;

LAN Design Group Assignment

2024

Contents

Introduction ......................................................................................... 2

Cabling ............................................................................................... 3

Wirelist ............................................................................................... 8

MDF .................................................................................................. 12

IDF ................................................................................................... 17

Wireless ............................................................................................. 25l00

Access Points ....................................................................................... 26

VoiceOver & Teams ............................................................................... 29

ClearPass ........................................................................................... 30

Vlans ................................................................................................ 32

Subnets ............................................................................................. 38

Security ............................................................................................. 42

Servers .............................................................................................. 45

Conclusion .......................................................................................... 49

Appendices ......................................................................................... 51

# Introduction

As a group, we collaborated to design the Local Area Network (LAN) for Letterkenny ATU. This project required us to dive deeply into the principles and practices of LAN design, discussing in detail the “why” and “how” behind the network’s architecture and implementation. A well-designed LAN is not only critical for efficient communication across the network but also for supporting the operational needs of Letterkenny ATU. Our design focuses on achieving an optimal balance between performance, scalability, and cost-effectiveness, ensuring the network can handle current demands and future growth.

Throughout the project, teamwork played a pivotal role in ensuring its success. Each member of the group was assigned specific tasks based on their strengths, allowing us to divide the workload efficiently. At every stage, we worked together to evaluate each other’s contributions, ensuring that all parts of the project aligned with our shared vision. This collaborative approach fostered a sense of accountability and allowed us to learn from one another, refining the project as we progressed. By pooling our efforts and ideas, we ensured that the final design reflected the collective input and expertise of the group.

The project also required careful consideration of the core components of a LAN design. We explored the requirements of Letterkenny ATU, identifying key elements such as scalability, security, redundancy, and performance. Our design includes a logical layout of network devices, an appropriate choice of hardware, and a structured cabling system that ensures reliability and easy maintenance.

Ultimately, we aimed to create a LAN design that is not only functional and effective but also cost-efficient and easy to manage. We believe our final proposal addresses the unique needs of Letterkenny ATU while adhering to industry standards and best practices for network design. This introduction highlights the thought process, teamwork, and methodologies employed in this project, setting the foundation for a detailed analysis of our LAN design.

# Cabling

Cabling is one of the most important parts of your network, cables are expected to last up to 15-20 years. It is likely that every other component in your network will be replaced before you need to replace or re-install your cabling, you shouldn’t cheap out on setting up your cables because you never know how many more cables you may need down the line the more you have the better. High quality cables can reduce downtime, maintenance and better network performance.

You should definitely consider, your network application, upgrades, life span, distance, cable routing, fire risk, existing cables, EMI and your environment before setting up your cabling system.

The type of network it is for will determine the type of cable best for the job. We should be prepared to make changes based on upgrade or additions to the network in the future. We should try set up a system we expect to last a minimum of 15 years. We should take into account the distance between or switches and devices and the available space to for running our cables (in the ceiling or floor for example). We need to check if there’ll be any electromagnetic interference and keep the environment in consideration in case of flooding or other limits.

There are 2 basic choices when it comes to picking your cabling type, copper or Fiber. Your decision should be based on your current network, what you plan on using your network for in the future how far you intend to go with your cables, cost and environment. Usually, copper is used if you don’t require high speeds and for short distances, but you can get copper cables that are capable of reach upwards of 100Gbs per second, there are often mixed networks now of copper cables for horizontal cabling and fiber cables where the fiber for the backbone cabling.

## Copper cables

Copper cables are a lot cheaper than fiber cabling and are much easier to remove because copper is the most commonly used form of cabling. There are a few different types of copper cables e.g. UTP, STP.

UTP (Unshielded twisted pair)

This is the most commonly used form of copper cabling, it consists of twisted pairs of wires covered in PVC or plenum. It should be installed by trained technicians; it should be installed in electrically quiet environments. The performance can be affected by field terminations, bend radius, tension and cinching which could all loosen the pair twists.

A close-up of a cable

Description automatically generated

### STP (Shielded Twisted pair)

STP is effective at reducing EMI (electromagnetic interference) and increasing cable distance. EMI is caused by sources like motors, fluorescent lights, generators, air conditioners, and printers. While STP cables offer shielding, they can be less balanced than UTP due to the added metal. Proper grounding of the metal is necessary to eliminate EMI effects on the conductors.

Shielded cables are more expensive, harder to bend, and more challenging to install compared to UTP. Their thickness can also take up more space in conduits. STP consists of twisted pairs of wires shielded by metal, typically with either foil sheaths or copper braids. Copper braids offer about 90% coverage and are better at blocking lower-frequency EMI, while foil sheaths provide 100% coverage and protect against a broader range of interference. Combining both is ideal for maximum protection.

### Solid and Stranded Conductors

Copper cable conductors are either solid or stranded it doesn’t matter if the cable is shielded or not.

Solid conductors are designed for both backbone and horizontal cabling, it is great for running it between rooms which is great for our use of connecting to so many devices. However, they shouldn’t be bent which makes it harder for laying out the cabling system. There isn’t much loss of connectivity as it travels through the cable at long lengths.

Stranded conductors are used as a patch cable between the pcs and the outlet and other devices, it is more flexible which is great for setting up computer rooms, but it reduces the signal as it travels through the cable, so it is recommended to have shorter cables.

We will use each form for different purposes, the solid conductors will be for back bone cabling and room to room connections, and we will use stranded conductors for connecting the pcs to the low-end switches.

A close-up of a copper conductor

Description automatically generated

### Cable Categories

Primarily we will talk about CAT5e and CAT6 because they are the most viable cable categories to use.

Enhanced Category 5 or CAT5e cables were officially released in 1999 was designed to allow twisted-pair cabling that supports full-duplex and 100-MHz applications like 100BASE-TX for example. CAT5e has stricter performance requirements, including measures for near-end crosstalk (PS-NEXT), far-end crosstalk (EL-FEXT) and combined far-end crosstalk (PS-ELFEXT). It also includes testing for both the channel and components.

Category 6(CAT 6) is best for handily Gigabit Ethernet. It is a 100-ohm cable with a frequency of 250 mhz. CAT 6 has far more stringent performance parameters than CAT5e and is characterized by channel, link and component testing. In addition, CAT 6 components must be backward compatible with over level components, but all the channels will run on the lowest level.

For our campus, we plan to use STP cabling with both a copper braid and foil sheath to prevent interference and avoid disruptions to classes or work using Cat 6.This will be for our horizontal cabling. This solution will also help protect the cables from Ireland’s harsh, damp weather. The main challenges are cost and flexibility.

A table with numbers and symbols

Description automatically generated

### Fiber cable

Fiber optic cables transmit information using light. They consist of a core, a continuous strand of glass or plastic, measured in microns by the outer diameter size. This core serves as the pathway for light signals carrying data.

Fiber is the cable of choice for applications that demand high bandwidth, long-range capabilities, and resistance to electrical interference. It is also the most widely used backbone cable.

A close-up of a wire

Description automatically generated

### The advantages of fiber

**Greater Bandwidth**: Fiber offers significantly higher bandwidth than copper, supporting speeds up to 10Gbps and providing future-proof capabilities for network design. It can carry more data with greater accuracy.

**Low Attenuation and Longer Distances**: Fiber optic signals experience minimal signal loss, allowing data to travel at high speeds over longer distances. Depending on the cable type, wavelength, and network setup, fiber can support distances from 300m to 40km.

**Security**: Fiber ensures secure data transmission, as it doesn’t emit signals and is difficult to tap. Any attempt to tap the cable causes light leakage, leading to failure.

**Immunity**: Fiber offers reliable data transmission, unaffected by environmental factors that impact copper cables, such as EMI, crosstalk, and impedance. It can be placed near industrial equipment without interference and is less sensitive to temperature changes.

**Design**: Fiber is lightweight, thin, and more durable than copper, with pulling strength up to 10 times greater. Its compact size makes handling easier.

### Multimode vs. single mode

There are two types of fiber cables: multimode and single mode. Multimode fiber is commonly used within buildings, while single-mode fiber, offering higher performance, is typically used in campus networks between buildings.

Multimode cables have a large-diameter core and multiple light pathways, available in two core sizes: 50-micron and 62.5-micron. A table with numbers and text

Description automatically generated with medium confidence

Multimode fiber cable is suitable for most general data and voice applications. Both 50-micron and 62.5-micron cables have the same 125-micron cladding diameter, but 50-micron cable has a smaller core. Both types can use LED and laser light sources, with the 50-micron cable offering longer link lengths and higher speeds, especially at the 850-nm wavelength. For new installations, 50-micron cable is recommended for backbone, horizontal, and intrabuilding connections. While 62.5-micron multimode fiber is still in use due to existing installations, 50-micron is preferred for new projects. Multimode fiber is typically orange, with 50-micron optimized for 10-Gigabit applications being aqua.

Single-mode fiber, with an 8–10-micron core, allows only one light pathway, using a single wavelength of light that stays centred within the core. This gives single-mode cable up to 50 times more distance than multimode cable, making it ideal for long-haul connections, cable television, and campus backbone applications. Telecom companies use single mode for connections between switching offices. Single-mode fiber is traditionally yellow.

We primarily would be using multi-mode fiber for our campus, and we will use single-mode fibre for connecting to the CoLab building.

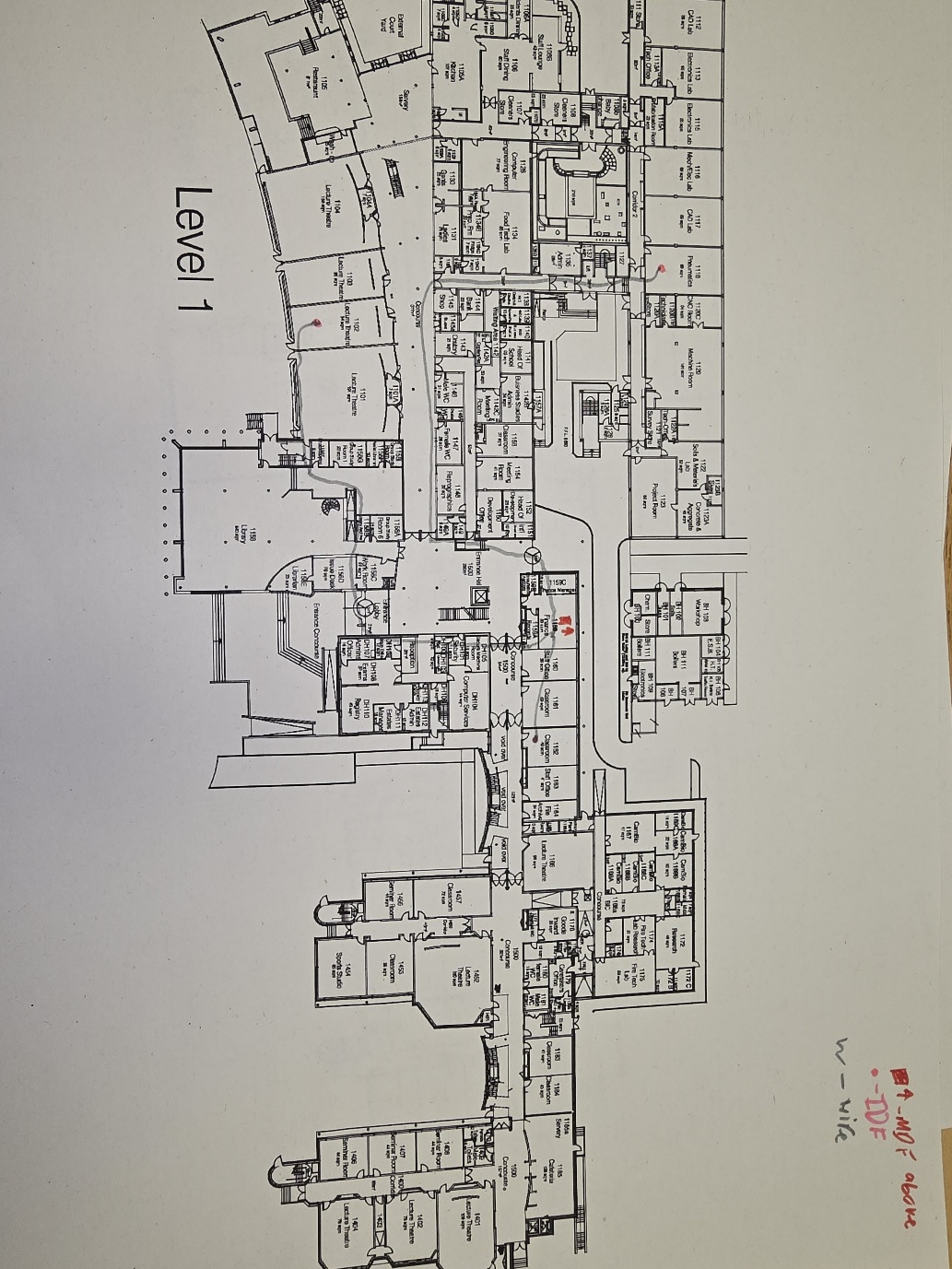
A diagram of different types of microelectronics

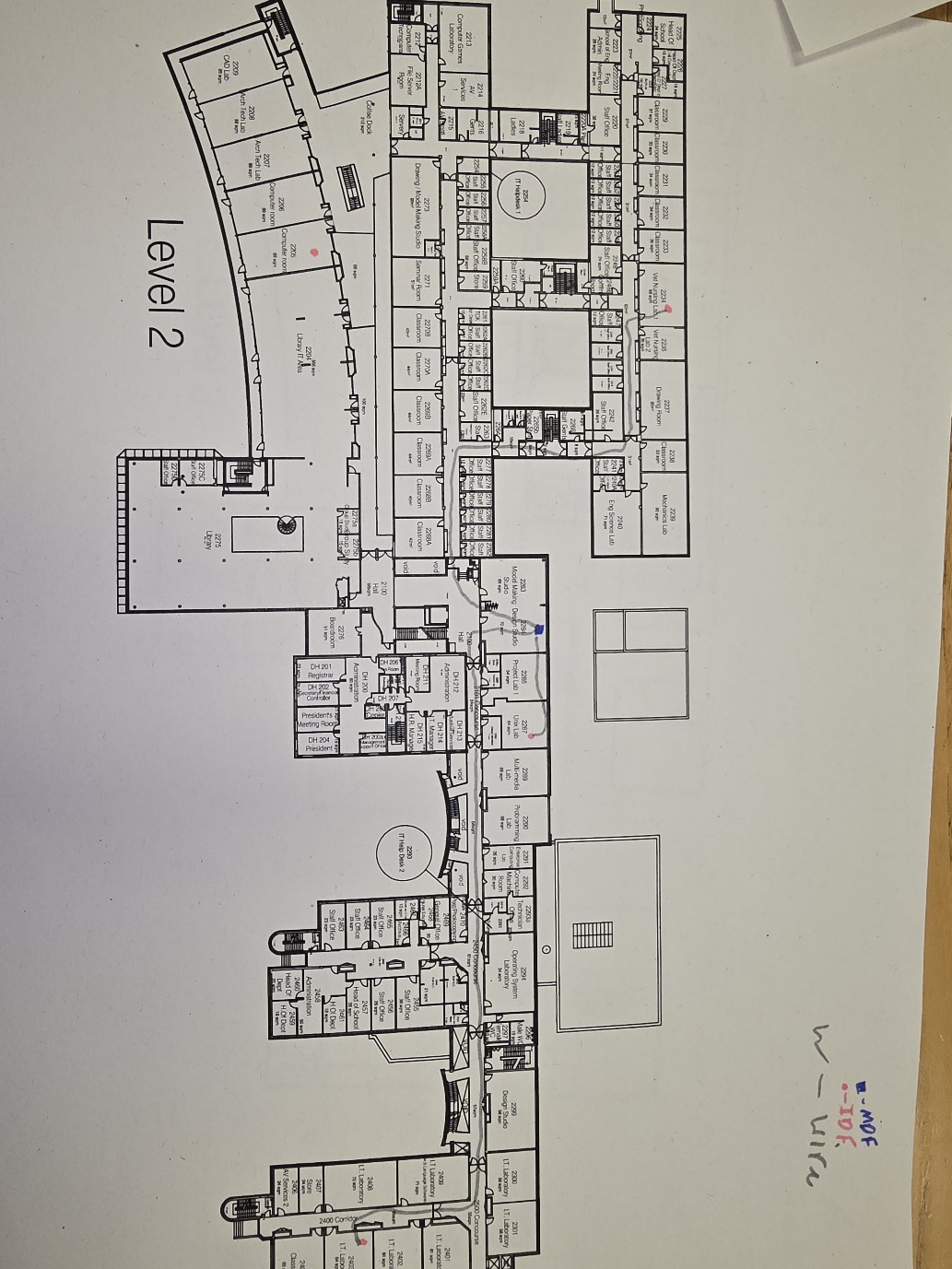
Description automatically generated

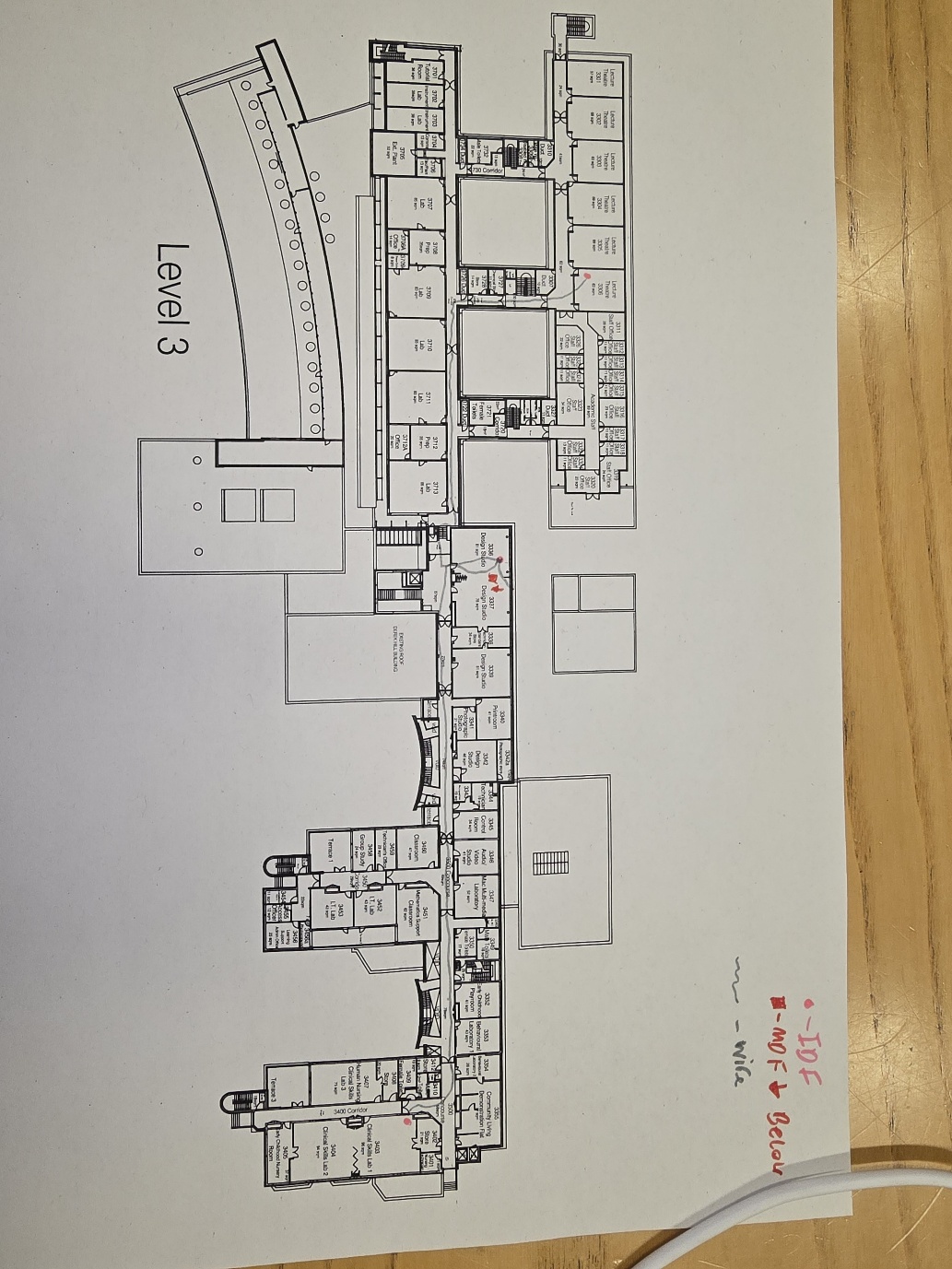
# Wirelist



This is our wire list it shows the number of devices and switches per IDF, it also shows the type of cable we are using in multimode fiber and single mode fiber cabling. The distance between each IDF is recorded and the distance between the IDF and the MDF is recorded as well.  
The cabling will be labled based on the IDF they are in for example in IDF 1\_a it will be labelled 1A-210, 1A representing the IDF number and 210 being the device number.







These are the maps of our wiring showing the IDF, MDF and the wires connecting from the IDF to the MDF.

# MDF

**What Is a Main Distribution Frame (MDF) Room?**

It is a central network hub thus why it is called the main distribution frame as its used commonly in data centres and enterprise networks as its essential for a smooth flow of data and allows better connectivity over all networks which makes it a more seamless operation. It is pivotal in any networking environment as it is the pivotal point where all communication lines congregate also for communication devices like data cables, internet connections and telephone lines.

So, the MDF room integrates outgoing and incoming communication lines within the Letterkenny ATU campus. The physical MDF is a set or singular panels where all the communications from all different parts of the Letterkenny ATU campus where it will be concluded or connected and for the case of the Letterkenny ATU it is a singular panel. Cables can be routed out to rooms or individual offices or rooms via individual offices intermediate distribution frames (IDFs) or network switches.



**What makes a good Main Distribution Frame (MDF) Room?**

**Clear identification in the MDF room**

* You should use clear labelling in the main distribution room on the hardware in the room and have it colour coordinated tags to speed up with identification of what each is and helps with visibility and easier to fix issues that arrive that way.
* Make sure each label only includes vital information like the Ip address, device name and its purpose and not much else as it would be overwhelming and only need what is essential.
* Also, we will need to implement a consistent naming templet in the mdf room for cables on both ends of the cables with matching identifiers to help during troubleshooting or upgrading to make it less confusing.
* Use rack-mounted trays or shelving systems to better organize smaller components. Ensure enough spacing between devices for proper airflow and easy access during maintenance tasks.
* Frequently review your setup and adjust as needed when new equipment arrives, or existing gear is upgraded or added upon.

**Power and Cooling for a Better MDF**

* **Assess the power needs of all devices:** Each piece of equipment has a specific wattage requirement that must be considered. It is crucial to avoid circuit overloads.
* **Plan for power redundancy:** Use uninterruptible power supplies (UPS) to ensure operations continue during power outages. This safeguards sensitive data and maintains network uptime.
* **Choose appropriate cooling solutions:** Cooling options range from simple air conditioners to advanced HVAC systems tailored for IT environments. Regularly monitor temperature levels to prevent overheating.
* **Manage airflow effectively:** Proper ventilation is essential to disperse heat generated by active equipment, maintaining an optimal environment for your networking gear.

**Safety And Maintenace**

**Implement security measures:**

* Use access control systems to limit entry to authorized personnel.
* Install biometric scanners for additional security.
* Set up surveillance cameras and alarms to monitor and protect sensitive equipment and data.

**Install fire protection systems:**

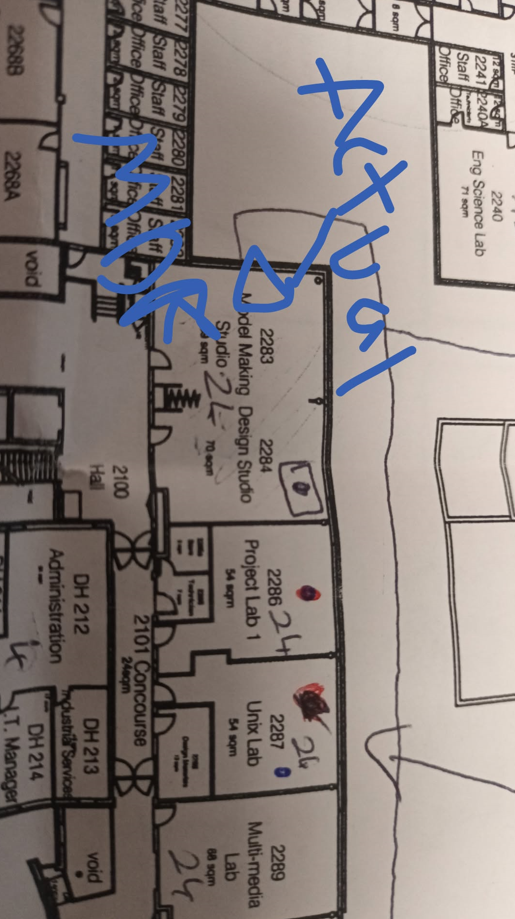
* Choose suitable fire suppression systems, such as fire extinguishers or sprinklers, to safeguard networking equipment from fire-related damage.
* Conduct regular inspections and maintenance of the fire suppression system to ensure it functions properly to ensure that it functions in the event of a fire.

**Regular maintenance tasks:**

* Schedule periodic inspections, maintenance, and cleaning of networking equipment and MDF room infrastructure to catch issues before they arrive such as checking to make sure wiring is all good and other physical hardware.
* Keep monitoring the temperature and humidity levels so that the equipment keeps running smoothly and ideally.
* Regular upkeep helps identify potential issues before they turn into major problems.

**Additional Things to Keep in Mind When Building a MDF room**

* **Make sure to have elevated floors:** Elevated floors, also known as raised floors, are crucial in an MDF (Main Distribution Frame) room. They provide a space beneath the floor for routing power cables, network cables, and cooling systems. This setup not only helps in managing cables neatly but also enhances cooling efficiency by allowing air to circulate better. Additionally, elevated floors can help in preventing damage from any potential water leakage or flooding incidents.
* **Do not have floors with carpet:** Carpets in an MDF room can cause several issues. Firstly, they generate and accumulate static electricity, which can be harmful to electronic equipment. Moreover, carpets trap dust and other particles that can affect the performance and longevity of your networking gear. Instead, use anti-static flooring materials, such as vinyl or rubber, which are easier to clean and maintain.
* **Have on an Outside wall:** Placing the MDF room against an outside wall can offer several advantages. It allows for easier installation of external cooling units, improving the efficiency of your HVAC system. Moreover, having access to an outside wall can facilitate the entry and exit of cables, minimizing the complexity of cable routing. This placement also provides better options for ventilation and natural cooling, helping to maintain optimal temperatures for your equipment.
* **No Emi interference: A room with little to no EMI interference is great for connectivity in the MDF room and makes for less issues.**
* **Room to Expand Into:** This is self-explanatory but having room to expand into for things you may want in the future is good for long term sustainability of the MDF room.



**Why This Room was Chosen**

The room 2283/2284 was chosen because it meets a lot of the criteria mentioned above like:

It has room to expand in the event we need to add more stuff into the MDF room and thus makes it ideal space wise

It is central to a lot of the ATU Letterkenny which is an estimated 200 meters which makes it an ideal spot in that aspect.

It is on an outside wall which is an aspect we would want we are choosing an ideal MDF room which this meets.

It has no carpet so it would be more cost effective which we would put towards other aspects of the MDF room.

It is on the 2nd floor of the Letterkenny ATU so it would be ideal in that sense to avoid potential flooding in the event of severe weather on the ground floor.

**Things We Would Need To Add**

We would need to add an elevated floor which would allow for better physical and logical connections between the equipment in the MDF room and the building's infrastructure thus making it a better EFI (Equipment Facility Interface).

We would need to add safety procedures and air conditioning units for the room to keep it properly temperate for its environment and add things in the event of a fire or so that we have so fire redundancy

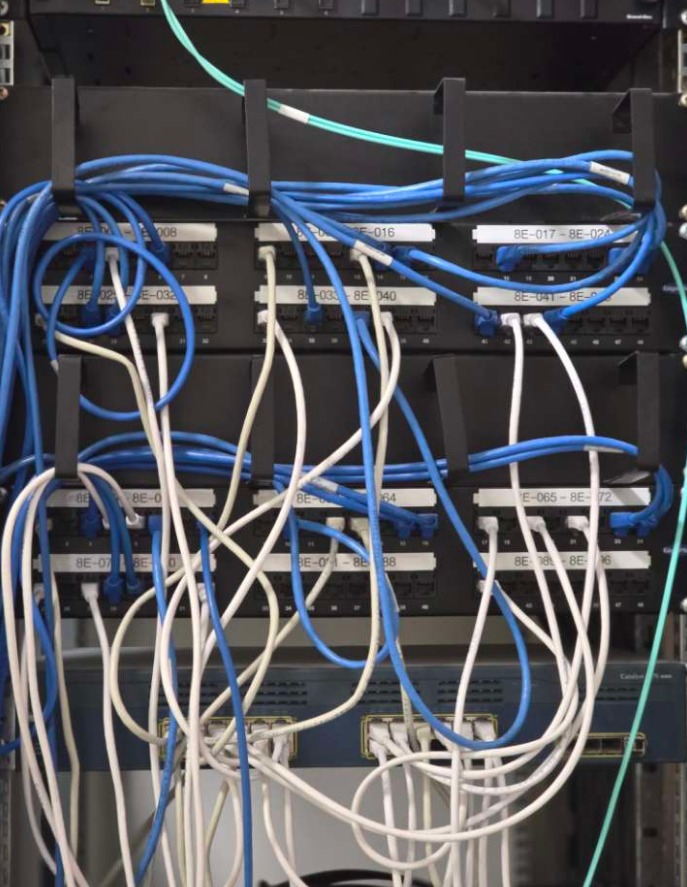
Implement security procedures like access control facilities, biometric scanners for additional security and add surveillance cameras for additional security of the MDF room.

This is just a brief explanation as I have mentioned it in detail above what a good one would have so we would add to that detail to ensure that it was great.

# **IDF**

**What is an IDF?**

An IDF (intermediate distribution frame) is a free-standing or wall-mounted rack used to create a connection between end user devices (e.g. PCs, printers, routers, VoIP phones) and the MDF (main distribution frame). IDFs can contain circuit termination equipment from various auxiliary components in central office environments. In both LAN and WAN environments, IDFs use numerous devices to operate, including backup systems (e.g. disk drives or RAID systems), connections (e.g. as coaxial, category and fiber optic cables) and networking devices, such as hubs, switches, routers etc. WANs and LANs often use IDFs which is the basis of this project as we are creating a Local Area Network. An IDF will primarily be at a central office or on customer premises.



**Designing and IDF Room?**

**Accessibility:** The IDF room should be adequately placed so technicians or other members have easy access to it and making sure maintenance staff can easily access it as well in case of any disruptions to the system.

**Environmental Factors:** An IDF should be placed in a room below 29 degrees Celsius and with a humidity level between 40-55% to prevent the equipment from overheating, avoiding dusty areas is also necessary or maintain the area well to avoid so.

**Proximity to End-User Areas:** When setting up the IDF we need to place it in an area so it can reach as many devices as possible, whilst taking into consideration the max length of the CAT6 cable that is 100m but for sake of performance and to avoid interference we are using 90 of the 100.

**Planning for Growth:** As for any business you should have spare room in the IDF stand as in the future the business may need to expand its services and as such require more maximum capacity from the IDF. By doing this you avoid further costs down the line of installing new stands or replacing older equipment with newer as with extra storage you can instantly insert new devices and makes it faster to set up.

**Maintenance:** An IDF closet requires regular maintenance to ensure the efficient operation and management of network infrastructure. Implement a maintenance schedule that includes routine inspections, updates, and equipment replacements. Additionally, incorporate regular firmware updates and security patches into the schedule. This proactive approach helps prevent data loss, network downtime, and security breaches.

**Benefits of IDFs?**

**Organisation:** IDFs play a critical role in organizing and streamlining network cabling. They transform what could easily become a chaotic tangle of wires into a neatly structured and centralized system. By consolidating cables into designated areas within an IDF, documenting the location of the incoming cable, labelling each cable, network management becomes significantly more efficient. This organization not only enhances the overall appearance of the infrastructure but also simplifies maintenance and troubleshooting processes. Instead of dealing with a disorganized mass of cables, technicians can quickly identify and address issues, saving valuable time and reducing the risk of errors. In short, IDFs are essential for maintaining a clean, professional, and manageable network setup

**Scalability:** As your network grows, IDFs make it easier to add new equipment or cabling without the need for a complete infrastructure overhaul. This streamlined approach enables your system to adapt seamlessly to expansion, supporting scalability and minimizing disruptions.

**Troubleshooting:** When network issues occur, IDFs enable you to localize problems to specific floors or zones. This targeted approach significantly speeds up the process of identifying and resolving issues compared to dealing with a disorganized network setup.

**Flexibility:** IDFs are designed to support various types of network equipment and cabling. Whether your system requires copper, fiber optics, or a combination of both, IDFs offer the flexibility to accommodate diverse configurations.

**Security:** Many IDFs are housed within lockable cabinets or racks, providing an added layer of physical security. This feature safeguards your valuable network equipment by preventing unauthorized access, accidental tampering, or potential damage. By restricting physical access to the equipment, these secure enclosures help maintain the integrity and reliability of your network infrastructure.

### **Switches in IDFs**

Switches are essential networking devices in IDFs that manage and distribute data to endpoint devices within a specific floor or zone.

#### **Functions of Switches**

1. **Data Distribution**:
   1. Switches connect to endpoint devices like computers, phones, and printers via structured cabling.
   2. They forward data packets only to the intended recipient device, ensuring efficient data flow.
2. **Connectivity Management**:
   1. Provide multiple ports to connect devices within the same local area network (LAN).
   2. Aggregate traffic from multiple devices to a single uplink connecting to the Main Distribution Frame (MDF).
3. **VLAN Support**:
   1. Allow for the creation of Virtual Local Area Networks (VLANs), enabling network segmentation for better security and traffic management.
4. **Power Over Ethernet (PoE)**:
   1. Many switches support PoE, providing power to connected devices like IP phones, cameras, and access points without needing separate power supplies.

#### **Advantages of Switches in IDFs**

* Enable efficient use of bandwidth and minimize network congestion.
* Simplify cable management by centralizing connections.
* Allow for scalability as network needs grow.

### **Routers in IDFs**

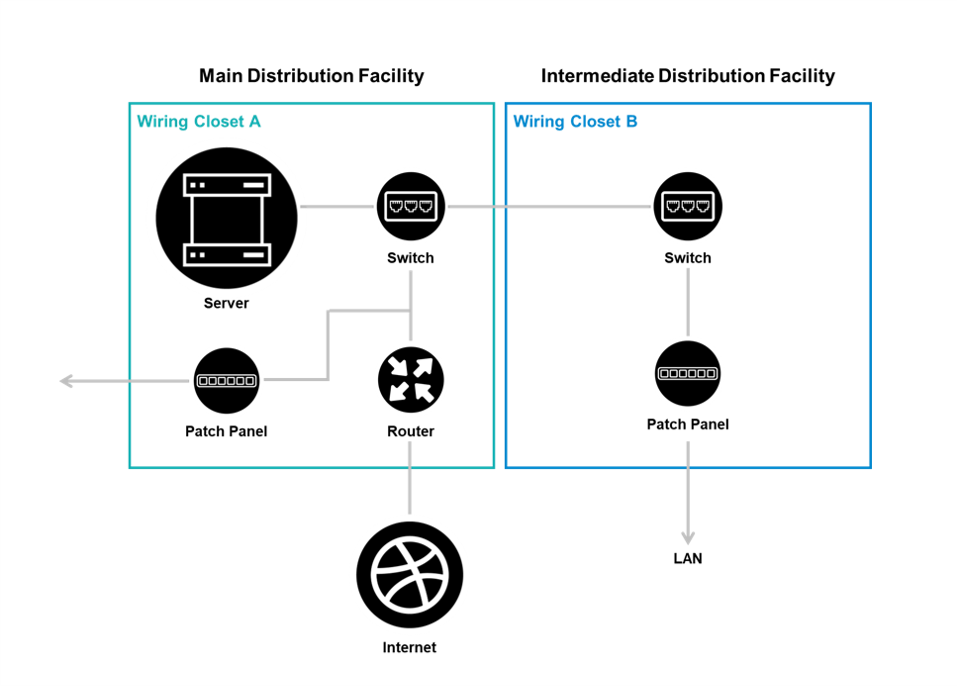
Routers in an IDF are less common but may be used in certain setups to manage data flow between different networks or to provide specialized services.

#### **Functions of Routers**

1. **Inter-network Communication**:
   1. Connects different networks, such as connecting a building's internal network to the internet.
2. **Traffic Management**:
   1. Routes data packets between networks based on IP addressing.
3. **Security Features**:
   1. Often include firewalls, virtual private network (VPN) support, and access control lists (ACLs) for enhanced security.
4. **Dynamic Routing**:
   1. Uses protocols like OSPF to determine optimal paths for data to travel between networks.

#### **When Routers Are Used in IDFs**

* Typically found in larger networks where the IDF needs to serve as a localized gateway for specific zones.
* Useful for separating different network segments or managing traffic between VLANs and the external network.



**Implementation off an IDF in Our Network**

**Level 1**

The following rooms will have an IDF:

IDF\_1A - Room W1118

IDF\_1B - Room W1102

IDF\_1C - Room E1401

**Level 2**

The following rooms will have an IDF:

IDF\_2A – Room E2403

IDF\_2B – Room E2287

IDF\_2C – Room W2205

IDF\_2D – Room W2260

**Level 3**

The following rooms will have an IDF:

IDF-3A - W3708

IDF\_3B – E3339

IDF\_3C - E3352

**CoLab Building**

As the CoLab building is rather small in size compared to the rest of the main building we will be only integrating 1 IDF per floor as that will be sufficient enough for the amount of devices necessary on the premise. The following rooms will have an IDF:

**Level 1**

IDF\_CL1 CL119/120

**Level 2**

IDF\_CL2 CL212/213

**Level 3**

We didn’t put an IDF on this floor as from the maps we have there is only a single room on this floor and as such it wouldn’t be cost efficient to include it.

**Conclusion of Implementation**

The above rooms have been allotted IDF racks as their dispersions are perfectly placed in order to cover every possible room on each floor with keeping in mind the max length of our CAT6 cabling. No room is a far stretch for any of the above mentioned IDFs encapsulating the need for fast and reliable connection between devices. The IDFs have also been placed in mind with the MDFs location to further encapsulate the needs of the network which is located in Room 2283/84, the placement of this MDF is crucial as it is on the second story in a room with exterior access and finally a central location which in tandem helps lay out our IDFs.

# Wireless

A diagram of a computer network

Description automatically generated

Our campus network implements a wireless design integrated with a wired backbone. The network uses Radio Frequency connections between nodes, supported by 240 strategically placed Access Points across the campus. This setup provides a complete wireless coverage, eliminating the “dead spots” and ensuring seamless connectivity.

**WiFi 6 and 6GHz Band Integration**

In order to ensure a high-speed and future-ready connectivity, we have adopted Wi-Fi 6 on campus. Wi-Fi 6 offers:

* Higher data transfer speeds, increased network capacity, and reduced latency.
* It supports 6GHz band. This frequency band provides more channels and reduces interference, making it ideal for high-performance areas.

Our implementation uses Aruba Access Points 635, which features tri-band support. This feature ensures that coverage is robust and provides exceptional performance in more high-traffic areas such as the library and computer labs.

# Access points

A white object with a barcode on it

Description automatically generated

An Access Point is a device that acts as a central transmitter and receiver for wireless signals, enabling seamless connectivity.

We selected Aruba Access Points due to their superior features:

1. Wide Coverage: The industrial grade Access Points effectively cover larger areas.
2. High Capacity: They can support hundreds of wireless clients at the one time, making them ideal for a high-density environment such as the college campus.

Access Points will be strategically placed on ceilings or high walls to maximize signal reach and minimize interference. The placement plan ensures optimal performance based on a specific area’s needs:

* Library: High-density Access Points with overlapping coverage for uninterrupted service.
* Classrooms/multi-use rooms: Standard Access for consistent connectivity.
* Computer Labs: A single Access Point per lab to provide reliable and dedicated connections.
* Common Areas: Access Points will be deployed to ensure connectivity in social spaces, enabling collaborative work and online communication.
* Offices: Dedicated Access Points will support staff devices, providing a secure and robust connection for daily operations.
* Outdoor Areas: Outdoor-grade Access Points will cover open spaces, enabling wireless access even outside of the buildings.
* Lecture Halls: High-density Access Points will support Wi-Fi access for large groups during workshops, seminars or lectures.

This layout ensures seamless roaming and consistent wireless performance, even in areas with heavy usage or simultaneous connections. The strategic placement design aims to minimize dead zones around the campus and provide an optimal experience for everyone on the network.

# WEP or WPA

We employed strong security protocols on the wireless network to ensure a balance between compatibility and modern security standards. These include:

1. **WEP (Wired Equivalent Privacy)**

A computer screen with a green line

Description automatically generated with medium confidence

WEP encrypts data in order to protect Wi-Fi transmission so that outsiders who are not part of the network won't be able to read the messages or data within. The process uses static encryption keys to provide confidentiality for the data and offers a level of security similar to that of a wired network.

**Advantages of WEP:**

* Compatible with older devices that may not support the newer types of protocols found in most modern networks.
* Easy to set up and configure on legacy equipment.

**Disadvantages**

* As WEP uses static keys the encryption tends to be weak. This means that modern tools can easily crack the encryption and gain access to the network.
* WEP is outdated and is no longer considered secure by modern standards.

1. **WPA (Wi-Fi Protected Access)**

A diagram of a internet security system

Description automatically generated

WPA was developed as a more advanced and secure protocol than that of WEP. It uses dynamic encryption keys with stronger authentication mechanisms to enhance security. There are multiple versions of WPA:

* WPA (original): An improvement over WEP, using Temporal Key Integrity Protocol.
* WPA2: Introduced Advanced Encryption Standard, providing stronger encryption and security.
* WPA3: The newest version offers advanced protection, such as improved encryption for public networks and defence against brute-force attacks.

**Advantages**

* Strong encryption with dynamic key management.
* WPA2 and WPA3 are widely supported by modern devices.
* Additional features such as the segmentation of the network and guest access with WPA3 are provided.

**Disadvantages**

* Limited compatibility with older devices.
* Higher overhead compared to WEP due to the stronger encryption.

**Which is better?**

WPA is the better option for securing the campus networks. This is due to:

* Security: WPA offers better and more stronger encryption and is more resistant to vulnerabilities that plague WEP. WPA3 is the most secure option because it ensures robust data protection on both public and private networks.
* Compatibility: Most modern devices support WPA protocols while WEP is necessary for only legacy devices.
* Performance: WPA2/3 provides strong security while also not noticeably impacting network performance.

Adopting WPA2/3 for our campus network will ensure a high level of security and support a wide range of modern devices.

**Future-Ready Design**

Using both Wi-Fi 6 and 6GHz band, the campus network will support modern technologies and offer scalability for future demands. This will ensure faster speeds, reduced congestion and reliable connectivity if the campus were to expand in the near future.

# Voice Over & Teams

**Voiceover IP**

A diagram of a cloud network

Description automatically generated

Voice over IP (VoIP) operates similarly to traditional phone calls but utilizes an internet connection instead of standard telephone cabling. The process involves converting a user's voice from audio signals into digital data, which is then transmitted over the internet. If the call is made to a regular phone number, the digital signal is converted back into a traditional telephone signal before reaching the recipient.

Additionally, VoIP can route both incoming and outgoing calls through existing telephone networks, ensuring compatibility with standard telecommunication systems.

One of the key advantages of VoIP is its flexibility. Users can make calls from anywhere as long as they have a stable internet connection and a compatible device. This mobility makes it an ideal solution for remote work, enabling individuals to stay connected whether they are at home or in other locations.

While it is very useful, we will not be using VoIP within the college.

**Microsoft teams**

A diagram of a company's team

Description automatically generated

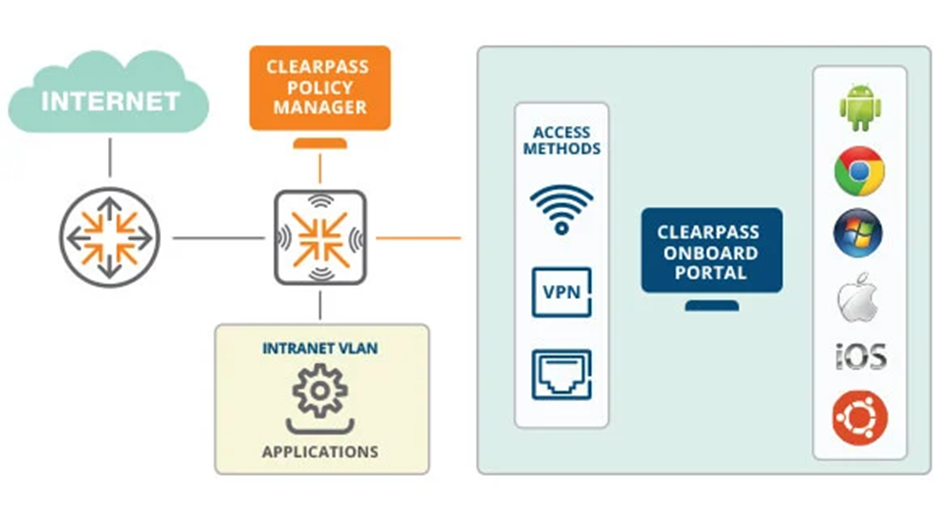
Microsoft Teams is a cloud-based collaboration platform widely used for communication and teamwork. On our campus, where Microsoft products are already extensively utilized, adopting Teams was a logical choice over traditional Voice over IP (VoIP) systems.

With Teams, we can enable two-way persistent chat with one or multiple participants, fostering continuous and seamless communication. Groups can be created to support various departments or student organizations, facilitating focused discussions and collaboration. Additionally, meetings can be easily scheduled, providing a centralized platform for virtual gatherings and coordination.

Another significant feature of Teams is its ability to integrate with the Public Switched Telephone Network (PSTN). This allows Teams to function as a fully capable telephone system, enabling users to make and receive calls as if using a traditional phone line. This flexibility and functionality make Teams an efficient and comprehensive solution for our campus communication needs.

Since most of the campus servers have already been migrated to the cloud, adopting a cloud-based communication system like Microsoft Teams was a practical and strategic choice. By implementing Teams, we align our communication tools with the campus's existing cloud infrastructure, ensuring seamless integration, improved accessibility, and enhanced scalability.

# Clear Pass



As our network is configured using Aruba the ClearPass policy management platform to grant access levels and keep the network secure. It allows for the devices in the college to securely connect to the network in compliance with the security policies we have implemented. During its implementation different levels of access was granted to devices based on roles, the device type or what the cybersecurity posture is.

The ClearPass solution works in four different ways:

1. **Identification**

The IT department in the college will use ClearPass identify which devices are being used, how many are connected to the network, where they are connected from and which OS they support.

1. **Enforcement**

With the built-in certificate authority, the IT department can now write security procedures to establish better network security. These policies can now be enforced on any new devices being added to the network with the involvement of the IT department, creating a quicker connection time for said new devices. Once a new device has been connected to the network, the ClearPass solution uses an active and passive profiling method in order to monitor the network, further adding to the security.

1. **Protection**

The IT department will use ClearPass OnGuard in order to decide whether a device can access the college network based on its ‘level of health’. Using this process, critical endpoint health checks are automated while also posture assessments so that all devices on the network meet the same requirements.

1. **Integration**

As ClearPass offers a dynamic implementation using a variety of third-party integrations, we decided it was the best solution for which to create a seamless with our different platforms. Some of the third-party systems we implemented include:

* Firewalls
* SIEM (Security Information and Event Management)
* Enterprise mobility management
* Mobile device management
* ClearPass

This solution provides our IT department with the real-time insight into the different activities occurring on the college network, allow them to address any issues that may arise.

# Vlans

### VLAN Plan Overview A VLAN (Virtual Local Area Network) is a logical group of network devices that appear to be on the same network segment, even if they are physically located on different parts of the network. VLANs are designed to improve network performance, enhance security, and simplify network management by grouping users or devices with similar requirements. They can be used to segment network traffic, reduce broadcast traffic, and apply specific policies or restrictions to different groups within an organization.

### In this section, we will present a VLAN plan showing VLAN IDs and how these VLANs can be structured across different departments.

### **VLAN Plan and VLAN IDs**

### To ensure efficient management of network resources, we can implement VLANs for various departments, floors, and use cases. Below is an example VLAN plan that shows how VLANs can be organized with specific VLAN IDs for different segments of the network.

### **VLAN Plan**

### **VLAN ID**: 10

### **VLAN Name**: Faculty

### **Description**: VLAN for faculty and academic staff. Allows access to resources like email, academic files, and the intranet.

### **Assigned Devices/Groups**: Faculty computers, faculty wireless access points (APs)

### **VLAN ID**: 20

### **VLAN Name**: Students

### **Description**: VLAN for students, segregating their network traffic from faculty and administration. It may have restricted access to certain resources.

### **Assigned Devices/Groups**: Student computers, student wireless APs, student labs

### 

### **VLAN ID**: 30

### **VLAN Name**: Administration

### **Description**: VLAN for administrative staff, for access to student records, university management software, etc.

### **Assigned Devices/Groups**: Admin computers, HR and Finance departments

### 

### **VLAN ID**: 40

### **VLAN Name**: Library

### **Description**: VLAN for library services, such as library management systems, online databases, and user access.

### **Assigned Devices/Groups**: Library workstations, library wireless APs, printers

### 

### **VLAN ID**: 50

### **VLAN Name**: Research

### **Description**: VLAN for research departments and labs, providing high-speed access to research resources and dedicated servers.

### **Assigned Devices/Groups**: Research labs, high-performance computing clusters

### 

### **VLAN ID**: 60

### **VLAN Name**: Security Cameras

### **Description**: VLAN for security cameras and other surveillance equipment.

### **Assigned Devices/Groups**: Security cameras, video surveillance servers

### 

### **VLAN ID**: 70

### **VLAN Name** V: Wireless

### **Description**: VLAN for wireless infrastructure, which can be split between student, faculty, and staff networks.

### **Assigned Devices/Groups**: Wireless controllers, wireless APs for students, faculty, and staff

### 

### **VLAN ID**: 80

### **VLAN Name**: Servers

### **Description**: VLAN for university-wide servers such as DNS, DHCP, and other critical infrastructure servers.

### **Assigned Devices/Groups**: File servers, DNS/DHCP servers, authentication servers

### 

### **VLAN ID**: 90

### **VLAN Name**: Data Center

### **Description**: VLAN for the data centre infrastructure, with high availability and redundancy for critical applications.

### **Assigned Devices/Groups**: Data centre racks, storage devices, backup systems

### 

### **VLAN ID**: 100

### **VLAN Name**: IT Management

### **Description**: VLAN for IT department, used for managing network infrastructure, monitoring, and maintaining systems.

### **Assigned Devices/Groups**: Network switches, routers, monitoring tools, IT staff devices

### 

### **VLAN ID**: 110

### **VLAN Name**: Academic Labs

### **Description**: VLAN for academic labs, where specialized software and equipment are used by students and faculty.

### **Assigned Devices/Groups**: Computer labs, specialized lab equipment

### 

### **Key Thoughts:**

### **Security**: VLANs should be segmented to minimize the risk of cross-network access, especially between student and administrative VLANs.

### **Performance**: Some high-bandwidth areas like research labs, the data centre, and VoIP should have dedicated VLANs to avoid congestion.

### **Guest Access**: Ensure that the Guest VLAN is properly secured, providing internet access without allowing access to internal university resources.

### **Quality of Service (QoS)**: For critical services like VoIP (VLAN 70), it's important to configure QoS to prioritize voice traffic over regular data traffic.

### 

### **Benefits of VLANs and ClearPass Integration**

### **Enhanced Security**: VLANs provide logical isolation between departments. With ClearPass, network access is further controlled through policies that ensure only authorized users can access specific VLANs, reducing the risk of unauthorized access to sensitive data.

### **Improved Network Performance**: By segmenting traffic into different VLANs, network administrators can reduce congestion in the network and ensure that critical traffic, like IT or sales data, gets the necessary bandwidth and priority.

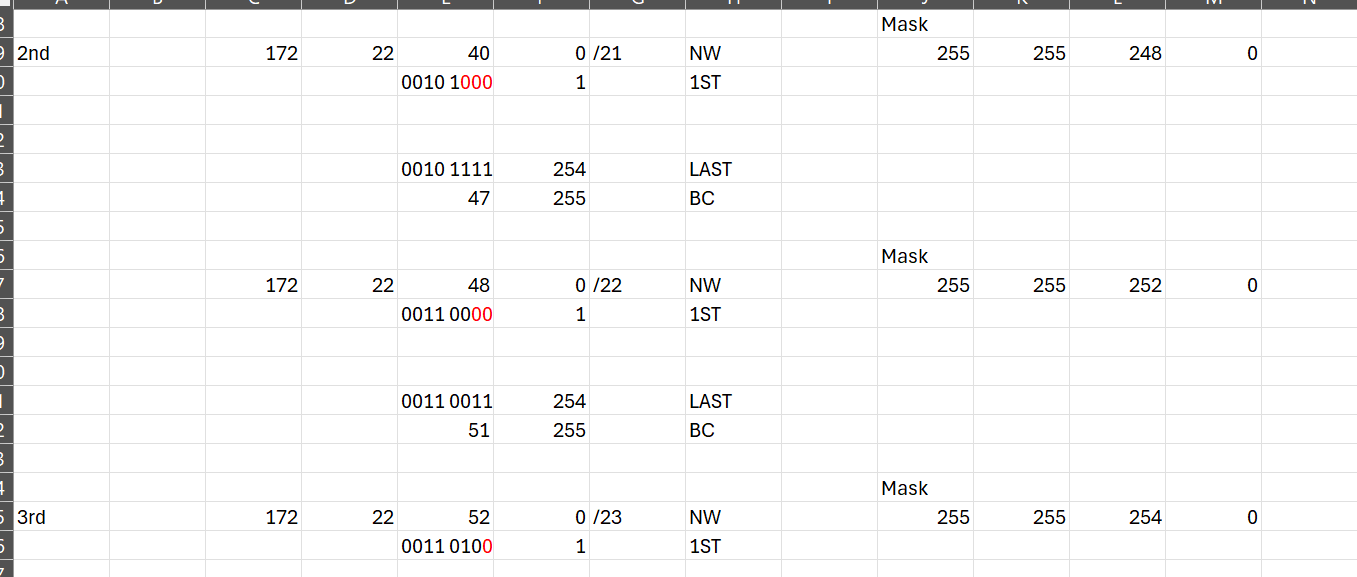
### **Simplified Management**: VLANs, combined with ClearPass, simplify network management. Administrators can easily configure policies for each department, apply access control rules, and automate VLAN assignments based on user roles or device types.

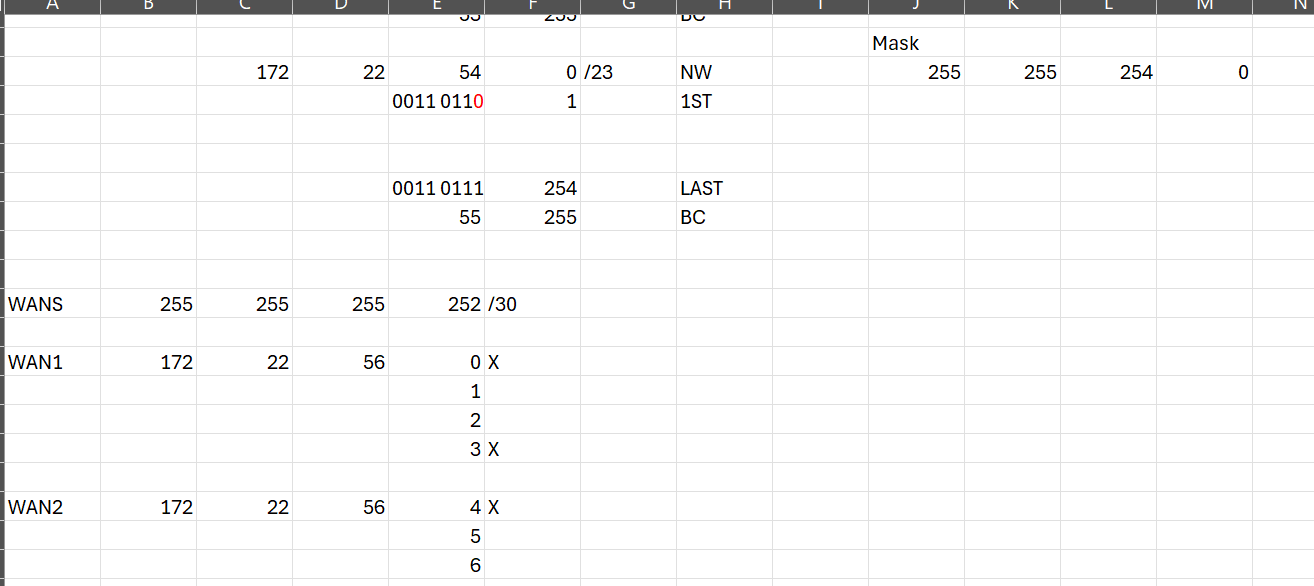
### **Scalability**: VLANs allow the network to scale without needing to add additional physical network infrastructure. As the organization grows, new VLANs can be created to accommodate additional departments, teams, or locations.

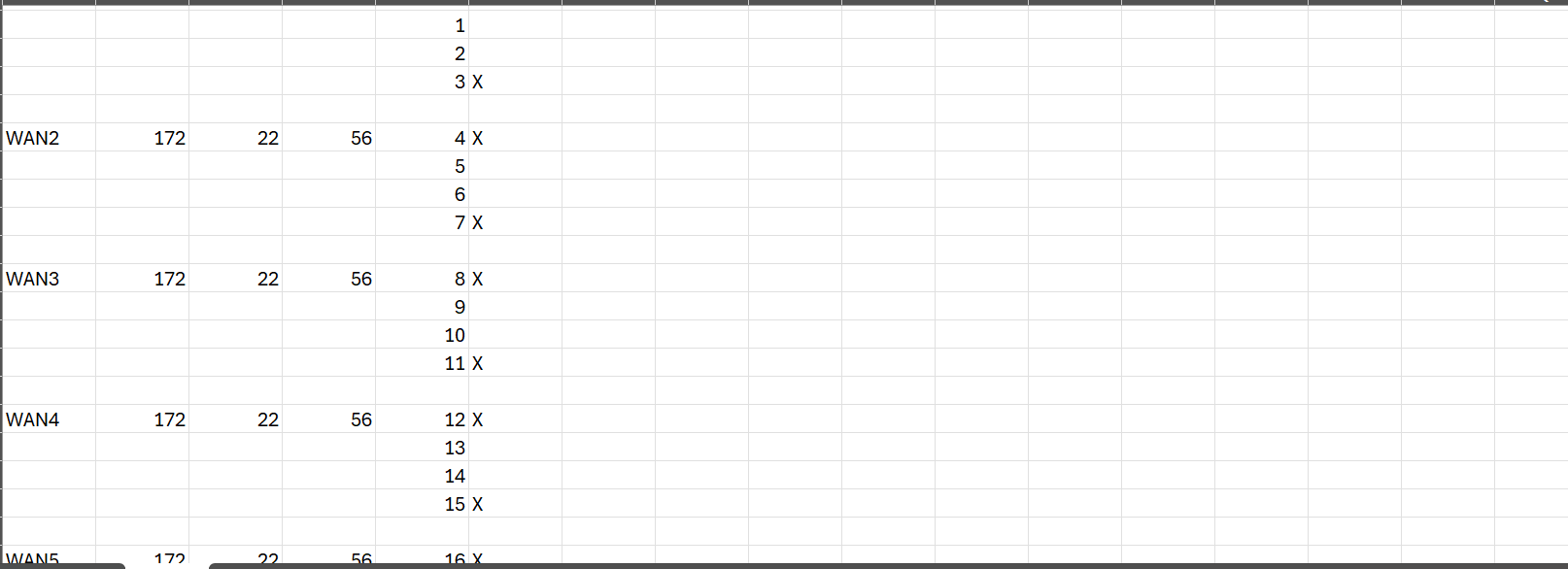
### A VLAN plan is an essential part of modern network design, enabling efficient traffic management, improved security, and flexibility in how network resources are accessed. The integration of ClearPass allows for dynamic and secure VLAN management, ensuring that users are assigned to the appropriate VLAN based on their identity, role, and device compliance. By using VLANs and ClearPass, organizations can segment their network traffic effectively, provide secure access to resources, and ensure that their network is both scalable and manageable.

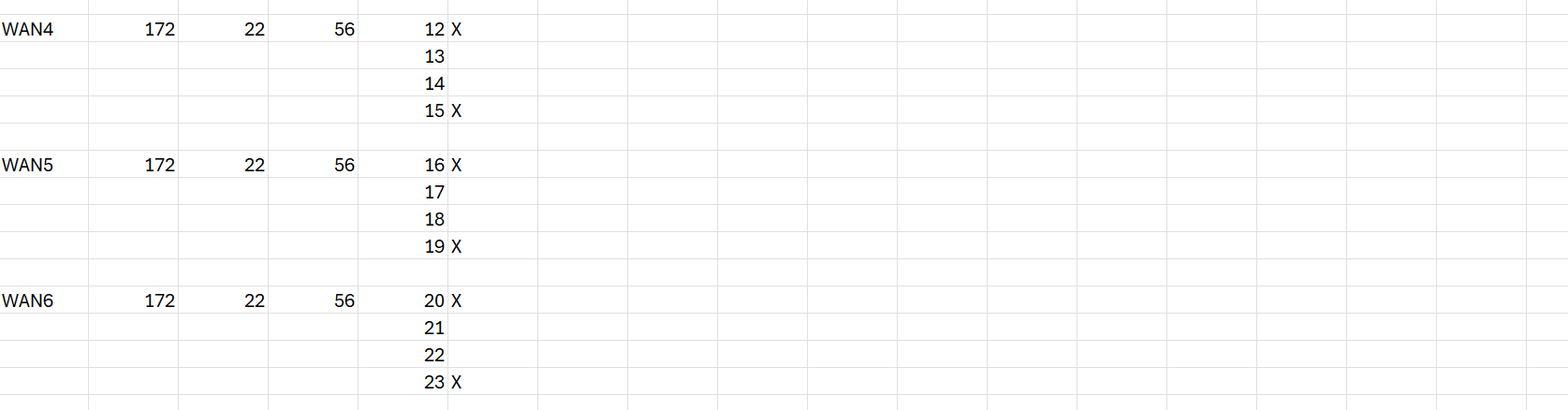
# Subnets











In modern networking, the efficient division of a large network into smaller subnets is essential for optimizing performance, improving security, and facilitating management. The subnetting of a given IP address allows organizations to separate network traffic and allocate resources based on specific needs. In this essay, we will discuss the subnetting of the **172.22.0.0/16** network, which has been broken down into several subnets to accommodate different floors and Wide Area Network (WAN) links. We will also explore the router specifications, address usage, and provide a full IP address layout along with detailed subnet specifications.

The provided network is **172.22.0.0/16**, which represents a large network capable of supporting a wide range of IP addresses. To optimize this network for various needs, the IP address space has been subnetted into several smaller subnets. Here's a breakdown of how many subnets is used:

1. **1st Floor Subnets**:
   1. **172.22.0.0/19** – This subnet accommodates a large range of devices, with a subnet mask of 255.255.224.0. It provides a total of 8192 IP addresses, from **172.22.0.0** to **172.22.31.255**.
   2. **172.22.32.0/21** – This subnet has a mask of 255.255.248.0 and provides 2048 addresses, ranging from **172.22.32.0** to **172.22.39.255**.
2. **2nd Floor Subnets**:
   1. **172.22.40.0/21** – Another **/21** subnet, with a subnet mask of 255.255.248.0, ranging from **172.22.40.0** to **172.22.47.255**.
   2. **172.22.48.0/22** – This subnet has a subnet mask of 255.255.252.0 and includes IP addresses from **172.22.48.0** to **172.22.51.255**.
3. **3rd Floor Subnets**:
   1. **172.22.52.0/23** – A **/23** subnet, with a subnet mask of 255.255.254.0, accommodating addresses from **172.22.52.0** to **172.22.53.255**.
   2. **172.22.54.0/23** – Another **/23** subnet, with the same mask of 255.255.254.0, ranging from **172.22.54.0** to **172.22.55.255**.
4. **WAN Subnets**:
   1. **172.22.56.0/30** – These subnets are used for point-to-point links. Each subnet, with a **/30** mask (255.255.255.252), supports exactly 4 IP addresses. There are six such WAN subnets, ranging from **172.22.56.0** to **172.22.56.23**.

#### **IP Address Usage**

The IP addresses in the network have been used strategically to ensure there is enough room for all the devices across various floors and WAN connections. Below is an overview of how the addresses are distributed:

1. **Floor 1 Subnets:**
   1. The first subnet, **172.22.0.0/19**, spans from **172.22.0.0** to **172.22.31.255**.
   2. The second subnet, **172.22.32.0/21**, spans from **172.22.32.0** to **172.22.39.255**.
2. **Floor 2 Subnets:**
   1. The first subnet, **172.22.40.0/21**, spans from **172.22.40.0** to **172.22.47.255**.
   2. The second subnet, **172.22.48.0/22**, spans from **172.22.48.0** to **172.22.51.255**.
3. **Floor 3 Subnets:**
   1. The first subnet, **172.22.52.0/23**, spans from **172.22.52.0** to **172.22.53.255**.
   2. The second subnet, **172.22.54.0/23**, spans from **172.22.54.0** to **172.22.55.255**.
4. **WAN Subnets:**
   1. The six **/30** subnets are used for point-to-point links. These subnets range from **172.22.56.0** to **172.22.56.23**. Each of these subnets is used for a specific WAN connection, and each can support two usable IP addresses, which are ideal for router-to-router communication.

The address distribution ensures that there are enough IP addresses for all devices on each floor while also leaving sufficient room for future growth.

#### **Router Specifications**

The router configuration plays a critical role in ensuring that data is properly routed across the subnets. For a network of this size, the router must be able to handle multiple subnets and provide sufficient routing capabilities.

* **Router Interface**: The router needs to have interfaces configured for each subnet. Each subnet (e.g., **172.22.0.0/19**, **172.22.32.0/21**) must have its own subnet address on the router for proper communication within the network and to external networks.
* **Routing Protocol**: A dynamic routing protocol like **RIP**, **OSPF**, or **EIGRP** should be used to facilitate communication between the subnets. This allows the router to dynamically learn about other subnets and adjust routes when network changes occur.
* **Router IP Addressing**: Each router interface will have an IP address assigned from the appropriate subnet range. For example, the router interface for the **172.22.0.0/19** subnet will use an IP like **172.22.0.1**, while the interface for the **172.22.56.0/30** subnet (WAN1) will use **172.22.56.1**.

#### **Full IP Address Layout and Subnet Specifications**

Here’s a detailed layout of the full IP address allocation for the subnets:

1. **Main Network (172.22.0.0/16)**:
   1. Subnet Mask: **255.255.0.0**
   2. Range: **172.22.0.0 - 172.22.255.255**
2. **1st Floor:**
   1. **172.22.0.0/19**:
      1. Range: **172.22.0.0 - 172.22.31.255**
      2. First IP: **172.22.0.1**
      3. Last IP: **172.22.31.254**
      4. Broadcast: **172.22.31.255**
   2. **172.22.32.0/21**:
      1. Range: **172.22.32.0 - 172.22.39.255**
      2. First IP: **172.22.32.1**
      3. Last IP: **172.22.39.254**
      4. Broadcast: **172.22.39.255**
3. **2nd Floor:**
   1. **172.22.40.0/21**:
      1. Range: **172.22.40.0 - 172.22.47.255**
      2. First IP: **172.22.40.1**
      3. Last IP: **172.22.47.254**
      4. Broadcast: **172.22.47.255**
   2. **172.22.48.0/22**:
      1. Range: **172.22.48.0 - 172.22.51.255**
      2. First IP: **172.22.48.1**
      3. Last IP: **172.22.51.254**
      4. Broadcast: **172.22.51.255**
4. **3rd Floor:**
   1. **172.22.52.0/23**:
      1. Range: **172.22.52.0 - 172.22.53.255**
      2. First IP: **172.22.52.1**
      3. Last IP: **172.22.53.254**
      4. Broadcast: **172.22.53.255**
   2. **172.22.54.0/23**:
      1. Range: **172.22.54.0 - 172.22.55.255**
      2. First IP: **172.22.54.1**
      3. Last IP: **172.22.55.254**
      4. Broadcast: **172.22.55.255**
5. **WAN Subnets (each /30)**:
   1. **172.22.56.0/30**:
      1. Range: **172.22.56.0 - 172.22.56.3**
      2. First IP: **172.22.56.1**
      3. Last IP: **172.22.56.2**
      4. Broadcast: **172.22.56.3**
   2. And similarly for other WAN subnets (WAN2, WAN3, etc.).

The subnetting of the **172.22.0.0/16** network allows for efficient management of resources, separating different floors and WAN connections into dedicated subnets. This provides flexibility, scalability, and optimal performance across the network. The router specifications, including the configuration of interfaces for each subnet and the use of dynamic routing protocols, ensure seamless communication between devices across different segments of the network. The detailed IP address layout provides a clear view of how the IP address space is allocated, facilitating proper network operation and management.

# Security

Servers are a core component at ATU Donegal, supporting academic and administrative functions. The university deploys multiple layers of security to safeguard these assets against unauthorized access, data breaches, and service disruptions.

**Server Hardening:**

Server hardening ensures systems are hardened against potential threats, including:

* Minimal Installation: Only necessary software and services are installed.
* Access Controls:
* Default accounts are disabled or subjected to strong passwords.
* Access is allowed remotely only to those with authorized IPs and users.
* Patch Management: Operating systems and applications are routinely updated according to their respective patch cycles.

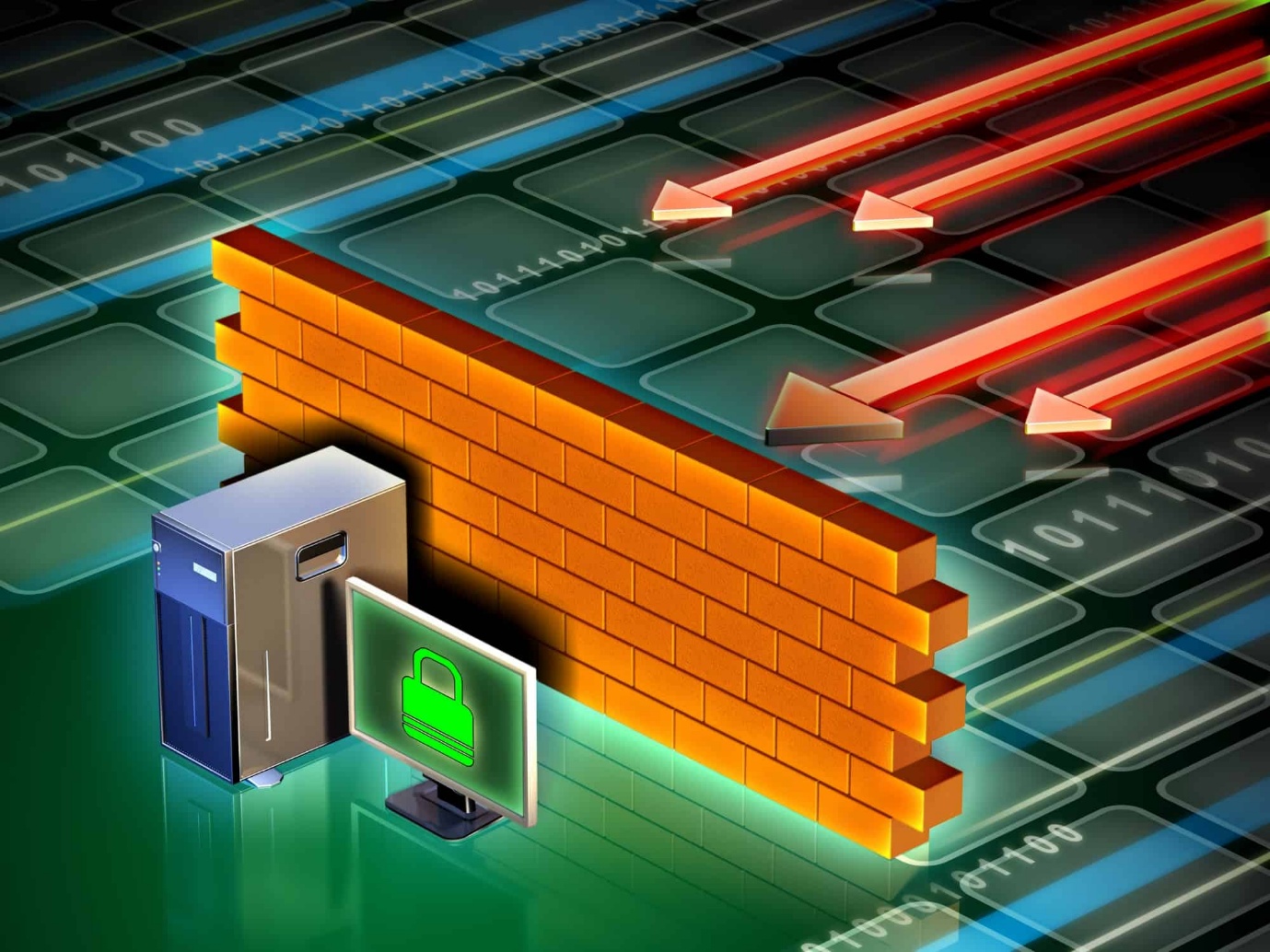
**Authentication and Access Control**

* Multi-Factor Authentication (MFA): Mandatory for administrative access, combining passwords, tokens, and biometrics.
* Role-Based Access Control: Attaches access based on the role performed, restricting sensitive data only to the one who needs it.
* Logging and Monitoring: Logs all access attempts and generates alerts for suspicious activity.

**Firewall Integration**

Servers are protected by:

* Host-Based Firewalls: Control traffic to essential ports and protocols.
* Network Segmentation: Groups servers by function, with strict inter-segment traffic rules.



**Data Protection**

* Encryption:
* At Rest: Server-stored data is encrypted using AES-256.
* In Transit: The transportation of data is fully protected by secure protocols such as HTTPS and SSH.

* Backups:
* Regular backups are encrypted in diverse geographical locations.
* Data integrity of backups is ensured via routine testing.

* Access Policies: Controls around sensitive data should be strict and follow the governance as laid out in GDPR.

**Application Security**

* Regular code reviews are conducted to ensure that hosted applications are secure, along with periodic vulnerability assessments.
* Injection attacks are prevented by proper input validation.
* Third-party software is updated in due time to avoid risks.

**Virtualization and Cloud Security**

* Virtual Machines: VMs operate in isolation, making compromise containment easier and enabling fast recovery via snapshots.
* Cloud Servers:
* Enforce IAM policies.
* Encrypt data at rest and restrict access to vetted providers.
* Incident Response and Recovery

ATU Donegal is well-equipped with plans in case any incident occurs:

* Incident Management: It includes detection, containment, eradication, and recovery.
* Disaster Recovery: Systems set up to be redundant, automatic failover in case of outages for minimal disruption.

**Physical Security**

Servers located on-premises servers' benefit from:

* Biometric and keycard controls on access
* 24/7 surveillance and environmental monitoring
* Redundant power supply and cooling systems

# Servers

At ATU Donegal, servers are an integral part of the academic, research, and administrative services within the institution. These servers house important services that students, staff, and faculty use for resource access, collaboration tools, and network infrastructure.

**1. Types of Servers at ATU Donegal**

The servers at ATU Donegal are varied to cater to different needs within the institution: 

* **File Servers:**

These servers store and manage access to files, including course materials, student records, research data, and administrative documents. File servers provide centralized storage with easy access across the campus network.

* **Web Servers:**

ATU Donegal makes use of web servers to host the university's websites, including internal and external resources. These servers make available information on courses, services, campus events, and academic departments.

* **Email Servers:**

Email servers cater to the emails of an institution. The servers ensure that this communication is delivered securely and reliably to students, faculty members, and staff within the institution. They are integrated with webmail systems for easy access from anywhere.

* **Database Servers:**

The database servers of the university persist the critical information required regarding student records, financial data, and academic records of the students. These servers efficiently create a structured way to query large sums of data required at any given time for university operations.

* **Application Servers:**

Application servers house independent software applications used academically and administratively. Applications using these servers may also contain learning management systems or course registration and research resources online.

* **Virtualization Servers:**

Virtualization technology is being implemented in ATU Donegal for running more than one virtual server on a single physical machine to optimize resource utilization and reduce hardware costs, thereby providing flexibility in managing computing resources.

* **Backup Servers**

These are special servers for storing copies of important data. This ensures that all your important files and databases are recovered just in case of data loss or when the system crashes. These servers create backups periodically through automated systems.

**2. Server Infrastructure**

The server infrastructure in ATU Donegal has been designed to be reliable, scalable, and high performance:

* **Data Center:**

Out-of-the-box, servers are normally installed in a dedicated on-campus data center. Such a facility is provided with appropriate power supplies, cooling systems, and physical security arrangements so as to maintain uptimes and protect the servers from natural eventualities.

* **Network Connectivity:**

All these servers are connected through the university's internal network, which grants all systems fast and secure connections among one another. By using redundant paths for networking, along with high-capacity switches, the servers continue communicating and operating without interruption from hardware failures.

* **Scalability:**

In all, the server environment of the ATU Donegal site is scaled based on their ever-growing needs. Depending on demands, it may be due to adding more storage capacity to putting fresh Virtual servers.

* **Redundancy and High Availability:**

To minimize service interruptions, the ATU Donegal server setup uses redundancy mechanisms that include backup power supplies for power failure, RAID configurations for redundancy in storage, and failover systems for continuity in case of hardware failure.

**3. Server Management**

Good management of servers ensures a smooth and efficient running system for the university's IT infrastructure as follows.

* **Monitoring and Maintenance:**

Performance, health, and uptime are monitored continuously. It monitors CPU usage, disk space, and network traffic, among other key metrics. Software updates, hardware diagnosis, and system optimization are done periodically to maintain the efficiency of servers.

* **Configuration Management:**

Configuration management tools are applied in the standardization of server settings and ensuring consistency in application of changes across the environment. This helps minimize errors and maintains stability in the servers.

* **Resource Utilization:**

Administrators make use of resource management utilities for proper computing resource apportioning so that the servers do not get too overwhelmed, ensuring optimum performance. In this, resources might be virtualized in various virtual machines.

**4. Server Software and Services**

The servers operating at ATU Donegal serve a range of academic and administrative activities, from OSes to different applications, some of which include:

* **Operating Systems:**

These usually run enterprise-level operating systems, such as Linux for open-source services, or Windows Server for application hosting and integration. Such an operating system provides the environment for hosting university services and ensures compatibility with various applications.

* **Database Management Systems:**

Database servers use DBMS software such as MySQL, PostgreSQL, or Microsoft SQL Server to manage and query large datasets. Such systems are optimized for handling huge volumes of student data, research information, and administrative records.

* **Collaboration Tools:**

Servers also host collaboration tools such as email, file sharing, and calendaring software. These platforms support communication and project management among faculty, staff, and students.

* **Learning Management Systems (LMS):**

Application servers host the university's LMS platforms, such as Moodle and Blackboard. These systems enable students and staff to share course materials, submit assignments, and view grades.

**5. Backup and Disaster Recovery**

ATU Donegal has dedicated backup servers that mirror critical data from other servers to ensure data integrity within the university. It does regular backups of server configurations, applications, and data so that in case failure occurs, the university would be able to recover and restore services faster.

* **Offsite Backup:**

In addition to on-site backups, offsite backup solutions are used for added security, ensuring that data is protected even in the case of a catastrophic failure at the primary data centre.

* **Disaster Recovery Plans:**

The ATU Donegal has included plans for disaster recovery in the case of server restoration processes. These plans ensure that in the case of system failure, servers can be restored within a specified time frame to minimize disruptions in the operations of the university.

# Conclusion

Throughout this project, we carefully and thoroughly planned the LAN design for Letterkenny ATU, covering all major aspects of the network infrastructure such as cabling, MDF and IDF setup, wireless access, VLANs, subnets, and security protocols. This process highlighted how important an organized and well-thought out network design is for performance, scalability, and cost-effectiveness of a LAN design.

We chose high-quality copper and fiber optic cables to ensure the network is reliable and long-lasting. The MDF serves as the central hub, while the IDFs distribute connectivity across the campus, ensuring smooth, effective communication. Wireless access is supported by Aruba Access Points, delivering strong and uninterrupted connections throughout the campus.

Security was a top priority in our design. We incorporated WPA2/3 wireless protocols, VLAN segmentation, and Aruba ClearPass for advanced access control, creating a network that is both high-performing and secure against potential threats. We also made scalability a focus by including Wi-Fi 6 and hardware redundancy, ensuring the network can adapt to future growth or technological changes.

Teamwork was vital to the success of this project. Each member brought unique skills and perspectives, and by collaborating effectively, we created a cohesive and well-rounded design. The result is a network infrastructure that meets the needs of students, faculty, and staff at Letterkenny ATU, providing fast, reliable, and secure connectivity for all involved.

# Appendices

*Best Types of Network Security That Protect Data in 2024* (no date). Available at: <https://nordlayer.com/learn/network-security/types/> (Accessed: 9 December 2024).

Calderon, J. (2024) *Main Distribution Frame (MDF Room): A Comprehensive Guide*, *Nfina*. Available at: <https://nfina.com/mdf-room/> (Accessed: 9 December 2024).

*Intermediate Distribution Frames: Quick Guide to IDFs | iFeeltech* (no date). Available at: <https://ifeeltech.com/intermediate-distribution-frames-guide/#toggle-id-5> (Accessed: 9 December 2024).

*MDF vs. IDF Explained: Differences and Roles in Network Design* (no date). Available at: <https://www.cablesandkits.com/learning-center/faq-mdf-vs-idf> (Accessed: 9 December 2024).

Tablan, P. (no date) *What is Aruba ClearPass? How Does it Protect Your Network?* Available at: <https://www.kelsercorp.com/blog/what-is-aruba-clearpass-and-how-does-it-protect-your-network> (Accessed: 3 December 2024).

*What Are the Advantages of VoIP? | Vonage* (no date). Available at: <https://www.vonage.com/resources/articles/what-are-advantages-of-voip/> (Accessed: 9 December 2024).

*What Is a Main Distribution Frame (MDF) Room? | Pure Storage* (no date). Available at: <https://www.purestorage.com/knowledge/what-is-main-distribution-frame-room.html> (Accessed: 9 December 2024).

*What is a subnet (subnetwork)? | Definition from TechTarget* (no date). Available at: <https://www.techtarget.com/searchnetworking/definition/subnet> (Accessed: 9 December 2024).

*What Is an Access Point in Networking? | Juniper Networks US* (no date). Available at: <https://www.juniper.net/us/en/research-topics/what-is-an-access-point-in-networking.html> (Accessed: 9 December 2024).

*What is an intermediate distribution frame (IDF)?* (no date). Available at: <https://www.techtarget.com/whatis/definition/intermediate-distribution-frame-IDF> (Accessed: 9 December 2024).

*What is Aruba Clearpass and Why You Should Care?* (no date). Available at: <https://info.hummingbirdnetworks.com/blog/what-is-aruba-clearpass-and-why-you-should-care> (Accessed: 9 December 2024).

*What Is Network Security? Definition and Types | Fortinet* (no date). Available at: <https://www.fortinet.com/resources/cyberglossary/what-is-network-security> (Accessed: 9 December 2024).

*What is Wi-Fi Protected Access (WPA)? - Definition from WhatIs.com* (no date) *Mobile Computing*. Available at: <https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access> (Accessed: 9 December 2024).

*What Should You Include in Your IDF Technology Plan? | Donwil* (no date). Available at: <https://www.donwil.com/what-should-you-include-in-your-idf-technology-plan/> (Accessed: 9 December 2024).

Williams, R. (2021) *Microsoft Teams development: All you need to know*, *Microsoft 365 Developer Blog*. Available at: <https://devblogs.microsoft.com/microsoft365dev/microsoft-teams-development-all-you-need-to-know/> (Accessed: 9 December 2024).

*Wired Equivalent Privacy (WEP): Definition & Risks | Okta UK* (no date). Available at: <https://www.okta.com/uk/identity-101/wep/> (Accessed: 9 December 2024).

*Wireless Networking Overview* (no date). Available at: <https://www.intel.com/content/www/us/en/support/articles/000006856/wireless/legacy-intel-wireless-products.html> (Accessed: 9 December 2024).

*What is Computer Security and Its Types |Archana Choudary* (5/12/24). Available at: <https://www.edureka.co/blog/what-is-computer-security/> (Accessed: 9 December 2024).

*Types of servers: functions and characteristics of 18 server types in computer networks.* Available at: <https://servercore.com/blog/articles/types-of-servers-functions-and-characteristics-of-18-server-types-in-computer-networks/> (Accessed: 9 December 2024).