Unit 9, Assignment 2—Network Hardware

Thomas Robinson

SOLIHULL COLLEGE

Task One/Four (P3, P4)

End Devices

- **Desktops** are fixed computers that are commonly found at or under a desk. They are rarely moved and are most often connected with a wired connection.
- **Laptops** are able to be carried around to various locations and are therefore often connected wirelessly. If used as a primary computer at a fixed location, they are often "docked". In this scenario they can be connected with a wired connection.
- **Mobile Devices** include smartphones and tablets that have no convenient facility for connecting to a wired network. Almost always they only connect to a network wirelessly.
- **Servers** are devices that host applications and services on a network. These can include core services to making a network function (such as DNS and DHCP) as well other services; in this case a file server for backups and a media server.

Connection Media

- **Ethernet cables** are a standard type used to connect devices together in a network. They send data over copper wires and are split into Categories, which dictate how much data they can throughput and over what distance. The common connector type is an RJ45 type and the ethernet standard is ratified as part of IEEE 802.3.
- **Fibre optic cables** are used for applications where high bandwidth or longer distances are required. Rather than sending data using electrical signals down copper wires, fibre cables send pulses of light down microscopic glass or plastic tubes. There are many types of fibre-optic cabling and varying standards for different needs.
- **Wi-Fi** is a standard for wireless connectivity commonly used to connect end-devices to a LAN. **Wireless Access Points** allow end devices to connect to a network wirelessly. There are many versions which are all standardised as part of the IEEE 802.11 family.

Interconnection Devices

- **Routers** are a device that can distribute ('route') network traffic to the correct device on a network. They are also used to connect multiple networks together and route traffic between them. They are a layer 3 device since they deal with the IP address of devices.
- **Switches** allow more wired devices to connect to a network by intelligently 'switching' packets to the correct port based on the destination of the data. They are a primarily a layer 2 device, only dealing with devices' MAC addresses.

- **Hubs** are similar to switches, however rather than intelligently switching data, they broadcast any data received across all ports at the same time.
- **Modems** convert (modulate/demodulate) a digital signal for transmission down an analogue medium, such as a telephone line. In the context of networking, they are used for Dial-Up and DSL internet connections to send internet traffic along analogue telephone lines.
- **Repeaters** boost (retransmit) a signal to allow it to be transmitted over a longest distance. They are more commonly used for analogue transfer methods that suffer more over longer distances when compared to digital. They do not have to be limited to wired connections; another use of a repeater is for allowing cellular connectivity inside a building that may otherwise receive a poor signal.
- **Bridges** refer to devices that connect two or more networks together ('bridging' them together) and allows them to communicate.
- A **Gateway** is a device that allows access to another network. In the context of a home, the router would function as the gateway device to the network of the Internet Service Provider which thus enables internet access.
- A **Network Interface Card** (NIC) is a part of a device that facilitates a connection to a network. Commonly, this would be in the form of an ethernet port.
- **Media Extenders** are a type of repeater that can allow a connection to be extended over a greater distance. Sometimes it is necessary to change the transfer method to facilitate this, for example it is not uncommon to run HDMI signals down an ethernet cable to allow them to be run for longer distances. At either end there will be a media converter to allow connection over a normal HDMI plug.

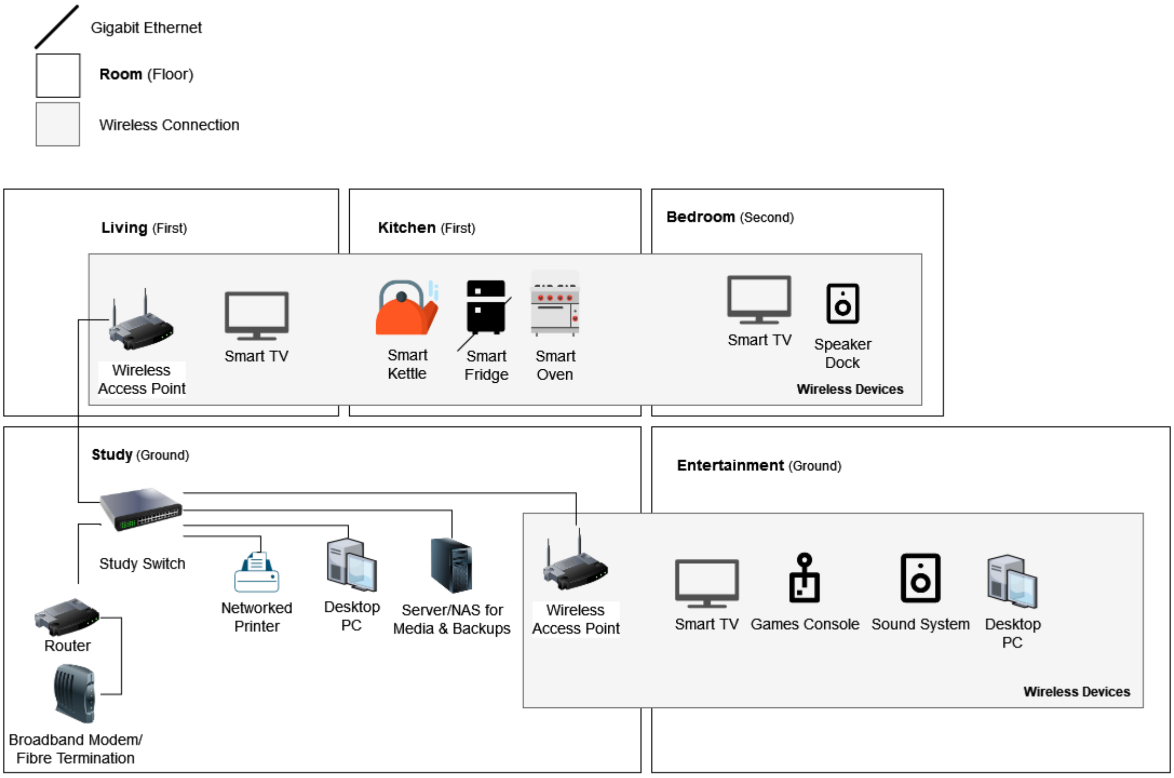
Software

- A device's **Operating System** provides the base upon which applications and programs run.
  For the user, it provides an interface – a textual CLI (command line interface) or a GUI (graphical user interface).
  For developers, it provides APIs (programming interfaces) for common tasks shared amongst many programs, such as writing files and displaying graphics. A computer is essentially inoperable without an operating system installed.
- **Security Software** can include **Anti-Virus Utilities**, which are software tools used to scan for and remove viruses and other

malicious programs. Often, they will scan downloaded files and run periodic scheduled scans. Examples of antivirus utilities include Avast, Norton, Malwarebytes and the built-in Windows Security program. These are required to prevent information being from a users' computer or to stop the computer being used as part of a botnet or as a cryptocurrency coin miner.

- **Firewalls** are used to filter the network traffic in and out of a computer or network. They will inspect data packets and block them based on protocol, port, source/destination or application. As an example, the built-in Windows Firewall blocks inter-PC traffic on WiFi networks marked as 'public,' like those in a coffee shop or at a railway station. In most networks, the gateway device also has its own firewall that dictates what traffic is let into or sent out of a network.

Task Two/Three (M2, D1)



Throughout the House

Internet Access

Internet access throughout the house is provided by wireless access positioned to cover the entire house. In the study, devices are connected with ethernet cables. This provides a reliable hard-wired connection to the devices in the study and flexible wireless connectivity elsewhere in the house.

Alternatively, ethernet cabling could be run to each room to facilitate wired connections within them. This would give a more permanent and reliable connection to devices, most notably in the entertainment room. However, this would require more infrastructure to be set-up, with cables run inside of walls, which may not be possible.

The connection to the internet was assumed to be located on the ground floor near the study. The type of internet connection was also not specified, so a wired broadband or fibre connection was also assumed. The modem or ONT (optical network termination) for this is connected to a router. This router also acts as a DHCP server and DNS forwarder, giving out IP addresses to devices on the LAN and relaying DNS queries to an external service such as Google DNS or CloudFlare DNS.

Wi-Fi Access

As mentioned previously, wireless access points situated around the house provide Wi-Fi connectivity. More than one WAP is used to ensure the entire house receives coverage. These are both connected with ethernet rather than wirelessly uplinked to ensure the wireless connection is able to provide the best throughput possible, particularly for devices in the entertainment room. Additional access points could be added in future to increase coverage around the house.

Access to Media & Backups

The media and backup server is located in the study and is connected using ethernet to a switch in the study, which in-turn is connected to the router. It is assumed that one device is used for both purposes.

An off-the-self NAS (network attached storage) solution such as a Synology or QNAP device would provide easy management of user accounts and permissions and allow all clients on the network to connect securely and only access what they should be able to. The downside of this is cost and performance—these solutions are often costly and lacking in CPU power that may be required to transcode video for a media server. A custom server, such as a HPE MicroServer could be procured for this task, though services such as file sharing would need to be manually set up and maintained.

This is connected using a wired connection since it will be dealing with a large amount of traffic, being a file and media server. A Wi-Fi connection could be overwhelmed by this, and a large file transfer would also affect the wireless performance of other devices, which would not be acceptable.

Rooms & Components

The Study

Inside the study on the ground floor, all devices are connected using a wired ethernet connection due to their proximity to the switch. This includes the desktop computer, the server and the networked printer.

This switch was used to allow more wired devices to connect to the network and was chosen over a hub since being an active device, they can support faster network speeds and facilitate more reliable data transfer due to this. Additionally, if in future VLANs were considered, a managed switch would allow this to be implemented.

Additionally connected to the switch in the study is a wireless access point, which provides Wi-Fi access to the ground floor.

Entertainment Room

Within the entertainment room on the ground floor, devices are connected wirelessly to an access point in the nearby study room.

These devices were not connected with a wired ethernet connection to facilitate an easier setup; using WiFi there is no need to run cables through walls and etc. A wireless connection can provide ample bandwidth even for high-quality video streaming and game downloads; therefore, I deemed this solution acceptable. Unfortunately, wireless connections are inherently less reliable than wired connections due to congestion and interference, so the connectivity for these devices may be less reliable than it could be.

Living Room

Moving up a floor to the living room, the only end-device here is a smart TV. This is connected to the network via Wi-Fi. As previous, a wireless connection is more than ample for this application.

Also in the living room is a wireless access point. This provides Wi-Fi coverage to the upper floors of the house. As mentioned previously, it is connected with a wired connection.

Kitchen

The smart appliances in the kitchen are all connected wirelessly via Wi-Fi.

Depending on the device, it may be possible to connect using an alternative wireless communications standard, such as Z-Wave or Zigbee, which are both designed for smart-home applications. This would require an extra hub to facilitate their connection to the network, however it would mean there are less Wi-Fi clients which can cause congestion and bandwidth issues.

Bedroom

As previous, the Smart TV and the Speaker Dock in the bedroom are both connected to the network wirelessly using Wi-Fi.