ATU LAN Design 2023

Ronan Smyth (L00176857), John Paul Cosgrove (L00176459), Javier Diaz Jimenez(L00179582), Mykhailo Shpyl(L00179131).

BSc Computer Science – Advanced IT Infrastructure.

Table of Contents

[Introduction 0](#_Toc153355690)

[Extended Star Topology 0](#_Toc153355691)

[Network Topology 0](#_Toc153355692)

[Extended Star Topology 0](#_Toc153355693)

[Benefits 0](#_Toc153355694)

[Hardware – Switches and Routers 1](#_Toc153355695)

[Edge Switches 1](#_Toc153355696)

[Routers: 2](#_Toc153355697)

[Core switches 4](#_Toc153355698)

[Access Points 6](#_Toc153355699)

[Summary 7](#_Toc153355700)

[Switches: 7](#_Toc153355701)

[Routers: 7](#_Toc153355702)

[Core Switches: 8](#_Toc153355703)

[Access Points: 8](#_Toc153355704)

[Hardware Advantages & Disadvantages 8](#_Toc153355705)

[Switch Series Disadvantages 8](#_Toc153355706)

[Switch Model Advantages 10](#_Toc153355707)

[Router Model Advantages 12](#_Toc153355708)

[IDFs 14](#_Toc153355709)

[Main Building - Level 1 14](#_Toc153355710)

[Main Building - Level 2 14](#_Toc153355711)

[Main Building - Level 3 14](#_Toc153355712)

[Colab - Level 1 15](#_Toc153355713)

[Colab - Level 2 15](#_Toc153355714)

[An Danlann 15](#_Toc153355715)

[Killybegs Satellite Campus 15](#_Toc153355716)

[Cabling 16](#_Toc153355717)

[Distance 16](#_Toc153355718)

[Copper Cabling 16](#_Toc153355719)

[Connectors 16](#_Toc153355720)

[Structured Cabling System 17](#_Toc153355721)

[Horizontal Cabling 17](#_Toc153355722)

[Backbone Cabling 17](#_Toc153355723)

[IDF and MDF Placement 18](#_Toc153355724)

[MDF Placement 18](#_Toc153355725)

[Level 1 18](#_Toc153355726)

[Level 3 18](#_Toc153355727)

[Colab 18](#_Toc153355728)

[An Danlann 19](#_Toc153355729)

[Killybegs 19](#_Toc153355730)

[Maps 20](#_Toc153355731)

[Access Points 25](#_Toc153355732)

[Broadcast & Collision Domains 26](#_Toc153355733)

[VLANS 26](#_Toc153355734)

[Switches 26](#_Toc153355735)

[Internal Servers & Services 27](#_Toc153355736)

[NTP (Network Time Protocol) 27](#_Toc153355737)

[Considerations: 27](#_Toc153355738)

[DNS (Domain Name Server) 27](#_Toc153355739)

[Considerations: 27](#_Toc153355740)

[DHCP (Dynamic Host Configuration Protocol) 27](#_Toc153355741)

[Considerations: 27](#_Toc153355742)

[SSH (Secure Shell) 27](#_Toc153355743)

[Considerations: 28](#_Toc153355744)

[Proxy Server 28](#_Toc153355745)

[Considerations: 28](#_Toc153355746)

[File Servers 28](#_Toc153355747)

[Considerations: 28](#_Toc153355748)

[Application servers 28](#_Toc153355749)

[Considerations: 28](#_Toc153355750)

[Web servers 29](#_Toc153355751)

[Considerations: 29](#_Toc153355752)

[Print servers 29](#_Toc153355753)

[Considerations: 29](#_Toc153355754)

[Where to store services: 29](#_Toc153355755)

[IP addressing 30](#_Toc153355756)

[Security 33](#_Toc153355757)

[Firewalls 33](#_Toc153355758)

[Wi-Fi authentication 33](#_Toc153355759)

[802.1X 33](#_Toc153355760)

[VPN 34](#_Toc153355761)

[NAC 34](#_Toc153355762)

[Antivirus Software 34](#_Toc153355763)

[Zero-trust policies 34](#_Toc153355764)

[Email 34](#_Toc153355765)

[Authentication key storage 34](#_Toc153355766)

[Internal asset access 35](#_Toc153355767)

[Software installation across student devices 35](#_Toc153355768)

[Conclusion 35](#_Toc153355769)

[References: 36](#_Toc153355770)

# Introduction

The aim of this LAN design proposal is to calculate the most efficient, cost-effective and secure layout for the upcoming ATU network overhaul.

An extended star topology will be implemented due to its facility when considering installation, scalability and maintenance. The extended star is also an industry standard and has shown the capability of handling the amounts of traffic expected at ATU for the foreseeable future.

A central Main Distribution Frame (MDF) location will be selected as well as several Intermediate Distribution Frames (IDF) to minimize traffic throughout the building. The cable connections for these will be illustrated on maps of the building.

A full overview of the required cabling will be outlined including the type, specification and quantity.

The switches (high and low end), routers and cabling which will be discussed in this proposal have been chosen to accommodate the requirements of an extended start topology.

A subnetting ideology has been selected to maximize efficiency while ensuring security. The subnetting is somewhat different to what exists in the university at present and may be more costly, though the benefit to cost ratio is believed to justify the additional expense. VLANS corresponding to the subnets will also be implemented.

In terms of servers, though most services like storage are now hosted on the cloud, DNS and DHCP are still hosted locally and will be discussed in this document. Services being hosted on the cloud also effects network traffic flow which will also be addressed.

Security of the network and the information contained therein is paramount, at present more than ever before. A detailed network security plan will be implemented on the LAN to moderate increasing online threats.

It is our hope that the combination of the above technologies and methodologies will result in an efficient network design capable of accommodating current network demands at ATU and also be adequate for future expansion.

# Extended Star Topology



Figure 1- Extended Star Topology(‘Extended Star Topology | Importance and Uses of Extended Star Topology’, 2020)

## Network Topology

A network topology refers to the physical and logical organisation of nodes and connections within a network. Represented as a graph, network topologies detail the structure of networks and the positioning of traffic flows. A well-defined and strategically planned topology facilitates the identification and resolution of faults, resulting in the enhancement of data transfer efficiency for an organisation.(Gillis, 2021)

## Extended Star Topology

The star topology stands out as the most prevalent network configuration employed across various sectors, including offices, residences, and other industries. This topology entails connecting all nodes to a singular hub or switch, which is directly linked to a central hub or switch. The central hub functions as a focal point for communication and facilitates the transmission of messages among connected nodes.(Gillis, 2021)

### Benefits

1. Star topology serves to interconnect computers by channelling them to a central point. This proves particularly effective in scenarios where multiple computers need to be connected over short distances. (Gillis, 2021)
2. Enables the seamless transmission of data and information across the network, any node within the system can send messages to any other node, assuming all nodes are linked to a common central hub or switch. (Gillis, 2021)
3. The reliability of networks is enhanced. By virtue of nodes being connected to a central hub, the probability of network failure is minimized. The independence of nodes, each directly linked to a single central hub or switch, contributes to a more robust network with reduced risk of failure. (Gillis, 2021)
4. Star topologies are scalable, network not distributed with the addition of new devices.(Gillis, 2021)
5. Troubleshooting issues is simplified due to the direct one-to-one connection between each device and the hub. The distinct advantage lies in the ability to pinpoint and isolate a faulty device without impacting other nodes in the network.(Gillis, 2021)

# Hardware – Switches and Routers

## Edge Switches

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Aspect** | **Aruba 5400R zl2 Switch Series** | **HP 1950 Switch Series** | **Cisco Catalyst 9300 Series** |
| Port Configuration | 24, 48, 96 GbE with 1/10/40GbE uplinks | 12, 24 GbE with 10GbE uplinks | 24, 48 GbE with Multigigabit and 10GbE uplinks |
| High-Density Wireless Support | Optimized with Aruba APs, Smart Rate ports | Limited support | Optimized with Cisco APs, Wi-Fi 6 support |
| PoE Capabilities | PoE/PoE+/HPoE (up to 60W/port) | PoE/PoE+ (up to 30W/port) | PoE+/UPOE (up to 60W/port) |
| Network Management | Aruba AirWave, Central, NetEdit, ZTP | Web Managed, CLI, SNMP | Cisco DNA Center |
| Layer Support | Full Layer 3 (OSPF, BGP, VRF) | Layer 2, Layer 3 Lite (Static, RIP) | Full Layer 3 (OSPF, EIGRP, BGP) |
| Stacking Capability | VSF (up to 10 switches) | IRF (up to 9 switches) | StackWise-480 (up to 9 switches) |
| Software Defined Networking (SDN) | Yes, ArubaOS-Switch, OpenFlow, ClearPass | Limited SDN features | Yes, Cisco DNA, full SDN capabilities |
| Security Features | ACLs, RADIUS, TACACS+, 802.1X, MACsec | ACLs, RADIUS, SSL, 802.1X | ACLs, RADIUS, TACACS+, 802.1X, TrustSec, ETA, MACsec |
| Redundancy | Redundant mgmt/power, hot-swappable | No redundant power, fixed fans | Redundant power, modular fans |
| Energy Efficiency | EEE, Intelligent Power Management | EEE, low power consumption | EEE, superior power management |
| Scalability | Enterprise edge to core, highly scalable | Small-sized deployments, limited scalability | Large-scale deployments, highly scalable |
| Interoperability | Excellent with multi-vendor environments | Good with HP and third-party devices | Best with Cisco environments, some third-party compatibility |
| Warranty and Support | Limited Lifetime Warranty, next-business-day replacement | Limited Lifetime Warranty, next-business-day replacement | Limited Lifetime Warranty, 1-year software warranty, optional SMARTnet |
| Price (approximate) | 4,000−10,000 depending on features | 1,000−3,000 depending on features | 5,000−15,000 depending on features |

In the edge switches category, the Aruba 5400R zl2 series offers a balanced mix of features, making it suitable for a university environment. It provides versatile port configurations with high-speed uplinks, accommodating various network sizes. The switch supports high-density wireless with optimization for Aruba access points, ensuring seamless connectivity for a large number of devices.

The Aruba switch excels in PoE capabilities, offering high-power options (up to 60W per port) that are essential for powering devices like access points and security cameras commonly found in university setups. Additionally, its network management tools, including AirWave and Central, provide comprehensive visibility and control over the network, crucial for managing a large number of devices.

The switch's full Layer 3 support with advanced routing protocols is beneficial for complex network topologies, which are often present in educational institutions. Its stacking capability through VSF simplifies management, allowing up to 10 switches to function as a single unit.

While the Cisco Catalyst 9300 Series offers more extensive features, including full Layer 3 capabilities and advanced security features, the Aruba 5400R zl2 series provides a robust and cost-effective solution tailored to the needs of a university environment.

## Routers:

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Model** | **Aruba 7205** | **HP FlexNetwork MSR930** | **Cisco 4451-X** |
| Form Factor | Fixed | Fixed | Modular |
| Throughput | Up to 2 Gbps | Up to 500 Mbps | Up to 2 Gbps |
| Flash Memory | 4 GB | 512 MB | 8 GB |
| RAM | 4 GB | 512 MB | 2 GB (default), up to 16 GB |
| WAN Ports | 2 x 10/100/1000Base-T | 2 x Gigabit Ethernet | 4 x Gigabit Ethernet |
| LAN Ports | 4 x 10/100/1000Base-T | 4 x Gigabit Ethernet | 4 x Gigabit Ethernet |
| Integrated Wi-Fi | Yes | No | No |
| PoE Ports | No | No | Optional |
| Redundancy Features | Yes | Yes | Yes |
| Security Features | Firewall, VPN, AAA, Stateful Firewall, Role-based Access Control | Firewall, VPN, NAT, Stateful Packet Inspection | Firewall, VPN, IPS, AAA, Advanced Malware Protection |
| Management | Aruba AirWave | HP Intelligent Management Center (IMC) | Cisco IOS XE, Cisco DNA Center |
| Scalability | Multi-gigabit port expansion, Virtual Switching Framework (VSF) | Modular hardware, Optional modules for increased functionality | Service modules, High availability configurations |
| Network Access Control (NAC) | ClearPass Policy Manager (optional) | Optional with IMC modules | Cisco ISE (optional) |
| Additional Security Capabilities | Intrusion Detection and Prevention System (IDPS), Encrypted Traffic Analysis | Static URL filtering, Application-level gateway | Next-Generation Encryption, Trustworthy Systems |
| Switch Compatibility | Seamless integration with Aruba switches and network management | Compatible with HP and third-party switches, Comware OS for interoperability | High compatibility with Cisco switches and network ecosystem |
| Support and Warranty | Enhanced support options, Limited lifetime warranty | Standard and extended warranty options, Support services | Cisco SMARTnet Service, Limited lifetime warranty |
| Price Range (Approx.) | 4,000−6,000 | 1,000−1,500 | 10,000−15,000 |

For routers, the Aruba 7205 Series is a mid-range option suitable for a university campus. It offers a fixed form factor with good throughput and integrates well with Aruba's network management tools. The router provides advanced Layer 3 features, making it suitable for campus networks with medium to large enterprise campuses.

The Aruba router stands out in terms of modularity and routing capabilities, offering a balanced set of features for a university environment. Its integrated services, including wireless LAN controller functionality, make it a comprehensive solution for managing both wired and wireless networks.

While the Cisco 4451-X offers higher performance and a broader range of integrated services, the Aruba 7205 Series provides a cost-effective solution that meets the specific needs of a university, especially if the emphasis is on wireless infrastructure.

## Core switches

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Model** | **Aruba 8325** | **Cisco Catalyst 9500** | **Juniper EX4600** |
| Form Factor | Fixed | Fixed | Fixed |
| Switching Capacity | Up to 6.4 Tbps | Up to 6.4 Tbps | Up to 1.44 Tbps |
| Forwarding Rate | Up to 950 Mpps | Up to 2 Bpps | Up to 1.5 Mpps |
| Rack Units | 1U | 1U-2U depending on model | 1U |
| PoE Capabilities | PoE, PoE+, and UPOE available | PoE, PoE+, and UPOE available | PoE and PoE+ available |
| Port Density | 32 x 100GbE or 128 x 25GbE | Up to 48 x 100GbE | 24 x 40GbE or 72 x 10GbE |
| Redundancy | Redundant power supplies, fans | Redundant power supplies, fans | Redundant power supplies, fans |
| Security Features | ACLs, RA Guard, DHCP Snooping, IP Source Guard, etc. | ACLs, RA Guard, DHCP Snooping, TrustSec, etc. | ACLs, Firewall filters, DDoS protection, etc. |
| Management | Aruba NetEdit, Aruba AirWave | Cisco DNA Center, CLI, SNMP | Junos Space, CLI, SNMP |
| Stackable/Chassis | Virtual Switching Framework (VSF) | StackWise Virtual, VSS | Virtual Chassis |
| Energy Efficiency | Energy Efficient Ethernet (EEE) | EnergyWise, EEE | EEE, Low power modes |
| QoS Capabilities | Advanced QoS with deep packet inspection | Modular QoS CLI, Auto-QoS | Advanced QoS features |
| Software Defined Networking | ArubaOS-CX with Network Analytics Engine | Cisco IOS XE with SD-Access | Junos OS with PyEZ |
| Price (approximate) | 60,490.50 | 21,536.00 | 21,918.00 |

In the core switches category, the Aruba 8325 is a strong contender. It offers a fixed form factor with high switching capacity, making it suitable for the core of a large-scale network like a university. The switch supports Power over Ethernet (PoE), allowing it to power devices like IP cameras and phones.

The Aruba 8325 includes robust security features such as Access Control Lists (ACLs) and DHCP Snooping, ensuring the integrity of the network. Its management tools, Aruba NetEdit and Aruba AirWave, provide comprehensive control and monitoring capabilities, crucial for a network of this scale.

While the Cisco Catalyst 9500 Series offers similar features, the Aruba 8325 provides competitive performance at a potentially more cost-effective price point, making it an attractive option for a university's core network.

## Access Points

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Specification** | **Aruba AP-535** | **Cisco Catalyst 9120AX** | **Ruckus R750** |
| Wi-Fi Standard | Wi-Fi 6 (802.11ax) | Wi-Fi 6 (802.11ax) | Wi-Fi 6 (802.11ax) |
| MIMO Technology | 4x4:4 with MU-MIMO | 4x4:4 with MU-MIMO | 4x4:4 with MU-MIMO |
| Maximum Data Rate | Up to 5.4 Gbps | Up to 5.2 Gbps | Up to 3.5 Gbps |
| Radio Bands | Dual-radio (2.4 GHz and 5 GHz) | Dual-radio (2.4 GHz and 5 GHz) | Dual-radio (2.4 GHz and 5 GHz) |
| Ethernet Ports | 1 x 2.5/1G/100M Ethernet port | 1 x Multigigabit Ethernet port | 1 x 2.5GbE port |
| Power Options | PoE, PoE+, DC power | PoE, PoE+, UPOE, DC power | PoE+, DC power |
| Antenna | Integrated Omni-directional | Integrated Omni-directional | Integrated Omni-directional |
| Spatial Streams | Up to 4 spatial streams | Up to 4 spatial streams | Up to 4 spatial streams |
| Client Capacity | 1024 | 400 | 1024 |
| Security | WPA3, Enhanced Open, AES | WPA3, Enhanced Open, AES | WPA3, Enhanced Open, AES |
| Management | Aruba Central or Aruba AirWave | Cisco DNA Center, Prime Infrastructure | Ruckus SmartZone, Unleashed |
| IoT Readiness | Yes (with USB and Zigbee) | Yes (with optional modules) | Yes (with IoT Suite) |
| Location Services | Aruba location services | Cisco DNA Spaces | Ruckus location services |
| Environmental | Plenum rated, indoor use | Plenum rated, indoor use | Plenum rated, indoor use |
| Warranty and Support | Limited Lifetime Warranty | Limited Lifetime Warranty | Limited Lifetime Warranty |
| Quality of Service | Advanced QoS features | Cisco QoS | Advanced QoS features |
| Price (approximate) | 1,618 | 2,282.97 | 1,290.60 |

For access points, the Aruba AP-535 is a leading choice. It supports the latest Wi-Fi 6 standard, ensuring high data rates and improved performance, crucial for a university with a large number of concurrent users. With 4x4:4 MIMO technology and up to 5.4 Gbps maximum data rate, it provides excellent coverage and capacity.

The Aruba AP-535 offers advanced security features, including WPA3 and Enhanced Open, ensuring a secure wireless environment for students and faculty. Its management tools, Aruba Central or AirWave, provide centralized control, making it easier to manage a large number of access points.

While Cisco and Ruckus also offer competitive options, the Aruba AP-535 stands out for its comprehensive features, high data rates, and advanced security, making it a suitable choice for a university environment.

## Summary

In the dynamic landscape of a bustling university environment, Aruba's network infrastructure emerges as a robust and tailored solution to meet the diverse needs of over 5,000 students and more than 1,500 devices. Let's delve into the key considerations across switches, routers, core switches, and access points to understand why Aruba stands out.

### Switches:

Aruba's 5400R zl2 series strikes a balance, offering a versatile edge solution for the university network. With high PoE capabilities, robust Layer 3 support, and seamless integration with Aruba's management tools, it caters to the demands of a dynamic and ever-expanding campus. While Cisco may boast more extensive features, Aruba's cost-effective approach aligns with the practical needs of a university setting.

### Routers:

In the realm of routers, the Aruba 7205 Series takes center stage, providing a harmonious blend of features perfectly suited for a campus environment. Its emphasis on wireless integration and comprehensive network management aligns seamlessly with the diverse needs of a university's user base. While Cisco's routers offer higher performance, Aruba's focus on practical integration makes it a compelling choice for a cost-conscious educational institution.

### Core Switches:

For the core of the network, Aruba's 8325 takes the spotlight with high switching capacity, robust security features, and competitive pricing. In the heartbeat of a university network, stability and reliability are paramount, and Aruba's fixed form factor ensures just that. While Cisco may present comparable features, Aruba's pricing adds a layer of financial sensibility crucial for an educational institution.

### Access Points:

Aruba's AP-535 leads the pack in access points, offering Wi-Fi 6 support, advanced security, and centralized management. In a university where connectivity is the lifeblood, the AP-535 ensures high performance and a secure wireless environment. While competitors like Cisco and Ruckus are formidable, Aruba's comprehensive features make it the go-to choice for an institution with a myriad of users and devices.

In essence, Aruba's network infrastructure provides not just a solution but a tailored ecosystem that aligns with the unique demands of a large university. Its integrated approach ensures efficiency in management, scalability to accommodate the growing user base, and a cost-effective stance that resonates with the practical considerations of an educational institution. As the heartbeat of the university network, Aruba sets the stage for seamless connectivity, robust security, and scalable performance, paving the way for a digitally empowered learning environment.

## Hardware Advantages & Disadvantages

### Switch Series Disadvantages

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Aspect** | **Aruba 5400R zl2 Switch Series Disadvantages** | **HP 1950 Switch Series Disadvantages** | **Cisco Catalyst 9300 Series Disadvantages** |
| Port Configuration | May lack the Multigigabit ports available on the Cisco series | Limited number of ports and uplink capabilities compared to the others | Could be more expensive due to advanced port capabilities |
| High-Density Wireless Support | May not support the latest Wi-Fi 6 standard as well as Cisco | Limited wireless support could hinder future scalability | Potential higher cost due to optimization for Cisco APs |
| PoE Capabilities | May not offer the advanced UPOE available in Cisco switches | Lower PoE budget per port may not support some high-power devices | Higher costs for advanced PoE capabilities |
| Network Management | Different management platforms may require additional training | Less advanced network management features compared to Aruba and Cisco | Cisco DNA Center could be complex and expensive for small networks |
| Layer Support | Full Layer 3 may be unnecessary for some deployments, adding to cost | Layer 3 Lite may not meet the needs of more complex routing environments | Full Layer 3 capabilities may come with a premium price tag |
| Stacking Capability | VSF limited to 10 switches may not be enough for some large deployments | IRF limited to 9 switches could be a scalability concern | StackWise-480 may require additional investment in specific Cisco hardware |
| Software Defined Networking (SDN) | SDN capabilities may not be as comprehensive as Cisco's DNA platform | Limited SDN features could restrict future network programmability and automation | Full SDN capabilities may lead to higher initial and ongoing costs |
| Security Features | Security feature set may not be as extensive as Cisco's | Less comprehensive security features could be a concern for sensitive environments | Advanced security features could increase complexity and cost |
| Redundancy | Redundant management and power may not be as modular as Cisco's | Lack of redundant power and fixed fans could pose a risk for mission-critical environments | Redundant power and modular fans come at a higher cost |
| Energy Efficiency | Intelligent Power Management may not be as advanced as Cisco's | Low power consumption may indicate less performance or capabilities | Superior power management could reflect in the product's higher price |
| Scalability | While highly scalable, may not match the sheer scale of Cisco's offerings | Limited scalability may not be suitable for growing enterprise networks | Scalability comes with a higher cost, potentially over-provisioning for small to medium networks |
| Interoperability | Excellent with multi-vendor environments but may have nuances in Cisco-heavy ecosystems | Good interoperability but potentially less so than Aruba and Cisco | Best with Cisco environments, which may lead to vendor lock-in and higher costs |
| Warranty and Support | Next-business-day replacement is standard but may not match Cisco's SMARTnet options | Same as Aruba, may lack the comprehensive support options of Cisco | SMARTnet support comes at an additional cost, increasing total cost of ownership |
| Price (approximate) | Mid-range cost but may be higher than necessary for some deployments | More affordable but may lack features needed for future-proofing | Highest cost, which may not be justifiable for all network environments |

### Switch Model Advantages

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Aspect** | **Aruba 5400R zl2 Switch Series Advantages** | **HP 1950 Switch Series Advantages** | **Cisco Catalyst 9300 Series Advantages** |
| Port Configuration | Versatile port configurations with high-speed uplinks, suitable for various network sizes | Adequate for small to mid-sized networks with essential 10GbE uplinks | Advanced Multigigabit ports and high-speed uplinks, ideal for high-throughput applications |
| High-Density Wireless Support | Optimized integration with Aruba APs, Smart Rate ports for high-speed AP connections | Sufficient for basic wireless deployments, offering essential services | Optimized for the latest Wi-Fi 6 standard with Cisco APs, future-proofing wireless infrastructure |
| PoE Capabilities | Offers high-power PoE options up to 60W per port, catering to power-hungry devices | Provides essential PoE capabilities for standard PoE devices | Advanced PoE options with UPOE, supporting even more power-intensive devices |
| Network Management | Comprehensive management tools including AirWave and Central for streamlined operations | Simple web management and CLI, suitable for less complex networks | State-of-the-art Cisco DNA Center for a unified approach to network management and automation |
| Layer Support | Full Layer 3 support with advanced routing protocols, ideal for complex network topologies | Offers basic Layer 3 capabilities, sufficient for simple routing needs | Full Layer 3 features with support for proprietary protocols like EIGRP, suitable for advanced networks |
| Stacking Capability | VSF allows for simplified management of up to 10 switches as a single unit | IRF provides easy management for up to 9 switches, aiding in scalability | StackWise-480 offers high-performance stacking and easy scalability for up to 9 switches |
| Software Defined Networking (SDN) | Support for SDN with ArubaOS-Switch and ClearPass for enhanced network programmability | Limited SDN features can be suitable for networks not requiring complex automation | Full SDN capabilities with Cisco DNA, offering a future-proof platform for network innovation |
| Security Features | Robust security features including ACLs, RADIUS, TACACS+, and MACsec for comprehensive protection | Basic security features adequate for small to medium-sized businesses | Extensive security suite with TrustSec, ETA, and MACsec, providing top-tier network security |
| Redundancy | Redundant management and power options ensure network uptime and reliability | Fixed configuration with essential features offers a balance between cost and performance | Modular redundancy options provide the highest reliability for mission-critical environments |
| Energy Efficiency | Energy Efficient Ethernet and intelligent power management for cost-effective operations | Low power consumption ideal for budget-conscious deployments | Superior power management features for energy savings at scale |
| Scalability | Designed to scale from the edge to the core, meeting diverse enterprise needs | Suitable for small-sized deployments, offering a balance of performance and cost | Highly scalable, perfect for large-scale deployments with demanding performance requirements |

### Router Model Advantages

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature/Aspect** | **Aruba 7205** | **HP FlexNetwork MSR930** | **Cisco 4451-X** |
| Performance | Designed for medium to large enterprise campuses, offers high throughput | Targeted at small to medium-sized businesses, moderate performance | High-performance router suitable for large enterprises and data center edges |
| Modularity | Fixed configuration with some modular capabilities for interfaces | Some models offer modular interface options | Highly modular with a wide range of interface options |
| Routing Capabilities | Advanced Layer 3 features, suitable for campus networks | Good Layer 3 capabilities for branch offices and small enterprises | Extensive Layer 3 features, suitable for complex enterprise networks |
| Integrated Services | Offers wireless LAN controller functionality, strong in wireless integration | Basic integrated services with an emphasis on routing and VPN | Wide range of integrated services including security, voice, and application services |
| Security Features | Robust security features with integration into Aruba's security ecosystem | Basic to intermediate security features suitable for SMBs | Advanced security features with encryption, firewall, intrusion prevention, etc. |
| Management | Centralized management with Aruba AirWave and Aruba Central | HP IMC (Intelligent Management Center) for network management | Cisco IOS XE for on-device management and Cisco DNA Center for centralized management |
| Redundancy and Resiliency | Supports high availability features for critical network uptime | Offers some redundancy options like dual power supplies | Supports advanced redundancy features, including dual IOS and modular components |
| Scalability | Scalable within the Aruba network ecosystem, especially for wireless deployments | Limited scalability compared to the other two options | Highly scalable with services and hardware that can grow with network demands |
| Energy Efficiency | Energy-efficient operations with Aruba's Eco-Mode | Energy-efficient design for reduced operational costs | Energy-efficient with features like variable speed fans and efficient power supplies |
| Price | Competitive within its feature set, good for value-conscious enterprise networks | Generally more affordable, aimed at cost-sensitive deployments | Higher price due to advanced features and performance |
| Ideal Use Case | Ideal for organizations with a heavy emphasis on wireless infrastructure | Suited for small to medium-sized branch offices with moderate routing needs | Best for large enterprise networks requiring high throughput and service integration |

# IDFs

When referring to maps, IDFs numbers are discussed from west to east.

We are striving for microsegmentation whereby each device has a dedicated port on a switch.

All connection between device and port on edge switches are doubled to increase reliability and redundancy as per instruction from the ATU Head Technician.

All totals are approximate and based on current available information.

The chosen low-end switch for the make-up of IDF is the Aruba 5400 ZL2 which are available in many sized up to 288 ports which includes power over ethernet to ensure correct shutdown in the event of loss of power. The number of ports required in the IDFs can be seen below and the size and number of switches calculated accordingly.

## Main Building - Level 1

IDF 1 on level 1 will require around 175 connections for computers in classrooms and offices. It will also require around 10 printers and 15 wireless routers. That amounts to a total of 200 ports required on edge switches but since each connection is to be doubled it is actually a necessity of 400 ports on low-end switches in the IDF.

IDF 2, in the canteen and library area will require connect for an estimated 24 computers. It will also require 2 cash registers, 2 credit card readers, 15 access points and 10 printers. That amounts to a necessity of 106 ports on low-end switches in the IDF.

IDF 3, in the east wing, will serve about 85 computers, 1 cash register, 1 credit card reader, as well as approximately 20 printers and 15 access points which amounts to a total necessity of 244 ports on low-end switches in the IDF.

## Main Building - Level 2

IDF 1 on level 2 will require around 146 connections for computers in classrooms and offices. It will also require around 10 printers and 15 wireless routers which amounts to a total necessity of 342 ports on low-end switches in the IDF.

IDF 2, in the coffee dock and library area will require connect for an estimated 236 computers. It will also require 1 cash register, 1 credit card readers, 15 access points and 20 printers, due to the CAD lab, Architectural technology labs and library printing zone found nearby. That amounts to a total necessity of 566 ports on low-end switches in the IDF.

IDF 3, in the east wing, will serve about 394 computers as well as approximately 20 printers and 15 access points. As the MDF is located at this level and in this area, some connections may be better placed on edge switches in the MDF. However, this has not been represented on the maps for the sake of consistency. That amounts to a total necessity of 858 ports on low-end switches in the IDF.

## Main Building - Level 3

IDF 1 on level 3 will require around 85 connections for computers in classrooms and offices. It will also require around 10 printers and 15 wireless routers. IDF 1 on level 3 will require 220 dedicated ports.

IDF 2 will require connect for an estimated 173 computers. It will also require 15 access points and 20 printers. IDF 1 on level 3 will require 416 dedicated ports. A high concentration of devices are found directly above the MDF and a decision may be made to connect to a low-end switch therein though this has not been expressed on the maps.

## Colab - Level 1

IDF 1 and IDF 2 on level 1 will each require around 200 connections for computers in offices. It will also require around 20 printers and 15 wireless routers in total for that level. Thus, IDF 1 and 2 in the Colab will require 470 switch ports or 235 each.

## Colab - Level 2

IDF 1, the only one on level 2 of the Colab, will require around 100 connections for computers in offices. It will also require around 20 printers and 15 wireless routers. This IDF will require 270 switch ports.

## An Danlann

IDF 1 is found on level 2 of An Danlann to protect against flooding and also in proximity to the highest concentration of connections. It will require around 40 connections for computers in offices. It will also require 1 cash register, 1 credit card reader, around 10 printers and 15 wireless routers. The IDF in An Danlann will require approximately 134 ports in the IDF.

## Killybegs Satellite Campus

IDF 1 on level 1 of the campus, to protect against flooding and also to be in proximity to the highest concentration of connections, will require around 100 connections for computers in classrooms and offices. It will also require around 10 printers and 15 wireless routers. The Killybegs IDF should comprise some 270 edge switch ports.

# Cabling

## Distance

The maximum distance between a machine on the network and an IDF is 99 meters. However, best practice is to plan for a 75-meter separation. Therefore, IDF positions shown on the maps have been allocated in accordance with best-practice standard.

## Copper Cabling

Augmented Category 6 or CAT6a copper cabling has been selected for our workspace cabling. CAT6a is designed to support 10-gigabit ethernet over a 100-meter horizontal UTP channel. It more than satisfies TIA and EIA standards and also, goes beyond IEEE 802.3an by establishing the electrical requirements for the permanent link and cabling components. The cost is slightly higher that CAT 6 cabling though the benefits in terms of bandwidth, seen in the table below, clearly show the advantage is worth the cost. Moreover, the increase in price realized if considering CAT7 has been deemed to be unjustifiable.A table with text and images

Description automatically generated

Figure 2 - Comparison of copper cabling categories (Szyper et al, 2007)

## Connectors

For each length of CAT6a cable between devices and switches in the IDFs, 2 RJ45 connectors will be needed, that is, one for each end of the cable length.

For the ends of each length of fibre-optic cable, both single-and multi-mode, LC connectors have been chosen.

LC connectors, being the more modern choice, have several advantages when compared to the alternative, SC connectors. Firstly, they allow for higher port density in network panels and racks being smaller and more compact. Secondly, their latch mechanism, like the RJ45, is easier to insert and remove than SC connectors. Finally, as they are the more modern option, they are increasingly compatible with a broad range of networking equipment which is likely to continue in future.

# Structured Cabling System

## Horizontal Cabling

To connect devices to low-end switches in the IDFs, CAT6a copper cable will be deployed at a distance of no more than 75m.

The actual permitted distance is 99 meters though industry best-practice standards is to restrict horizontal cabling to 75 meters. That breaks down to a maximum of 3 meters between network devices and wiring blocks, 90 meters between wiring blocks and patch panels, and 6 meters from the patch panel to the switch inside the IDF or MDF, as shown below.

A diagram of a network connection

Description automatically generated

Figure 3 - Horizontal cabling layout and distances (FS Community, 2021)

## Backbone Cabling

To construct the backbone cabling, fibre-optic cabling will be used. This will connect the IDFs on the first, second and third levels on top of, IDFs in The Colab building and An Danlann, to the MDF on the level 2.

For backbone cabling connections, fibre optic cable will be used to deal with bandwidth demands on the network caused by network traffic. The adopted policy is to use multi-mode fibre-optic cable inside the university buildings and to use single-mode fibre-optic between buildings, in other words, for IDFs located greater distances from the MDF. Fibre-optic connections can be seen as orange (multi-mode) and yellow (single-Mode) lines on the following maps.

On the ground floor, running the fibre-optic cabling above the ceiling makes sense so as to facilitate the vertical connection upwards to the MDF.

Whereas, on the level 3, running the fibre-optic cabling underfloor may be best so as to allow a downward vertical connection to the MDF below.

In practice, considering the physical building make-up, some flexibility may be needed.

# IDF and MDF Placement

## MDF Placement

There are 3 levels in the ATU main building. The MDF will be located in a central location on level 2 to protect against water damage in case of flooding. The location of the MDF will be where the Design studio is currently located. It connects to the ISP vertically through entrance facility to the underground fibre-optic cable, installed by the ISP.

Two IDFs can be seen on the following maps on the level 2 to the right of the MDF while a third is to be located to the right of the MDF on the map.

To the left of the MDF, an IDF will be located in the library to accommodate the high amount of network traffic generated by the library IT area, which currently contains around 92 computers. Furthermore, 2 computer rooms, 2 architecture technology labs and a CAD lab are adjacent to the library IT area with approximately 32 computers each as well as printers.

Another is to be positioned in the center of H-block. This will accommodate for traffic created by the 146 computers as well as printers in the classrooms, computer games lab, drawing/model-making studio and offices.

To the right of the MDF on the level-2 map, an IDF will be placed in the design studio 2299 for proximity to the 263 computers and other devices currently connected in the south-east block.

## Level 1

Below, on level 1 we see 3 IDFs. Again, one is in the center of H-block to serve the high concentration of approximately 100 connections found in the north-west corner.

Another is to be located in lecture theatre 1101 as this and the adjacent lecture theatres, library and university administration offices may be too far from the IDF in H-block to guarantee a reliable connection. The registers and credit-card machines in the restaurant are also a consideration in making this decision.

The third IDF on the level 1 will be located in the goods-inwards room near the concourse is currently located. This location is central to south-east block of ATU and will serve the 85 computers in addition to printers and other connections found in that end of the building.

Multi-mode fibre optic cable will run above the ceiling to the finance office and connect vertically to the MDF above.

## Level 3

Level 3, hosting fewer connections, will contain only 2 IDFs. One in the center of H-block which hosts 75 computers as well as other devices. While the other will be in a central location in the south-east block in the early childhood studies playroom which connects around 181 computers in addition to other devices.

Like on the ground floor, multi-mode fibre-optic cable runs underfloor to the design studio in room 3336 and 3337 and connects vertically to the MDF below.

## Colab

To deal with the high number of small enterprises and subsequent traffic on level 1 of the Colab, 2 IDFs will be deployed. They are connected in parallel to the MDF through, as afore mentioned, multi-mode fibre-optic cable inside the Colab and single-mode traversing the outside distance between the buildings.

The smaller amount of traffic on level 2 can be accommodated by a single, central IDF on that floor. This is connect in the same way as those on level 1.

## An Danlann

A single IDF will be located on the second floor of an Danlann for proximity to the greater concentration of connections found there. The IDF will be connected to the MDF via single-mode fibre-optic cable due to the distance between it and the MDF.

## Killybegs

Killybegs campus, which is a satellite campus located 70km away from the main ATU campus, will be connected using the internet service provider’s existing fibre-optic line. It will contain 1 IDF and no map of the campus is available.

Note: The first map presented is the main building, level 2. The reason for this is that the MDF is located on this level and all connections are in relation to that.

# Maps

A floor plan of a building

Description automatically generated

A diagram of a building

Description automatically generated

A blueprint of a building

Description automatically generated

A diagram of a building

Description automatically generated

A diagram of a building

Description automatically generated

# Access Points

250 wireless routers will be purchased. The selected router will be the Aruba AP-535 wireless router for the reasons previously mentioned.

ATU Letterkenny campus is 18,000m2. The average indoor coverage of a 5g router is 15m2 (Chattanooga, 2023).

Access point routers will consequently be placed at a distribution of roughly one router per 30m2. Consideration will have to be given for solid walls and areas where traffic may be higher.

The university main building has been divided into 3 sections where approximately 15 wireless routers will be needed, namely H-Block, the canteen/ library areas and the east block. As there is no library nor canteen on level three, only 2 sections are needed here. As such, a total of 120 access points are to be found in the main building composed of 8 sections of 15 wireless routers (3 sections on level 1 & 2 and 2 sections on level 3).

A total of 200 Aruba AP-535 wireless routers will be purchased with 80 being estimated for the Colab, An Danlann and the Killybegs campus. As mentioned above, 120 will e required for the three levels of the main building. There will then be an access of 20 wireless routers to deal with areas of high traffic and physical obstacles like solid walls.

Wireless routers will be ceiling-mounted where possible to avoid interference on the ground.

# Broadcast & Collision Domains

Broadcast domain: A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer (Wikipedia, 2023).

Broadcast domains need to be properly administered to regulate traffic and ensure information is sent only to its intended recipients.

Collision domain: The portion of the network where the packets can collide when sent across a shared media (Cisco Learning Network, 2020).

Collision domains need to be limited so as to ensure traffic flows smoothly and does not block up the system.

## VLANS

The use of VLANS will facilitate data sharing across relevant groups. For example, all users in the School of Business VLAN can easily access common libraries or share files.

VLANS also have security and administration benefits.

We will employ VLANS to separate broadcast domains limiting the members of the VLAN to the broadcast domain.

## Switches

Microsegmentation is mainly used to enhance the efficiency or security of the network.

Switches, which are implicit microsegmentation, are used to reduce and limit collision domains.

The microsegmentation performed by the switches we have employed results in the reduction of collision domains. Only two nodes will be present as a result of the collision domain reduction (Rouse, 2016).

# Internal Servers & Services

## NTP (Network Time Protocol)

NTPs are designed to synchronise the clocks over a network, it acts as a timekeeper within a network, helping devices maintain synchronization for various purposes, including logging, security, and coordination of events.

GPS disciplined clock will be also used as stratum 0 device as it provides accurate time sources as its directly connected to the satellite.

### Considerations:

* Enhanced security.
* Log consistency – Synchronised timekeeping is useful for troubleshooting, forensic analysis, and auditing.
* GPS provides greater accuracy for timekeeping.

## DNS (Domain Name Server)

DNS translates human readable domain names into numerical IP addresses. It enables users to access various elements of the internet with domain names such as websites. Keeping DNS server local allows the organisation more control, reduced latency which means faster response times for DNS queries, reduces security risks such as DNS poisoning and offers more control over privacy protecting sensitive data.

### Considerations:

* More control over configuration of DNS server.
* Reduced latency.
* Reduced security risk.
* More control over privacy.

## DHCP (Dynamic Host Configuration Protocol)

DHCP server is responsible for automatically assigning IP addresses and network configurations to devices within a local network. Using a local DHCP server allows the organisation more control over, like with most locally implemented services it will have reduced latency and reduced security risks especially with the implementation of DNS snooping.

### Considerations:

* Security measures – isolating this service reduces exposure to external threats.
* Reduced Latency.
* IP address management – allows organisation to configure DHCP to suit their own needs.

## SSH (Secure Shell)

SSH provides a secure and encrypted method for accessing and managing network devices, servers, and computers within a local network. An SSH is essential for a local network as it encrypts data being transmitted which prevents eavesdropping, access to this service should be limited to authorised users only to increase security. Additionally, it reduces exposure of sensitive data to potential threats on the broader internet and it is platform independent, meaning that it is available for various operating systems.

### Considerations:

* Secure data transmission
* Reduces exposure to external threats.
* Platform Independent.

## Proxy Server

Proxy servers act as an intermediate server that act as a gateway between a user’s device and the Internet. This is crucial for a local network as it masks IP addresses which protects the user’s privacy, acts as an additional layer of security as it inspects and filters incoming and outgoing traffic. It can also be configured to implement bandwidth throttling, which limits the speed at which data is transmitted between the client and the server.

### Considerations:

* Enhanced privacy.
* Increased security through filtering traffic.
* Balanced bandwidth – bandwidth throttling.

## File Servers

File servers act as dedicated storage systems within a network, providing a central location for users to store and retrieve files. Security is enhanced through access control mechanisms. Admins can define user permissions. Additionally, filer servers promote collaboration by enabling multiple users to access and work on shared files.

### Considerations:

* Dedicated storage for files.
* Security – Access controls.
* Promotes collaboration – allows multiple users to work on shared files.
* Data Integrity – include RAID to ensure data integrity.

## Application servers

Application servers play a central role in hosting and executing applications within a networked environment. They facilitate seamless communication between app layer and database servers, and support load balancing which ensures optimal performance and fault tolerance.

### Considerations:

* Servers are scalable.
* Performance optimization – load balancing.
* Security – secures communication channels, enforces access controls.

## Web servers

Web servers play a pivotal role in serving web content and apps to users over the Internet, it provides the infrastructure for hosting websites, web apps, and other internet-based content. They implement security features such as HTTPS for secure data transmission and mechanisms to prevent common web vulnerabilities.

### Considerations:

* Servers are scalable.
* Security – implement firewalls and intrusion detection systems.
* Regularly backup website data and configurations.

## Print servers

Print servers facilitate the management and distribution of print jobs within a network. They enhance efficiency by managing print queues, providing job status updates, and facilitating resource sharing.

### Considerations:

* Regular update of drivers.
* User authentication.
* Verify printer compatibility.
* Queue monitoring tool.

## Where to store services:

Most services will be stored on virtual machines, they will be hosted on the cloud but placed behind the firewall on the local network. The exceptions to this will be DHCP and DNS which will be stored on a physical device and stored exclusively on the local network.

# IP addressing

We will start with the private IP address of 172.16.0.0 and CIDR prefix 16 as this will make sure we can allocate enough routers on our network.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network Address** | **From** | **To** | **Broadcast** | **Purpose** |
| 172.16.0.0/20 | 172.16.0.1/20 | 172.16.15.254/20 | 172.16.15.255 | Classes |
| 172.16.16.0/20 | 172.16.16.1/20 | 172.16.31.254/20 | 172.16.31.255 | An Danlann |
| 172.16.32.0/20 | 172.16.32.1/20 | 172.16.47.254/20 | 172.16.47.255 | Wi-Fi |
| 172.16.48.0/20 | 172.16.48.1/20 | 172.16.63.254/20 | 172.16.63.255 | Lecturers |
| 172.16.64.0/20 | 172.16.64.1/20 | 172.16.79.254/20 | 172.16.79.255 | Colab |
| 172.16.80.0/20 | 172.16.80.1/20 | 172.16.95.254/20 | 172.16.95.255 | Technicians |
| 172.16.96.0/20 | 172.16.96.1/20 | 172.16.111.254/20 | 172.16.111.255 | Printers |
| 172.16.112.0/20 | 172.16.112.1/20 | 172.16.127.254/20 | 172.16.127.255 | Medical Centre |
| 172.16.128.0/20 | 172.16.128.1/20 | 172.16.143.254/20 | 172.16.143.255 | Killybegs |
| 172.16.144.0/20 | 172.16.144.1/20 | 172.16.159.254/20 | 172.16.159.255 | Admin Staff |
| 172.16.160.0/20 | 172.16.160.1/20 | 172.16.175.254/20 | 172.16.175.255 | Servers |

The following table will show the address spaces and each of their purposes. In each subnet we will allocate the WAN connection to each IDF.

Here you can see the WAN connection from the 172.16.x.x/16 subnet to each router and the IP for each endpoint. Each of the address IDF will be a router that runs its own VLAN to isolate each resource and avoid security problems.

Each of these VLANs will have the address space of 10.0.0.0/8 for the DHCP pools.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WAN network address** | **WAN address MDF** | **WAN address IDF** | **WAN Broadcast** | **WAN purpose** |
| 172.16.0.0/30 | 172.16.0.1/30 | 172.16.0.2/30 | 172.16.0.3 | Business, Education, Design |
| 172.16.0.4/30 | 172.16.0.5/30 | 172.16.0.6/30 | 172.16.0.7 | Science, Health |
| 172.16.0.8/30 | 172.16.0.9/30 | 172.16.0.10/30 | 172.16.0.11 | Engineering, Technology |
| 172.16.16.0/30 | 172.16.16.1/30 | 172.16.16.2/30 | 172.16.16.3 | An Danlann |
| 172.16.32.0/30 | 172.16.32.1/30 | 172.16.32.2/30 | 172.16.32.3 | Student, Staff Wi-Fi |
| 172.16.32.4/30 | 172.16.32.5/30 | 172.16.32.6/30 | 172.16.32.7 | Guest Wi-Fi |
| 172.16.48.0/30 | 172.16.48.1/30 | 172.16.48.2/30 | 172.16.48.3 | Lecturers |
| 172.16.64.0/30 | 172.16.64.1/30 | 172.16.64.2/30 | 172.16.64.3 | Colab |
| 172.16.80.0/30 | 172.16.80.1/30 | 172.16.80.2/30 | 172.16.80.3 | Technicians |
| 172.16.96.0/30 | 172.16.96.1/30 | 172.16.96.2/30 | 172.16.96.3 | Printers |
| 172.16.112.0/30 | 172.16.112.1/30 | 172.16.112.2/30 | 172.16.112.3 | Medical Centre |
| 172.16.128.0/30 | 172.16.128.1/30 | 172.16.128.2/30 | 172.16.128.3 | Killybegs |
| 172.16.144.0/30 | 172.16.144.1/30 | 172.16.144.2/30 | 172.16.144.3 | Admin Staff |
| 172.16.160.0/30 | 172.16.160.1/30 | 172.16.160.2/30 | 172.16.160.3 | Servers DMZ |

The only subnets that will be able to talk to everybody else will be technicians and admin staff. For the rest of subnets, no connections will be allowed between them. ICMP will also be blocked as to avoid any kind of recognisance for threat actors.

Splitting off by VLAN not only isolates the resources, but also avoids Broadcast Collisions and the IDFs in place will resolve any Domain Collisions.

Each department in the school (Such as Business, Science and Engineering) will have their own VLANs. The reason for using a VLAN for so many devices is that in the case of the compromise of the student systems, they do not store any sensitive information and can be recovered using system images, so in terms of cost it is not worth splitting the student networks by one VLAN per classroom.

By splitting VLANs by department we will also be able to provide custom rules for the firewall. For example, a student in the computing department should be allowed to run Wireshark, but someone in the Science department shouldn’t.

# Security

## Firewalls

We will have next gen firewalls, which will take care of packet filtering and deep packet inspection among others. Their capabilities are:

* Packet filtering
* Application awareness and control
* Signature detection
* Statistical anomaly detection
* Stateful protocol analysis detection

Packet filtering will examine each packet that goes through the firewall and determine whether to allow it to pass based on certain rules.

Application awareness and control is a necessary feature to understand the traffic that to the naked eye may seem malicious but its just a commonly known application. This way we can avoid false positives.

Signature detection will be used to detect and report commonly known threats or attacks.

Statistical anomaly detection monitors network traffic for unusual patterns or deviations from established baselines.

Stateful protocol analysis detection tracks the state of current connections and makes decisions based on the context of the communication.

Together, all these features will protect our network from external and internal threats or compromises such as someone infiltrating the network or malware infection. A next gen firewall will be placed between the IDF and MDF, and another one outside the Server IDF to make it a demilitarized zone.

## Wi-Fi authentication

Users that want to connect to the student network will need to have their internal EAP certificate and their username and password for the connection.

As for the guests in the network, only a password will be necessary and the NAC server will provide a temporary EAP certificate to encrypt the connection, as well as very restricted access to the network.

## 802.1X

We will use 802.1X to prevent unauthorized devices from connecting to our network.

Our server will oversee authorising the supplicants by using a RADIUS (Remote Authentication Dial-In User Service) server.

The configuration should support EAP-TLS, PEAP, and EAP-MSCHAPv2.

It is also critical to monitor and log all authentication attempts, failures, and suspicious activities. We also need to make sure that our security policies are up to date with the 802.1X IEEE standard.

## VPN

We will use a Remote Access VPN that supports IPSec and SSL/TLS called OpenVPN.

Teachers and staff may need to access resources only available through the university network as to avoid any possible data breaches, and a VPN is our solution for this. We will enforce the use of SSL/TLS certificates for connection as to avoid any weak password attacks.

These certificates will be given individually to each member of staff that will require access to the network from home in a secure manner to avoid the compromise of these keys.

Any connection will need to be verified my Multiple Factor Authentication or MFA, so in the case any threat actor would get access to these keys or compromise staff devices cannot access any internal assets.

## NAC

A NAC is required to restrict access to networks based on policies.

The Enforcement points for our network will be all the switches and routers, making sure they abide by the policies in place.

For the guest Wi-Fi endpoints, we will need to provide a temporary and restricted access to the network.

The NAC will be connected to our RADIUS server to provide authentication to our network devices.

## Antivirus Software

All computers and devices that are company property shall all always have the latest version of Microsoft Defender and Operative System.

All Antivirus detections shall be reported back to the Azure Security Dashboard for any SOC analyst to analyse.

## Zero-trust policies

All policies, reporting and procedures shall be handled by the Azure Security Centre, which is a cloud-based security management service ran by Microsoft Azure.

No user besides the Administrators should be allowed to run any software as Administrator to avoid any kind of malware from having system permissions.

Any windows events such as user program installs, Antivirus detections or any other malicious activity should be notified to the SOC team to analyse and take actions.

## Email

All email services such as SMTP and IMAP must be encrypted with the use of SSL/TLS and these services must be configures with their SPF records to avoid any kind of spoofing of email addresses.

## Authentication key storage

All keys shall be stored in the Azure Key Vault to protect all keys from internal attacks and assures that all the encryption compliance requirements are met.

## Internal asset access

Teachers may need to access private data. To assure that only the authorised people can access the data, they must connect through the VPN to access these resources.

## Software installation across student devices

All systems will be provided a copy of Microsoft Software centre. In here, only software that has been authorized beforehand by Administrators will be allowed to be installed and allow Administrators to install software to multiple computers remotely if they desire.

## Conclusion

All internal assets will be protected using VLANs and DMZs. Cross-communication will be prohibited based on firewall and NAC rules to avoid any kind of access to information you should not be accessing.

Using TLS/SSL for all internal and external services assures that if a MiTM attack were to take place, none of the internal information will be compromised as all traffic will be encrypted.

Attacks such as DNS or ARP spoofing would not be possible because of the firewalls put in place.

MFA will be used for all authentications in case any SSL/TLS certificates or passwords were to be compromised.

Software shall not be installed by users with Administrator permissions unless allowed by the Administrators in the Microsoft Software Centre.

Constant monitoring and reporting of the network activity is be managed by Azure Security Centre as to avoid any kind of local attack to circumvent these measures.

These rules should provide a secure environment where assets are protected and data will remain private, while still allowing students to carry out the necessary activities for their course.

# References:

6sense (no date) *Cisco Switches vs Aruba CX Switches: Networking Hardware Comparison*, *6sense*. Available at: <https://www.6sense.com/tech/networking-hardware/ciscoswitches-vs-arubacxswitches> (Accessed: 12 December 2023).

ArubaNetworking (2023) ‘HPE Aruba Networking Central’.

ArubaNetworks (2021a) ‘ARUBA 2930F SWITCH SERIES’.

ArubaNetworks (2021b) ‘ARUBA 5400R ZL2 SWITCH SERIES’.

ArubaNetworks (2023a) ‘ARUBA CX 8325 SWITCH SERIES’.

ArubaNetworks (2023b) *ClearPass Hardware Appliance Specifications and Components*. Available at: <https://www.arubanetworks.com/techdocs/ClearPass/6.10/Installation-Guide/Content/InstallationGuide/Hardware/HW-Appliance-Specs.htm> (Accessed: 12 December 2023).

ArubaNetworks (no date) *Reference Architectures*, *Validated Solution Guide*. Available at: <https://www.arubanetworks.com/techdocs/VSG/docs/010-campus-design/esp-campus-design-060-reference-architectures/> (Accessed: 12 December 2023).

BlackBox (2023) ‘6 REASONS CAT6A IS IN YOUR FUTURE’.

CDW (2023) *Cisco Catalyst 9500 - Network Advantage - switch - 40 ports - managed - rack-mountable - C9500-40X-A - Modular Switches*, *CDW.com*. Available at: <https://www.cdw.com/product/cisco-catalyst-9500-network-advantage-switch-40-ports-managed/4921024> (Accessed: 12 December 2023).

Chattanooga, E.P.B. (2023) *EPB Chattanooga - How far will your Wi-Fi signal reach?* Available at: <https://epb.com/get-connected/gig-internet/how-far-will-your-wi-fi-signal-reach/> (Accessed: 11 December 2023).

CiscoLearningNetwork (2020) *Broadcast Vs Collision domain*. Available at: <https://learningnetwork.cisco.com/s/question/0D53i00000KsyCjCAJ/broadcast-vs-collision-domain> (Accessed: 11 December 2023).

GeeksforGeeks (2020) ‘Advantage and Disadvantage of Routers’, *GeeksforGeeks*, 12 December. Available at: <https://www.geeksforgeeks.org/advantage-and-disadvantage-of-routers/> (Accessed: 12 December 2023).

Henry, M. (2022) ‘Lan Design PowerPoint 2022’.

Henry, M. (2023) ‘Walkthrough - Infrastructure Services 2023’.

HPEnterprise (2023) *HPE Aruba Networking CX 8325 Switch Series | HPE Store US*. Available at: <https://buy.hpe.com/us/en/networking/switches/fixed-port-l3-managed-ethernet-switches/aruba-8325-switch-products/hpe-aruba-networking-cx-8325-switch-series/p/1011156780> (Accessed: 12 December 2023).

HPEnterprise, H.P. (2023) *Aruba Mobility Master Controller - Specifications*. Available at: <https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00016271en_us> (Accessed: 12 December 2023).

Kyle (no date) *Aruba vs. Cisco Catalyst: Which Switch is Best for Your Network?* Available at: <https://info.hummingbirdnetworks.com/blog/aruba-vs.-cisco-catalyst-which-switch-is-best-for-your-network> (Accessed: 12 December 2023).

McLAUGHLIN, P. (no date) ‘Category 8 Questions Answered’.

RFWirelessWorld (no date) *Advantages of Routers | disadvantages of Routers*. Available at: <https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-Routers.html> (Accessed: 12 December 2023).

Rouse, M. (2016) ‘Microsegmentation’, *Techopedia*, 30 November. Available at: <https://www.techopedia.com/definition/13989/microsegmentation-collision-domains> (Accessed: 11 December 2023).

router-switch (2002) ‘Cisco Switches vs. HPE / Aruba Switches’.

router-switch (2023) *Aruba Overview, Comparison, and Featured Products*. Available at: <https://www.router-switch.com/aruba-networks.html> (Accessed: 12 December 2023).

Satish, K. (2023) *Advantage and Disadvantage of Routers*. Available at: <https://www.tutorialspoint.com/advantage-and-disadvantage-of-routers> (Accessed: 12 December 2023).

SHI (2023) *HPE Aruba 8325-48Y8C | www.shi.com*. Available at: <https://www.shi.com/product/36964291/HPE-Aruba-8325-48Y8C> (Accessed: 12 December 2023).

Szyper, R. *et al.* (2007) ‘Guide to Structured Cabling’, *Black Box Corporation.* [Preprint].

Wikipedia (2023) ‘Broadcast domain’, *Wikipedia*. Available at: <https://en.wikipedia.org/w/index.php?title=Broadcast_domain&oldid=1182268596> (Accessed: 11 December 2023).

HPE Aruba Networking. “Access Points.”. Available at: [//www.arubanetworks.com/products/wireless/access-points/](https://doi.org/www.arubanetworks.com/products/wireless/access-points/) ( Accessed: December 8, 2023).

HPE Aruba Networking. “Aruba CX 8325 Switch Series Data Sheet.” Available at: [//www.arubanetworks.com/resource/aruba-8325-switch-series-data-sheet/](https://doi.org/www.arubanetworks.com/resource/aruba-8325-switch-series-data-sheet/) ( Accessed: December 8, 2023).

HPE Aruba Networking. “Network Switches for Enterprise.”. Available at: [//www.arubanetworks.com/products/switches/](https://doi.org/www.arubanetworks.com/products/switches/) ( Accessed: December 8, 2023).

HPE Aruba Networking. “The Stackable Aruba 2930F Switch Series.” [//www.arubanetworks.com/products/switches/access/2930f-series/](https://doi.org/www.arubanetworks.com/products/switches/access/2930f-series/) ( Accessed: December 8, 2023).

Inc, Gartner. “HPE (Aruba) vs Extreme Networks 2023 | Gartner Peer Insights.” Gartner. Accessed. Available at: <https://www.gartner.com/market/enterprise-wired-wireless-lan-access-infrastructure/compare/aruba-vs-extreme-networks> (Accessed: December 8, 2023).

‘Extended Star Topology | Importance and Uses of Extended Star Topology’ (2020) *EDUCBA*, 4 February. Available at: https://www.educba.com/extended-star-topology/ (Accessed: 12 December 2023).

Gillis, A. (2021) *What Is Network Topology? - Definition from SearchNetworking*, *Networking*. Available at: https://www.techtarget.com/searchnetworking/definition/network-topology (Accessed: 12 December 2023).

FS Community (2021) *Structured Cabling: Backbone Cabling vs Horizontal Cabling | FS Community*, *Knowledge*. Available at: <https://community.fs.com:7003/article/horizontal-cabling-vs-backbone-cabling.html> (Accessed: 13 December 2023).

FS Community (2021) Structured Cabling: Backbone Cabling vs Horizontal Cabling | FS Community, Knowledge. Available at: <https://community.fs.com:7003/article/horizontal-cabling-vs-backbone-cabling.html>