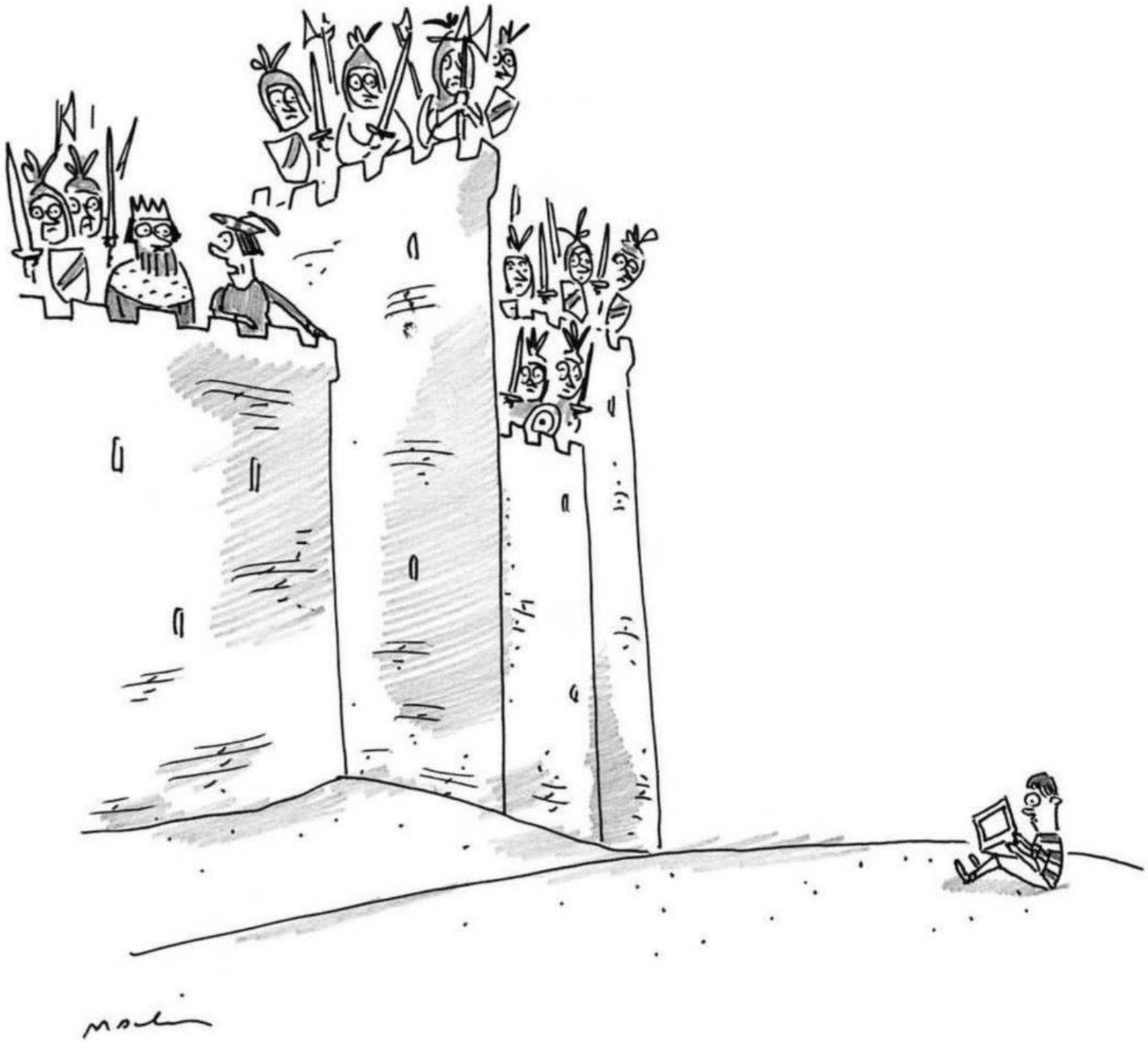
Network Security
(6CCS3NSE - 7CCSMNSE)

Diego Sempreboni
Department of Informatics
King's College London, UK

Second term 2019/20
Lecture 1

Security?

Security?



"Bad news, Your Majesty—it's a cyberattack."

Objectives and learning outcomes

- At the end of this lecture you should understand:
  - Basic security terminology
  - OSI model and network layers
  - Different kinds of attacks: jamming, sniffing, spoofing

Security = policy + mechanism

- Security realised through Policy + Mechanism

- Security design needs to ask and answer:
  - Who/What is being protected?
  - Who/What is attacking?
  - What are their powers?

- The answers to these questions are called **threat model**

Security = policy + mechanism

- Principals: actors and participants
  - Often called **roles**
- Policy codifies “desired/undesired” behaviours
- Action permitted/disallowed to principals
- On “object" being protected
- Examples:
  - Only “root” can execute this script
  - IP packet can be sent by the host in src field
  - Voter can vote at most once in election

Types of policies (Security Principles)

- **Confidentiality**: Assures that private or confidential information is not disclosed to unauthorised individuals.

- **Integrity**: Assures that information and programs are changed only in a specified and authorised manner.

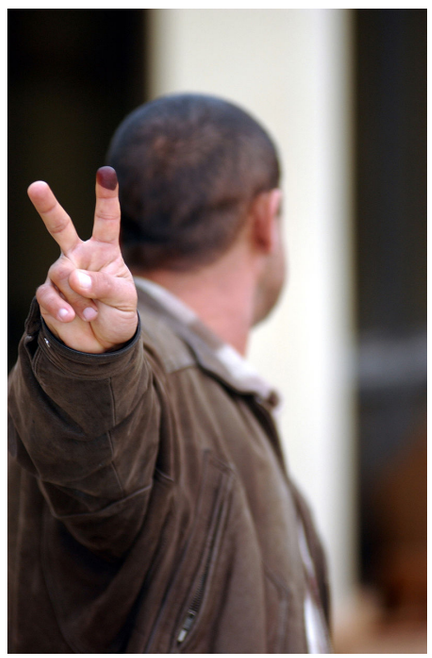
- **Availability**: Assures that systems work promptly and service is not denied to authorised users.

Mechanism: means of enforcing policy

- Only “root” can execute this script
  - Use password for root + check if user ID is root

- IP packet has been sent by the host in src field
  - Digital signature signed by key belonging to the host

- Voter has voted at most once in election
  - In many countries, voters’ fingers are marked with indelible ink to detect if they return back, in others your name is deleted from a database



Types of security mechanisms

- **Deter**: make it “too difficult” or “not worthwhile” to attack

- **Detect**: monitor for attacks

- **Deny**: prevent unauthorised access

- Others:
  - Delay: slow down users (more suited for physical security)
  - Recover : take remedial steps after attack
  - Insure: pass consequences of risk to someone else!

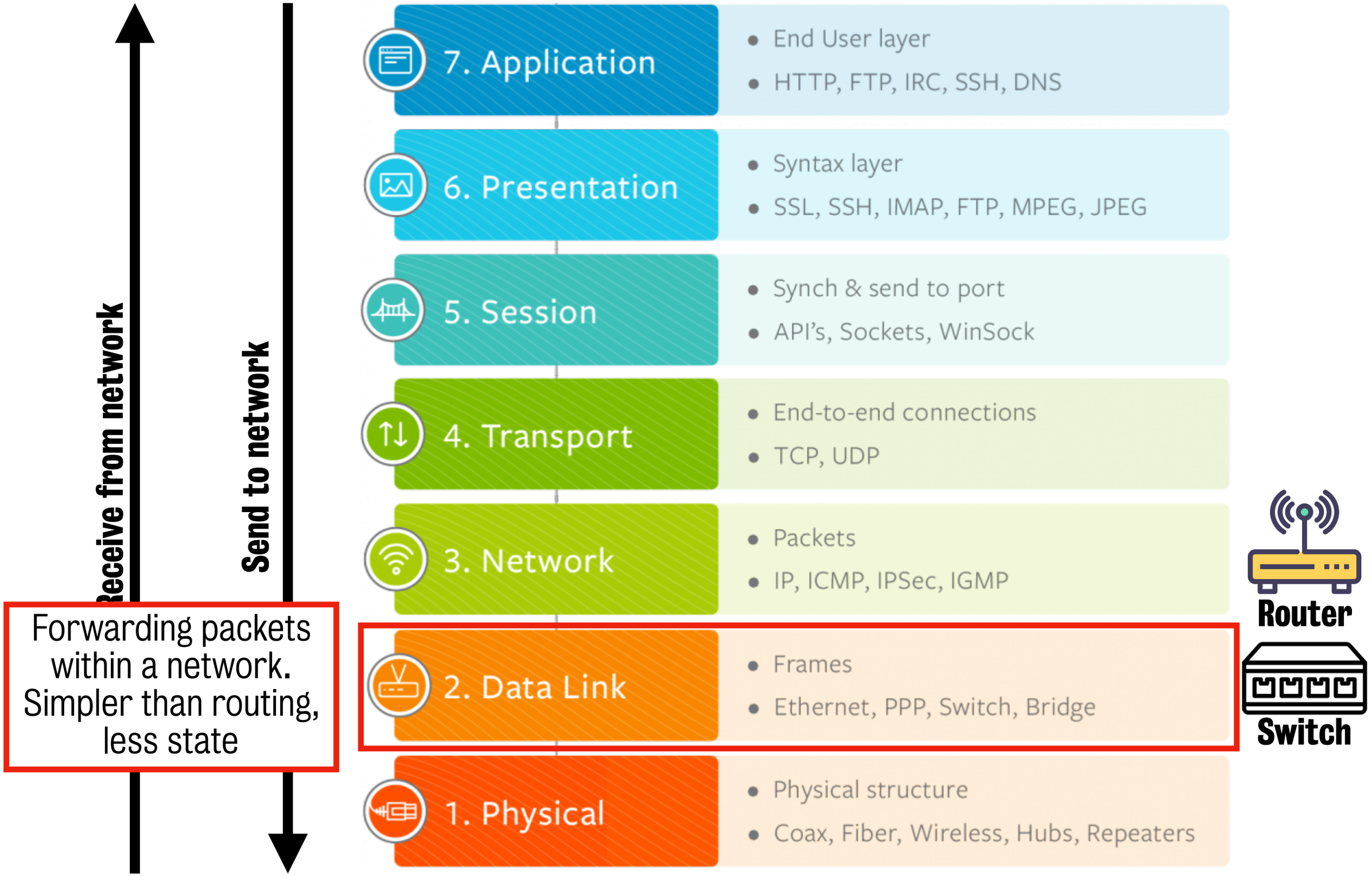
Mechanisms may involve...

- Identification of principals: e.g., username to identify users
- Authentication: e.g., password check to ensure a user is who they claim to be
- Authorisation: checking if the principal is allowed to do the requested action
- Physical protection: locks and enclosures offer physical protection to resource
- Encryption/Decryption algorithms
- Economics: a common assumption from economics is rational self-interested adversaries E.g., spammer won't pay to spam, hence if emails are associated with a cost, like a "postage stamp", we will have lesser spam
- Deception: get an adversary to reveal self. E.g., **honeypots** are extremely vulnerable servers which are deployed as "weak entities", to see who will attack, and how they will attack it. Lessons learned from honeypot can be used to protect production servers
- Randomness, unpredictability: e.g., for passwords, the more random they are, the more secure they will be

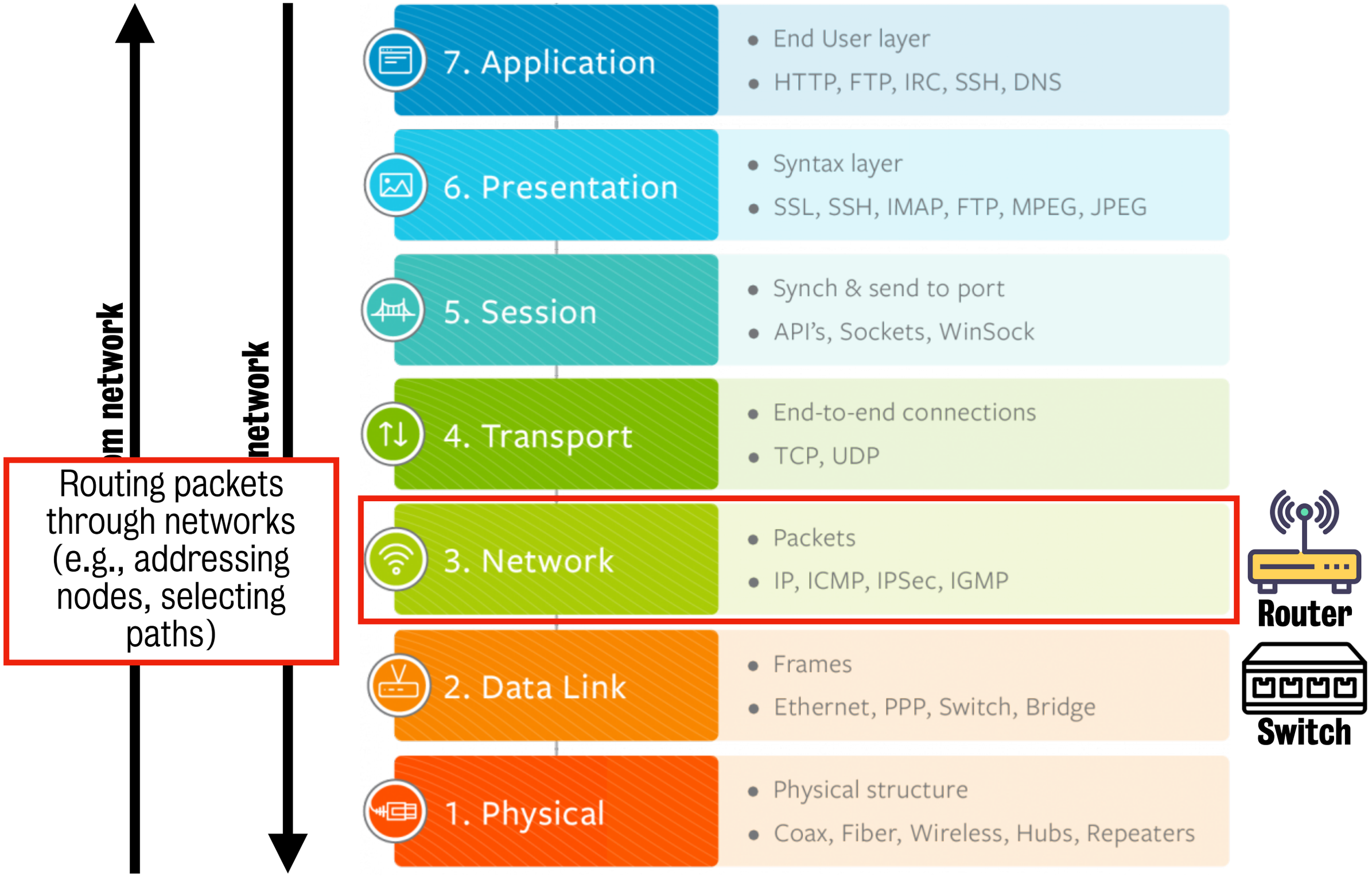
OSI Model and basics of network terminology

The OSI model: a recap

The OSI model: a recap

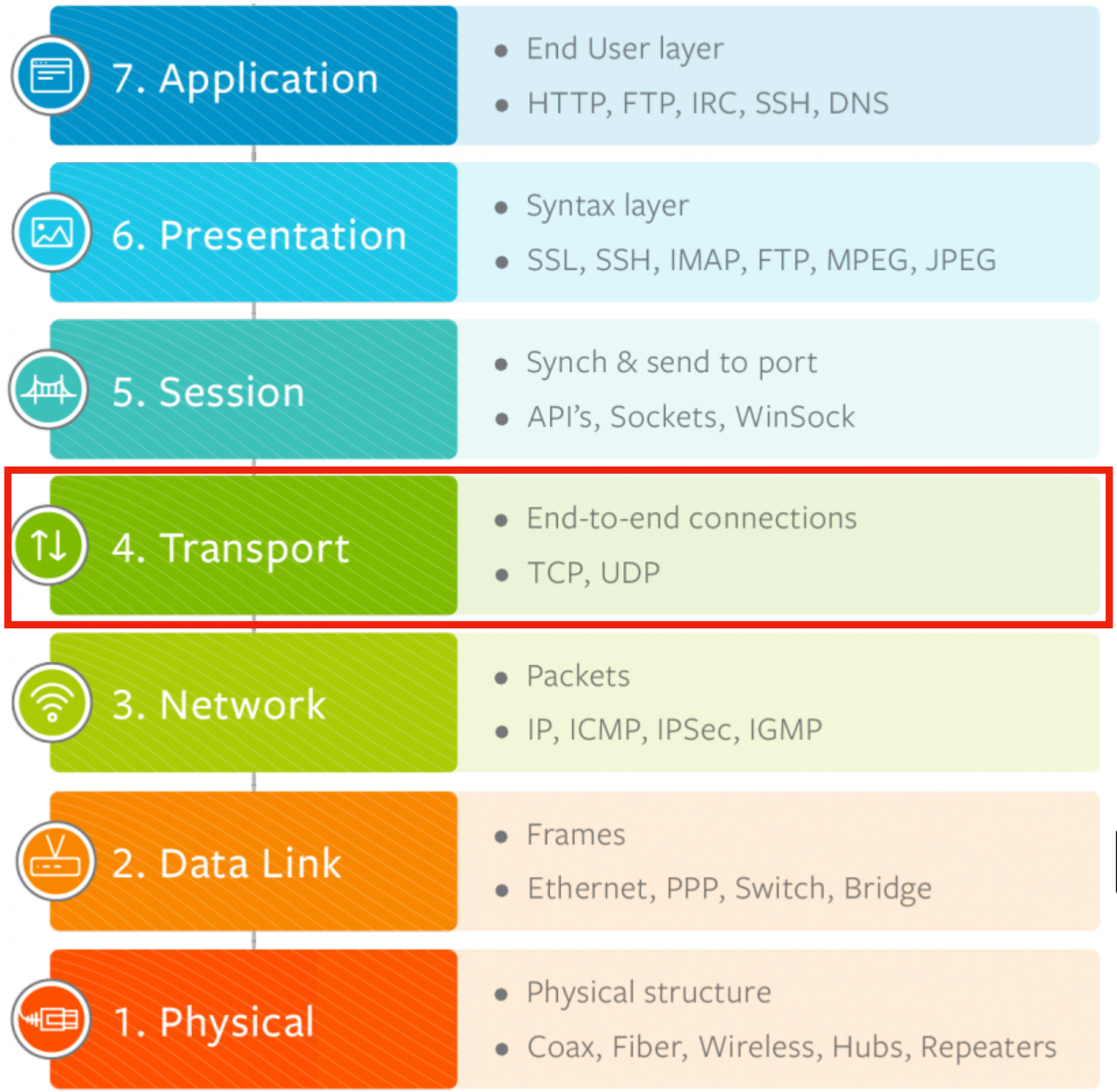


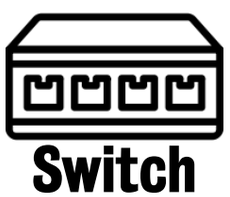
The OSI model: a recap



The OSI model: a recap

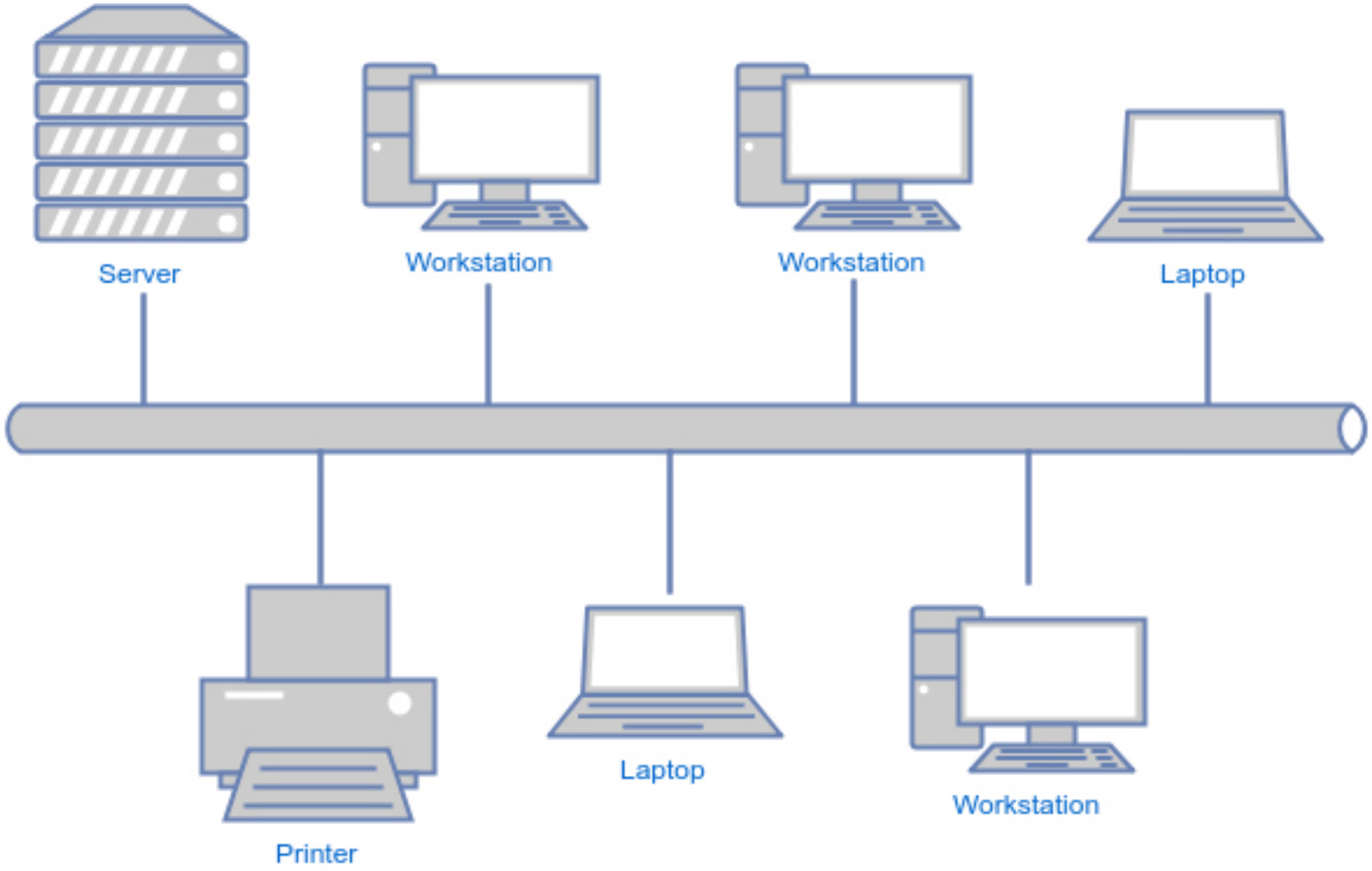
End-to-end connectivity. Creating an ordered stream of bytes. Error detection and recovery





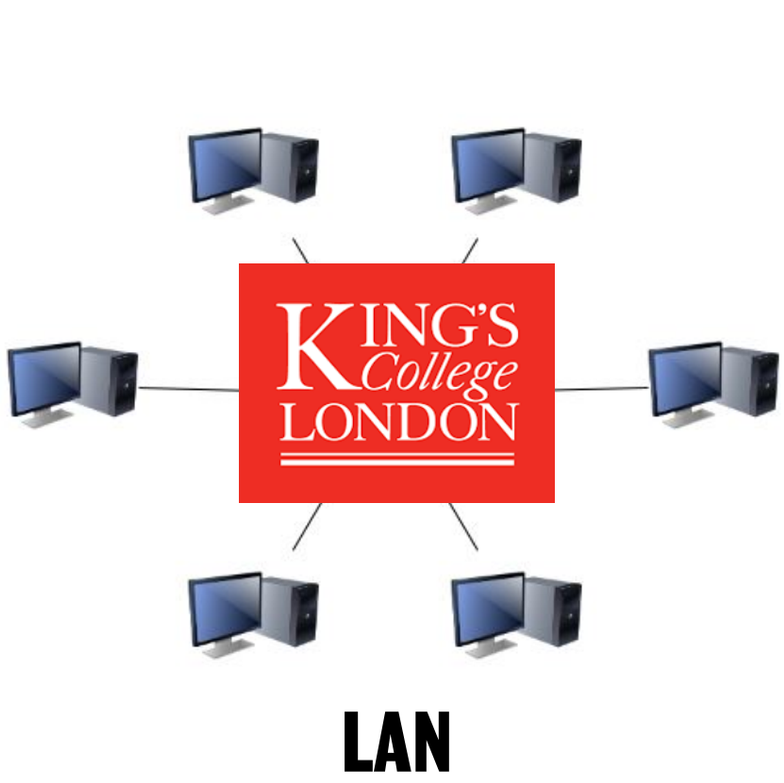
How to think about the link layer

- The general model of a link layer, whether wired or wireless, is a broadcast medium. The common "medium" is easily accessed by anyone, leading to simple attacks.

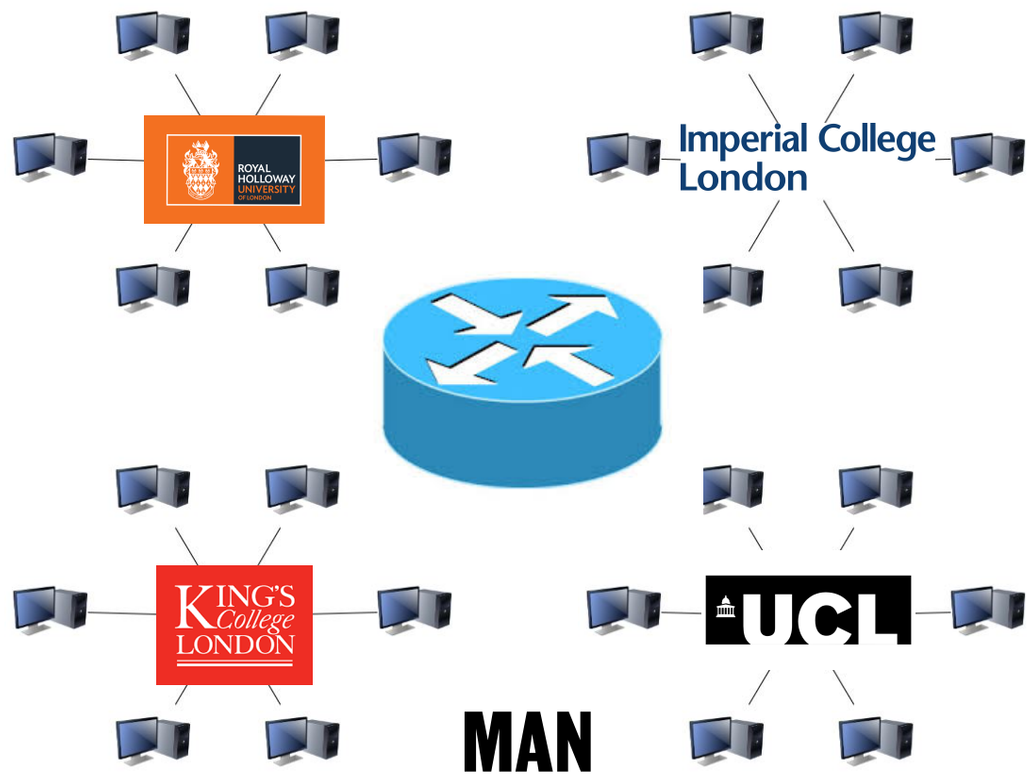


How to think about the network layer

- The network layer is needed to **route** between different LANs.
- The Internet is a network of networks.
- Info needs to be shared to find routs, but network operators want to keep private data private!



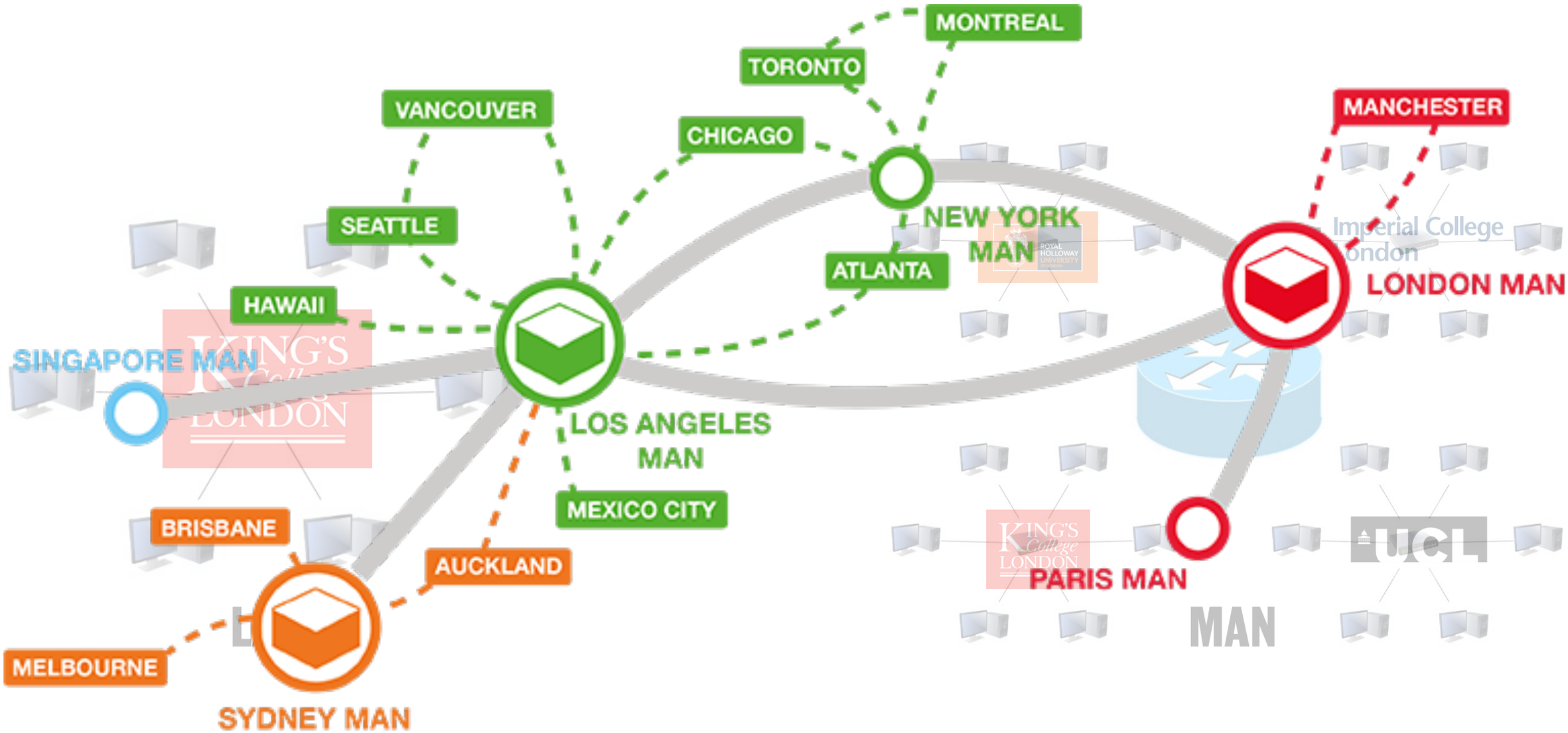
LAN



MAN

How to think about the network layer

- The network layer is needed to **route** between different LANs.
- The Internet is a network of networks.
- Info needs to be shared to find routs, but network operators want to keep private data private!



How to think about the transport layer

- As an “end-to-end” pipe for bits, from sender to receiver
- With optional add-on capabilities such as:
  - Reliability -> correct for errors
  - Ordering of data (Typically FIFO, data is delivered in the order it was sent to receiver)
  - Dealing with network effects such as congestion

In the OSI model...

- Each layer and protocol
  - Exposes **information**
  - Exposes **functionality**

- Seemingly secure functionality at layer 2 could enable attacks at layer 3

- Sophisticated attacks often exploits multiple layers

Different kinds of attacks

Jamming

Jamming

- Affecting availability for legitimate packets by talking too much

Jamming at the link layer

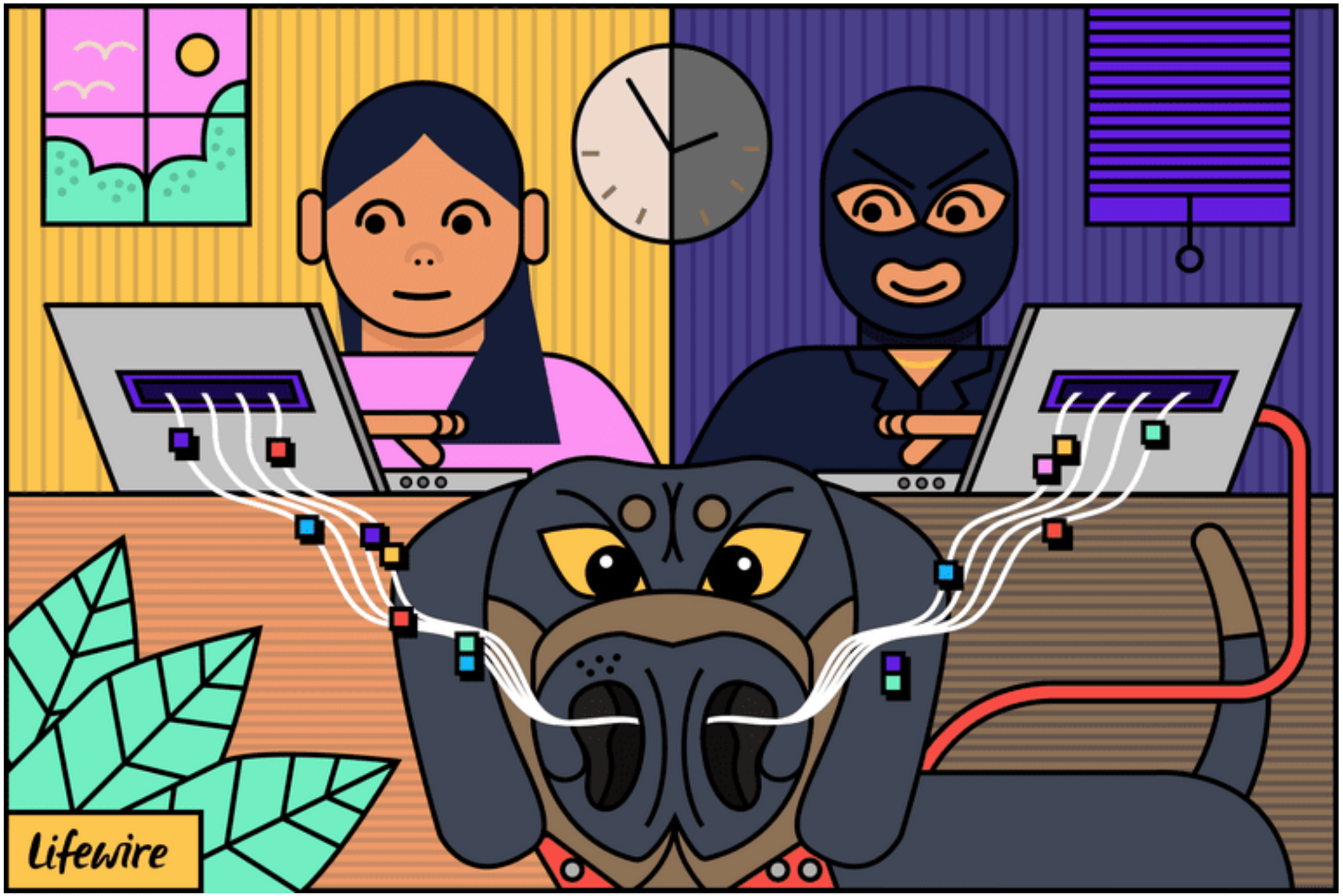
- The link layer typically broadcast-based
- Users must be polite: one user talks at a time
- Jamming: hogging broadcast medium so no one can talk. Works easily on ethernet, WIFI...

A portable jammer...

- WIFI
- 3G/4G
  - 5-20 meters
- £ 100-200

... a less portable one

Sniffing



What is network packet sniffing

- Sniffing attacks involve listening to network conversations that are not intended for you
- Network card returns packets destined for you. But card may be put in a **promiscuous** mode to get all packets from network
- Sniffing can have a benign purpose: it is very useful for network debugging and diagnostics

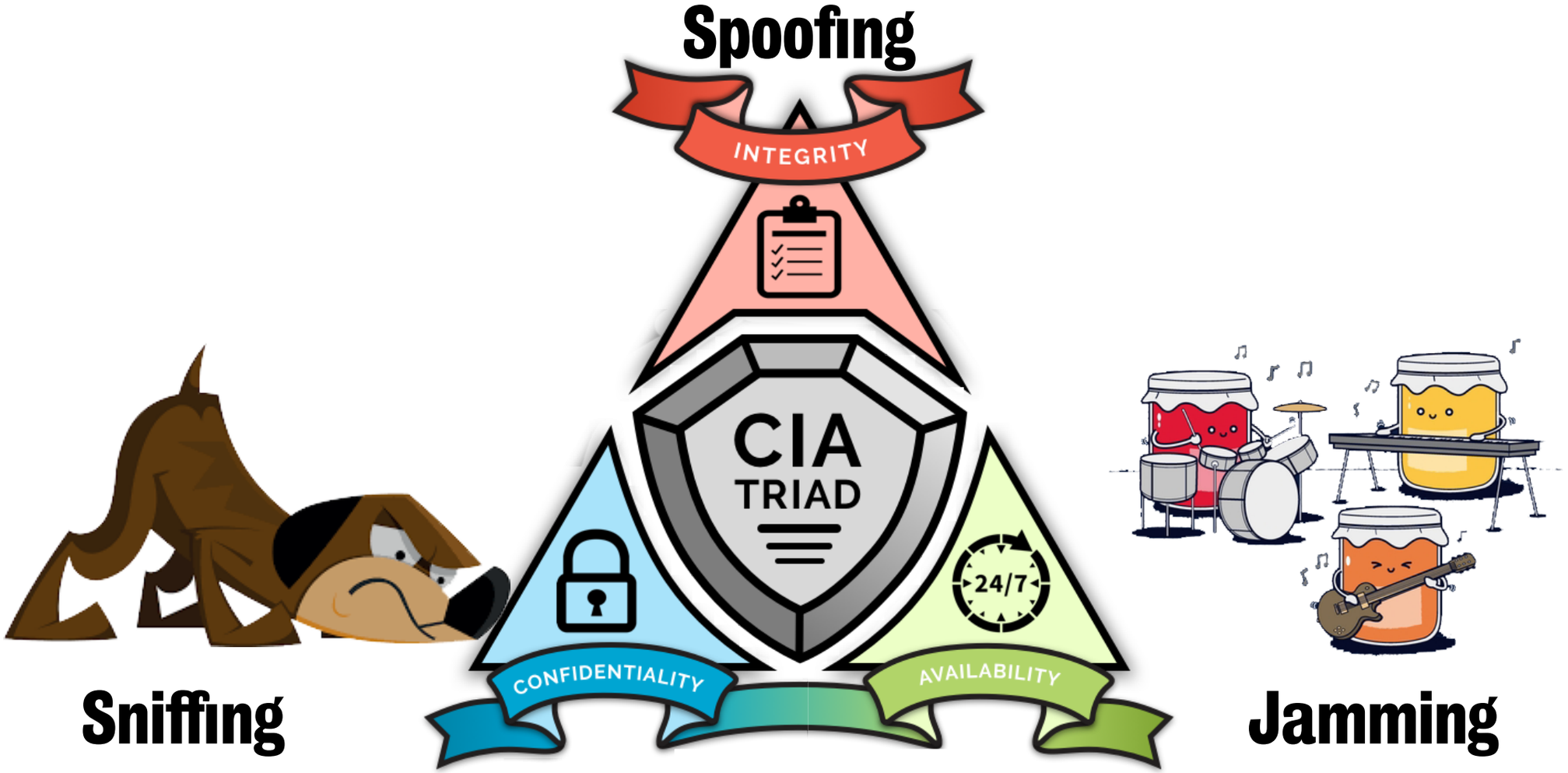
Spoofing

Spoofing attacks

- Pretending to be somebody you are not (masquerading), BUT
- What is a “somebody” on the Internet?
  - An IP address
- What is “somebody” on the LAN?
  - A MAC address
- Spoofing forms the basis of a lot of attacks
  - Why? Because it is very easy to change your address

What attack for what

Spoofing



Sniffing

Jamming

Recall from CIS: Each of the above can be tackled in standard ways

What attack for what

Security property	Attack	Defense
Confidentiality	Sniffing	Encrypt
Integrity	Spoofing	Message digest + sign
Availability	Jamming	Account and policy

BUT: **These solutions may not always be practical!**

LAB time (EPISODE 0)

- NO LAB time this week.