Module Two

CSG1105 Applied Communications

What is an IP address?

- Consider an international phone number. Phone numbers are not really numbers, they're a code to direct where a call must go, a process called *routing*.
- If I want to call a number in the United Kingdom in the County of Ledbury. First, I must give a code to tell the phone that the number is an international number, that code is 0011.
- I then need to use the national prefix for the United Kingdom which is 44.
- Next, I need to use the access code or area code for the County of Ledbury which is 01531
- I need to give the actual phone number which corresponds to the handset for the person that I wish to speak to e.g. 632306 which is the Ledbury Town Council. 0011-44-1531-632306.

IPv4 Addresses

- IP is short for Internet Protocol, the mechanism for delivering content on the Internet
- There are currently **two** IP address systems, IPv4 and IPv6. We will look at IPv6 later in the unit. For the moment, when the term “IP address” is used, assume that it is an IPv4 address.
- IP addresses are 32-bit numbers that have a similar purpose to phone numbers and have a simple structure to direct where the data must be sent.
- The network portion identifies the target network and the host portion identifies the target device.
- Consider the IP address 192.168.1.205
- Network Portion, Host Portion

Network routing

- When we considered the phone system, there were multiple levels of addressing: country, region or network provider, local region etc.
- This means that it is easy to direct a call to the correct landline subscriber, no matter their location (mobiles add complexity to this)
- IPv4 addressing was designed in the 1970's to link large computer systems owned by the US government and research institutions
- IPv4 addressing has no hierarchy inbuilt in the address, meaning that routing devices need to how to reach all other networks

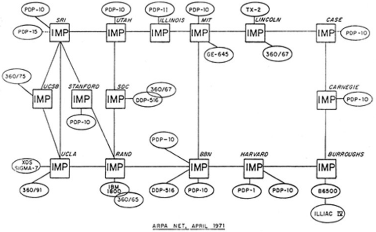


Figure 1: ARPANet 1971

Dotted-Decimal 1

- IP addresses are 32 bit numbers
- This allows ~ 4.3 billion unique values 0 -> 4,294,967,295 ($2^{32} - 1$)
- We will see later that
  1. The addressing scheme reduces this range
  2. We've run out of IPv4 addresses (cross-reference CIDR, NAT & IPv6) as there are many more than 4.3 billion devices connected to the Internet (computers, phones, IoT devices etc.).
- The address 192.168.1.205 is a **dotted decimal** representation which is more readable than 3232235981 (decimal) or 0xC0A801CD (hexadecimal)
- In many browsers, you can use decimal and hexadecimal are valid values in URLs
- http://3232235981, http://0xC0A801CD and http://192.168.1.205 are all the same

Dotted-Decimal 2

- Dotted decimal is where the 32 bit number is divided into four 8 bit **bytes**
- The number 3232235981 in decimal is **11000000101010000000000111001101** In binary
- Divide into bytes 11000000101010000000000111001101
- Convert to decimal and separate with dots 192.168.1.205
- Earlier we saw the IP address 192.168.1.205 divided into network and host portions
- In that example, three bytes (24 bits) was the network address and 1 byte (8 bits) was the host address
- The network address is **not** always 24 bits, nor is is always on a byte aligned boundary

Interlude - A review of the Binary numbering System

- Convert 205 to binary by subtracting highest power of 2
  - Subtract 128 from 205 leaving 77 and place ‘1’ in the 2^7 column
  - Subtract 64 from 77 leaving 13 and place ‘1’ in the 2^6 column
  - Can’t subtract 32 from 13, place ‘0’ in the 2^5 column
  - Can’t subtract 16 from 13, place ‘0’ in the 2^4 column
  - Subtract 8 rom 13 leaving 5 and place ‘1’ in the 2^3 column
  - Subtract 4 from 5 leaving 1 and place ‘1’ in the 2^2 column
  - Can’t subtract 2 from 1, place ‘0’ in the 2^1 column
  - Subtract 1 from 1 leaving 0 and place ‘1’ in the 2^0 column

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	0	0	1	1	0	1

Interlude - A review of the Binary numbering System

- Convert 10101000 to decimal by adding powers of two

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

$$= 1 \text{ x } 2^7 + 0 \text{ x } 2^6 + 1 \text{ x } 2^5 + 0 \text{ x } 2^4 + 1 \text{ x } 2^3 + 0 \text{ x } 2^2 + 0 \text{ x } 2^1 + 0 \text{ x } 2^0$$

$$= 1 \text{ x } 128 + 0 \text{ x } 64 + 1 \text{ x } 32 + 0 \text{ x } 16 + 1 \text{ x } 8 + 0 \text{ x } 4 + 0 \text{ x } 2 + 0 \text{ x } 1$$

$$= 168$$

The Subnet Mask 1

- The subnet mask (or net mask) is a value that allows us to separate the network address from the host address
- It is a 32 bit value that is AND'ed with the IP address
- The AND operator outputs TRUE (or 1) only when both inputs are TRUE.
- The following is a Truth table for AND.

a	b	a AND b
0	0	0
0	1	0
1	0	0
1	1	1

The Subnet Mask 2

- Our previous example had 24 bits of network address and eight bits of host address 192.168.1.205
- Converted to binary 11000000.10101000.00000001.11001101
- This therefore uses a Subnet mask of 255.255.255.0
- Converted to binary 11111111.11111111.11111111.00000000
- Perform the AND to give the network address

11000000	10101000	00000001	11001101
11111111	11111111	11111111	00000000
11000000	10101000	00000001	00000000

- Network address - 192.168.1.0

The Subnet Mask 3

- Use the wildcard (the subnet mask with all bits inverted) to get the host address

11000000	10101000	00000001	11001101
00000000	00000000	00000000	11111111
00000000	00000000	00000000	11001101

- Host ID 205

Connection Models

- Now that we understand how to find the network address, how is it used?
- Early networks used **Circuit Switching**
- Modern networks use **Packet Switching**
- IP Networks like the Internet use Packet Switching

Circuit Switching 1

- Based on the original fixed-line phone system
- Each subscriber had a connection to the local exchange which labelled that connection with a number
- To make a call, the subscriber would lift the handset and a light would appear against their number at the local exchange
- An operator at the exchange would plug a headset into that connection and ask what number was required
- If it was a number on the local exchange, the operator would connect a cord between the two connections. When one user hung up, the light would go out and the cord was removed
- If it was a number on a remote exchange, the operator would connect the user to the next exchange
- A long-distance call could require multiple operators being contacted and each establishing a link from one exchange to the next

Circuit Switching 2

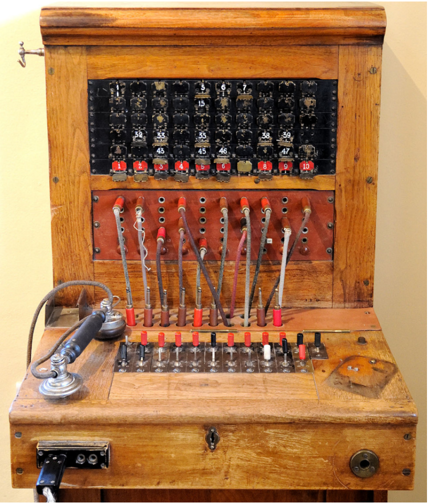


Figure 2: Old Phone Exchange

Circuit Switching 3

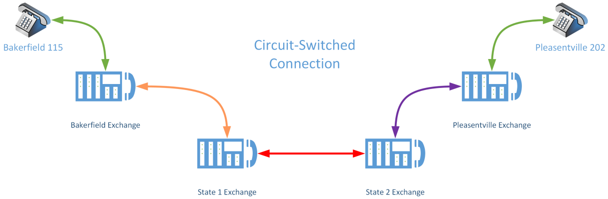


Figure 3: Circuit Switching

- Operators were later replaced by automatic exchanges
- One of the issues with circuit switching is that only a single connection can exist at a time
- If one subscriber stays on the line for a long period, they cannot be contacted by other callers
- Any other person in the residence wishing to make a call will have to wait until the caller finishes (this pre-dates mobile phones and the Internet)

Multiplexing

- Phone carriers needed to maximise the use of trunk lines between exchanges
- One way was to have several conversations happening on a single cable
- A simple method for achieving this was Time Division Multiplexing
- Multiple connections would be given short duration access to the trunk
- To each user, the sound appeared continuous
- This was an **analog** technique for a single cable
- Each of the individual subscribers still could only have a single connection

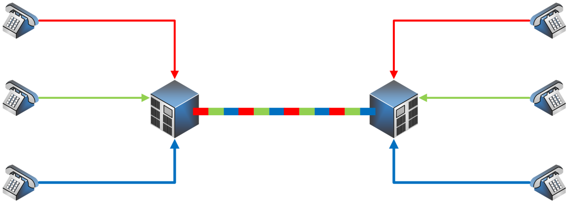


Figure 4: Time Division Multiplexing

Interlude - Analog and Digital

- The telephone network operated by converting sound to electrical pulses using analog signalling. Analog signals vary continuously over time.

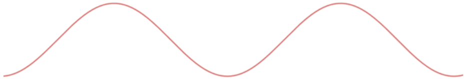


Figure 5: analog

- Computer systems use digital signalling where values are discrete ones and zeros.

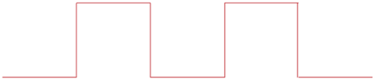


Figure 6: digital

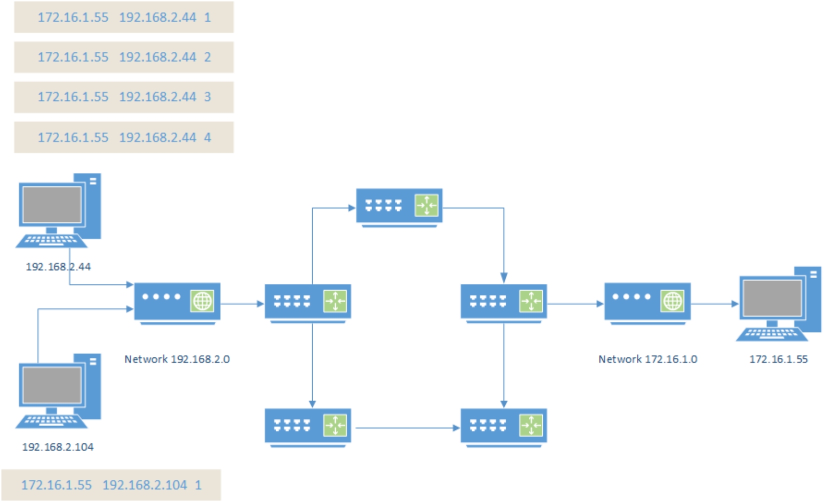
Packet Switching 1

- Packet switching is a **Digital** technique that may be used over multiple connections
- Like Multiplexing, it allows multiple messages to be transmitted over the same link
- Messages are divided up into fragments called **Packets** that may sent independently of one another
- A short message may be interleaved with the packets of a longer message
- Each Packet contains a Destination Address and a Source address
- The destination address is used by each node in the network to make a routing decision
- Each also needs to contain information to rebuild the message when it is received

An Analogy

- You are an technophobic author who is sending your printed manuscript (a book in the making) to your editor.
- To save costs, you snail-mail each chapter in a separate envelope
- Each chapter has a chapter number as well as page numbers
- This allows each chapter and page to be reassembled in the correct order
- Any missing chapters/pages will be noted by the editor who can ask for them to be resent
- The post office reads the post code to forward each envelope to the state mail exchange of the destination
- The state mail exchange will forward each envelope to the post office in charge of a post code
- The post office will assign the delivery of each envelope to a delivery agent who uses the street address complete the delivery
- The system can handle mail from multiple sources in the same transport as each has its own address for final delivery

Packet Switching 2



172.16.1.55 192.168.2.44 1

172.16.1.55 192.168.2.44 2

172.16.1.55 192.168.2.44 3

172.16.1.55 192.168.2.44 4

192.168.2.44

Network 192.168.2.0

Network 172.16.1.0

172.16.1.55

192.168.2.104

172.16.1.55 192.168.2.104 1

Figure 7: Packet Switching

Network Reference Models

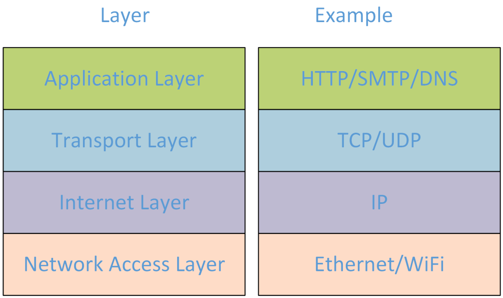
- So far we have talked about URLs, DNS, Client/Server and IP Addresses
- We need a way of expressing the relationship of various components of a networking architecture
- Network models are a way of comprehending the complexity of the process of communication across a network.
- It also provides a modular architecture that may allow the substitution of one implementation of a layer with an alternate implementation without altering the interface to the layer above.
- In the last 50 years, there have been many models in use, may of which were proprietary (SNA,DNA)
- The dominant models in use today are **ISO/OSI** (which will be covered later) and **TCP/IP**. Both of these are Open Standards.

The TCP/IP Model

- We have already been introduced to IP, the Internet Protocol and the concept of packet switching
- The IP is analogous to the envelope in a previous slide
- TCP, the **Transmission Control Protocol**, is the mechanism that ensures all parts of the message are received by the correct application and in the correct order [1]
- We also need a mechanism for delivering Packets from node to node through the network
- TCP, IP, the delivery mechanism, and a number of application protocols like DNS are collectively called the **TCP/IP Protocol Suite**

[1] TCP does quite a bit more that we will cover later

The TCP/IP Stack



Layer	Example
Application Layer	HTTP/SMTP/DNS
Transport Layer	TCP/UDP
Internet Layer	IP
Network Access Layer	Ethernet/WiFi

Figure 8: TCP/IP Stack

Peer Layer Communication 1

- Each layer provides services to the layer above and uses the services of the layer below
- A message constructed in the application layer will be passed to the Transport layer for segmentation
- The segments will be passed to the Internet layer for routing as packets
- The packets will be passed to the network access layer for local delivery in frames to the next routing node
- The network access layer will also convert the bits making up the frame into a signalling format suitable for the medium connecting to the next routing node
- When the message is received by the destination, it moves up through each of the layers to the target application
- This is the **Physical** path the message takes
- **Logically**, each layer communicates with the peer layer a the target system

Peer Layer Communication 2

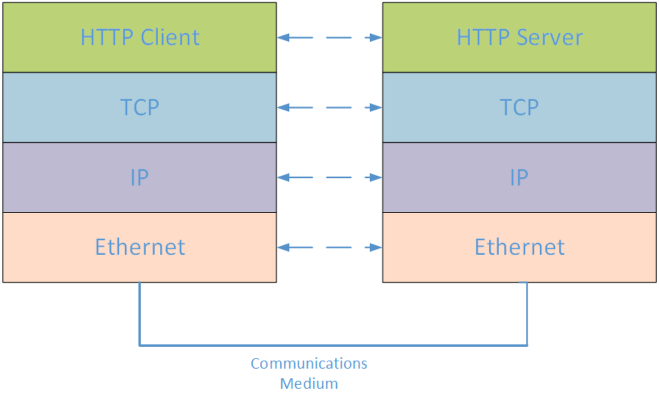
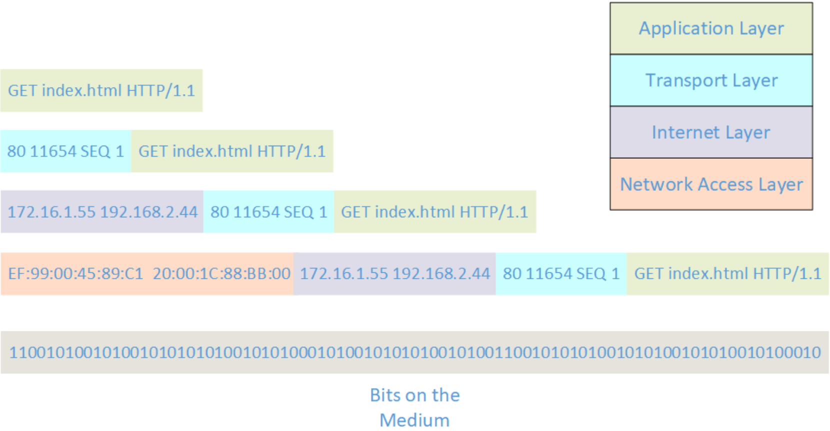


Figure 9: Peer Layer Communication

Encapsulation 1

- Each layer will add a header to the message containing information pertinent to that layer's function
- This process is called **Encapsulation**
- At each node, the receiving device will interpret the headers of the Network Access Layer and as necessary remove and replace them before forwarding a message to the next node
- At the destination, the message is passed up the Network stack and each layer removes it's header before passing the message upwards
- This process is call **De-encapsulation**

Encapsulation 2



Application Layer

Transport Layer

Internet Layer

Network Access Layer

GET index.html HTTP/1.1

80 11654 SEQ 1 GET index.html HTTP/1.1

172.16.1.55 192.168.2.44 80 11654 SEQ 1 GET index.html HTTP/1.1

EF:99:00:45:89:C1 20:00:1C:88:BB:00 172.16.1.55 192.168.2.44 80 11654 SEQ 1 GET index.html HTTP/1.1

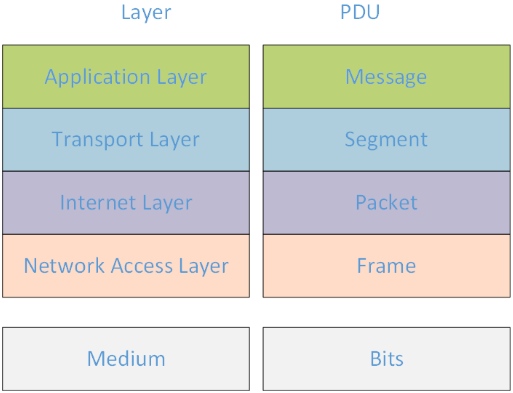
110010100101001010101010010101000101001010101001010011001010101001010100101010010100010

Bits on the
Medium

Figure 10: Encapsulation

Protocol Data Units (PDUs)

- The data structure constructed by each layer has a specific name
- Generically, they are called PDUs (Protocol Data Units)



Layer	PDU
Application Layer	Message
Transport Layer	Segment
Internet Layer	Packet
Network Access Layer	Frame
Medium	Bits

Figure 11: PDUs