.10.0

    netmask 255.255.255.0

    broadcast 192.168.10.255

    gateway 192.168.10.2

ifconfig device_name down

ifconfig device_name up
```

Routing Table

The IP layer consults the routing table to figure out how an IP packet is sent towards the destination

```
route
```

Adding entries to the routining table

```
route add -net 192.168.1.0 netmask 255.255.255.0 ens33
```

Setting default gateway

```
route add default gw 192.168.1.1
```

Telnet

Login to remote machine using telnet

```
telnet <ip address> <port>

telnet 192.168.1.1 24
```

SSH

Set the password for root account

```
sudo passwd root
```

Login to remote machine using SSH

```
ssh root@hostname
```

Generating ssh-key

```
ssh-keygen -t rsa
```

Permit users to login as root

```
vim /etc/ssh/sshd_config
PermitRootLogin yes
```

Copy ssh ID to the server

```
ssh-copy-id root@hostname
echo “IdentityFile ~/.ssh/id_rsa" >> ~/.ssh/config
```

Restarting SSH Server

```
service sshd restart
ssh root@hostname
```

Client Server

IP Tables

Check current rules

```
iptables -L
```

Start / Stop / Restart and Get Status of iptables

```
service iptables start | stop | status | restart
```

Delete all the rules

```
iptables -F
```

Blocking access to facebook.com

```
iptables -A OUTPUT -s 0/0 -d 31.13.78.35 -j DENY
```

```
iptables -A INPUT -s 31.13.78.35 -j DROP
```

Describe following rules

```
iptables -A INPUT -i lo -p all -j ACCEPT

iptables -A INPUT -p all -s localhost -i eth0 -j DROP

iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j ACCEPT

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP
--sport 1024:65535 --dport 80 -j ACCEPT
```

Netcat

Netcat listener

```
nc -l -p 58603
```

```
nc 127.0.0.1 58603
```

Command Execution

```
mkfifo /tmp/f
```

```
cat /tmp/f | /bin/bash -i 2>&1 | nc -l -p 58603 > /tmp/f
```

```
nc 127.0.0.1 58603
```

Share files

```
nc -l -p 58603 < filename
```

```
nc 127.0.0.1 -p 58603 > filename
```

Netstat

Display generic statistic about the network activity of the local system

```
netstat
```

Shows information about all active connections

```
netstat -an
```

Displays the routing table for all IP addresses bound to the server

```
netstat -rn
```

Display statistics about active Internet connections

```
netstat -natp
```

Nmap

Nmap Pinging

ARP (-PR) / ICMP (-PE) / TCP SYN (-PS) / TCP ACK (-PA) / UDP (-PU)

ex : TCP SYN Ping

```
nmap -PS target
```

No Ping (-PN)

Nmap Scanning

TCP SYN or Stealth (-sS) / TCP Connect (-sT) / UDP (-sU)

ex : TCP Connect Scan

```
nmap -sT target
```

TCP Null (-sN) / FIN (-sF) / Xmas (-sX)

ex : Xmas Scan

```
nmap -sX target -p x,z
```

Detecting Operating System

```
nmap -O -sS target -p x,y,z
```

Service Version Detection

```
nmap -sV -sS target -p x,y,z
```

https://nmap.org/book/man-port-scanning-techniques.html

Basic Scanning Techniques

- Open - Open State that means application listening is active for TCP & UDP connection.
- Close - Close State means application is not listening but they are accessible.
- Filtered - Filtered State that means port Responding is blocked by a packet filtered because of that it's hard to identify the port is Open or not.
- Unfiltered - it's hard to determine for Nmap port is open or close but they are accessible.
- Open - Filtered - this is the mutual state where you doesn't know port is open or not. You've to scan with technique like Null, Fin, Xmas.
- Close - Filtered - Even in this state Nmap is not able to identify port is open or Close. for information you've to scan IP ID idle scan only is the way to know more.

TCP Dump

List Devices

```
tcpdump -D
```

TCP Dump

```
tcpdump -i device_name port xxxx
tcpdump -i eth0 port 139
```

Write data into a file in a binary format

```
tcpdump -i eth0 -w tdump
```

Convert data to human readable

```
tcpdump -i eth0 -r file1 > file2
```

Collect specific amount of data

```
tcpdump -i eth0 -c 100 -w file1
```