Networking

Network Devices:

Router:

```
Router is a network device that forwards data based on a logical address. In the
case of TCP/IP networks, the router forward data based on ip addresses of systems.
Example: When we want to visit google.com, our request go trough the router (DNS
convert name to IP), and the request will be sent over the internet to the
google.com web server IP.
```

Hub:

```
 Network device that connects all devices on a LAN. When a device send data to the
hub on one port, the hub will broadcast there to all other attached devices.
```

Switch:

```
A switch is a smart version of a hub, because it understands where to send data,
instead of sending it to everyone. It achieves this by using MAC addresses as
unique identifiers for recipients of incoming data, so it can send it to the right
system.
```

Bridge:

```
A network bridge device connects separate networks to make them into one larget
network. This is different than a router, which allows networks to be connected but
work independently.
```

Firewall:

```
A firewall is a network device that provides fundamental network security, by
monitoring incoming and outgoing traffic and determine whether to allow or block
it, based on rules.
Firewalls can come in software form or hardware form as a physical devices that are
plugged into the network infrastructure.
```

Ports and services:

Port 20,21 - File transfer protocol (FTP):

```
This protocol is used to transfer files between systems, where users can connect to
an FTP and can view, upload or download files.
```

Port 22 - Secure Shell (SSH):

```
SSH allows users to connect to a remote host, such as a server if they have SSH
open. This channel is encrypted so any data moved between two connected systems
will not be clearly visible.
```

Port 23 - Telnet:

```
This service was used before SSH and offers the same functionality, however Telnet
does not use encryption, so the traffic can be captured and read by an attacket.
```

Port 25 - Simple Mail Transfer Protocol (SMTP):

```
This protocol is used to send emails between servers withing the network, or to
external networks, such as over the internet. This is just a transport method, to
download a view e-mails we need an email client and POP3 OR IMAP
```

Port 53 - Domain Name System (DNS):

```
DNS Operates on TCP and UDP ports 53 and uses relational databases to convert
human-readble hostnames and domain names (such as google.com) into their respective
IP.
Example: securityblue.team -> 3.9.68.12
```

Port 67,68 - Dynamic Host Configuration Protocol (DHCP):

```
DHCP is design to assign IP address-related information to any hosts on the network
automatically, such as the subnet mask and ip address.
```

Port 80 - Hypertext Transfer Protocol (HTTP):

```
HTTP allows clients to connect to web servers and request content, witch appears in
the form of file downloads, web pages, and streaming services.
```

```
HTTP is not encrypted it is possible to conduct sniffing attacks, and see cleartext
data as it is transmitted between the client and the server, such as passwords.
```

Port 443 - Hypertext Transfer Protocol Secure (HTTPS):

```
HTTPS is a secure version of HTTP, and has the same functionality of retrieving
content from web servers. However, the difference between the two is that HTTPS
uses encruption to protect the transfer of data between a web server an a client.
To turn HTTP into HTTPS, it uses Tranport Layer Security (TLS) formerly known as
secure socket layer (SSL). Sites that use HTTP are less susceptible to man-in-the-
middle and sniffing attacks.
```