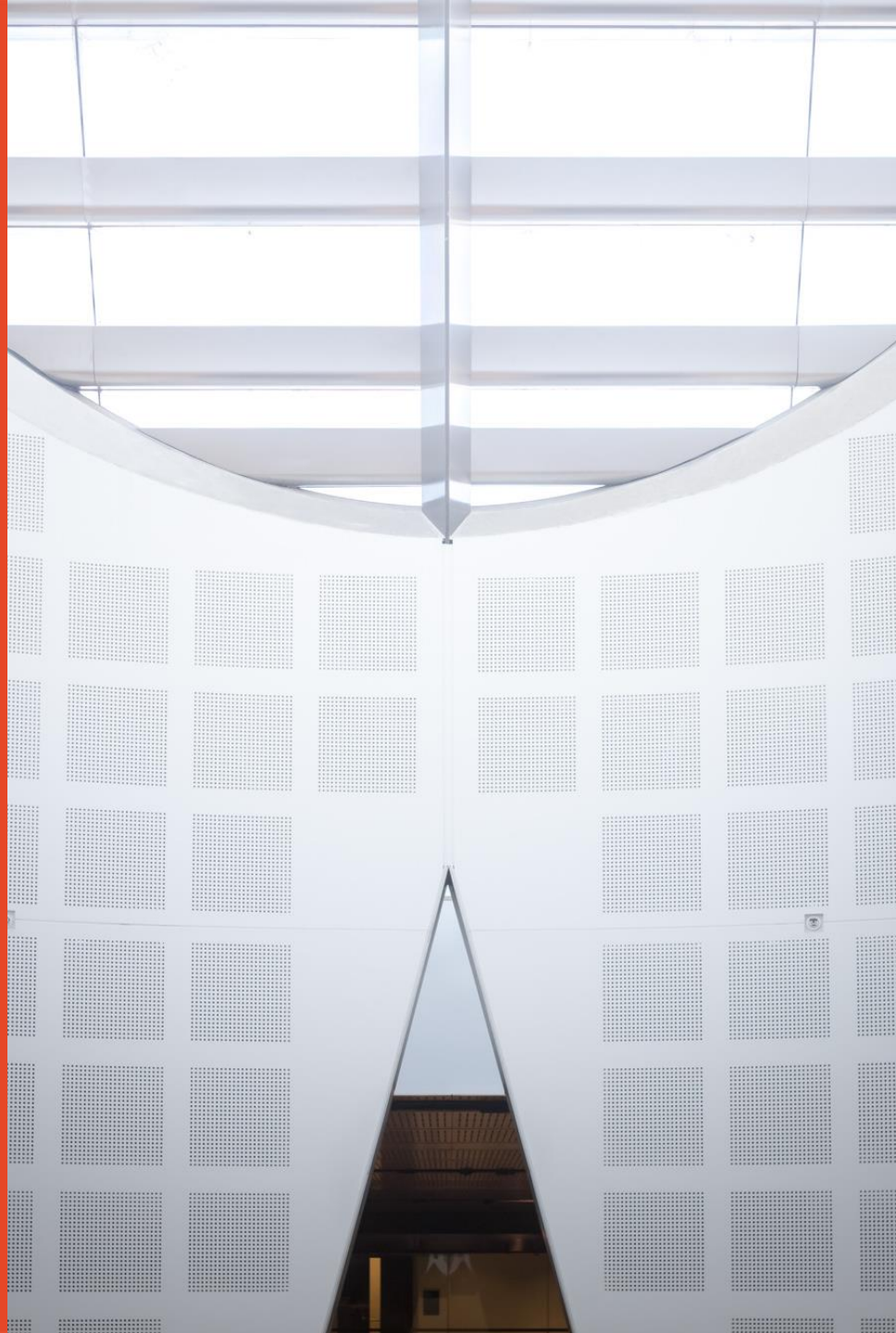
Topic 1.5 Networking Fundamentals

Presented by
Dong YUAN

School of Electrical and Computer Engineering

dong.yuan@sydney.edu.au

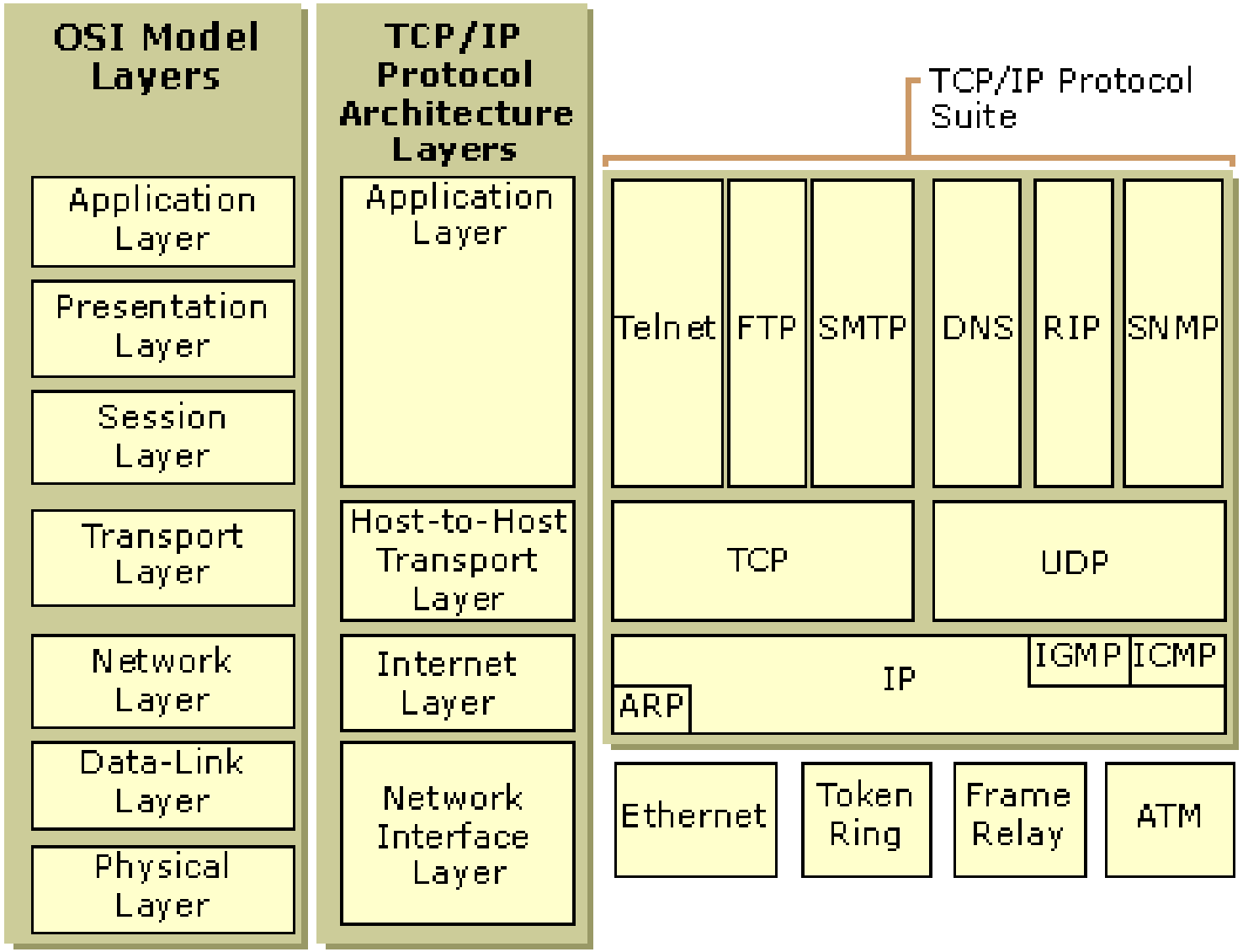
THE UNIVERSITY OF SYDNEY



Contents

- Network Models and Architecture
- Network Devices
- Packet Switching, Routing and TCP/IP

The Internet models



Where is SDN?

ISO OSI reference model

- *Reference model*
  - formally defines what is meant by a layer, a service etc.
- *Service architecture*
  - describes the services provided by each layer and the service access point
- *Protocol architecture*
  - set of protocols that implement the service architecture
  - compliant service architectures may still use non-compliant protocol architectures

Physical layer

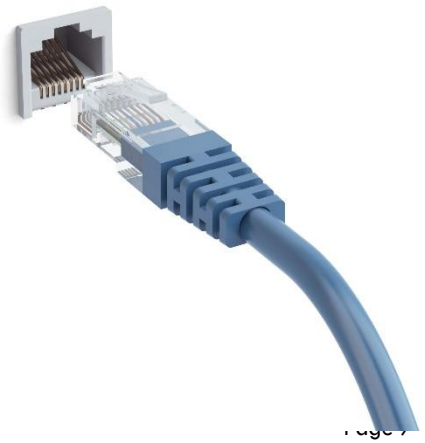
- Moves bits between physically connected end-systems
- Standard prescribes
  - coding scheme to represent a bit
  - shapes and sizes of connectors
  - bit-level synchronization
- Internet
  - technology to move bits on a wire, wireless link, satellite channel etc.

Datalink layer

- (Reliable) communication over a single link.
- Introduces the notion of a *frame*
  - set of bits that belong together
  - *Idle* markers tell us that a link is not carrying a frame
  - *Begin* and *end* markers delimit a frame
- Internet has a variety of datalink layer protocols
  - most common is Ethernet
  - others are FDDI, SONET, HDLC
  - Wireless protocols
- Datalink layer protocols are the first layer of software
- Very dependent on underlying physical link properties
- Usually bundle both physical and datalink in hardware.

Datalink Layer (MAC layer)

- Ethernet
  - Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses, and error-checking data so that damaged frames can be detected and discarded; most often, higher-layer protocols trigger retransmission of lost frames. As per the OSI model, Ethernet provides services up to and including the data link layer.
  - need datalink-layer address
  - also need to decide who gets to speak next
  - these functions are provided by *Medium ACcess sublayer (MAC)*
  - *Up to hundreds of Gbit/s*



Network layer

- Carry data from source to destination.
- Logically concatenates a set of links to form the abstraction of an end-to-end link
- Allows an end-system to communicate with any other end-system by computing a route between them
- Hides idiosyncrasies of datalink layer
- Provides unique network-wide addresses
- Found both in end-systems and in intermediate systems
  - At end-system, hides details of datalink layer
  - At Intermediate system, participate in routing protocol to create routing tables, be responsible for forwarding packets

Network layer

- Internet
  - network layer is provided by Internet Protocol (IP)
  - found in all end-systems and intermediate systems
  - provides abstraction of end-to-end link
  - segmentation and reassembly
  - packet-forwarding, routing, scheduling
  - unique IP addresses
  - can be layered over anything, but only best-effort service

Transport layer

- Reliable end-to-end communication.
- creates the abstraction of an *error-controlled*, *flow-controlled* and *multiplexed* end-to-end link

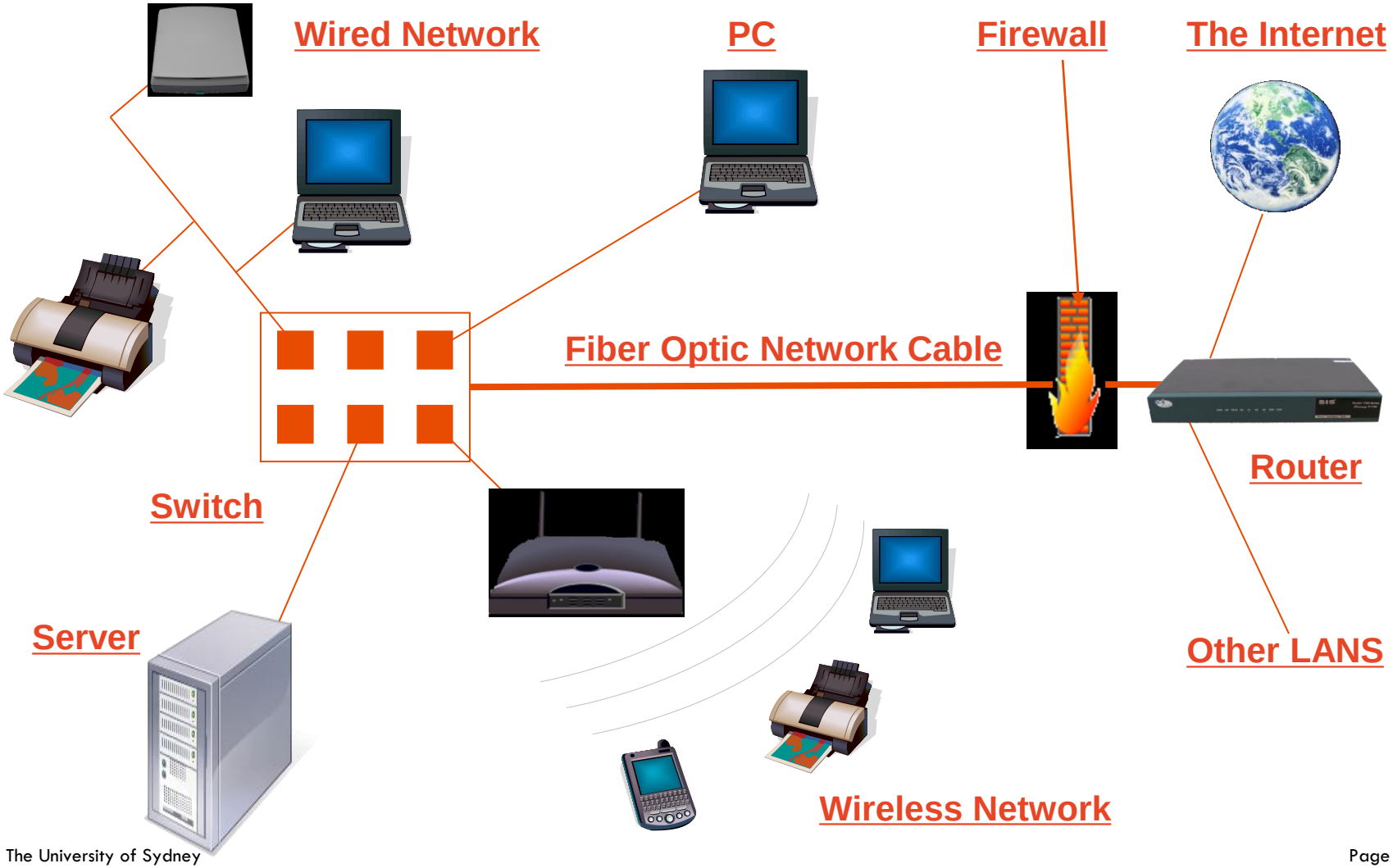
  (Network layer provides only a 'raw' end-to-end service)
- Some transport layers provide fewer services
  - e.g. simple error detection, no flow control, and no retransmission

- Internet
  - TCP provides error control, flow control, multiplexing
  - UDP provides only multiplexing

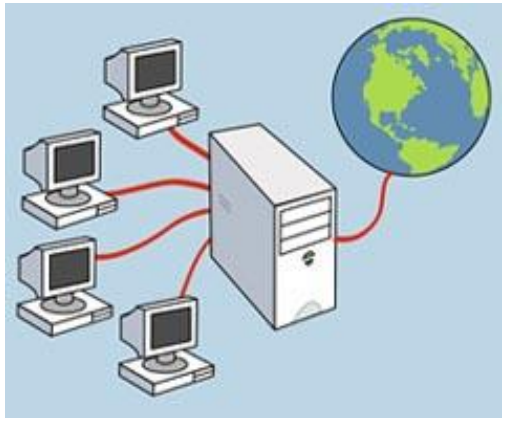
Other layers

- Session layer
  - Provides *full-duplex service, expedited data delivery,* and *session synchronization*
  - Not common
    - Internet doesn't have a standard session layer
- Presentation layer
  - Hides data representation differences between applications
  - Internet has no standard presentation layer
- Application layer
  - The set of applications that use the network
  - Doesn't provide services to any other layer

The Network Diagram

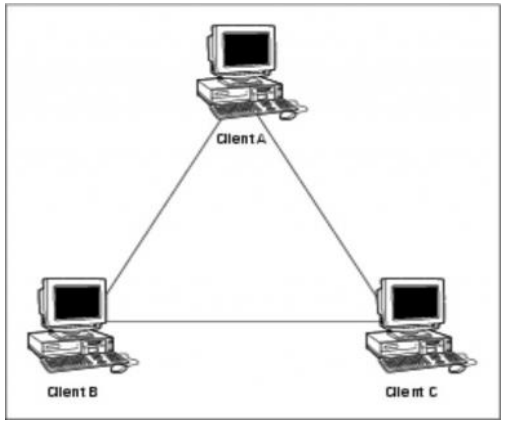


The Three Types of Networks



LOCAL AREA

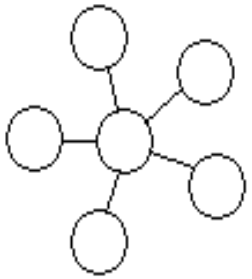
WIDE AREA



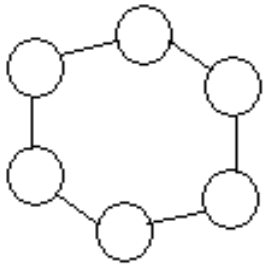
PEER TO PEER

Network Topologies

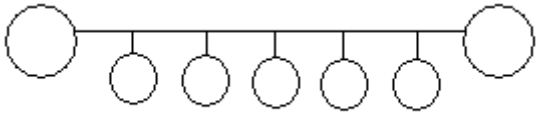
– Network Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate are determined by the network's topology.



Star



Ring



Bus

Contents

- Network Models and Architecture
- Network Devices
- Packet Switching and Routing

Network Devices

- Network Interface Card (NIC)
- Repeater
- Hub
- Bridge
- Switch
- Routers
- Gateway
- Modem

- Can you describe their functions?

Network Interface Card (NIC)

- NIC provides the physical interface between computer and cabling.
- It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.
- The following factors should be taken into consideration when choosing a NIC:
  - Preparing data
  - Sending and controlling data
  - Configuration
  - Drivers
  - Compatibility
  - Performance

Repeater and Bridge

- Repeaters are nothing more than amplifiers and, as such, are very inexpensive.
- Repeaters can only be used to regenerate signals between similar network segments.

- Bridge joins similar topologies and are used to divide network segments.
  - If it is aware of the destination address, it is able to forward packets; otherwise a bridge will forward the packets to all segments. They are more intelligent than repeaters but are unable to move data across multiple networks simultaneously.
- Unlike repeaters, bridges can filter out noise.

Hubs and Switches

- Hubs are devices used to link several computers together.
- A network switch is a computer networking device that connects network segments.
  - Low-end network switches appear nearly identical to network hubs, but a switch contains more "intelligence" (and a slightly higher price tag) than a network hub.
  - Data travels faster through switches because data is not sequenced as it is in a hub
  - The information is more secure when it passes through a switch as opposed to a hub.
  - Information travels more efficiently through a switch because travels directly to it’s destination as opposed to being broadcast to all PC’s on the network hub.

Router and Gateway

- Routers are specialized computers that send your messages and those of every other Internet user speeding to their destinations along thousands of pathways.
  - Routers are crucial devices that let messages flow between networks, rather than within networks.
- Gateway is a passage to connect two networks together that may work upon different networking models.
  - They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than router and switch.

Modem

- A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Repeaters, bridges, routers, and gateways

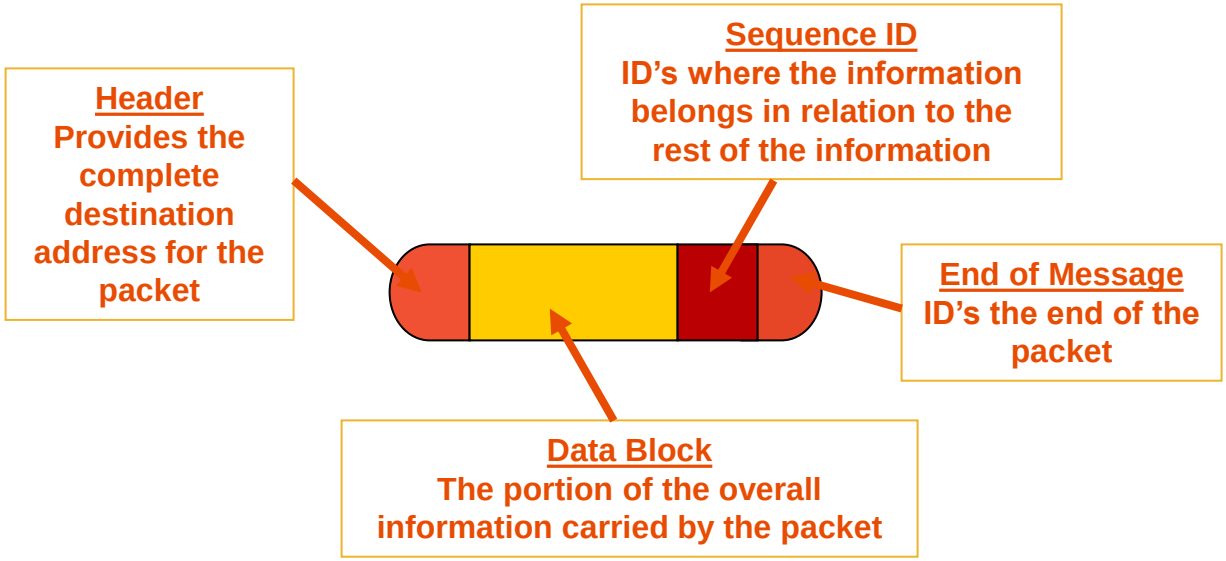
- Repeaters/Hubs: at physical level (L1)
- Bridges/Switch: at datalink level (L2)
  - based on MAC addresses
  - discover attached stations by listening
- Routers/Switch: at network level (L3)
  - participate in routing protocols
- Gateways: at any level (L7)
  - Depending on the requirement
- Gain functionality at the expense of forwarding speed
  - for best performance, push functionality as low as possible

Contents

- Network Models and Architecture
- Network Devices
- Packet Switching and Routing

PACKETS

A page on the Internet—whether it's full of words, images or both—doesn't come to you in one shipment. It's translated into digital information, chopped into 1500 byte pieces called PACKETS, and sent to you like a puzzle that needs to be reassembled. Each part of the packet has a specific function:



Types of switching services

- Packet vs. circuit switches
  - packets have headers
- Connectionless vs. connection oriented
  - connection oriented switches need a call setup
  - setup is handled in *control plane* by *switch controller*
  - connectionless switches deal with *self-contained* datagrams

	Connectionless (router)	*Connection-oriented (switching system)*
Packet switch	Internet router	ATM switching system
Circuit switch	??	Telephone switching system

Packet switching

- The Ethernet (IEEE 802.3) standard transmits data in little chunks called **packets**
- Break long messages into short "packets"
  - Keeps one user from hogging a line
  - Each packet is tagged with where it's going
- Route each packet separately
  - Each packet often takes a different route
  - Packets often arrive out of order
  - Receiver must reconstruct original message

Network Layer: Routing

Goals:

- understand principles behind network layer services:
  - routing (path selection)
  - dealing with scale
  - how a router works
- implementation at scale across the Internet

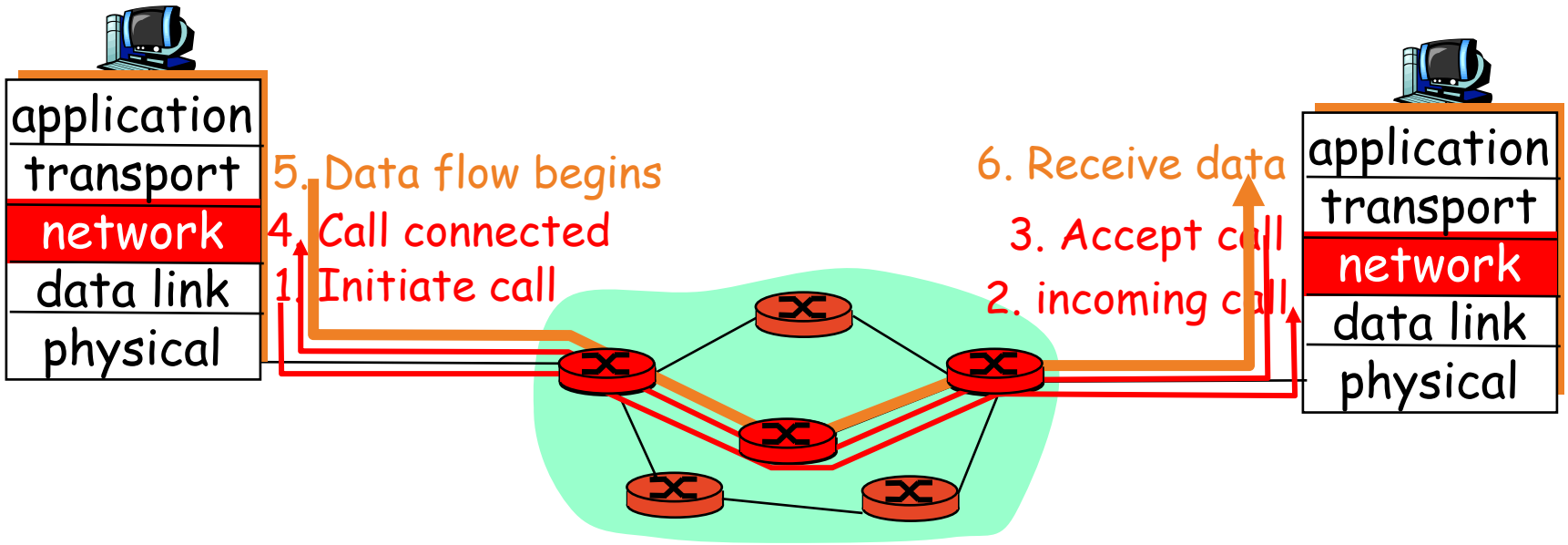
Three important functions:

- *path determination:* route taken by packets from source to dest. *Routing algorithms*
- *switching:* move packets from router's input to appropriate router output
- *call setup:* some network architectures require router call setup along path before data flows

Virtual Circuits (VC) – ATM

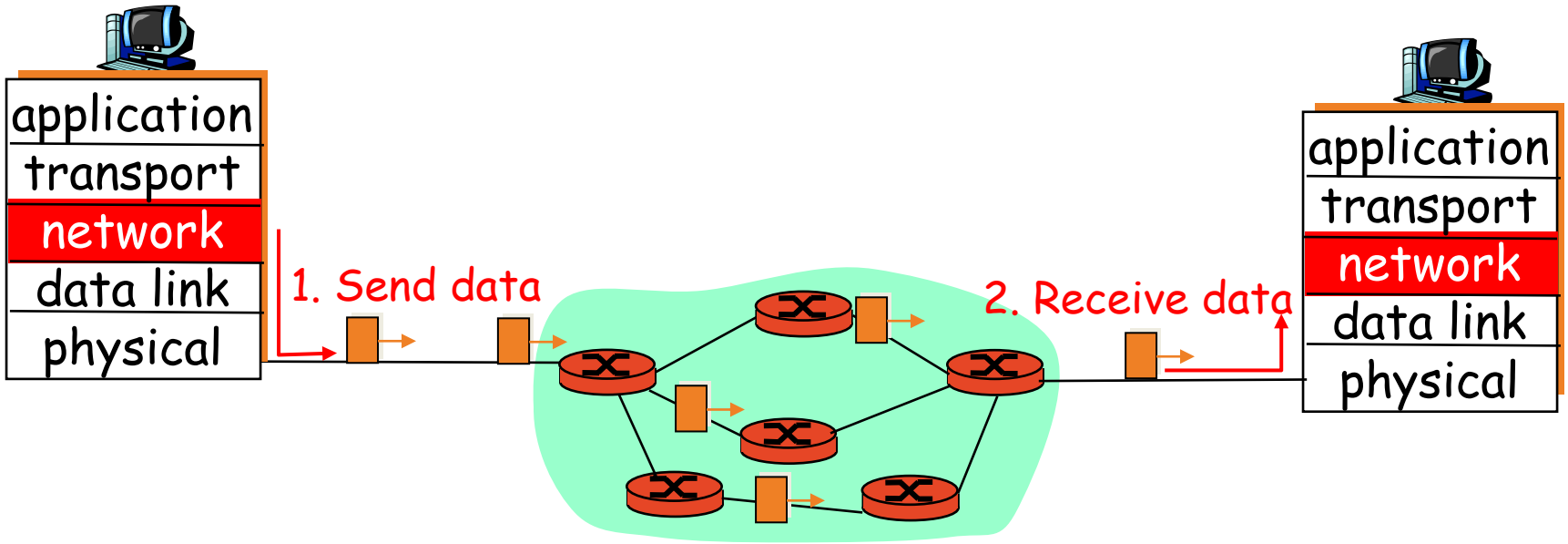
"source-to-dest path behaves much like telephone circuit"

- performance-wise (bandwidth reserve)
- network actions along source-to-dest path



Datagram networks: the Internet model

- No call setup at network layer
- Routers: no state about end-to-end connections
  - no network-level concept of "connection"
- Packets typically routed using destination host ID
  - packets between same source-dest pair may take different paths



Datagram or VC network

Internet (Datagram)

- data exchange among computers
  - "elastic" service, no strict timing req.
- "smart" end systems (computers)
  - can adapt, perform control, error recovery
  - simple inside network, complexity at "edge"
- many link types
  - different characteristics
  - uniform service difficult

ATM (VC)

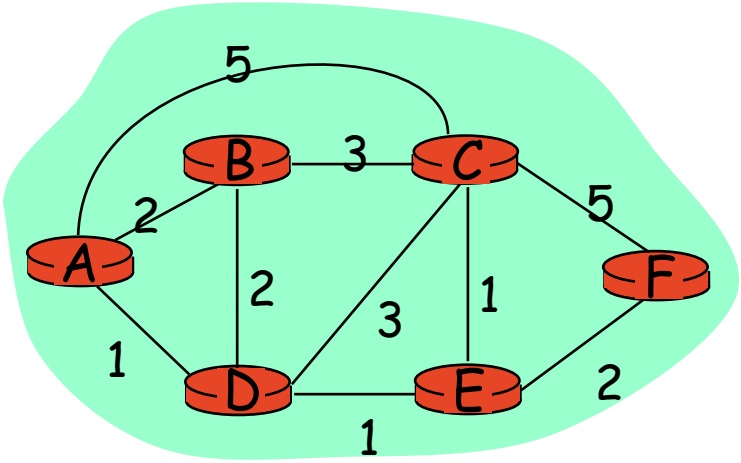
- evolved from telephony
- human conversation:
  - strict timing, reliability requirements
  - need for guaranteed service
- "dumb" end systems
  - telephones
  - complexity inside network
- VC Benefits:
  - Fast forwarding
  - Traffic Engineering.

Routing

Goal: determine "good" path (sequence of routers) thru network from source to dest.

Graph abstraction for routing algorithms:

- graph nodes are routers
- graph edges are physical links
  - link cost: delay, $ cost, or congestion level



"good" path:

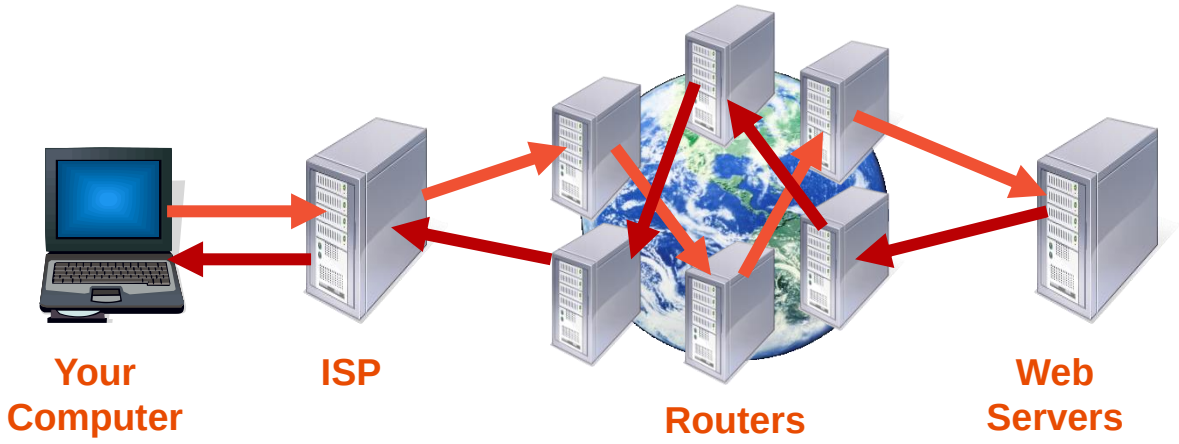
typically means minimum cost path

other def's possible

How Information Travel Through the Internet

When you connect to a Web site through an ISP and start exchanging information, there isn't a fixed connection between your computer and the Web server computer hosting the Web site.

Instead, information is exchanged using the best possible path at that particular time. Special computers called routers determine these paths, avoiding slow links and favouring fast ones.



Intranet and Internet Specifications

- ***Intranet:*** An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network.
- An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet.
- ***Internet:*** is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

Important protocols in TCP/IP stack

TCP/IP – UPD/IP

- TCP stands for **Transmission Control Protocol**

  TCP software breaks messages into packets, hands them off to the IP software for delivery, and then orders and reassembles the packets at their destination

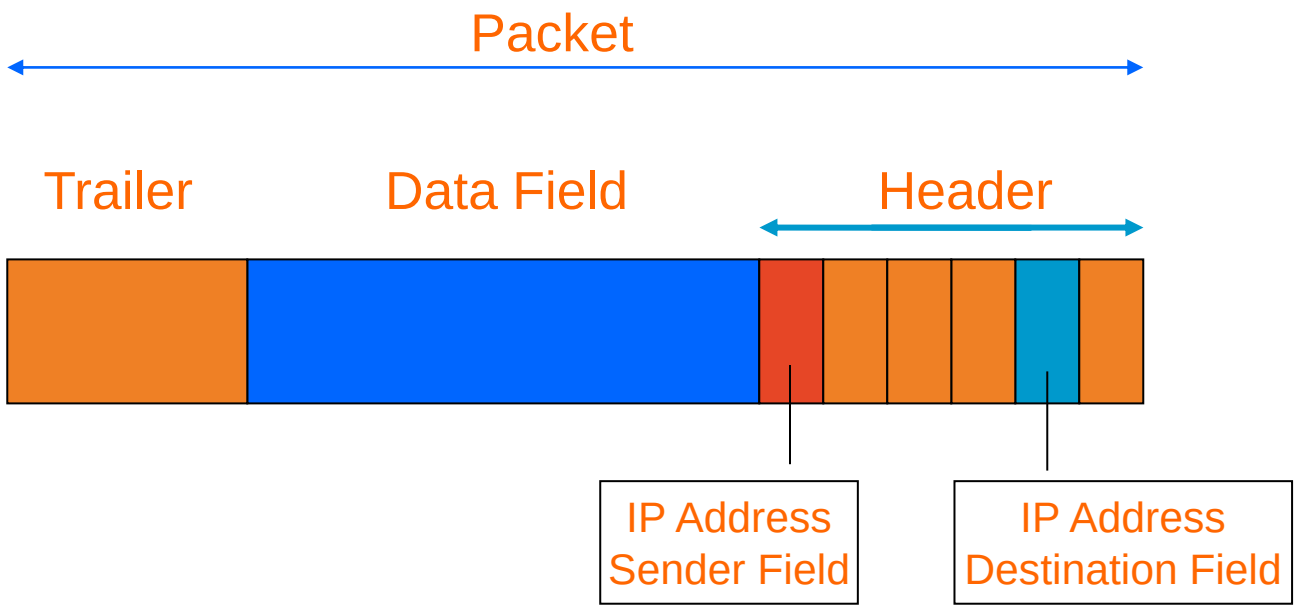
- IP stands for **Internet Protocol**

  IP software deals with the routing of packets through the maze of interconnected networks to their final destination

- UDP stands for User Datagram Protocol
  - It is an alternative to TCP
  - The main difference is that TCP is highly reliable, at the cost of decreased performance, while UDP is less reliable, but generally faster

A TCP/IP network packet

– Here is the basic structure of any one of trillions of packets traversing the Internet at this moment



Internet Protocol

- IP is the network layer
  - packet delivery service (host-to-host).
  - translation between different data-link protocols
  - IP addresses are *logical* addresses (not physical), that include a network ID and a host ID.
  - Every host must have a unique IP address.

- IP provides connectionless, unreliable delivery of *IP datagrams*.
  - *Connectionless*: each datagram is independent of all others.
  - *Unreliable*: there is no guarantee that datagrams are delivered correctly or even delivered at all.

Mapping IP Addresses to Hardware Addresses

- IP Addresses are not recognized by hardware.
- If we know the IP address of a host, how do we find out the hardware address ?
- The process of finding the hardware address of a host given the IP address is called

Address Resolution

ARP

- The *Address Resolution Protocol* is used by a sending host when it knows the IP address of the destination but needs the Ethernet (or whatever) address.
- ARP is a broadcast protocol - every host on the network receives the request.
- Each host checks the request against it's IP address - the right one responds.
- hosts *remember* the hardware addresses of each other.

ICMP- *Internet Control Message Protocol*

- ICMP is a protocol used for exchanging control messages.
- ICMP uses IP to deliver messages.
- ICMP messages are usually generated and processed by the IP software, not the user process.

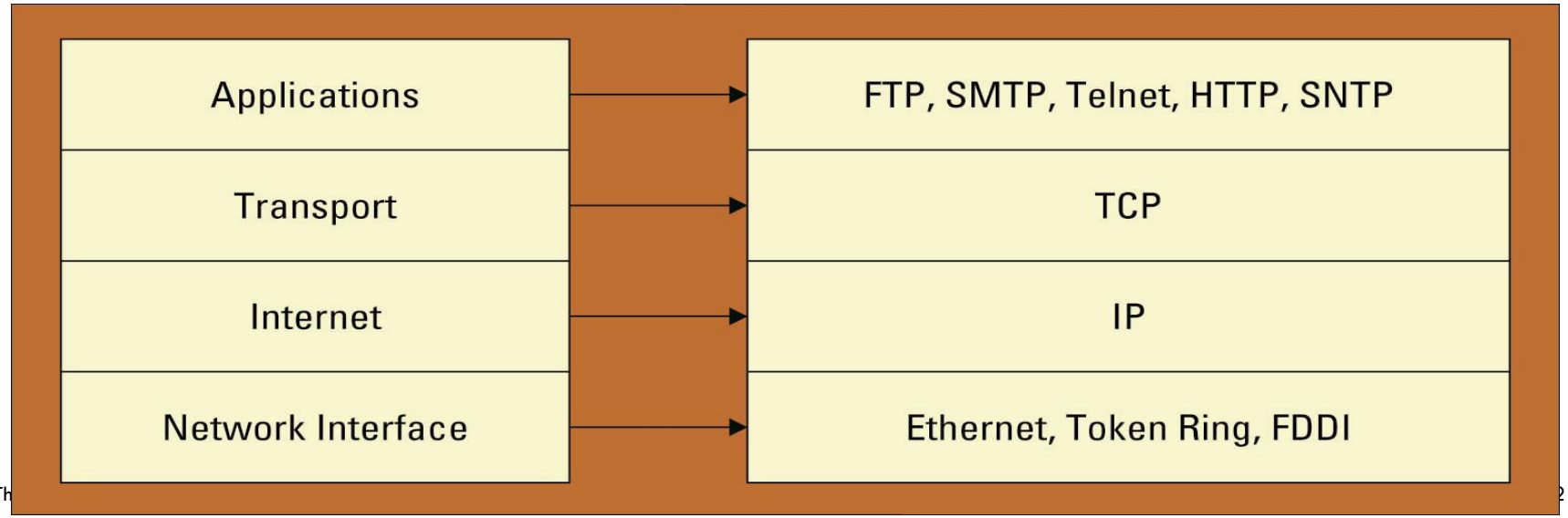
- If packets arrive too fast - the receiver discards excessive packets and sends an ICMP message to the sender.
- If an error is found (header checksum problem) the packet is discarded and an ICMP message is sent to the sender.

TCP - *Transmission Control Protocol*

- TCP is an alternative transport layer protocol supported by TCP/IP.
- *Connection oriented* – A virtual connection is established before any user data is transferred.
  - If the connection cannot be established, the user program is notified (finds out).
  - If the connection is ever interrupted, the user program(s) is finds out there is a problem.
- *Reliable* – Every transmission of data is acknowledged by the receiver.
  - Reliable does not mean that things don't go wrong, it means that we find out when things go wrong.
  - If the sender does not receive acknowledgement within a specified amount of time, the sender retransmits the data.

TCP/IP

- TCP/IP provides the technical foundation for the public Internet as well as for large numbers of private network. It is defined in terms of layers.
- Do you use TCP/IP ?
  - If you are on the Internet, yes, you are using TCP/IP.
- TCP/IP layers (at left, with particular implementations at right)

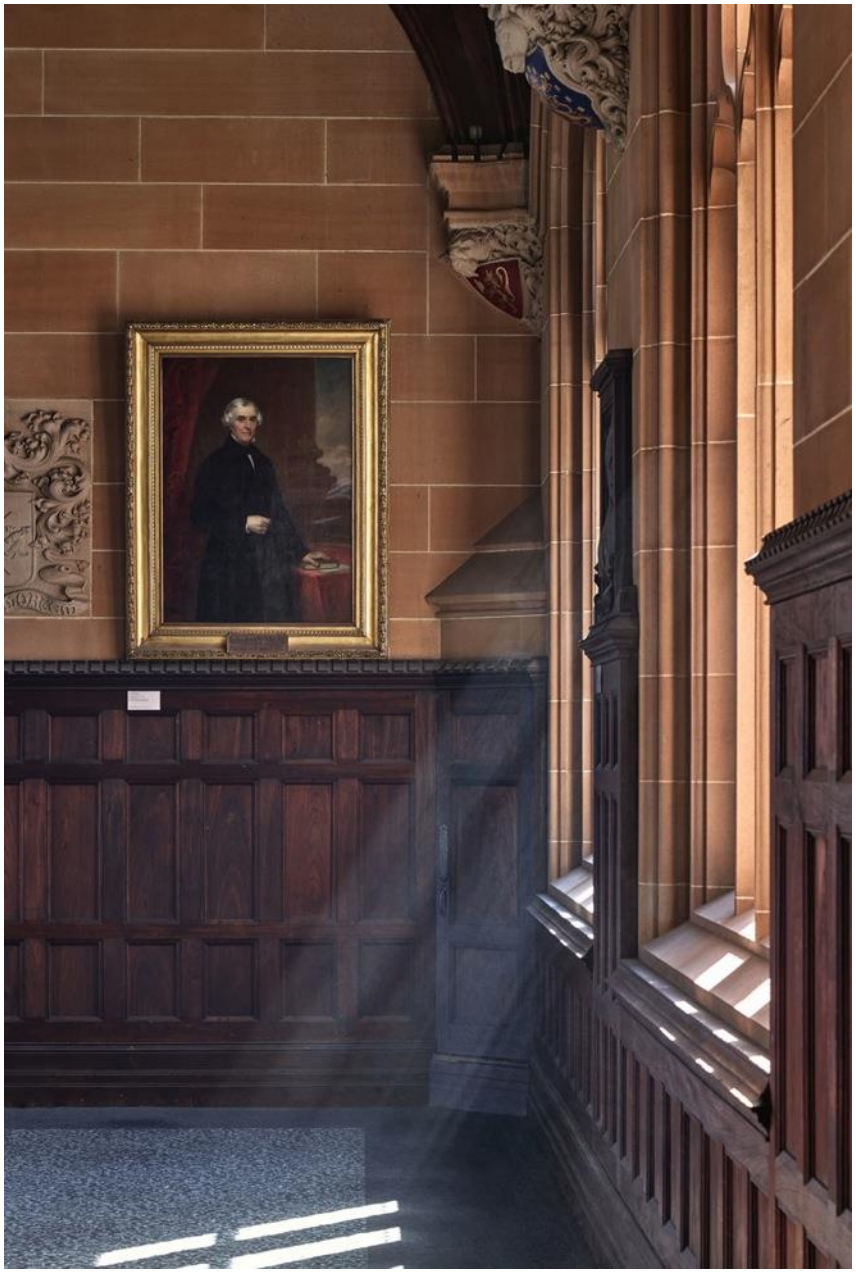


Problems in TCP/IP

- Built for the wide area
- Congestion control
- Security
- Etc.

Thank you!

End



THE UNIVERSITY OF SYDNEY