

# **EAGLE FANG KARATE DOJO**

Network Design Technical Plan

HEP506 – Networking



Abertay  
University

LUKE  
GILBERT

## Table Of Contents

<b>INTRODUCTION .....</b>	<b>1</b>
Client Requirements.....	2
<b>DESIGN CONSTRAINTS .....</b>	<b>3</b>
Cost .....	3
Technical Knowledge .....	3
Physical Layout .....	3
Performance .....	3
Security .....	3
Hardware.....	4
Robustness .....	4
<b>NETWORK DESIGN .....</b>	<b>5</b>
Network Topology.....	5
Star Topology .....	6
Office Subnet .....	7
Main Hall Subnet .....	7
IP Addressing Scheme Design .....	8
Static and Dynamic IP Addresses .....	9
Static IP Addressing .....	9
Dynamic IP Addressing .....	9
Physical Network Layout .....	10
ISP Package Selection .....	10
<b>NETWORK HARDWARE REQUIREMENTS .....</b>	<b>11</b>
Required Hardware List .....	11
Hardware Choice Rationale .....	12
<b>NETWORK SECURITY .....</b>	<b>13</b>
IPv6 .....	13
Firewall.....	13
Authentication.....	14
Encryption .....	14
Content Filtering .....	14
Physical Security .....	14
<b>NETWORK TROUBLESHOOTING AND ANALYSIS .....</b>	<b>15</b>
<b>FUTURE PROOFING AND REDUNDANCY .....</b>	<b>16</b>

<b>NETWORK DESIGN CRITIQUE.....</b>	<b>17</b>
Design Strengths .....	17
Improvement Areas .....	17
<b>DISASTER PLAN (MAIN HALL WAP).....</b>	<b>18</b>
<b>DISASTER SCENARIO (PANDEMIC) .....</b>	<b>19</b>

## **References**

**APPENDIX A – NETWORK DESIGN BRIEF**

**APPENDIX B – PASSWORD SECURITY POLICY**

# INTRODUCTION

This technical plan has been prepared to detail the design of the network for the Eagle Fang Karate Dojo and aims to give insight into the rationale behind the design decisions made. The technical plan itself has been prepared in accordance with client requirements (Appendix A) and will cover the following key aspects of the network:

- Design Constraints
- Topology of The Network
- Physical Network Layout
- ISP Package Selection
- Details of All Required Hardware
- Network Security
- Network Diagnostics and Troubleshooting
- Future Network Development and Maintenance
- Disaster Planning

## Client Requirements

The network plan adheres closely to the requirements which have been provided by the client. This ensures that the network design is fit for purpose and allows specific resources and focus can be placed on key areas for the client's business needs.

A brief list of the client requirements can be seen below:

- Smooth High Quality Video Streaming and Broadcasting
- Network Content Filtering Controls
- Office printer, Smart TV, staff mobile phones able to connect to the network
- No network access for students and visitors
- Company related files stored on network
- Wi-fi connections used where possible
- Good network security
- Simplicity for end users
- Network ping functionality

## DESIGN CONSTRAINTS

Using the client requirements, the design constraints for the network can be formulated, adhering to these will ensure the design is fit for purpose.

### Cost

Since the company is relatively small in scale (5 employees) it is prudent that the network design is as cost efficient as possible. The design should meet the specified requirements without excessive redundancy.

### Technical Knowledge

It is made clear that employees at the Dojo have limited technical knowledge when it comes to networks meaning the design and usage of the network should be kept as simple as possible. This helps to lower the cognitive burden for users and allow them to focus on the business needs of the network rather than the finer details of how it is implemented.

### Physical Layout

Two main areas are noted, the office and the main hall. It is noted that these areas are separated by metal walls likely to block Wi-Fi transmission between areas. The main hall is noted to be quite large and the office smaller in size.

### Performance

The network is required to provide network speeds which can accomplish buffer-less streaming of 4K / UHD videos and broadcasting training classes remotely to students if required.

### Security

Specific security requirements have not been identified by the client however it is the designer's due diligence to ensure that a minimum level of security is provided for the network to ensure that company sensitive information is kept safe.

## Hardware

The dojo already possesses several hardware components which are used in the proposed network design such as a printer, USB, laptops, mobile phones etc. Some of the existing devices will dictate connection mediums as not all devices support wireless connection. The company will require some devices such as routers, switches etc. to facilitate the network design the details of which will be detailed further in the plan.

## Robustness

With no specific requirements outlined by the client, it is assumed that a minimal level is required given the cost constraints highlighted. As the company scales, outages might be more impactful on business performance and require a more detailed assessment.

# NETWORK DESIGN

The network design comprises several different aspects. Each section discussed will detail the design choice made for the network design and the rationale behind its choice as it relates to the client requirements and constraints.

## Network Topology

Given the physical layout of the dojo the proposed network topology for the network is a hybrid topology. The network will comprise of two separate subnets both of which will be of star topology (Wikipedia Contributors, 2020). in nature, and which are connected via. a physical medium.

Each subnet will comprise a central hub in the form of a switch or wireless access point (WAP). All devices will connect to this central node on the star via. either wired or wireless means.

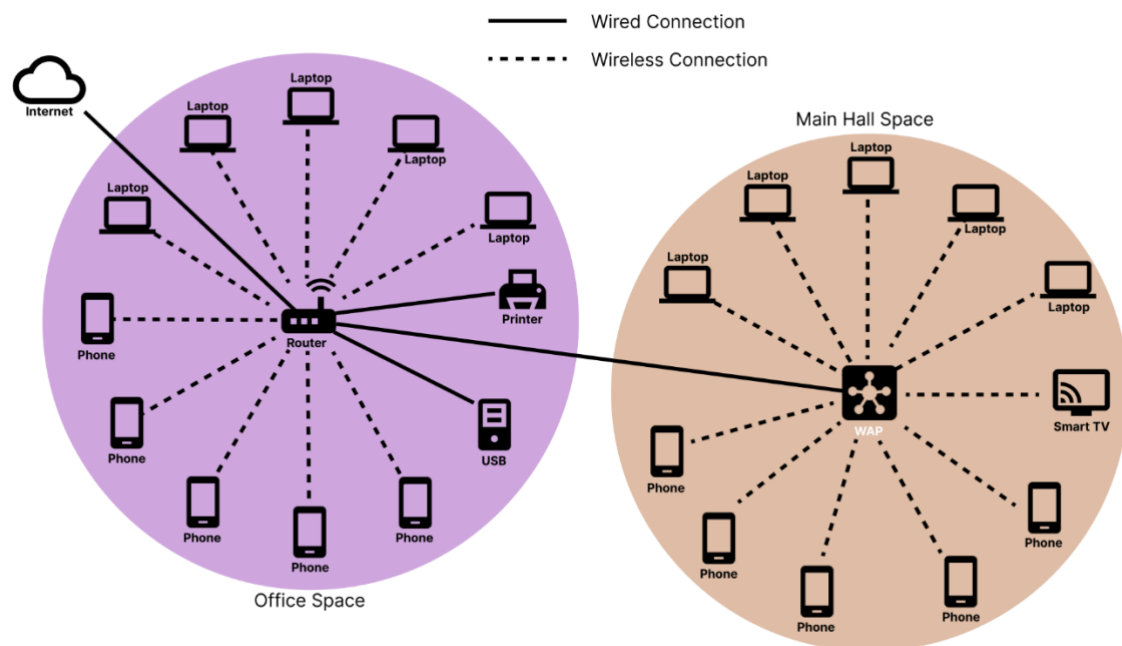


Figure 3.0.1 - Proposed Network Design Layout



## Star Topology

The star network topology is characterised by a central node with “spokes” in the form of connections (wired or wireless) to the other devices on the network. There are several aspects to this topology which have driven its choice for the network design, these are summarised below:

- **Cost Effective:** Star topologies can get costly when using wired connections. However, effort has been made to minimise the cabling required in favour of using Wi-Fi to connect nodes to the central hubs of the star and thus reduce the cost impact. It is worth noting that star topologies do have the additional cost of the central hubs and switches to facilitate their implementation.
- **Network Performance:** Each node on the network has their own direct connection to the hub so there is no likelihood of data collision on the network leading to it being highly performant. It is worth noting that since all the network traffic is funnelled the central hub (router, WAP etc.) bottlenecks can be formed in network traffic and performance of the network is inherently linked to the technical capabilities of the central hub (i.e. bandwidth).
- **Extensibility:** Adding and removing devices/subnets is easy to implement giving the network design the ability to easily scale as the company grows and effectively future proofs the network.
- **Security:** With a central hub which all the network traffic passes through it is well suited to implementing security measures such as firewalls, content filters etc. with this being able to be refined for each subnet within the network if required. The use of subnets also for the isolation of security threats within a subnet to stop it spreading to the rest of the network.
- **Robustness and Reliability:** Star topologies provide sound robustness as failures in any of the “spoke” connections or devices doesn’t result in failure of the entire network. It is worth noting however that the topology has single point of failure in the central node which if it fails will cause a network wide failure.

## Office Subnet

The office subnet uses the ISP provided router as its central node which serves multiple purposes including a WAP, Switch, Firewall etc. This central node is what connects the network to the WAN (internet) and connects the two subnets together. The router is noted to have a USB port for which a USB device can connect to store company files for access via the network. Due to the capabilities of the existing printer, it must be connected to the router via physical medium. The router is noted to have a 4-port switch, 3 ports of which will be used to facilitate the wired connections to the WAN (Internet), Printer and Main Hall Subnet, this leaves flexibility in the future use of the final port for perhaps another subnet if the business scales up over time or any other future devices which do not support wireless connections.

## Main Hall Subnet

The main hall subnet follows the same topology as the office. Its central node is a WAP which allows devices in the main hall to connect wirelessly. This is connected back to the Office subnet using a physical medium as due to the warehouse construction of the building it is likely that any Wi-Fi signals would be blocked or hindered.

## IP Addressing Scheme Design

With multiple subnets present on the network it is prudent to describe the IP addressing system for the network. The network is proposed to utilise IPv6 addressing, though IPv4 is the more common protocol, the industry is slowly aiming to fully transition all networks to using IPv6.

The IP addressing plan would begin firstly with the ISP allocating an IPv6 address block to the location (the dojo). Which will look something like:

2001:ABCD:1234:123**0**:0000:0000:0000:0000 / 60

The zero shown in **bold** here will be what is used to determine the subnet within the network, since for IPv6 there are 16 possible values this can be, there is capacity for 16 subnets. This allows for flexibility and scalability. The following IPv6 addresses will be used for the network:

- 2001:ABCD:1234:123**0**:: / 64 (Office)
- 2001:ABCD:1234:123**1**:: / 64 (Main Hall)

Allocating addresses in this way is known as a “Location First” approach. This should be sufficient for the current business requirements though further address allocations can be requested if the client wishes to further subdivide into more subnets based on other aspects such as business departments.

IPv6 was built with security in mind and as such it offers several features which help to enhance the security of network communications using the protocol such as Data Authentication, Data Encryption and Encapsulation which help add confidentiality and security to the transferred data packet. IPv6 offers a streamlined packet header which makes it more cost efficient and can in some cases result in faster internet speeds. By using IPv6, the requirement for the use of NAT as with IPv4 is removed leading to a more streamlined and simpler network architecture which can enhance network performance for video streaming (LinkedIn, 2024).

## Static and Dynamic IP Addresses

This section will look at the allocation of static and dynamic IP addresses as part of the network design and give rationale as to why each type has been chosen for a given node on the network.

### Static IP Addressing

These addresses are manually assigned to devices on the network by the admin.

The following devices on the network will be assigned static IP addresses:

- Employee Laptops
- USB Drive (File Server)
- Printer
- Smart TV
- Any business essential devices added to the network

The allocation of static IP addresses for laptops is for one main reason, the client has noted that they wish to be able to ping employees' laptops to check who is in work. Having these IP addresses as static allows the person pinging to be able to associate an IP address on the network with a user. Other devices on the network that have been assigned static IP addresses benefit from faster upload and download speeds on the network with increased stability which will lend itself well to the client's request for smooth high-quality video streaming using the network. Static IP addresses for the printer, file server and smart tv is particularly beneficial when it comes to remote access of these devices by users on the network as they can easily be located and utilised by users (Fortinet, n.d.).

### Dynamic IP Addressing

Static IP addressing has many benefits which it comes to performance on a given network, but they can be expensive and inflexible. It is for this reason that not all devices have been given static IP addresses and will utilise dynamic IP addressing instead. This can prove to be more cost effective when it comes to adding/removing non-business essential devices to the network and gives much more flexibility when it comes to the reuse of addresses when devices join and leave the network (Fortinet, n.d.).

The following devices on the network will be assigned dynamic IP addresses:

- Employee Phones
- Any devices which aren't business essential added to the network

## Physical Network Layout

The network plan has adequate considerations for the physical layout and constraints put in place. One of the main physical challenges which the design addresses is the connection between the two rooms (Office and Main Hall). Due to the construction of the building the use of a physical medium will be required to connect the two subnets as any wi-fi signals will be hindered by the walls. No explicit dimensions of either room are mentioned so it is assumed that the router provided by the ISP and a relatively inexpensive WAP should suffice for facilitating the subnets.

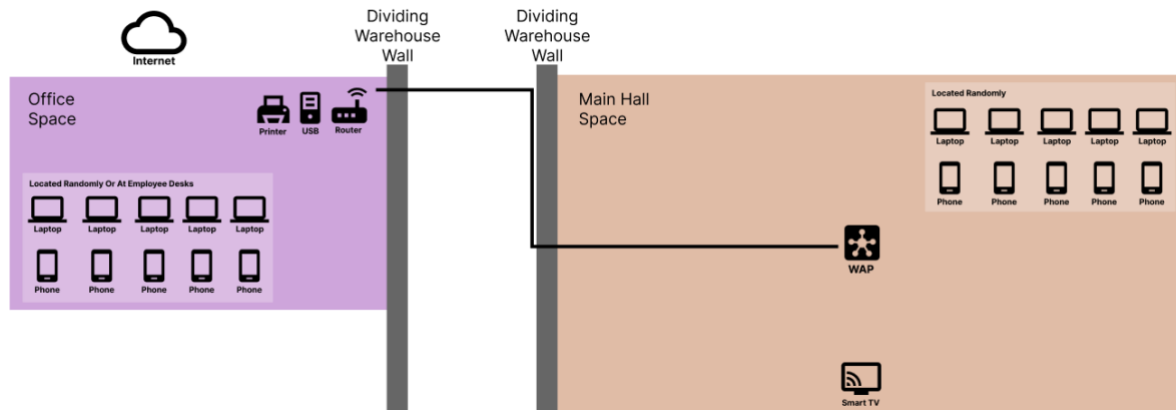


Figure 3.2 - Network Physical Layout

## ISP Package Selection

The client requires the ability to stream and broadcast high quality video as part of their business operations. According to Netflix the recommended minimum bandwidth required for UHD streaming is to be at least 15 Mb/s (Netflix, 2019). Google on the other hand recommends at least 20 Mb/s for 4K video streaming (Google, 2024).

If we consider a scenario where all 5 employees are looking to seamlessly stream 4K quality video at once using the network, then the bandwidth would have to have at least 100 Mb/s capacity. This means that in principle the use of the ISP's Silver Package (100 Mb/s) would be appropriate for the business needs of the client. However, this would mean full utilisation of the network bandwidth in this case. As the company grows and employs more people it may require upgrading this ISP package to something more substantial.

## NETWORK HARDWARE REQUIREMENTS

To implement the proposed design, there will be various hardware components required, some of which the company is already in possession of. This section will detail the hardware requirements to implement the network in full including all hardware and connection mediums. This section will also aim to give an estimate of costing to implement this however this will be an estimate as no floor plans for the building have been provided to estimate cable lengths required.

### Required Hardware List

The following is a list of the required hardware for the network with some indicative prices:

- 1 x Router (Synology RT2600ac Hybrid Wired/Wireless Provided by the ISP)	£0.00
- 1 x Printer (Already Owned, Suitable for Wired Connection)	£0.00
- 5 x Laptops and Smartphones (Already Owned – 1 / employee)	£0.00
- 1 x Wireless Access Point (e.g TL-WA801N)	£24.94
o At least 100 Mb/s bandwidth capacity	
o At least 1 ethernet port	
o Supports wireless connection for at least 11 devices (phones, laptops and Smart TV)	
- 1 x Cat 5e patch lead (Connect Router to Printer – say 2m long)	£1.45
- 2 x Cat 5e ethernet lead (Connect Router to Internet and Connect Router to WAP – say 0.5m long and 10m long)	£7.18
- 2 x CLEARSTOP Locking Access Point Cover   Lockable Router Protector Guard	£80.60
Total Hardware Cost	£114.17
+ 15 % Contingency	<b>£131.29</b>

## Hardware Choice Rationale

A router is provided by the ISP which has numerous capabilities such as 4 ethernet ports, WAP (up to 100 devices), a USB port and various other security functions (firewall, content filter etc.).

The wireless access point for the main hall has been chosen as it only need to provide a node for devices in the main hall to wirelessly connect to which in turn connects back to the router in the office which is connected to the internet. The direction of this network traffic flow means that the WAP in the main hall doesn't need to provide additional security measures such as firewalls etc. as this is handled by the router in the office.

Cabling for the network has been chosen as Cat5e which has a bandwidth transmission capacity of 1 Gb/s. It is noted that this exceeds the currently proposed 100 Mb/s bandwidth package for the network, but it is thought that this stage that this degree of future proofing for the network is necessary especially when the total length of cabling is so minimal that it makes the cost of Cat5 and Cat5e similar.

# NETWORK SECURITY

Network security is critical to network design. The security for the network will be tackled in a holistic manner looking at a multi-layered approach.

This will include the following measures:

- IPv6 (Network Layer)
- Firewall (Network/Transport/Application Layers)
- Authentication (Application Layer)
- Encryption (Presentation Layer)
- Content Filtering (Application Layer)
- Physical Security (Physical Layer)

## IPv6

IPv6 was designed with security in mind and as such offers several benefits to the security of the network and its data. The authentication header in IPv6 ensures the integrity of data packet payload transmitted using it and allows the receiver to verify the validity of the source in which the data has come from. Using the Encapsulation Security Payload Header in IPv6 the header data for a packet can be encrypted to ensure confidentiality and security of the data packet.

## Firewall

The ISP router has firewall functionality built-in which is good for network security by monitoring the ingoing and outgoing traffic on the network and making decisions on whether to allow or deny that traffic. The network has purposely been designed so that all traffic must pass through the firewall (router) before it can enter or leave the network. This means that security measures aren't required on each device as their network traffic is managed by the firewall. The firewall will utilise an access control list which is the set of rules it uses to determine whether to deny or allow network traffic.



## Authentication

Authentication and access control forms a key part of how users gain access to the network. Authentication can take many forms with the following being recommended to be implemented as part of the network design:

- Username and Password

Each user for the network will be given a username in the form of their company email which they can use to login to the network, along with this username users will be required to create their own secure password to gain entry to use the network. A security policy detailing how to create a strong password has been provided in the appendices (Appendix B).

## Encryption

It is proposed that IPSec is used in conjunction with IPv6 to encrypt the data packets and their headers sent and received on the network. This will help to ensure that data on the network's security and privacy are upheld.

The network will utilise WPA2 as the form of encryption for all Wi-Fi connections. For the network this is used instead of WPA3 as WPA2 is more common and supported on a wider range of devices and it cannot be confirmed yet that all proposed devices on the network will support WPA3.

## Content Filtering

Client requirements dictate that regular employees shouldn't be able to access social media sites but that the boss should be able to. This is achieved using the content filter provided by the ISP router. Profiles can be created in the content filter for admins and employees with the appropriate filtering rules applied to suit requirements.

## Physical Security

Whilst a server room is not proposed as part of the network design care should still be taken as to the physical security of the network critical components such as the router and WAP as these are a single point of failure in the topology.

It is recommended that the following measures of physical security be implemented for the network:

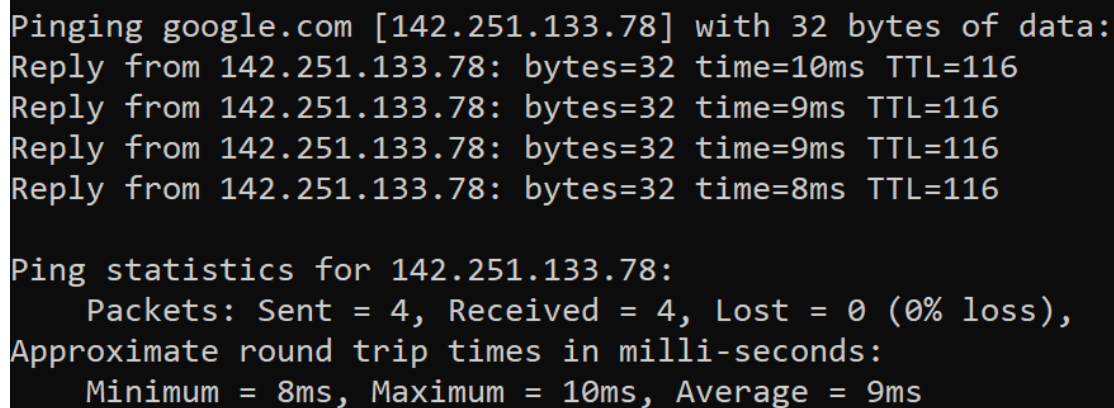
- Office doors and windows to be secured appropriately with lock and key when unoccupied to ensure the security of the router and file server.
- WAP in the main hall to be situated on the wall (secured by locked enclosure) or on the ceiling (secured by dome enclosure) as to prevent tampering by students

## NETWORK TROUBLESHOOTING AND ANALYSIS

As stated in the requirements, the client only requires knowledge of the ping network function to check which of the employees are online. This figure below shows how this feature can be used and the expected outputs:

Using the command window enter the following, inserting the IP address of the laptop you wish to ping where indicated:

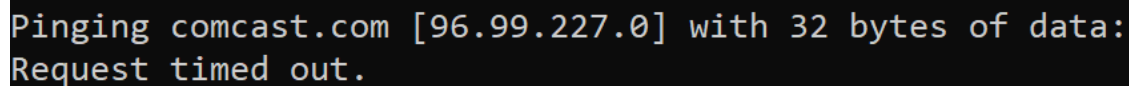
**ping [Employee Laptop IP Address]**

A screenshot of a command prompt window showing the output of a successful ping command. The text is as follows:

```
Pinging google.com [142.251.133.78] with 32 bytes of data:
Reply from 142.251.133.78: bytes=32 time=10ms TTL=116
Reply from 142.251.133.78: bytes=32 time=9ms TTL=116
Reply from 142.251.133.78: bytes=32 time=9ms TTL=116
Reply from 142.251.133.78: bytes=32 time=8ms TTL=116

Ping statistics for 142.251.133.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 10ms, Average = 9ms
```

*Figure 6.0.1 – Example of Successful Network Ping (Kinsta, 2022)*

A screenshot of a command prompt window showing the output of an unsuccessful ping command. The text is as follows:

```
Pinging comcast.com [96.99.227.0] with 32 bytes of data:
Request timed out.
```

*Figure 6.0.2 – Example of Unsuccessful Network Ping (Kinsta, 2022)*

## FUTURE PROOFING AND REDUNDANCY

A degree of redundancy and future proofing has been provided but kept to a minimum to keep costs lower for the client.

Below is a summary of these measures and the impact they will have on the network:

- **Cat 5e Cabling** – Allows bandwidths of up to 1 Gb/s facilitating any future bandwidth upgrades to the network.
- **WAP device capacity** – Allows for significant number of devices to connect wirelessly to the network (up to 100 devices)
- **Spare Switch Port** – One spare switch port allowing for additional subnets if required.
- **IPv6 Subnets** – 2/16 possible subnets used in current network design meaning 14 spare subnets

# NETWORK DESIGN CRITIQUE

This section will look to summarise the main aspects of what works well in the design. It will also examine areas of improvement for the design which the client may wish to implement.

## Design Strengths

- **Star Topology:** Central node allows for effective network traffic handling and security for each subnet. Resiliency achieved as outages of spokes will not result in entire network outage. Minimised wired connections. Highly performant due to avoidance of data collisions. Ease of adding and removing wireless devices makes network expandable.
- **IPv6 Addressing:** Adapting to modern technology helping to transition from IPv4. Enhanced security through encryption and encapsulation. More address spaces mean better scalability of network.
- **Network Security:** Physical security measures ensuring access and physical damage to hardware is minimised. Firewall within the router monitors network traffic providing protection from external threats.
- **Cost Efficiency:** Minimised use of wired network connections. Appropriate ISP package selected to meet client requirements. No excessive redundancy in the network. Simplistic network design allowing for minimising of maintenance costs.

## Improvement Areas

- **Redundancy:** With the single point of failure being the central node of the subnets failure of this would mean a significant outage. Consider future upgrades with further subnetting, redundant connections and even additional ISPs when cost can be justified. There should also be consideration for data backups using a cloud service, this might be too costly currently for the clients needs.
- **Scalability:** ISP package was chosen to be most cost effective for current business needs, however as the company expands this could become a bottleneck for the network and should be reviewed regularly to suit business needs.
- **Setup Complexity:** Using IPv6 and Firewalls will require careful consideration by an experienced network admin to setup to ensure they work correctly.
- **Multi-Factor Authentication (MFA):** Current design only uses single factor authentication for network access to make the experience simpler for end users however consider the use of MFA to improve security.

## DISASTER PLAN (MAIN HALL WAP)

This section will briefly outline the disaster plan for the WAP in the main hall. It is reasonable given the exposure to persons out with the business (students) that vandalism and theft is a real threat for the WAP in the main hall.

As such risk control measures have been implemented to sufficiently defend this asset against these types of threats. The following has been implemented in the network design as a means of defence:

- WAP positioned on ceiling (if possible): Limits the ability to access the WAP discretely.
- Protective Dome: Obscures the asset from lines of sight and acts as a protective cover to protect against physical attacks

## DISASTER SCENARIO (PANDEMIC)

Given recent history it is entirely possible that another pandemic could force people to work from home for significant length of time. The network has accounted for this with the provision of a VPN as part of the ISP router functionality.

Once setup, the VPN will allow remote users to securely connect to the business network to communicate with other devices on the network such as the file server or printer. The VPN will help to ensure secure transmissions between the user and the network however it is good practice to still require network traffic to pass through the firewall before going into the network as an enhanced level of security. The figure below explains how this will work in practice.

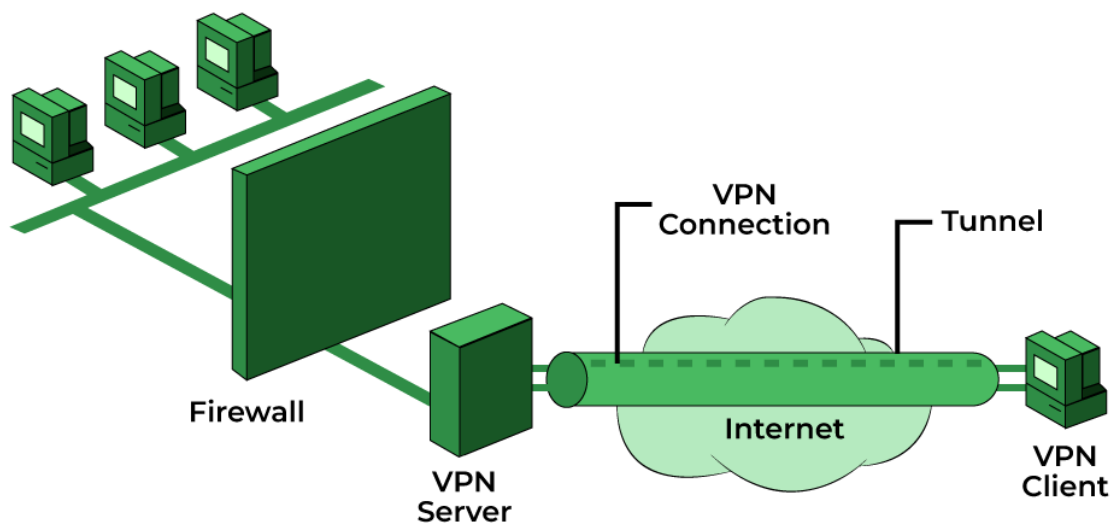


Figure 10.1 - Indicative Diagram of VPN on the Network (Geeks for Geeks, 2022)

## References

Fortinet (n.d.). *Static vs. Dynamic IP Address: Similarities and Differences*. [online] Fortinet. Available at: <https://www.fortinet.com/resources/cyberglossary/static-vs-dynamic-ip#:~:text=A%20static%20IP%20address%20is%20the%20better%20option%20for%20enterprises>.

Geeks for Geeks (2022). *Relationship Between VPN and Firewall*. [online] GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/relationship-between-vpn-and-firewall/>.

Google (2024). *System requirements - YouTube Help*. [online] support.google.com. Available at: <https://support.google.com/youtube/answer/78358?hl=en-GB>.

Kinsta (2022). *How To Ping an IP Address*. [online] Kinsta®. Available at: <https://kinsta.com/knowledgebase/how-to-ping-an-ip-address/> [Accessed 16 Jun. 2024].

LinkedIn (2024). *Streaming into the Future: How Switching to IPv6 Fuels Growth and Innovation?* [online] www.linkedin.com. Available at: <https://www.linkedin.com/pulse/streaming-future-how-switching-ipv6-fuels-growth-innovation-n9crf/> [Accessed 15 Jun. 2024].

Netflix (2019). *Internet Connection Speed Recommendations*. [online] Help Center. Available at: <https://help.netflix.com/en/node/306>.

Wikipedia Contributors (2020). *Star network*. [online] Wikipedia. Available at: [https://en.wikipedia.org/wiki/Star\\_network](https://en.wikipedia.org/wiki/Star_network).

## *APPENDIX A – NETWORK DESIGN BRIEF*





# Abertay University

**School of Design and Informatics**

**Session 2023/24**

**HEP506: Networking**

**Module Tutor: Adam Greatrix**

**Unit 2 of Module Assessment 70%**

**Module Outcomes Assessed by this Assessment:**

**MO1: Understand concepts of advance network operations and models.**

**MO2: Apply and evaluate a range of network solutions concerning network devices and software protocols.**

**MO3: Critically analyse the architecture and implementation of networked systems and recommend improvements or solutions.**

**Date of Issue: Week 1**

**Submission Date: Monday 9am Week 8**

**Grade Release and Feedback date: Monday Week 11**

## Assessment Overview

The main component of assessment for this module is the comprehensive design of a network (70% weighting). Assessment of work is based on a plan document which should demonstrate reasoning, reflective and critical thought. It is therefore important to record thoughts, decisions, and designs in some form of personal journal; creating the plan is then much simpler.

## The Network Scenario

A Martial Arts school, Eagle Fang Karate, does not currently have a computer network.

The five employees of Eagle Fang Karate each have a laptop.

For internet access while at work, they currently use their own mobile phone's Hotspot, and connecting their laptops to their mobile phones via WiFi. However, their mobile phone signal is poor in the building, so the Internet connection is very slow and frustrating using this method.

When they want to print something, they take their laptop over to the Laser Printer and temporarily connect their laptop to the printer via a USB lead.

The printer does have an unused network port, which may be useful, but unfortunately it doesn't have WiFi capability.

They also have a USB Hard Drive on which they store company files. This is currently passed around the office and connected to laptops via a USB cable. It does not have any networking capabilities and is just a standard USB drive.

There are only two rooms to consider at the Dojo: A main hall where martial arts training takes place, and a smaller office which the five staff use when not teaching in the main hall. The building is of a warehouse type construction, with metal walls that are likely to block WiFi signals.

Eagle Fang Karate have given you the task of planning a network. To begin the process, they have given you the following list of goals:

1. Provide fast internet access to our five employees while they're at work. Fast enough so that YouTube doesn't sit there buffering all the time when we set it to 4K video and so we can watch Netflix in Ultra High Definition. We don't want to pay more than necessary for this as we don't have much money due to the cost-of-living crisis.
2. Prevent employees from viewing adult websites and TikTok.
3. Allow the boss (me) full access to all websites.
4. Connect our existing laser printer to the network so that we can print stuff without having to mess around with USB leads.
5. Make sure students and other visitors to the building can't gain wired or wireless access to the network.
6. We would like staff to be able to use our Internet with their mobile phones so it's faster and so we don't use up our mobile data.

7. We have a gigantic brand-new smart TV in the main hall. We want to use it to watch Netflix on in Ultra HD after Karate classes have finished in the evening. Again, no buffering or slow network connections here please.
8. We have a USB hard drive, which we insist is the only place where we store company related files (our laptops keep getting left on busses and stolen). We only work on these files while at the office so we aren't likely to need remote access to this. Currently we connect this to our laptops using a USB lead but would love this on the network.
9. We want to use WiFi, where possible. I don't like too many messy wires or holes in my walls, although it would be OK to put one cable through to the main hall if needed.
10. If another pandemic hits, we want to be able to stream live karate training classes to our students using that Zoom video conferencing thing. We can just take a laptop to the main hall for that or do it from home.
11. I want our network to be secure from hackers – we have secret martial art techniques that we don't want rivals stealing.
12. I want everything to be really simple as I'm not very good with technology.
13. However, I do want to ping employee laptops from home to see who's in work. You'll need to show me how to do that. That's all the network diagnostic and reporting tools that I'll need, just ping.

## **The Network Plan**

You are to produce a plan document that includes the design and critical thought for a plan of a network solution to an authentic scenario, including its hardware, architecture, resilience and security.

Your plan should cover the following:

- 1) A list of all hardware devices (nodes) for the network, including the devices people will use at work (e.g. laptops, mobile phones, printers, firewalls, routers, WiFi Access Points, etc).
  - a) The ISP provides an Internet (WAN) connection to a Synology RT2600ac Router, which can be placed anywhere in the office. It includes the following features:
    - i) Firewall.
    - ii) 4-port Switch.
    - iii) Wireless Access Point (maximum 100 devices).
    - iv) Content Filter (called Safe Access).
    - v) Threat Prevention.
    - vi) VPN Server for Remote Access.

- vii) A USB port to connect a USB hard drive to in order to create a network accessible drive or network attached storage.
- 2) A diagram of the network, including all hardware (nodes) and links (indicate WiFi or cable connection) between them.
  - a) You can use any tool you want to create this, for example the graphics tools in Word or a website like <https://www.smartdraw.com/network-diagram/network-diagram-software.htm>
  - b) You can either decide on your network topology before creating the diagram, or let the diagram dictate the topology.
- 3) A bullet list of requirements of the network, including:
  - a) Your interpretations of the list of requirements provided by the customer (see above).
  - b) The required package from the ISP. They offer (cheapest to most expensive):
    - i) 10Mbit/s "Bronze Package".
    - ii) 100Mbit/s "Silver Package".
    - iii) 1,000Mbit/s "Gold Package".
    - iv) 10,000Mbit/s "Platinum Package".
- 4) A list of constraints that may hinder or prevent any goals.
- 5) The number and types of users (e.g. administrators, staff, visitors, etc).
- 6) Comments on any devices with special requirements (e.g. minimum network speeds).
- 7) A diagram of the physical layout (just two adjacent square rooms – a big hall and a smaller office) of the building, including where devices are going to be located, where physical network connections are available, and the location of WiFi Access Points. There are many electrical outlets on every wall so you don't need to consider these.
- 8) A shopping list for anything the company does not already own and isn't provided by the ISP, including:
  - a) Any additional hardware needed.
  - b) And ethernet cables needed (number required and category).
- 9) A concise description of the design of your network, including:
  - a) Network Topology.
  - b) Category of network cable.
  - c) Choice of ISP package (see above).
  - d) Number of wired devices vs wireless devices vs hybrid devices (supporting both wired and wireless connections), and the maximum number of wired and wireless devices the network has capacity for with the current hardware.
  - e) State how many subnets you will choose to use, and why.
  - f) State whether you will choose to use Static IP Addresses or Dynamic IP Addressed managed by DHCP and why.
- 10) A critical evaluation of the network design.

- a) This should cover what is good about the proposed plan, what is poor and what could be improved.
- 11) Security
  - a) Windows Login Authentication – Write a brief password security policy (you can use a template for this if you wish), which includes recommendations on how to choose a good password and any requirements on complexity or length or other advice.
  - b) WiFi Authentication and Security – What type of WiFi security protocol or protocols (e.g. WPA) will you use and why?
  - c) Physical Security – List any recommendations for building access.
- 12) Document and justify any other considerations or additions, if required:
  - a) Future proofing the network.
  - b) Any redundancy or backup solutions.
- 13) Network Analysis
  - a) List any network analysis tool(s) required by the customer and why.
  - b) Where possible, provide an example of how the customer can use the tool(s) and how to interpret the results.
- 14) Disaster plan - Create a very brief disaster plan that covers any single asset of your choice:
  - a) Identify the asset.
  - b) Identifying a potential threat to that asset.
  - c) Choose and justify a risk control strategy (defence, transference, mitigation, acceptance, or termination).
- 15) Disaster Scenario – A new and deadly virus becomes prevalent. The government puts the whole country into full lockdown, forcing everyone to work from home only. No exceptions.
  - a) What features of your network are now required to support home working?
  - b) If your network doesn't support home working in its current state, what would you add to achieve this?

Your plan should be relatively concise (around 3000 words, maximum 4000 words) and aimed at people trained in networks and network jargon.

## **Grading the Assessment**

### **The plan (100% weighting)**

Should be well written and structured in a style suitable for a technical plan.

## **Submission**

***You must submit your plan using the link provided on the HEP506 module page in Canvas.***

- Network Plan: Up to a maximum of 4000 words of text (excluding any references, appendices, bibliography, etc, if included).

All submissions must be uploaded to the appropriate location within the Canvas system. The deadline for submissions is 9am and the system is likely to be busy at that time. **For this reason, you are advised to leave plenty of time (at least an hour) to successfully complete the upload process. If the Canvas system records a submission time after 9am then the work will be treated as a late submission.**

### HEP506 – Coursework Grading Criteria

	A+/A	B+/B	C+/C	D+/D	MF/F
<b>Explanation of issues (20%)</b>	Issue/problem to be considered critically is stated clearly and described comprehensively, delivering all relevant information necessary for full understanding.	Issue/problem to be considered critically is stated, described, and clarified so that understanding is not seriously impeded by omissions.	Issue/problem to be considered critically is stated but description leaves some terms undefined, ambiguities may be unexplored, boundaries undetermined, or backgrounds unknown.	Issue/problem to be considered critically is stated but is lacking any description with terms undefined,	Issue/problem to be considered critically is stated without clarification or description.
<b>Evidence <i>Selecting and using information to investigate a point of view or conclusion</i> (20%)</b>	Information is taken from source(s) with excellent interpretation/evaluation to develop a comprehensive analysis or synthesis. Viewpoints of experts are questioned thoroughly.	Information is taken from source(s) with very good interpretation/evaluation to develop a coherent analysis or synthesis. Viewpoints of experts are subject to questioning.	Information is taken from source(s) with some interpretation/evaluation. Viewpoints of experts are taken as mostly fact, with some questioning.	Information is taken from source(s) with brief interpretation/evaluation. Viewpoints of experts are taken as mostly fact, with little questioning.	Information is taken from source(s) without any interpretation/evaluation. Viewpoints of experts are taken as fact, without question.
<b>Influence of context and</b>	Thoroughly (systematically and	Identifies own and others'	Questions some assumptions. Identifies	Shows an emerging	Limited awareness of present

<b>assumptions (20%)</b>	methodically) analyses own and others' assumptions and carefully evaluates the relevance of contexts when presenting a position.	assumptions and several relevant contexts when presenting a position.	several relevant contexts when presenting a position. May be more aware of others' assumptions than one's own (or vice versa).	awareness of present assumptions (sometimes labels assertions as assumptions). Begins to identify some contexts when presenting a position.	assumptions Limited identification of context when presenting a position.
<b>Student's position (perspective, thesis/hypothesis) (10%)</b>	Specific position (perspective, thesis/hypothesis) is imaginative, taking into account the complexities of an issue. Limits of position (perspective, thesis/hypothesis) are acknowledged. Others' points of view are synthesized within position (perspective, thesis/hypothesis).	Specific position (perspective, thesis/hypothesis) takes into account the complexities of an issue. Others' points of view are acknowledged within position (perspective, thesis/hypothesis).	Specific position (perspective, thesis/hypothesis) acknowledges different sides of an issue.	Specific position (perspective, thesis/hypothesis) is stated, but is simplistic and obvious	Specific position (perspective, thesis/hypothesis) is lacking or flawed.
<b>Conclusions and related outcomes (implications and consequences) (20%)</b>	Conclusions and related outcomes (consequences and implications) are logical and reflect student's informed evaluation	Conclusion is logically tied to a range of information, including opposing viewpoints; related outcomes (consequences and	Conclusion is logically tied to information (because information is chosen to fit the desired conclusion); most related outcomes	Conclusion is loosely tied to the information presented in the report.	Conclusion is inconsistently tied to some of the information discussed; related outcomes (consequences and implications) are

	and ability to place evidence and perspectives discussed in priority order.	implications) are identified clearly.	(consequences and implications) are identified clearly.		oversimplified.
--	---	---------------------------------------	---	--	-----------------

Component	Maximum Score	Literal grade
Network Plan	50	<u>&gt;84% (A+)</u> <u>&gt;69% (A)</u> <u>&gt;64% (B+)</u> <u>&gt;59% (B)</u> <u>&gt;55% (C+)</u> <u>&gt;49% (C)</u> <u>&gt;44 (D+)</u> <u>&gt;39 (D)</u> <u>&gt;35 (MF)</u> <u>&lt;=35 (F)</u>



## *APPENDIX B – PASSWORD SECURITY POLICY*

## EAGLE FANG DOJO – NETWORK PASSWORD SECURITY POLICY

### OVERVIEW

Passwords form a key line of defence against hackers and malicious actors gaining access to your network and by extension, your sensitive business information. Poorly chosen passwords can compromise the entirety of the Eagle Fang Dojo's network and have a serious impact on the business. Considering this all-Eagle Fang Dojo employees are responsible for choosing a secure password.

### PURPOSE

The purpose of this policy is to set a standard for the creation of passwords which will be strong enough to provide sufficient protection for the network. It will also outline how these passwords should be protected and how often they should be changed.

### AUDIENCE

This policy applies to all employees of Eagle Fang Dojo who have an account on any system which resides at the Eagle Fang Dojo, has access to the network or stores any non-public Eagle Fang Dojo information.

X

## POLICY DETAIL

### USER NETWORK PASSWORDS

Passwords for Eagle Fang Dojo network access must be implemented according to the following guidelines:

- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#\$%^&\* \_+=?/~';',<>|\).
- Passwords must not be easily tied back to the account owner such as:
  - username, social security number, nickname, relative's names, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for 1 year

### SYSTEM-LEVEL PASSWORDS

All system-level passwords must adhere to the following guidelines:

- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use

---

## PASSWORD PROTECTION /R

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Eagle Fang Dojo information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- Eagle Fang Dojo passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
  - o Take control of the passwords and protect them
  - o Report the discovery to IT
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.

- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
  - o Take control of the passwords and protect them
  - o Report the discovery to IT /R
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with Eagle Fang Dojo

---

## APPLICATION DEVELOPMENT STANDARDS

Application developers must ensure their programs follow security precautions in this policy and industry standards.