Imperial College London

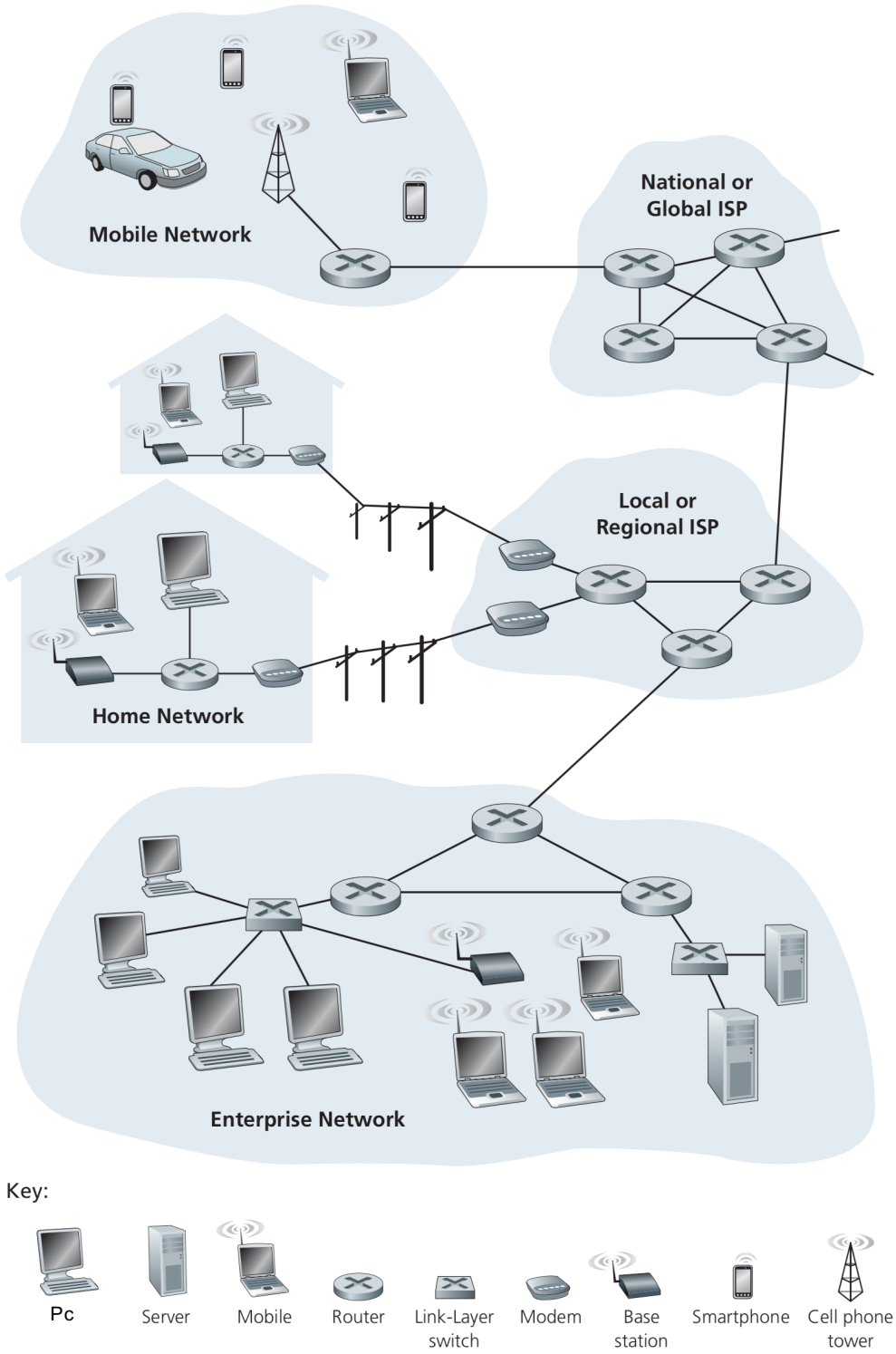
Network and Web Security

Networks background

Dr Sergio Maffeis
Department of Computing
Course web page: https://331.cybersec.fun

The Internet

- *Hosts* (laptops, servers, "things", etc) are the providers and/or consumers of *services*
  - Each host is reachable via an IP address, such as 155.198.140.14
- A network of networks
  - Also know as Autonomous Systems (AS), identified by AS numbers
  - An AS controls one or more ranges of IP addresses
- A packet switched network
  - *Packet* (or *datagram*): message that is sent as a single unit on the network
    - Typically composed of *headers + payload*
    - Headers contain addresses, plus additional protocol information
  - Each packet needs to be routed between endpoints based on hierarchical addressing
- Built on the TCP/IP protocol stack



IP addresses

Imperial College London

Only the first 3 bytes are significant

- CIDR notation for IP ranges: 123.456.789.0/24
  - Range covers all the addresses beginning with the first 24 bits of the IP above, that is 123.456.789.0-123.456.789.255
- Different network services are multiplexed through the same IP address using *ports*
  - 155.198.140.14**:80**
  - Common services **tend** to be hosted on standard ports
    - SSH: 22, DNS: 53, HTTP: 80, HTTPS: 443
    - We shall see that this does not always hold in practice
- One machine can have multiple IPs
  - Over time: connect at home, at work, on the go
  - At the same time
    - Client with wireless and Ethernet connections
    - *Dual-homed host* (firewall, gateway) connecting two different networks
    - Generally, one IP per network interface
- Multiple machines may share the same IP
  - Home router connecting desktop, laptop, iPhone
  - Port- or name-based virtual hosting of websites
  - Any-cast replication of hosts for CDNs, DNS

IP is associated with network interface.
Wi-Fi & Ethernet are two different interfaces

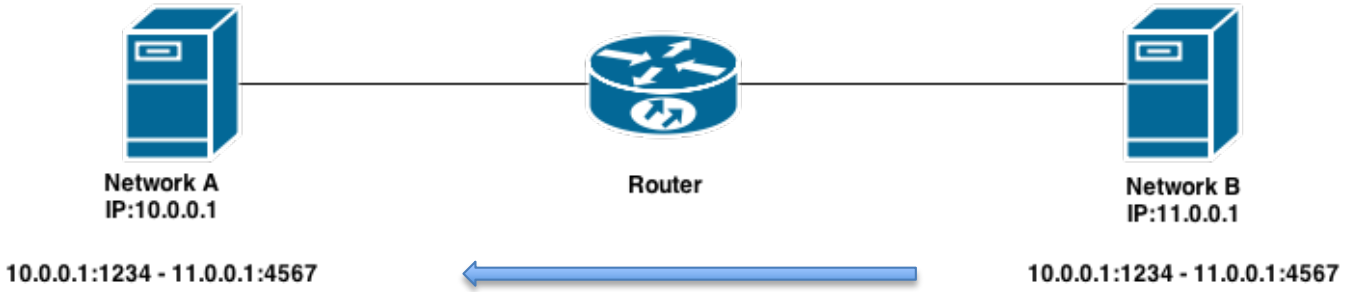
One-to-Many (External IP -> Internal IP)

Different machines around the global shares the same IP
(For reducing latency)

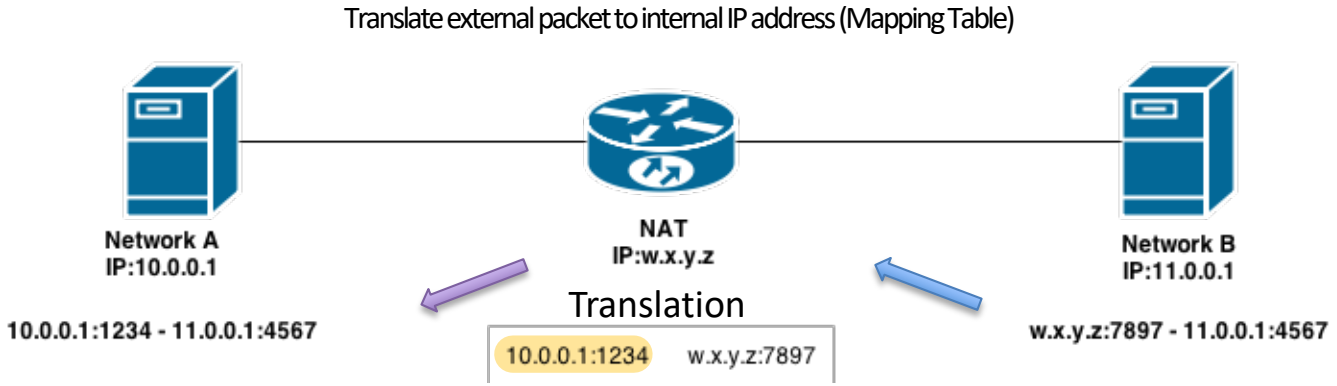
Network intermediaries

Imperial College London

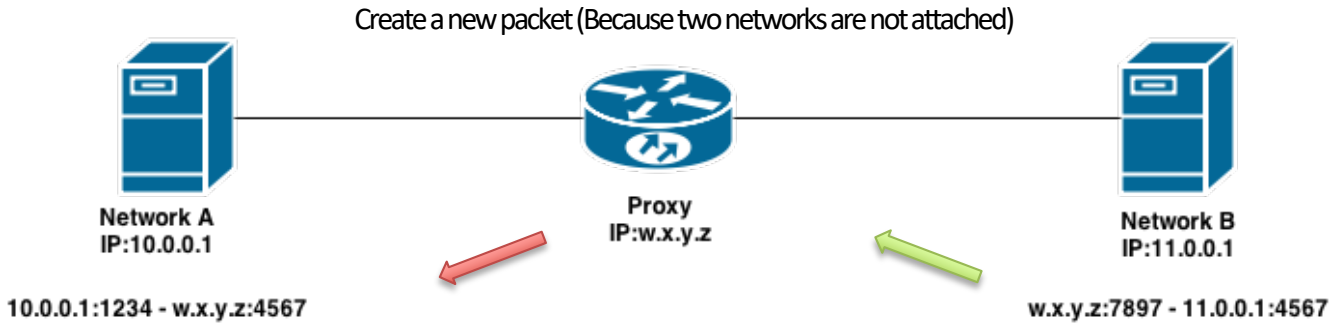
- Router
  - Connects two different networks
  - Does not modify packet addresses



- Network Address Translator (NAT)
  - Exposes a local network via the ports of 1 IP address
  - Modifies packet's IP addresses to effect the mapping

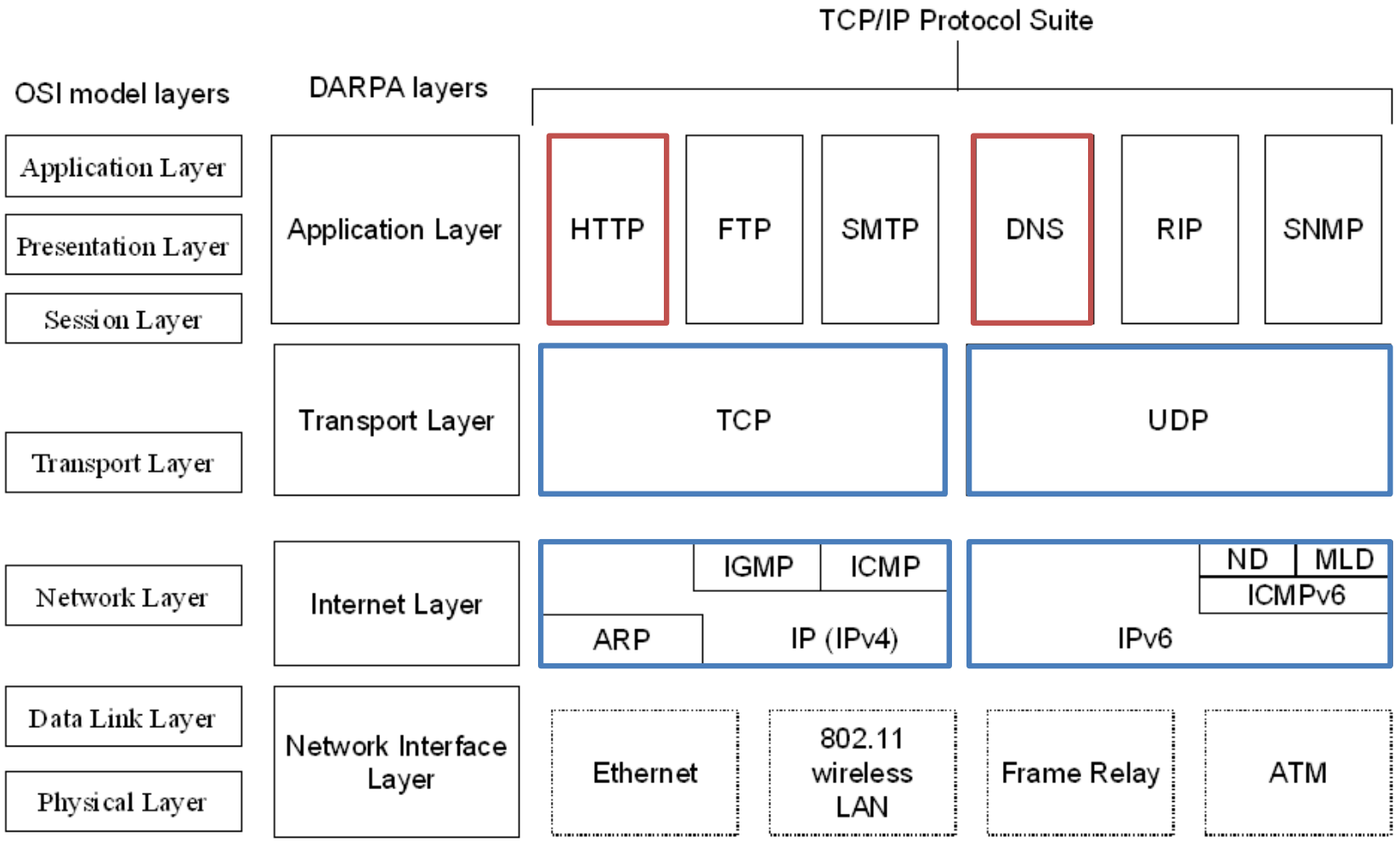


- Proxy
  - A and B communicate to proxy, not directly to each other
  - There are 2 independent packets



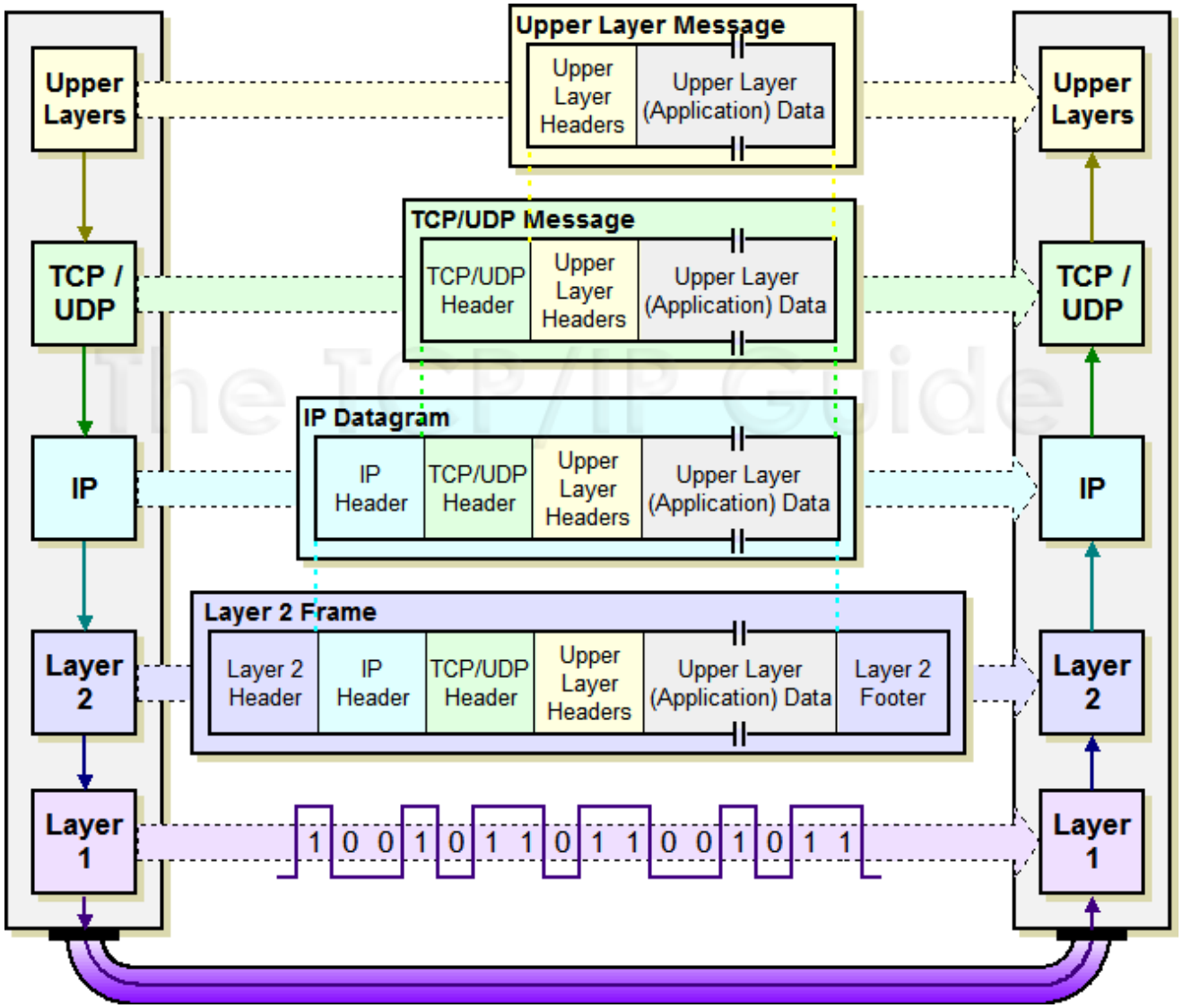
Layers and protocols

Imperial College London



Datagram encapsulation

Imperial College London



Processing at different layers

Imperial College London