NETWORK MODELS: VULNERABILITIES AND CONTROLS

Lecture 8b

COMPSCI 726

Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

August 4, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

LAYERED MODEL CONCEPT

- Issue: Building complex systems is hard
- Approach: **Divide and conquer**
  - Split into smaller steps (or layers)
- Basic idea: Each step is dependent on the previous step but does not require to know how the previous one was completed

EXAMPLE: COURIER DELIVERY OF A GIFT PACKAGE

- Alice is planning to send a gift together with a letter to Bob
- She uses a courier service to deliver the package containing both items
- Let’s break it down into a series of steps

COURIER DELIVERY OF A PACKAGE

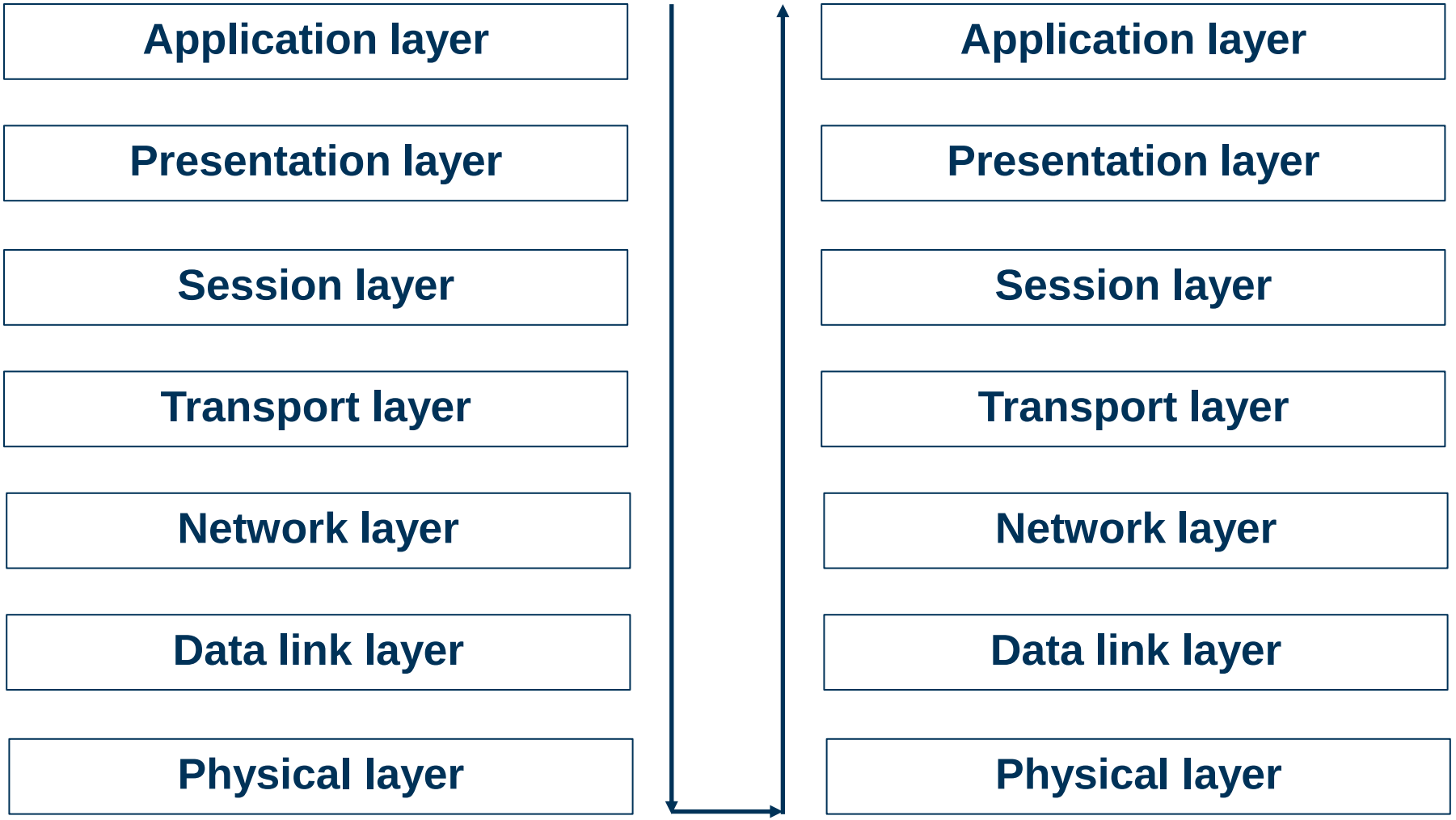
Buying gift and writing letter	Receiving the letter and gift
Wrapping each item	Un-wrapping each item
Packing both in a packet	Unpacking the packet
Contacting courier company	Delivering to destination
Moving to central store	Moving to central store
Dispatching	Validating dispatching
Shipping	Receiving shipments

MAPPING TO OSI* MODEL

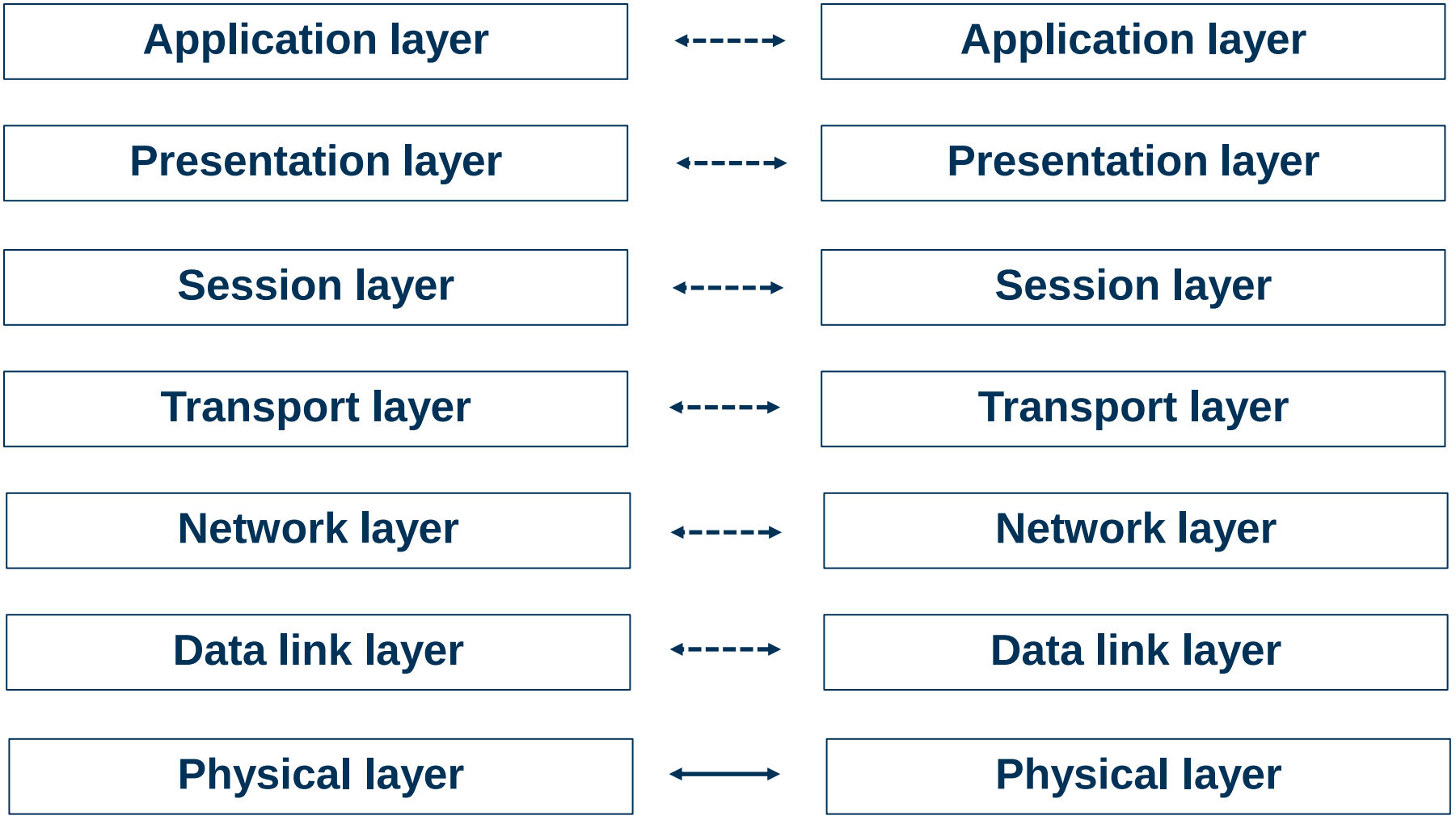
Writing letter and buying gift	Application layer
Wrapping each item	Presentation layer
Packing both in a packet	Session layer
Contacting courier company	Transport layer
Moving to central store	Network layer
Dispatching	Data link layer
Shipping	Physical layer

*OSI stands for Open Systems Interconnection

OSI MODEL: DATA FLOW



OSI MODEL: LOGICAL PATHS



OSI MODEL AND SECURITY

- Networking enables our devices to connect to the world
- It also lets the world to connect to our devices
  - It might not be desirable in some cases
- It is a prime concern for security
- Vulnerabilities and exploits make our devices insecure

PHYSICAL LAYER

- A layer responsible for physical communication between hops by generating, transmitting, or receiving voltage signals
- All other layers depend upon the integrity of the physical layer
- Hardest to maintain an audit log or monitor
- Difficult to perform error correction

PHYSICAL LAYER: VULNERABILITIES

- Loss of power
- Physical theft of data and hardware
- Physical damage or destruction of data and hardware
- Unauthorised changes to the functional environment
  - Removable media
  - Adding/removing resources
- Undetectable interception of data (eavesdropping)

PHYSICAL LAYER: CONTROLS

- Electromagnetic shielding
- Locked perimeters and enclosures
- Video surveillance
- Cryptography

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!