Temasek Junior College

2024 JC2 H2 Computing

Networking 4 – Network Protocols

1 The Need for Communication Protocol

A protocol is a set of rules for data transmission which are agreed by both sender and receiver. These rules need to be standard across all devices in order for these devices to communicate with each other.

At the simplest level, a protocol could define that a positive voltage represents a bit of value 1. At the other extreme, a protocol could define the format of the first 40 bytes in a packet.

The protocol determines the following:

- the type of error checking to be used
- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message

There are a variety of standard protocols from which programmers can choose. Each has advantages and disadvantages; for example, some are simpler than others, some are more reliable, and some are faster.

From a user's point of view, the only interesting aspect about protocols is that your computer or device must support the right ones if you want to communicate with other computers. The protocol can be implemented either in hardware or in software.

Protocol Suite

A protocol suite refers to a collection of related protocols that are designed to work together. Each protocol in a suite handles one aspect of communication; together, the protocols in a suite cover all aspects of communication, including hardware failures and other exceptional conditions.

The Internet Protocol suite is the standard network model and communication protocol stack used on the Internet and on most other computer networks. The predominant one is the Transmission Control Protocol / Internet Protocol (TCP/IP)

2 TCP/IP Protocol Suite

A collection of protocols that are used on the Internet. The protocol suite is named after two of the most common protocols – **TCP** (Transmission Control Protocol) and **IP** (internet Protocol). Before TCP/IP became the de-facto standard other protocol suites like IPX and SPX were common (Novell).

2.1 Layering Architecture

The fundamental abstraction used to collect protocols into a unified whole is known as a layering model. A layering model describes how all aspects of a communication problem can be partitioned into pieces that work together. Each piece is known as a layer; the terminology arises because protocols in a suite are organized into a linear sequence.

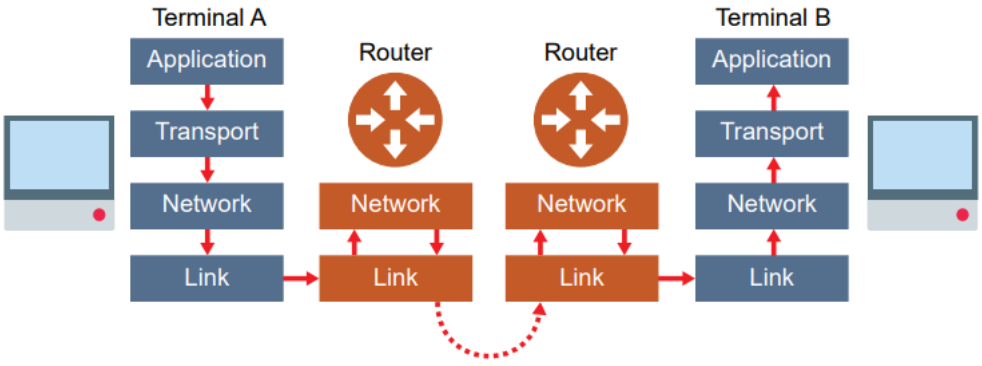
- Reasons for Layering:
  1. Simplifies the network model enabling programmers to specialise in a particular level or layer of the networking model.
  2. It provides design modularity.
  3. Allows for standardised interfaces to be produced by networking vendors.
  4. Encourages interoperability.

The Transmission Control Protocol / Internet Protocol (TCP/IP) protocol stack is a set of networking protocols that work together as four connected layers, passing incoming and outgoing data packets up and down the layers during network communication.

The four layers are:

- Application Layer
- Transport Layer
- Internet (Network) Layer
- Link (Network Interface) Layer

Note that some textbooks consider the TCP/IP stack to have 5 layers: Physical, Link, Internet (Network), Transport and Application layers.



2.1.1 Layer 4 – Application Layer

The application layer sits at the top of the stack and uses protocols relating to the application being used to transmit data over a network.

Examples are HTTP & FTP (web-based), POP3 & SMTP (Email), SSL & TLS (Security) and SNMP (Network Management).

Imagine the following text data is to be sent via a browser using the Hypertext Transfer Protocol (HTTP):

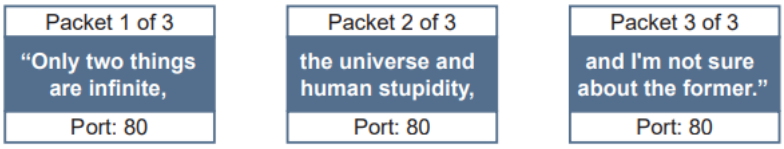
> **"Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."**
> *Albert Einstein*

2.1.2 Layer 3 – Transport Layer

The transport layer transports application-layer messages between application endpoints. In the Internet there are two transport protocols, TCP and UDP, either of which can transport application layer messages.

In this example, the transport layer uses the Transmission Control Protocol (TCP) to establish an end-to-end connection with the recipient computer. The data is then split into packets and labelled with the packet number, the total number of packets and the port number through which the packet should route. This ensures it is handled by the correct application on the recipient computer. In the example below, port 80 is used as this is a common port used by the HTTP protocol, called upon by the destination browser.

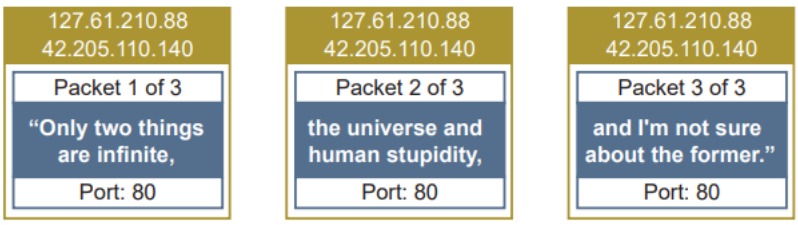
If any packets go astray during the connection, the transport layer requests retransmission of lost packets. Receipt of packets is also acknowledged.



2.1.3 Layer 2 – Internet (Network) Layer

The Internet (or Network) layer transports data packets (datagrams) across network boundaries from one host to another. Possible Internet layer include IP, ICMP & IGMP.

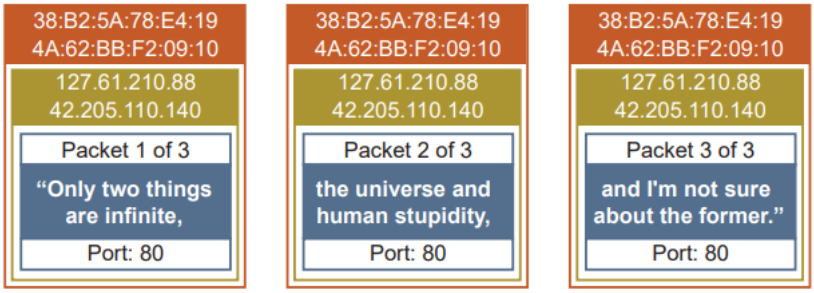
The Internet layer adds the source and destination IP addresses. Routers operate on the network layer and will use these IP addresses to forward the packets on to the destination. The addition of an IP address to the port number forms a socket, e.g. 42.205.110.140:80, in the same way that the addition of a person's name is added to a street address on an envelope in order to direct the letter to the correct person within a building. A socket specifies which device the packet must be sent to and the application being used on that device.



2.1.4 Layer 1 – Link (Network Interface) Layer

The Link (or Network Interface) Layer contains the physical/logical network components used to interconnect hosts or nodes in a network. Examples include ISDN, Ethernet, ATM, Wi-Fi, 4G, satellite or fibre.

The link layer is the physical connection between network nodes and adds the unique Media Access Control (MAC) addresses identifying the Network Interface Cards (NICs) of the source and destination computers. This means that once the packet finds the correct network using the IP address, it can then locate the correct piece of hardware. The destination MAC address is that of the device that the packet is being sent to next. Unless the two computers are on the same network, the destination MAC address will initially be the MAC address of the first router that the packet will be sent to.



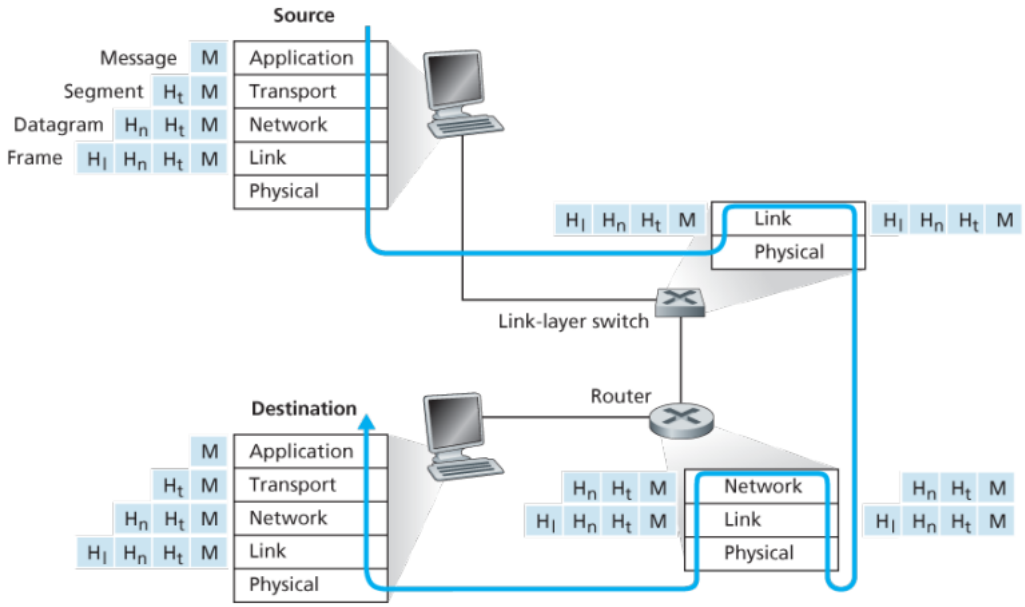
At the receiving end, the MAC address is stripped off by the link layer, which passes the packets on to the network layer. The IP addresses are then removed by the network layer which passes them on to the transport layer to remove the port numbers and reassemble the packets in the correct order.

The resulting data is then passed to the application which presents the data for the user. Since routers operate on the network layer, source and destination MAC addresses are changed at each router node. Packets, therefore, move up and down the lower layers in the stack as they pass through each router or switch between the client and the server as shown in the figure in page 2.

2.2 Encapsulation

Various protocols operate at each layer of the stack, each with different roles. In each layer, the data to be sent is wrapped, or encapsulated in an envelope containing new packet data as it descends the layers and is unwrapped again at the receiving end in a networking equivalent of a game of pass the parcel.

The figure below shows the physical path that data takes down a sending end system's protocol stack, up and down the protocol stacks of an intervening link-layer switch and router, and then up the protocol stack at the receiving end system.

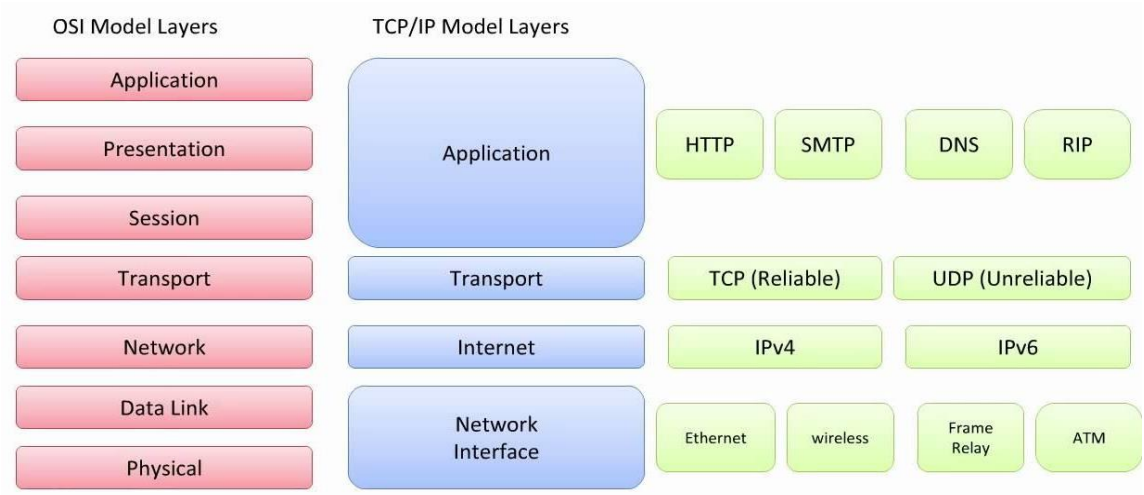


2.3 OSI Model vs TCP/IP Model

TCP/IP Protocol stack is not the only protocol stack around. Back in the late 1970s, the International Organization for Standardization (ISO) proposed that computer networks be organized around seven layers, called the Open Systems Interconnection (OSI) model [ISO 2016]. The OSI model took shape when the protocols that were to become the Internet protocols were in their infancy and were but one of many different protocol suites under development.

The 2 additional layers present in the OSI model are the presentation and the session layer. The presentation layer provides services that allow communicating applications to interpret the meaning of data exchanged, including data compression, encryption etc. The session layer provides for delimiting and synchronization of data exchange, including the means to build a checkpointing and recovery scheme.

Since we are currently using the TCP/IP model, it is up to a developer to decide whether the services provided by 2 additional layers are important, if so, they may build those functionality into their applications.



3 Some Important Protocols

These are some examples of protocols for different purposes in summary. We will elaborate on some of these protocols in this section.

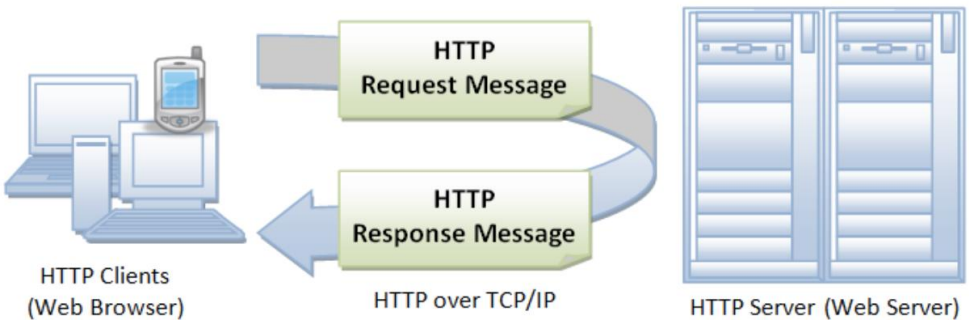
Protocol	Layer	Full name and purpose
HTTP	Application	Hypertext Transfer Protocol. Used to make a request for a webpage. The server returns the page or an error code if there was a problem with the request.
HTTPS	Application	Hypertext Transfer Protocol Secure. Sends an encrypted request for a webpage. The server returns the encrypted page or an error code if there was a problem with the request.
FTP	Application	File Transfer Protocol. Used to upload or download a file. The server opens a data connection (over which the file will be transferred) or sends an error code if there was a problem with the request.
SMTP	Application	Simple Mail Transfer Protocol. Used to send an email to an email server. The server returns a code indicating whether or not the email could be delivered.
POP	Application	Post Office Protocol. Used to request any new emails for a specific email account. The server returns the emails (if there are any).
IMAP	Application	Internet Message Access Protocol. Used to synchronise a client email account with an account on a mail server. The server returns new emails (if there are any) and deletes any emails that were deleted locally on the client application. This allows a user to use multiple devices to access their email account.
DHCP	Application	Dynamic Host Configuration Protocol. Used to assign IP addresses and other configuration options to devices in a network.

TCP	Transport	Transmission Control Protocol. When data is to be sent (whether from client or server), the data is split into packets and each packet is given a sequence number. This is a **reliable** transmission protocol. At the receiving end, the packets are checked. If any packets go missing, they will be resent.
UDP	Transport	User Datagram Protocol. Data is split into packets (as with TCP). However, this is an **unreliable** transmission protocol. If any packets arrive out of sequence or are missing, they are ignored. UDP is suitable where data does not have to be 100% accurate but speed is important, e.g. with some video streaming services or VOIP.
IP	Network (Internet)	Internet Protocol. Creates a new packet (imagine putting the packet from the transport layer into a new envelope). Adds the source and destination IP addresses to allow the packet to be delivered. These are the packets that are routed across the internet.
Ethernet and Wi-Fi protocols	Link (data link)	Encapsulates the data from the previous layer into frames (another kind of packet) with a source and destination MAC address, and manages multiple transmissions on the media.

3.1 HTTP (HyperText Transfer Protocol) / HTTPS – Application Layer

- HTTP (Hypertext Transfer Protocol) is perhaps the most popular application protocol used in the Internet (or The WEB).

- HTTP is an *asymmetric request-response client-server* protocol as illustrated. An HTTP client sends a request message to an HTTP server. The server, in turn, returns a response message. In other words, HTTP is a *pull protocol*, the client *pulls* information from the server (instead of server *pushes* information down to the client).



- HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.

- HTTP uses a variety of message types. Here are some examples:

  - **GET**: This requests a resource from the server, for example, a web page
  - **HEAD**: This requests just the header of the data (its metadata) from the server
  - **POST**: Sends data to the server from a web form
  - **PUT**: Sends data to the server to be uploaded as a resource, for example, uploading a photo
  - **DELETE**: Tells the server to delete a resource, for example, deleting a photo

- HTTP is not secure. If the messages sent between the client and the server are intercepted, an interceptor would be able to see all the details of the transactions. Hence HTTP is gradually being replaced with HTTP Secure (HTTPS) for the majority of websites and certainly all those sites which may ask you for personal information, such as your email address or your bank details. It is only through HTTPS that e-commerce has flourished.

- HTTPS encrypts the data exchanged between client and server. It works by providing a digital certificate containing a public encryption key. The authenticity of the certificate is checked automatically in your browser through a number of root certificates administered by certification authorities. Your browser uses the public encryption key to encrypt the data and it is only the authorised server that has the corresponding private key to decrypt it. Once a secure link is established using these public/private keys, other encryption systems can be negotiated to handle the bulk of the transfer.

3.2 IP (Internet Protocol) – Internet (Network) Layer

- The communications protocol of the public Internet, many wide area networks (WANs) and most local area networks (LANs). The Internet Protocol (IP) is part of the TCP/IP protocol suite, and the terms “IP network” and “TCP/IP network” are synonymous.

- IP is responsible for routing individual datagrams and addressing. Responsible for packet formatting and the logical addressing scheme, IP is a connectionless protocol and acts as an intermediary between higher protocols.

- Packet Switching - IP uses a packet-switched architecture, in which data are broken up into smaller “packets”, with each packet containing a source address and destination address. IP packets are handed over to a data link layer protocol, such as Ethernet, for the actual, physical transmission to the next node in the network path.

3.2.1 IP address structure

- Internet address - The address of a connected device in an IP network (TCP/IP network), which is the worldwide standard both inhouse and on the Internet. It is a 32-bit number uniquely identifying a node on a network using Internet Protocol. An IP address is normally displayed in dotted decimal notation, e.g. 128.121.4.5.

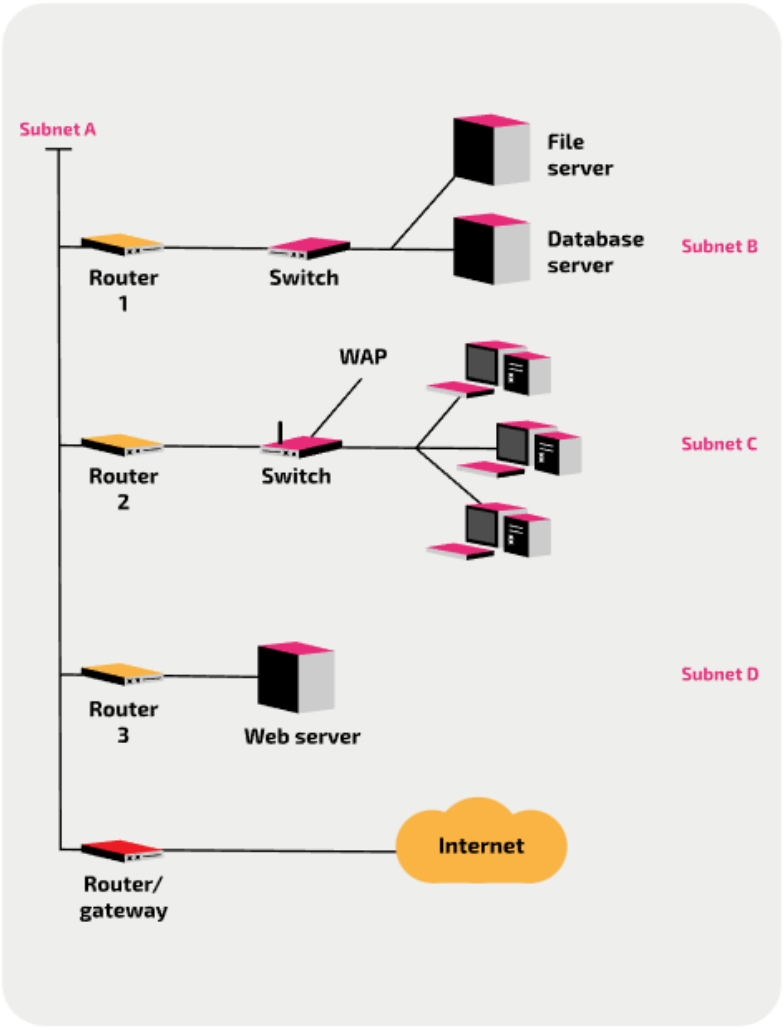
- The initial bits are the same for all the hosts on a particular network. By inspecting these initial bits, the network to which the host belongs can be identified. These initial bits are called the **network id**. The remaining bits in the address identify a particular host in that network and so they are called the **host id**.

- When a router sees an IP packet, it examines the network part of the address to identify the best path to forward the packet so that it reaches the destination network.

- When an IP packet arrives at its destination network, the host bits are examined to ensure it is sent to the correct device on that network.

3.2.2 Subnetting a network

- Subnets are subdivisions of networks that are treated logically as separate networks.The network id of each subnet is different.
- Organisations use subnets to subdivide large networks into smaller, more efficient subnetworks. One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routes, increasing network speeds.
- Subnets are connected by routers. A router has two network interfaces. On one interface it has an IP address that belongs to one of the networks, and on the second interface it has an IP address for the other network.
- The diagram below shows a simple scenario of a network that has been divided into four subnets. One subnet provides the backbone that allows the (other) subnets to communicate with each other.
- Conventionally the router is given the first or last address in the range. So, if the host id is 8 bits, the router would be allocated the id 1 or 254 (0 and 255 are reserved and cannot be used).



3.2.3 Static vs Dynamic IP addresses

S.NO	Static IP Address	Dynamic IP address
1.	It is provided by ISP (Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2.	Static ip address does not change any time, it means if a static ip address is provided then it can't be changed or modified.	While dynamic ip address change any time.
3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address's risk.
4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.
5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can't be trace.
6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.
7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.

3.2.4 IPv4 and IPv6

- So far all of the information about IP addresses has referred to IP version 4 (IPv4), which uses a 32-bit address structure and has facilitated the growth of the internet over the last four decades. However, the growth of the internet has been exponential and there are now not enough addresses.

- From early 2000, work began on the successor to IPv4. IPv6 uses 128-bit IP addresses. Whilst this is a fourfold increase in the size of the address, each additional bit doubles the range of possible addresses. This means that for IPv6 there are a colossal 2^{128} addresses. In comparison, the 32 bits in IPv4 result in only a possible 2^{32} addresses.

- IPv6 addresses are written in hexadecimal as 32 hex digits in blocks of 4. Here is an example IPv6 address:

  `2001:0db8:0000:0042:0000:8a2e:0370:7334`

- The structure of IPv6 addresses is similar to that of IPv4, in that the initial bits specify the network and the following bits specify the hosts.

- IPv6 has been designed to coexist with IPv4 so both systems can be run in parallel. It also offers a number of improvements with security and is slowly starting to be adopted around the world.

3.3 Domain Name System (DNS) Protocol – Application Layer

- DNS is a directory service for converting human-readable addresses into numeric IP addresses. For example, when a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name.

- For example, when a user enters a URL (e.g. https://www.raspberrypi.org/learn/index.html) into a web browser's address bar, this sequence of events happens:
  - The browser sends the domain name part of the URL, including the 'www' part (e.g. www.raspberrypi.org), to a domain name server. This is usually provided by your ISP.
  - The domain name server checks for the URL in its lookup table
  - The domain name server sends the corresponding IP address back to the browser
  - The browser sends a request for the resource identified in the path (/learn/index.html) to the web server located at the IP address
  - The resource is then returned to the browser

What if the URL is not in the domain name server's lookup table?

- Imagine we are looking to resolve www.raspberrypi.org
  - '`org`' is the Top Level Domain.
  - '`raspberrypi`' is the Domain.
  - '`www`' is the Subdomain.

- If the local domain name server does not find the URL in its lookup table, it passes the request to a Top Level domain name server. There are separate servers for most of the top-level domains such as '.com', '.org' and '.uk', each administered by a different authority. The request is therefore passed to the domain name server for '.org'

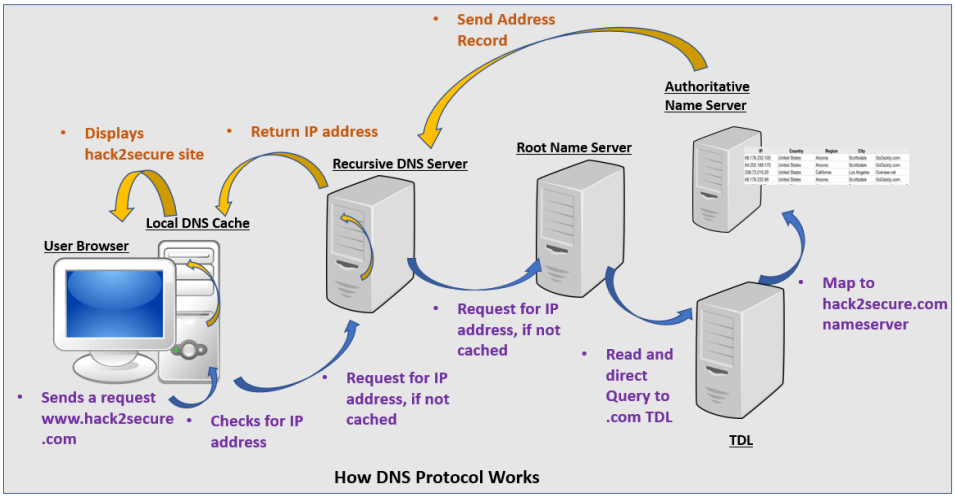
- The top-level domain name server will probably know the IP address of the full URL 'www.raspberrypi.org' and it will reply with the IP address.

- However, some organisations manage all the addresses of the subdomains for their organisations. Hence if the top-level domain name server does not know the answer, it will know the address of the domain name server that manages all the addresses for the raspberrypi domain. The request will now be forwarded to that server.

- The raspberrypi domain name server will know the IP address of all the sub-domains within raspberrypi such as 'www.raspberrypi.org' and it will respond with the correct IP address.

- At all the stages the results may have been cached with previous requests, so a full look-up may not happen.

- All of this happens in a few milliseconds and then your device gets the IP address it needs to access the resource.



3.4 Ethernet – Link (Network Interface/Data Link) Layer

- The first layer of the TCP/IP – Link Layer, or the first two layers of the Open Systems Interconnection (OSI) model deal with the physical structure of the network and the means by which network devices can send information from one device on a network to another. By far, the most popular set of protocols for the Physical and Data Link layers is Ethernet.

- Ethernet is a standard that refers to a family of wired computer networking technologies and protocols that are commonly used in local area networks.

- The current incarnation of Ethernet is defined by the IEEE standard known as 802.3.

- Ethernet uses an access method called **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other nodes have already transmitted on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. A collision occurs when this happens. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally affect the speed of transmission on the network.

- Physical connections are made between computer devices and/or infrastructure devices (hubs, switches, routers) using copper or fibre optic cable. The specification of the cable will make a difference to the speeds that can be achieved on the network.

- The actual transmission speed of Ethernet is measured in millions of bits per second, or Mbps. Ethernet comes in three different speed versions: 10 Mbps, known as *Standard Ethernet;* 100 Mbps, known as *Fast Ethernet;* and 1,000 Mbps, known as *Gigabit Ethernet.* Network transmission speed refers to the maximum speed that can be achieved over the network under ideal conditions. Actual throughput of an Ethernet network rarely reaches this maximum speed.

- Devices communicating over Ethernet divide streams of data into shorter pieces called frames. Each frame contains a source and destination address; these are the MAC addresses, which are encoded onto each network interface card. The Ethernet standard also includes error-checking data so that damaged frames can be detected and discarded.

References:

Network standards and protocols – Isaac Computer Science
https://isaaccomputerscience.org/concepts/net_network_protocols?examBoard=all&stage=all&topic=networking

Definition – Subnet (Subnetwork)
https://www.techtarget.com/searchnetworking/definition/subnet

OCR AS and A Level Computer Science – Section 5 Networks and web technologies

Computer Networking – A Top-down Approach (7th Edition)

Difference between Static and Dynamic IP address
https://www.geeksforgeeks.org/difference-between-static-and-dynamic-ip-address/

Annex A – Hardware in Networks

Network Interface Card

- Often abbreviated as NIC, an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

- A network interface card (NIC) provides the hardware interface to enable the transfer of data between a device and a network. An NIC may connect to a network physically or wirelessly. Most devices are equipped with a built-in NIC.

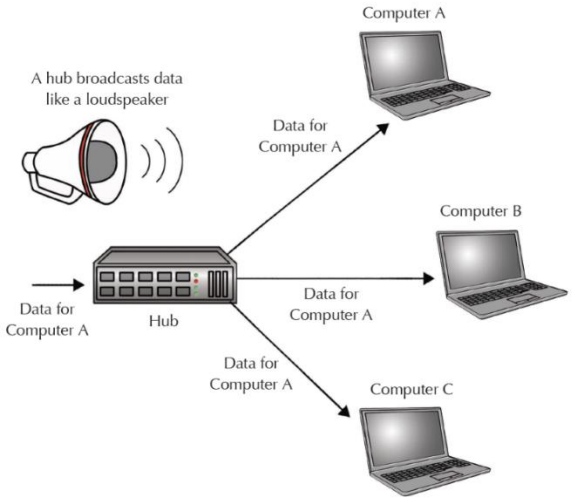
Repeater (Physical Layer [Layer 1] Device)

- A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analogue or digital signals distorted by transmission loss. Analogue repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.
- In a data network, a repeater can relay messages between subnetworks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.

Hub (Physical Layer [Layer 1] Device)

- A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

- In this way, a hub acts like a loudspeaker as it broadcasts the data to all its connected devices without limiting the data to only the specific device it was intended for.

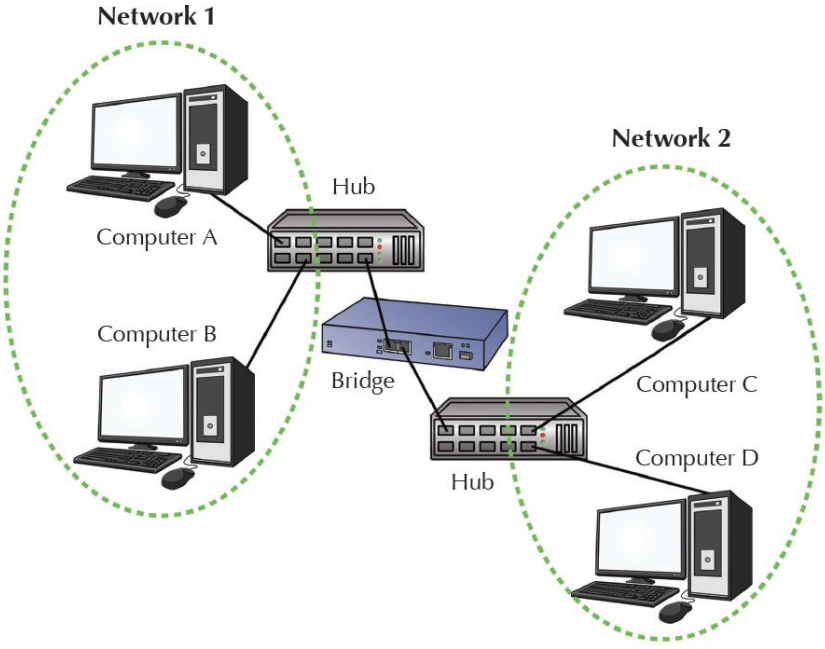


Bridge (Data Link Layer [Layer 2] Device)

- A device that connects two ***local-area networks (LANs), or two segments of the same LAN***. Bridges are typically used to connect two LANs that use the same protocol so that the combined network can cover a larger physical area. It operates at the Data Link Layer of the OSI model.

- Unlike a hub that simply repeats data to all connected devices, a bridge filters traffic using MAC addresses to keep track of the devices that are connected to each side of the bridge. Based on the destination MAC address, the bridge either forwards or discards the frame.

- Suppose the bridge receives a packet from computer A. The bridge first examines the destination MAC address stored in the packet's header and decides whether to forward or drop the packet. If the destination MAC address is that of computer B, the bridge will drop the packet as computers A and B are on the same side of the bridge. On the other hand, if the destination MAC address is that of computer C or D, the bridge will forward the packet to the other half of the network and on towards its intended destination.

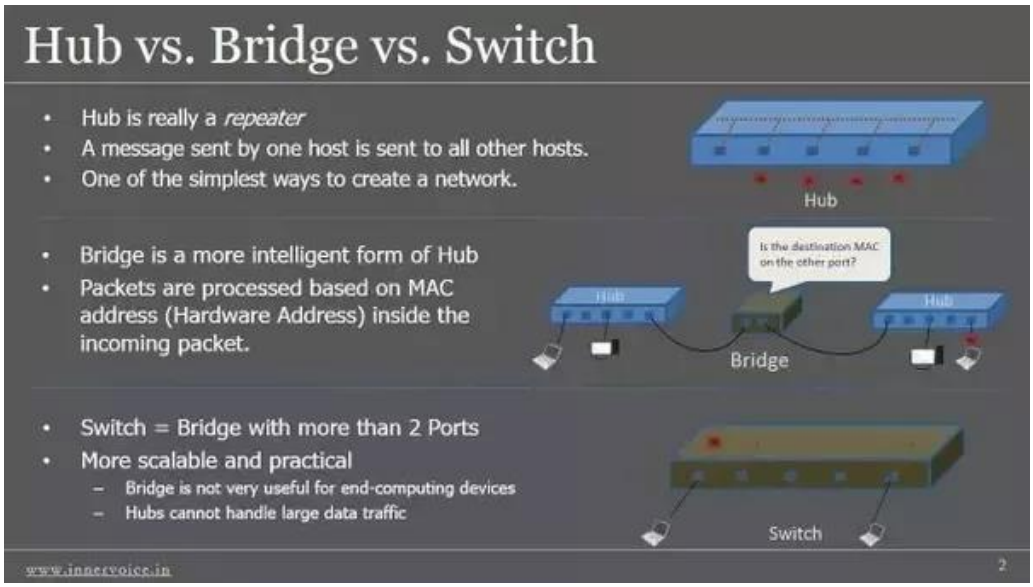


- A network bridge that connects more than two networks together is also called a network switch. Most large networks use bridges and switches instead of hubs as these devices are more “intelligent” and will send packets through a connection only if the bridge or switch determines that the intended recipient is on the other end, hence avoiding unnecessary bottlenecks. This makes using bridges and switches more efficient than using hubs.

Switch (Data Link Layer [Layer 2] Device)

- A more intelligent bridge. Has more ports than a bridge.

Basis for Comparison	Bridge	Switch
Basic	A bridge can connect fewer LAN.	A switch can connect more networks compared to the bridge.
Buffer	Bridges do not have buffers.	Switch has a buffer for each link connected to it.
Types	Simple bridge, multiport bridge and transparent bridge.	Store-and-forward switch and cut-through switch.
Error	Bridges do not perform error checking.	Switches perform error checking.



Router (Network Layer [Layer 3] Device)

- A router forwards packets between separate networks. While a bridge combines two similar networks that use the same protocol into a single network, a router keeps the connected networks (which may use fundamentally different protocols) separate and forwards packets between them using Internet protocols. The Internet uses routers extensively to forward packets from one host to another.

- In order for a router to forward packets between different networks using Internet protocols, both the device sending the packet and the device receiving the packet must be identified using IP addresses.

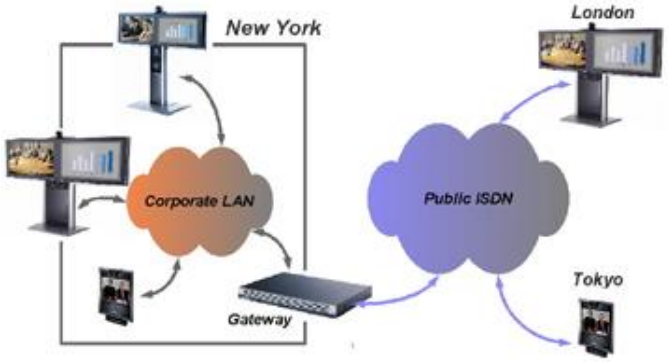
- Note that bridges forward packets based on permanent MAC addresses, while routers forward packets based on IP addresses that may change dynamically.

- Networks connected by routers are called internetworks because they create a larger network of interconnected, smaller networks.

Gateway (Network Layer [Layer 3] Device)

- Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data.

- In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, allow users on different e-mail systems to exchange messages.



Annex B – Software in Networks

Network Operating Systems (NOS)

- LAN Operating System - nucleus of a LAN.
- Performs tasks such as administration, file management and security.
- A network operating system (NOS) provides services to clients over a network. Both the client/server and peer-to-peer networking models use network operating systems, and as such, NOSes must be able to handle typical network duties such as the following:
    - Providing access to remote printers, managing which users are using which printers when, managing how print jobs are queued, and recognizing when devices are not available to the network.
    - Enabling and managing access to files on remote systems and determining who can access what files and who cannot.
    - Granting access to remote applications and resources, such as the Internet, and making those resources seem like local resources to the user (the network is ideally transparent to the user).
    - Providing routing services, including support for major networking protocols, so that the operating system knows what data to send where.
    - Monitoring the system and security, so as to provide proper security against viruses, hackers, and data corruption.
    - Providing basic network administration utilities (such as SNMP, or Simple Network Management Protocol), enabling an administrator to perform tasks involving managing network resources and users. Applications Software for LANs.
- Examples of NOS are Novell NetWare, Sun Solaris, Linus, Windows 2000 and Mac OS X.

Shared Applications Software

- LAN-based applications software is licensed for sharing.

Groupware

- Type of multi-user software designed to benefit a group of people
- Users linked together via a LAN can send e-mail, schedule meetings (e.g. google calendar)
- Chat systems, video conferencing, and screen sharing are different types of groupware.


Look for Collaboration Software with these 3 Main Features
Communication Tools
Allow the exchange of messages between parties
• Email, Voice mail, Instant messaging, VoIP or video calls
Conferencing Tools
Allow real-time discussions among members
• Video conferencing, IM teleconferencing, Social media group chats, forums or community boards, application sharing
Coordination Tools
Facilitate group activities, schedule, and deliverables
• Calendars, Time trackers, spreadsheets, client portals, alerts, and status updates