CSCI369 Ethical Hacking

Week 3 –TCP/IP Basics & Capturing Traffic

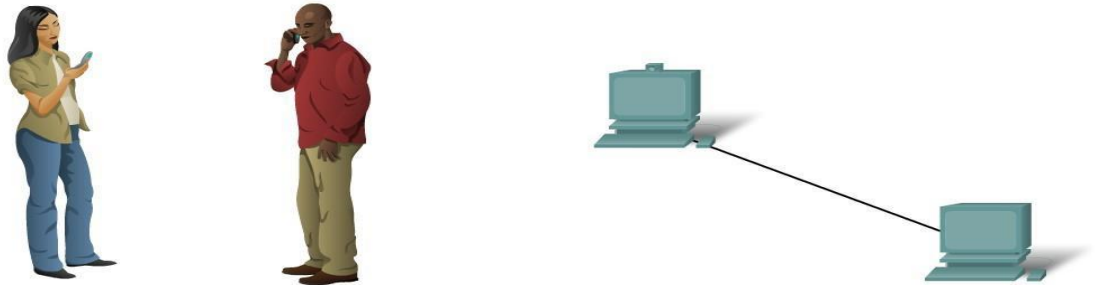
Instructor: Dr. Manoj Kumar

Faculty of Engineering and Information Sciences

These slides are based on the lecture slides prepared by Dr. Joonsang Baek and Dr. Manoj Kumar

Network Structure

- Define the elements of communication
  - 3 common elements of communication
    - message source
    - the channel
    - message destination



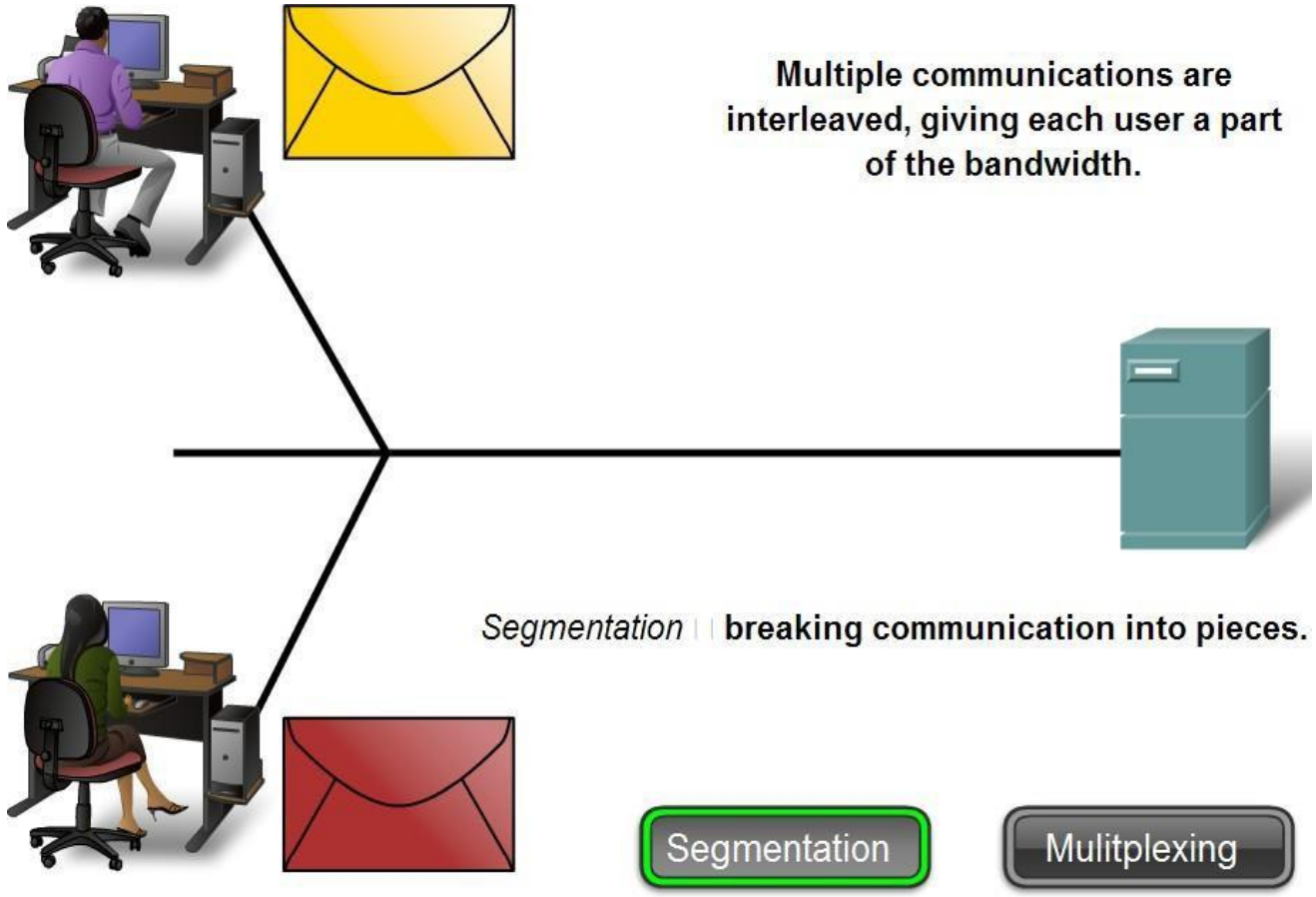
- Define a network

  data or information networks capable of carrying many different types of communications

Network Structure

- Describe how messages are communicated

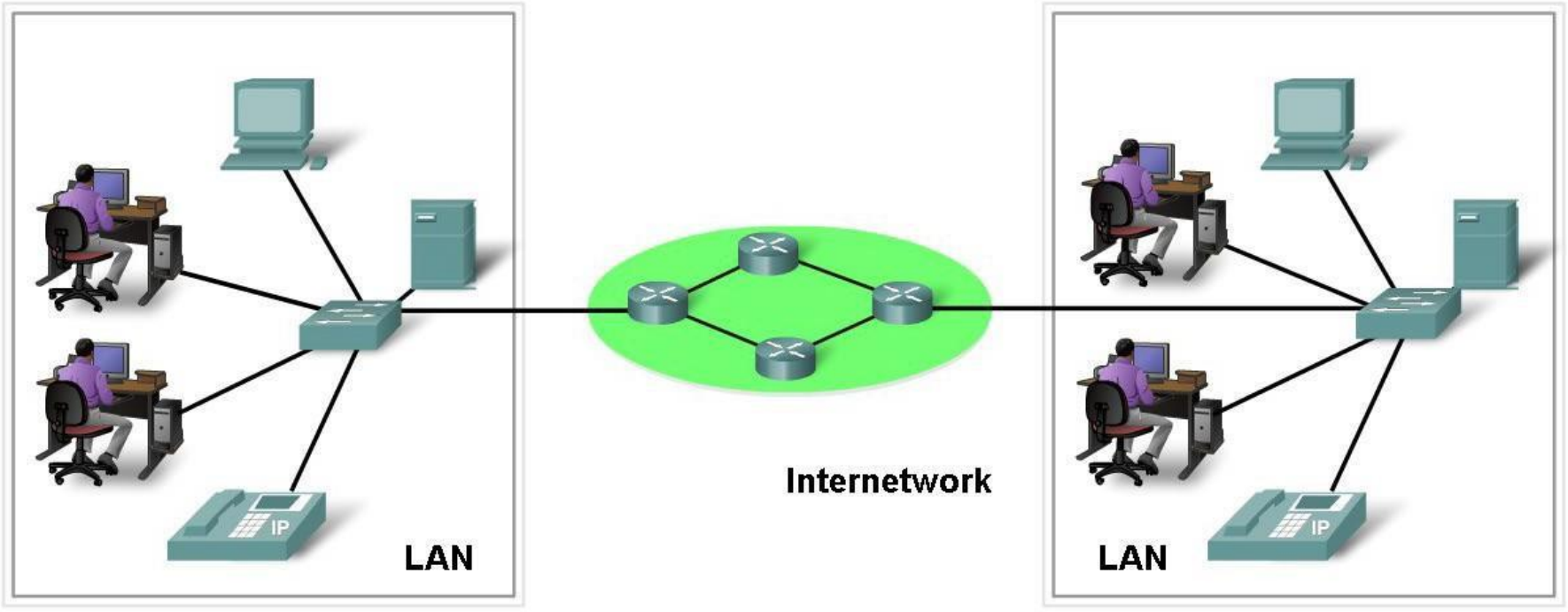
  Data is sent across a network in small “chunks” called segments



UNIVERSITY OF WOLLONGONG IN DUBAI

Network Structure

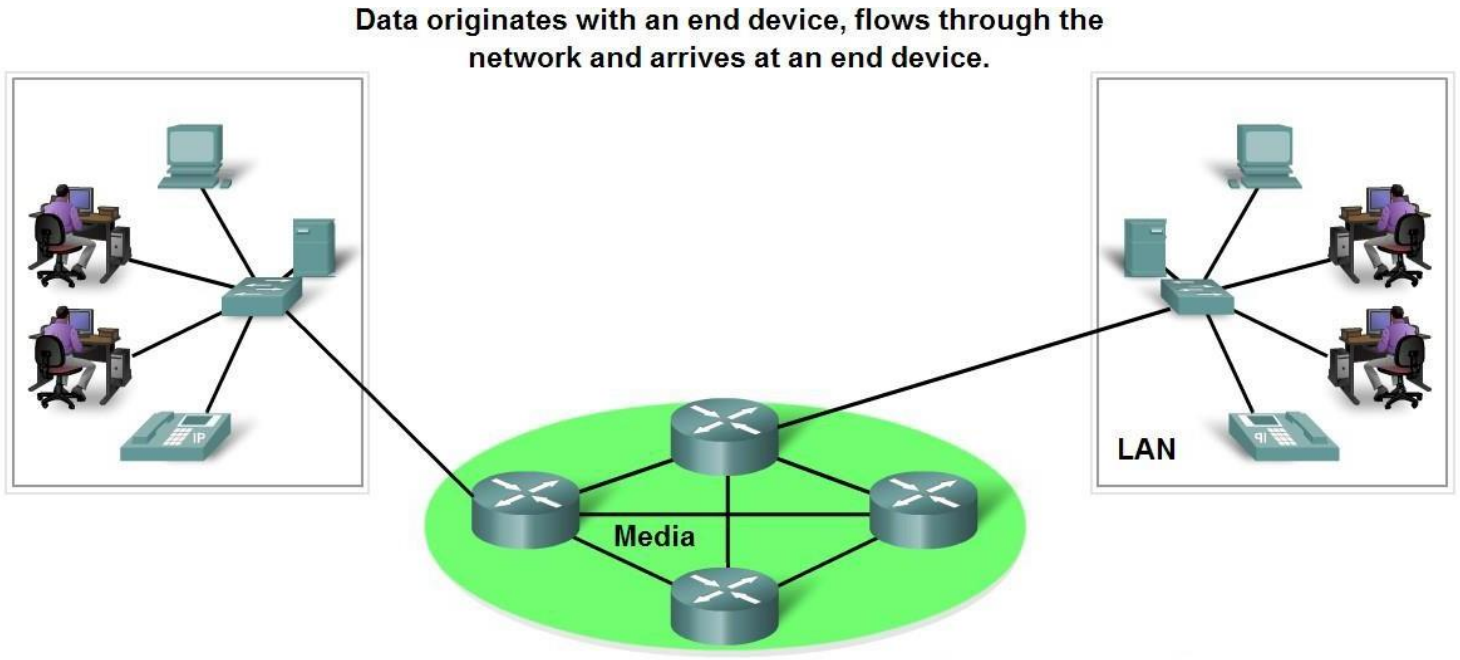
- Define the components of a network
  - Network components
    - hardware
    - software



UNIVERSITY OF WOLLONGONG IN DUBAI

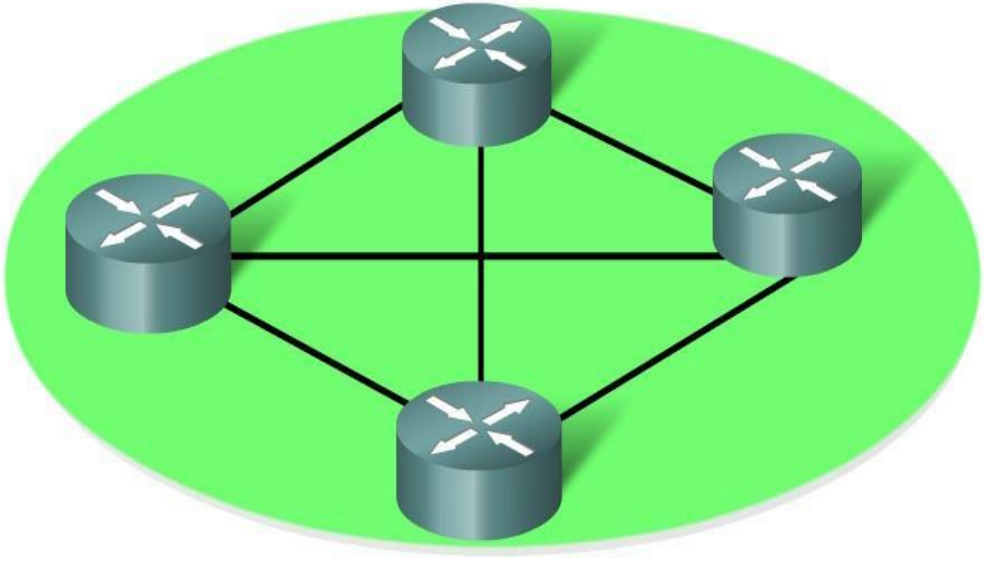
Network Structure

- End Devices and their Role in the Network
  - –End devices form interface with human network & communications network
  - –Role of end devices:
    - client
    - server
    - both client and server



Network Structure

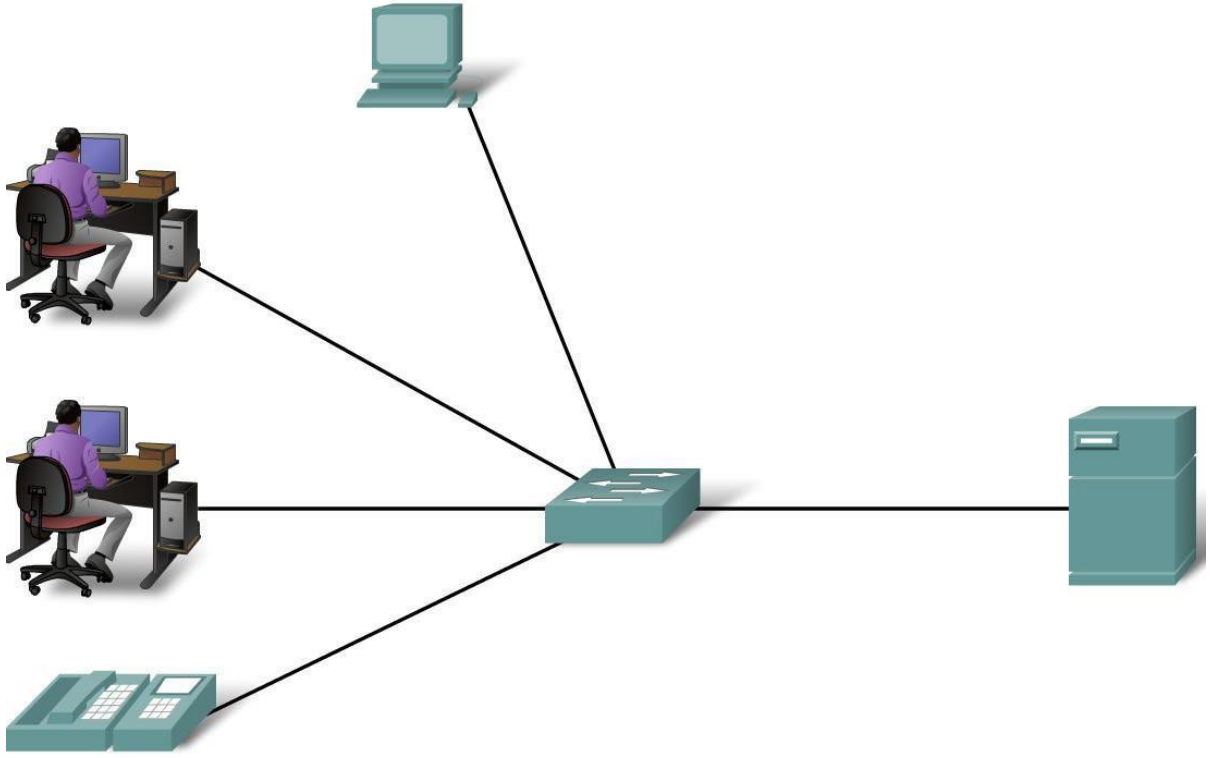
- Identify the role of an **intermediary device** in a data network and be able to contrast that role with the role of an end device
  - Role of an intermediary device
    - provides connectivity and ensures data flows across network



Network Types

- Define Local Area Networks (LANs)

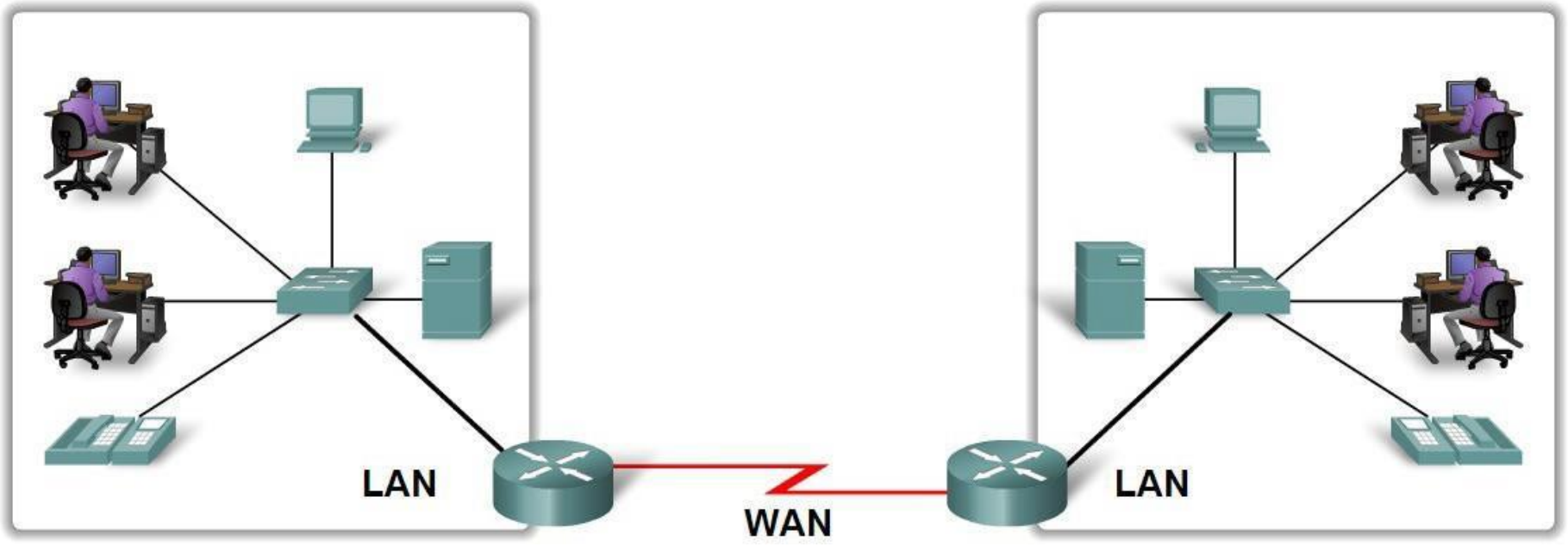
  - A network serving a home, building or campus is considered a Local Area Network (LAN)



Network Types

- Define Wide Area Networks (WANs)

  - LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN)



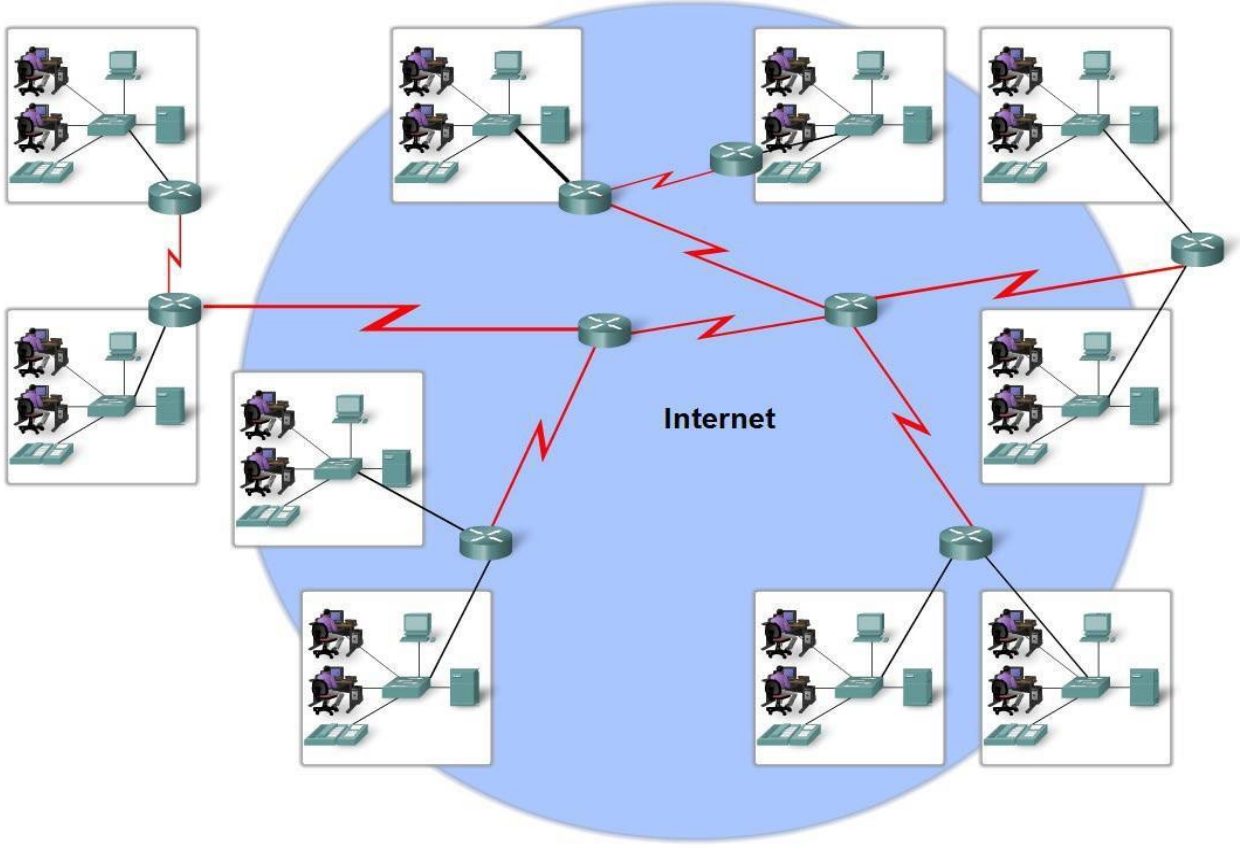
UNIVERSITY OF WOLLONGONG IN DUBAI

Network Types

- Define the Internet

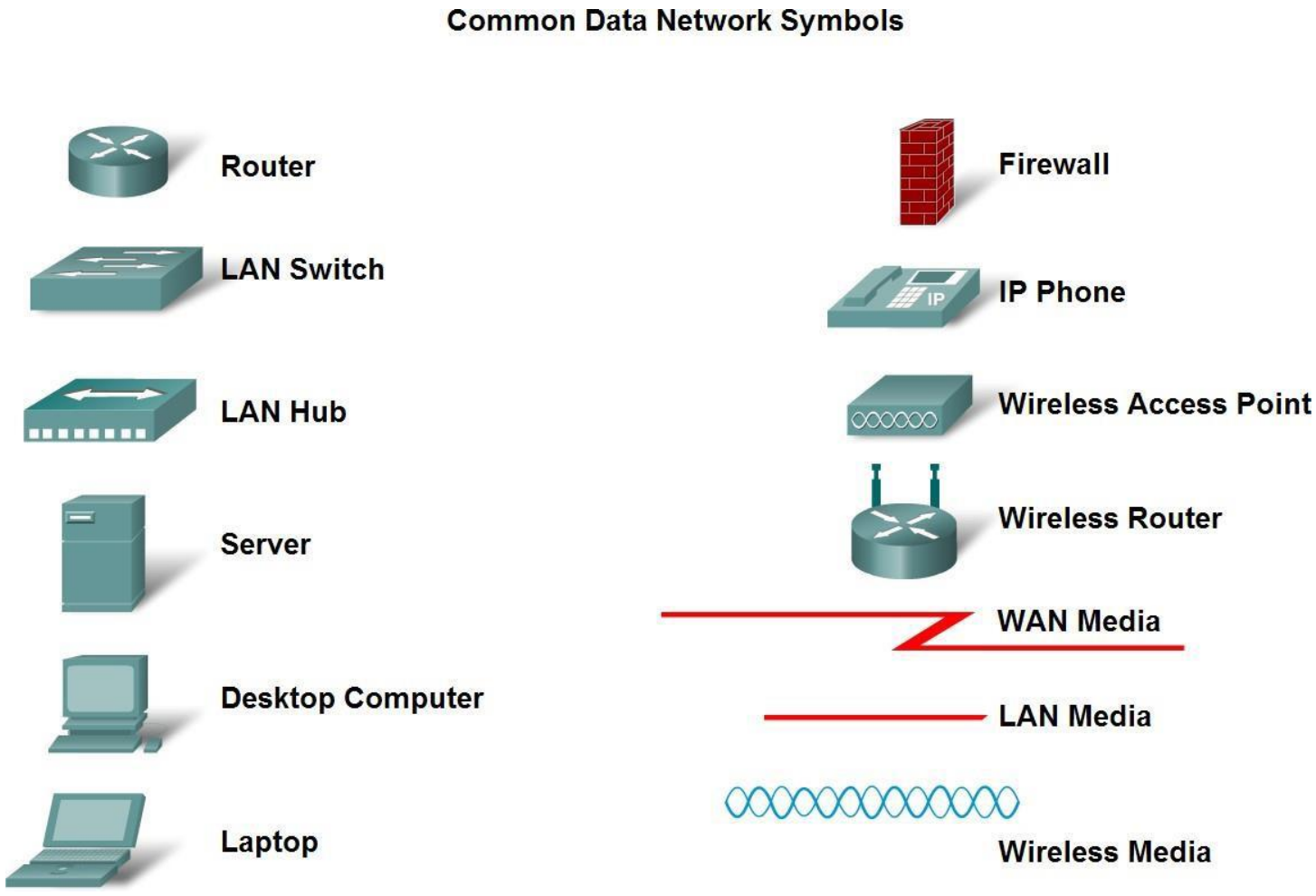
  The internet is defined as a

  global mesh of interconnected networks



Network Devices

- Describe network representations

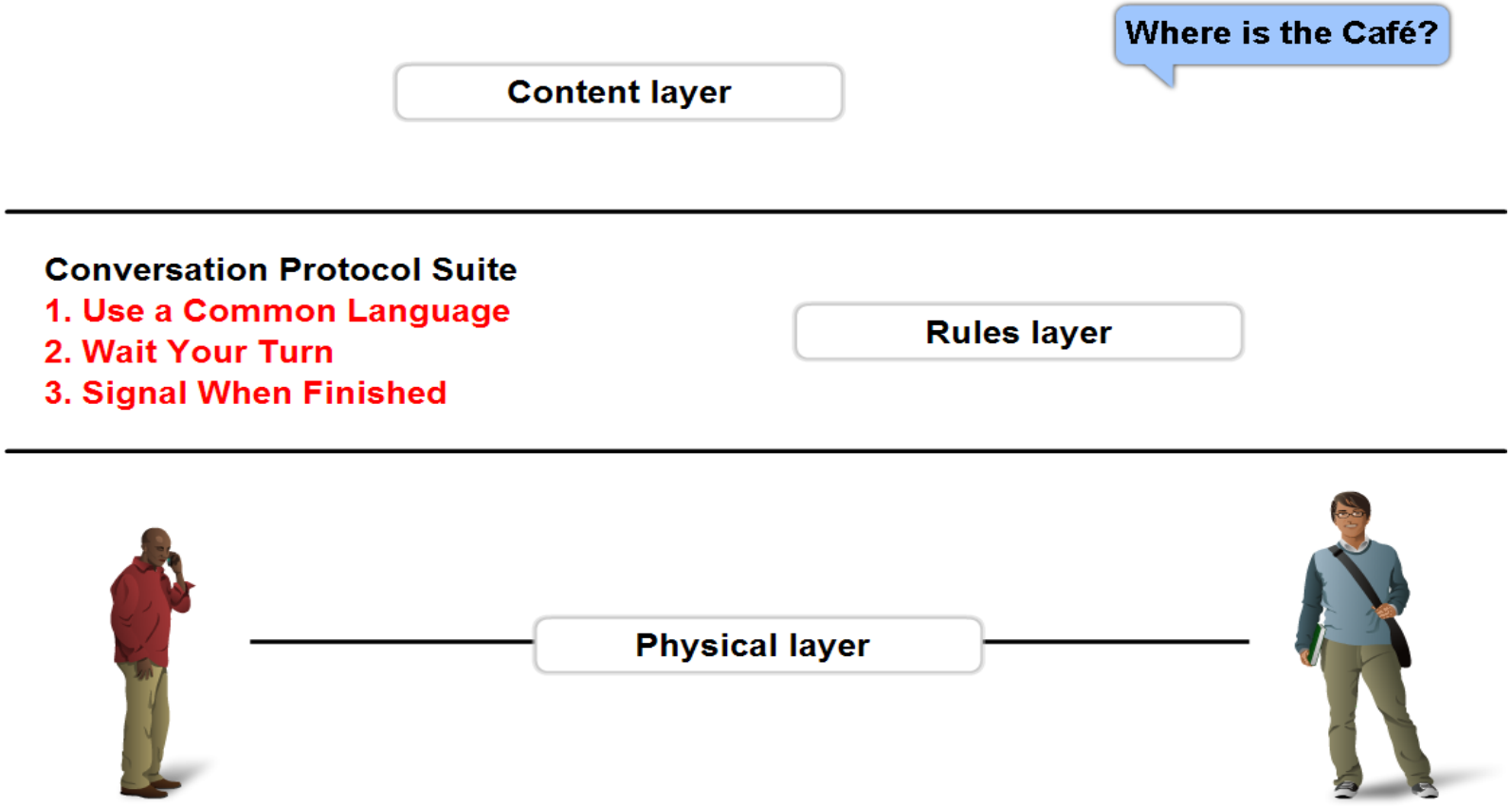


UNIVERSITY OF WOLLONGONG IN DUBAI

Function of Protocol in Network Communication

- The importance of protocols and how they are used to facilitate communication over data networks

  A protocol is a set of predetermined rules



UNIVERSITY OF WOLLONGONG IN DUBAI

Function of Protocol in Network Communication

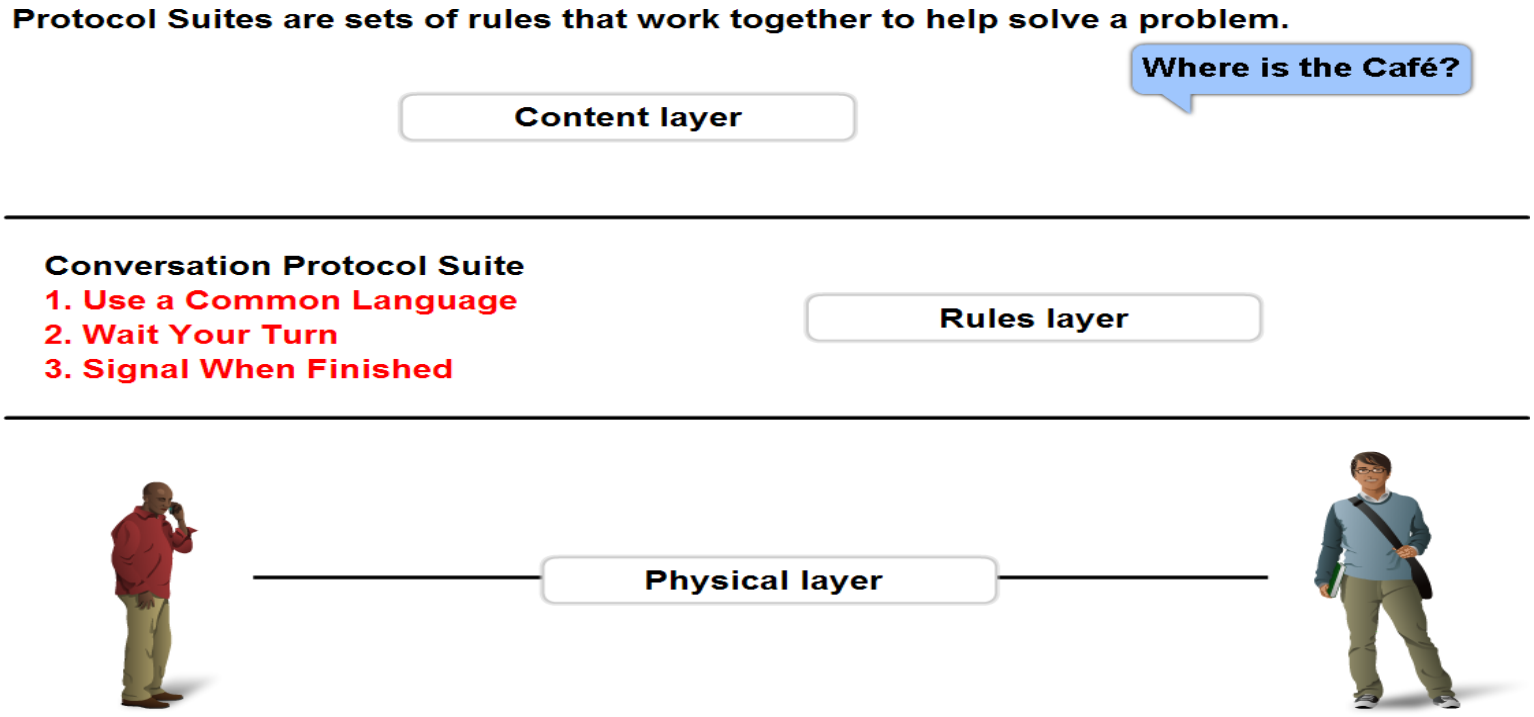
- Explain network protocols

  Network protocols are used to allow devices to communicate successfully

Protocols provide:
The format or structure of the message
The process by which networking devices share information about pathways to other networks
How and when error and system messages are passed between devices
The setting up and termination of data transfer sessions

Function of Protocol in Network Communication

- Describe Protocol suites and industry standards

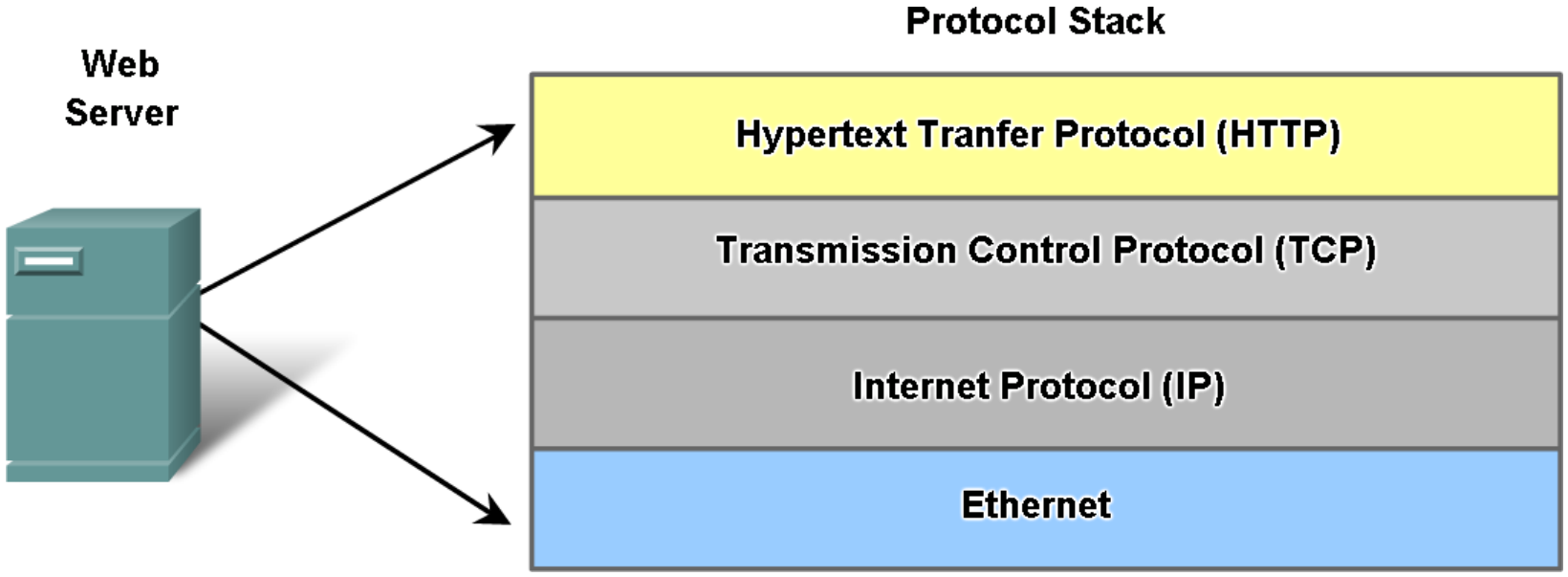


A standard is

a process or protocol that has been endorsed by the networking industry and ratified by a standards organization

Function of Protocol in Network Communication

- Define different protocols and how they interact

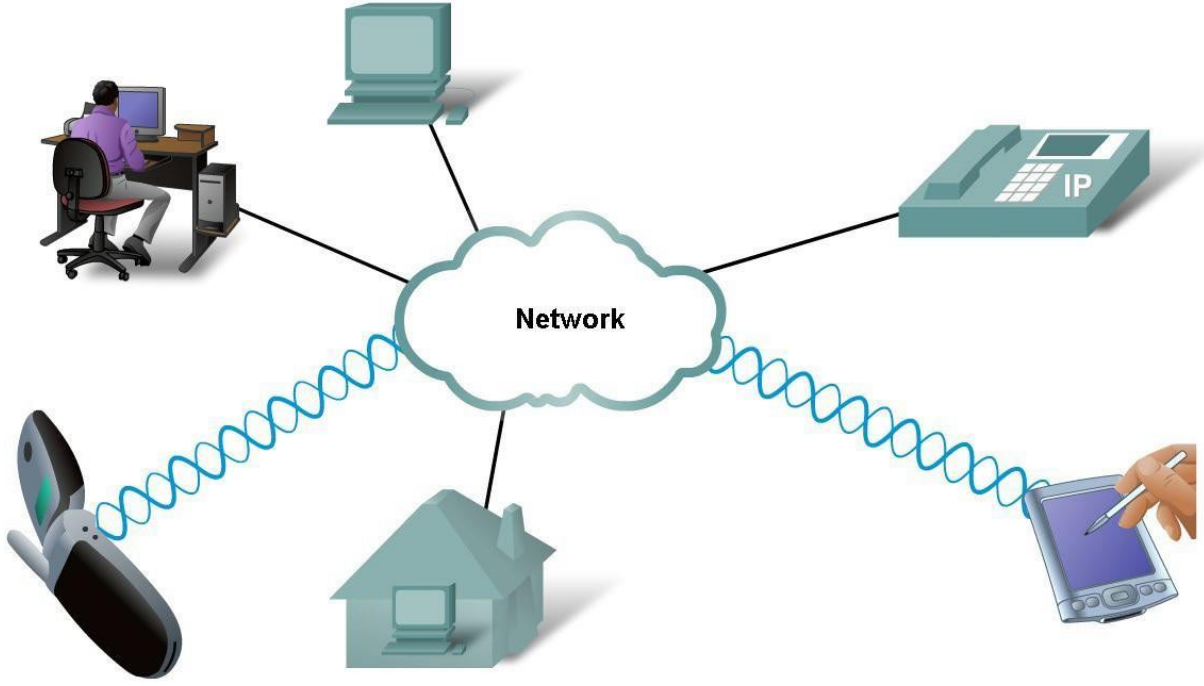


UNIVERSITY OF WOLLONGONG IN DUBAI

Function of Protocol in Network Communication

- Technology independent Protocols

  -Many diverse types of devices can communicate using the same sets of protocols. This is because protocols specify network functionality, not the underlying technology to support this functionality.

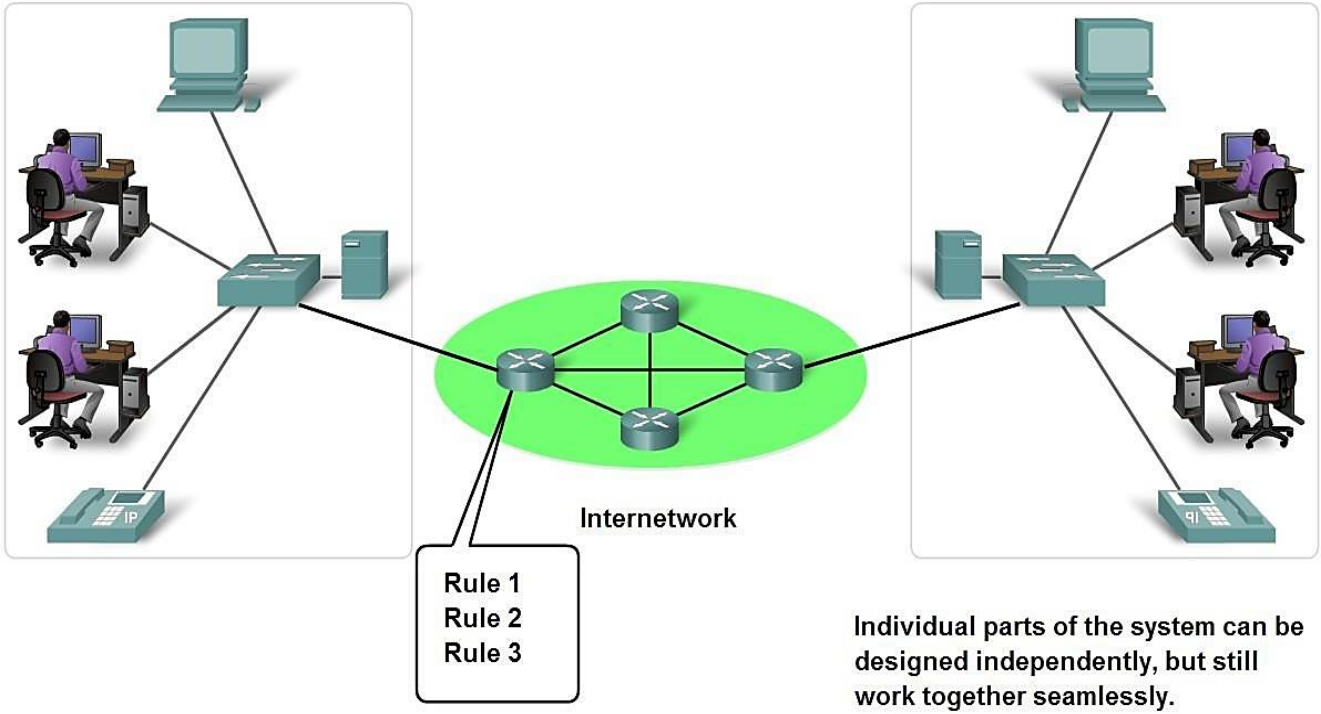


UNIVERSITY
OF WOLLONGONG
IN DUBAI

Layers with TCP/IP and OSI Model

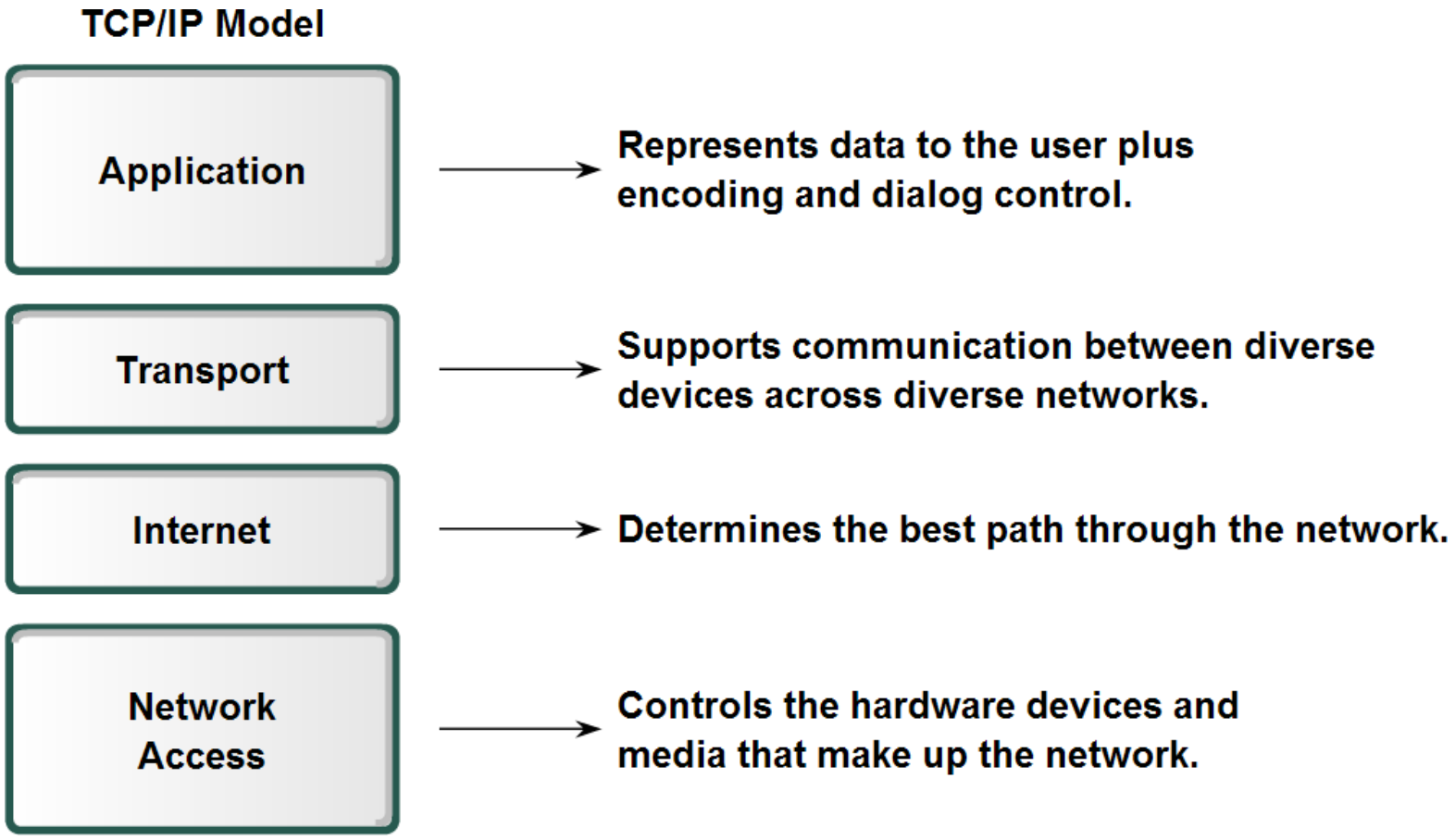
- Explain the benefits of using a layered model
  - Benefits include
    - Assists in protocol design
    - Changes in one layer do not affect other layers
    - provides a common language

Using a layered model helps in the design of complex, multi-use, multi-vendor networks.



Layers with TCP/IP and OSI Model

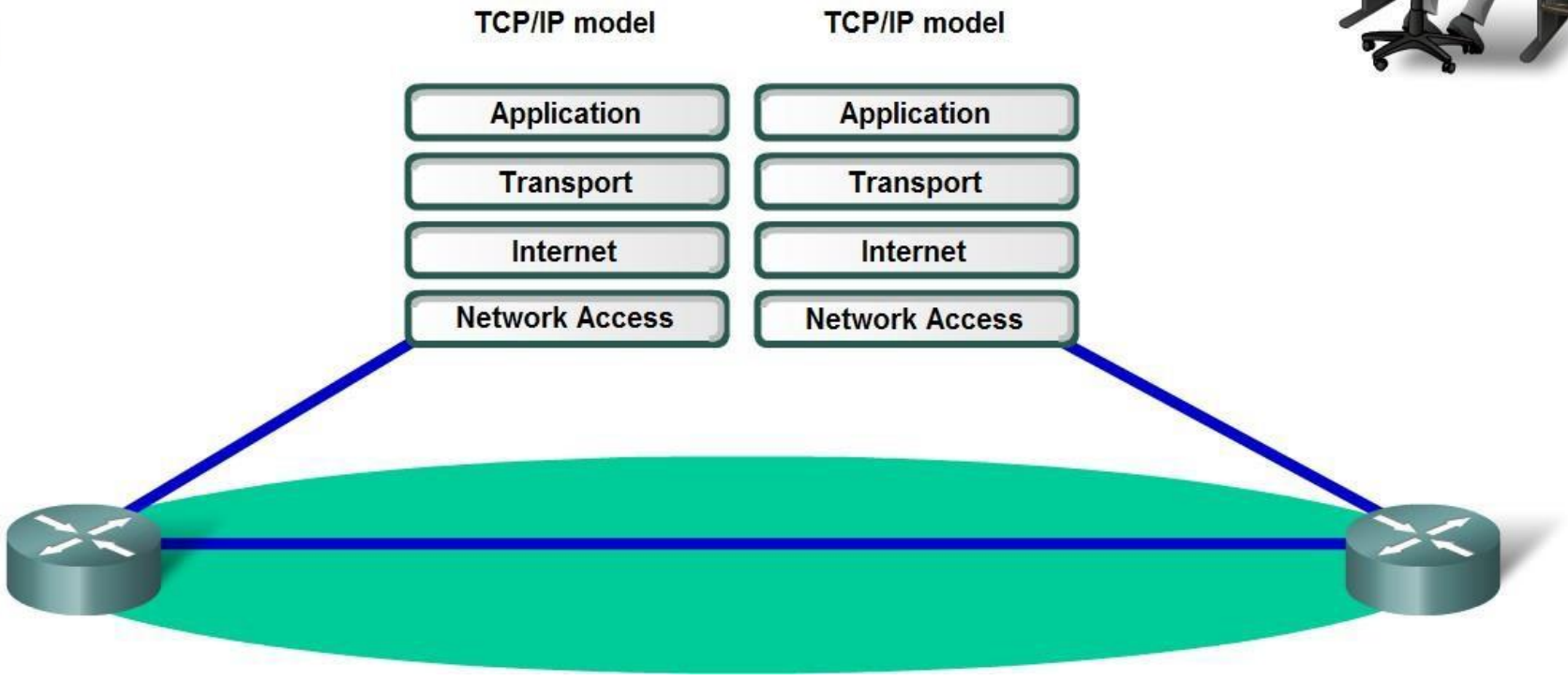
- Describe TCP/IP Mode



UNIVERSITY OF WOLLONGONG IN DUBAI

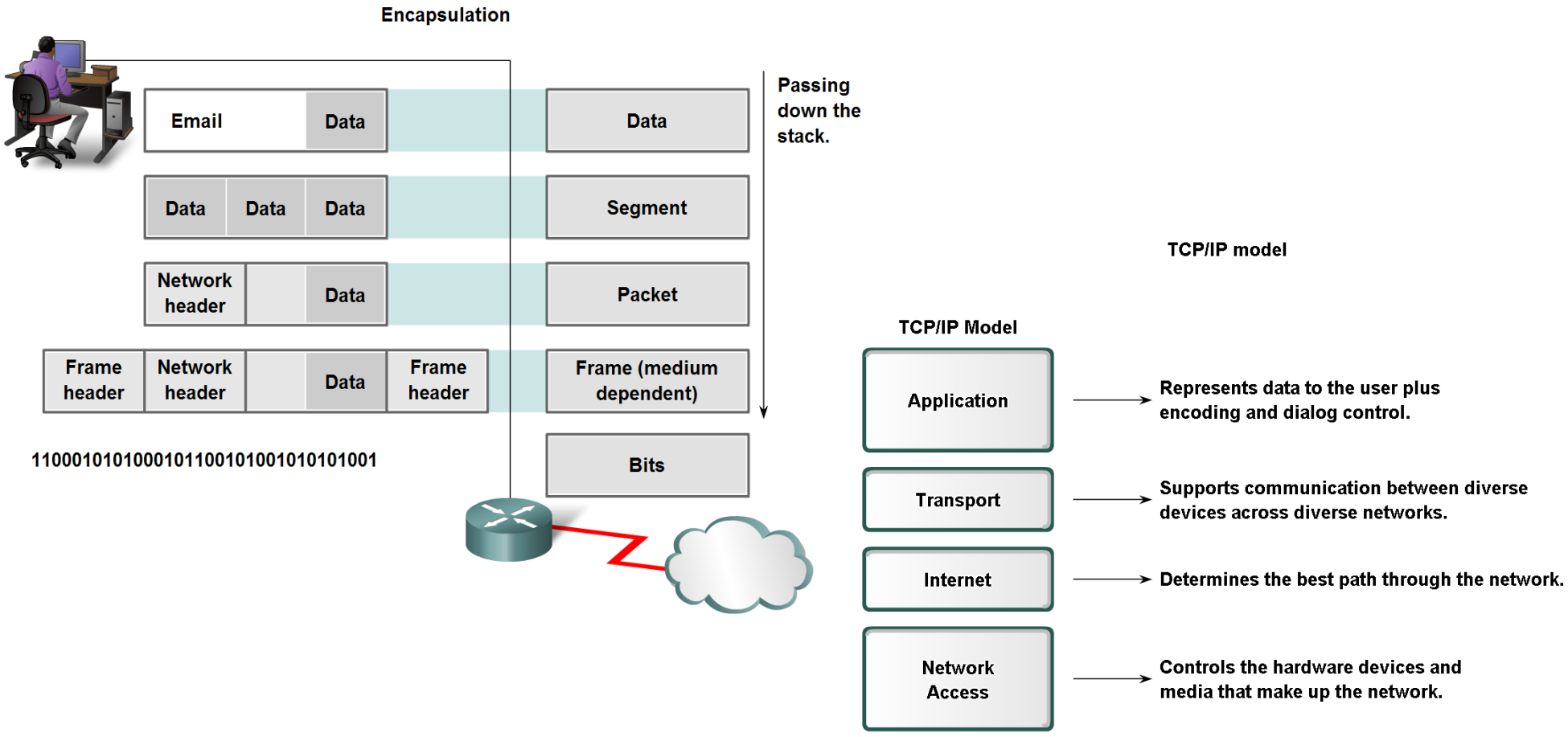
Layers with TCP/IP and OSI Model

- Describe the Communication Process



Layers with TCP/IP and OSI Model

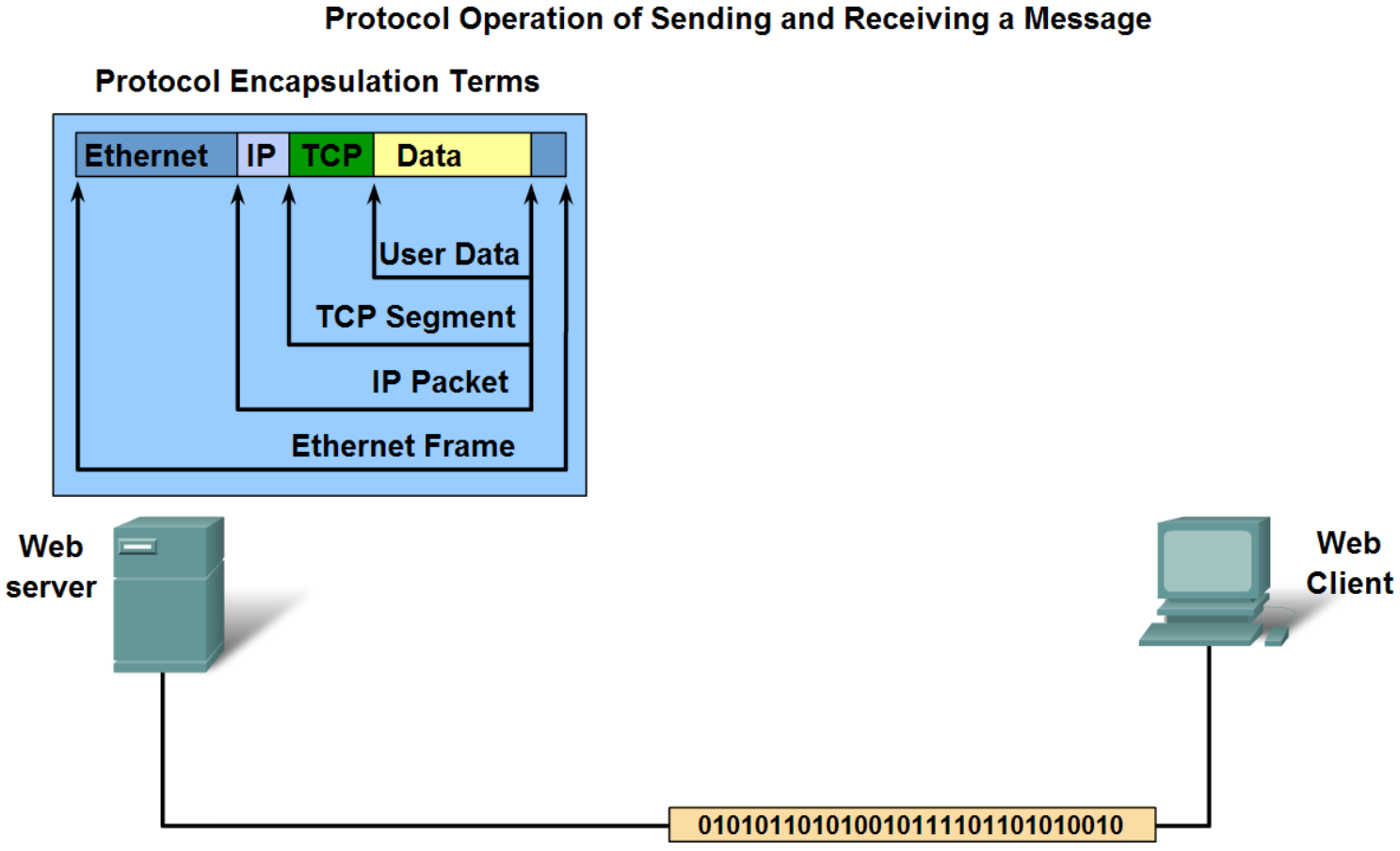
- Explain protocol data units (PDU) and encapsulation



UNIVERSITY OF WOLLONGONG IN DUBAI

Layers with TCP/IP and OSI Model

- Describe the process of sending and receiving messages



UNIVERSITY OF WOLLONGONG IN DUBAI

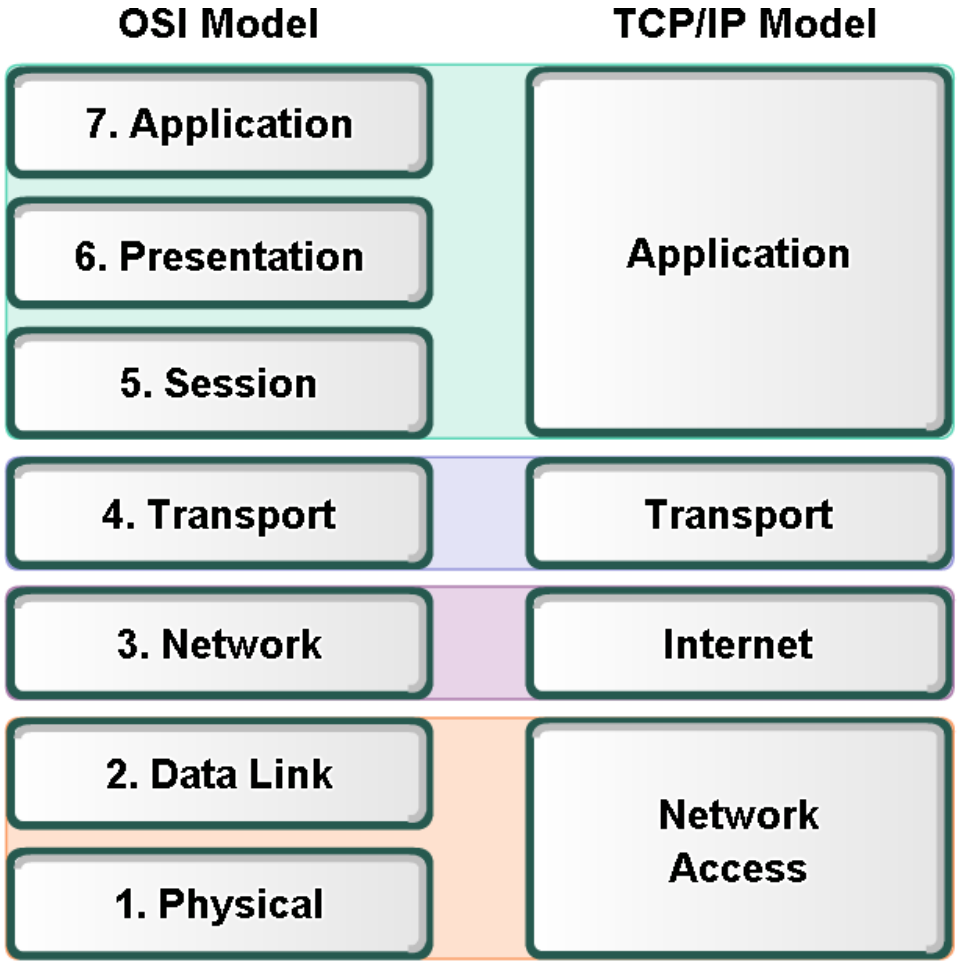
Layers with TCP/IP and OSI Model

- Define OSI

UNIVERSITY
OF WOLLONGONG
IN DUBAI

Layers with TCP/IP and OSI Model

- Compare OSI and TCP/IP model

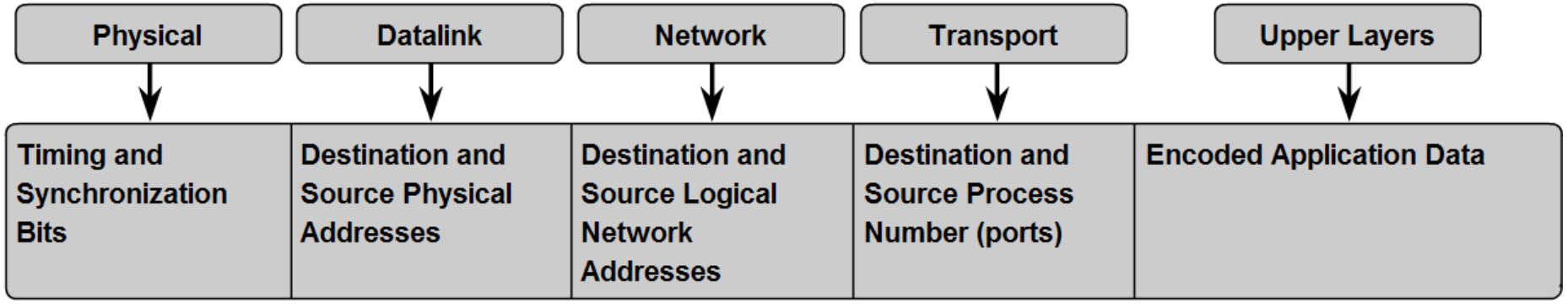


The key parallels are in the Transport and Network layers.

UNIVERSITY OF WOLLONGONG IN DUBAI

Addressing and Naming Schemes

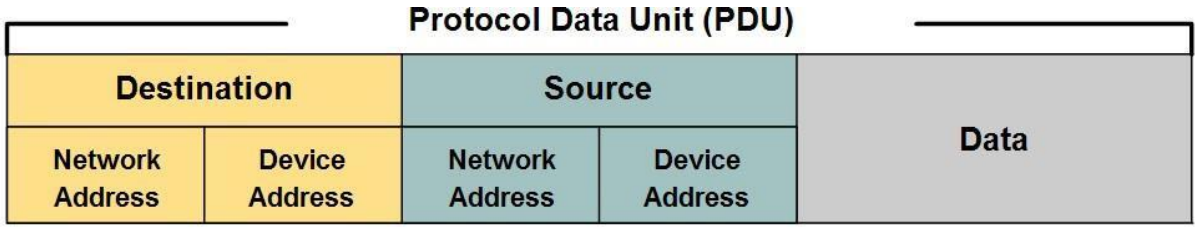
- Explain how labels in encapsulation headers are used to manage communication in data networks

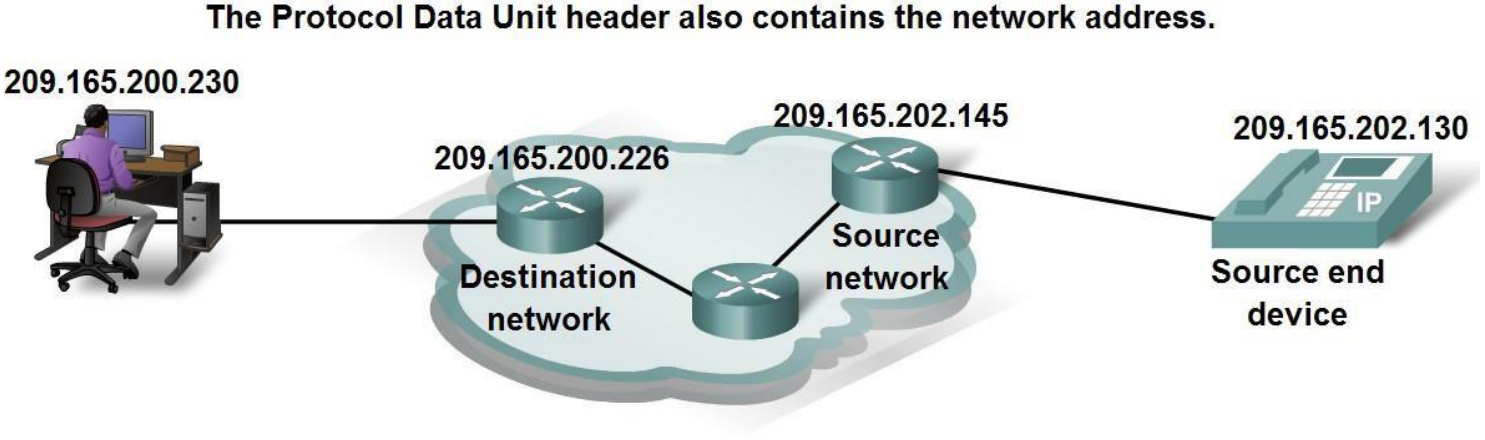


UNIVERSITY OF WOLLONGONG IN DUBAI

Addressing and Naming Schemes

- Explain how labels in encapsulation headers are used to manage communication in data networks





UNIVERSITY OF WOLLONGONG IN DUBAI

The Application Layer

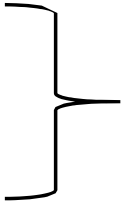
- Some important main applications
  - HTTP: The primary protocol used to communicate over the web
  - FTP: Allows different OSs to transfer files between one another
  - SMTP (Simple Mail Transfer Protocol) : Transmits email messages across the Internet
  - SNMP (Simple Network Management Protocol): Primarily used to monitor devices on a network, such as monitoring a router's state remotely ➔ Should be disabled (Security problem)

The Application Layer

- Some important main applications
  - SSH: Enables users to securely log on to a remote server and issue commands interactively
  - Telnet: Enables users to insecurely log on to a remote server and issue commands interactively.

The Transport Layer

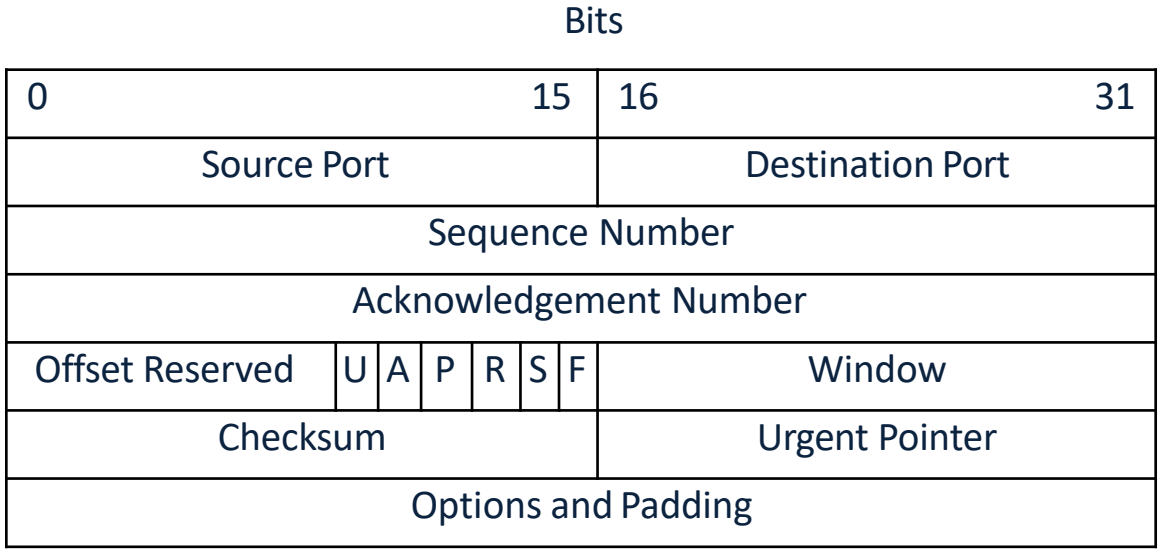
- Main function
  - Data is encapsulated into segments
  - Segments can be TCP or UDP
- TCP
  - Connection-oriented protocol: Sender does not send any data to the destination until the destination node acknowledges that it's listening to the sender
    - ✓The sender sends a `SYN` packet to the receiver
    - ✓The receiver sends `SYN-ACK` to the sender
    - ✓The sender sends `ACK` to the receiver



Three-way handshake

The Transport Layer

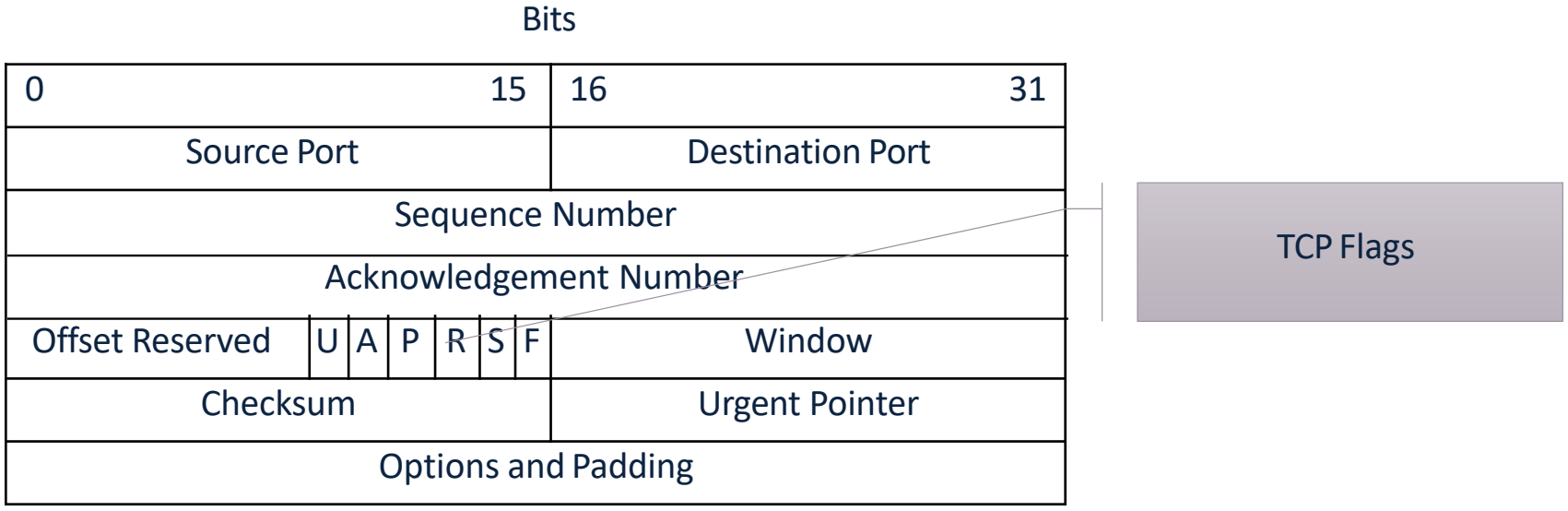
- TCP Segment Header



TCP Header Diagram

The Transport Layer

- TCP Segment Header



TCP Header Diagram

The Transport Layer

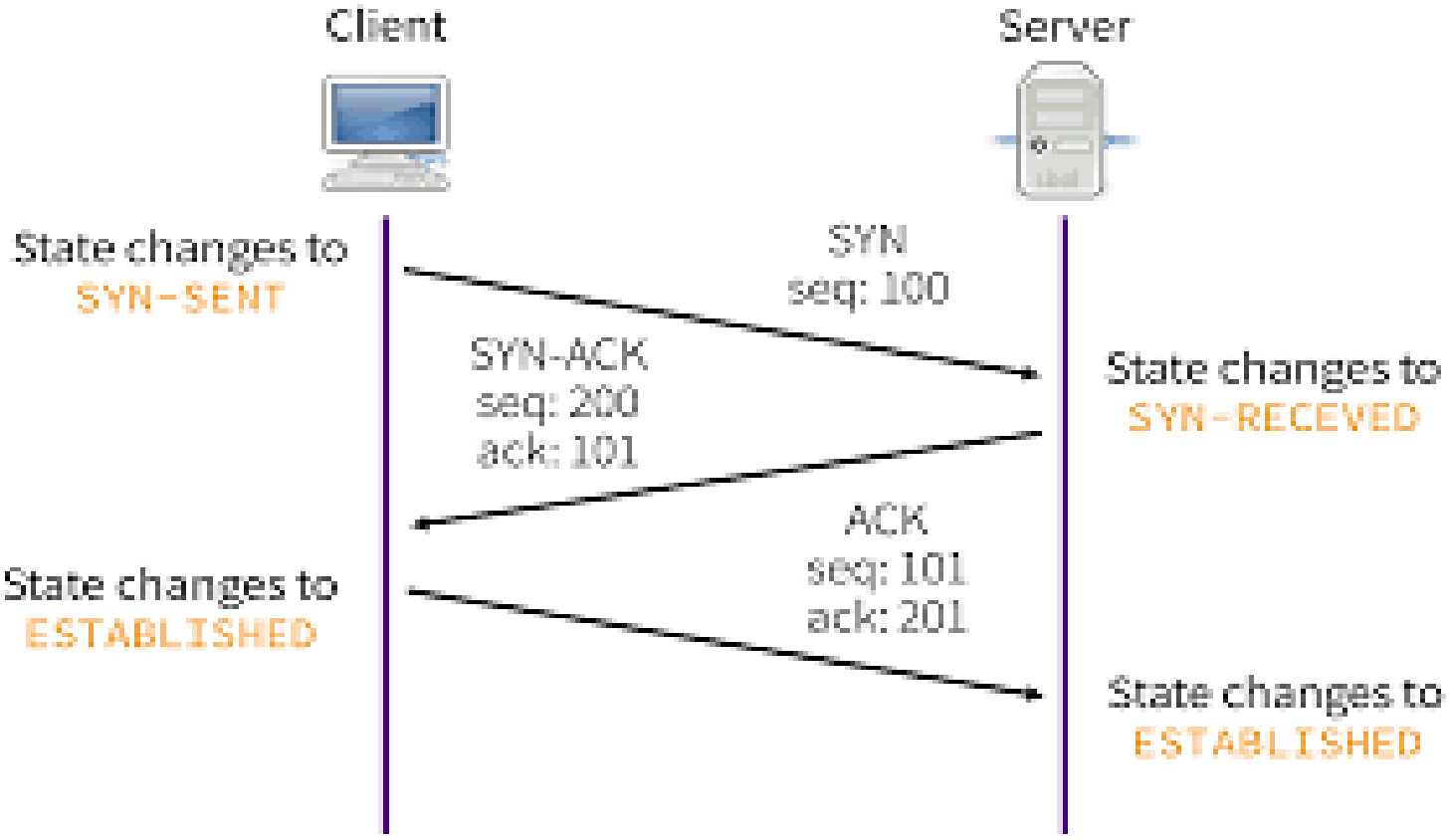
- TCP Flags
  - Can be set 0 (off) or 1 (on)
    - ✓ `SYN` flag – This signifies the beginning of a session
    - ✓ `ACK` flag – This acknowledges a connection request
    - ✓ `PSH` flag – This flag is used to deliver data directly to an application (Data is not buffered; it is sent immediately)
    - ✓ `URG` flag – This flag is used to signify urgent data
    - ✓ `RST` flag – This resets or drops a connection
    - ✓ `FIN` flag – The indicates that the connection is finished

The Transport Layer

- Sequence Number (SN)
  - The SN is a 32-bit number, which allows sending receiving nodes to keep track of data transmission. (Data ordering/missing packets)
  - The three-way handshake with SNs:
    1. A sequence number from the sending node (SENDER_SN) is put in the Sequence Number field of a `SYN` segment and is sent to the receiving node.
    2. The receiving nodes extracts the SENDER_SN from the `SYN` segment and puts SENDER_SN+1 in the Acknowledgement Number field; also the receiving nodes selects a RECEIVER_SN and puts it in the Sequence Number field of a `SYN-ACK` segment, which is sent to the sending node.
    3. The sending nodes extracts the RECEIVER_SN from the `SYN-ACK` segment and puts RECEIVER_SN+1 in the Acknowledgement Number field; also the receiving nodes puts SENDER_SN+1 in the sequence number field of a `ACK` segment, which is sent to the receiving node.

The Transport Layer

- Illustration (Three-way handshake with SN)



The Transport Layer

- TCP Ports
  - 16 bits for both source and destination ports
  - A port is a logical component of TCP connection assigned to a process requiring network connectivity
  - A port is the way a client program specifies a specific server program
  - Some important ports (to remember)
    - ✓20 and 21: FTP, 20 – data transfer, 21 – control
    - ✓25: SMTP
    - ✓53: DNS
    - ✓80: HTTP
    - ✓443: HTTPS (Secure HTTP)
    - ✓110: POP3 (Post Office Protocol 3)

The Transport Layer

- UDP
  - UDP does not need to verify whether the receiver is listening or ready to accept the packets
    - ✓ It has no handshaking dialogues
    - ✓ No guarantee of delivery, ordering and/or duplicate protection
  - Connectionless transmission
  - Unreliable but fast
    - ✓ Used in applications in which queries must be fast and only consist of a single request such as DNS, SNMP and DHCP

The Internet Layer

- Main function
  - Responsible for routing a packet (datagram) to a destination address
  - Routing is done by using an IP address
  - Connectionless transmission like UDP

The Internet Layer

- IP address basics (IPv4)
  - IP address: 4 numbers separated by decimals; each number represents 1 byte = 8 bits = 1 *octet*
    - ✓ Ex) 128.214.18.16 = 1000000.11010110.00010010.00010000 (Binary)
  - Each IP address is separated into a network address and a host address ➔ One part of the IP address represents a network prefix and the other part represents a host
    - ✓ EX) 192.168.1.231 belongs to Class C address, which uses the first three numbers to identify the network and the last number to identify the host

The Internet Layer

- IP address classes
  - Class A address – network.host.host.host
    - ✓ The first byte is reserved for the network address (network prefix) and the last three bytes are assigned to host computers
    - ✓ Range: 1.x.x.x to 126.x.x.x (127.x.x.x is reserved for loopback IP)
  - Class B address – network.network.host.host
    - ✓ The first two bytes are reserved for the network address and the last two bytes are assigned to host computers
    - ✓ Range: 128.0.x.x to 191.255.x.x
  - Class C address – network.network.network.host
    - ✓ The first three bytes are reserved for the network address and the last one byte is assigned to host computers
    - ✓ Range: 192.0.0.x to 223.255.255.x
  - Class D for multicast, Class E for R&D and study

The Internet Layer

- The number of IP addresses available for hosts
  - 2^x-2, where x is the number of bits in an octet of host
  - For example in Class C address, x =8, so the number of hosts = $2^8-2=254$
  - The reason why 2 is subtracted is that x.x.x.0 is not used and x.x.x.255 is reserved as broadcast address
  - How many IP addresses are available for hosts in Class B address? $2^{16}-2= 65534$

The Internet Layer

- Subnet mask
  - A bitmask that yields the network prefix (network address) when applied by a bitwise AND operation with any IP address in the network
  - Example
    - ✓ Network prefix of an IP address 192.168.54.3 with a subnet mask 255.255.255.0 is 192.168.54
    - ✓ An IP address 192.168.54.3 with a subnet mask 255.255.0.0 produces a network prefix 192.168 ➔ This means that to be on the same network, two machines must have IP addresses starting with 192.168

The Internet Layer

- Default gateway (First-hop router)
  - The default gateway is a router to which a host computer sends traffic if it does not know where the destination IP address
  - If a computer tries to communicate with another computer on the same network it sends the data directly to it
  - If the computer is on a separate network it forwards the data to whatever IP address is specified in the default gateway. Because a router will be attached to multiple networks it knows where these other networks are so it can route traffic to them
  - Routers also have default gateways so that if they do not know where the destination is it also sends the data onto its own default gateway.
  - This continues up the IP network hierarchy until it eventually finds a router that is part of the destination network.

The Internet Layer

- IPv6 addressing
  - Developed to increase the space of IP address (The size of IPv4 address space = 2^{32})
  - IPv6 uses 16 bytes address: The size of IPv6 address space = 2^{128}
  - Example:
    - ✓1111:0cb7:75a2:0110:1234:3a2e:1113:7777

1111 ➔ 0001 0001 0001 0001
0cb7 ➔ 0000 1100 10110111
75a2 ➔ 0111 0101 10100010
0110 ➔ 0000 0001 0001 0000
1234 ➔ 0001 0010 0011 0100
3a2e ➔ 0011 1010 0010 1110
1113 ➔ 0001 0001 0001 0011
7777 ➔ 0111 0111 0111 0111

128-bit representation of Ipv6 address

The Internet Layer

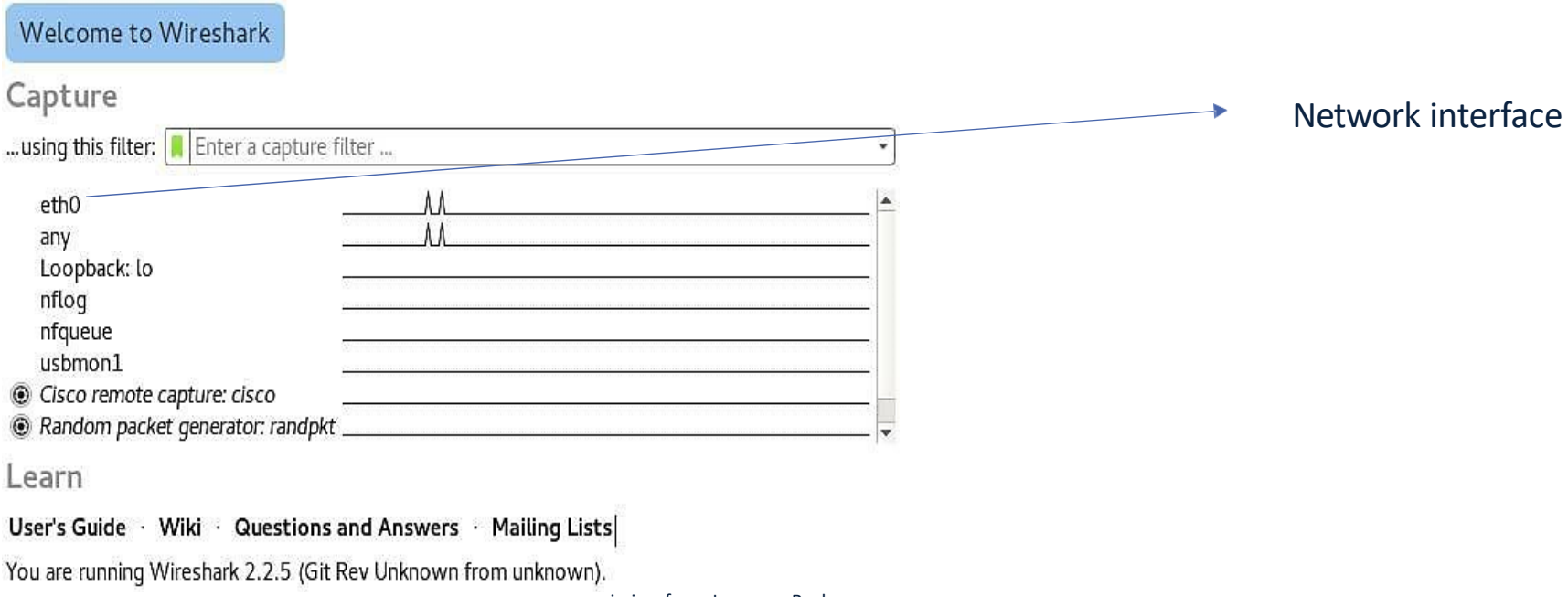
- ICMP (Internet Control Message Protocol)
  - It is used by network devices, including routers, to send error messages and operational information such as “Requested service is not available” or “Destination network unreachable”
  - It is used in the `ping` tool
    - ✓ A source sends ICMP `ECHO_REQUEST` to a destination system
    - ✓ If the system is live, it will respond by sending ICMP `ECHO_REPLY`
  - It is also used in the `traceroute` tool
    - ✓ In UNIX-like OS, `traceroute` has an option (`-I`) to use ICMP (By default, UDP is used)

Introduction to Wireshark

- Wireshark
  - A well-known network analysis tool previously known as Ethereal.
  - It captures packets in real time and displays them in human-readable format.
  - Main features include filters and color coding to analyse network traffic and inspect individual packets.

Capturing packets

- Selecting interfaces
  - After launching Wireshark, a user can select a network interface and start capturing packets on that interface.

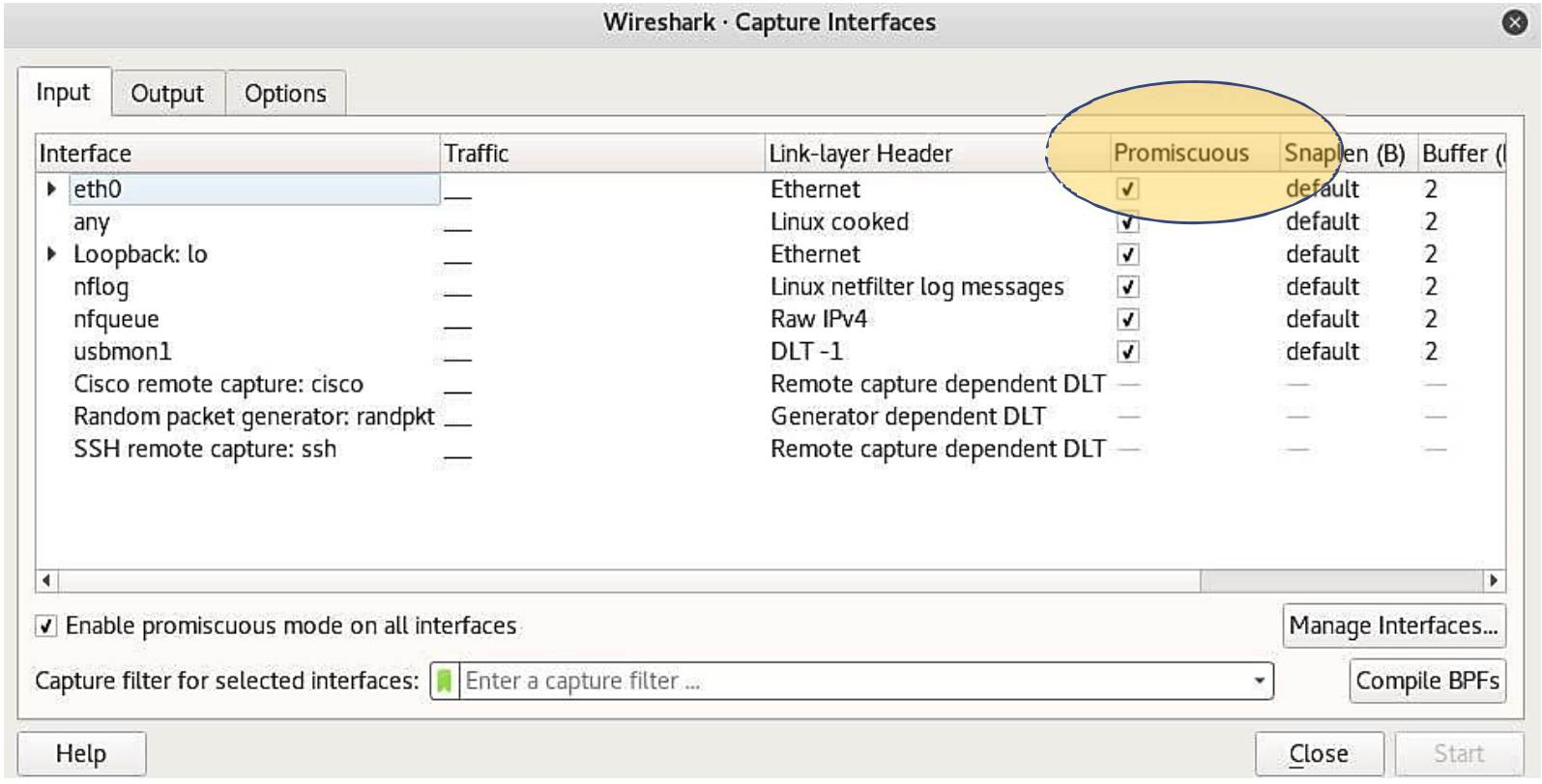


permission from Joonsang Baek

Capturing Traffic

- Promiscuous mode
  - Promiscuous mode is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the CPU.
  - This mode is normally used for packet sniffing which may take place on a router or on a computer connected to a hub or a part of a WLAN.
  - By default, Wireshark runs in promiscuous mode, but can be updated in the Capture ➔ Option panel

Capturing Traffic



UNIVERSITY
OF WOLLONGONG
IN DUBAI

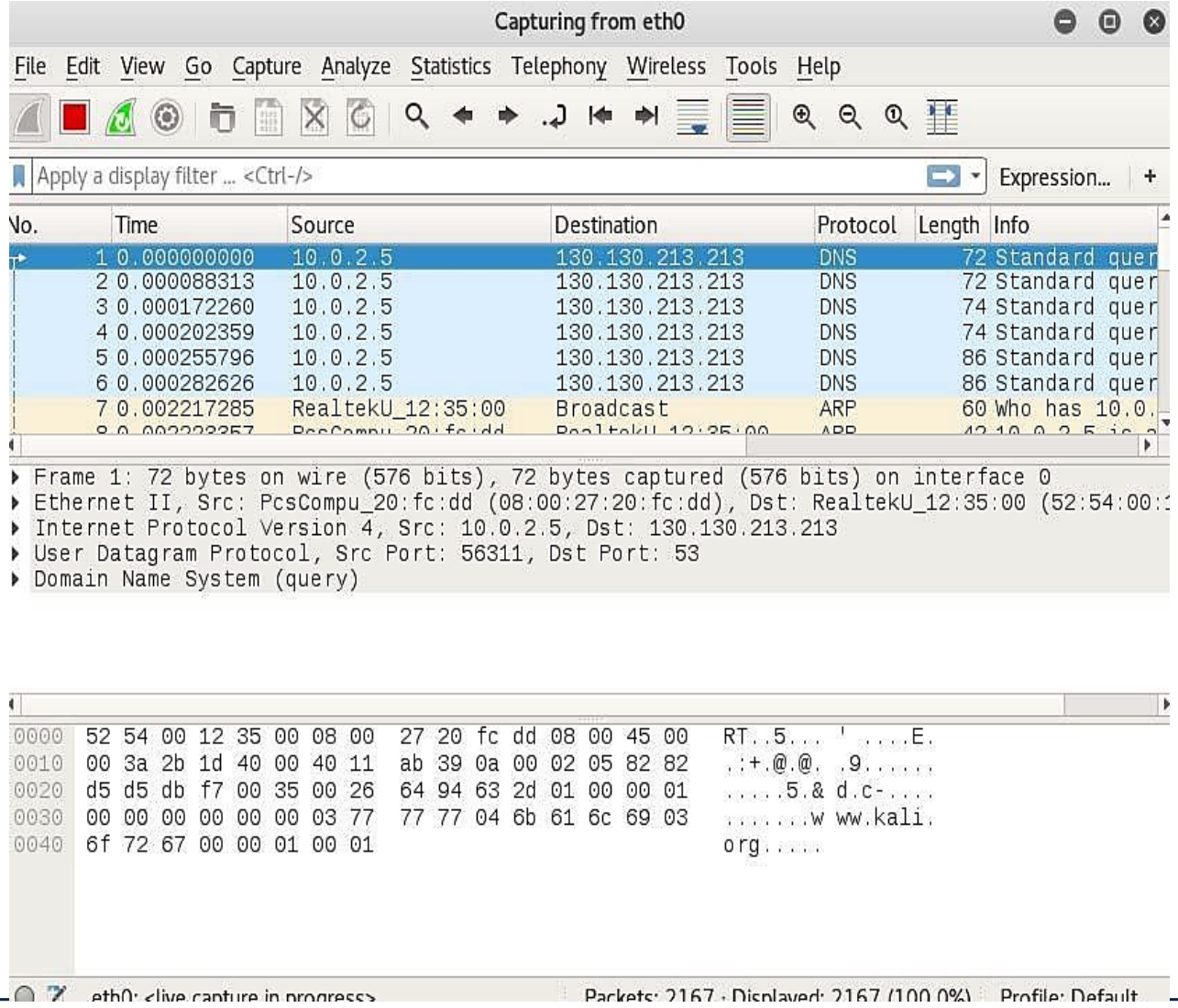
UNIVERSITY
OF WOLLONGONG
IN DUBAI

Capturing Traffic

- Packet capturing: Upon selecting a network interface, the packets start to appear in real time; Wireshark captures each packet sent to or from the system.

- In promiscuous mode, a user can see all the other packets on the network instead of only packets addressed to the user's network adapter.

Capturing Traffic



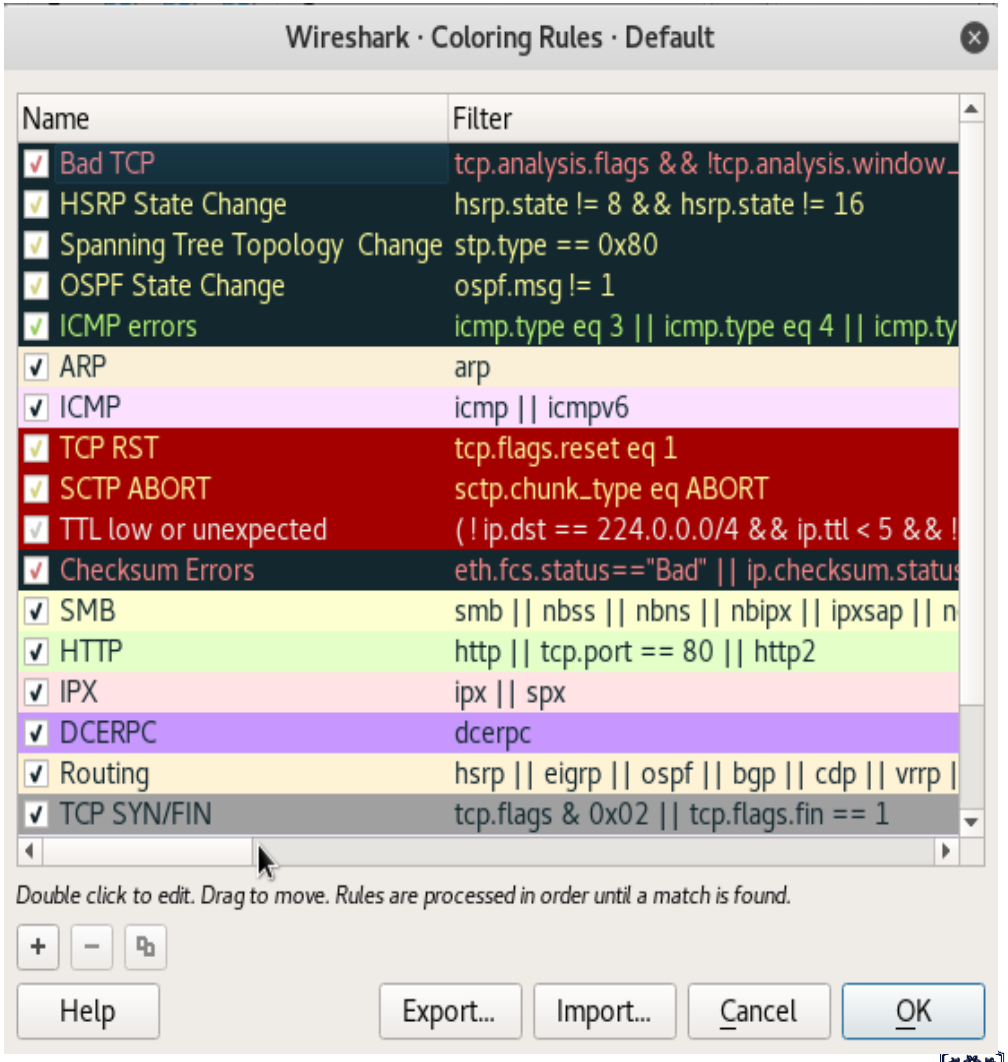
Color Coding

- Wireshark uses colors to identify the types of traffic at a glance.
- Examples (by default):
  - Light purple: TCP traffic
  - Light blue: UDP traffic
  - Black: Packets with errors
- Current (default) color setting can be seen on View

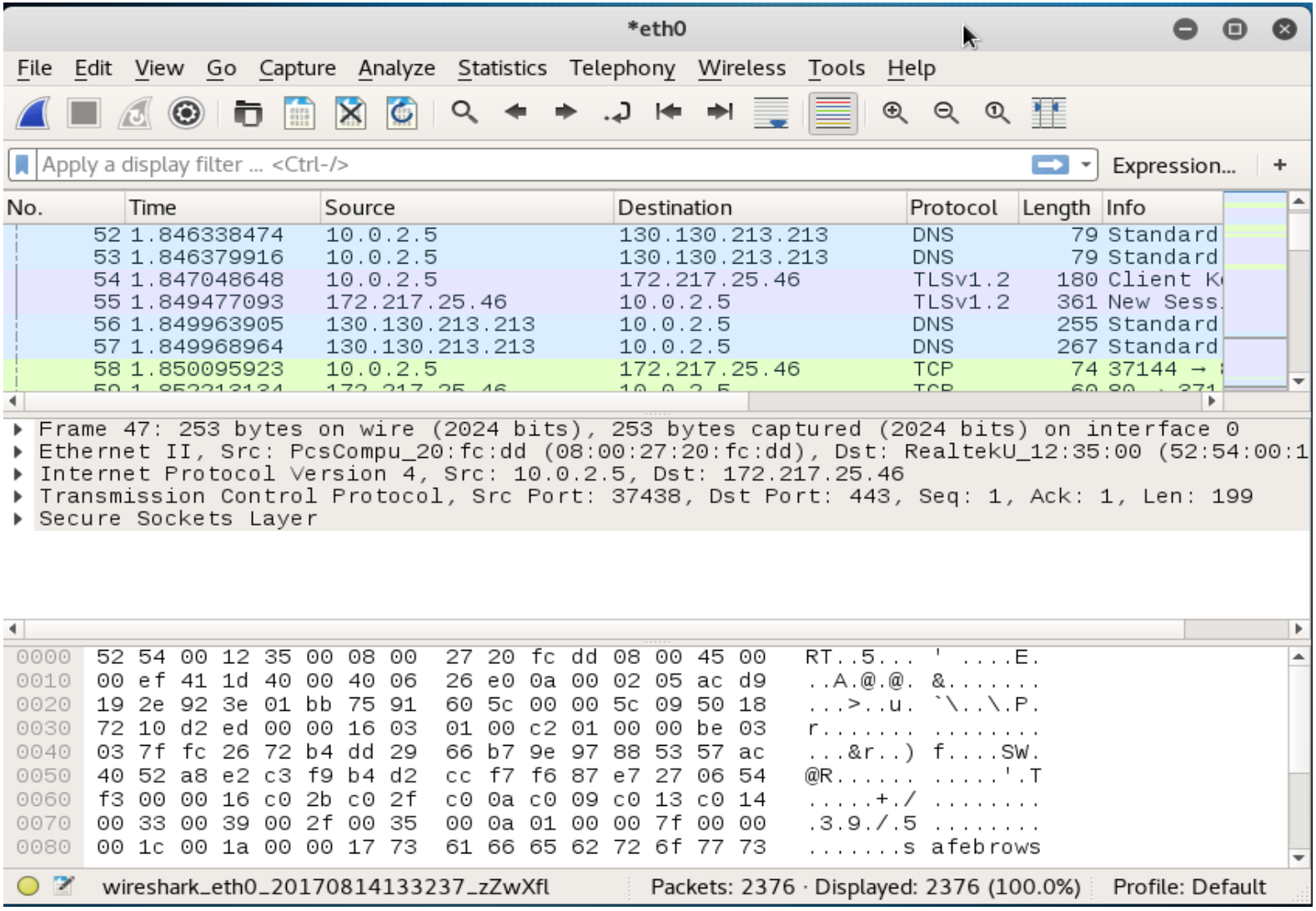
➔ Coloring Rules (Modification is possible)

Color Coding

- Default color coding rules



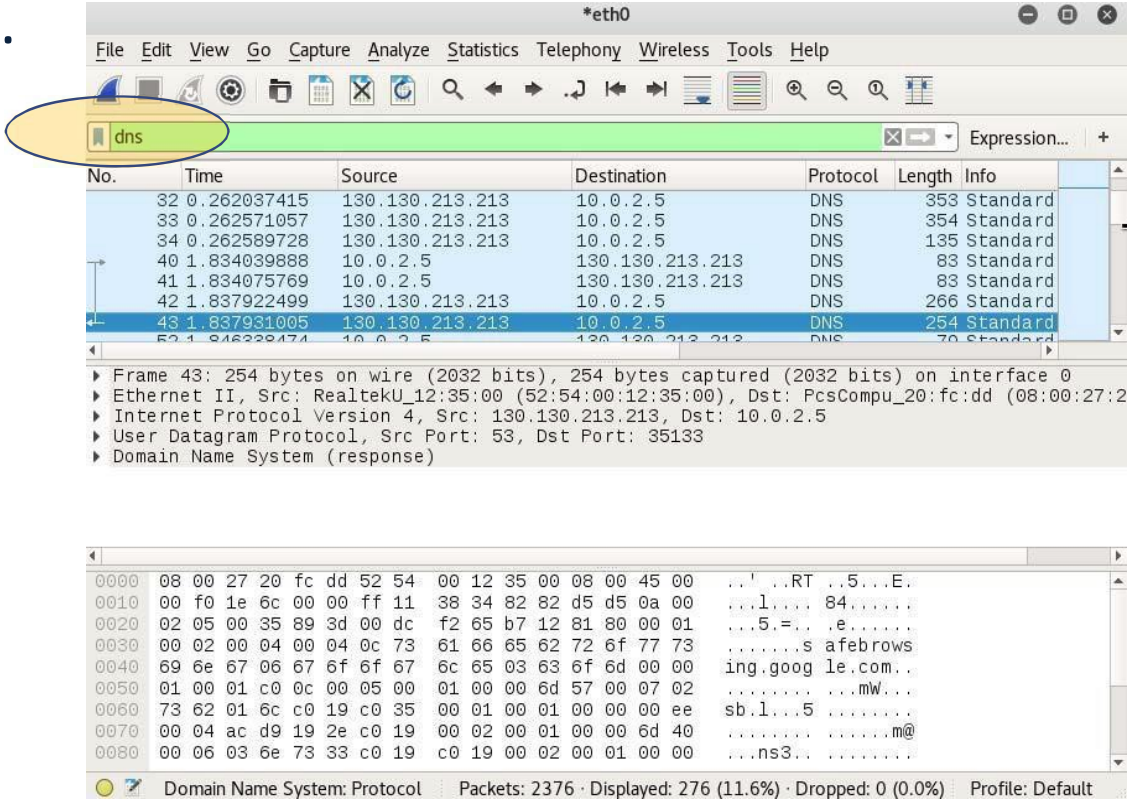
Color Coding



Packets captures by Wireshark

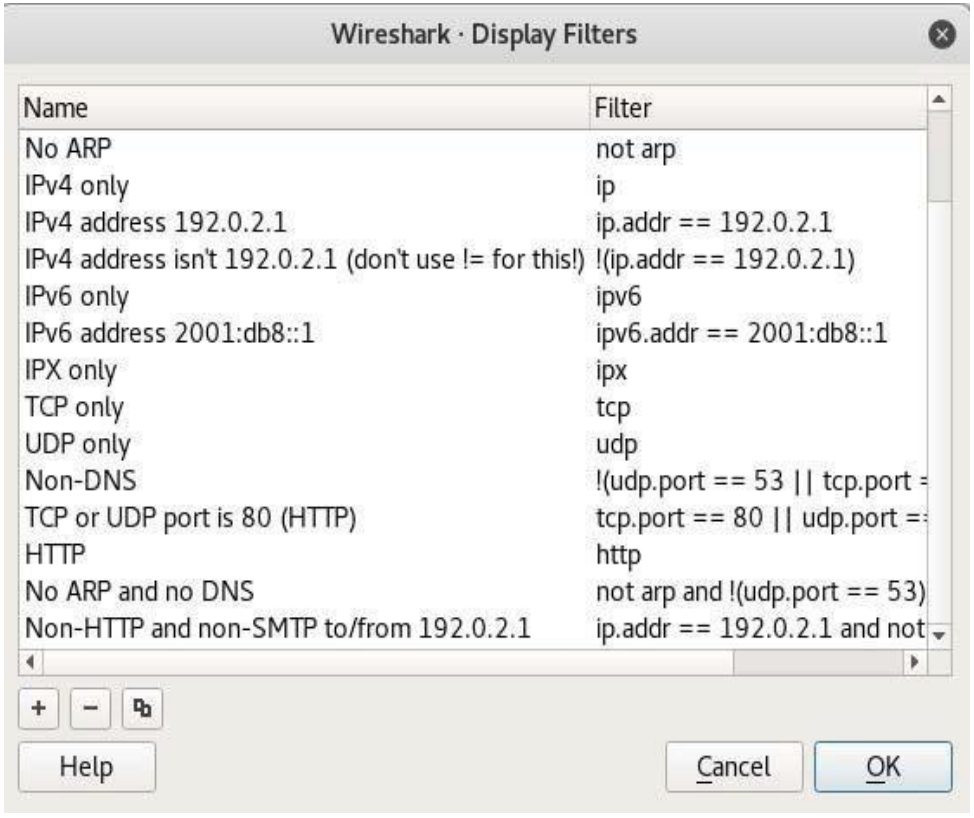
Filtering Packets

- Filter Box
  - The most basic way to filter packets in Wireshark is to enter keywords in the Filter Box.



Filtering Packets

- Default filters
  - ➢ Analyze ➔ Display Filters will list default filters included in Wireshark.

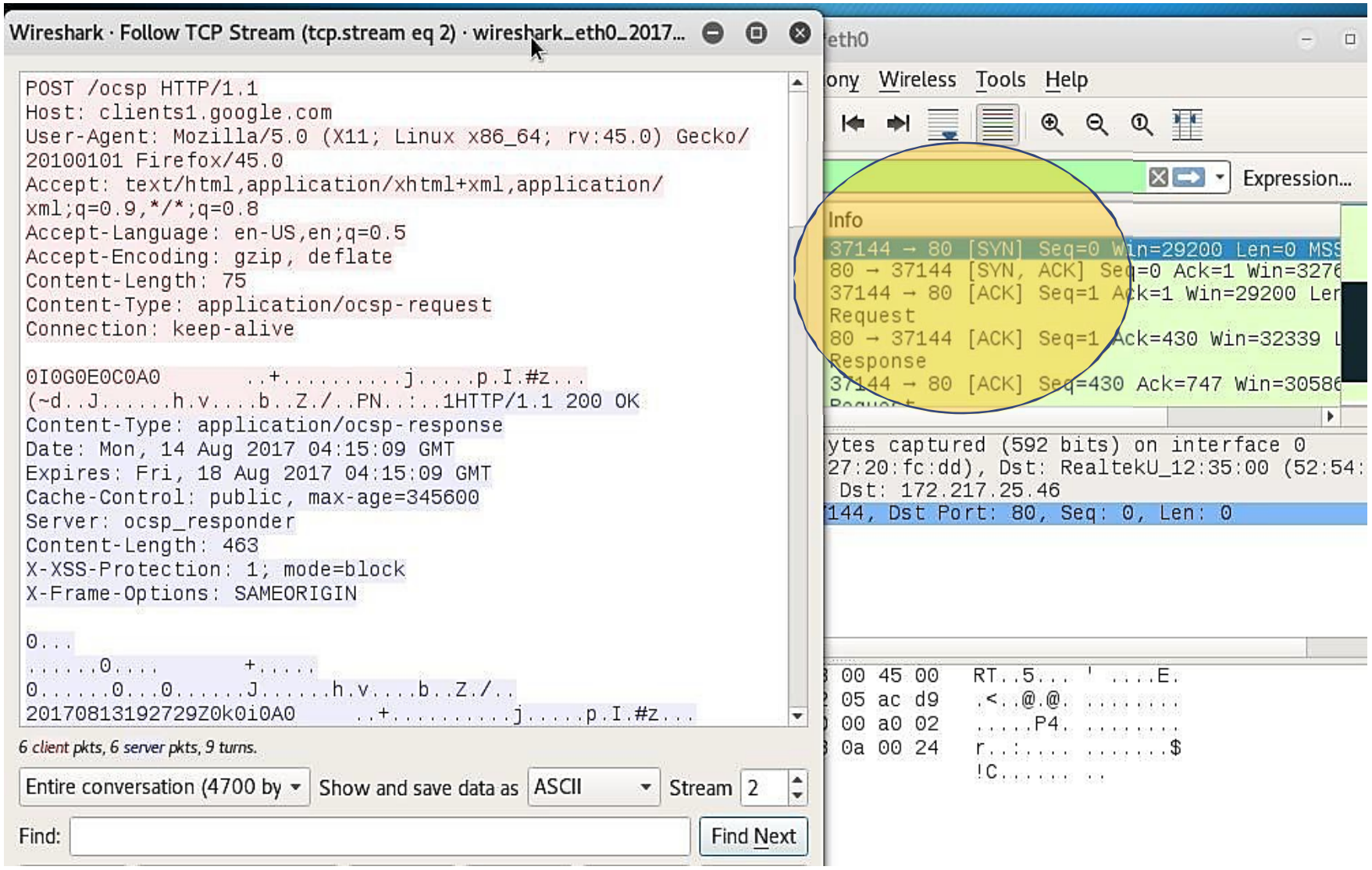


Inspecting Packets Example (1)

- Another interesting thing you can do is right-click a packet and select Follow ➔ TCP Stream.

  - ➢ You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.
  - ➢ Next slide (Screen shot)

Inspecting Packets Examples (1)



Inspecting Packets Example (2)

- In fact, Wireshark will enable us to capture a username and a password entered to an insecure website
- A filter you need in this regard is
  - `http.request.method == "POST"`
  - Once you locate a packet right-click the packet and select Follow
  - ➔ TCP Stream
  - And examine the content

Inspecting Packets Example (3)

- By using Wireshark, connections based on the secure application protocol like SSL can be analysed.

3141	36.398756	10.9.26.59	162.125.34.129	TLSv1.2	237 Client Hello
3186	36.556681	162.125.34.129	10.9.26.59	TLSv1.2	1514 Server Hello
3187	36.556682	162.125.34.129	10.9.26.59	TLSv1.2	1514 Certificate [TCP segment of a reassembled PDU]
3188	36.556684	162.125.34.129	10.9.26.59	TLSv1.2	156 Server Key Exchange, Server Hello Done
3190	36.561857	10.9.26.59	162.125.34.129	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3238	36.716422	162.125.34.129	10.9.26.59	TLSv1.2	296 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
3239	36.719132	10.9.26.59	162.125.34.129	TLSv1.2	473 Application Data

An example of connection based on SSL

Any Questions?

Let’s do the activity using Wireshark for capturing and analyzing network packet logs ☺