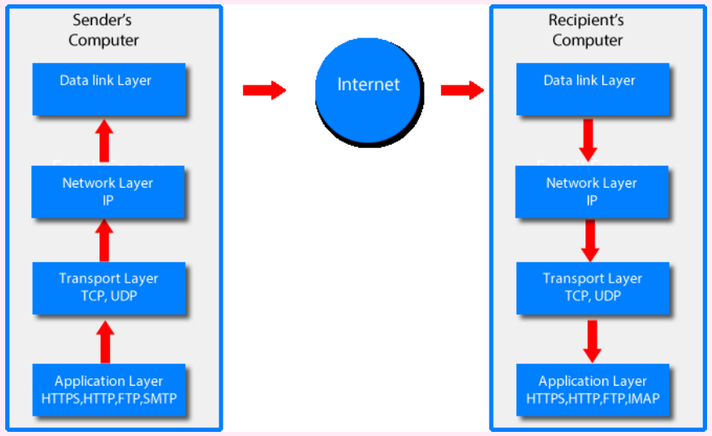
TCP/IP

A **network protocol** is a set of rules that allow computers to communicate and exchange information over a network.

TCP (Transport Control Protocol) When files are sent over the internet they are broken up into small chunks called **packets**. A typical packet size is 1500 bytes. When they arrive at the destination computer they are reassembled back into the original format. TCP handles and controls all this. TCP waits for acknowledgements to verify whether the packets have reached their destination. TCP will also retransmit packets of they have not arrived at the destination or become corrupted.

The **internet protocol** is a set of rules that govern the transmission of data across the internet. The TCP and IP work closely together and are referred to as TCP/IP.

The **TCP/IP stack** is made up of four layers that pass data between each layer.



The **application layer** contains protocols associated to the particular application such as HTTP, HTTPS for web browsers, FTP for file transfer or SMTP and POP3 for email for instance. The application layer interacts with the user via appropriate application software (eg web browser / ftp client / email client).

The **transport layer** establishes the end to end connection. When files are sent over the internet they are broken up into small chunks called **packets**. When they arrive at the destination computer they are reassembled back into the original format. It is the role of the transport layer to split the data into packets and pass the data onto the **network** layer. On the recipient's computer the transport layer reassembles the packets into the original form. TCP and UDP are the main protocols used in this layer. The packets are given an ID by this layer to allow them to be reassembled. The transport layer chooses the port number for sender and receiver.

Consider the following message: "Friends, Romans, Countrymen lend me you ears. I have come to bury Caesar not to praise him". The transport layer will break it up into packets:

Packet 1/4
Source Port: 25 Destination Port: 110
Friends, Romans, Countrymen

Packet 2/4
Source Port: 25 Destination Port: 110
lend me you ears.

Packet 3/4
Source Port: 25 Destination Port: 110
I have come to bury Caesar

Packet 4/4
Source Port: 25 Destination Port: 110
not to praise him

The **network layer** adds the source and destination IP address and route the packets over the network. At the destination the network layer strips out the IP addresses.

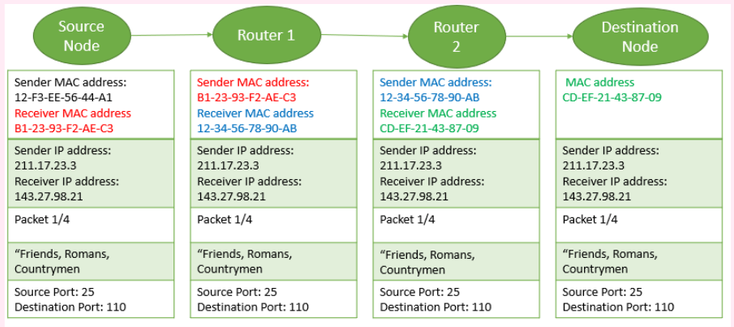
Sender IP address: 211.17.23.3 Receiver IP address: 143.27.98.21	Sender IP address: 211.17.23.3 Receiver IP address: 143.27.98.21	Sender IP address: 211.17.23.3 Receiver IP address: 143.27.98.21	Sender IP address: 211.17.23.3 Receiver IP address: 143.27.98.21
Packet 1/4	Packet 2/4	Packet 3/4	Packet 4/4
Source Port: 25 Destination Port: 110	Source Port: 25 Destination Port: 110	Source Port: 25 Destination Port: 110	Source Port: 25 Destination Port: 110
Friends, Romans, Countrymen	lend me you ears.	I have come to bury Caesar	not to praise him

The **data link layer** has a network card and deals with the physical connection and adds the physical addresses (MAC address) of the hardware to the packets that it receives from the network layer. Each network interface card has a unique MAC address that is a 12 digit hexadecimal code (e.g. 12-F3-EE-56-44-A1). For each step the sender and receiver MAC address is removed then a new sender and receiver MAC address is added. The receiver MAC address becomes the sender MAC address.

The purpose of a **MAC address** is to provide a unique *hardware address* every *node* on a network. A node is a point at which a device (e.g., a computer, printer or router) is connected to the network.

MAC address and hopping
When data are sent over the internet they pass through a number of routers. The packets contain the destination IP address but the packets need also to include information on the route it takes across the internet. Packets need to know which routers to hop between. So packets need to know the MAC address of the next router. At each step the MAC address is stripped out, and the source MAC address is replaced by the destination address of the previous hop and the destination MAC address is replaced by the MAC address of the next router.

At each step the source MAC address is replaced by the destination address of the current node and the destination MAC address is replaced by the MAC address of the next node



A port is the end point between a networked device and other networked devices through which packets enter and leave. By convention depending on the protocol a specific port number will be used. A client port number is temporarily assigned for the duration of a connection. At the server end the service continually listens waiting for instructions from clients. The port numbers are added to the packet in the transport layer and determine which application layer protocol to use

Port number	**Protocol**
20	FTP
22	SSH
25	SMTP
80	HTTP
110	POP3
443	HTTPS

A **socket** is a connection between two applications over a network that allows data to be exchanged. A socket includes the IP address and the port number. The port number and IP address together are called the socket. e.g. 127.0.0.1: 5000 where 127.0.0.1 is the IP address and 5000 is the port number.

Application Layer Protocols

SSH allows remote login of a machine. It allows a secure connection where data being sent over the network are encrypted. A series of commands can be used to perform tasks on the remote machine. Allows remote login access by a network administrator to servers that could be at another location. Servers may not have their own terminal (no keyboard, mouse, or monitor) so the only way to access the servers is via SSH. SSH allows tunneling through which other applications eg SMTP can operate more secure

Some common shell commands

Command	Example	Explanation
pwd	pwd	States current directory (folder)
ls	ls	List contents of a folder
touch	touch filename.txt	Create file
mkdir	mkdir dirname	Make a folder
cd	cd dirname	Change directory (folder)
rm	rm filename.txt	Delete file
mv	mv file1.txt file2.txt	Rename file
cp	cp file1.txt file2.txt	Copy file
head	head file1.txt	Show the contents of the top of the file
echo	echo “Hello World” > file.txt	Print message
cat	cat file1.txt file2.txt	Concatenate (append) files.

Web server

- A web server is a computer on which are stored all the elements of a website including text images and other multimedia content as well as the HTML and CSS files.
- The web server will be able to understand HTTP requests from clients and respond to those requests.
- The web server will continuously be listening out for requests from clients.

HTTP – Hypertext transfer protocol

HTTP is the protocol used for the world wide web. A request for a web page from a server by a client web browser is made to a web server that is hosting the web site. The server then sends the web page to the client along with a status response.

Example request sent by client. GET is used to request a resource from a server by a client.

```
GET /index.html HTTP/1.1
```

POST is used to send data from the client to the server.
Example status response sent by server

```
HTTP/1.1 200 OK
```

Several GET requests may be needed to download different parts of a page e.g. images and other multimedia content.

HTTP response status codes
1xx – Information
2xx – Success
3xx – redirection
4xx – Client error
5xx- Server error

HTTPS – Secure Hypertext transfer protocol

HTTPS is a secure way of transferring data between a web browser and a server. During transfer the data are **encrypted.** If the data are intercepted it is very difficult to find out what data are in the messages.

HTTPS is most often used for e-commerce and online banking, where sensitive data such as credit card numbers and passwords are encrypted.

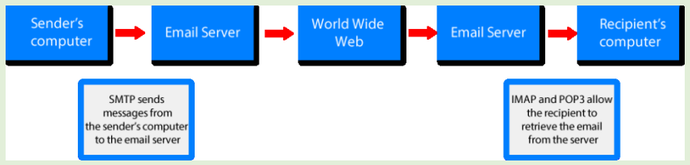
FTP – File Transfer Protocol

FTP is used to transfer files between two computers. It is usually used to download or upload large files between a client and server.

Common commands
open – start a session
pwd – present working directory
dir - list contents of directory
get – download a file
mget – download one or more files
mput – upload one or more files
put – upload a file
cd – change directory
close – close a session

Email

The email server distributes incoming email messages to users and sends outgoing messages across the internet. Email is sent by the sender client to the email server. It is stored there until the recipient requests access and then the email is forwarded to the receiver’s computer. The email server stores all mail. Outgoing mail uses SMTP to send from the client to the server. The sender mail server sends the message to the receiver mail server. Incoming mail uses POP3.



Email protocols (SMTP, POP3)

- SMTP (simple mail transfer protocol): Sends the mail from the user client onto the mail server.
- POP3 (Post office protocol): Retrieves the mail from the mail server to the client (user) when requested and the email is removed from the server. Only allows retrieval of email onto a single network.