Introduction to Networks and Wireshark

Bootcamp 101 Day 1

Why do people sit in the corner when it is cold?
-Victoria

Cybersecurity

Where Are we?

Networking is critical for nearly all these roles. A solid understanding of networking is fundamental to almost all cybersecurity.

Security Analyst	Security Operations Center Analyst (SOC)	Security Engineer	Systems Engineer
Cyber Threat Analyst	Cyber Defense Analyst	Incident Response Analyst	Intelligence Analyst
Information Assurance Technician	Risk Analyst	Forensics Investigator	Systems Administrator
Network Engineer	It Auditor	Application Security Engineer	Penetration Tester
Information Analyst	Systems Security Analyst	IT Specialist	Web Engineer - Application Security

Today’s Objectives

By the end of class, you will be able to:

- ☐ Define basic networking terms and explain how data is transmitted over the network.
- ☐ Describe how protocols structure and define the data transmitted over the network.
- ☐ Outline the OSI Model and explain each layer.
- ☐ Compare and contrast the OSI and TCP/UDP model.
- ☐ Capture communication over the network using Wireshark.
- ☐ Explain the basics of a packet in Wireshark.

Introduction to Networking

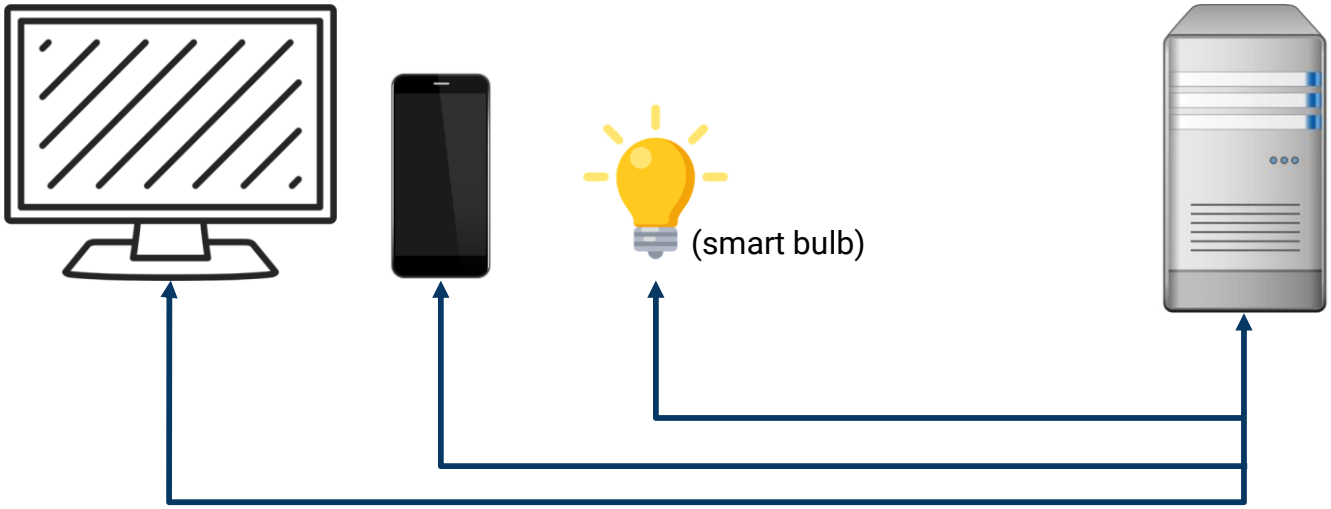
A network is a group of computer systems and computing devices that are linked together through communication channels to facilitate communication and resource sharing among a wide range of users.

Network Communication: The Client Server Model

Network communication occurs largely between **clients** and **servers**.

Network Communication: The Client Server Model

Multiple clients often communicate with a single server.



The Journey of a File

Client / Server Model

A lot of this seems like magic!

1. The Client sends a request for info to the server.

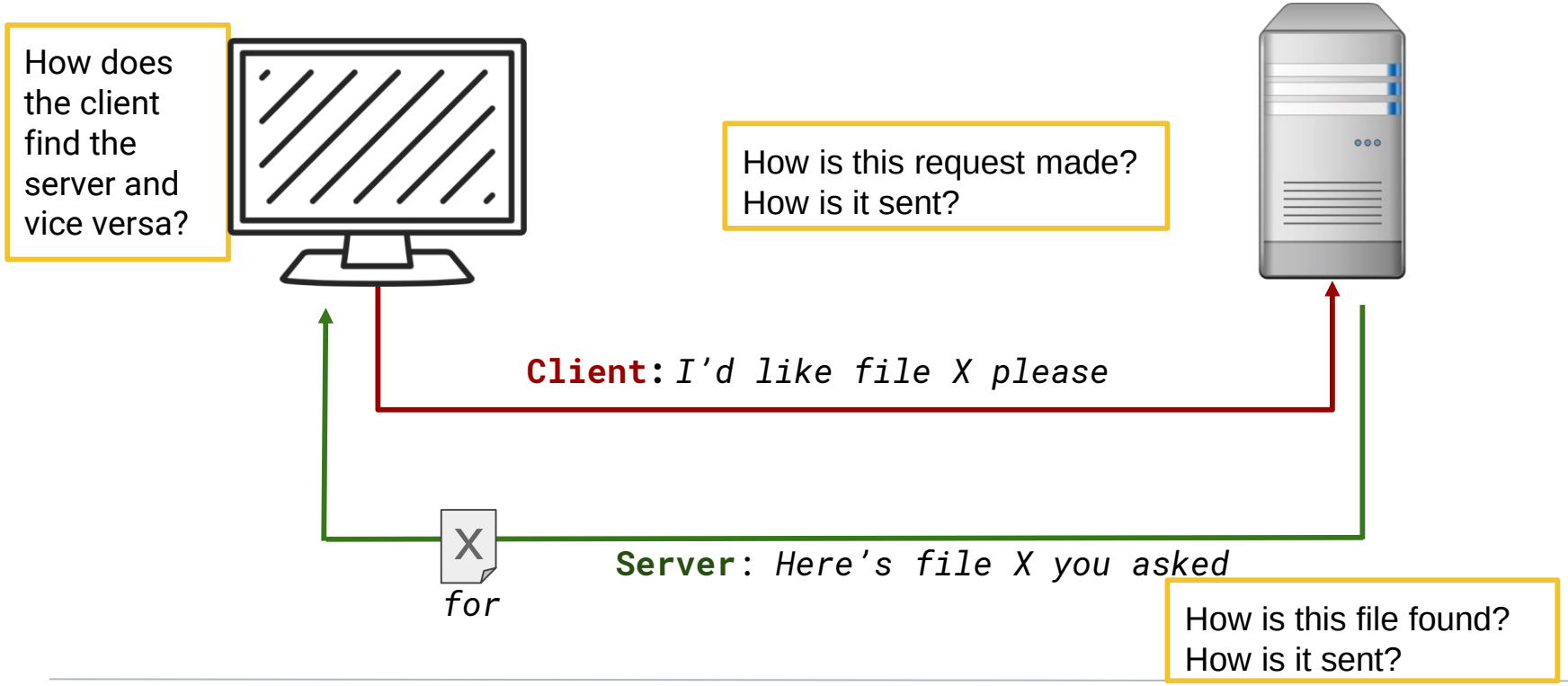
Client: *I'd like file X please*

2. The server responds with dat

Server: *Here's file X you asked for*

Client / Server Model

But there's a lot to learn about this "*simple*" process:



Activity: Explaining Communication

In this activity, you will pair up and think about how some common tasks might fit into the client / server framework.

Suggested Time:
10 Minutes

Activity: Explaining Communication

Instructions:

With a partner, investigate and explain how each of the following might work in communicating over the network:

- ☐ File Transfer
- ☐ Email
- ☐ Web Page

For each scenario, think about and try to explain each of the following:

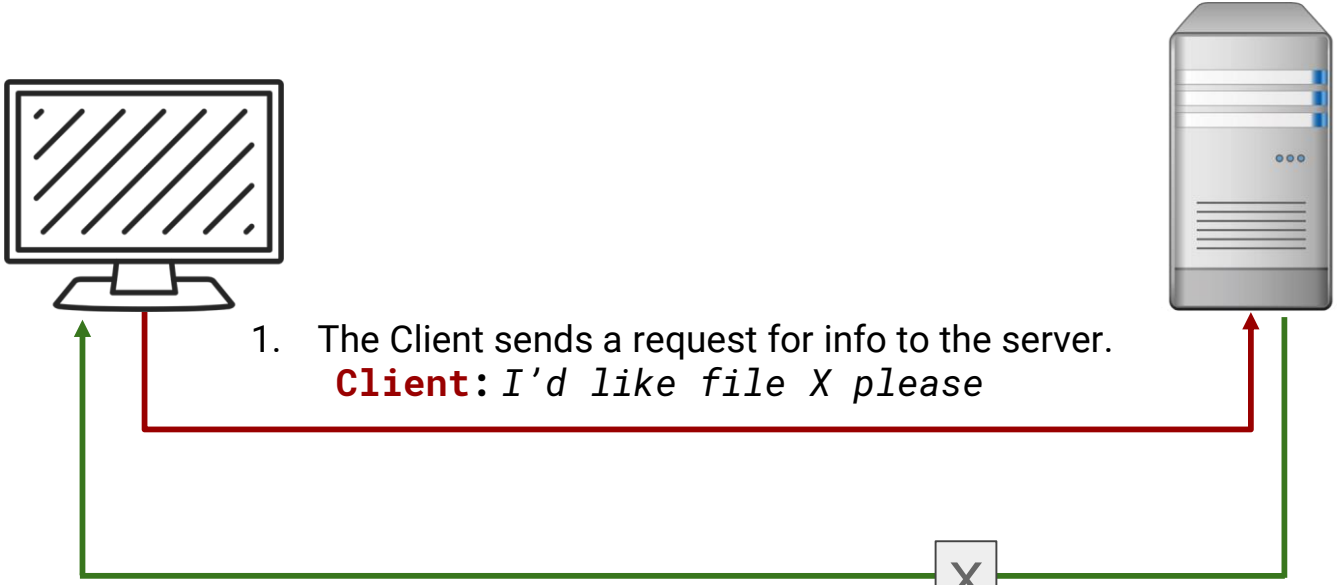
- ☐ Who is the client? The server?
- ☐ What does the request look like? The response?
- ☐ What work does the client do? The server?
- ☐ What is being communicated?

Use Google to help you in your investigation!

10 Minutes

Explaining Communication Review

File Transfer:



1. The Client sends a request for info to the server.
   Client: *I'd like file X please*

2. The server responds with dat
   Server: *Here's file X you asked for*

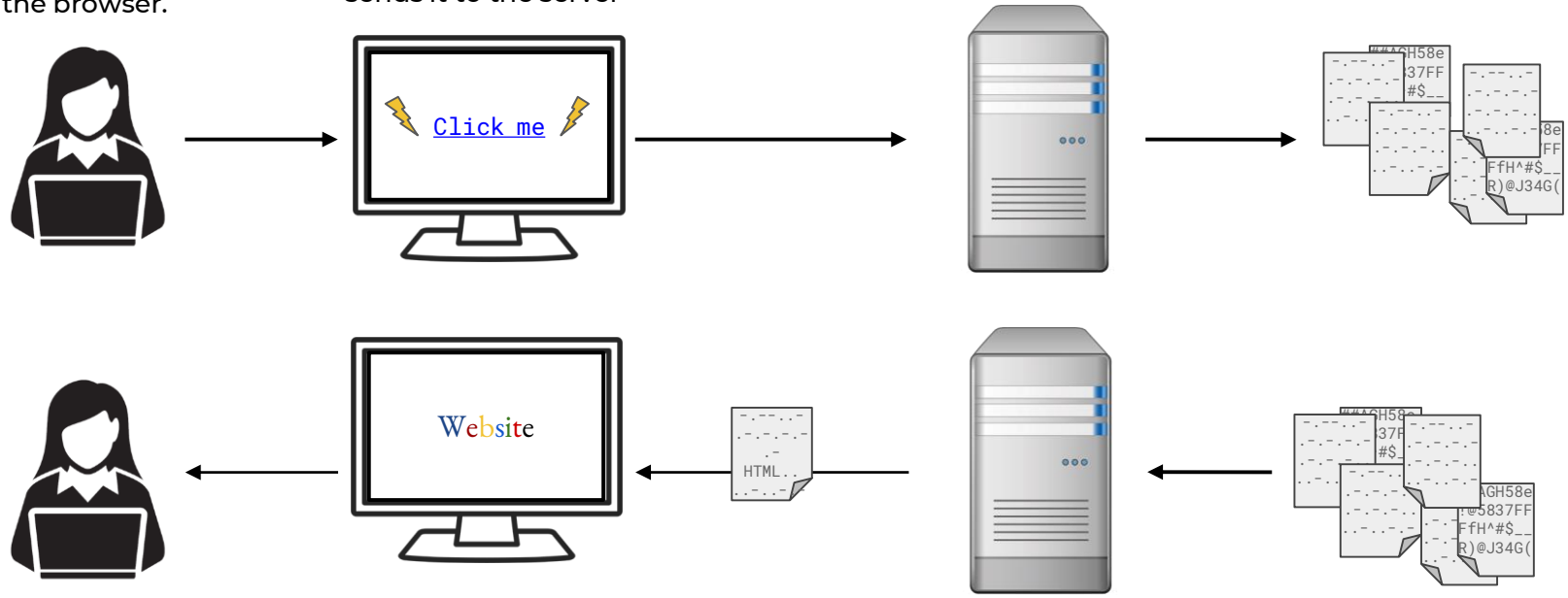
Explaining Communication Review

Web Pages:

User selects a link in the browser.

Browser formats the request and sends it to the server

Server finds the requested web pages.

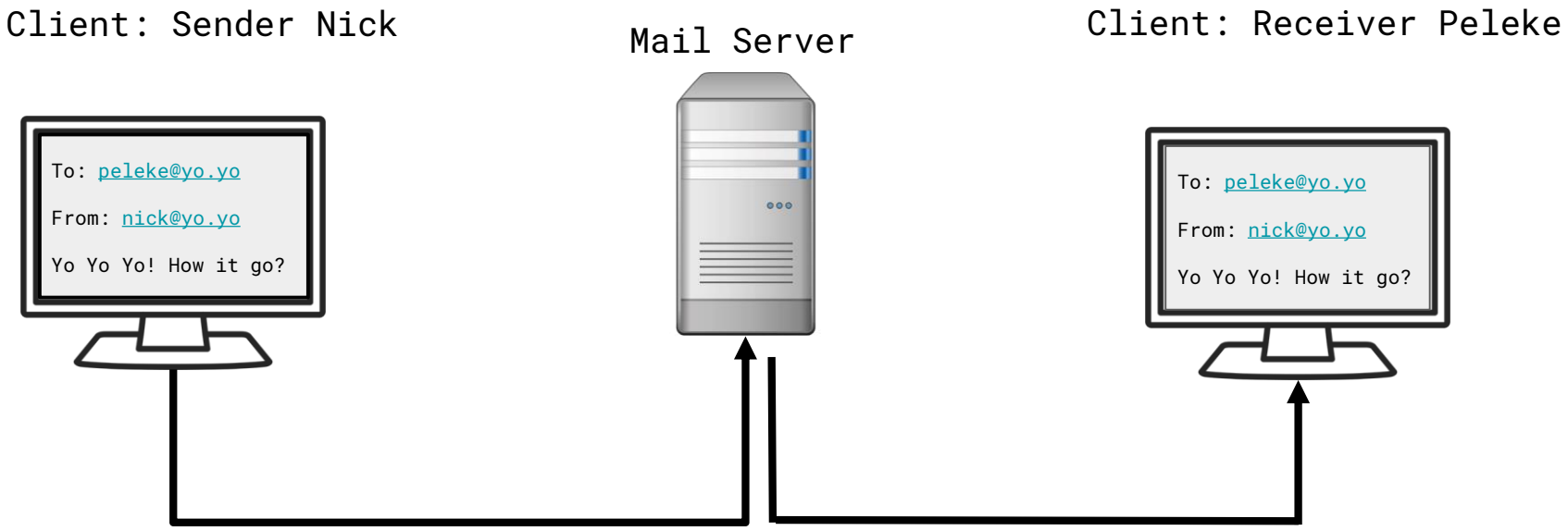


Browser receives HTML and renders it into a user display

Server formats the response and sends it to the client (browser).

Explaining Communication Review

Email:

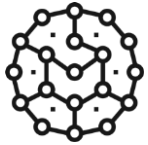


For some communication, there may be more than one server behind the scenes doing work.

Explaining Communication Review

Networking Definitions

Network: A system of computers and other devices (printers, smart objects) that are connected to each other.



Network Communication: Transmission of data between two or more computers over a network.

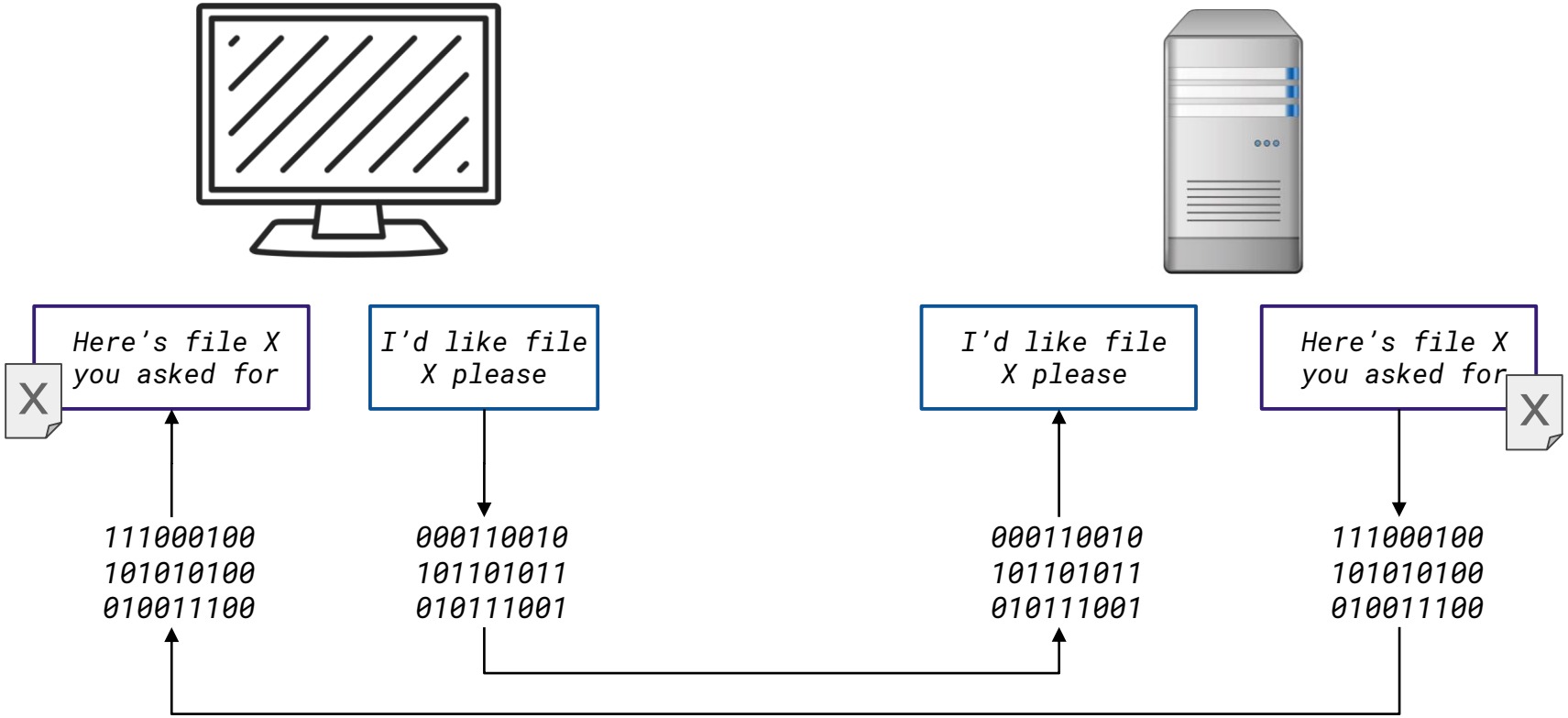
Client / Server: Multiple end devices (clients) communicating over a network with a single central computer (server)

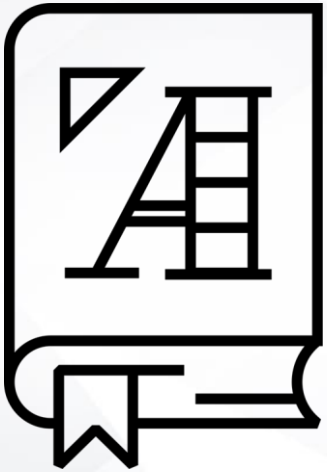
Request / Response: A basic method of computer communication, in which one computer sends a request for data to a second computer that responds to that request.

Introduction to Protocols

Request/Response and Binary

All digital data is transmitted via binary.



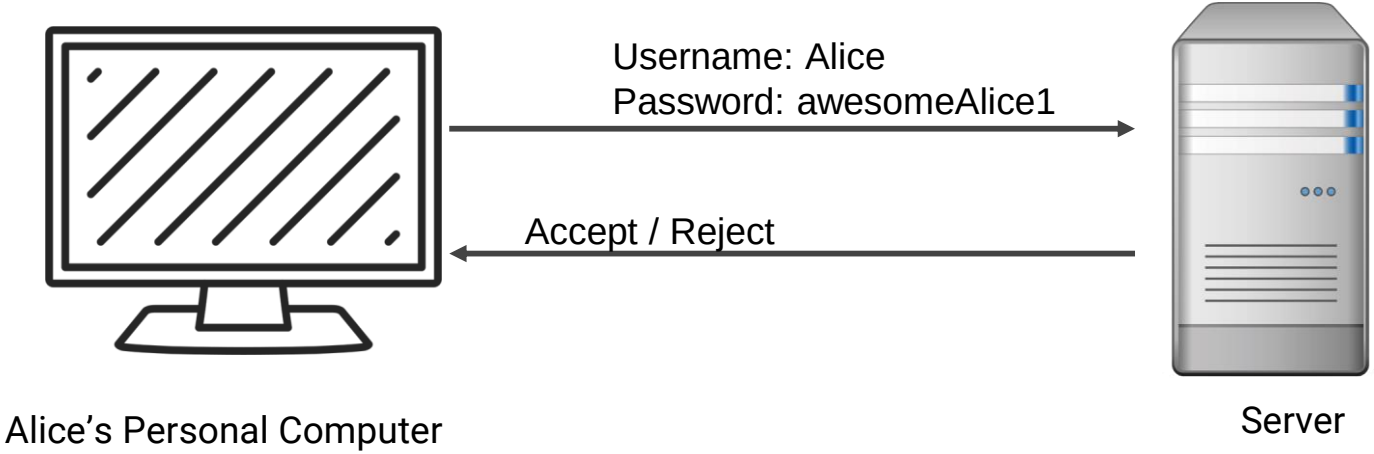


A Protocol is a set of standardized rules that specify how interactions between communicating entities should work.

How networks communicate and provide structure to the binary data that is transmitted.

Protocol Example: Authentication

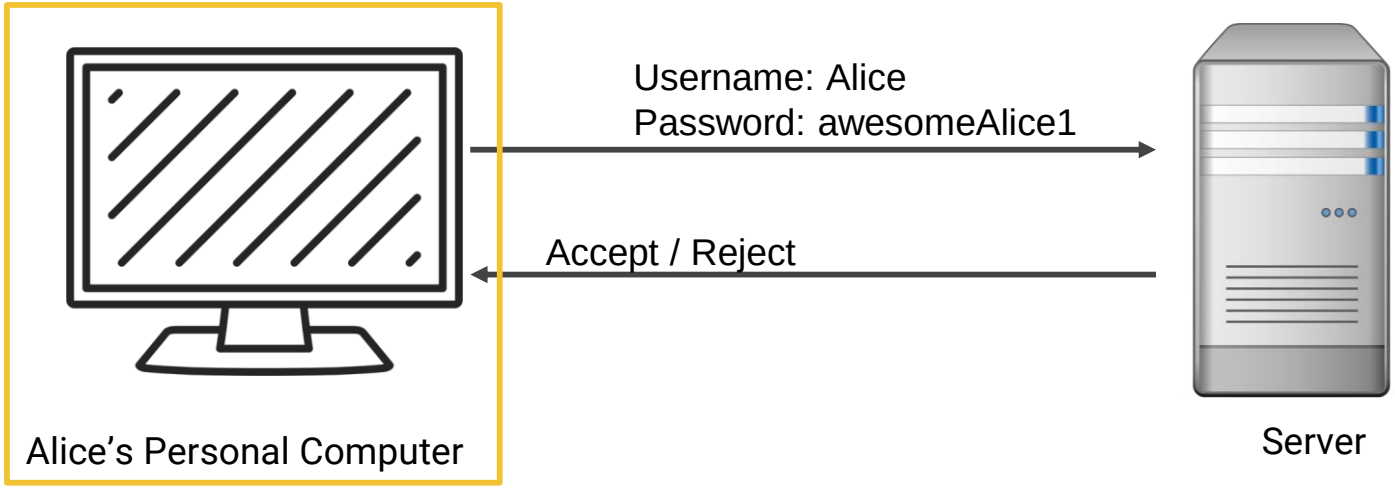
PAP: Password Authentication Protocol



PAP Two-Way Handshake

Protocol Example: Authentication

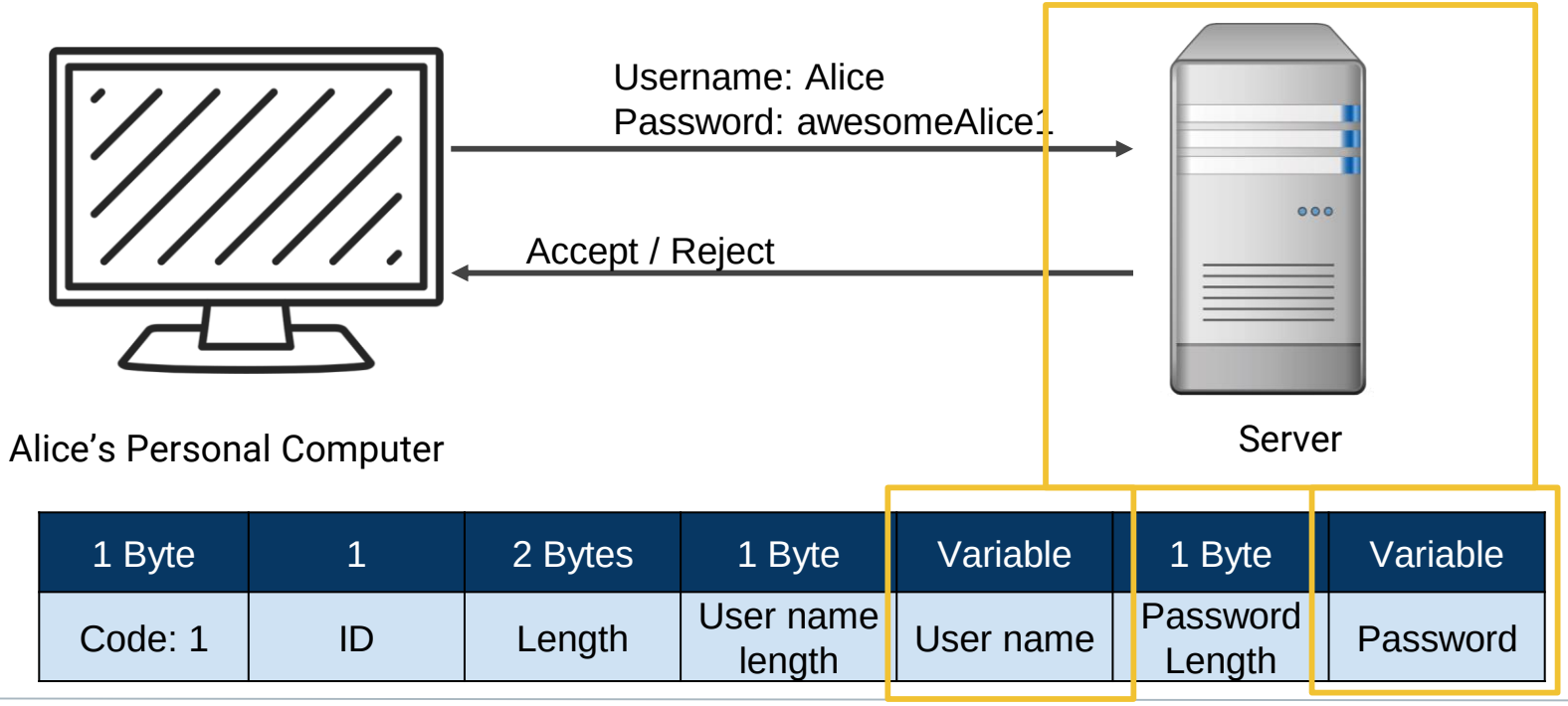
Client request contains bits in a specific order and length, per the standard and rules of the protocol.



1 Byte	1	2 Bytes	1 Byte	Variable	1 Byte	Variable
Code: 1	ID	Length	User name length	User name	Password Length	Password

Protocol Example: Authentication

The server receiving the request will know where to look in the bitstream for content: the username and password.



Ports

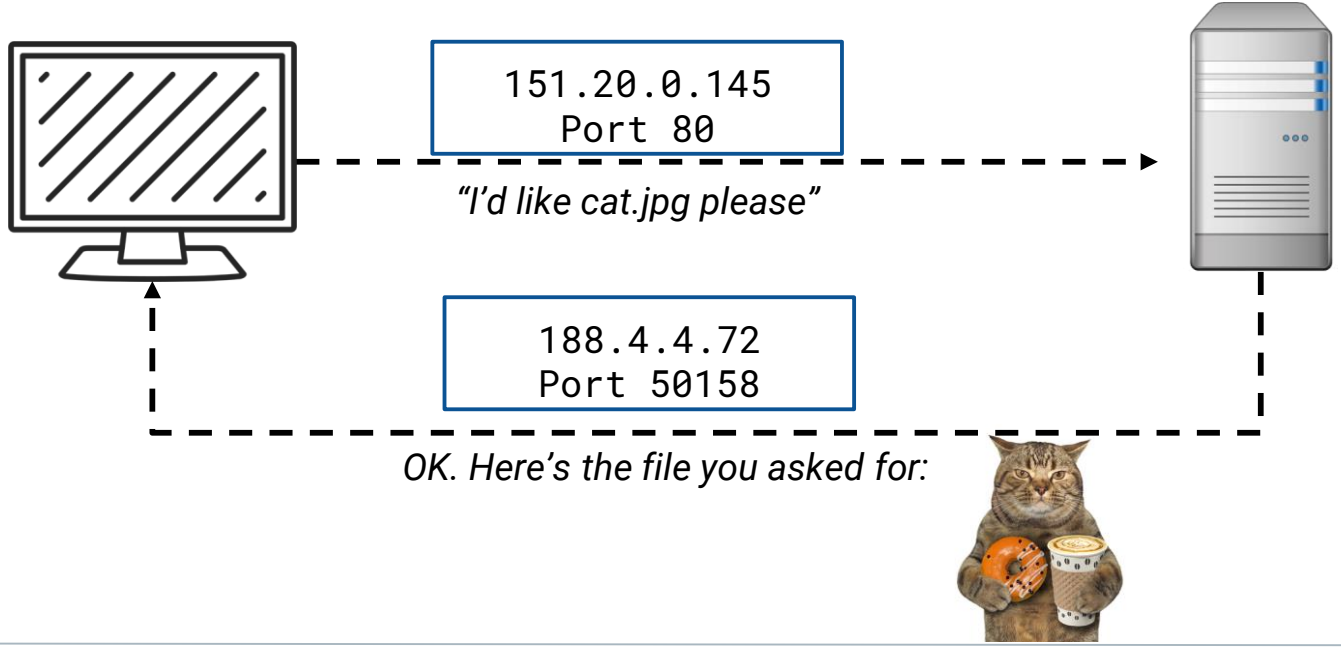
Ports are access points used by data that is packaged and interpreted by protocols.

```
0 - 1023: System Ports

1024 - 49151: Registered Ports

49152 - 65536: Dynamic / Private Ports
```

Source / Destination Ports

Source Port: Randomly generated from unregistered port range

Destination Port: Dependent on the protocol



Activity: Ports and Protocols

In this activity, you will identify the correct port number and functions for a given list of protocols.

Activities/02_Stu_Ports/ReadMe.md

Suggested Time:

Times Up! Let’s Review.

Ports and Protocols

Today’s Objectives: Checkpoint

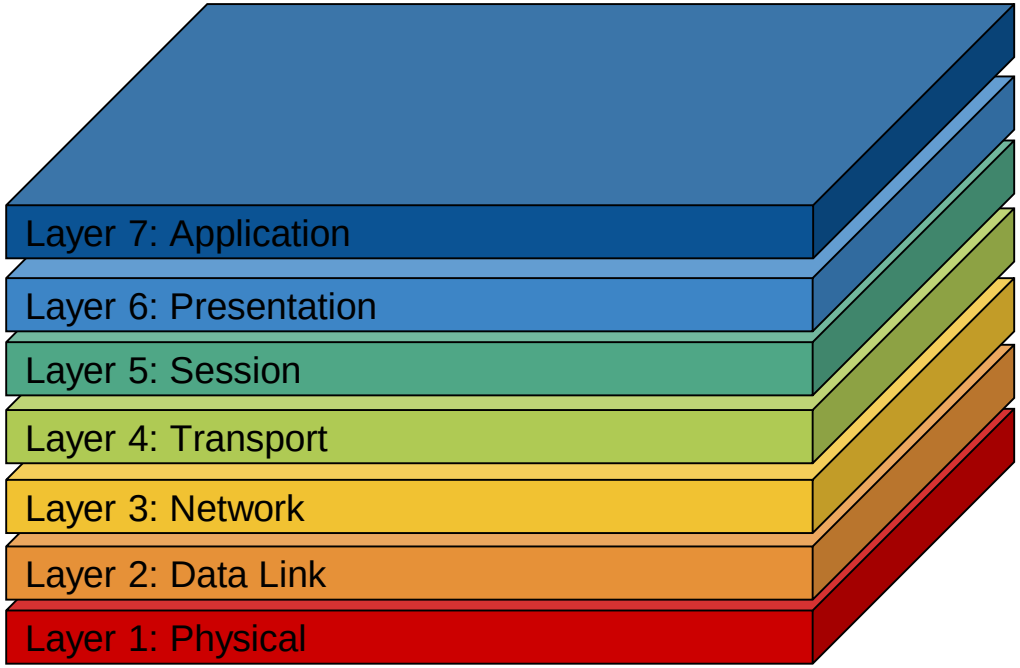
By the end of class, you will be able to:

- [x] Define basic networking terms and explain how data is transmitted over the network.
- [x] Describe how protocols structure and define the data transmitted over the network.
- [ ] Define the OSI Model and explain each layer.
- [ ] Compare and contrast the OSI and TCP/UDP model.
- [ ] Capture communication over the network using Wireshark.
- [ ] Explain the basics of a packet in Wireshark.

The OSI Model

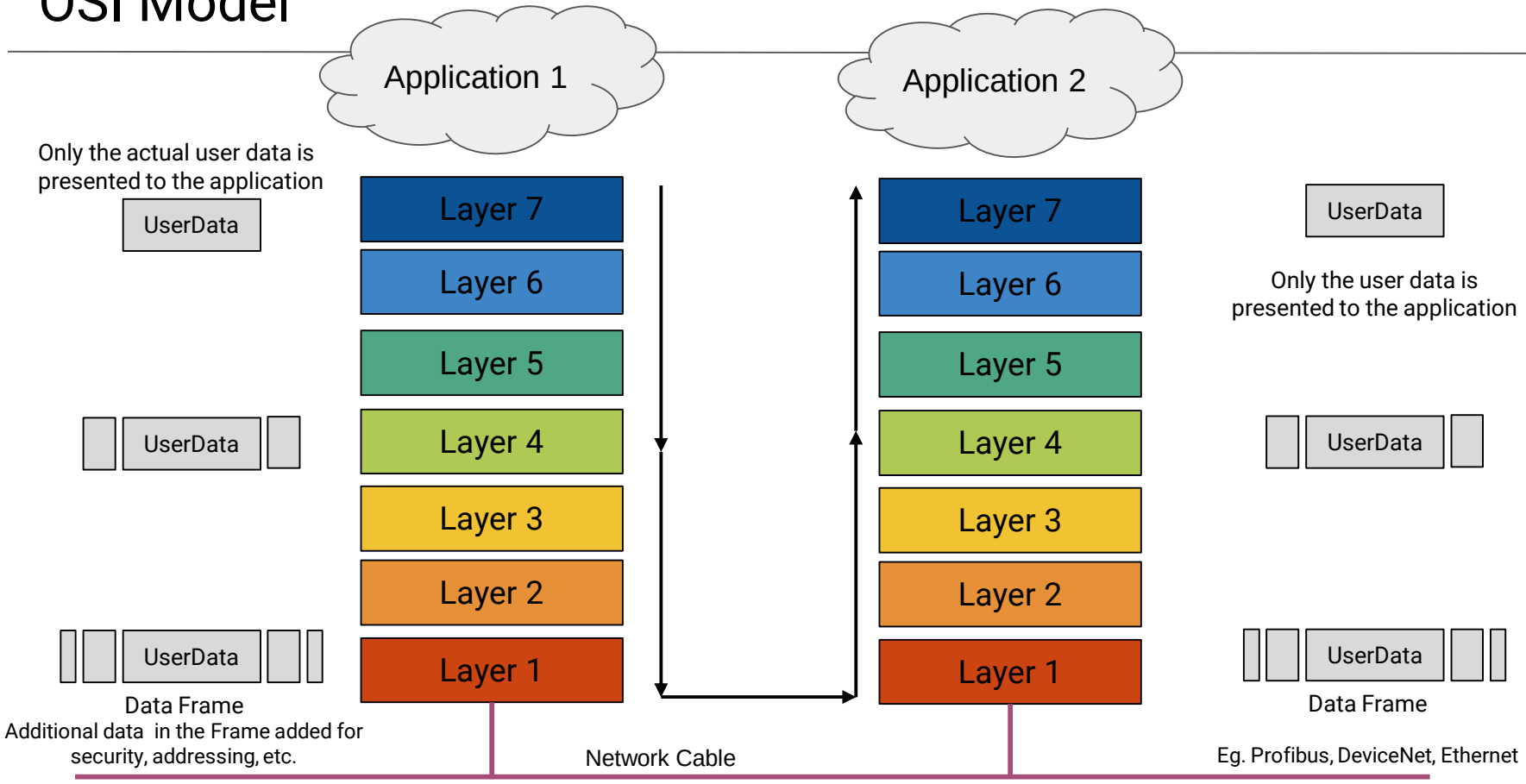
The Open Systems Interconnection (OSI) Model

The OSI Model provides a framework to better categorize and conceptualize the overwhelming volume of ports and protocols.

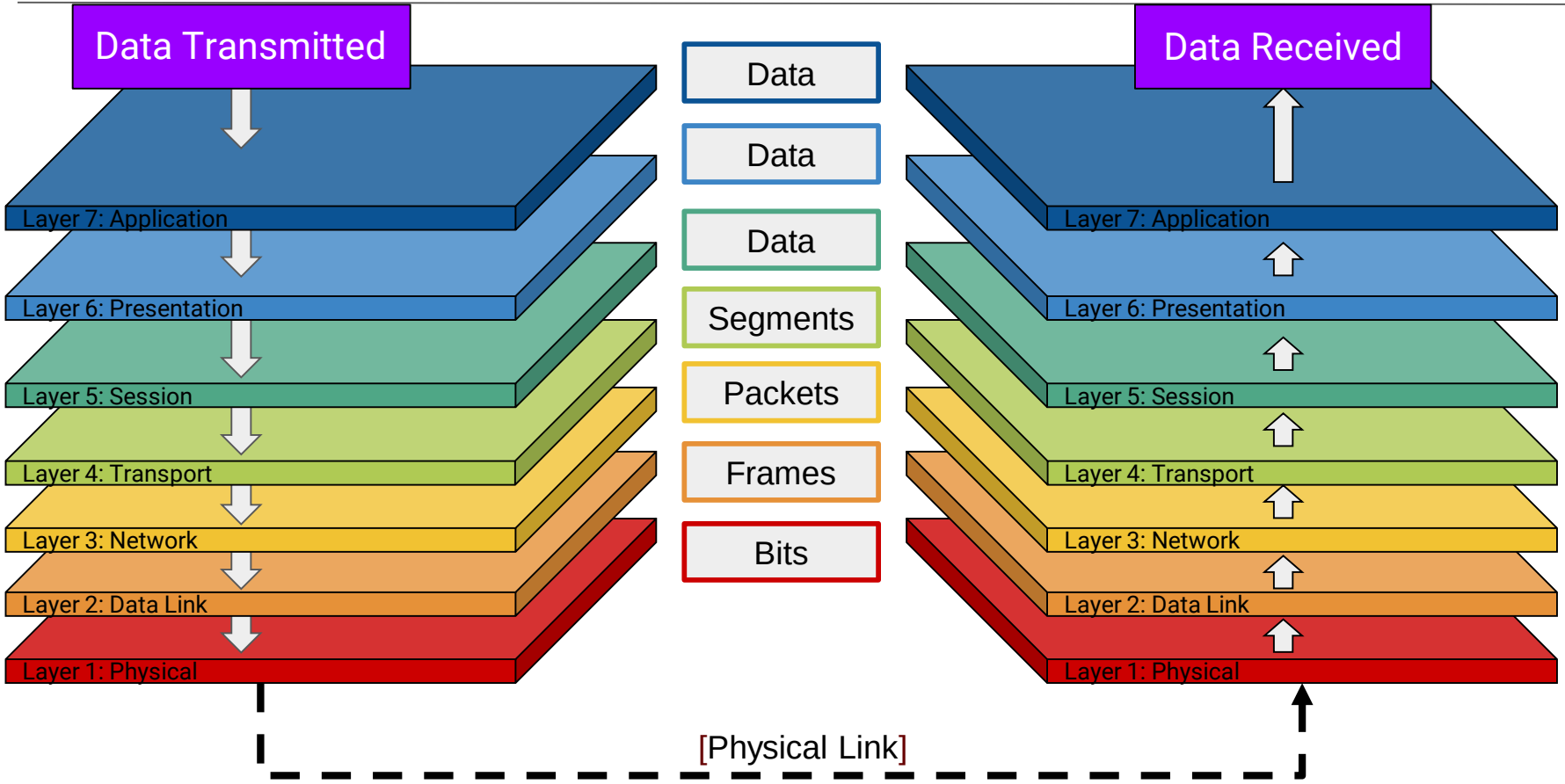


The OSI Model depicts the travel of communication through 7 layers, slowly growing the data frame to incorporate aspects like protocol information, security measures, and other pertinent information.

OSI Model

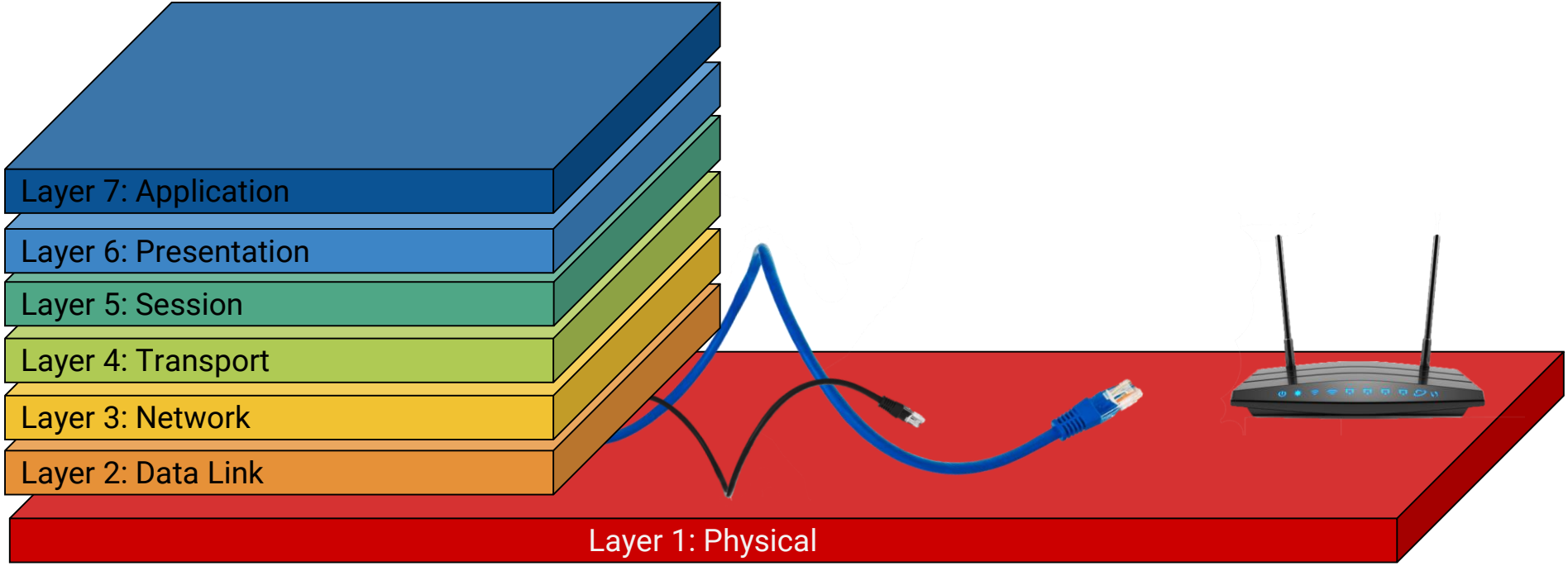

Application 1
Application 2
Only the actual user data is presented to the application
UserData
Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1
UserData
UserData
Data Frame
Additional data in the Frame added for security, addressing, etc.
Network Cable
Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1
UserData
Only the user data is presented to the application
UserData
UserData
Data Frame
Eg. Profibus, DeviceNet, Ethernet

OSI Model


Data Transmitted
Data Received
Layer 7: Application
Layer 6: Presentation
Layer 5: Session
Layer 4: Transport
Layer 3: Network
Layer 2: Data Link
Layer 1: Physical
Data
Data
Data
Segments
Packets
Frames
Bits
[Physical Link]

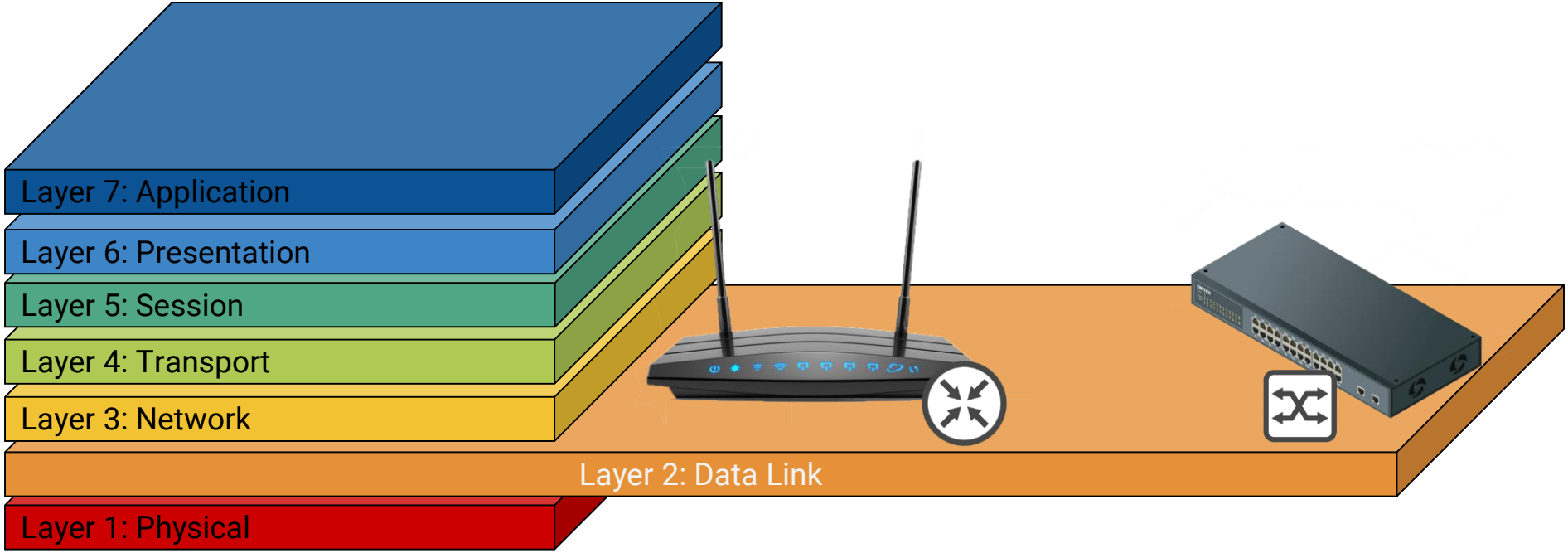
The OSI Model: Physical Layer

The Physical Layer is responsible for transmission of binary data via a physical medium. Handles how data is physically encoded and decoded.



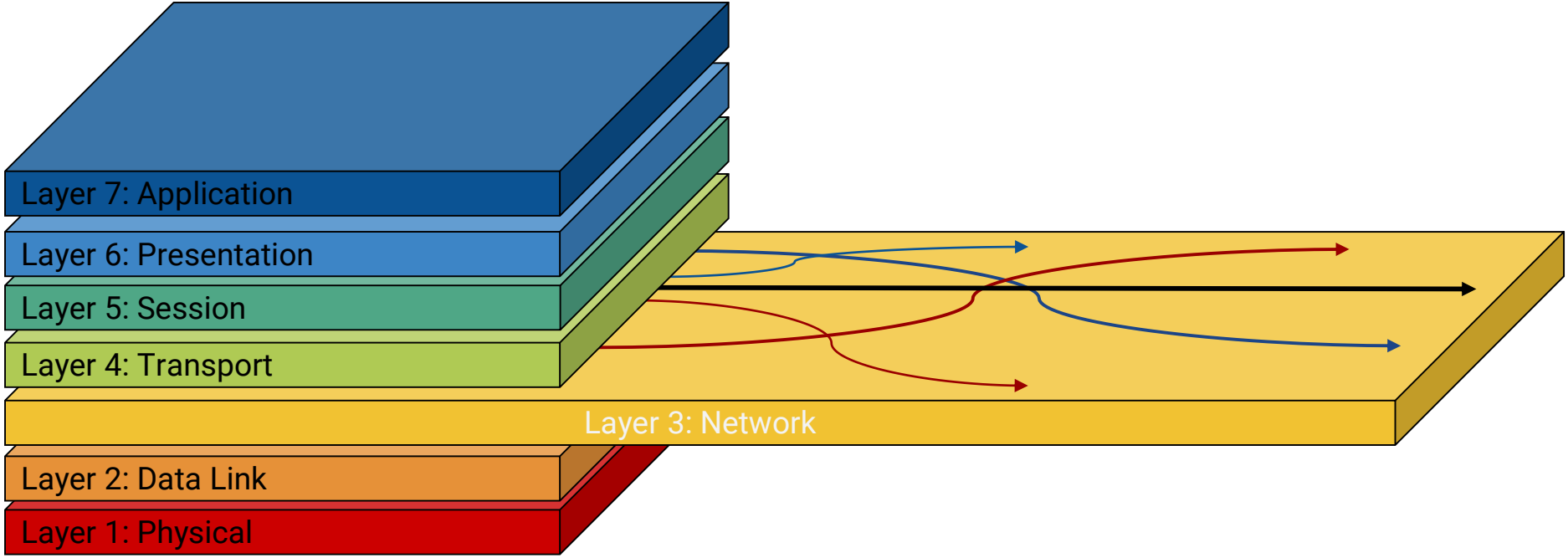
The OSI Model: Data Link

The Data Link layer establishes links between nodes and provides error-free handling of data transfer over the Physical layer.



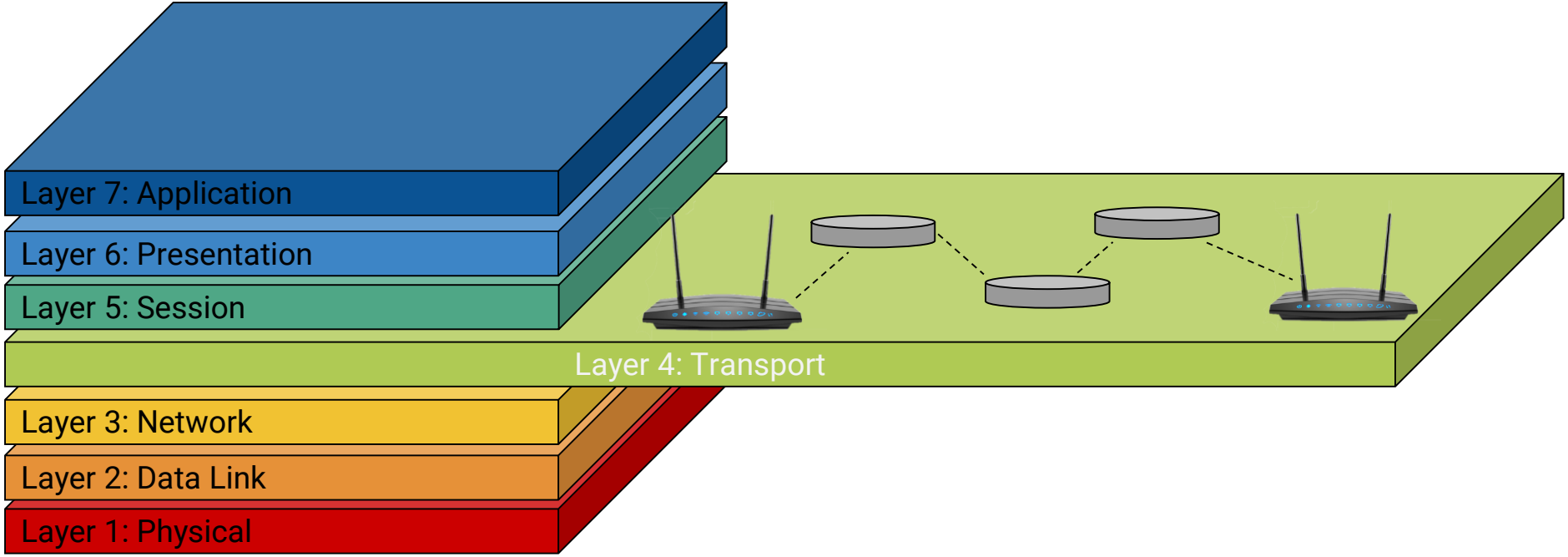
The OSI Model: Network Layer

The Network layer is responsible for routing data through physical networks, deciding which physical path the data will take, and ensure that it gets to the correct destination.



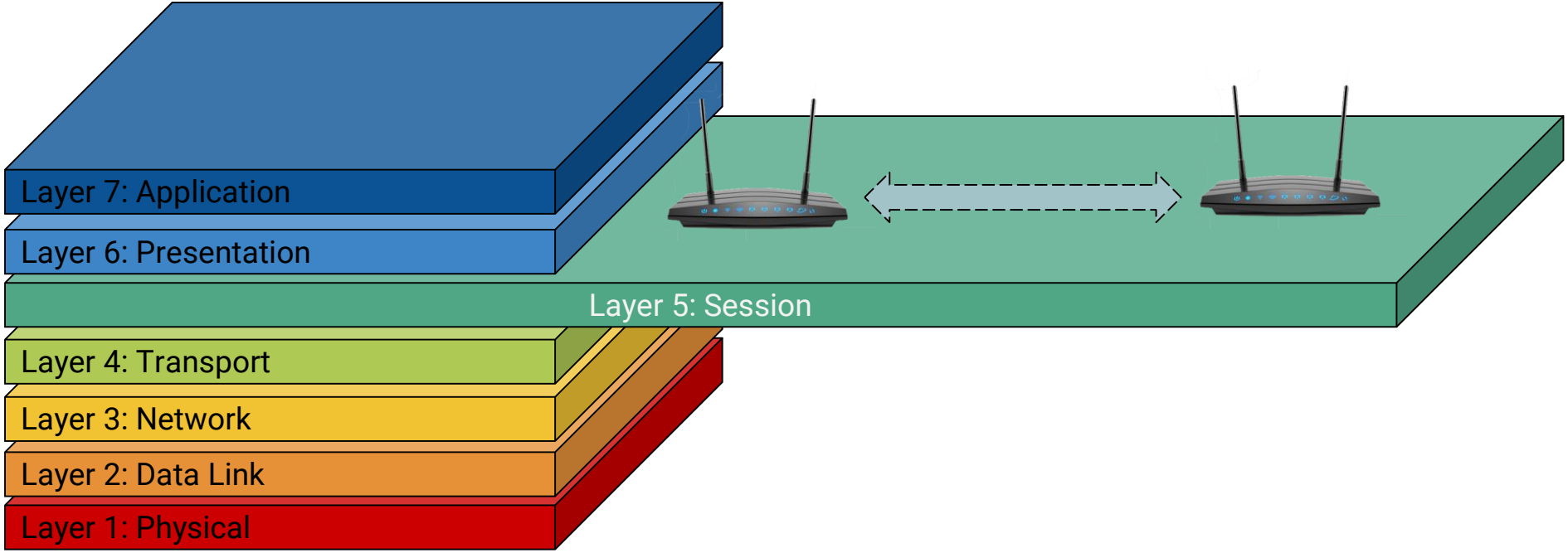
The OSI Model: Transport

The Transport Layer is responsible for actually transmitting data across the network. (It puts data onto the network.)



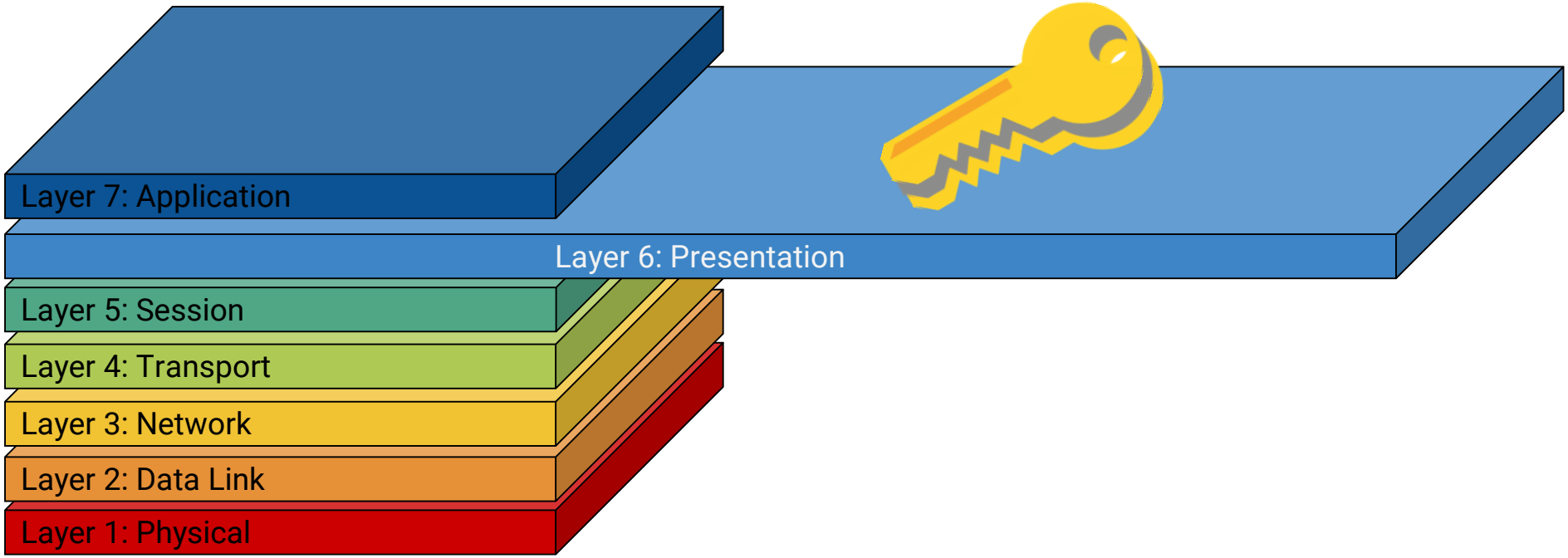
The OSI Model: Session Layer

The Session Layer manages connections between ports on computers and handles data flow.



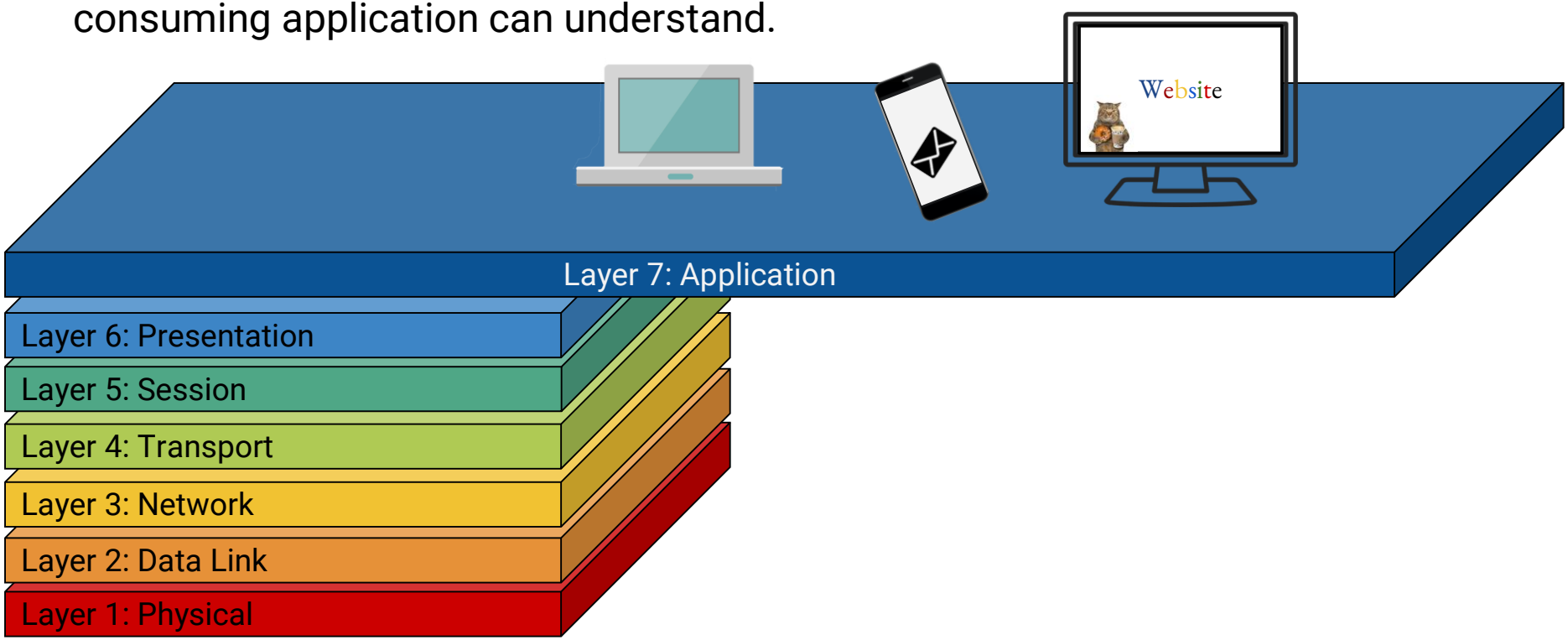
The OSI Model: Presentation Layer

The Presentation layer is the translator for the network. It formats the data to be presented to the Application layer. Handles data representation, de/encryption, character set translation and conversion.



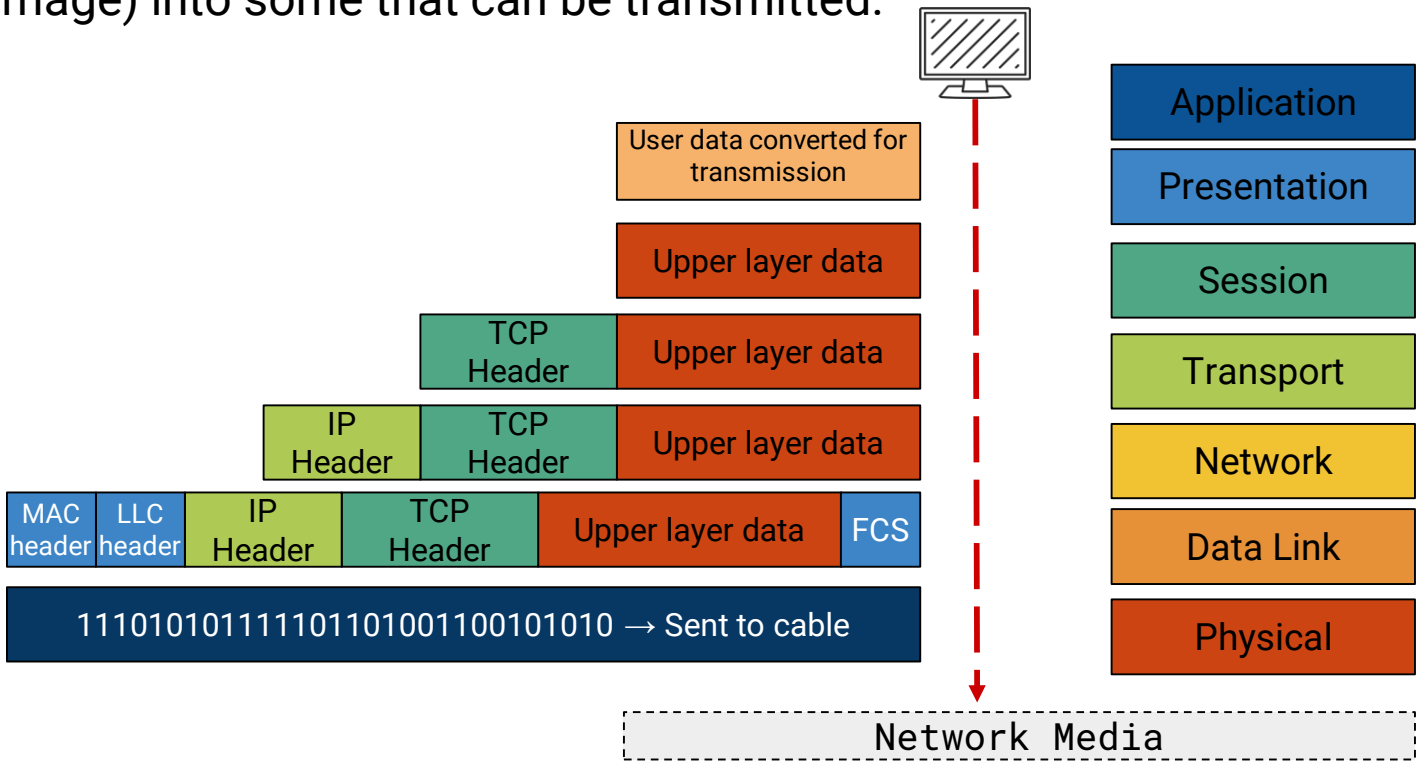
The OSI Model: Application Layer

The Application Layer is responsible for representing data in a way the consuming application can understand.



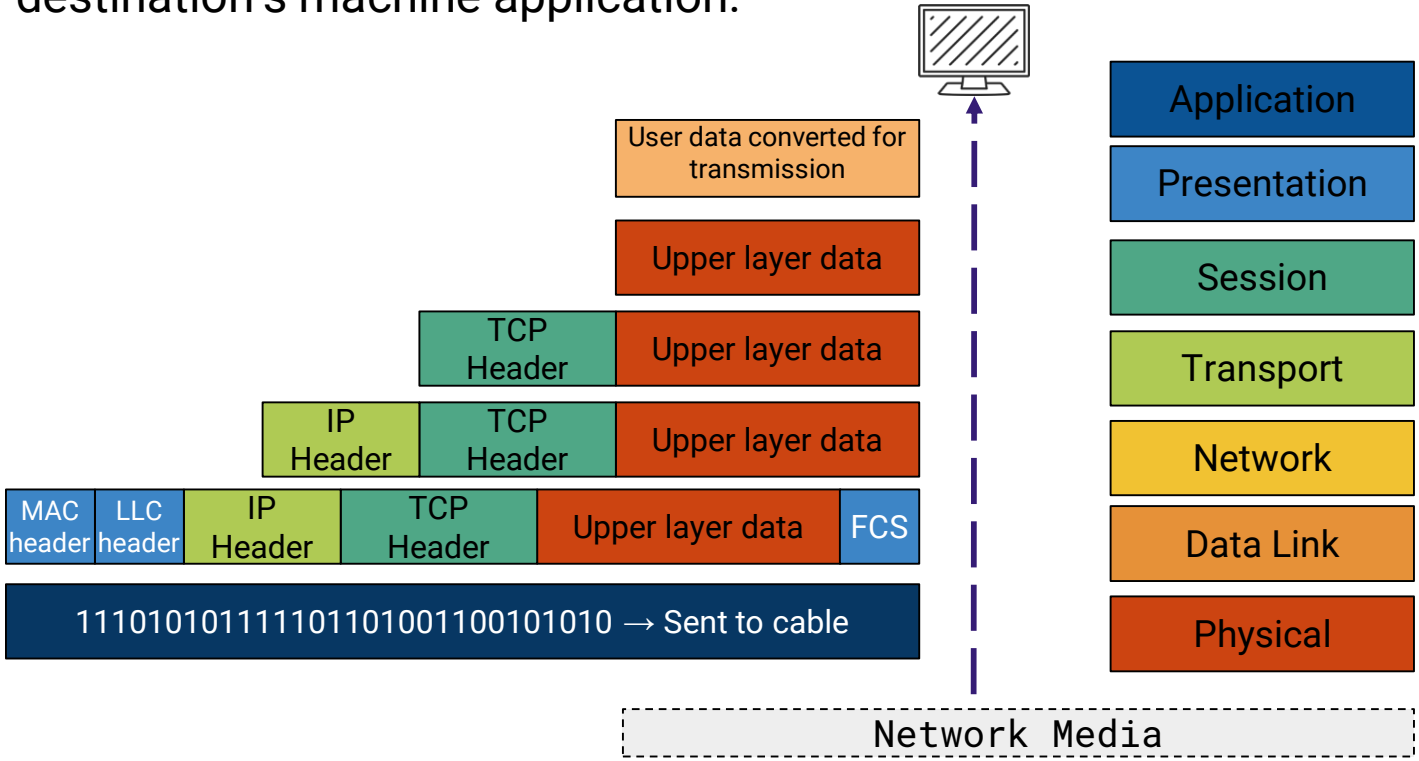
Encapsulation / Decapsulation

Encapsulation converts data from an application on the source machine (like an image) into some that can be transmitted.



Encapsulation / Decapsulation

Decapsulation converts transmitted data into something that can be used on the destination's machine application.



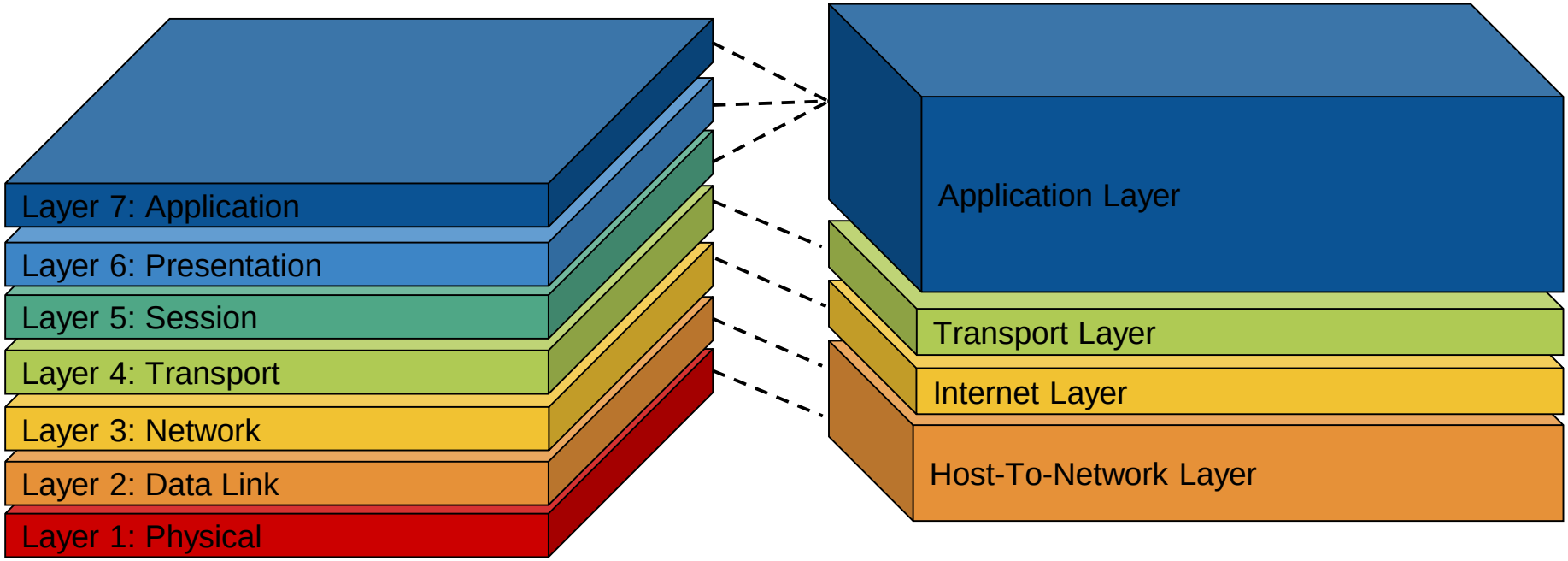
OSI Model

Twitter OSI Model

- **Physical Layer:** You just thought of a tweet that you *need* to share with the world, so you whip out your smartphone.
- **Data Link Layer:** Your 280 character tweet is converted into binary 1s and 0s.
- **Network Layer:** Your tweet is routed over various LAN and WANs. (Directing your tweet's travel path).
- **Transport Layer:** Packs up your 280 character tweet and sends it into the Twittershpere.
- **Session Layer:** Provides order to a session. Like the traffic cop of data between transfers.
- **Presentation Layer:** Translates binary 1s and 0s into a comprehensible format.
- **Application Layer:** Your tweet is ready to be viewed by the world!

TCP / IP Model

The Transmission Control Protocol / Internet Potocol Model is another model, more in accordance with cybersecurity issues.



Activity: Fill in the Blanks

In this activity, you will practice familiarizing yourself with the OSI model.

Suggested Time:
10 Minutes

Times Up! Let’s Review.

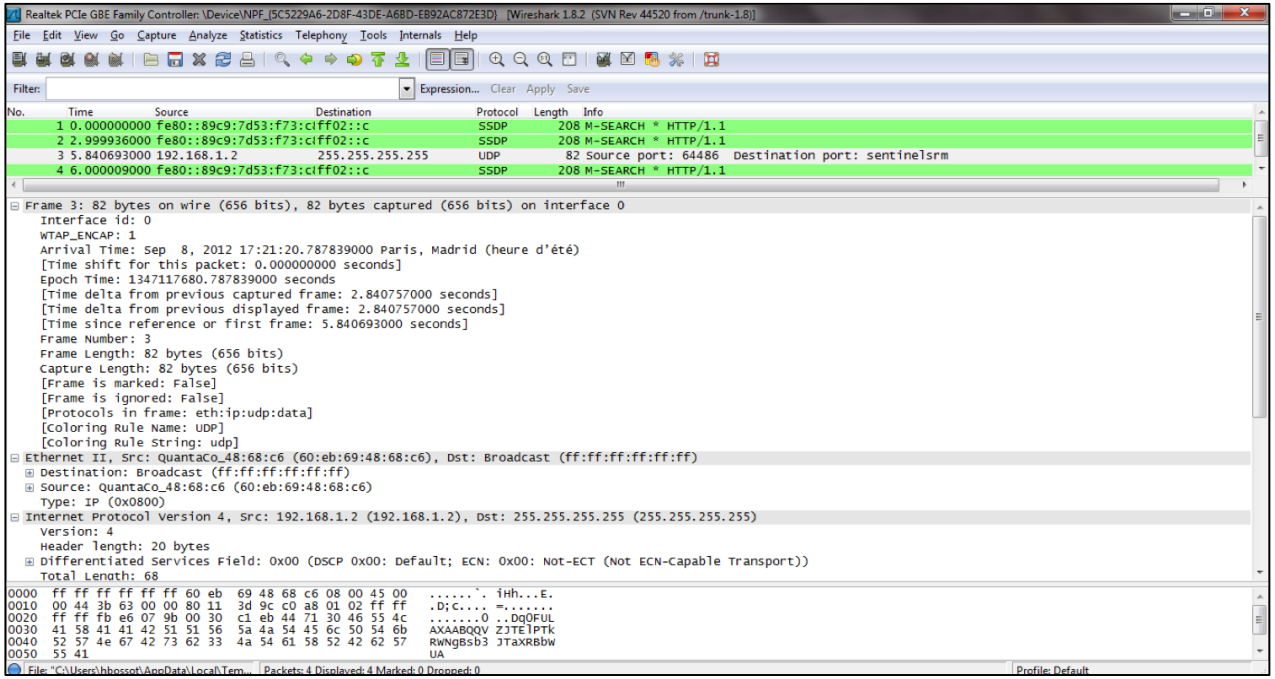
Fill in the Blanks

Take A Break

Intro to Wireshark

Packets and Wireshark

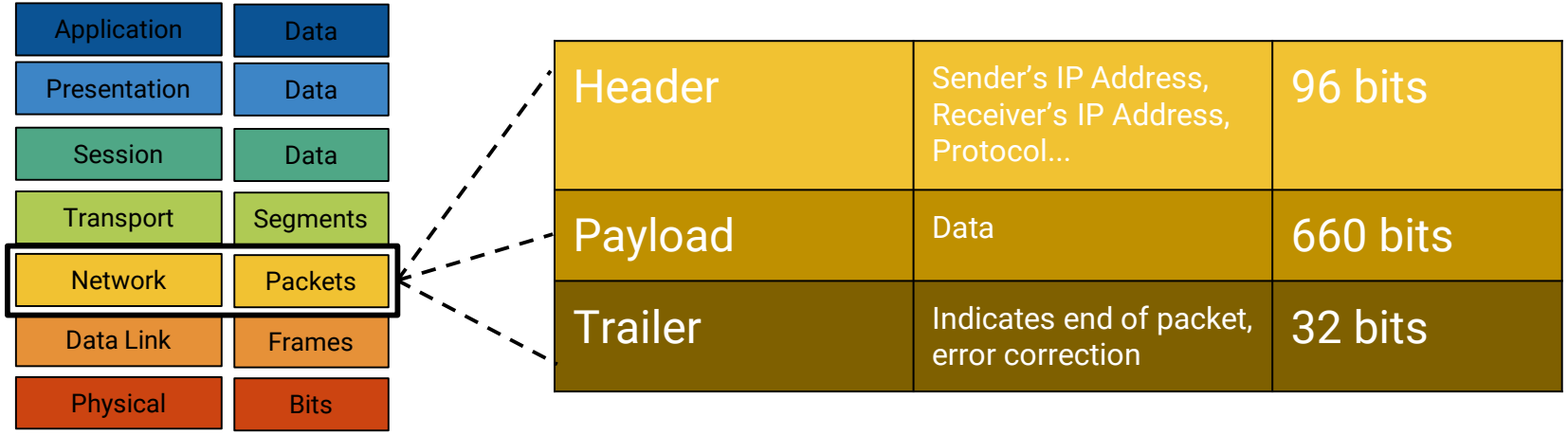
Communication between devices over a network is facilitated through the transfer of packets.



Wireshark is a tool that allows us to look at real communicati on across the network and monitor the network for activities of connected devices.

Packets

Communication between devices over a network is facilitated through the transfer of tiny packets.



Each packet contains:

- The address of its origin
- The address of its destination
- Some information that connects it to related packets being transmitted

Packets

Communication between devices over a network is facilitated through the transfer of tiny packets.

Application	Data
Presentation	Data
Session	Data
Transport	Segments
Network	Packets
Data Link	Frames
Physical	Bits

Header	Sender's IP Address, Receiver's IP Address, Protocol...	96 bits
Payload	Data	660 bits
Trailer	Indicates end of packet, error correction	32 bits

4 packets all part of the same email

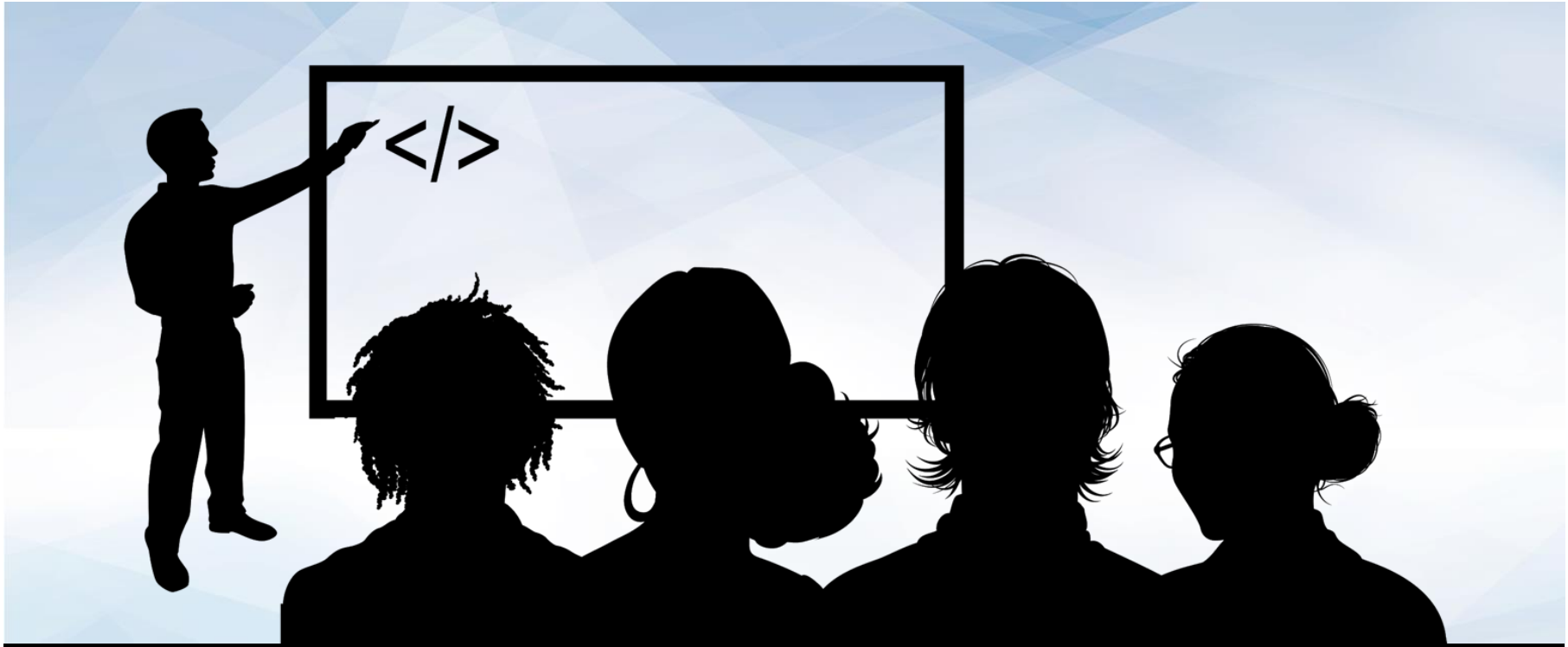
No.	Time	Source	Destination	Protocol	Length	Info
38	4.002121	10.10.1.4	74.53.140.153	SMTP	15…	C: DATA fragment, 1452 bytes
39	4.002139	10.10.1.4	74.53.140.153	SMTP	15…	C: DATA fragment, 1452 bytes
40	4.342535	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=463 Ack=5959 Win=17424 Len=0
41	4.342568	10.10.1.4	74.53.140.153	SMTP	15…	C: DATA fragment, 1452 bytes
42	4.342595	10.10.1.4	74.53.140.153	SMTP	15…	C: DATA fragment, 1452 bytes

Activity: Install Wireshark

In this activity, you will install the wireshark application.

Instruction sent via Slack.

Suggested Time:
5 Minutes



Instructor Demonstration

Wireshark Walkthrough

Wi-Fi: en0

Apply a display filter ... <⌘/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
679	3.996355	172.217.15.100	192.168.0.103	UDP	71	443 → 58494 Len=29
680	3.998872	192.30.253.125	192.168.0.103	TCP	68	[TCP ACKed unseen segment] 443 → 50824 [ACK] Seq=1 Ack=2 Win=31 Len=0 TSval=551440535 TS
681	3.998876	192.30.253.124	192.168.0.103	TCP	66	[TCP ACKed unseen segment] 443 → 50524 [ACK] Seq=1 Ack=2 Win=31 Len=0 TSval=551440535 TS
682	4.014050	192.168.0.103	69.172.200.235	HTTP	521	GET / HTTP/1.1
683	4.063496	192.168.0.103	172.217.3.110	UDP	198	57827 → 443 Len=156
684	4.063564	192.168.0.103	172.217.3.110	UDP	518	57827 → 443 Len=476
685	4.074744	172.217.3.110	192.168.0.103	UDP	75	443 → 57827 Len=33
686	4.097008	69.172.200.235	192.168.0.103	HTTP	489	HTTP/1.1 302 Moved Temporarily (text/html)
687	4.097065	192.168.0.103	69.172.200.235	TCP	54	51214 → 80 [ACK] Seq=1402 Ack=1306 Win=65535 Len=0
688	4.099299	192.168.0.103	69.172.200.235	TCP	78	51220 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1046145444 TSecr=0 SACK_PER
689	4.131280	172.217.3.110	192.168.0.103	UDP	391	443 → 57827 Len=349
690	4.131723	172.217.3.110	192.168.0.103	UDP	139	443 → 57827 Len=97
691	4.132446	192.168.0.103	172.217.3.110	UDP	83	57827 → 443 Len=41

1. Packet List Pane

```
▼ Internet Protocol Version 4, Src: 172.217.15.100, Dst: 192.168.0.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 57
    Identification: 0x0000 (0)
  ▼ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 56
    Protocol: UDP (17)
    Header checksum: 0xc547 [validation disabled]
```

2. Packet Details Pane

```
0000  8c 85 90 76 23 bd 30 b5  c2 55 79 c8 08 00 45 20   ···v#·0· ·Uy···E
0010  00 39 00 00 40 00 38 11  c5 47 ac d9 0f 64 c0 a8   ·9··@·8· ·G···d··
0020  00 67 01 bb e4 7e 00 25  db 12 10 00 fb 2c 30 04   ·g···~·% ·····,0·
0030  8b 8e 2b a8 67 2f 5e dd  37 be 25 5a 5e 1e 2c 4d   ··+·g/^· 7·%Z^·,M
0040  d5 ad 6d 72 9a f1 43                               ··mr··C
```

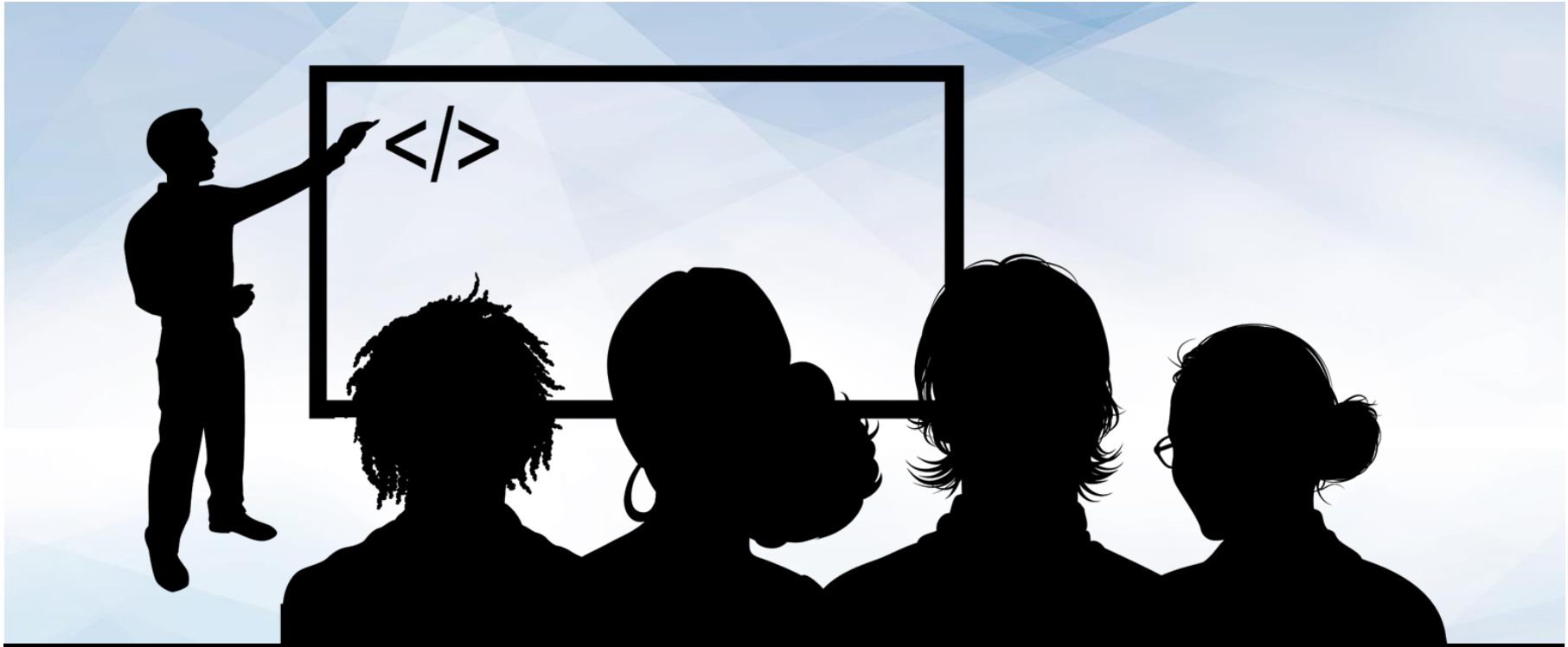
3. Packet Bytes Pane

Activity: Diving with the Wiresharks

In this activity, you will conduct a capture, investigate a packet capture files, and answer a series of questions about the traffic in a file.

Activities/05-Stu_DivingWiththeWiresharks/readme

Suggested Time:
10 Minutes



Instructor Demonstration

Inspecting a Packet

Activity: My First Sniff

In this activity, you complete your own practice capture.

Instruction sent via Slack.

Suggested Time:
10 Minutes

Today’s Objectives

By the end of class, you will be able to:

- Define basic networking terms and explain how data is transmitted over the network.
- Describe how protocols structure and define the data transmitted over the network.
- Define the OSI Model and explain each layer.
- Compare and contrast the OSI and TCP/UDP model.
- Capture communication over the network using Wireshark.
- Explain the basics of a packet in Wireshark.