

Network Security for CCSM

Computer Networking



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



CCSM Certification Examination

Domains	Weights
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR), & Incident Response	10%
3. Access Control Concepts	22%
4. Network Security	24%
5. Security Operations	18%



Network Security for the CCSM Certification

Agenda:

**Computer
Networking**

**Network Threats
and Attacks**

**Network
Infrastructure**

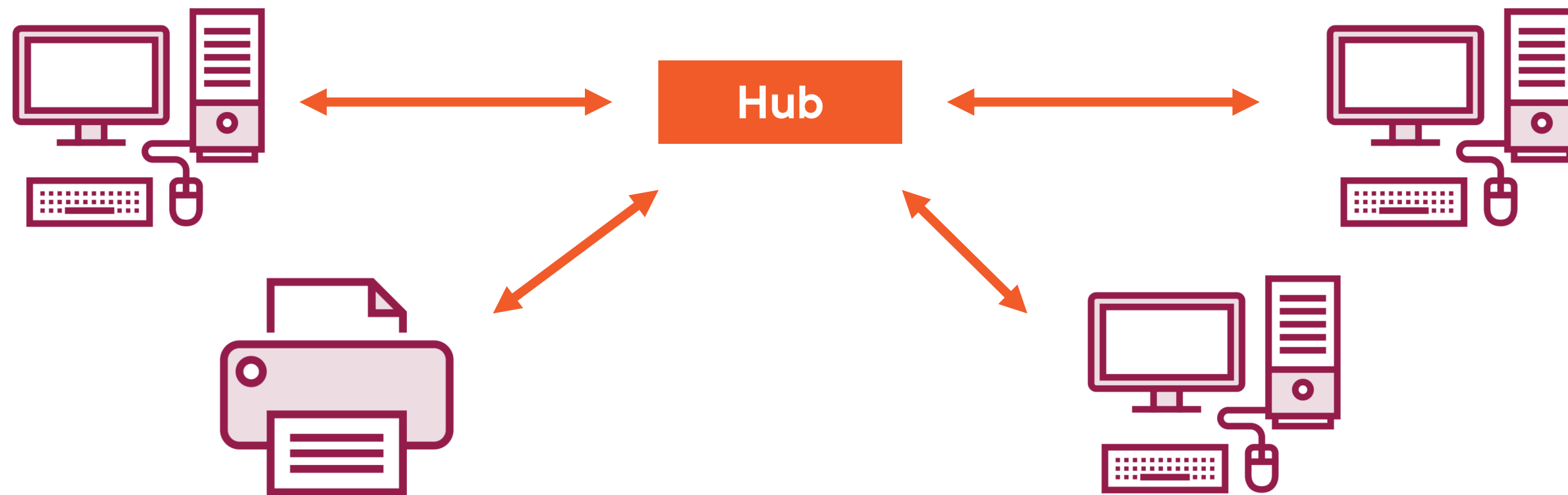


Computer Networking



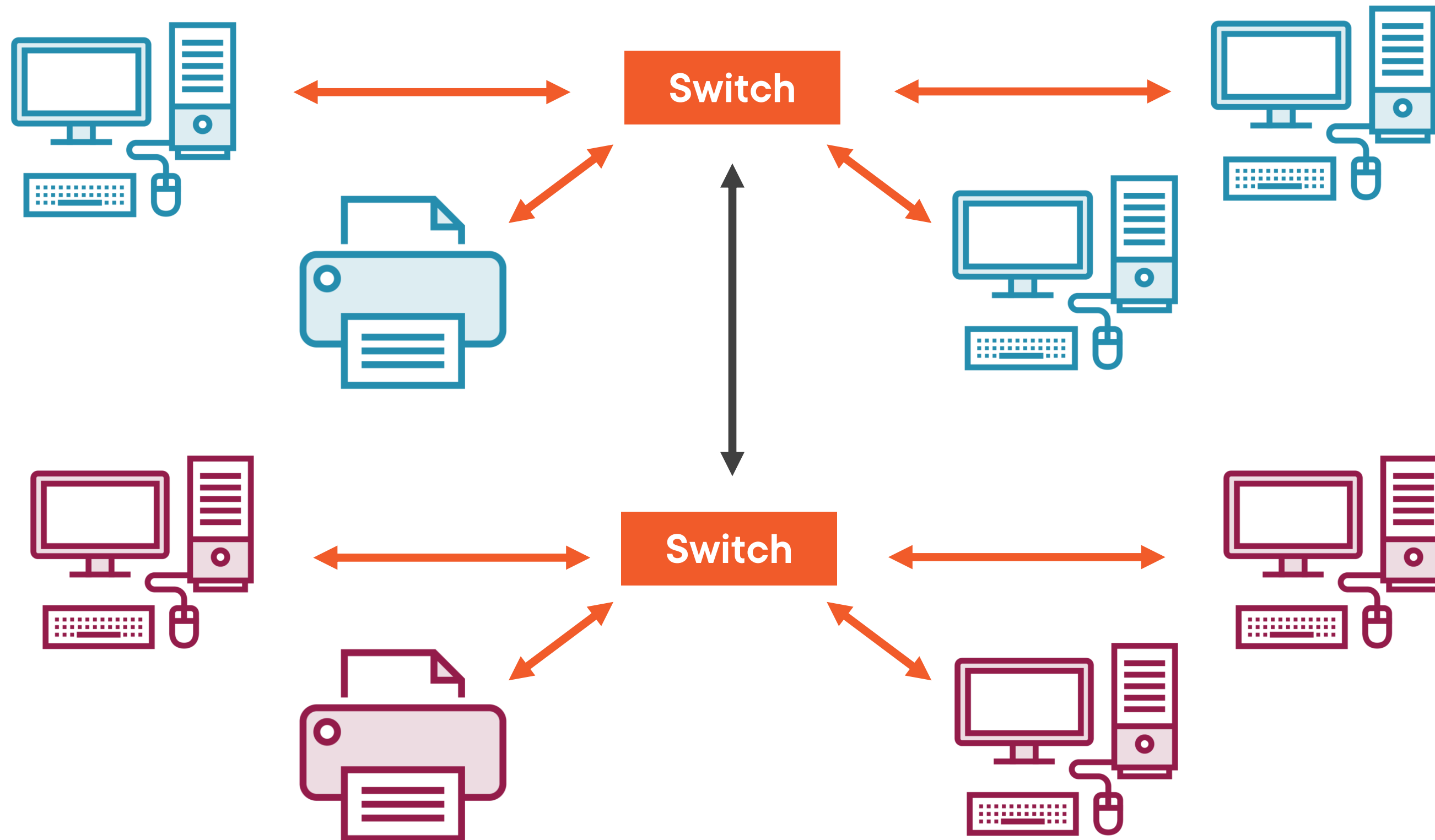
The Evolution of Networking

A network is defined as two or more devices that communicate with each other



The Evolution of Networking

A network is defined as two or more devices that communicate with each other



Network Transmission



Wired

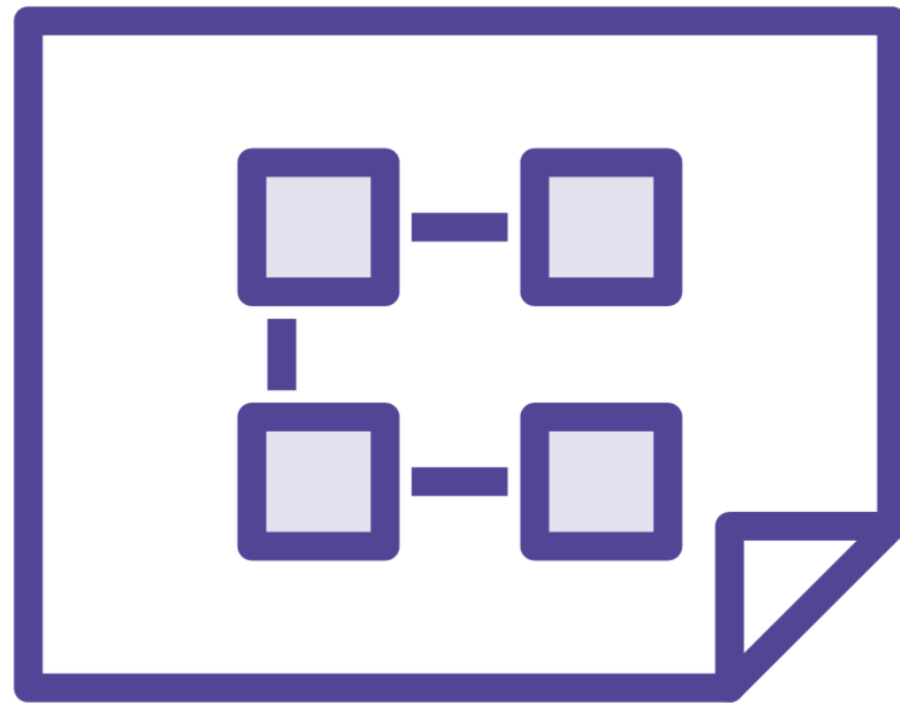
- Copper
- Coaxial
- Fiber

Wireless

- WiFi
- Satellite
- Microwave
- Infrared



Network Types



Local Area Networks (LANs)

Wide Area Networks (WANs)

Personal Area Networks (PANs)

Internet

Key Points Review



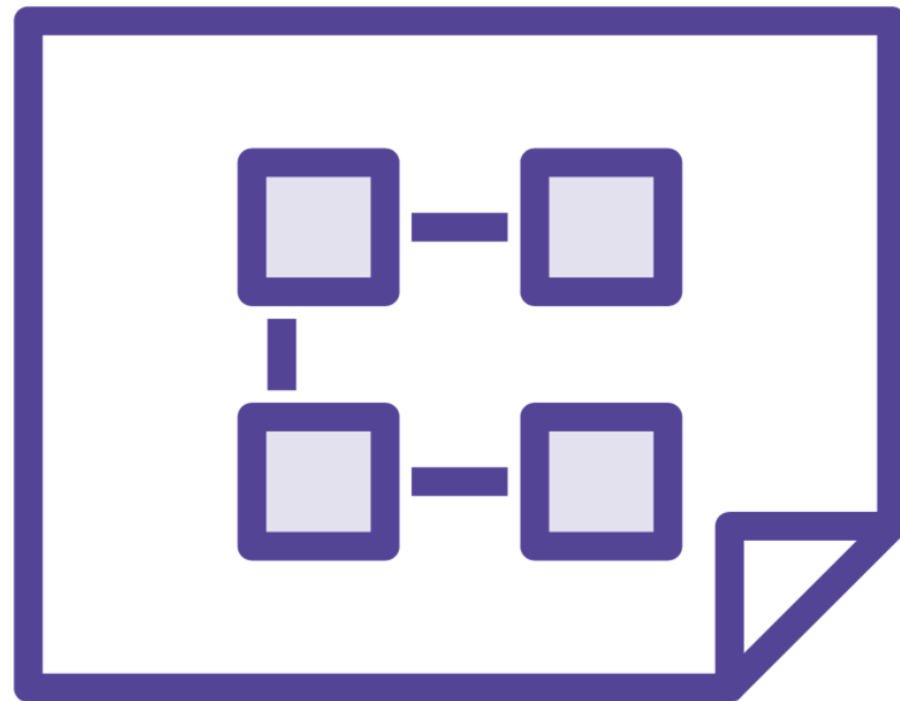
Networks can be very small and simple



Network Communications



ISO 7498



Open Systems Interconnect (OSI) Model
- ISO7498-2 – Security in the OSI model

Used as a reference to describe communications functions

OSI Layers

Application

Presentation

Session

Transport

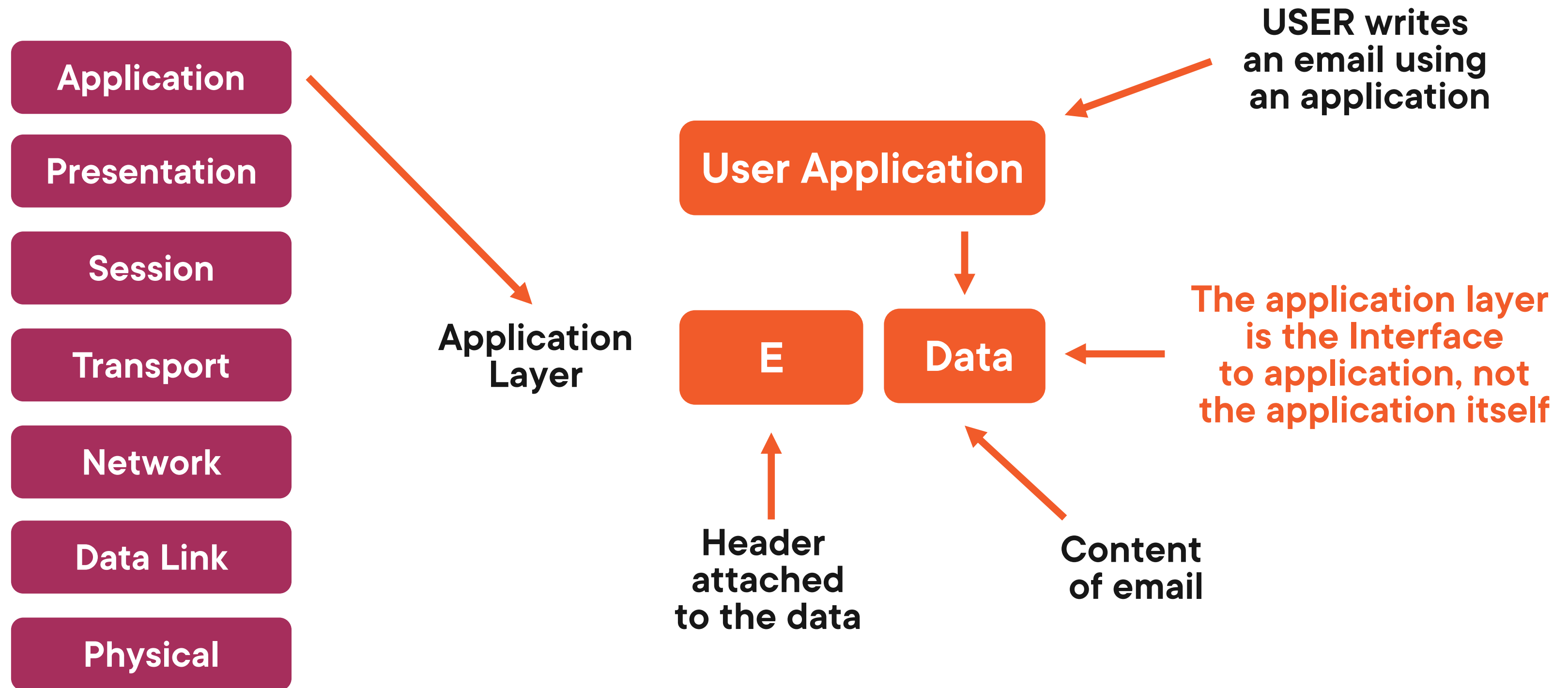
Network

Data Link

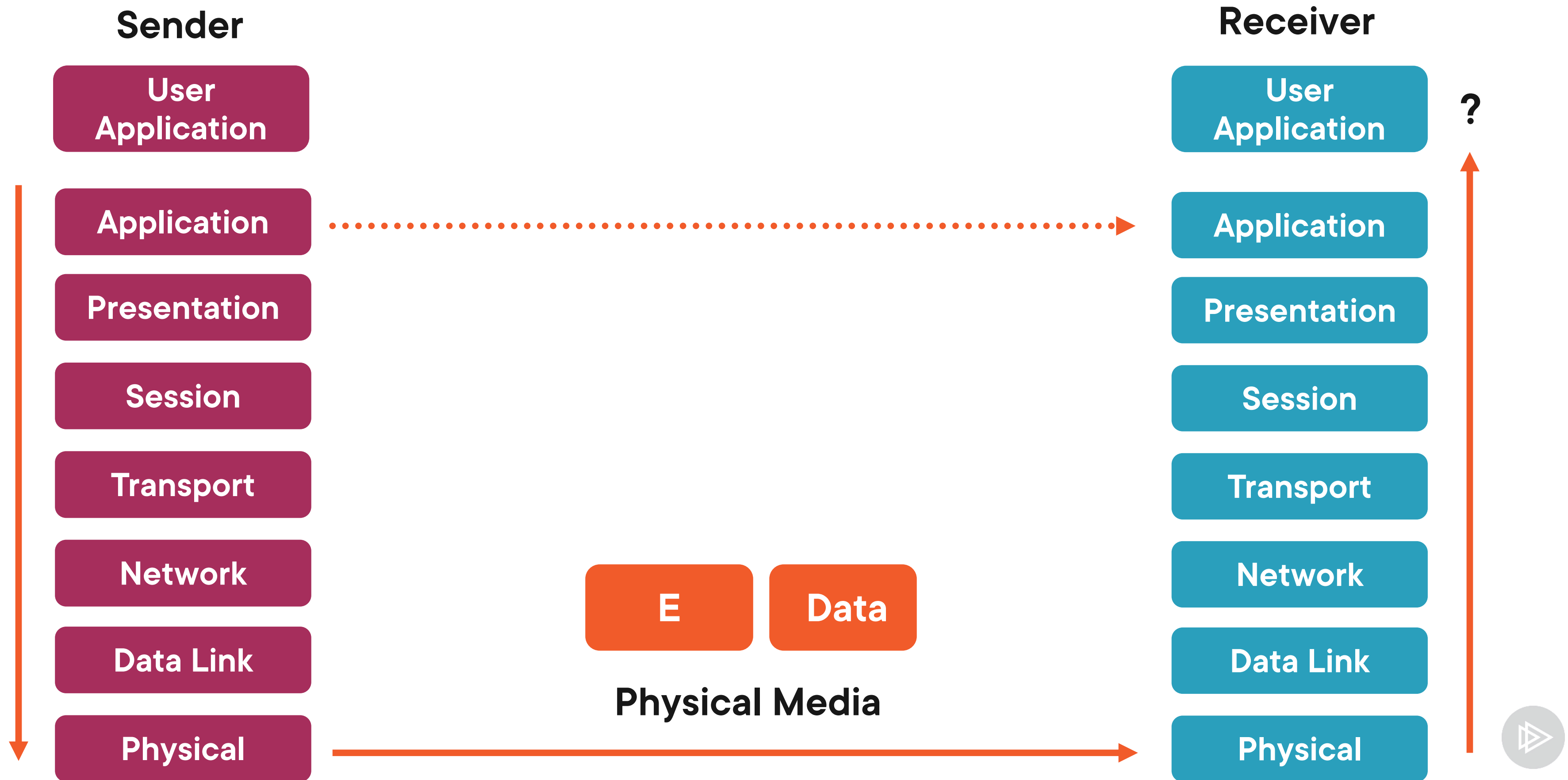
Physical



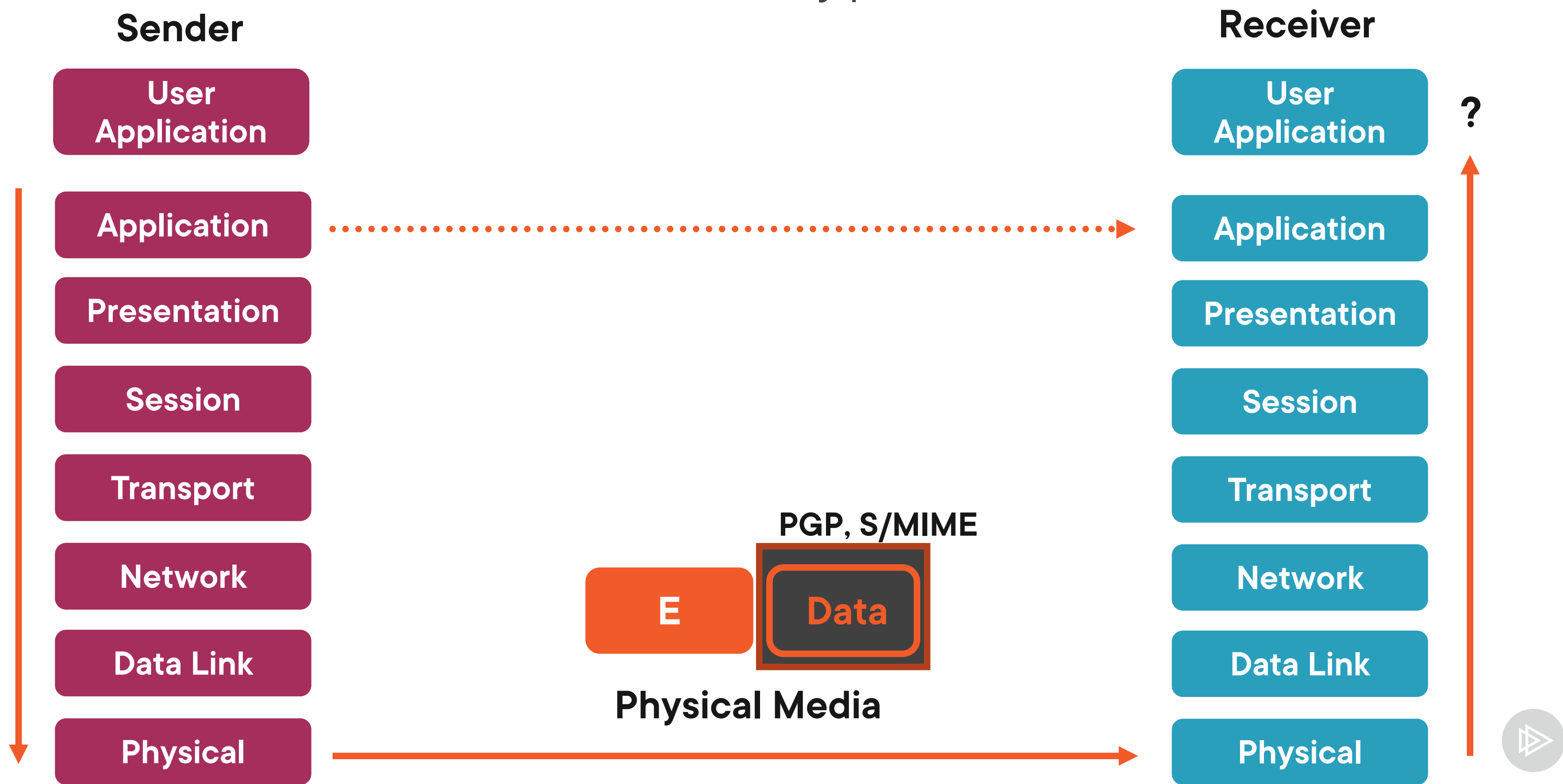
OSI Application Layer



Use of Header



Email Encryption



Presentation Layer

Sender

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Formatting, Compression

P

E

Data

Physical Media

Receiver

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical



Session Layer

Sender

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Receiver

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Session Management, Login, PPTP, L2TP

S

P

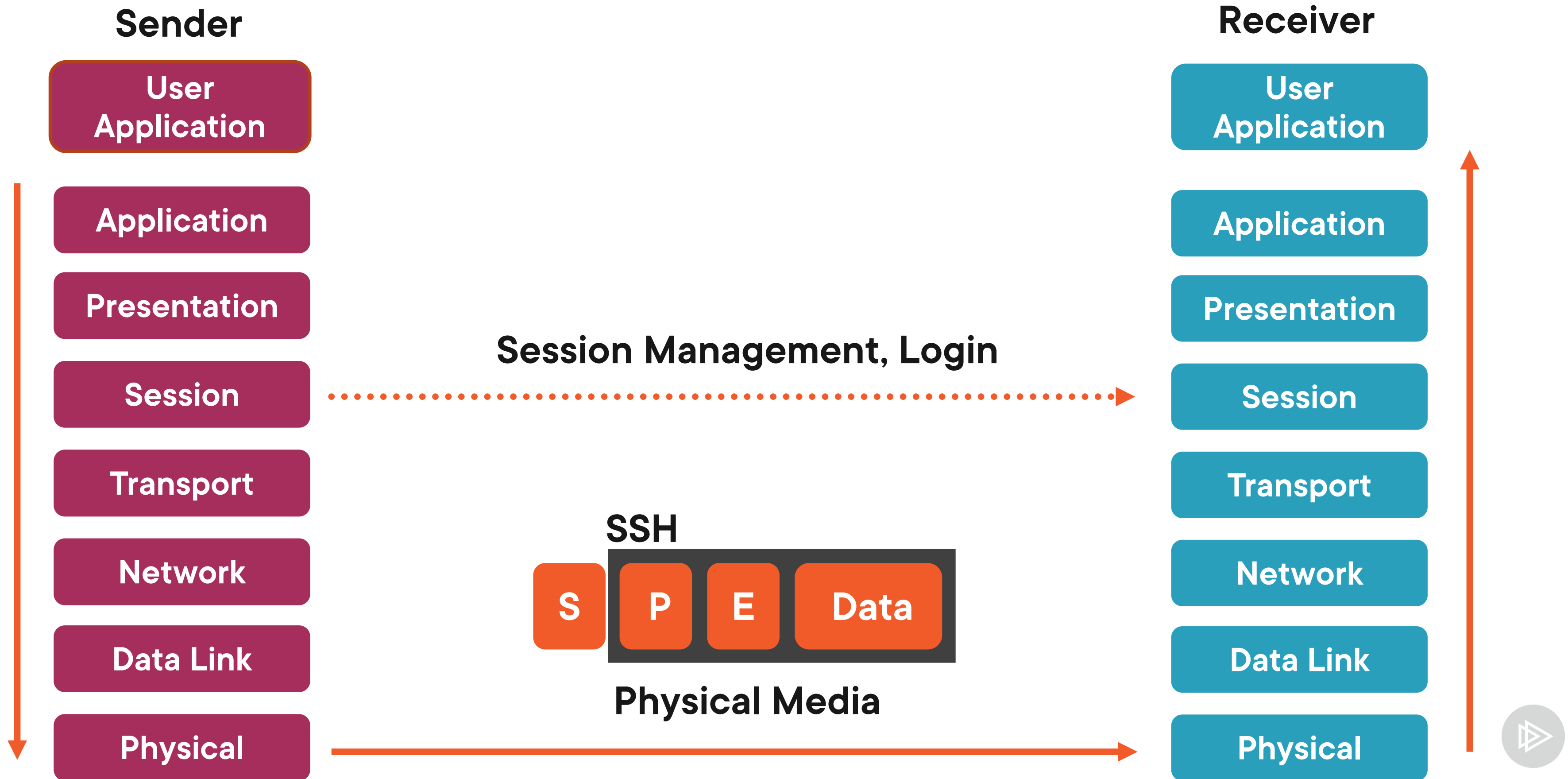
E

Data

Physical Media



Session Layer Encryption



The Lower Layers



Transport Layer

Sender

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Receiver

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

TCP/UDP

Packet or stream

T

S

P

E

Data

Physical Media

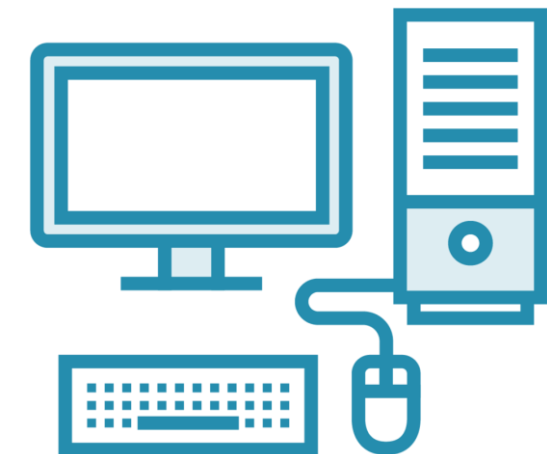


TCP Handshake

Host A



Host B



SYN (3200)

SYN(4800), ACK (3201)

ACK (4801)

Data, ACK

FIN (3890)

ACK (3891)

FIN (5900) ACK (3891)

ACK (5901)



Network Layer

Sender

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Receiver

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Datagram

I

T

S

P

E

Data

IP, ICMP, IGMP

Physical Media



Internet Protocol v4

172 . 16 . 254 . 2
10101100.00010000.11111110.00000010

32 bit IP addresses

Shortage of addresses available

Subject to spoofing, alteration, lost packets



IP v6

Version	Traffic Class	Flow Label
Payload Length	Next Hdr	Hop Limit
Source address		
Destination address		

128 bit IP addresses

**Developed together with IP Security (IPSec)
to prevent spoofing and alteration**



Data Link Layer

Sender

User
Application

Application

Presentation

Session

Transport

Network

Data Link

Physical

Frame

D

I

T

S

P

E

Data

PPP

Physical Media

Receiver

User
Application

Application

Presentation

Session

Transport

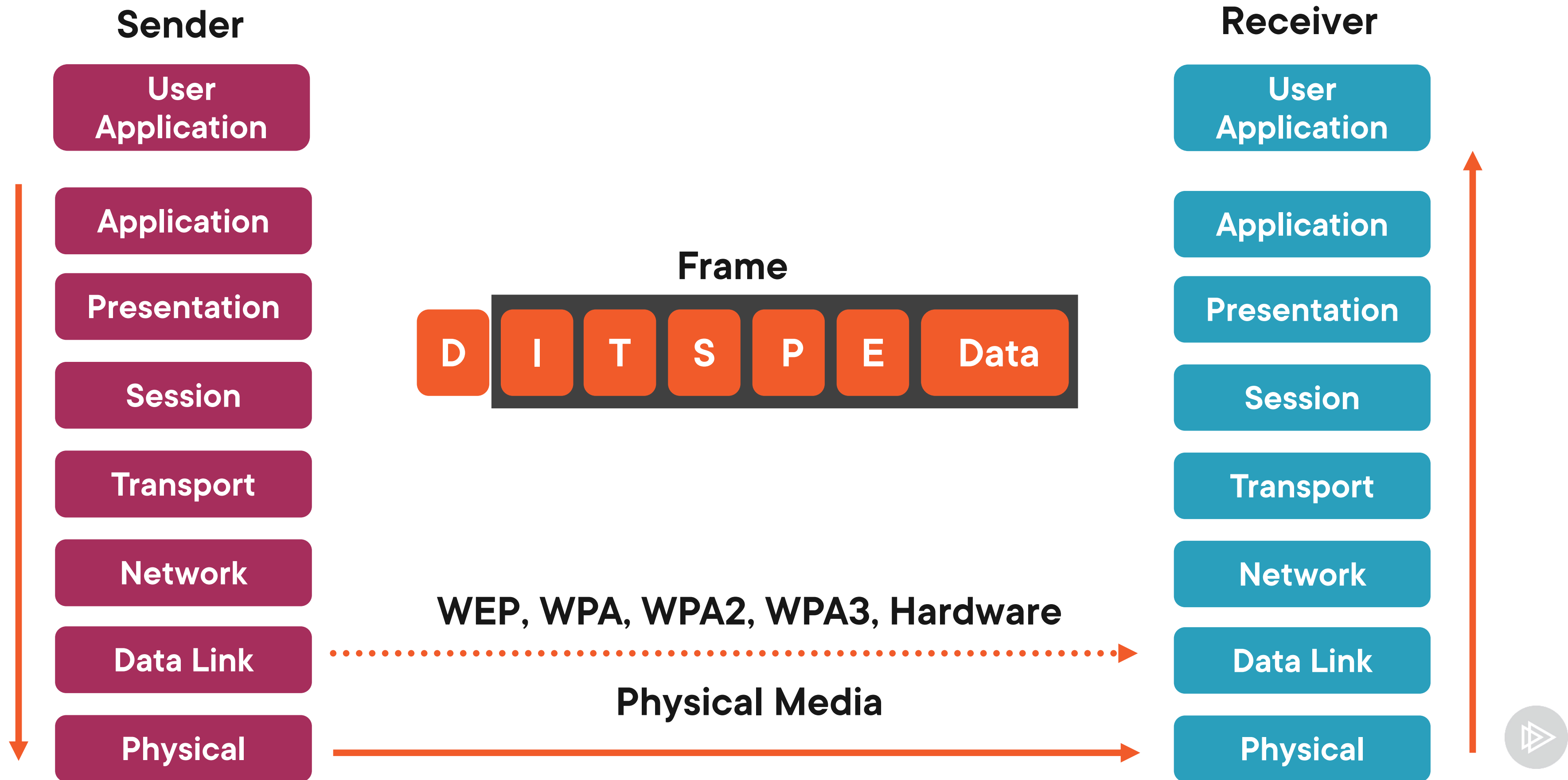
Network

Data Link

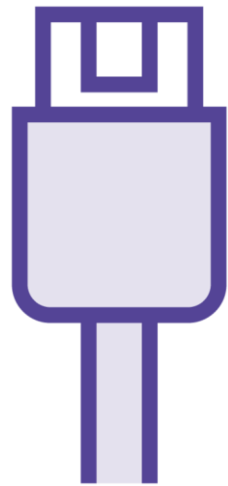
Physical



Data Link Layer Encryption



Physical Layer



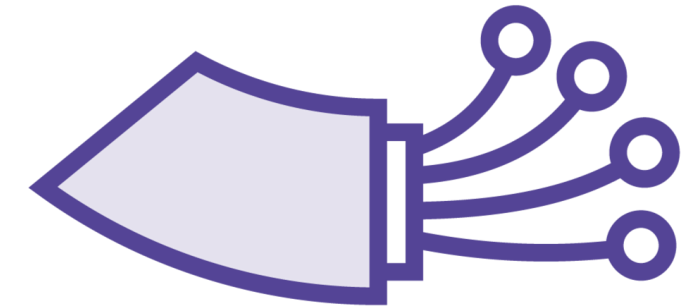
Wired

- CAT 5e
- Coaxial



Wireless

- WiFi
- RFID
- Satellite
- Microwave



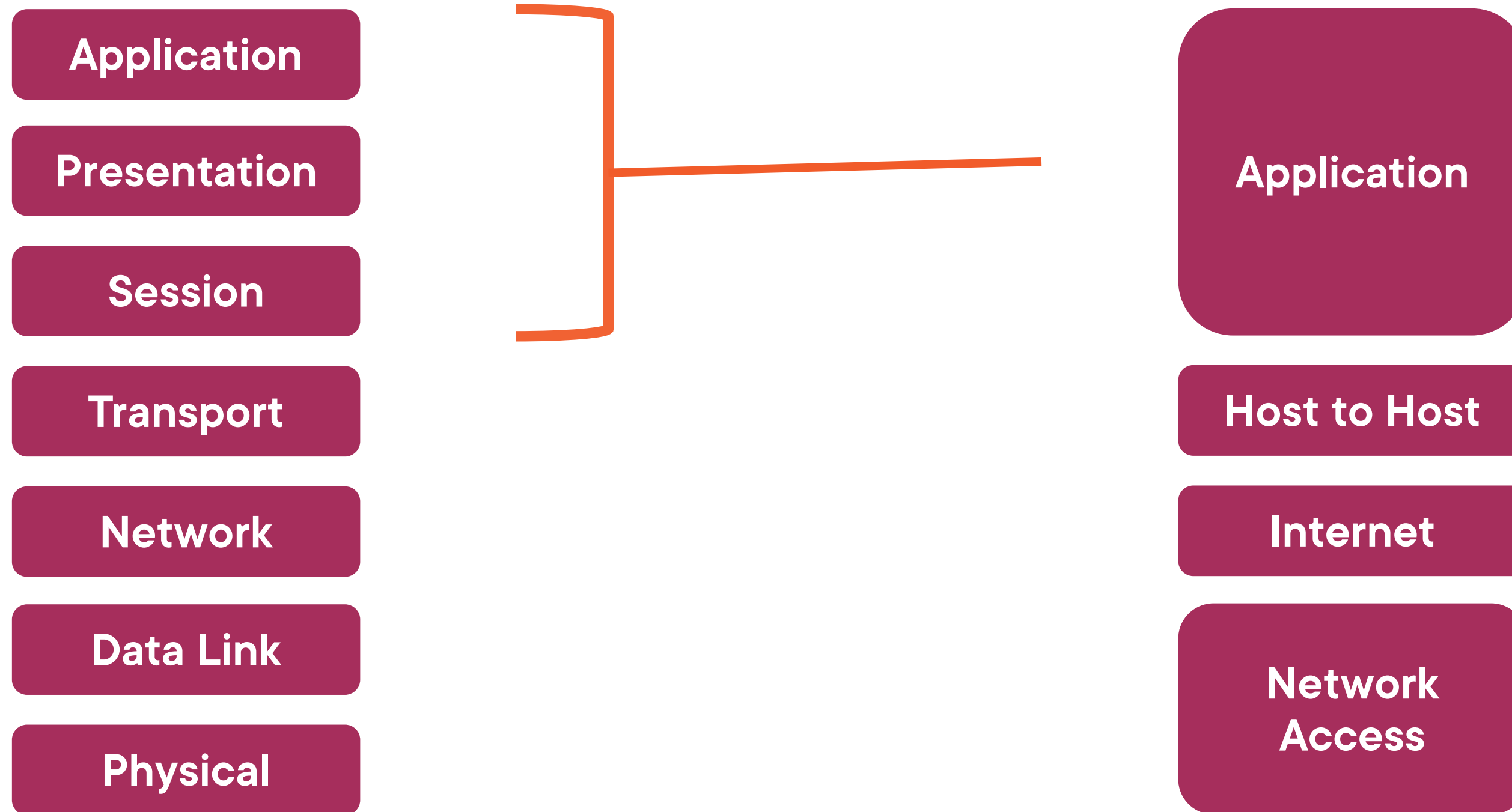
Fiber



OSI and TCP/IP



OSI Compared to TCP/IP



Domain Name System



The Internet is based on binary values

As people we like natural names

DNS converts natural names to IP addresses

- Apple.com = 17.253.144.10

If DNS does not work then most users will not be able to reach a website

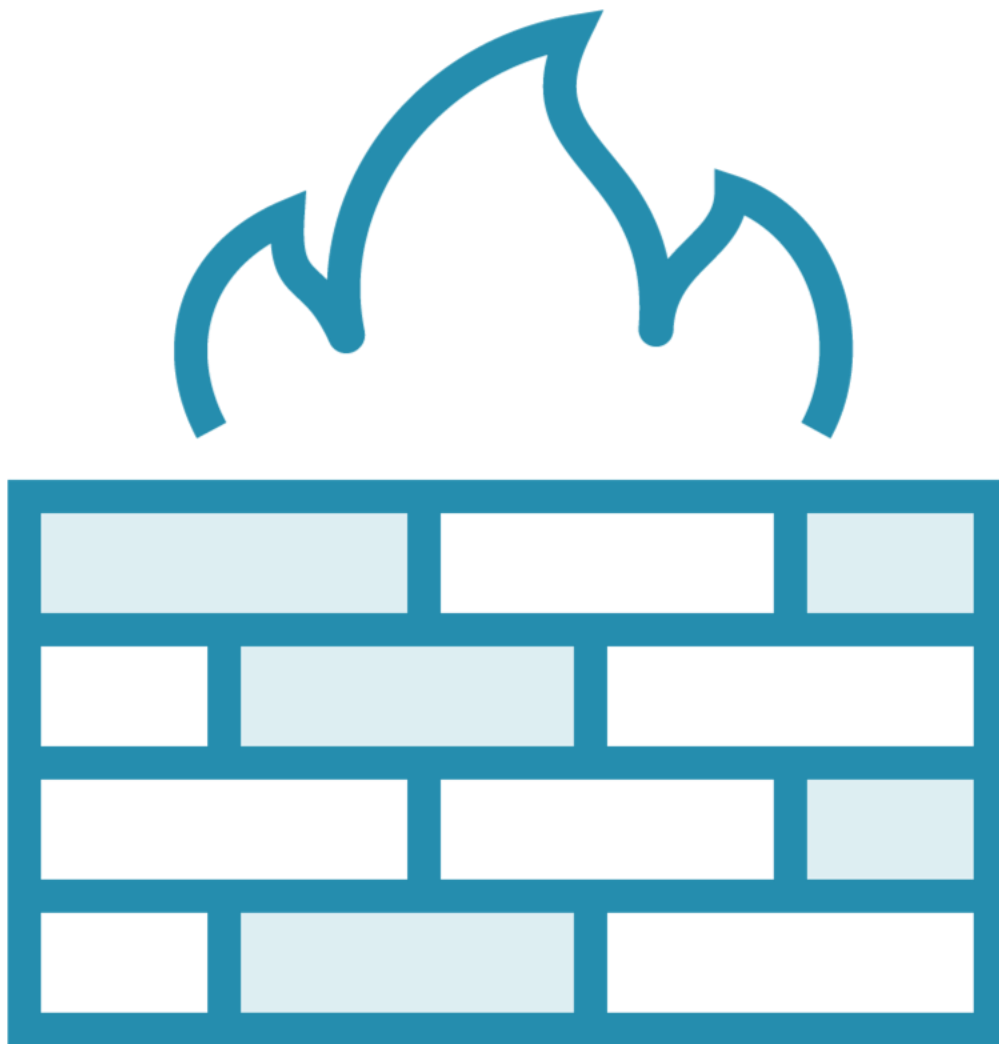


Ports

“Doorways” to control traffic

Common Ports:

- 20,21 FTP
- 22 SSH
- 23 Telnet
- 25 SMTP email
- 53 DNS
- 80 http
- 110 POP3
- 443 TLS



Key Points Review



The OSI is an excellent reference model to understand the process of network communications

TCP/IP is the basis used by many devices and systems to communicate

