# Cyber Security
# Lession 20

# In the previous lession…

# Understanding Identity and Access Management

(Chapter 3)

# Introduction

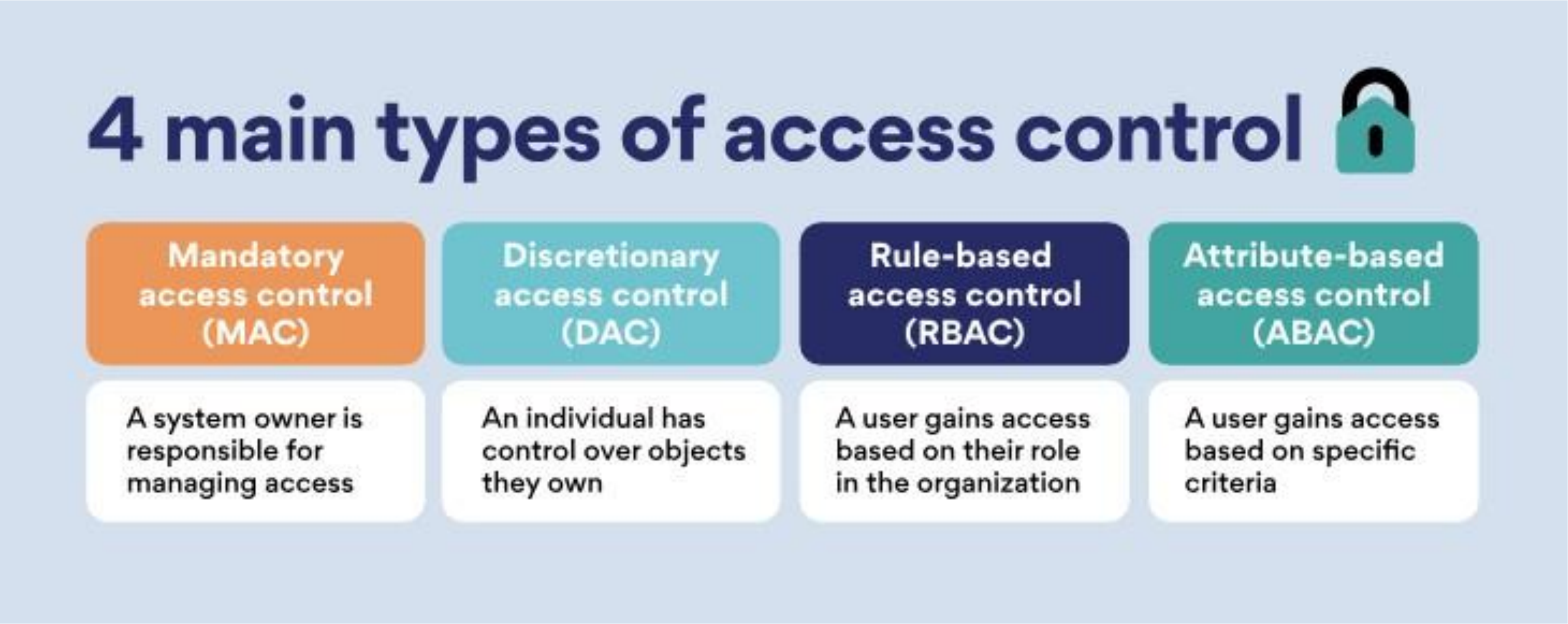
- Exploring Authentication Management DONE
- Managing Accounts DONE
- Comparing Authentication Services DONE
- Comparing Access Control Schemes DONE

# Comparing Access Control Schemes

- You grant access using one of several different access control schemes (sometimes referred to as access control models) :
  - ✓ Role-based access control
  - ✓ Rule-based access control
  - ✓ Discretionary access control (DAC)
  - ✓ Mandatory access control (MAC)
  - ✓ Attribute-based access control (ABAC)

Access Control Models
ABAC
DAC
Rule-BAC
Role-BAC
MAC

# Comparing Access Control Schemes



## 4 main types of access control

**Mandatory access control (MAC)**

A system owner is responsible for managing access

**Discretionary access control (DAC)**

An individual has control over objects they own

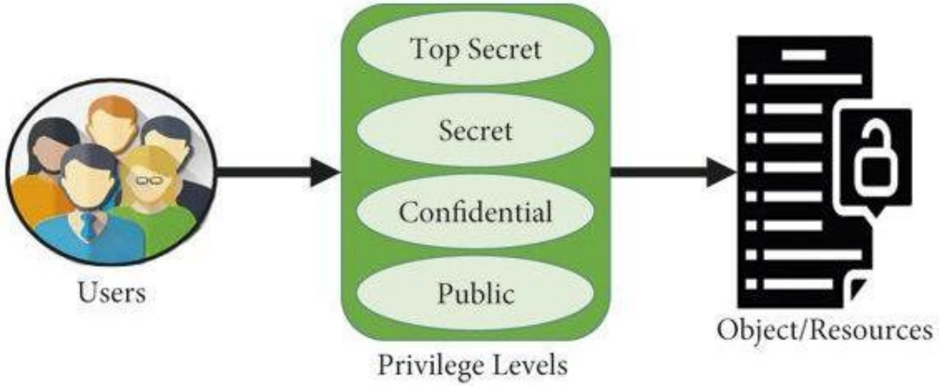
**Rule-based access control (RBAC)**

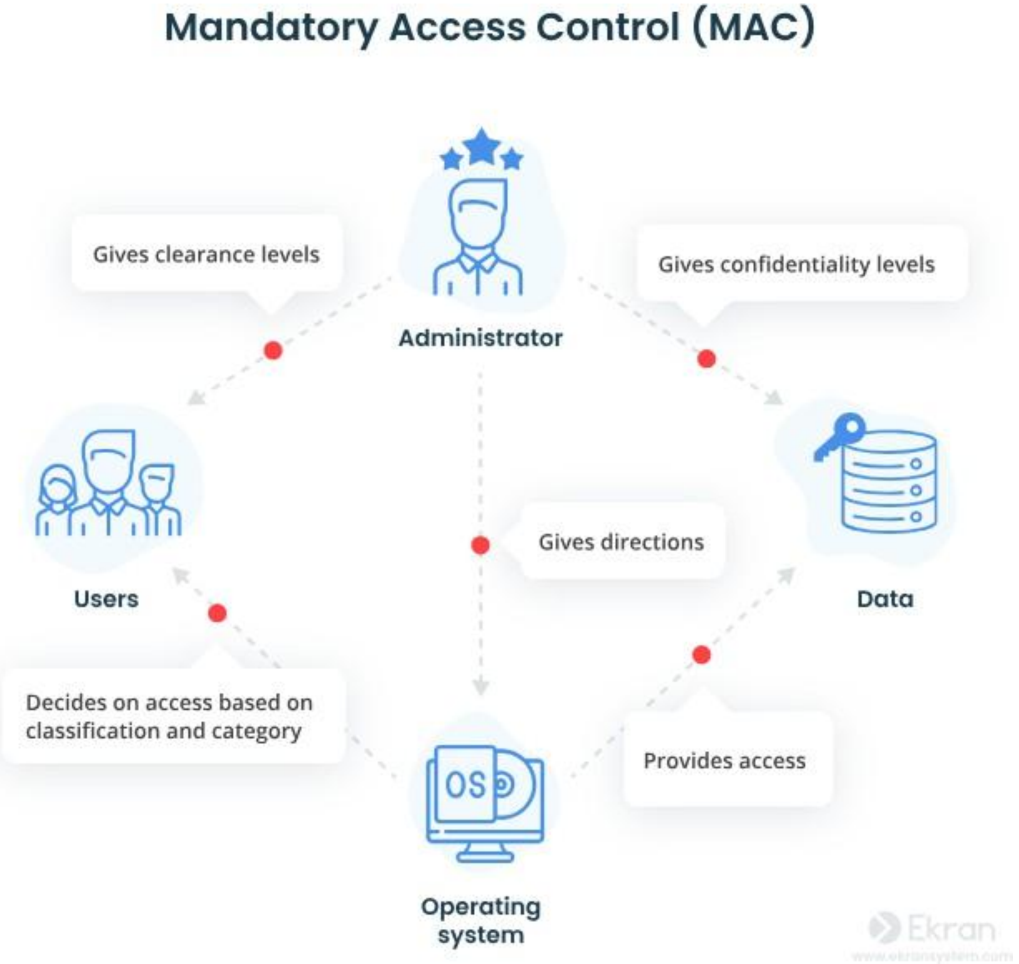
A user gains access based on their role in the organization

**Attribute-based access control (ABAC)**

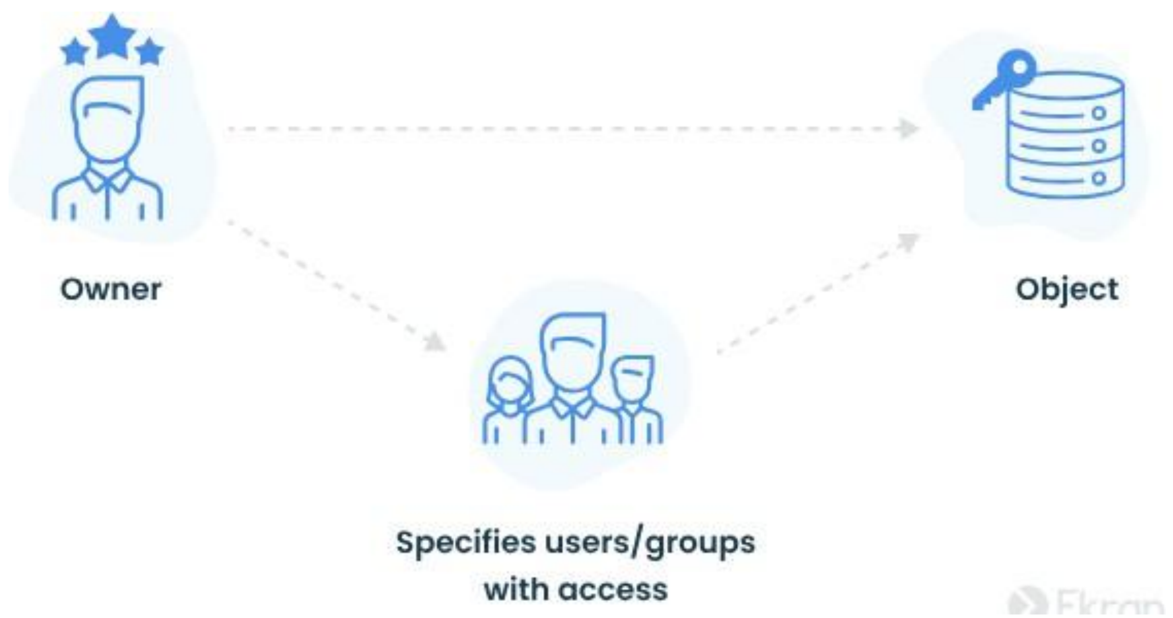
A user gains access based on specific criteria

# Mandatory Access Control (MAC)



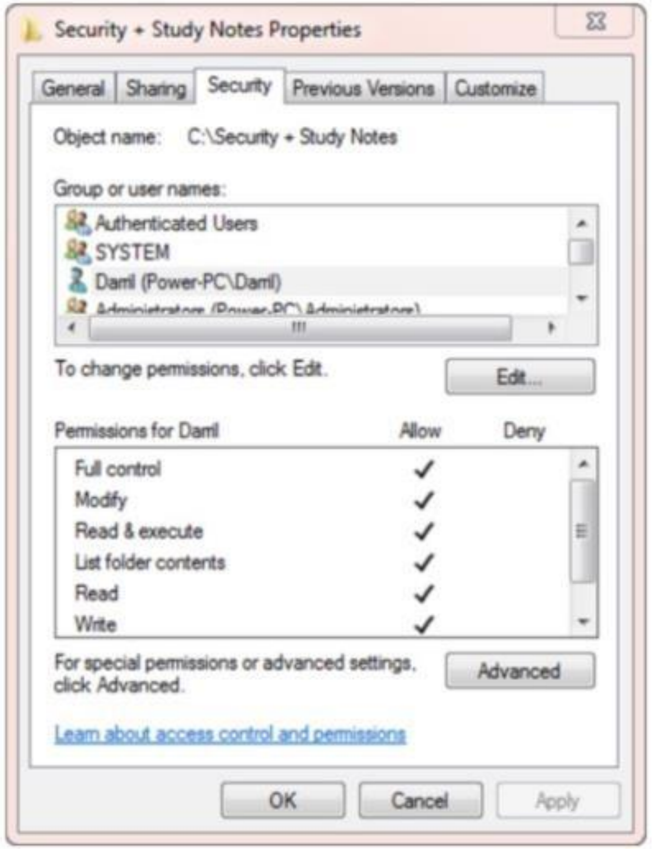

Mandatory Access Control (MAC)
Gives clearance levels
Administrator
Gives confidentiality levels
Users
Gives directions
Data
Decides on access based on classification and category
OS
Provides access
Operating system
Ekran

# Discretionary Access Control (DAC)



# Discretionary Access Control example

- Filesystem Permissions
  - ✓ Write
  - ✓ Read
  - ✓ Read & execute
  - ✓ Modify
  - ✓ Full control



Security + Study Notes Properties

Object name: C:\Security + Study Notes

Group or user names:

- Authenticated Users
- SYSTEM
- Daml (Power-PC\Daml)
- Administrators (Power-PC\Administrators)

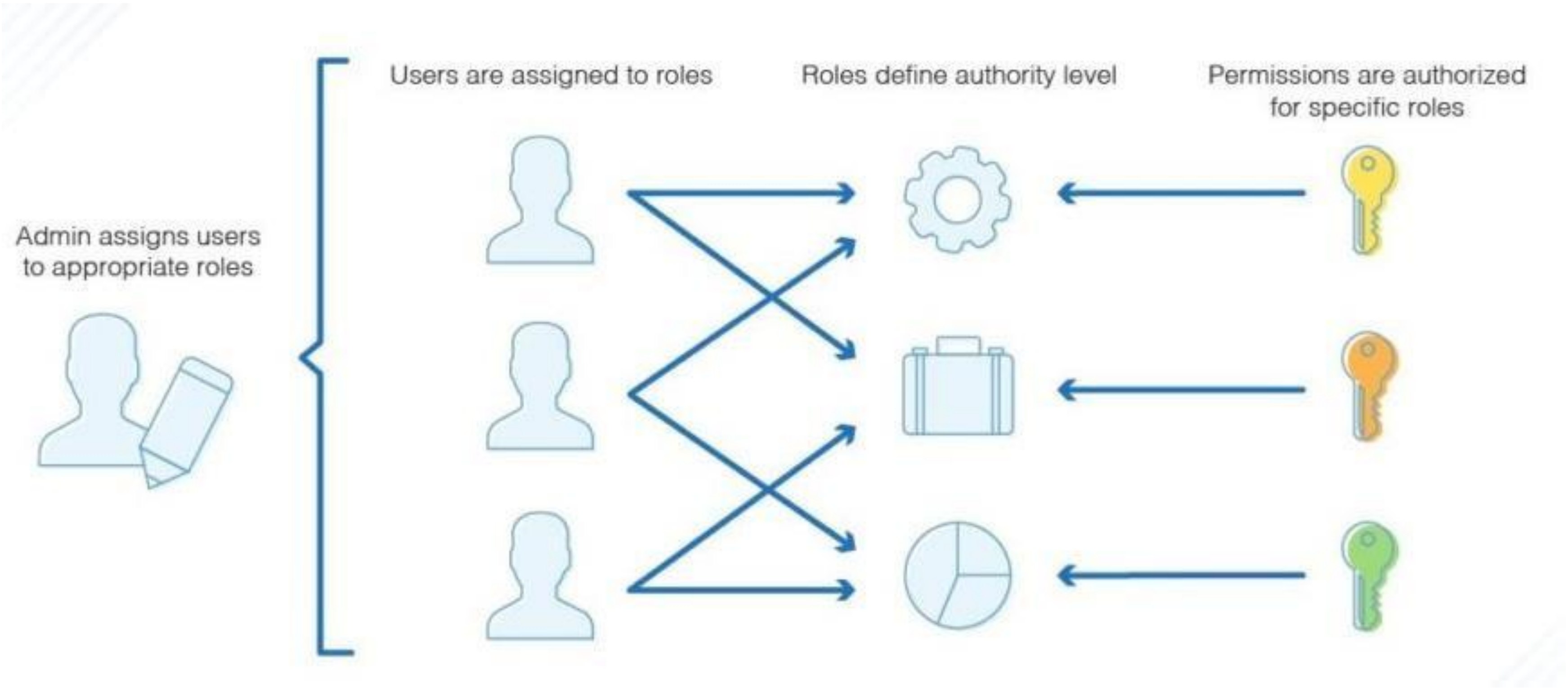
To change permissions, click Edit.

| Permissions for Daml | Allow | Deny |
|---|---|---|
| Full control | ✓ | |
| Modify | ✓ | |
| Read & execute | ✓ | |
| List folder contents | ✓ | |
| Read | ✓ | |
| Write | ✓ | |

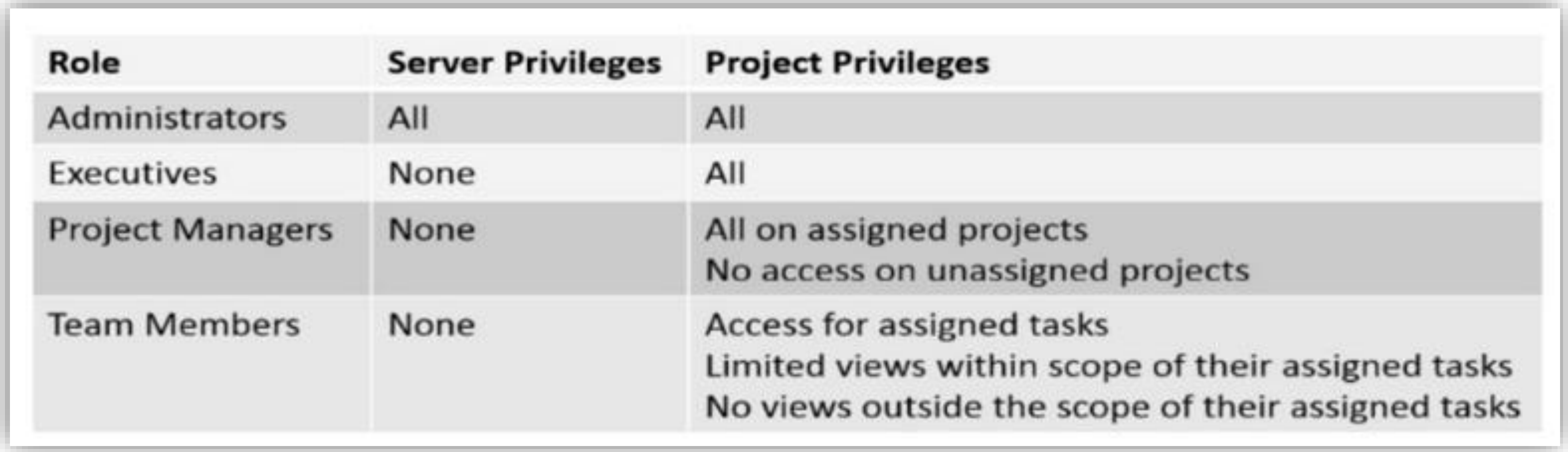
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

# Role-Based Access Control (RBAC)

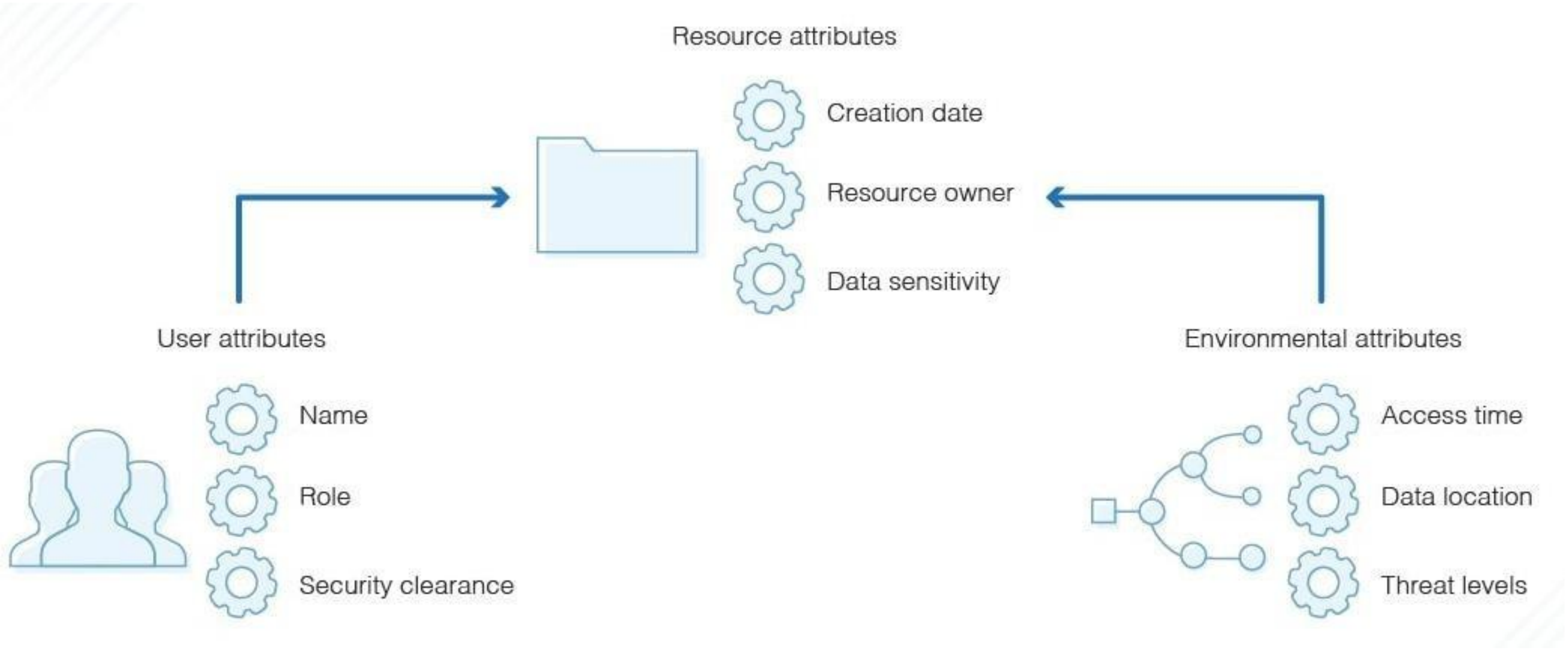

Admin assigns users
to appropriate roles
Users are assigned to roles
Roles define authority level
Permissions are authorized
for specific roles

# Role-Based Access Control Example



| Role | Server Privileges | Project Privileges |
|---|---|---|
| Administrators | All | All |
| Executives | None | All |
| Project Managers | None | All on assigned projects<br>No access on unassigned projects |
| Team Members | None | Access for assigned tasks<br>Limited views within scope of their assigned tasks<br>No views outside the scope of their assigned tasks |

# Attribute Based Access Control (ABAC)



Resource attributes

- Creation date
- Resource owner
- Data sensitivity

User attributes

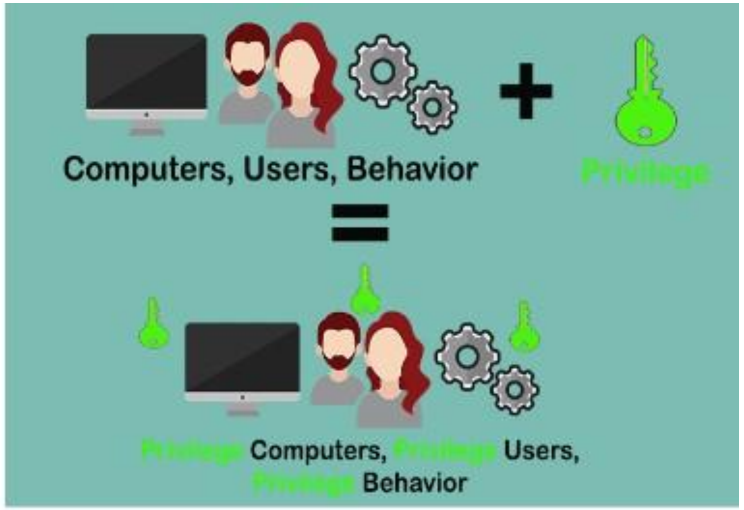
- Name
- Role
- Security clearance

Environmental attributes

- Access time
- Data location
- Threat levels

# ABAC Example

- User or group membership
- IP location
- Device


Computers, Users, Behavior
+
Privilege
=
Privilege Computers, Privilege Users,
Privilege Behavior

# Lession 20

# Exploring Network Technologies and Tools

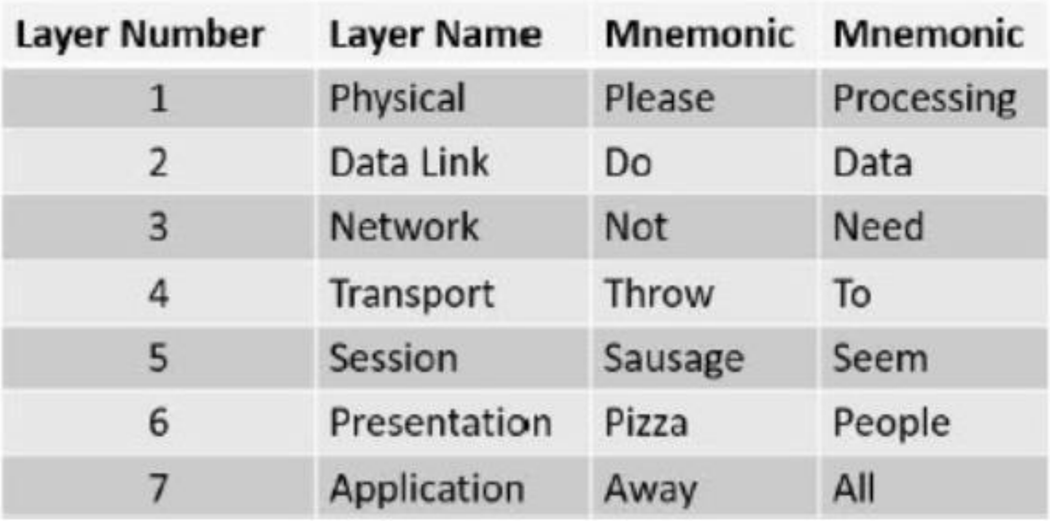
(Chapter 4)

# Introduction

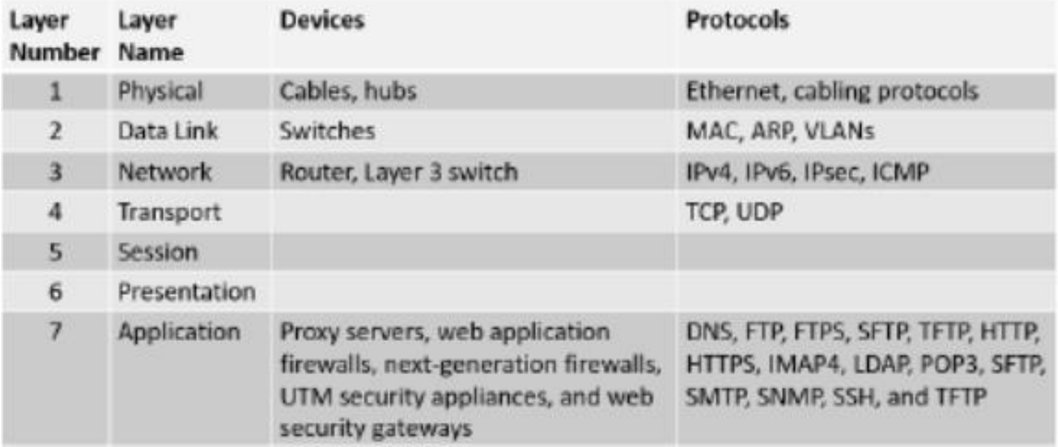
- Reviewing Basic Networking Concepts
- Basic Networking Protocols
- Understanding Basic Network Devices
- Implementing Network Designs
- Routing and Switching

# Open Systems Interconnection (OSI) model

- The OSI reference model conceptually divides different networking requirements into seven separate layers;
- It’s primarily theoretical and rarely used in day-to-day maintenance, some of the knowledge often slips away;
- The layers from Layer 1 to Layer 7 are Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- You may have heard about a “Layer 8 error” - this is another way of saying “user error” and users interact with applications;
- A user on the mythical Layer 8 interacts with applications, which are on Layer 7.



| Layer Number | Layer Name | Mnemonic | Mnemonic |
|---|---|---|---|
| 1 | Physical | Please | Processing |
| 2 | Data Link | Do | Data |
| 3 | Network | Not | Need |
| 4 | Transport | Throw | To |
| 5 | Session | Sausage | Seem |
| 6 | Presentation | Pizza | People |
| 7 | Application | Away | All |



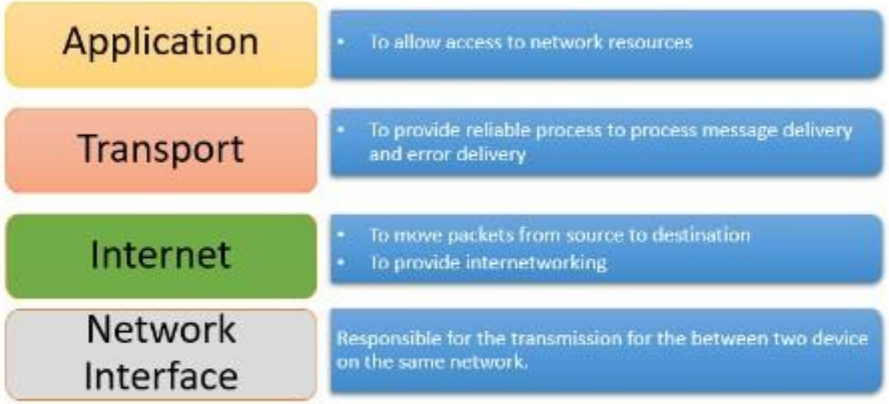
| Layer Number | Layer Name | Devices | Protocols |
|---|---|---|---|
| 1 | Physical | Cables, hubs | Ethernet, cabling protocols |
| 2 | Data Link | Switches | MAC, ARP, VLANs |
| 3 | Network | Router, Layer 3 switch | IPv4, IPv6, IPsec, ICMP |
| 4 | Transport | | TCP, UDP |
| 5 | Session | | |
| 6 | Presentation | | |
| 7 | Application | Proxy servers, web application firewalls, next-generation firewalls, UTM security appliances, and web security gateways | DNS, FTP, FTPS, SFTP, TFTP, HTTP, HTTPS, IMAP4, LDAP, POP3, SFTP, SMTP, SNMP, SSH, and TFTP |

# TCP/IP model

- TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP Stack is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork;
- TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them;
- It helps you to create a virtual network when multiple computer networks are connected together
- The purpose of TCP/IP model is to allow communication over large distances;
- Support for a flexible TCP/IP architecture;
- Adding more system to a network is easy;
- In TCP IP protocols suite, the network remains intact until the source, and destination machines were functioning properly;
- TCP is a connection-oriented protocol;
- TCP offers reliability and ensures that data which arrives out of sequence should put back into order;
- TCP allows you to implement flow control, so sender never overpowers a receiver with data;
- The functionality of the TCP IP model is divided into four layers, and each includes specific protocols.

- TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform and all these four TCP IP layers work collaboratively to transmit the data from one layer to another :

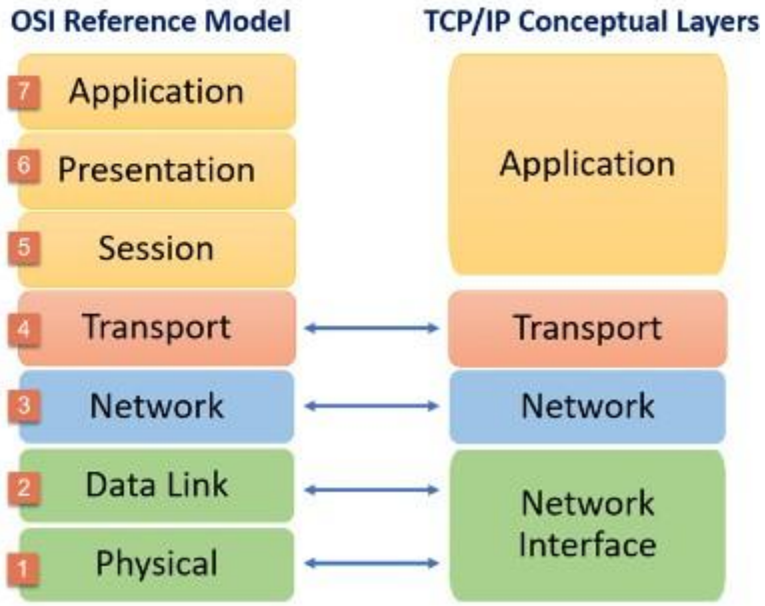
✓ Application Layer;<br>
✓ Transport Layer;<br>
✓ Internet Layer;<br>
✓ Network Interface.



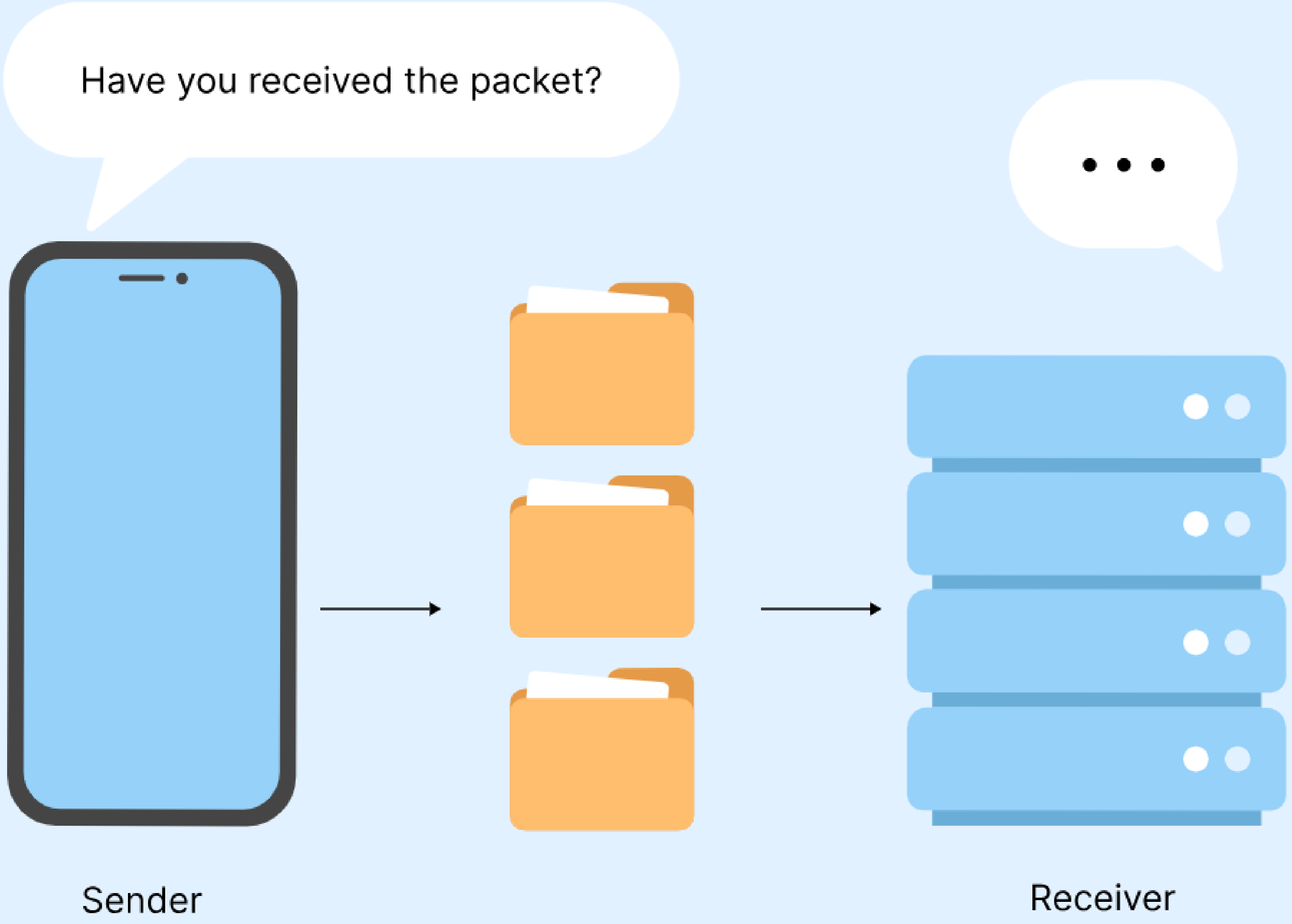
| | |
|---|---|
| Application | • To allow access to network resources |
| Transport | • To provide reliable process to process message delivery and error delivery |
| Internet | • To move packets from source to destination<br>• To provide internetworking |
| Network Interface | Responsible for the transmission for the between two device on the same network. |

# OSI vs TCP/IP

- OSI has 7 layers, whereas TCP/IP has 4 layers;
- The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. On the other hand, TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can be transmitted between them;
- OSI header is 5 bytes, whereas TCP/IP header size is 20 bytes;
- OSI refers to Open Systems Interconnection, whereas TCP/IP refers to Transmission Control Protocol;
- OSI follows a vertical approach, whereas TCP/IP follows a horizontal approach;
- OSI model, the transport layer, is only connection-oriented, whereas the TCP/IP model is both connection-oriented and connectionless;
- OSI model is developed by ISO (International Standard Organization), whereas TCP Model is Developed by ARPANET (Advanced Research Project Agency Network);
- OSI model helps you to standardize router, switch, motherboard, and other hardware, whereas TCP/IP helps you to establish a connection between different types of computers.



# How UDP works

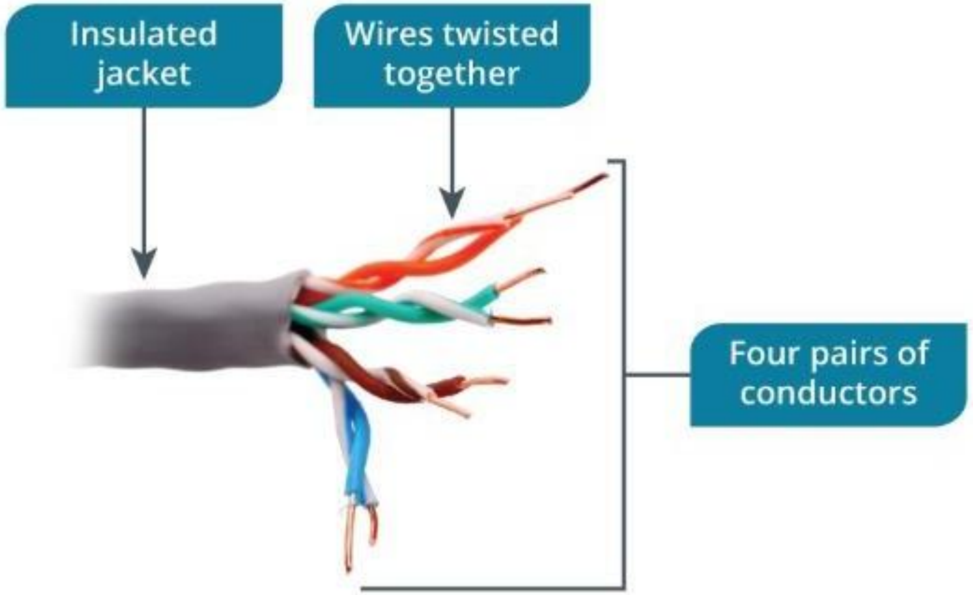


# Layer 1: Physical (OSI)

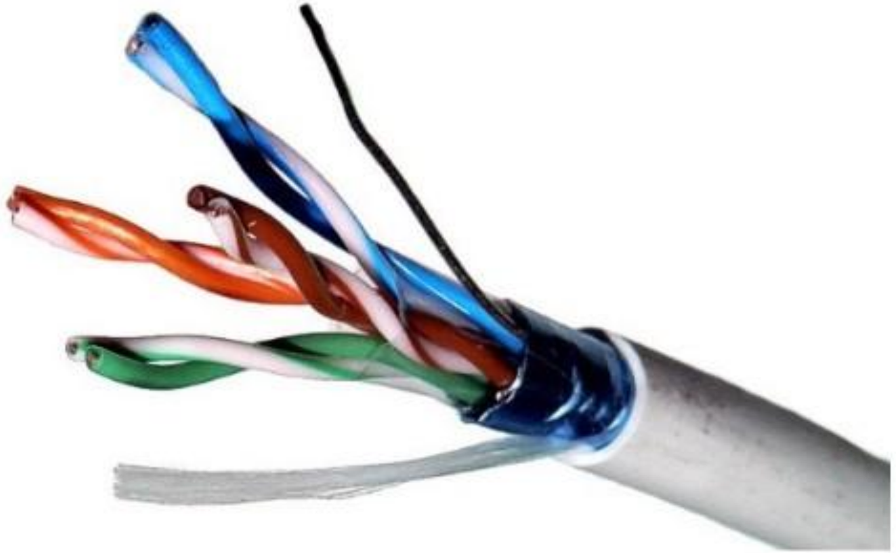
- The Physical layer is associated with the physical hardware;
- It includes specifications for cable types, such as 1000BaseT, connectors, and hubs;
- Computing devices such as computers, servers, routers, and switches transmit data onto the transmission medium in a bitstream;
- This bitstream is formatted according to specifications at higher-level OSI layers.

# Unshielded Twisted Pair

- Copper wire cabling carrying electrical signals;
- Four balanced wire pairs;
- Twisted at different rates and balanced to reduce interference;
- Signal attenuation limits maximum distance to 100 m.



# Shielded Twisted Pair

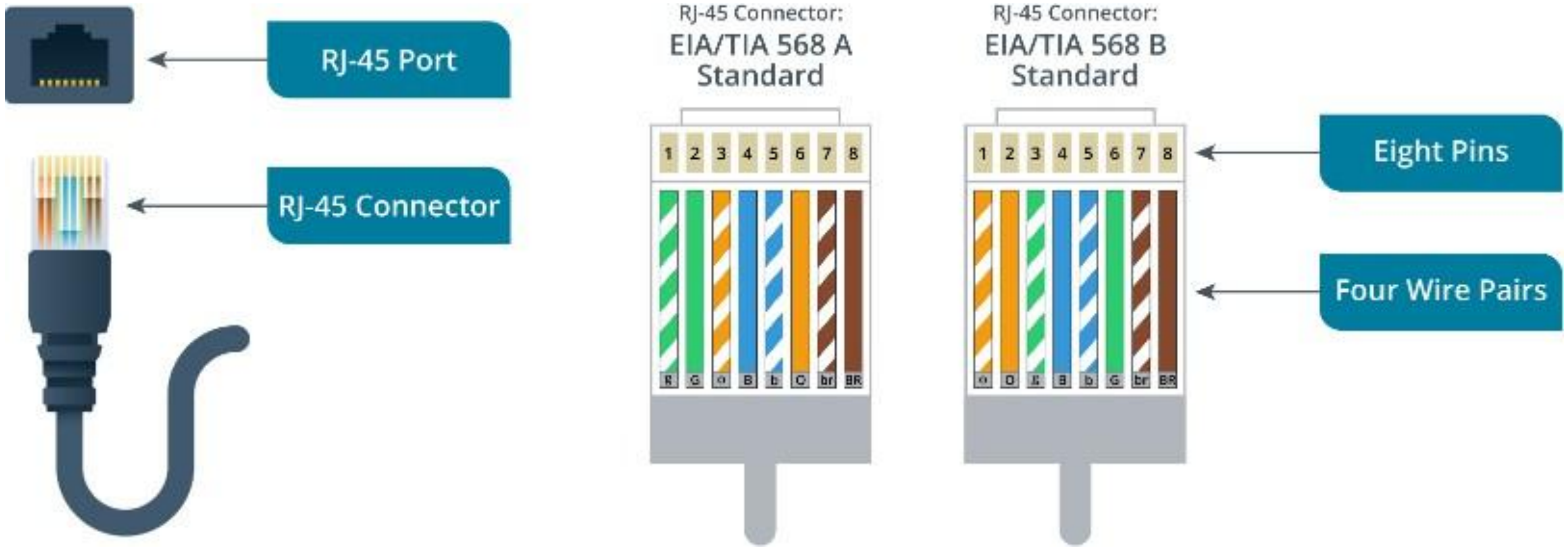


- Screening or shielding as extra protection against interference
  - ✓ Used for 10G Ethernet+ in datacenters for higher reliability
  - ✓ Used when cabling is near external interference sources (fluorescent lighting, power lines, motors, and generators)
- Screened cable has one thin outer foil shield around all pairs (ScTP, F/UTP, FTP);
- Fully shielded cabling has a braided outer screen and foil-shielded pairs (S/FTP and F/FTP);
- Shield elements in cable, connector, and patch panels must be bonded.

# Cat Standards

| Cat | Max. Transfer Rate | Max. Distance | Network Application |
|---|---|---|---|
| 5 | 100 Mbps | 100 m (328 ft) | 100BASE-TX (Fast Ethernet) |
| 5e | 1 Gbps | 100 m (328 ft) | 1000BASE-T (Gigabit Ethernet) |
| 6 | 1 Gbps | 100 m (328 ft) | 1000BASE-T (Gigabit Ethernet) |
|  | 10 Gbps | 55 m (180 ft) | 10GBASE-T (10 Gigabit Ethernet) |
| 6A | 10 Gbps | 100 m (328 ft) | 10GBASE-T (10 Gigabit Ethernet) |

# Copper Cabling Connectors

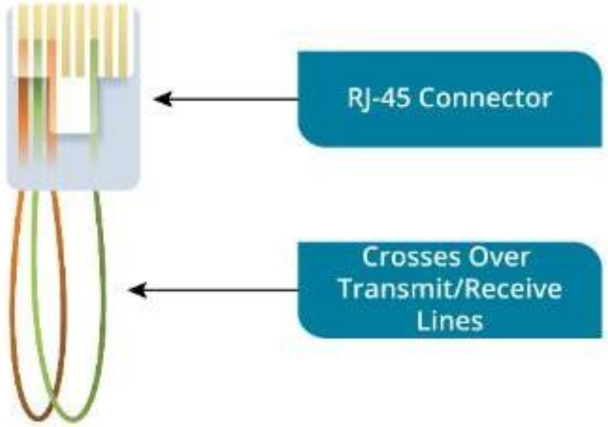


# Copper Cabling Installation Tools

- Patch cords are crimped to RJ-45 connectors;
- Structured cable is terminated to insulation displacement connect (IDC) blocks in wall ports and patch panels;
- Punchdown tool
  - ✓ Terminate to IDCs;
- Cable stripper
  - ✓ Remove insulation;
- Crimper
  - ✓ Add RJ-45 connector.

# Copper Cabling Test Tools

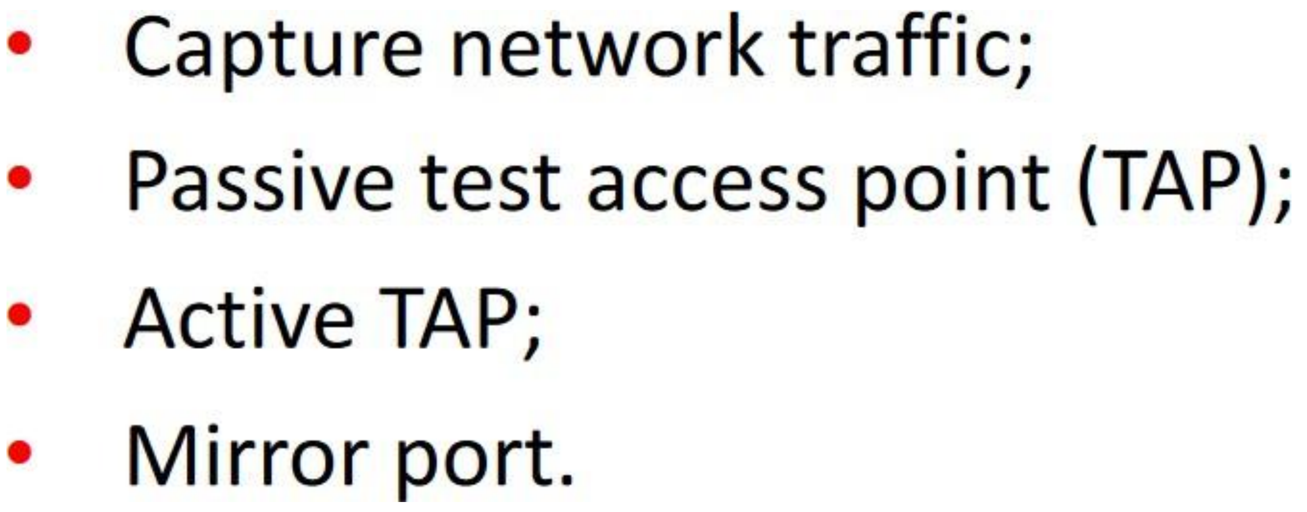
- Validate and test cable installation;
- Cable tester
  - ✓ Verify termination;
- Toner probe
  - ✓ Trace a cable;
- Loopback plug
  - ✓ Test NIC or switch port.



RJ-45 Connector

Crosses Over Transmit/Receive Lines

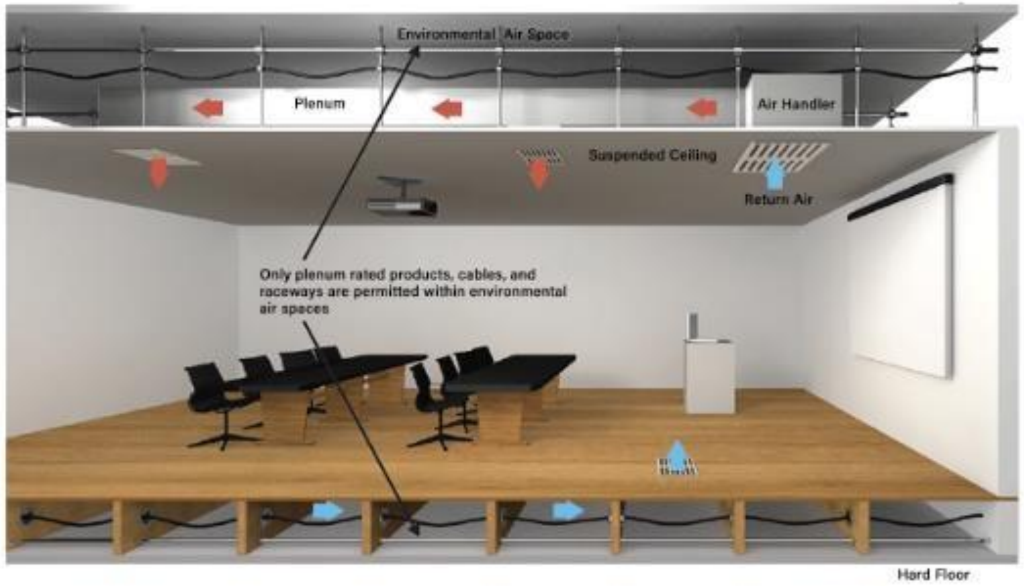
# Network Taps



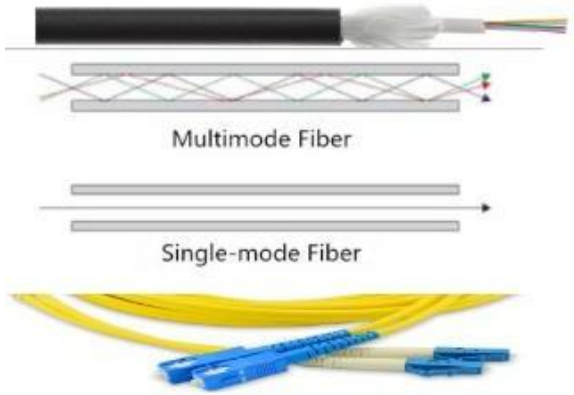
- Capture network traffic;
- Passive test access point (TAP);
- Active TAP;
- Mirror port.

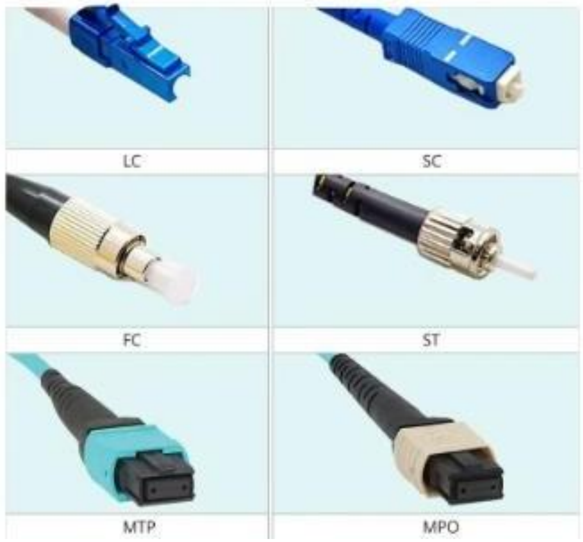
# Copper Cabling Installation Considerations

- Installation to plenum spaces
  - ✓ Building/fire safety regulations;
  - ✓ Plenum rated cable;
- Installation as outside plant (OSP)
  - ✓ Aerial, conduit, and direct burial;
  - ✓ Protection against weathering.


Environmental Air Space
Plenum
Air Handler
Suspended Ceiling
Return Air
Only plenum rated products, cables, and raceways are permitted within environmental air spaces
Hard Floor

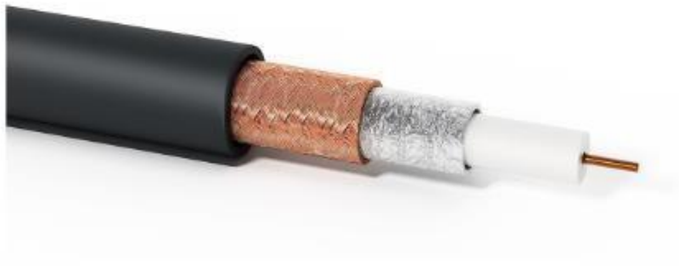
# Optical Cabling





- Fiber optic cable types
  - ✓ Single-mode fiber (SMF);
  - ✓ Multi-mode fiber (MMF);
- Connector types
  - ✓ Lucent connector (LC);
  - ✓ Subscriber connector (SC);
  - ✓ Fiber optic connector (FC)
  - ✓ Straight tip (ST);
  - ✓ Multi-fiber terminating push-in (MTP);
  - ✓ Multi-fiber push-on (MPO).

# Coaxial Cabling



Coaxial F-Connector

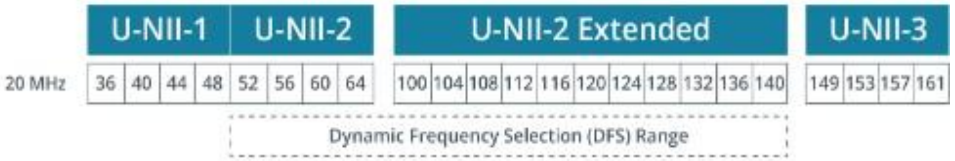
- Construction of 5 parts;
- Uses F-type connector.

# Access Points

- IEEE 802.11 / Wi-Fi;
- Infrastructure mode WLAN
  - ✓ Access point interconnects wireless clients (stations);
  - ✓ Infrastructure Basic Service Set (BSS);
  - ✓ Basic Service Set Identifier (BSSID)
    - ➢ MAC address of AP radio;
- Can bridge with wired network via a switch;

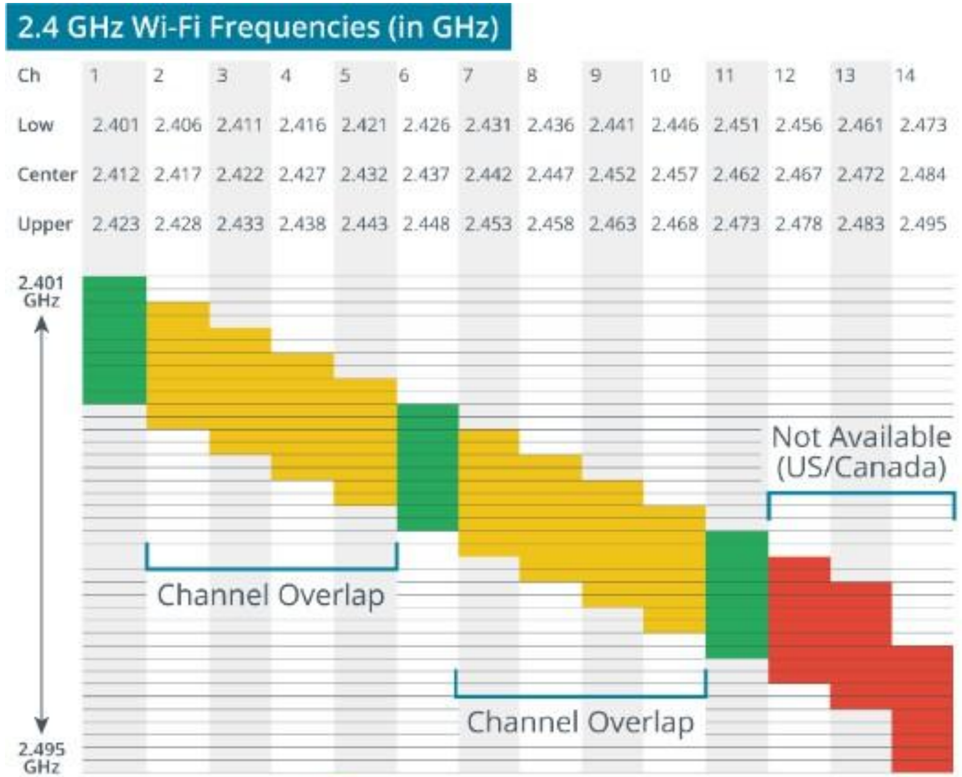
# 802.11a and the 5 GHz Frequency Band

- 2.4 GHz
  - ✓ Better propagation, but fewer channels and greater interference risk;
- 5 GHz
  - ✓ Shorter range, but less congested;
- IEEE 802.11a (54 Mbps)
  - ✓ 23 x non-overlapping 20 MHz channels;
  - ✓ Dynamic Frequency Selection (DFS) and regulatory impacts.



| | U-NII-1 | U-NII-2 | U-NII-2 Extended | U-NII-3 |
|---|---|---|---|---|
| 20 MHz | 36 40 44 48 | 52 56 60 64 | 100 104 108 112 116 120 124 128 132 136 140 | 149 153 157 161 |

# 802.11b/g and the 2.4 GHz Frequency Band



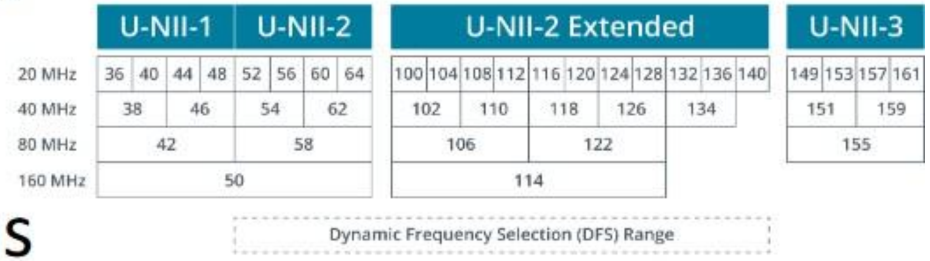
2.4 GHz Wi-Fi Frequencies (in GHz)

| Ch | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Low | 2.401 | 2.406 | 2.411 | 2.416 | 2.421 | 2.426 | 2.431 | 2.436 | 2.441 | 2.446 | 2.451 | 2.456 | 2.461 | 2.473 |
| Center | 2.412 | 2.417 | 2.422 | 2.427 | 2.432 | 2.437 | 2.442 | 2.447 | 2.452 | 2.457 | 2.462 | 2.467 | 2.472 | 2.484 |
| Upper | 2.423 | 2.428 | 2.433 | 2.438 | 2.443 | 2.448 | 2.453 | 2.458 | 2.463 | 2.468 | 2.473 | 2.478 | 2.483 | 2.495 |

- IEEE 802.11b (11 Mbps)
  - ✓ 14 x 5 MHz channels;
  - ✓ Wi-Fi still needs 20 MHz channel bandwidth;
  - ✓ Channels require careful configuration to avoid overlap;
- IEEE 802.11g (54 Mbps)
  - ✓ 802.11b compatibility mode.

# 802.11n

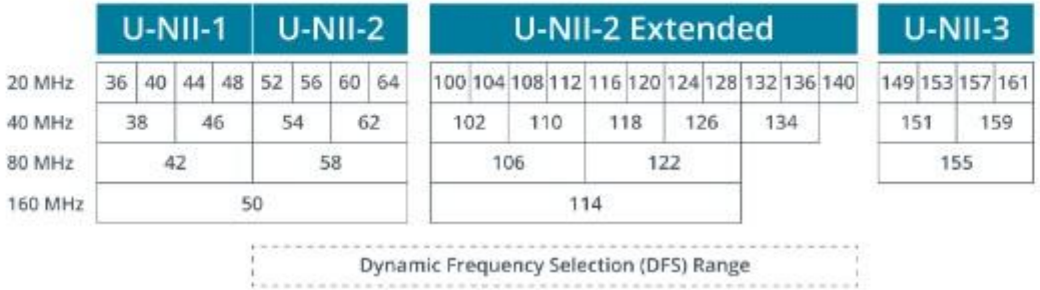
- Dual band radios
  - ✓ 5 GHz or 2.4 GHz;
- 40 MHz channel bonding;
- Multiple input multiple output (MIMO)
  - ✓ Use of multiple antennas to improve reliability and bandwidth;
  - ✓ 72 Mbps per stream;
- Wi-Fi 4.



| | U-NII-1 | | | | U-NII-2 | | | | U-NII-2 Extended | | | | | | | | | | | U-NII-3 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 MHz | 36 | 40 | 44 | 48 | 52 | 56 | 60 | 64 | 100 | 104 | 108 | 112 | 116 | 120 | 124 | 128 | 132 | 136 | 140 | 149 | 153 | 157 | 161 |
| 40 MHz | 38 | | 46 | | 54 | | 62 | | 102 | | 110 | | 118 | | 126 | | 134 | | | 151 | | 159 | |
| 80 MHz | 42 | | | | 58 | | | | 106 | | | | 122 | | | | | | | 155 | | | |
| 160 MHz | 50 | | | | | | | | 114 | | | | | | | | | | | | | | |

Dynamic Frequency Selection (DFS) Range

# Wi-Fi 5 and Wi-Fi 6

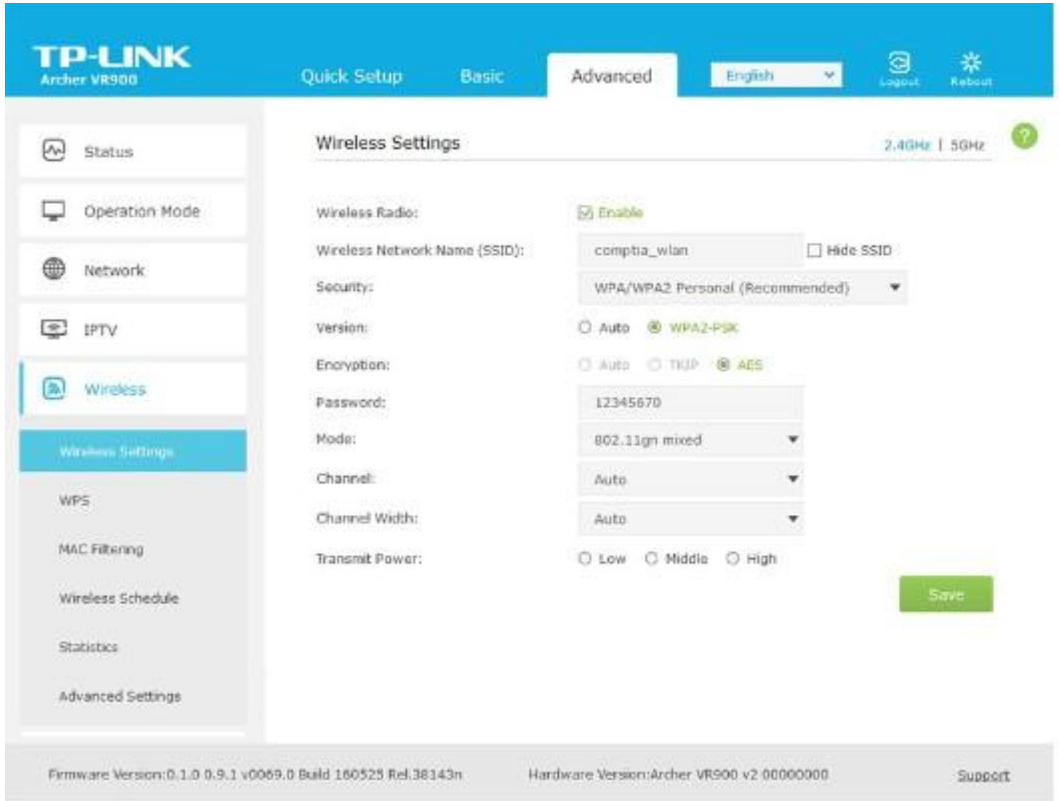


| | U-NII-1 | | | | U-NII-2 | | | | U-NII-2 Extended | | | | | | | | | | | U-NII-3 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 MHz | 36 | 40 | 44 | 48 | 52 | 56 | 60 | 64 | 100 | 104 | 108 | 112 | 116 | 120 | 124 | 128 | 132 | 136 | 140 | 149 | 153 | 157 | 161 |
| 40 MHz | 38 | | 46 | | 54 | | 62 | | 102 | | 110 | | 118 | | 126 | | 134 | | | 151 | | 159 | |
| 80 MHz | 42 | | | | 58 | | | | 106 | | | | 122 | | | | | | | 155 | | | |
| 160 MHz | 50 | | | | | | | | 114 | | | | | | | | | | | | | | |

Dynamic Frequency Selection (DFS) Range

- Wi-Fi 5 (802.11ac)
  - ✓ 5 GHz only;
  - ✓ Tri-band radios;
  - ✓ 80 and 160 MHz channel bonding;
- Multiuser MIMO
  - ✓ Connect stations simultaneously;
- Wi-Fi 6 (802.11ax)
  - ✓ 2.4 GHz or 5 GHz (plus new 6 GHz band);
  - ✓ Downlink and uplink MU-MIMO;
  - ✓ Orthogonal frequency division multiple access (OFDMA).

# Wireless LAN Installation Considerations



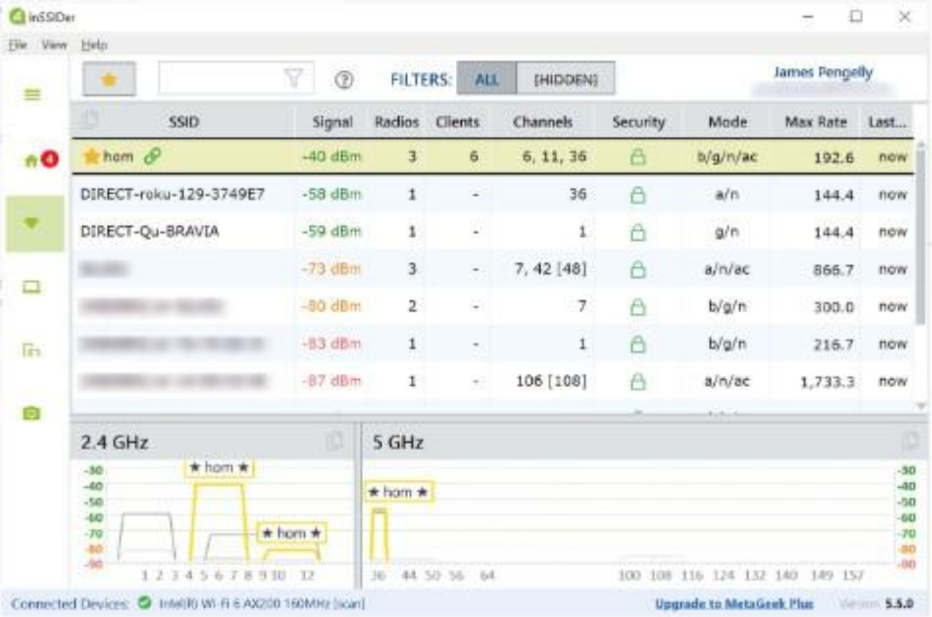
Wireless Settings

| | |
|---|---|
| Wireless Radio: | ☑ Enable |
| Wireless Network Name (SSID): | comptia_wlan ☐ Hide SSID |
| Security: | WPA/WPA2 Personal (Recommended) |
| Version: | ○ Auto ● WPA2-PSK |
| Encryption: | ○ Auto ○ TKIP ● AES |
| Password: | 12345670 |
| Mode: | 802.11gn mixed |
| Channel: | Auto |
| Channel Width: | Auto |
| Transmit Power: | ○ Low ○ Middle ○ High |

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n Hardware Version:Archer VR900 v2 00000000

- Network name or Service Set Identifier (SSID);
- Frequency band use
  - ✓ Same SSID or different SSID per band
  - ✓ Operation mode (legacy standards support)
- Channel usage
  - ✓ Non-overlapping;
  - ✓ Channel width/bonding.

# Wi-Fi Analyzers



| SSID | Signal | Radios | Clients | Channels | Security | Mode | Max Rate | Last... |
|---|---|---|---|---|---|---|---|---|
| hom | -40 dBm | 3 | 6 | 6, 11, 36 | 🔒 | b/g/n/ac | 192.6 | now |
| DIRECT-roku-129-3749E7 | -58 dBm | 1 | - | 36 | 🔒 | a/n | 144.4 | now |
| DIRECT-Qu-BRAVIA | -59 dBm | 1 | - | 1 | 🔒 | g/n | 144.4 | now |
| [redacted] | -73 dBm | 3 | - | 7, 42 [48] | 🔒 | a/n/ac | 866.7 | now |
| [redacted] | -80 dBm | 2 | - | 7 | 🔒 | b/g/n | 300.0 | now |
| [redacted] | -83 dBm | 1 | - | 1 | 🔒 | b/g/n | 216.7 | now |
| [redacted] | -87 dBm | 1 | - | 106 [108] | 🔒 | a/n/ac | 1,733.3 | now |

- Software installed to mobile device
  - ✓ Reports configuration of nearby wireless networks;
  - ✓ Signal strength on each channel;
- Signal strength
  - ✓ Decibels-milliwatt (dBm);
  - ✓ Negative values with closer to zero better performance;
  - ✓ Logarithmic scale
    - ➢ 3 dBm difference represents halving or doubling;
- Signal-to-noise ratio (SNR).

# Long Range Fixed Wireless

- Wireless bridges configured using microwave antennas
  - ✓ Line of sight;
  - ✓ High gain;
- Licensed spectrum use
  - ✓ Legal right to remove interference sources;
- Unlicensed spectrum
  - ✓ Shared use of frequency band;
  - ✓ Regulatory requirements on power;
  - ✓ Transmit power, gain, and Effective Isotropic Radiated Power (EIRP).

# Bluetooth, RFID, and NFC

- Bluetooth
  - ✓ Connectivity for wireless peripherals;
- Radio Frequency ID (RFI)
  - ✓ Wireless asset tags;
  - ✓ Inventory control;
- Nearfield Communications (NFC)
  - ✓ Contactless payments.

# Cellular Radio Internet Connections

- 3G
  - ✓ Global System for Mobile Communication (GSM) providers
    - ➢ Subscriber Identity Module (SIM) card;
  - ✓ Code Division Multiple Access (CDMA) providers;
- 4G
  - ✓ Long Term Evolution (LTE) converged standard using SIM cards ;
- 5G
  - ✓ Connection through array of massive MIMO antennas;
  - ✓ Roaming and fixed access.

# Layer 2: Data Link (OSI)

- The Data Link layer is responsible for ensuring that data is transmitted to specific devices on the network;
- It formats the data into frames and adds a header that includes media access control (MAC) addresses for the source and destination devices and the Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses;
- The Data Link layer is responsible for ensuring that data is transmitted to specific devices on the network;
- It formats the data into frames and adds a header that includes media access control (MAC) addresses for the source and destination devices;
- It adds frame check sequence data to the frame to detect errors, but it doesn't support error correction;
- The Data Link layer simply discards frames with detected errors;
- Flow control functions are also available on this layer;
- Traditional switches (Layer 2 switches) operate on this layer;
- Computer network interface cards have a MAC assigned, and switches map the computer MAC addresses to physical ports on the switch;
- Systems use the Address Resolution Protocol (ARP) to resolve IPv4 addresses to MAC addresses;
- VLANs are defined on this layer;
- Layer 2 attacks attempt to exploit vulnerabilities in MAC addressing and ARP;
- Main Layer 2 attacks are Address Resolution Protocol (ARP) poisoning, media access control (MAC) flooding, and MAC cloning.

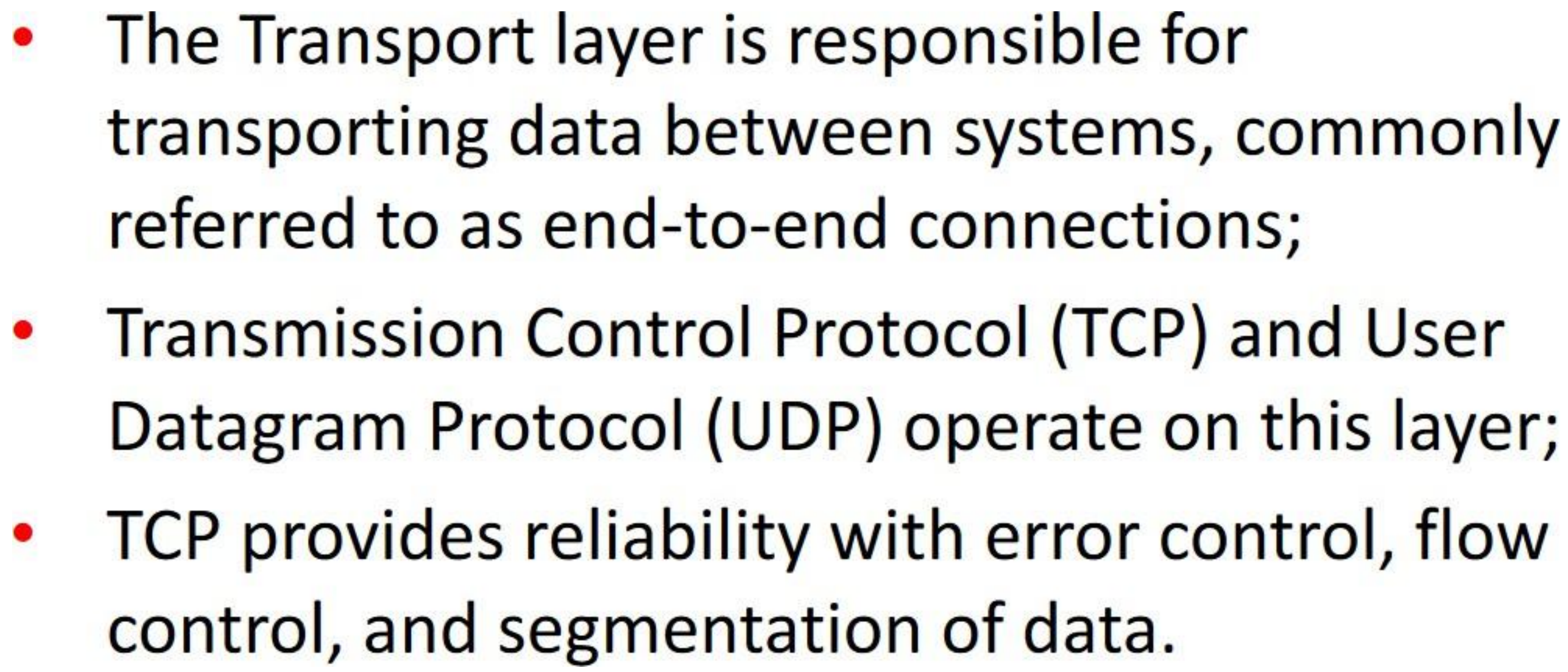
# Layer 3: Network (OSI)

- The Network layer uses logical addressing in the form of IP addresses at this layer;
- This includes both IPv4 addresses and IPv6 addresses;
- Packets identify where the traffic originated (the source IP address) and where it is going (the destination IP address);
- Other protocols that operate on this layer are IPsec and ICMP;
- Routers and Layer 3 switches operate on this layer.

# Layer 2: Internet Layer (TCP/IP)

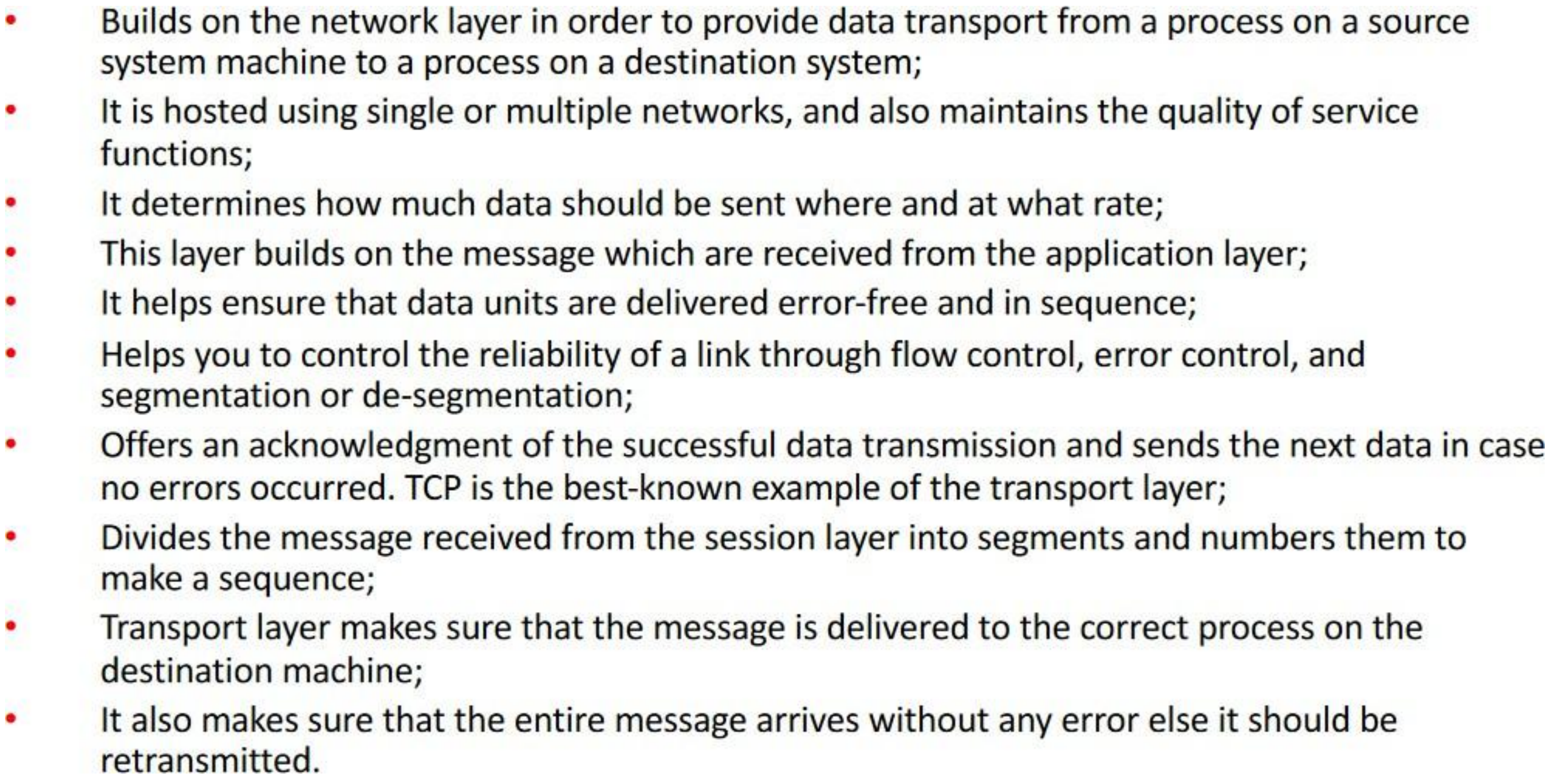
- It is also known as a network layer (TCP/IP);
- The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take;
- Offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks;
- Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol;
- Layer-management protocols that belong to the network layer are:
  - ✓ Routing protocols;
  - ✓ Multicast group management;
  - ✓ Network-layer address assignment.

# Layer 4: Transport (OSI)



- The Transport layer is responsible for transporting data between systems, commonly referred to as end-to-end connections;
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) operate on this layer;
- TCP provides reliability with error control, flow control, and segmentation of data.

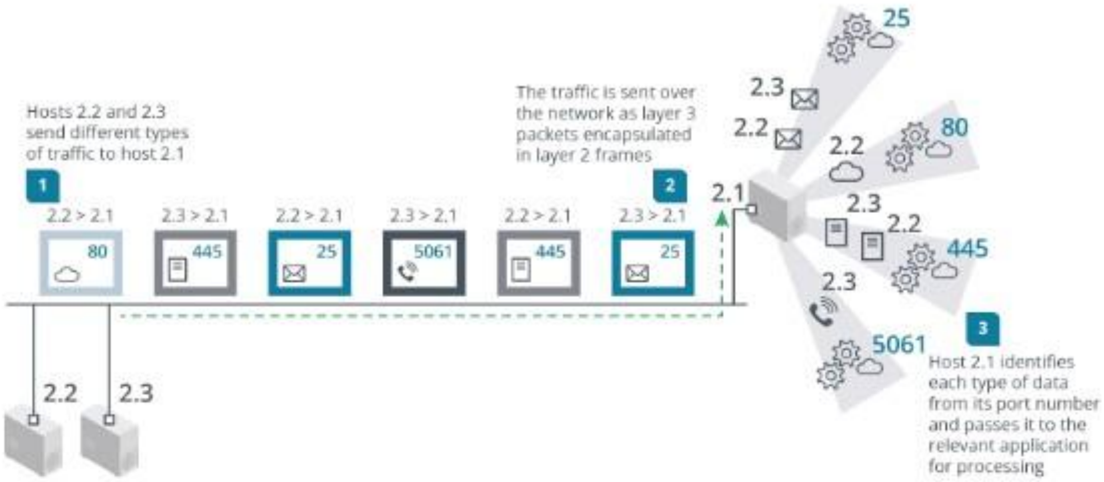
# Layer 3: Transport Layer (TCP/IP)



- Builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system;
- It is hosted using single or multiple networks, and also maintains the quality of service functions;
- It determines how much data should be sent where and at what rate;
- This layer builds on the message which are received from the application layer;
- It helps ensure that data units are delivered error-free and in sequence;
- Helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation;
- Offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer;
- Divides the message received from the session layer into segments and numbers them to make a sequence;
- Transport layer makes sure that the message is delivered to the correct process on the destination machine;
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

# Protocols and Ports

- Transport layer
  - ✓ Identify each application protocol;
  - ✓ Track sessions;
- Protocol ports
  - ✓ Server port;
  - ✓ Client port.

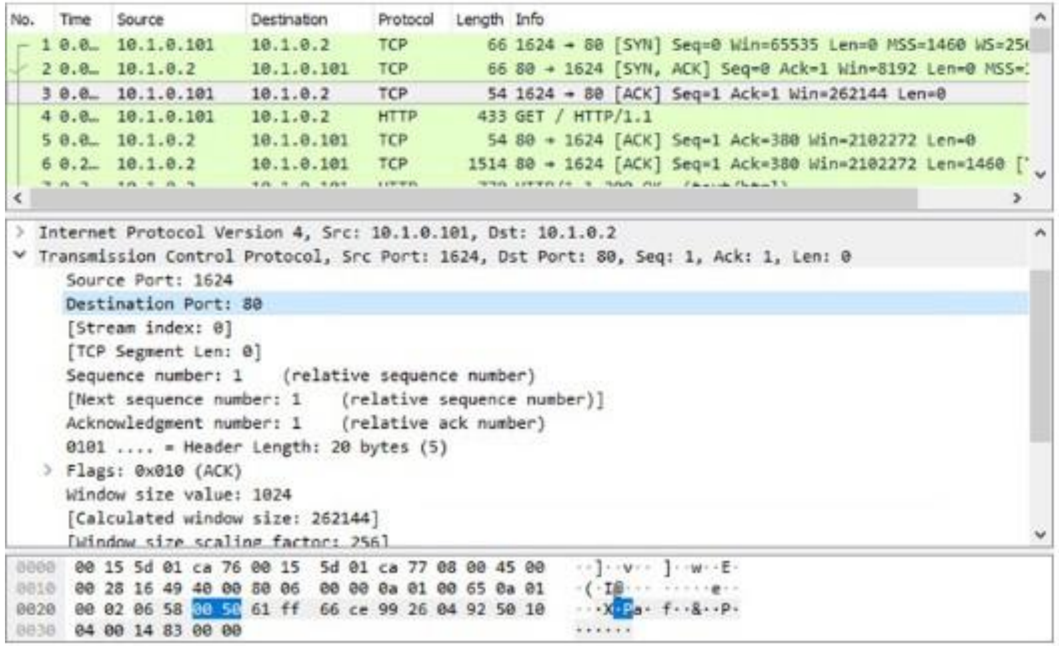


1 Hosts 2.2 and 2.3 send different types of traffic to host 2.1

2 The traffic is sent over the network as layer 3 packets encapsulated in layer 2 frames

3 Host 2.1 identifies each type of data from its port number and passes it to the relevant application for processing

# Transmission Control Protocol



```
No.  Time  Source       Destination  Protocol  Length Info
 1 0.0…  10.1.0.101   10.1.0.2     TCP           66 1624 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=25
 2 0.0…  10.1.0.2     10.1.0.101   TCP           66 80 → 1624 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=
 3 0.0…  10.1.0.101   10.1.0.2     TCP           54 1624 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 4 0.0…  10.1.0.101   10.1.0.2     HTTP         433 GET / HTTP/1.1
 5 0.0…  10.1.0.2     10.1.0.101   TCP           54 80 → 1624 [ACK] Seq=1 Ack=380 Win=2102272 Len=0
 6 0.2…  10.1.0.2     10.1.0.101   TCP         1514 80 → 1624 [ACK] Seq=1 Ack=380 Win=2102272 Len=1460 ['
```

```
> Internet Protocol Version 4, Src: 10.1.0.101, Dst: 10.1.0.2
v Transmission Control Protocol, Src Port: 1624, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
      Source Port: 1624
      Destination Port: 80
      [Stream index: 0]
      [TCP Segment Len: 0]
      Sequence number: 1    (relative sequence number)
      [Next sequence number: 1    (relative sequence number)]
      Acknowledgment number: 1    (relative ack number)
      0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x010 (ACK)
      Window size value: 1024
      [Calculated window size: 262144]
      [Window size scaling factor: 256]
```

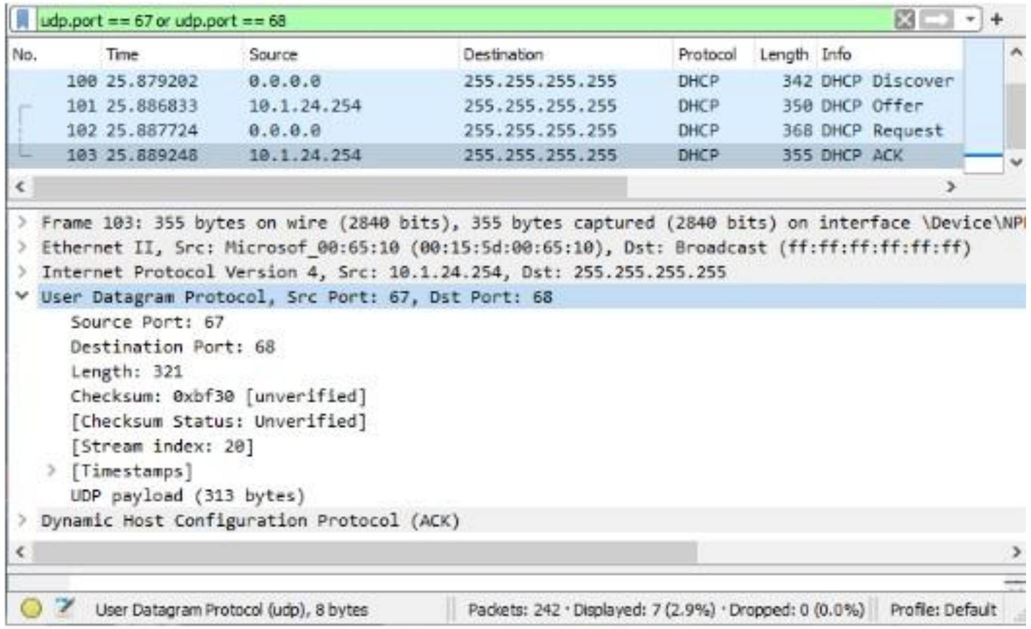
```
0000  00 15 5d 01 ca 76 00 15  5d 01 ca 77 08 00 45 00   ··]··v·· ]··w··E·
0010  00 28 16 49 40 00 80 06  00 00 0a 01 00 65 0a 01   ·(·I@··· ·····e··
0020  00 02 06 58 00 50 61 ff  66 ce 99 26 04 92 50 10   ···X·Pa· f··&··P·
0030  04 00 14 83 00 00                                  ······
```

*Screenshot courtesy of Wireshark*

- Connection-oriented transport protocol
  - ✓ Establish connection
  - ✓ Assign each packet sequence number
  - ✓ Allow the receiver to acknowledge (ACK)
  - ✓ Allow the receiver to send a negative acknowledgement (NACK)
  - ✓ Allow the graceful termination of a session
- TCP-based application protocols
  - ✓ HyperText Transfer Protocol Secure (HTTPS)
  - ✓ Secure Shell (SSH)

# User Datagram Protocol

- Connectionless, unreliable delivery;
- Smaller header;
- UDP-based application protocols
  - ✓ Dynamic Host Configuration Protocol (DHCP);
  - ✓ Trivial File Transfer Protocol (TFTP);



```
udp.port == 67 or udp.port == 68

No.     Time        Source          Destination       Protocol  Length Info
    100 25.879202   0.0.0.0         255.255.255.255   DHCP         342 DHCP Discover
    101 25.886833   10.1.24.254     255.255.255.255   DHCP         350 DHCP Offer
    102 25.887724   0.0.0.0         255.255.255.255   DHCP         368 DHCP Request
    103 25.889248   10.1.24.254     255.255.255.255   DHCP         355 DHCP ACK
```

```
> Frame 103: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NP
> Ethernet II, Src: Microsof_00:65:10 (00:15:5d:00:65:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.1.24.254, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 321
    Checksum: 0xbf30 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 20]
  > [Timestamps]
    UDP payload (313 bytes)
> Dynamic Host Configuration Protocol (ACK)
```

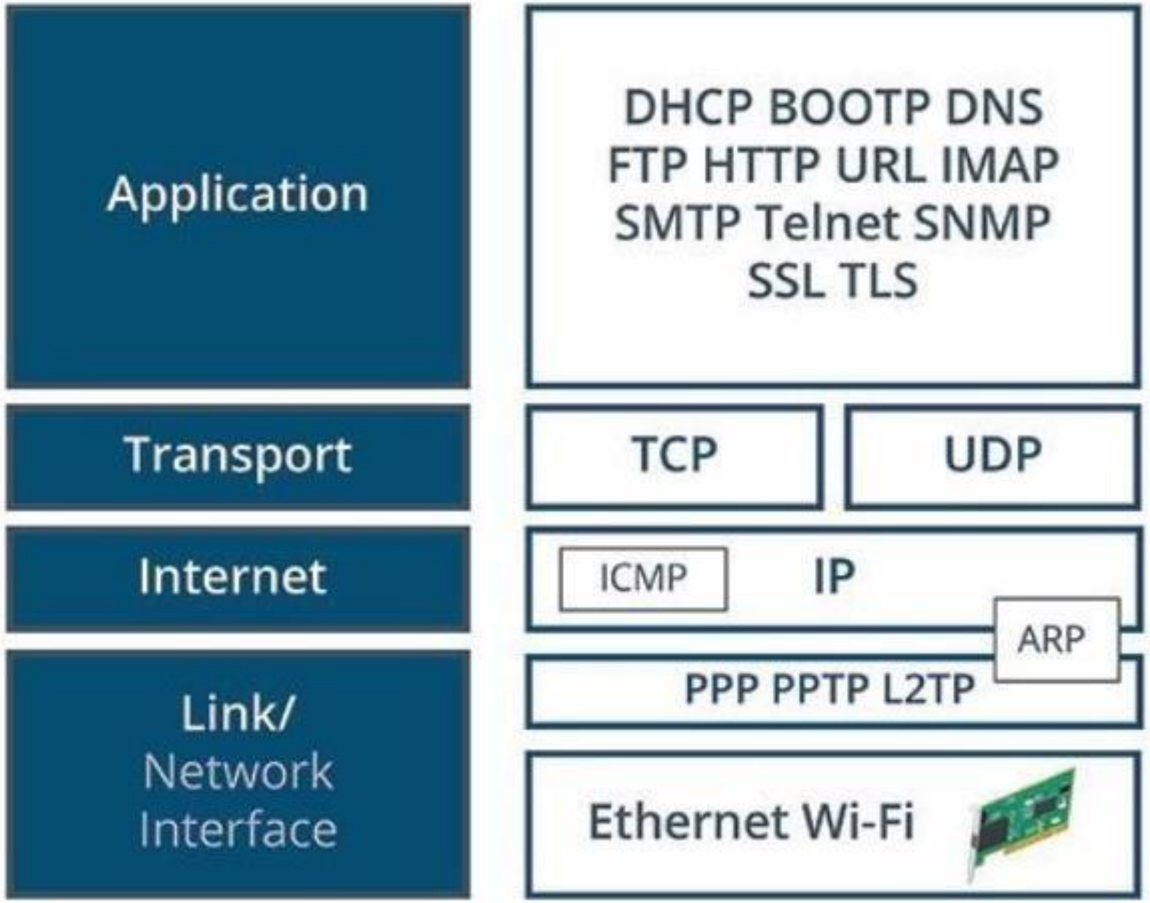
User Datagram Protocol (udp), 8 bytes | Packets: 242 · Displayed: 7 (2.9%) · Dropped: 0 (0.0%) | Profile: Default

*Screenshot courtesy of Wireshark.*

# Well-known Ports

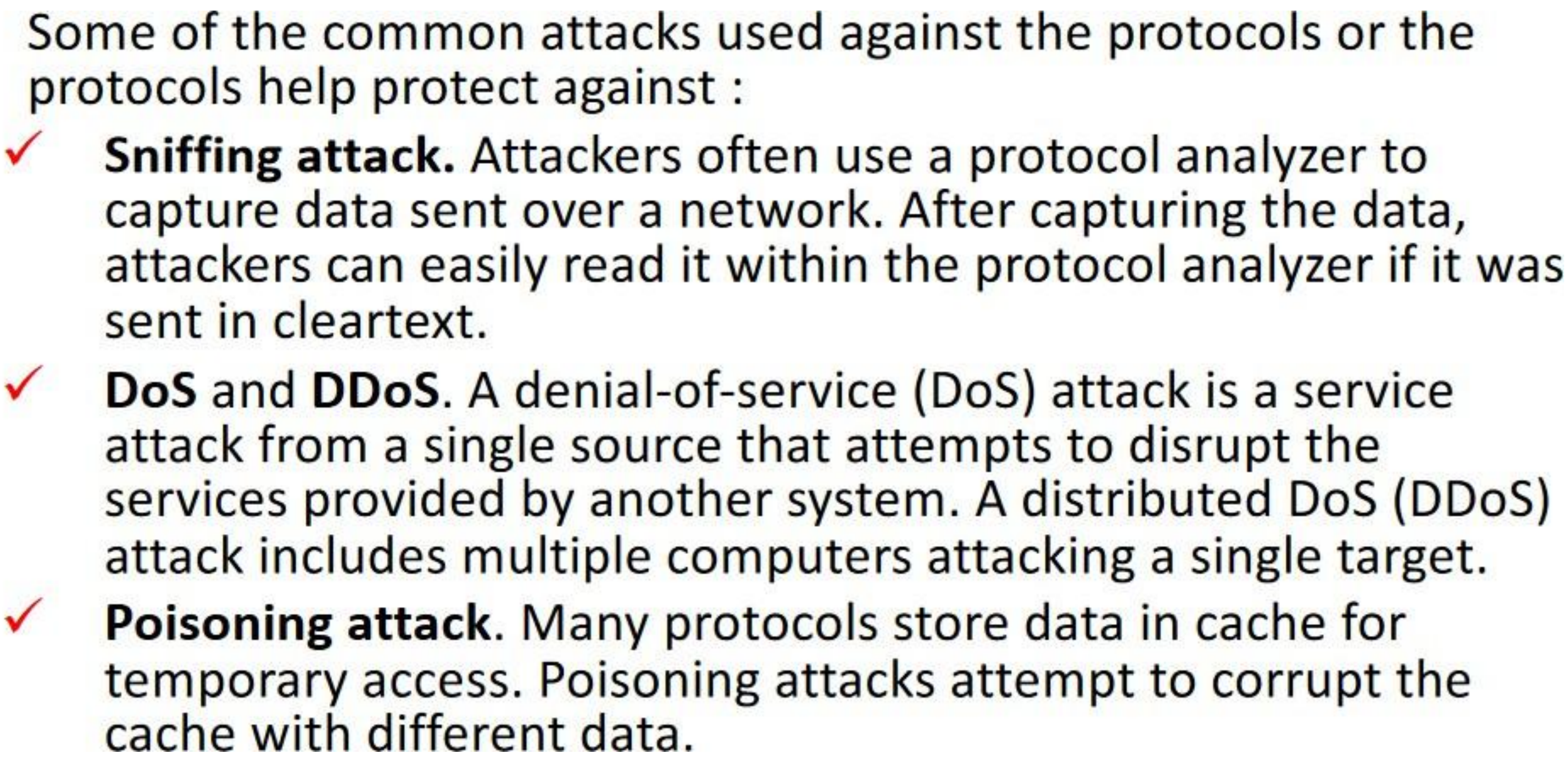
| | | | | | |
|---|---|---|---|---|---|
| Networking | DNS<br>UDP/53<br>TCP/53 | DHCP<br>UDP/67<br>UDP/68 | NBT<br>UDP/TCP<br>137-139 | SNMP<br>UDP/161<br>UDP/162 | LDAP<br>TCP/389 |
| Remote access | SSH<br>TCP/22 | Telnet<br>TCP/23 | RDP<br>TCP/3389 | | |
| File transfer | FTP<br>TCP/20<br>TCP/21 | HTTP<br>TCP/80 | HTTPS<br>TCP/443 | SMB<br>TCP/445 | |
| Email | SMTP<br>TCP/25 | POP3<br>TCP/110 | IMAP<br>TCP/143 | | |

# TCP/IP



Application
DHCP BOOTP DNS
FTP HTTP URL IMAP
SMTP Telnet SNMP
SSL TLS
Transport
TCP
UDP
Internet
ICMP
IP
ARP
PPP PPTP L2TP
Link/
Network
Interface
Ethernet Wi-Fi

# Related Attacks



- Some of the common attacks used against the protocols or the protocols help protect against :

  ✓ **Sniffing attack.** Attackers often use a protocol analyzer to capture data sent over a network. After capturing the data, attackers can easily read it within the protocol analyzer if it was sent in cleartext.

  ✓ **DoS** and **DDoS**. A denial-of-service (DoS) attack is a service attack from a single source that attempts to disrupt the services provided by another system. A distributed DoS (DDoS) attack includes multiple computers attacking a single target.

  ✓ **Poisoning attack**. Many protocols store data in cache for temporary access. Poisoning attacks attempt to corrupt the cache with different data.

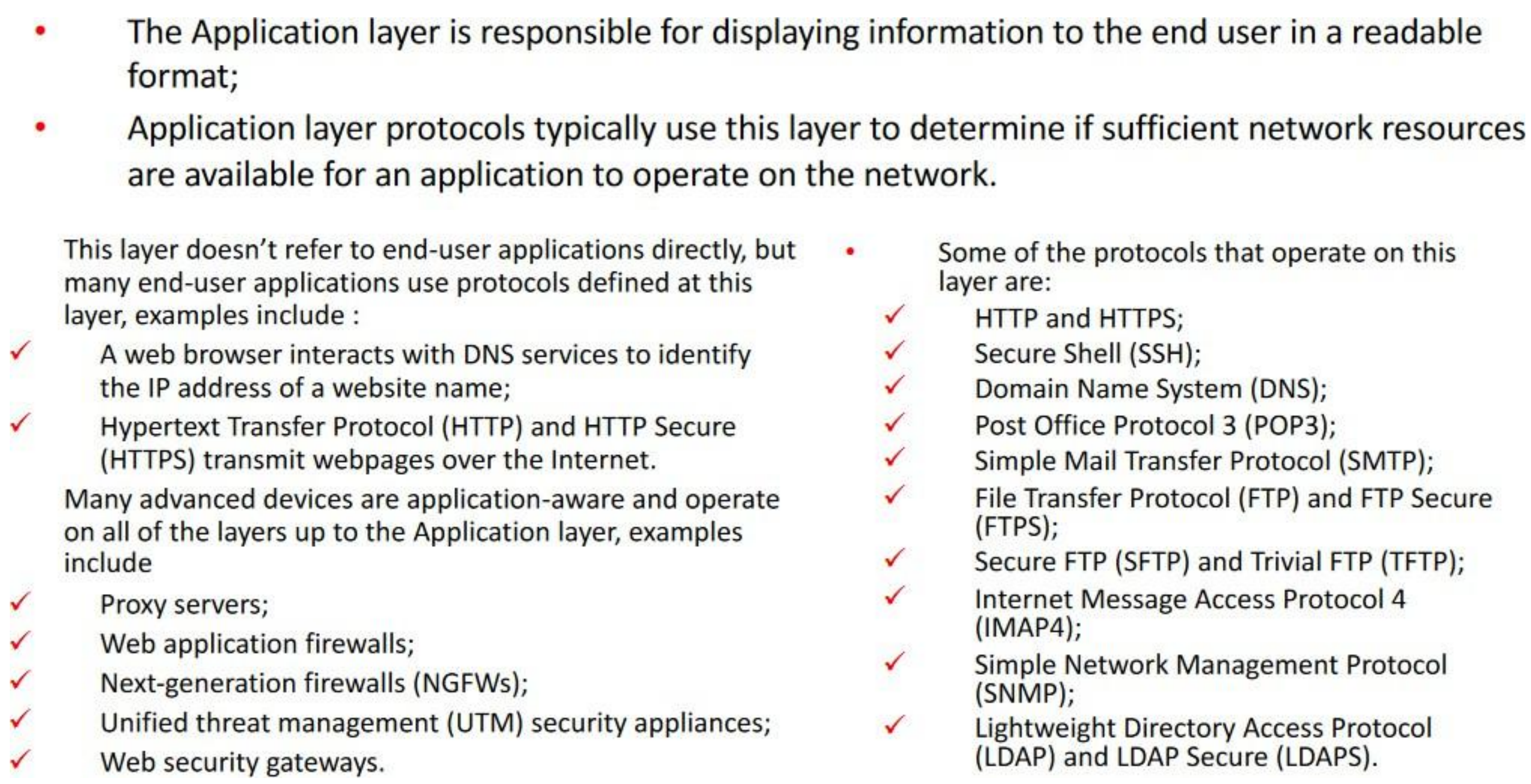
# Layer 5: Session

- The Session layer is responsible for establishing, maintaining, and terminating sessions between systems;
- In this context, a session refers to an extended connection between two systems, sometimes referred to as dialogues or conversations;
- If you log on to a webpage, the Session layer establishes a connection with the web server and keeps it open while you’re interacting with the webpages;
- When you close the pages, the Session layer terminates the session;
- If you’re like many users, you probably have more than one application open at a time and each of these is a different session, and the Session layer manages them separately.

# Layer 6: Presentation

- The Presentation layer is responsible for formatting the data needed by the end-user applications.
- American Standard Code for Information Interchange (ASCII) and Extended Binary Coded Decimal Interchange Code (EBCDIC) are two standards that define codes used to display characters on this layer.

# Layer 7: Application



- The Application layer is responsible for displaying information to the end user in a readable format;
- Application layer protocols typically use this layer to determine if sufficient network resources are available for an application to operate on the network.

This layer doesn't refer to end-user applications directly, but many end-user applications use protocols defined at this layer, examples include :

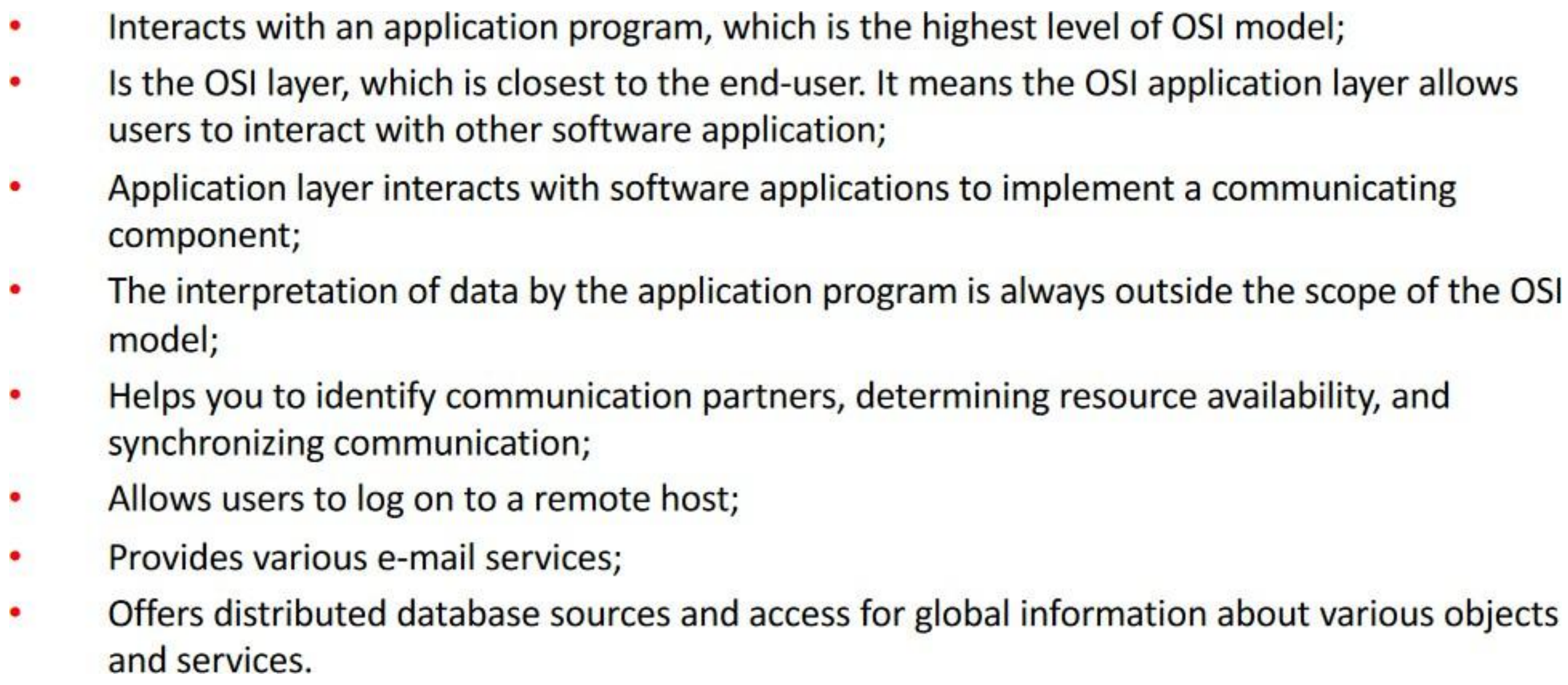
- ✓ A web browser interacts with DNS services to identify the IP address of a website name;
- ✓ Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) transmit webpages over the Internet.

Many advanced devices are application-aware and operate on all of the layers up to the Application layer, examples include

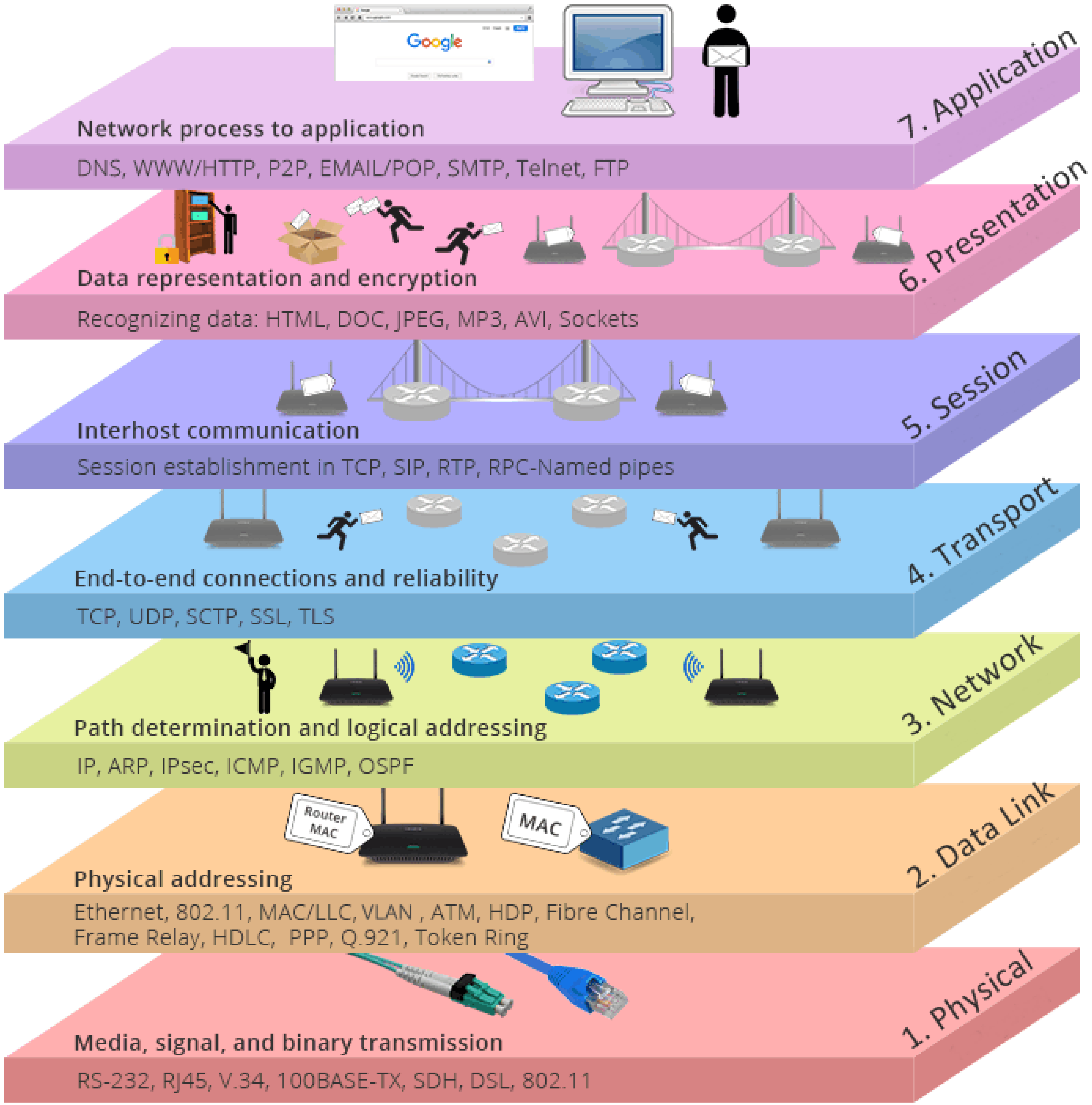
- ✓ Proxy servers;
- ✓ Web application firewalls;
- ✓ Next-generation firewalls (NGFWs);
- ✓ Unified threat management (UTM) security appliances;
- ✓ Web security gateways.

- Some of the protocols that operate on this layer are:
  - ✓ HTTP and HTTPS;
  - ✓ Secure Shell (SSH);
  - ✓ Domain Name System (DNS);
  - ✓ Post Office Protocol 3 (POP3);
  - ✓ Simple Mail Transfer Protocol (SMTP);
  - ✓ File Transfer Protocol (FTP) and FTP Secure (FTPS);
  - ✓ Secure FTP (SFTP) and Trivial FTP (TFTP);
  - ✓ Internet Message Access Protocol 4 (IMAP4);
  - ✓ Simple Network Management Protocol (SNMP);
  - ✓ Lightweight Directory Access Protocol (LDAP) and LDAP Secure (LDAPS).

# Layer 4: Application Layer (TCP/IP)



- Interacts with an application program, which is the highest level of OSI model;
- Is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application;
- Application layer interacts with software applications to implement a communicating component;
- The interpretation of data by the application program is always outside the scope of the OSI model;
- Helps you to identify communication partners, determining resource availability, and synchronizing communication;
- Allows users to log on to a remote host;
- Provides various e-mail services;
- Offers distributed database sources and access for global information about various objects and services.



7. Application

Network process to application

DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP

6. Presentation

Data representation and encryption

Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets

5. Session

Interhost communication

Session establishment in TCP, SIP, RTP, RPC-Named pipes

4. Transport

End-to-end connections and reliability

TCP, UDP, SCTP, SSL, TLS

3. Network

Path determination and logical addressing

IP, ARP, IPsec, ICMP, IGMP, OSPF

2. Data Link

Physical addressing

Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring

1. Physical

Media, signal, and binary transmission

RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11