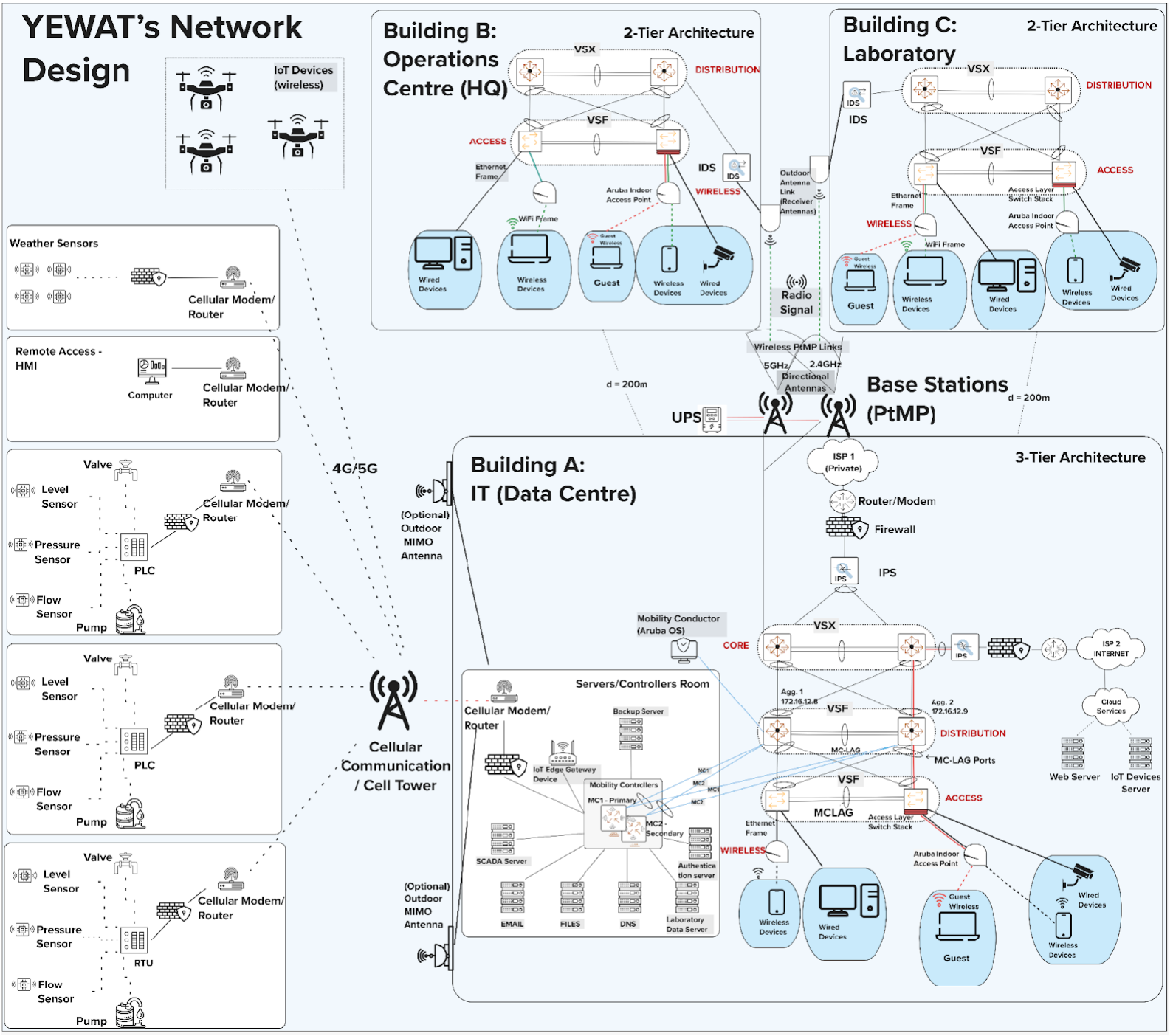
UNIVERSITY of York

Summative Assessment
Networks and Mobile Architecture

Created by: Christina Antonopoulou

Due to word limitations,all abbreviations are included in Appendix 2.

Task 1



Picture 1 Network Design

Introduction

The purpose of this design in Picture 1 and Appendix 1 is to create a robust and secure hybrid network for YEWAT integrating wired SCADA sensors, wireless IoT devices and drones, whilst ensuring reliable communication across buildings despite environmental challenges.

Internal Network Design

Small networks usually use a cost-effective flat design, where hubs and switches are connected in one direction and expand when required [1]. For mid-sized companies, like YEWAT, which has at least 100 workstations, Cisco recommends a collapsed core-distribution design [2], while Aruba suggests a three- tier design for connecting multiple buildings [3]. Considering the expansion of IoTs and IT building's (IT) role in supporting multiple buildings, a three-tier architecture was chosen. While the Laboratory (LAB) and Operations Centre (OC) will adopt a two-tier architecture. The core layer in IT was intentionally added to reduce complexity and allow network scalability as YEWAT grows [4].

IT supports 15 guest devices with internet only-access and 75 business and miscellaneous devices, both wireless and wired, with intranet and internet access. All on-premises servers are housed in the IT server room, which must meet specific requirements such as temperature and humidity sensors, airflow planning, fire suppression, redundant power sources, cable management, physical security, and circuit requirements [5]. Centralising all on-premises servers in a server room, simplifies maintenance, reduces complexity, and enhances security by minimizing unnecessary access risks.

The LAB and OC support 75 and 100 wired and wireless business and miscellaneous devices with intranet and internet access, respectively. Both buildings also support 10 guest devices.

Each building connects wireless clients through the internal access points (APs) to access layer switches. Devices connected on an AP form a BSS, whilst APs connected access switches form an ESS. Accessswitches provide access to the network by sending traffic to the upper distribution layers. They also are responsible for port security, VLAN segmentation, and QoS [6].

To determine the number of switches required for each building, the concept of

oversubscription was considered, and it was assumed that the number of devices will increase in the future. The oversubscription ratio for access ports on the access to distribution uplink is 20:1 and for the distribution to core, a ratio of 4:1 is used [7]. We assume each switch has at least 24 downlink ports and 4 uplink ports. It is also recommended that an AP should have a maximum of 30 clients, so each building will have 2 APs [8].

Oversubscription example:

IT supports 90 end devices (40% wired, 60% wireless).

Connections (2 APs + 36 wired) / $ports$ = 38 / 24 ≈ 2 access switches

If each access switch has 2 uplinks of 10Gbps each, the total bandwidth from the access layer is 40Gbps.

Oversubscription access to distribution = 40 / 20 = 2Gbps (20:1)

So, for 2 access switches we will require distribution switches that can handle 2Gbps. If one distribution switch has 2 uplinks of 10Gbps:

Oversubscription distribution to core = 20 / 40 = 5Gbps (4:1)

Overall, although we could use 1 distribution and core switch, for redundancy and load balancing, 2 core (for the IT) and 2 distribution switches are used.

The access switches connect to the distribution layer switches which handle the routing and aggregation of network traffic between subnets or VLANs [9]. Their role is crucial to the network, as they control and filter the traffic based on ACL, they control broadcast through VLANs, and they provide redundancy and load balancing [10].

Distribution and access layer switches form VSF pairs. VSF allows the management of each pair as a single entity providing redundancy, simplifying their management and offering performance improvement through the aggregation of resources [11].

The IT distribution switches (layer 2 and 3) connect to two core layer switches which serve as the backbone of the network offering traffic aggregation, high speed data forwarding, routing, redundancy and scalability [12]. The core layer in this design is responsible for the interconnection of the aggregation layer switches from all buildings and it forwards traffic to YEWAT's WAN routers, and firewalls.

Core switches form a VSX, which allows them to appear as a single device to their clients. If one of them fails, the other one takes over which increases resiliency and availability and removes the need for Spanning Tree Protocol making full use of the MC-LAG [11]. Load balancing and QoS capabilities are also supported [11]. VSX, compared to VSF offers better high availability functionality and is recommended for this layer [3]. OC and LAB have layer 3 VSX pairs [13].

Usually, networks employ STP (Layer 2), but this protocol creates two important issues; at minimum half of the available bandwidth is not used by data traffic, and network topology changes can affect it [14]. With the use of MC-LAG, clients create a logical LAG interface between two MC-LAG peers who appear as one device. Traffic is load balanced between two switches, increasing performance of the uplinks, removing the need for STP and improving recovery time [3]. This mechanism adds resilience and redundancy, as one switch can support if the other fails [3].

In IT, IPS are configured behind the firewalls [15] to monitor WLAN traffic and prevent malicious activity. IDS offers fundamental detection capabilities and alerts administrators when a malicious activity occurs [16]. Since IT hosts the core network, IPS is preferred for preventive measures, whereas IDS will be used as additional security for the other buildings.

The Aruba Mobility Conductor (MCR) is responsible for the management and configuration of APs, gateways and controllers, allowing network administrators to manage and monitor network performance from a single location [17]. The MCR manages the Aruba Mobility Controllers which support the management and control of access points centrally. They are responsible for routing (layer 3), switching (layer 2), and the enforcement of policies based on user role, device type, application and network location [18]. Security features are in place for complete encryption (GRE tunnels, firewalls, WPA3 compatibility, 802.1X) [18].

Two controllers have been placed in the IT server room for redundancy, to manage and direct incoming traffic from the distribution layer, IoT devices and SCADA. The controller forwards all requests to the authentication server, and traffic is directed to the servers or to YEWAT's LAN or WAN depending on access/destination host.

Two distinct ISPs are recommended for network segmentation. Sensitive data is directed to the first provider, while the second receives non-sensitive data (web, guest traffic, IoT devices data, etc.) [19]. Despite cost implications, having a backup ISP is considered essential for security concerns. In case of temporary unavailability, the second ISP ensures uninterrupted business continuity.

Outdoor Network Design

Assuming 200m line of sight between buildings, a PtMP WLAN bridge is chosen. The bridge uses a base station with bi-directional antennas that transmit RF signals to multiple nodes [20]. Industrial WLANs favour this method as it eliminates the need for physical cables [21]. The solution employs TP Link high gain antennas with amplifiers, supporting PtMP at 5GHz and 2.4GHz [22]. Two base stations ensure load balancing and continuous data flow, even if one fails. An outdoor UPS system is recommended to prevent network downtime during power outages [23].

The SCADA units send traffic to PLCs/RTUs which is then routed through a firewall and cellular modems to the IT's cellular modem. Mobility controllers then direct the SCADA traffic to the appropriate server. Additionally, a remote access control centre is included for troubleshooting and maintenance [24]. Cellular technology was chosen over radio due to better coverage provided by existing cellular infrastructure in the surrounding area and does not require clear line-of-sight [25]. Cellular also offers easier installation and has less interference issues [26]. It also offers great scalability especially if the company decides to move SCADAs to the cloud [27].

Finally, IoTs will rely on 4G communication, which provides fast and high volumes of data transfers with a good range over long distances [28]. Their data will be received by a 4G/5G router/modem device in the IT, with their data being forwarded from the edge device to the cloud. Satellite connection was a possible option; however, it is more expensive and usually for field drones 4G/5G network is used [28].

Considering future IoT growth, cellular is used because it offers great scalability and coverage over radio communication [25]. Optionally, MIMO antennas can be implemented to increase 4G signal strength.

IP Address Design

Utilisation of VLANs and subnets enable efficient routing and addressing as well as logical segmentation for enhanced security and role-based access control. Since YEWAT is a mid-sized business, Class B is preferred (172.16.0.0-172.31.255.255).

VLANs are chosen based on building-specific needs, such as management for network devices and admin for admins to access network devices in an isolated secure environment [29]. Although a default /24 could be assigned to all subnets, VLSM practices were instead chosen to avoid IP wastage and to optimise available address space [30].

Table 1 contains the high-level IP addressing, and a more detailed IP addressing can be found in Appendix 2.

Building	VLAN Name	Subnet	VLAN
IT	Wired Devices	172.16.3.0/26	30
	Wireless Devices	172.16.4.0/26	40
	Guests	172.16.9.0/27	99
	Management	172.16.0.0/27	10
	Admin	172.16.1.0/27	15
	Servers	172.16.2.0/28	20
LAB	Wired Devices	172.16.13.0/26	30
	Wireless Devices	172.16.15.0/26	40
	Guests	172.16.9.32/28	99
	Management	172.16.0.32/28	10
	Admin	172.16.1.32/28	15
OC	Wired Devices	172.16.23.0/26	30
	Wireless Devices	172.16.24.0/26	40
	Guests	172.16.9.48/28	99
	Management	172.16.0.48/28	10
	Admin	172.16.1.48/28	15
SCADA	SCADA	172.16.6.0/24	60
	Management	172.16.0.80/28	10

	Admin	172.16.1.80/28	15
IoT	IoT	172.16.5.0/25	50
	Management	172.16.0.64/28	10
	Admin	172.16.1.64/28	15

Table 1 IP Addressing

Network Protocols

Table 2 contains the most important protocols used in YEWAT's network design.

Type	Protocol	Description/Purpose	Example
Routing	OSPF	Finds shortest path in IP networks	Routing between the three-layer switches
	BGP	Determines best routes for internet data transmission	Routing with ISPs
Addressing	IPv4/IPv6	Provides IP addresses for internet communication, IPv6 future proof	Addressing for a device 192.168.10.2
Dynamic Addressing	DHCP	Dynamically assigns IPs to network devices	New devices connected to the network
Network Layer	ICMP	Used for network diagnostics like ping, traceroute commands (reference)	Network admin checks network using "ping"
Security	RADIUS	Centralised authentication, authorisation, and accounting	Authenticates users, assigns roles and VLANs
	SSH	Secure remote access to devices	Admin configures switches remotely

	SSL/TLS	Secure communication over the network	Enforced for accessing cloud-based applications (e.g., HTTPS)
	IPSec	Encrypts data for site-to-site VPN connections	Between two buildings connecting LANs
	WPA3-Enteprise	Uses 802.1X standard for wireless security	Secures data transmission over the network
Management	SNMP	Monitors network devices	Switches and routers monitoring
	NTP	Clock synchronisation across network devices	Validates timestamps for accurate logs
Transport Layer / Communication	TCP	Reliable transmission protocol	Used for HTTP/s and other application protocols
	UDP	Less reliable, used for VoIP traffic	Video calls
	S/FTP	File transfer between devices	Users accessing files from the file server
	HTTP/S	Application/browser communication with servers	User accessing a URL
	SMTP/POP3S	Secure email communication	Users receiving/sending emails
	DNP3	Used between centrally located servers and distributed sensors	Communication between SCADA master and RTU
Other	ARP	Layer 2, maps IPs to MAC addresses	Two devices send frames to each other using MAC addresses
	ICCP	MC-LAG peer connectivity	Connectivity between two distribution switches
	CSMA/CA	Wireless data transmissions and collision management	A device checks if the channel is free before transmission

	DNS	Layer 7, IP address to human-readable name conversion	Google.com translates to 216.58.213.14
	4G/5G	Mobile communication [31]	Drone sending data to IoT Gateway

Table 2 Protocols

Task 2

2.1 Analysis of potential devices and methods to increase signal strength.

PtMP: To address signal strength issues, directional antennas, which have higher gains and focus on a single direction were chosen over omnidirectional to reduce signal interference from all directions [32]. These antennas are compatible with 802.11ax [33] and use TDMA [34] for efficient time slot management. It is recommended to use high gain antennas with powerful amplifiers to ensure reliable signal reach. For load balancing and redundancy, two antennas operating at different frequencies (5GHz and 2.4 GHz) are proposed. If one antenna fails, devices will continue to transmit through the other frequency, ensuring smooth network operation. For multiple remote locations PtMP is the best option [35].

To address interference due to weather conditions, it is recommended to install in each antenna a radome to protect them and reduce degradation [36]. It is also recommended to use spectrum analysers to identify any sources that can disrupt RF signals, so the issue can be addressed [36].

PtP WLAN bridge: Similar to PtMP, but with antennas or access points forming point to point connections [20].. Communication relies on the internal antennas of the APs, and although a viable option it would increase management complexity and load balancing wouldn't be as effective as with the PtMP. PtP's usually preferred when you have to connect two buildings [20].

WLAN Mesh: Similar to WDS, mesh is a non-hierarchical model where devices are linked together and appear as a single network. This type is recommended for temporary indoor or outdoor networks, where cabling isn't possible [37]. Most likely in YEWAT's case its implementation would be an expensive and complicated option [38], and it would increase the probability of duplicate connection risks and latency problems that could affect YEWAT's network

reliability [39].

Range Extenders/Repeaters: It is a recommended option for small-sized businesses that require signal boost within the building or different floors [40-41]. In our case this would not be helpful as there are multiple obstructions such as walls, distance etc. that could affect signal strength and we need to create reliable network connections between multiple buildings.

2.2 IoT & Network Resilience

IoT wireless technology is becoming increasingly popular to businesses, offering various wireless solutions [42], some of which are discussed below:

LoRaWAN is best suited for infrequent data transactions with low bandwidth [68] where security and encryption are not critical [43].

LPWAN is a low-cost unlicensed solution for IoTs, that allows customisation, but it is less reliable compared to cellular [44].

WiFi, although a widely used solution, it has limitations in scalability, security and coverage. FBI recommends that IoT devices should be connected on a separate network for security purposes [45]. Since the number of IoT devices in YEWAT is expected to increase, an alternative that would mitigate these issues and speed up the development time is cellular networks [46].

Disruptions in network connectivity are common [47]. Cellular solutions offer reliability, availability, and scalability due to their widespread deployment and existing infrastructure [48]. For the IoTs with critical tasks, an “Ultra-High-Availability-SIM” design continuously monitors the network. If a connection issue occurs, it switches to profile switch SIM 2, ensuring business continuity [49].

For future IoT devices requiring higher bandwidth and lower latency, a 5G cellular network can be implemented. However, not all devices can transition to 5G due to higher costs, and some do not require such high bandwidth [50].

Task 3

YEWAT's transition to wireless SCADA, while cost-effective [51], investment and actions must be taken to ensure cyber security measures are in place. H. Kim [52] points out that SCADA were not designed with security, and whilst threat actors had to make physical contact with the analog circuits nowadays with the transition to wireless, the attack surface is increased, and remote cyber-threats are more imminent.

Similarly, as the use of IoT devices grows, so does the possible vulnerability to attacks by malicious actors. A relevant example is the Mirai Botnet attack [53]. By hijacking IoT devices, intruders can use them as a gateway for launching cyber-attacks in the wider business network [54]. Common IoT security issues include unencrypted traffic, weak default passwords, lack of updates, and physical security [55 - 58].

Frequent cyber-attacks on IoTs and SCADA are firmware exploits, credential-based attacks, on-path attacks, DoS, man-in-the-middle attacks, MQTT and DNS Hijacking, PLCs Firmware vulnerabilities, SMS Brute-Force attack, and physical hardware-based attacks [55], [58].

A potential IoT cyberattack could impact data integrity, compromise environment-based monitoring and decisions, or provide access to the wider business network. Whereas a breach on the SCADA systems, could raise public safety and environmental concerns, and may have economic and national security implications [56].

YEWAT is ethically responsible for customer data and health protection (Data Protection Act 2018, Water Industry Act 1991 & Civil Contingencies Act 2004). Any compromise could endanger public health, cause reputational damage, financial loss, trigger lawsuits, and disrupt operations [56], [59-60]. Failure to implement security measures could result in sanctions and significant fines (Network and Information Systems (NIS) Regulations 2018) [60]. It's YEWAT's ethical responsibility to balance security requirements with social responsibility [61].

For the security of YEWAT's IoTs and SCADA, the following actions and best practices are recommended [55-58], [62-64]:

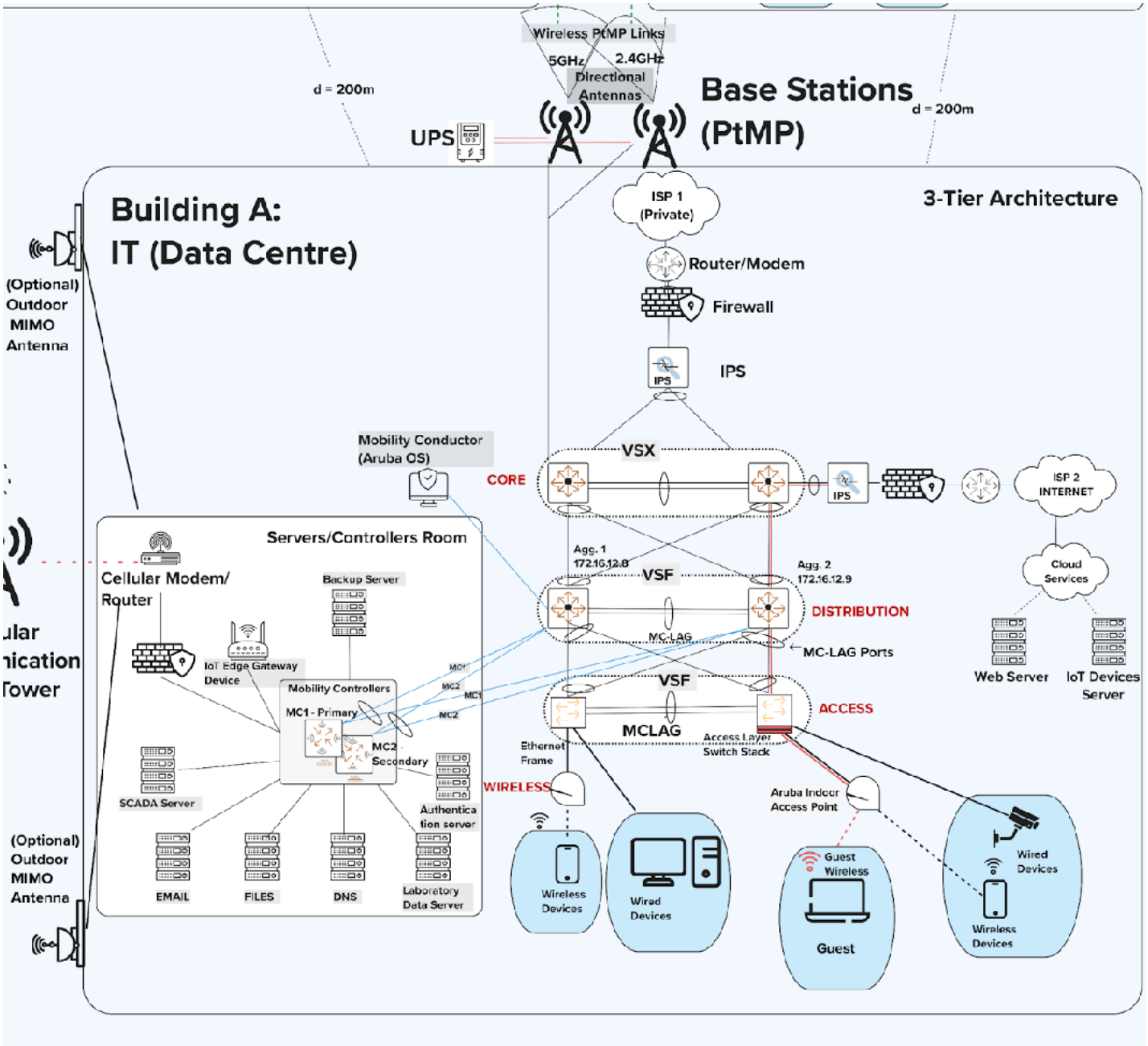
1. Assess cyber health and identify all managed and unmanaged devices.

2. Implement IoT/SCADA Security measures.
3. Perform regular risk assessments.
4. Plan for emergencies and cyberattacks.
5. Update all IoT/SCADA Credentials, automate zero-trust policies, implement multi-factor authentication and encryption to avoid credential and on-path attacks.
6. To avoid MQTT hijacking, MQTTS with username, password and certificate pinning must be used.
7. To avoid DNS hijacking, network monitoring, encryption and certificate pinning must be used.
8. To avoid SMS brute-force attack, plastic cards that hold the SIMs must not be disposed, SMS passwords must be reset and “trusted phone numbers” must be implemented.
9. To protect the PLCs, encrypted VPN must be used, and their firmware must be updated.
10. Regularly update all devices and sensors with the correct firmware, to avoid firmware vulnerable exploits.
11. Enforce physical security to IoTs/SCADAs, to avoid physical hardware-based attacks.
12. Assign unique device identities and use authentication to avoid man-in-the-middle attacks.
13. Improve incident response, manage third parties and the wider supply chain.
14. Increase awareness among personnel who are responsible for managing IoT/SCADA devices.
15. Complete annual self-assessments and present them to DEFRA.
16. Share threat intelligence with DEFRA and NCSC.
17. Develop and test response plans.
18. Comply with any industry-specific security regulations.

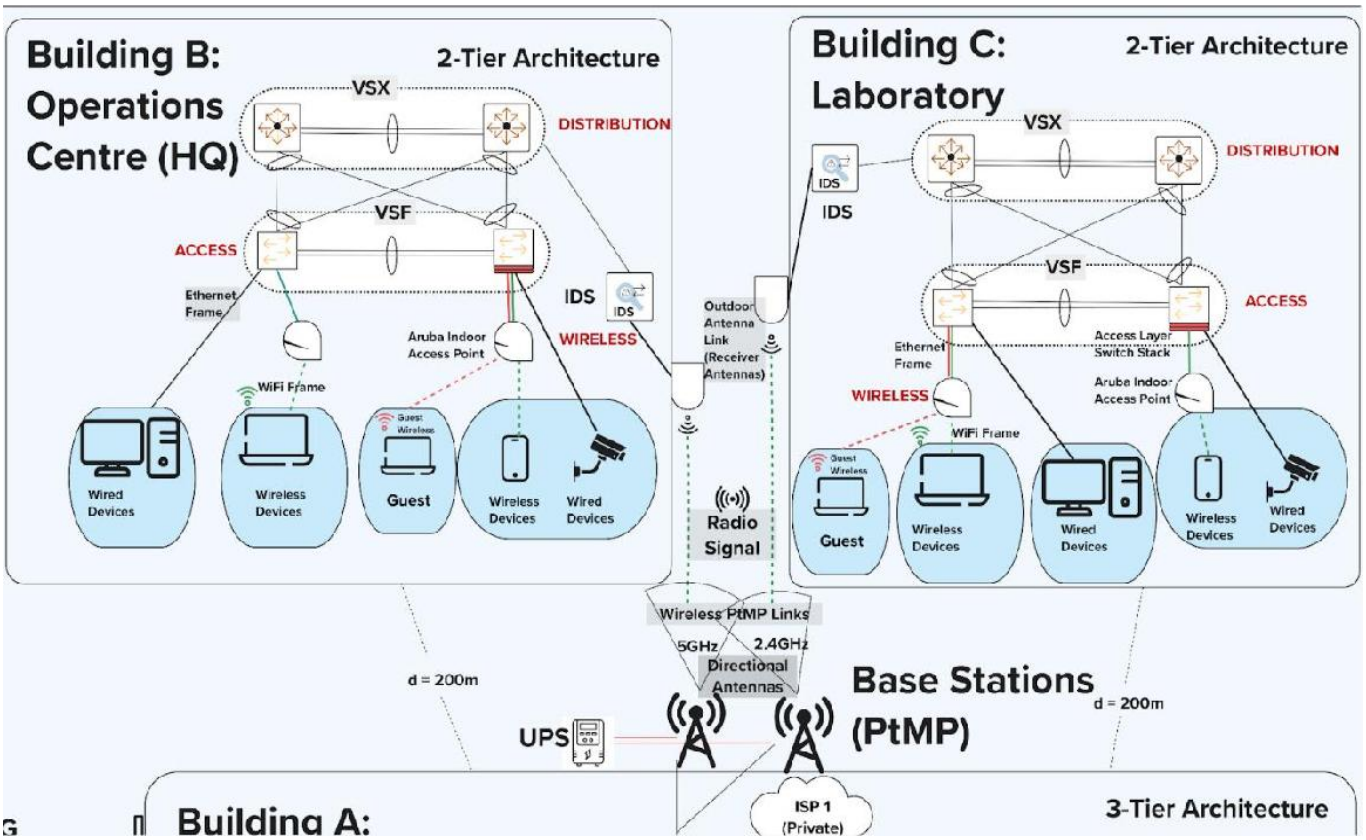
Appendices

Appendix 1

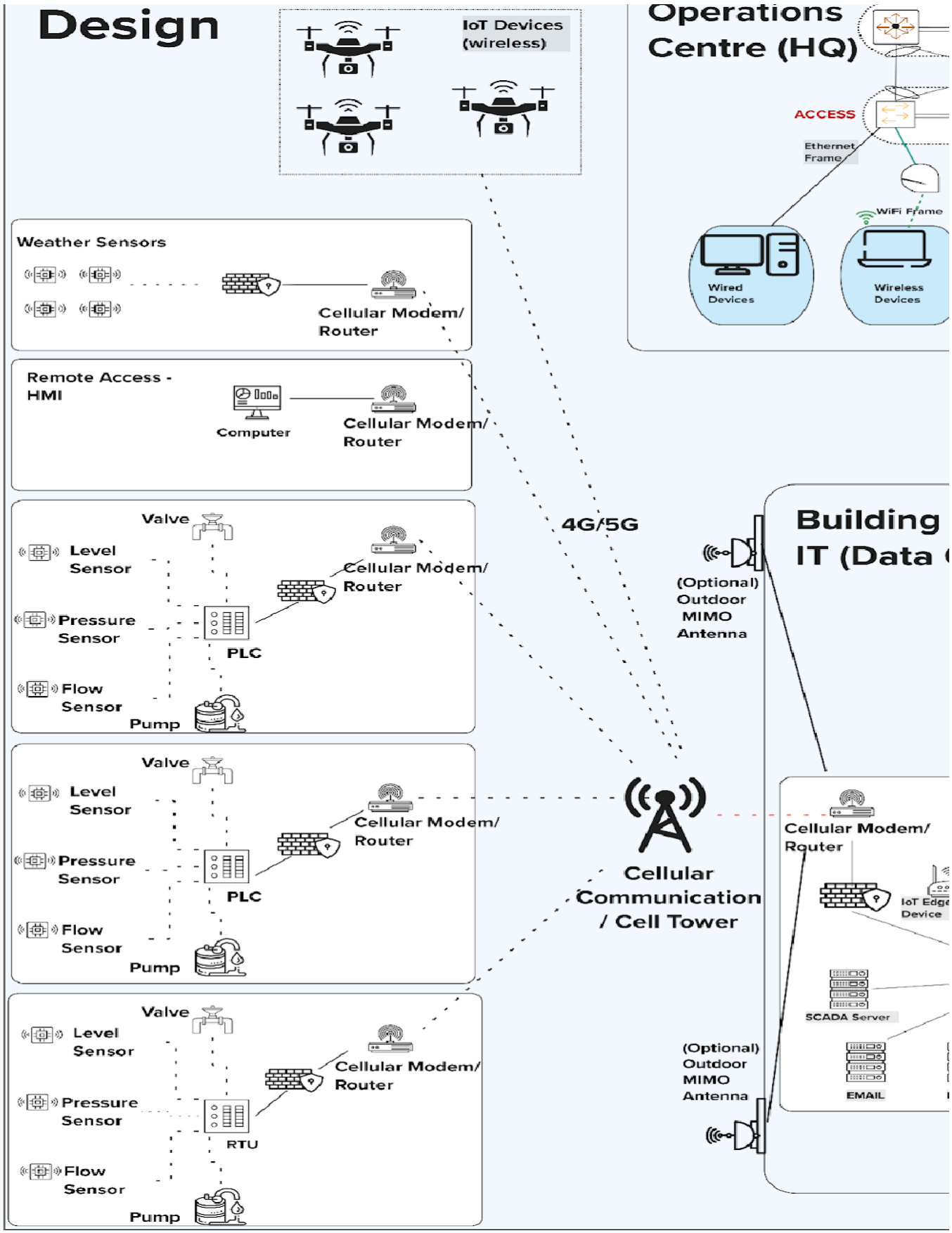
IT Building:



Laboratory and Operations Centre:



IoTs and SCADA:



Appendix 2

Building / Area	VLAN Name	VLAN ID	Subnet	Subnet Mask	Network Address / Broadcast	First / Last IP Address	No. Total Addresses	No. Used Addresses
IT	Management	10	172.16.0.0/**27**	255.255.255.224	172.16.0.0 / 172.16.0.31	172.16.0.1 / 172.16.0.30	32	30
	Admin	15	172.16.1.0/**27**	255.255.255.224	172.16.1.0 / 172.16.1.31	172.16.1.1 / 172.16.1.30	32	30
	Servers	20	172.16.2.0/**28**	255.255.255.240	172.16.2.0 / 172.16.2.15	172.16.2.1 / 172.16.2.14	16	14
	Wired Devices	30	172.16.3.0/**26**	255.255.255.192	172.16.3.0 / 172.16.3.63	172.16.3.1 / 172.16.3.62	64	62
	Wireless Devices	40	172.16.4.0/**26**	255.255.255.192	172.16.4.0 / 172.16.4.63	172.16.4.1 / 172.16.4.62	64	62
	Guests Devices	99	172.16.9.0/**27**	255.255.255.224	172.16.9.0 / 172.16.9.31	172.16.9.1 / 172.16.9.30	32	30
LAB	Management	10	172.16.0.32/**28**	255.255.255.240	172.16.0.32 / 172.16.0.47	172.16.0.33 / 172.16.0.46	16	14
	Admin	15	172.16.1.32/**28**	255.255.255.240	172.16.1.32 / 172.16.1.47	172.16.1.33 / 172.16.1.46	16	14
	Wired devices	30	172.16.13.0/**26**	255.255.255.192	172.16.13.0 / 172.16.13.63	172.16.13.1 / 172.16.13.62	64	62
	Wireless Devices	40	172.16.15.0/**26**	255.255.255.192	172.16.14.0 / 172.16.14.63	172.16.14.1 / 172.16.14.62	64	62
	Guests Devices	99	172.16.9.32/**28**	255.255.255.240	172.16.9.32 / 172.16.9.47	172.16.9.33 / 172.16.9.46	16	14
OC	Management	10	172.16.0.48/**28**	255.255.255.240	172.16.0.48 / 172.16.0.63	172.16.0.49 / 172.16.0.62	16	14

	Admin	15	172.16.1.48 /**28**	255.255.255.240	172.16.1.48 / 172.16.1.63	172.16.1.49 / 172.16.1.62	16	14
	Wired Devices	30	172.16.23.0 /**26**	255.255.255.192	172.16.23.0 / 172.16.23.63	172.16.23.1 / 172.16.23.62	64	62
	Wireless Devices	40	172.16.24.0 /**26**	255.255.255.192	172.16.24.0 / 172.16.24.63	172.16.24.1 / 172.16.24.62	64	62
	Guests	99	172.16.9.48 /**28**	255.255.255.240	172.16.9.48 / 172.16.9.63	172.16.9.49 / 172.16.9.62	16	14
IoT	Management	10	172.16.0.64 /**28**	255.255.255.240	172.16.0.64 / 172.16.0.79	172.16.0.65 / 172.16.0.78	16	14
	Admin	15	172.16.1.64 /**28**	255.255.255.240	172.16.1.64 / 172.16.1.79	172.16.1.65 / 172.16.1.78	16	14
	IoT Devices	50	172.16.5.0/ **25**	255.255.255.128	172.16.5.0 / 172.16.5.127	172.16.5.1 / 172.16.5.126	128	126
SCADA	Management	10	172.16.0.80 /**28**	255.255.255.240	172.16.0.80 / 172.16.0.95	172.16.0.81 / 172.16.0.94	16	14
	Admin	15	172.16.1.80 /**28**	255.255.255.240	172.16.1.80 / 172.16.1.95	172.16.1.81 / 172.16.1.94	16	14
	SCADA Devices	60	172.16.6.0/ **24**	255.255.255.	172.16.6.0 / 172.16.6.255	172.16.6.1 / 172.16.6.254	256	254

Appendix 3

The table below contains all the abbreviations mentioned in this report.

Abbreviation	Expanded Name
SCADA	Supervisory Control and Data Acquisition
AP	Access Point
BSS	Basic Service Set
ESS	Extended Service Set
VLAN	Virtual Local Area Network
QoS	Quality of Service
Gbps	Gigabits per Second
ACL	Access Control List
VSF	Virtual Switching Framework
VSX	Virtual Switching Extension
MC-LAG	Multi-Chassis Link Aggregation Group
STP	Spanning Tree Protocol
WLAN	Wireless Local Area Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
GRE tunnel	Generic Routing Encapsulation tunnel
WPA3	Wi-Fi Protected Access 3
MCR	Aruba Mobility Conductor
LAN	Local Area Network
WAN	Wide Area Network
PtMP	Point to Multipoint
GHz	Gigahertz
UPS	Uninterruptible Power Supply
PCL/RTU	Programmable Logic Controller/Remote Terminal Unit
IoT	Internet of Things
MIMO	Multiple-Input Multiple-Output
TDMA	Time Division Multiple Access
PtP	Point to Point
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
WiFi	Wireless Fidelity
MQTT	Message Queuing Telemetry Transport
DNS	Domain Name System
VPN	Virtual Private Network
Defra	Department for Environment, Food and Rural Affairs
NCSC	National Cyber Security Centre

REFERENCES

[1] J. Paul, “Explore hierarchical networks: Access, distribution, core layers,” Knowledge, 09-Dec-2023. [Online]. Available:

[2] “CCDE Study Guide: Enterprise Campus Architecture Design,” Ciscopress.com. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2448489. [Accessed: 14-Jun-2024].

[3] Arubanetworks.com. [Online]. Available: https://www.arubanetworks.com/assets/tg/AVD_Midsize-Campus-Design-Deploy.pdf. [Accessed: 14-Jun- 2024].

[4] “Enterprise campus 3.0 architecture: Overview and framework,” Cisco, 02-May-2021. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html. [Accessed: 14-Jun-2024].

[5] Racksolutions.co.uk. [Online]. Available: https://www.racksolutions.co.uk/news/blog/server-room-explained/. [Accessed: 14-Jun-2024].

[6] J. Paul, “Choose access layer switch for the access layer network,” Knowledge, 10-Jan-2020. [Online]. Available: https://community.fs.com/article/how-to-choose-the-right-access-layer-switch.html. [Accessed: 14-Jun-2024].

[7] “Designing Cisco Enterprise Campus Architecture models,” Ciscopress.com. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=1315434&seqNum=3. [Accessed: 14-Jun-2024].

[8] D. Cook, “How to determine maximum clients per access point,” *Linkedin.com*, 03-Feb-2022. [Online]. Available: https://www.linkedin.com/pulse/how-determine-maximum-clients-per-access-point-don-cook/. [Accessed: 23-Jun-2024].

[9] “The ultimate introduction to distribution switch,” Qsfptek.com. [Online]. Available: https://www.qsfptek.com/qt-news/the-ultimate-introduction-to-distribution-switch.html. [Accessed: 14- Jun-2024].

[10] “Access, distribution, and core layers explained,” ComputerNetworkingNotes, 04-May-2021. [Online]. Available: https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution- and-core-layers-explained.html. [Accessed: 14-Jun-2024].

[11] “A closer look: Aruba VSF vs Aruba VSX,” The Network DNA. [Online]. Available: https://www.thenetworkdna.com/2023/11/a-closer-look-aruba-vsf-vs-aruba-vsx.html. [Accessed: 14-Jun-2024].

[12] “What is Core Switch and How to Choose-QSFPTEK,” Qsfptek.com. [Online]. Available: https://www.qsfptek.com/qt-news/what-is-core-switch-and-how-to-choose. [Accessed: 14-Jun-2024].

[13] VSF versus VSX. (n.d.). Arubanetworks.com. Retrieved June 23, 2024, from https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7727/Content/Chp_getsta/VSX_sol_top_ovw/vsf-ver-vsx-10.htm

[14] “Introduction to OSPF,” Juniper.net. [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos/ospf/topics/topic-map/ospf-overview.html. [Accessed: 14-Jun-2024].

[15] “What is an Intrusion Prevention System (IPS)?,” Ibm.com, 14-Feb-2024. [Online]. Available: https://www.ibm.com/topics/intrusion-prevention-system. [Accessed: 14-Jun-2024].

[16] H. Ashtari, “IDS vs. IPS: Key difference and similarities,” Spiceworks Inc, 21-Mar-2022. [Online]. Available: https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/. [Accessed: 14- Jun-2024].

[17] Arubanetworks.com. [Online]. Available: https://www.arubanetworks.com/assets/ds/DS_MobilityConductor.pdf. [Accessed: 14-Jun-2024].

[18] Arubanetworks.com. [Online]. Available: https://www.arubanetworks.com/assets/ds/DS_VMC.pdf. [Accessed: 14-Jun-2024].

[19] "Why businesses need a secondary ISP to prevent connection problems," Copperband Tech, 21-Sep-2020. [Online]. Available: https://copperbandtech.com/why-businesses-need-a-secondary-isp-to-prevent-connection-problems/. [Accessed: 14-Jun-2024].

[20] D. D. Coleman and D. A. Westcott, Cwna: Certified wireless network administrator official study guide, 3E (exam Pw0-105), 3rd ed. Nashville, TN: John Wiley & Sons, 2012.

[21] H. Martel, "Wireless bridges vs wireless access points: How they work and where to deploy them," New Equipment Digest, 18-Sep-2023. [Online]. Available: https://www.newequipment.com/learning-center/article/21273835/wireless-bridges-vs-wireless-access-points-how-they-work-and-where-to-deploy-them. [Accessed: 20-Jun-2024].

[22] "TP-link," TP-Link. [Online]. Available: https://www.tp-link.com/my/business-networking/pharos-cpe/wbs510/. [Accessed: 20-Jun-2024].

[23] *Uninterruptible Power Supply*. (n.d.). Efoy-pro.com. Retrieved June 23, 2024, from https://www.efoy-pro.com/en/applications/telekommunikation/

[24] "SCADA systems," Inst Tools, 04-Aug-2020. [Online]. Available: https://instrumentationtools.com/scada-systems/. [Accessed: 15-Jun-2024].

[25] GEORGE C. POLYZOS, GEORGE XYLOMENOS, in Multimedia Communications. (n.d.). *Cellular Infrastructure*. Sciencedirect.com. Retrieved June 23, 2024, from https://www.sciencedirect.com/topics/engineering/cellular-infrastructure

[26] Chelsea. (2016, January 19). *Wireless communication for your SCADA system:Radio vs cellular vs satellite*. Scadata. https://scadata.net/wireless-communication-radio-cellular-satellite/

[27] Weinberg, A. (2021, March 21). *SCADA security in a cellular world*. FirstPoint. https://www.firstpoint-mg.com/blog/scada-security-in-a-cellular-world/

[28] Anjel, “Unlocking the sky: Cellular connectivity for commercial drones,” Webbing, 18-Feb-2024. [Online]. Available: https://webbingsolutions.com/unlocking-the-sky-cellular-connectivity-for-commercial-drones/. [Accessed: 17-Jun-2024].

[29] CISCO. (n.d.). *VLANAccess Control Lists*. Cisco.com. Retrieved June 23, 2024, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-2_5_e/configuration_guide/b_1525e_consolidated_2960x_cg/b_1525e_consolidated_2960x_cg_chapter_0110110.pdf

[30] H. Cardenas, “Difference between CIDR and VLSM,” *Linkedin.com*, 12-Sep-2023. [Online]. Available: https://www.linkedin.com/pulse/difference-between-cidr-vlsm-hector-cardenas/. [Accessed: 23-Jun- 2024].

[31] Mobile Communications, “What is the most effective mobile communication protocol for your use case?,” *Linkedin.com*, 19-Sep-2023. [Online]. Available: https://www.linkedin.com/advice/3/what-most-effective-mobile-communication-2c. [Accessed: 23-Jun-2024].

[32] S. Shock, “Want to end the great debate. Directional vs omnidirectional antennas?,” Novotech Technologies, 29-Mar-2023. [Online]. Available: https://novotech.com/learn/m2m-blog/blog/2023/03/29/want-to-end-the-great-debate-directional-vs-omnidirectional-antennas/. [Accessed: 20-Jun-2024].

[33] M. Chotalia and S. Gajjar, “Performance Comparison of IEEE 802.11ax, 802.11ac and 802.11n Using Network Simulator NS3,” in *Communications in Computer and Information Science*, Cham: Springer Nature Switzerland, 2023, pp. 191–203.

[34] S. Atmaca, C. Ceken, and I. Erturk, “Improving wireless TDMA/FDD MAC performance with multi-beam directional antennas,” *Iaeng.org*. [Online]. Available: https://www.iaeng.org/publication/WCECS2007/WCECS2007_pp353-358.pdf. [Accessed: 23-Jun-2024].

[35] “Point to Point & Multipoint Radio systems,” CSE Crosscom, 31-Oct-2023. [Online]. Available: https://csecrosscom.net/solutions/communications/linking-and-backhaul/point-to-point-multipoint-radio-systems/. [Accessed: 20-Jun-2024].

[36] “Intermittent connectivity issues in wireless bridges,” Cisco, 23-Jul-2021. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/wireless/aironet-antennas-accessories/66090-intermittent-wireless-bridges.html. [Accessed: 20-Jun-2024].

[37] E. Geier, “Wi-Fi Mesh: What to know about enterprise mesh networks,” Network World, 08-Jan-2019. [Online]. Available: https://www.networkworld.com/article/966846/wi-fi-mesh-what-to-know- about-enterprise-mesh-networks.html. [Accessed: 20-Jun-2024].

[38] “Mesh Topology Advantages and Disadvantages,” www.javatpoint.com. [Online]. Available: https://www.javatpoint.com/mesh-topology-advantages-and-disadvantages. [Accessed: 14-Jun-2024].

[39]“A Guide to Mesh Topology. Definition, Practices, and importance - zenarmor.com,” Zenarmor.com. [Online]. Available: https://www.zenarmor.com/docs/network-basics/what-is-mesh-topology. [Accessed: 19-Jun-2024]

[40] “Repeater vs access point,” Beambox.com, 17-Feb-2023.

[41] J. Etherington, “WiFi boosters: The key to seamless business operations,” Yourcommsgroup.com. [Online]. Available: https://www.yourcommsgroup.com/news/wifi-booster-business. [Accessed: 17-Jun-2024].

[42]F. Greer, “6 types of wireless IoT technology,” *Zipitwireless.com*, 19-Jun-2023.

[43] “Exploring IoT connectivity: Comparing cellular and LoRaWAN,” *1oT*. [Online]. Available: https://1ot.com/resources/blog/comparing-cellular-and-lorawan. [Accessed: 23-Jun-2024].

[44]Venture Insights, “IoT connectivity technologies: Cellular or LPWAN?,” *IoT For All*, 14-Nov-2018. [Online]. Available: https://www.iotforall.com/iot-connectivity-cellular-vs-lpwan. [Accessed: 23-Jun-2024].

[45]F. B. I. Portland, “Tech Tuesday: Internet of Things (IoT),” *Fbi.gov*, 03-Dec-2019. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of- things-iot. [Accessed: 23-Jun-2024].

[46] “Cellular vs WiFi for IoT: Choosing the best connectivity option,” *Eseye*, 19-Feb-2024. [Online]. Available: https://www.eseye.com/resources/iot-explained/cellular-vs-wifi-for-iot-choosing-the-best-connectivity-option/. [Accessed: 23-Jun-2024].

[47] H. Cardenas, “Network connectivity issues are leading cause of IT service outages,” *Linkedin.com*, 05-Apr-2024. [Online]. Available: https://www.linkedin.com/pulse/network-connectivity-issues-leading- cause-service-outages-cardenas-wpefc/. [Accessed: 23-Jun-2024].

[48] G. Manganaro and D. Leenaerts, “Wireless Infrastructure,” in *Advances in Analog and RF IC Design for Wireless Communication Systems*, Elsevier, 2013, pp. 1–6.

[49] Wirelesslogic, “Ultra High Availability,” *Wirelesslogic.com*. [Online]. Available: https://www.wirelesslogic.com/wp-content/uploads/2022/05/Wireless-Logic-Ultra-High-Availability-Solutions.pdf. [Accessed: 23-Jun-2024].

[50] N. Carter, “What is the better option for IoT connectivity, 4G or 5G?,” Linkedin.com, 02-May-2024. [Online]. Available: https://www.linkedin.com/pulse/what-better-option-iot-connectivity-4g-5g-neil- carter-mdlzc/. [Accessed: 23-Jun-2024].

[51] E. Kadaj, “SCADA & remote monitoring: The advantages of implementing wireless I/O,” Water Technology, 01-Nov-2007. [Online]. Available: https://www.watertechonline.com/home/article/14171211/scada-remote-monitoring-the-advantages-of-implementing-wireless-i-o. [Accessed: 18-Jun-2024].

[52] H. Kim, “Security and vulnerability of SCADA systems over IP-based wireless sensor networks,” Int. J. Distrib. Sens. Netw., vol. 8, no. 11, p. 268478, 2012.

[53] Cloudflare.com. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/glossary/mirai-botnet/. [Accessed: 18-Jun-2024].

[54] “IoT: The Internet of Things as a gateway for cyber attacks,” *itsa365*. [Online]. Available: https://www.itsa365.de/en/news-knowledge/2022/industry-news/iot-internet-of-things-as-gateway-for- cyber-attacks. [Accessed: 23-Jun-2024].

[55]D. Illing, “Common cyber-attacks in the IoT,” GlobalSign, 28-Feb-2023. [Online]. Available: https://www.globalsign.com/en/blog/common-cyber-attacks-in-the-iot. [Accessed: 18-Jun-2024].

[56] “Safeguarding the environment: Cybersecurity in environmental protection,” Cybersecurity Guide, 23-Oct-2020. [Online]. Available: https://cybersecurityguide.org/industries/environmental-protection/. [Accessed: 18-Jun-2024].

[57] P. Kaspian, “Zero Trust for infrastructure: A key step in addressing IoT security risks,” Palo Alto Networks Blog, 14-Jan-2022.

[58] Cloudflare.com. [Online]. Available: https://www.cloudflare.com/en-gb/learning/security/glossary/iot-security/. [Accessed: 18-Jun-2024].

[59] “Impact of cyber attack on your business,” Nibusinessinfo.co.uk. [Online]. Available: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business. [Accessed: 18-Jun-2024].

[60] J. Timmons and F. Paul Pittman, “Cybersecurity and the UK legal landscape,” Whitecase.com. [Online]. Available: https://www.whitecase.com/insight-alert/cybersecurity-and-uk-legal-landscape. [Accessed: 18-Jun-2024].

[61] P. Formosa, M. Wilson, and D. Richards, “A principlist framework for cybersecurity ethics,” Comput. Secur., vol. 109, no. 102382, p. 102382, 2021.

[62]“Security issues of IoT: Securing your IoT device in 2023,” Device Authority, 18-Sep-2023. [Online]. Available: https://deviceauthority.com/security-issues-of-iot-securing-your-iot-device-in-2023/. [Accessed: 18-Jun-2024].

[63] U. K. Water, “CYBER SECURITY PRINCIPLES FOR THE WATER INDUSTRY A report from the Water UK Cyber Security Good Practice Group,” Jan. 2016.

[64] Philippe Z Lin, Charles Perine, Rainer Vosseler Wen-Ya Lin, “Attacks From 4G/5G Core Networks Risks of the Industrial IoT in Compromised Campus Networks,” 2021. Available: https://documents.trendmicro.com/assets/white_papers/wp-attacks-from-4G-5G-core-networks.pdf [Accessed: 23-Jun-2024].