University of York

Department of Computer Science

Network Design for YEWAT - A Water Treatment Company

Including discussions around connectivity between the buildings, network resilience and security

Word Count: 2994 (including all text shown in tables)

23rd June 2024

Contents

1 Network Design

The OSI and TCP/IP models standardise the connection of devices, allowing them to communicate on networks[1][2]. Devices required to perform certain operations will automatically operate at the appropriate layer of each model. For example, a router works at the Network Layer of the OSI model, and at the Internet Layer in the TCP/IP model[3][4].

This report mainly concerns itself with the Physical, Data Link and Network layers in the OSI model[5]. The remaining layers are implemented in software within applications and operating systems[6].

Scalability and evolution of network design should also be considered[7]. Cost also seems to be a concern with YEWAT not wishing to pay to connect buildings with cables.

1.1 Protocols

Overall, across all layers, major protocols to which it is assumed systems adhere are listed below:

- Transmission Control Protocol (TCP) which arranges packets in order so that they can be delivered via Internet Protocol (IP)[8].
- IPv4 and IPv6 which send internet packets to the correct locations based on their addresses[9][10].
- Address Resolution Protocol (ARP) for translating IP addresses into MAC addresses[11].
- Border Gateway Protocol (BGP) which controls connections of endpoints on a Local Area Network (LAN) and over the internet[12].
- Dynamic Host Configuration (DHCP) Protocol which assigns an IP address to a device on a network[13].
- Remote Procedure Call (RPC) which allows one program to request the service of another[14].
- Multipurpose Internet Mail Extension (MIME) which allows users to exchange files (e.g. multimedia) via email[15].
- Hypertext Transfer Protocol (HTTP) which helps provide access to websites for users[16].
- Simple Mail Transfer Protocol (SMTP) for sending email messages[17].
- Domain Name System (DNS) for associating a website to an IP address[18][19].
- IPsec which adds encryption and authentication to IP[20].
- Transport Layer Security (TLS) which creates privacy and provides data integrity for internet communications[21].

- Subnetting protocol used for creating logically separate sections of a network[22].

1.2 Component choices

In the physical layer, the cost and capability of cables was considered. Ethernet (IEEE Standard 802.3-2022[23]) is by far the most popular choice in wired LAN networks[6], so Ethernet cables were selected. Cat 6a cables (standard ANSI/TIA-568.0-E[24]) were chosen as these provide speeds of up to 10Gbps and do not cost much more than slower cables[25]. Also. organisations will prefer to use more future-proof cables[6]. Cat 7 cables, conforming to BS ISO/IEC 14165-151:2017[26] were considered (capable of 40Gbps for not significantly more money[25]). However, they use a different connector (GG45)[25] and are not IEEE standard[27]. Also, some switches in do not support 40Gbps[28], so ultimately, Cat 7 cables were rejected. Cat 8 cables (ISO/IEC 11801-1:2017[29]) were rejected due to their expense[25]. However, if cost was not a consideration as previously noted, Cat 8 cables would be recommended for their speed capabilities[25].

In the Link layer, switches are used. These are better than using a broadcast link such as a hub because a switch will eliminate collisions; allow for transmission of data at different speeds; and can manage faults on the network[6]. These switches are configured to use store-and-forward switching because this will then also perform cyclic redundancy error checking before forwarding the frames[30]. Whilst this is slower than the cut-through switching method[30], it ensures that error checking takes place (complying with requirements of the link layer[5]).

Appendices A-C show switches at various points within each building. Different types of switches were considered for each subnetwork and at each tier, including a Cisco Catalyst 9300 series for tier 1 capable of providing 40Gbps[31][28]. However, this was rejected because the Cat 6a cables cannot achieve that speed. Therefore the cost was unjustified[32]. Ultimately D-Link's DXS-1210-12SC was selected for tier 1 switches for its number of ports and 10Gbps speed[33].

For tier 2 switches in internal subnets, groups of 5 computers are connected to Zyxel MG-108 switches[34]. This switch is unmanaged meaning it is plug-and-play, has a speed of 2.5Gbps, is relatively inexpensive[28][35] and will allow for extra computers (or potentially wireless access points) to be added. However, security implications should be considered carefully if wireless access points were added because wireless communication is more vulnerable to attacks than wired communication[36].

For the wireless connection between buildings (also at the data link layer), TP-Link's CPE710 wireless bridge (capable of 867Mbps) was chosen[37]. Whilst this speed is slower than that of the selected cables and would thus be a potential bottleneck, it is faster than some other bridges considered[38][39][40]. Bridges with higher speeds exist, but these require Radio Frequency line of sight. This means there needs to be a 10 degree zone measured out from the transmitter (called the Frensel zone) in which there can be no obstructions[41]. It is assumed this is not possible at YEWAT, however if it is possible, speeds to match the cable speed of 10Gbps could be achievable[41]. Using a laser link was ruled out because of the concern over weather conditions interfering with the signal[41].

It is assumed the SCADA sensors conform to IEC62541-12:2020[42] as specified by the Open Platforms Communications Unified Architecture[43]. Therefore, these sensors are capable of following a client-server relationship[43] and are directly connected to the network via switches. TP-Link's TL-SF1048 was chosen due to its low cost and high number of ports (48)[44].

At the network layer, we consider routers[6]. Several were investigated[45][46][47], but their speeds were unnecessary considering the speed limit of 10Gbps of the Cat 6a cables[25]. Instead, TP-Link's ER8411 is suggested for its 10Gbps ports[48].

We also consider security at this layer. Firewalls, filters, application gateways and Intrusion detection systems are all shown in appendices A-C as recommended[6][49]. However, in reality, filters and application gateways are also types of firewall[6]. For the devices labelled 'Firewall' in the appendices, SonicWall's NSa6700 is suggested as it has enough physical ports[50]. However, some ports are slower than others[50] and connection speeds to different subnets will need to be considered and prioritised.

The filter is a router that can be configured to drop certain packets arriving and prevent attacks such as Denial of Service and tracerouting[6]. The application gateway is a server that makes decisions based on policy about which traffic, for which applications to allow[6]. An intrusion detection system (IDS) is used to detect malicious content deep within packets[6]. For the filter and application gateway, a generic router and server can be configured for these purposes, but an IDS generally comprises a console; database and management servers; and the IDS sensor itself[51]. These are all shown as simply 'IDS Sensor' in the appendices for simplicity.

It is assumed the 4G networks for IoT devices are provided by existing telecommunications companies and that the data is transferred to YEWAT's cloud-based web server. For this server, it is suggested that a service such as Microsoft's Azure dedicated host service is used which may help with YEWAT's compliance requirements should isolation from other cloud customers be needed[52].

Data collected from IoT devices can thus be accessed via YEWAT's internet connection. However, using a private 4G network could be investigated[53]. This would involve installing infrastructure similar to public networks[54] including masts and antenna[55] which would prove costly[54]. Also, 4G networks could soon be obselete[56]. Furthermore, it might not be possible to lay cables which could be a requirement of a 4G network[55].

In order to achieve high availability, devices can be connected to more than one switch, router, or security device, providing an alternative route in the event of a hardware failure[6][57][58]. This idea has been implemented throughout much of the network with duplication of devices in key places.

1.3 Logical Separation

Appendix D shows connections between the buildings, ponds and internet. The SCADA sensors are physically separate from the buildings, however, they are logically separated from the other networks allowing for access to only selected employees using correct authentication as desired for security purposes[59].

The performance of large networks is improved using subnets connected via routers[60] which can ultimately be used to create virtual local area networks[61]. Each building has its own subnetwork for each of workstations, severs and routers/firewalls.

It is assumed that details of servers are as set out in table 2 of the brief meaning the sentence before it is not accurate since not all servers are located in the Data Centre according to the table.

1.4 IP Address design

RFC1918 defines the IP addresses available for use in a private network[49]. It advises the use of the 24 bit block of addresses[49]. This class A address was therefore selected[60]. Each building requires a different number of networks with different numbers of hosts. Allowing for possible growth, table 1.1 sumarises the allocation of addresses for each network (including network and broadcast addresses).

Building	Network	Allocation
Data Centre	Router	16
	Server	16
	Internal	64
	Sensors	256
Control room	Router	16
	Internal	128
Labs	Router	16
	Server	8
	Internal	64

Table 1.1 - Allocation of addresses for each network

Appendix E shows the address of each network and example IP addresses for hosts. Router 1 in the data centre acts as the Network Address Translation device which is the interface between the global IP address for the public internet and all private IP addresses across the network[62].

2 IT Director Concerns

2.1 Signal Strength

For wireless connections between buildings, three options were considered:

1. Private cellular 4G or 5G connections[63][53]
2. Each building having its own internet connection with inter-building connections happening through the public internet using a Virtual Private Network[64].
3. Point-to-point wireless bridging between the buildings[65][66]

A major benefit of option one would be that existing wireless IoT devices could be incorporated onto a private 4G network which would cut costs. However, as more IoT devices are added, more network congestion occurs. This would require more investment in the infrastructure to support it[67]. Furthermore, speed of the network may not be fast enough. Even 5G networks (which have a theoretical maximum speed of at least 10Gbps[68][69]) only have an average speed of 0.07-0.5Gbps in the UK[70][71][69]. Using a private 4G network for communication between the buildings could have a maximum speed of only 300Mbps[72]

Average speeds would be lower and there would be interference from increasing numbers of IoT devices. Therefore, a private 4G or 5G network is not recommended.

The second option would seem to be the best option given that it removes any concerns over signal strength. However, the brief states that there should be a wireless connection between the buildings and presumably this means a wired connection to the internet is impossible. A 5G broadband connection could be an alternative[73], but then the same limitation on speed would exist as with option one[73].

Point-to-point wireless bridging (the third option) is low cost[74] and allows for increased power making it possible to transmit over distances in the order of tens of kilometres[6]. This option was selected for its low cost, speed, and high signal strength.

Signal-to-noise ratio is known to be affected by changes in the weather[75]. To mitigate against this, techniques that regulate the power of signal transmission can be employed[75]. Also, modulation techniques can be adapted to suit conditions[6].

2.2 Network Resilience

Standard 802.11 Medium Access Control protocol will be used for the wireless bridges[76]. It uses CSMA/CA which is a random access protocol with collision avoidance[6]. CSMA/CA uses strong cyclic redundancy check codes and protocols that retransmit any frames containing errors[6]. This improves resilience in the network.

Regarding interference, it is worth noting that with a point-to-point wireless bridge, signals are less susceptible to interference and fading than with omni-directional devices[77][78].

Also, the selected wireless bridge operates at 5GHz and will therefore not be as susceptible to interference from the 4G IoT (and other) devices as one operating at 2.4GHz[6]. 4G devices typically operate at 0.8-2.6GHz[79]. Even with 5G IoT devices, these do not operate at 5GHz either[79]. Therefore, increasing the number of IoT devices is less likely to interfere with devices operating at 5GHz[6].

To increase wireless network resilience, another wireless bridge link between the laboratory and the control room could be added. This would provide a backup route in the event that one link to the data centre failed. This assumes a Radio Frequency line of sight exists (discussed in section 1.2). Alternatively, a multi-hop design could be used[6]. Although, this would necessitate placing at least one other wireless bridge on the campus[6]. If a multi-hop design is viable, other wireless bridges could be added to boost the signal between buildings. Or, an outdoor wireless access point such as TP-Link's EAP225-Outdoor could be considered[80]. However, in both scenarios, cables would need to be routed to these devices which would go against the requirement in the brief of not installing additional cables.

3 Chief Information Security Officer (CISO) Concerns

3.1 Security Concerns

IoT attacks are one of the top five emerging threats[81] and there is greater concern over security in wireless sensor networks than in wired ones[82]. However, this does not mean the transition to wireless IoT devices should be abandoned. If a risk assessment is conducted following ISO/IEC27001[83] using a risk rating methodology such as OWASP, threats can be identified and treated[84]. The key cyber-security issues of Confidentiality, Integrity and Availability[85], would be considered. Added to this, would be the issue of authenticity[6][36]. However, as required, only vulnerabilities with wireless cyber-physical devices and SCADA sensors are discussed here.

3.1.1 Wireless sensors

The brief states that the wireless cyber-physical devices connect to 4G networks. Any wireless network is vulnerable to frames being sniffed by a potential attacker using a receiver within the range of the sending device[6]. Security techniques applicable to wireless networks include the use of shared symmetric keys and the AES encryption standard[6]. Symmetric keys form a shared secret allowing a network and devices to authenticate each other[6]. Authentication (along with use of keys) is essential to cellular network security[86].

In the current design, 4G connectivity and security is provided by public telecommunications companies. How much trust in their security protocols is there? Key vulnerabilities exist in 4G networks (e.g. vulnerability to authentication relay attacks[87]). 5G authentication methods improve upon 4G methods[88]. Furthermore, 5G includes design for non-public-networks with specifically designed security features[89]. This includes the provision of EAP-TLS - a protocol designed to work in IoT (and similar) environments[6][88][89]. It reduces operational risks associated with symmetric key management by removing the need to store a vast quantity of long-term keys[88]. However, this is at the expense of overheads in certificate management which should be considered if a 5G private network were to be implemented[88].

As a result of this potential for improved security, could there be an argument for delaying the introduction of cyber-physical devices until they operate on 5G networks? Then, the idea of a 5G private network (discussed in section 2.1) could be revisited bringing the associated security requirements under YEWAT's control.

3.1.2 SCADA Sensors

Historically, key vulnerabilities have existed in SCADA systems[90][59]. These have included poor network security; lack of encryption; issues with authentication; and out of date operating systems[90][59]. Ensuring firewalls and intrusion detection systems are in place will improve network security[6][90]. Appendix A shows these devices in place. Ensuring broadcast packets do not enter the network is also key[59], as is ensuring operating systems are up-to-date[90].

For Authentication, in this security critical environment, either FIDO2 or MFA would provide the highest level of security[91]. MFA would be more appropriate since FIDO2 might mean users temporarily losing access to their accounts if they lost their security token[91].

Further improvements in SCADA security can be achieved with the integration of different technologies such as incorporating mobile nodes on an ad-hoc network[90]. Perhaps therefore, there is an argument for implementing a system that incorporates both SCADA sensors and wireless cyber-physical devices?

3.2 Legal Concerns

YEWAT must adhere to certain legal requirements. The most salient of these are:

1. The UK Data Protection Act (2018)[92] (the UK implementation of the European Union's General Data Protection Regulations (GDPR)[93]). If YEWAT wishes to store data generated by employees (e.g. through email or use of the internet), it would

need to ensure this conforms to article 5 of the UK GDPR[94]. Specifically, the data should be processed fairly, transparently, securely and employees should be notified of the purpose[94].

2. The Security of Network and Information Systems Regulations[95] which aims to improve network security of both digital and essential services. This includes requirements for reporting incidents, regulations for external service providers (such as existing 4G service providers) and monitoring of internal networks[95][96]

3. The Investigatory Powers Act of 2016[97]. This regulates the extent to which network traffic that may disclose the content of confidential information can be monitored without contravening the Human Rights Act of 1998[98][99]. Regulations associated with business use of network traffic were added to the act in 2018[100].

Jisc, an organisation that provides digital solutions for research and education, have developed a guide for laws that apply to networking in the UK[97]. The guide discusses the above and other considerations such as what to do in the event of uncovering of criminal activity[97]. It is a good source of information, and should be followed to ensure compliance.

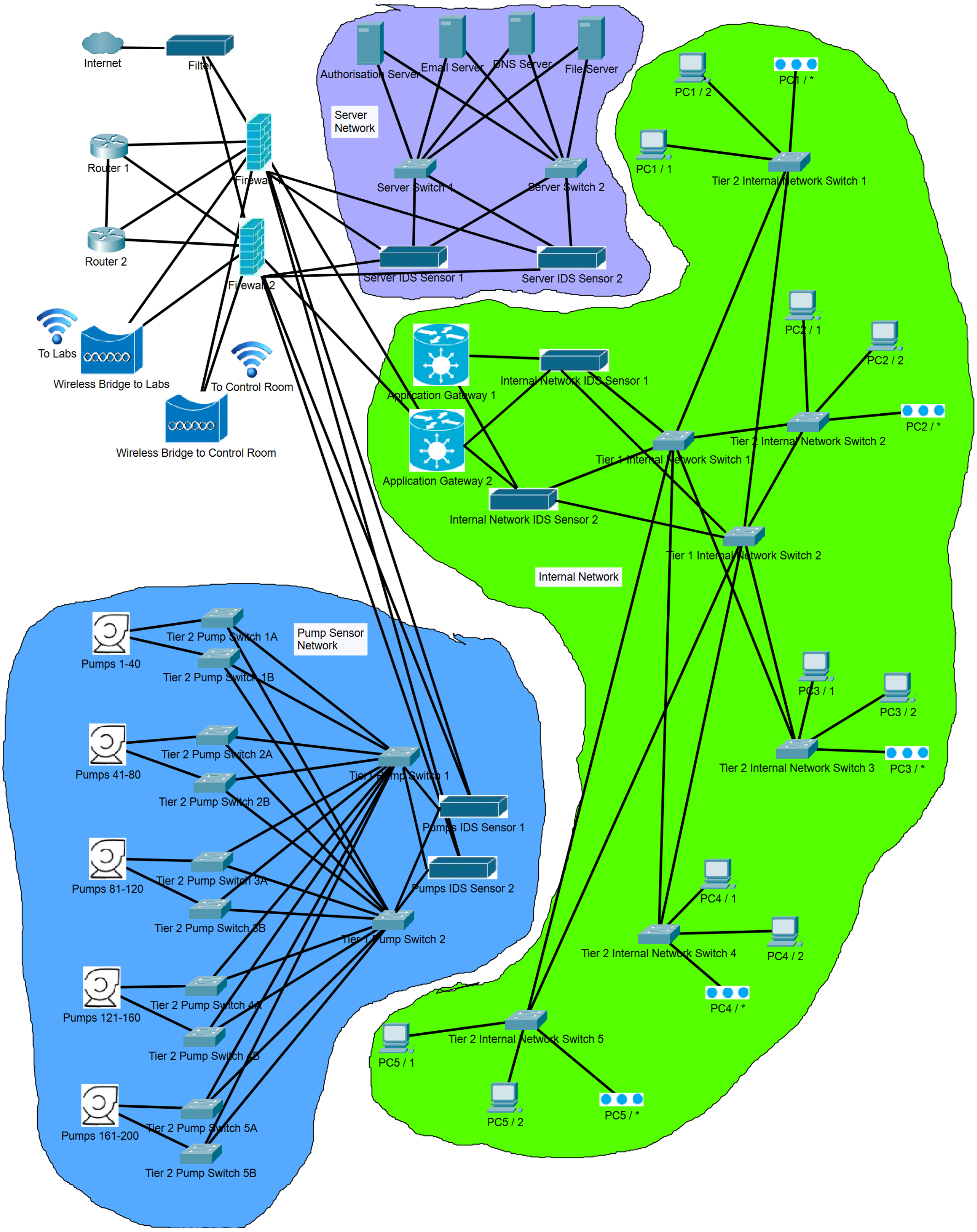
3.3 Ethical, Environmental and business Concerns

If a threat agent were to gain control of pump and gate systems, this could result in water being rendered unfit for consumption; or untreated wastewater being maliciously pumped into local rivers. Aside from disastrous environmental and ethical consequences (untreated water discharge has the potential to cause harm to fish in the water[101]), YEWAT's reputation would be damaged. Furthermore, water companies in the future could face unlimited fines for illegal discharge of untreated water[102]. The discussed legal requirements and security risk assessment procedure will act to prevent against such consequences resulting from cyber-attacks.

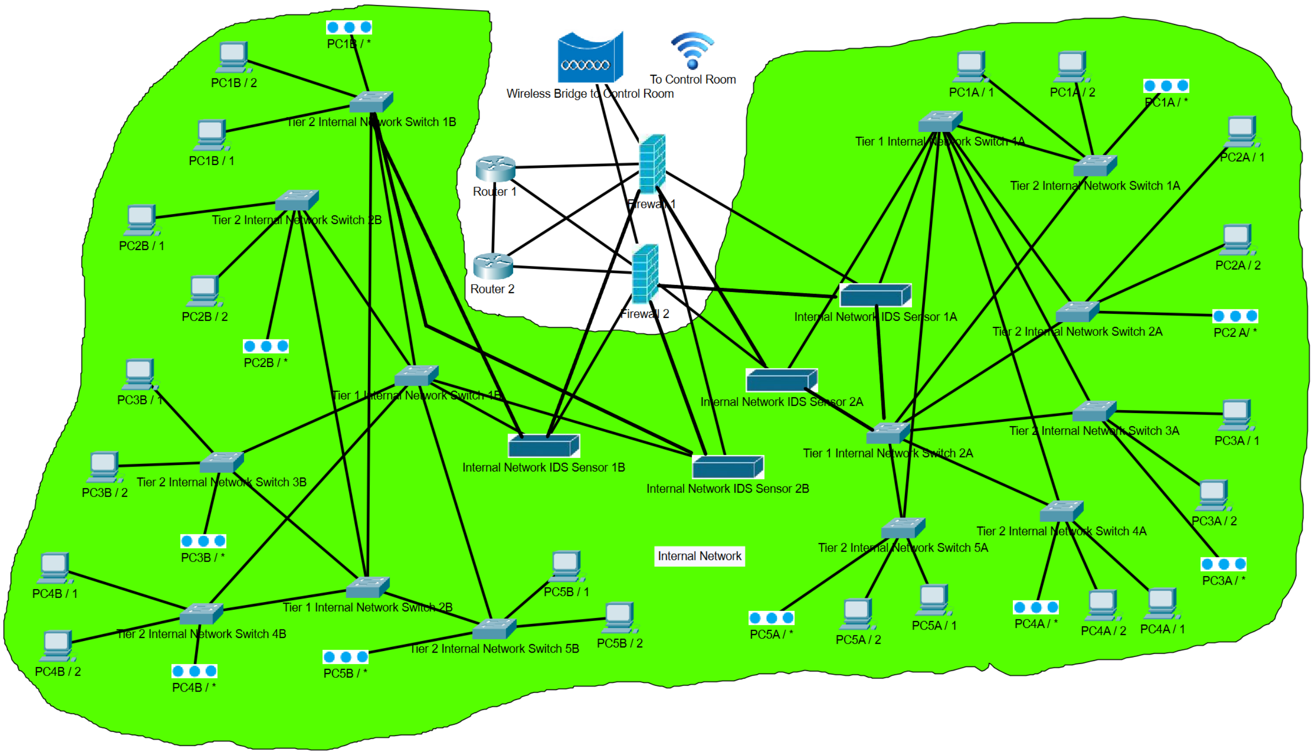
Energy efficiency is another environmental consideration for YEWAT. An increasing number of devices raises demand for power which is an environmental concern[103]. On-site renewable energy sources would help to mitigate against this[103].

Finaly, what of the consequences of a power outage? Could this result in flooding of homes? Or the unwanted release of untreated water? To avoid this, YEWAT should install a backup power supply to mitigate against this key vulnerability[104].

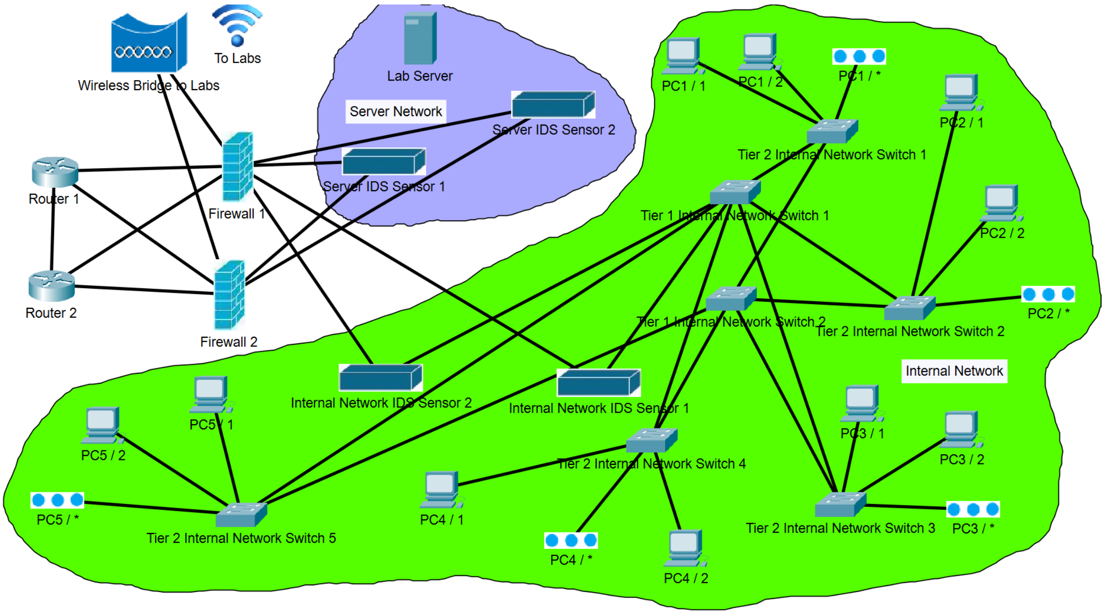
Appendix A - Network diagram for Data Centre



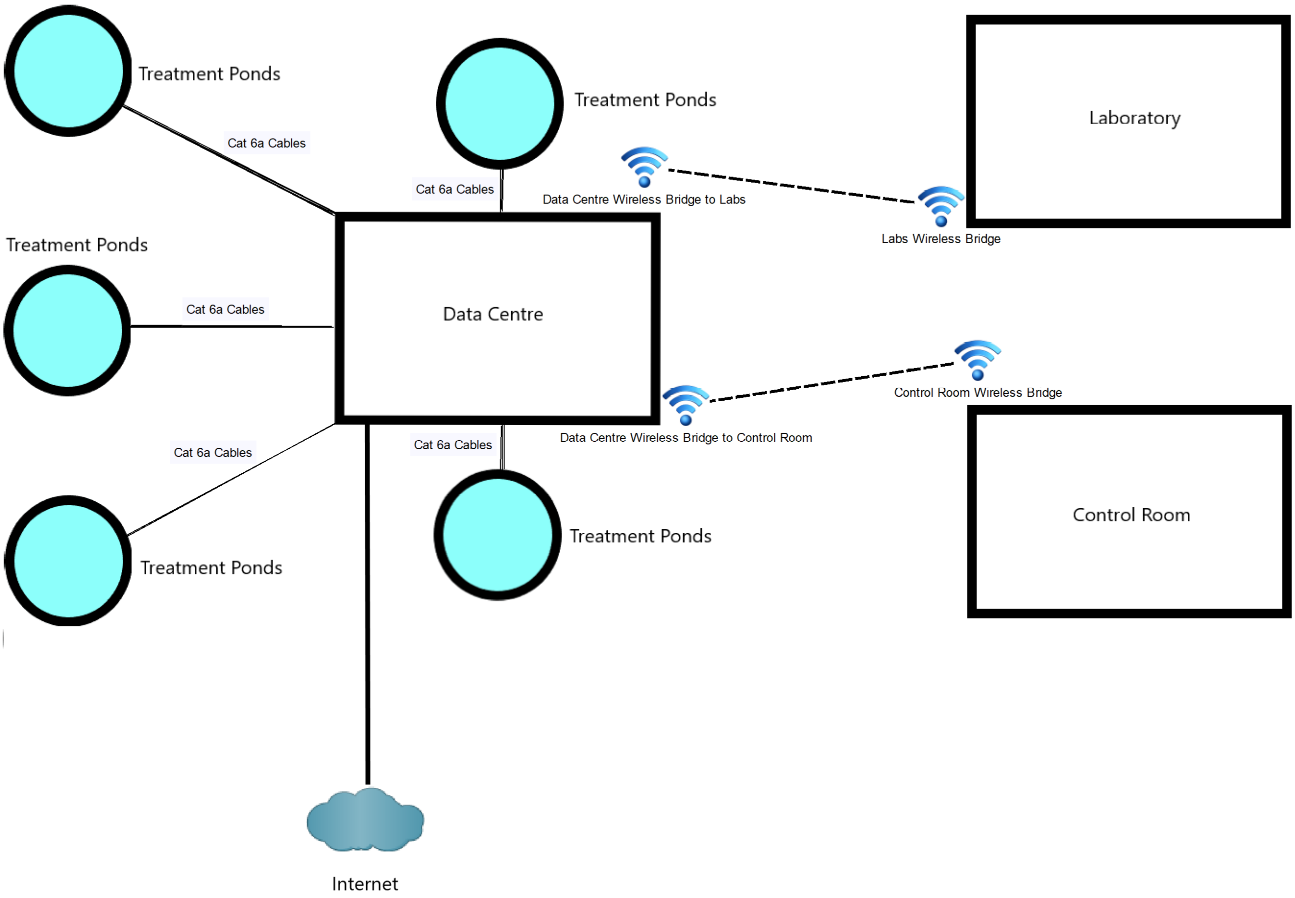
Appendix B - Network Diagram for Operational Control Room


PC1B / *
PC1B / 2
Tier 2 Internal Network Switch 1B
PC1B / 1
Wireless Bridge to Control Room
To Control Room
Router 1
Firewall 1
Router 2
Firewall 2
Tier 2 Internal Network Switch 2B
PC2B / 1
PC2B / 2
PC2B / *
PC3B / 1
Tier 1 Internal Network Switch 1B
Internal Network IDS Sensor 1B
Internal Network IDS Sensor 2B
PC3B / 2
Tier 2 Internal Network Switch 3B
PC3B / *
PC4B / 1
Tier 1 Internal Network Switch 2B
Tier 2 Internal Network Switch 4B
PC4B / 2
PC4B / *
PC5B / *
Tier 2 Internal Network Switch 5B
PC5B / 1
PC5B / 2
Internal Network
PC1A / 1
PC1A / 2
PC1A / *
Tier 1 Internal Network Switch 1A
Tier 2 Internal Network Switch 1A
PC2A / 1
PC2A / 2
Internal Network IDS Sensor 1A
Tier 2 Internal Network Switch 2A
PC2 A/ *
Internal Network IDS Sensor 2A
Tier 1 Internal Network Switch 2A
Tier 2 Internal Network Switch 3A
PC3A / 1
PC3A / 2
PC3A / *
Tier 2 Internal Network Switch 4A
Tier 2 Internal Network Switch 5A
PC5A / *
PC5A / 2
PC5A / 1
PC4A / *
PC4A / 2
PC4A / 1

Appendix C - Network Diagram for Laboratories


Wireless Bridge to Labs
To Labs
Lab Server
Server Network
Server IDS Sensor 2
Server IDS Sensor 1
Router 1
Firewall 1
Router 2
Firewall 2
PC1 / 1
PC1 / 2
PC1 / *
PC2 / 1
Tier 2 Internal Network Switch 1
Tier 1 Internal Network Switch 1
PC2 / 2
PC2 / *
Tier 1 Internal Network Switch 2
Tier 2 Internal Network Switch 2
Internal Network
Internal Network IDS Sensor 2
Internal Network IDS Sensor 1
PC5 / 1
PC5 / 2
PC3 / 1
PC3 / 2
Tier 2 Internal Network Switch 4
PC5 / *
Tier 2 Internal Network Switch 5
PC4 / 1
Tier 2 Internal Network Switch 3
PC3 / *
PC4 / *
PC4 / 2

Appendix D - Physical layout



Appendix E - Network addresses, subnet masks and example IP Addresses

Data Centre		
Network address and subnet mask	Device	IP Addresseses
10.0.0.0/24 255.255.255.0	Pumps IDS sensor 1	10.0.0.1
	Pumps IDS sensor 2	10.0.0.2
	Sensors 1 - 40 **	10.0.0.3 - 10.0.0.49
	Sensors 41 - 80 **	10.0.0.50 - 10.0.0.97
	Sensors 81 -120 **	10.0.0.98 - 10.0.0.143
	Sensors 121 - 160 **	10.0.0.144 - 10.0.0.190
	Sensors 161 - 200 **	10.0.0.191 - 10.0.0.237
10.0.1.0/26 255.255.255.192	Application Gateway 1	10.0.1.1
	Application Gateway 2	10.0.1.2
	Internal Network IDS sensor 1	10.0.1.3
	Internal Network IDS sensor 2	10.0.1.4
	PC 1 PCs (5 PCs*)	10.0.1.5 - 10.0.1.11
	PC 2 PCs (5 PCs*)	10.0.1.12 - 10.0.1.18
	PC 3 PCs (5 PCs*)	10.0.1.19 - 10.0.1.25
	PC 4 PCs (5 PCs*)	10.0.1.26 - 10.0.1.32
	PC 5 PCs (5 PCs*)	10.0.1.33 - 10.0.1.39
10.0.1.64/28 255.255.255.240	Router 1	10.0.1.65
	Router 2	10.0.1.66
	Filter	10.0.1.67
	Firewall 1	10.0.1.68
	Firewall 2	10.0.1.69
10.0.1.80/28 255.255.255.240	Server IDS sensor 1	10.0.1.81
	Server IDS sensor 2	10.0.1.82
	Auth. Server	10.0.1.83
	Email Server	10.0.1.84
	DNS Server	10.0.1.85
	File Server	10.0.1.86

Control Room		
Network address and subnet mask	Device	IP Addresses
10.0.2.0/25 255.255.255.128	Internal Network IDS sensor 1A	10.0.2.1
	Internal Network IDS sensor 2A	10.0.2.2
	Internal Network IDS sensor 1B	10.0.2.3
	Internal Network IDS sensor 2B	10.0.2.4
	PC 1 PCs (5PCs *)	10.0.2.5 - 10.0.2.11
	PC 2 PCs (5PCs *)	10.0.2.12 - 10.0.2.18
	PC 3 PCs (5PCs *)	10.0.2.19 - 10.0.2.25
	PC 4 PCs (5PCs *)	10.0.2.26 - 10.0.2.32
	PC 5 PCs (5PCs *)	10.0.2.33 - 10.0.2.39
	PC 6 PCs (5PCs *)	10.0.2.40 - 10.0.2.46
	PC 7 PCs (5PCs *)	10.0.2.47 - 10.0.2.53
	PC 8 PCs (5PCs *)	10.0.2.54 - 10.0.2.60
	PC 9 PCs (5PCs *)	10.0.2.61 - 10.0.2.67
	PC 10 PCs (5PCs *)	10.0.2.68 - 10.0.2.74
10.0.2.128/28 255.255.255.240	Router 1	10.0.2.129
	Router 2	10.0.2.130
	Firewall 1	10.0.2.131
	Firewall 2	10.0.2.132

Labs					
Network address and subnet mask	Device	IP Addresses	Network address and subnet mask	Device	IP Addresses
10.0.3.0/27 255.255.255.224	Internal Network IDS sensor 1	10.0.3.1	10.0.3.32/28 255.255.255.240	Router 1	10.0.3.33
	Internal Network IDS sensor 2	10.0.3.2		Router 2	10.0.3.34
	PC 1 PCs (5 PCs*)	10.0.3.3 - 10.0.3.9		Firewall 1	10.0.3.35
	PC 2 PCs (5 PCs*)	10.0.3.10 - 10.0.3.16		Firewall 2	10.0.3.36
	PC 3 PCs (5 PCs*)	10.0.3.17 - 10.0.3.23	10.0.3.48/29 255.255.255.248	Server IDS sensor 1	10.0.3.49
	PC 4 PCs (5 PCs*)	10.0.3.24 - 10.0.3.30		Server IDS sensor 2	10.0.3.50
	PC 5 PCs (5 PCs*)	10.0.3.31 - 10.0.3.37		Lab server	10.0.3.51

* Space for 7 PCs in this range because switches have the capacity

** Space for 47 sensors in this range because switches have the capacity

References

[1] AWS, *What is osi model?* Accessed 2024-26-05. [Online]. Available: https://aws.amazon.com/what-is/osi-model/.

[2] *NCP/TCP transition plan*, RFC 801, Nov. 1981. DOI: 10.17487/RFC0801. [Online]. Available: https://www.rfc-editor.org/info/rfc801.

[3] A. Sundararajan, A. Chavan, D. Saleem and A. Sarwat, 'A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security,' *Energies*, vol. 11, p. 2360, Sep. 2018. DOI: 10.3390/en11092360.

[4] H. Andrea, *Difference between routers and switches in tcp/ip networks*, Accessed 2024-27-05. [Online]. Available: https://www.networkstraining.com/router-vs-switch-in-networks/.

[5] 'Information technology - open systems interconnection - basic reference model: The basic model,' ISO/IEC, Tech. Rep., Jun. 1996.

[6] J. F. Kurose and K. W. Ross, *COMPUTER NETWORKING: A Top-Down Approach, 8th Edition*. Pearson Education Limited, 2022.

[7] Cisco Systems, Inc., *Campus lan and wireless lan solution design guide*, Accessed 2024-27-05. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html.

[8] W. Eddy, *Transmission Control Protocol (TCP)*, RFC 9293, Aug. 2022. DOI: 10.17487/RFC9293. [Online]. Available: https://www.rfc-editor.org/info/rfc9293.

[9] *Internet Protocol*, RFC 791, Sep. 1981. DOI: 10.17487/RFC0791. [Online]. Available: https://www.rfc-editor.org/info/rfc791.

[10] D. S. E. Deering and B. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 8200, Jul. 2017. DOI: 10.17487/RFC8200. [Online]. Available: https://www.rfc-editor.org/info/rfc8200.

[11] *An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, RFC 826, Nov. 1982. DOI: 10.17487/RFC0826. [Online]. Available: https://www.rfc-editor.org/info/rfc826.

[12] Y. Rekhter, S. Hares and T. Li, *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, Jan. 2006. DOI: 10.17487/RFC4271. [Online]. Available: https://www.rfc-editor.org/info/rfc4271.

[13] R. Droms and S. Alexander, *DHCP Options and BOOTP Vendor Extensions*, RFC 2132, Mar. 1997. DOI: 10.17487/RFC2132. [Online]. Available: https://www.rfc-editor.org/info/rfc2132.

[14] R. Thurlow, *RPC: Remote Procedure Call Protocol Specification Version 2*, RFC 5531, May 2009. DOI: 10.17487/RFC5531. [Online]. Available: https://www.rfc-editor.org/info/rfc5531.

[15] N. Freed and D. N. S. Borenstein, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*, RFC 2045, Nov. 1996. DOI: 10.17487/RFC2045. [Online]. Available: https://www.rfc-editor.org/info/rfc2045.

[16] R. T. Fielding, M. Nottingham and J. Reschke, *HTTP Semantics*, RFC 9110, Jun. 2022. DOI: 10.17487/RFC9110. [Online]. Available: https://www.rfc-editor.org/info/rfc9110.

[17] D. J. C. Klensin, *Simple Mail Transfer Protocol*, RFC 5321, Oct. 2008. DOI: 10.17487/RFC5321. [Online]. Available: https://www.rfc-editor.org/info/rfc5321.

[18] *Domain names - concepts and facilities*, RFC 1034, Nov. 1987. DOI: 10.17487/RFC1034. [Online]. Available: https://www.rfc-editor.org/info/rfc1034.

[19] *Domain names - implementation and specification*, RFC 1035, Nov. 1987. DOI: 10.17487/RFC1035. [Online]. Available: https://www.rfc-editor.org/info/rfc1035.

[20] S. Frankel and S. Krishnan, *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*, RFC 6071, Feb. 2011. DOI: 10.17487/RFC6071. [Online]. Available: https://www.rfc-editor.org/info/rfc6071.

[21] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, Aug. 2018. DOI: 10.17487/RFC8446. [Online]. Available: https://www.rfc-editor.org/info/rfc8446.

[22] *Internet Standard Subnetting Procedure*, RFC 950, Aug. 1985. DOI: 10.17487/RFC0950. [Online]. Available: https://www.rfc-editor.org/info/rfc950.

[23] 'Ieee standard for ethernet,' *IEEE Std 802.3-2022 (Revision of IEEE Std 802.3-2018)*, pp. 1–7025, 2022. DOI: 10.1109/IEEESTD.2022.9844436.

[24] Telecommunications Industry Association, *Ansi/tia-568.0-e: Generic telecommunications cabling for customer premises*, Telecommunications Industry Association (TIA), Available: TIA, 2020.

[25] D. Graham-Smith and S. Andrews, *Best ethernet cable 2024: The easy way to a high-speed, hassle-free network*, Accessed 2024-29-05. [Online]. Available: `https://www.expertreviews.co.uk/accessories/1407408/best-ethernet-cable`.

[26] *Bs iso/iec 14165-151:2017: Information technology. fibre channel: Fibre channel baset (fc-baset)*, eng, 2018.

[27] Aiyden, *Cat 7 ethernet cable, how much do you know?* Accessed 2024-09-06. [Online]. Available: `https://www.qsfptek.com/qt-news/cat7-cable-wiki.html`.

[28] L. LAURENTE-TICONG, *9 best network switches for 2024: Speed and features compared*, Accessed 2024-30-05. [Online]. Available: `https://www.enterprisenetworkingplanet.com/guides/network-switch-companies/`.

[29] *21/30446696 dc: Bs iso/iec 11801-1:2017 amd1. information technology. generic cabling for customer premises: Part 1. general requirements*, eng, 2021.

[30] M. J. Castelli, *LAN Switching First-Step*. Cisco Press, 2004.

[31] Cisco Systems, Inc., *Cisco catalyst 9000 at-a-glance*, Accessed 2024-30-05. [Online]. Available: `https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-aag-cte-en.html`.

[32] 4networks.co.uk, *Catalyst 9300 24-port poe+, network essentials*, Accessed 2024-30-05. [Online]. Available: `https://4networks.co.uk/c9300-24p-e.html`.

[33] D-Link, *10 gigabit smart managed fiber switch dxs-1210-12sc*, Accessed 2024-09-06. [Online]. Available: `https://www.dlink.com/en/products/dxs-1210--12sc-10-gigabit-smart-managed-fiber-switch`.

[34] ZYXEL Networks, *5/8-port 2.5gbe unmanaged switch mg100 series*, Accessed 2024-30-05. [Online]. Available: https://www.zyxel.com/global/en/products/switch/5-8-port-2-5gbe-unmanaged-switch-mg100-series.

[35] Bulk Devices, *Network switches*, Accessed 2024-30-05. [Online]. Available: https://bulkdevices.co.uk/networking-devices/switches/network-switches.

[36] Y. Zou, J. Zhu, X. Wang and L. Hanzo, 'A survey on wireless security: Technical challenges, recent advances, and future trends,' *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016. DOI: 10.1109/JPROC.2016.2558521.

[37] TP-Link, *Cpe710 5ghz ac 867mbps 23dbi outdoor cpe*, Accessed 2024-09-06. [Online]. Available: https://www.tp-link.com/uk/business-networking/pharos-cpe/cpe710/.

[38] tp-link, *Cpe210 2.4ghz 300mbps 9dbi outdoor cpe*, Accessed 2024-21-06. [Online]. Available: https://www.tp-link.com/uk/business-networking/outdoor-radio/cpe210/.

[39] Tycon Systems, *Ezbr-0214+*, Accessed 2024-21-06. [Online]. Available: https://tyconsystems.com/homepage/shop/ezbr-0214/.

[40] APC Communications Solutions Ltd, *Kuwfi 2 pack 300mbps wireless outdoor cpe kit point-to-point wireless access point 24g wifi bridge supports 1km transmission distance solution for pt*, Accessed 2024-21-06. [Online]. Available: https://kuwfi.shop/products/kuwfi-2-pack-300mbps-wireless-outdoor-cpe-kit-point-to-point-wireless-access-point-24g-wifi-bridge-supports-1km-transmission-distance-solution-for-pt-?VariantsId=10026.

[41] APC Communications Solutions Ltd, *What is a wireless bridge?* Accessed 2024-21-06. [Online]. Available: `https://www.apcsolutionsuk.com/what-is-a-wireless-bridge/`.

[42] *Bs en iec 62541-12:2020: Opc unified architecture: Discovery and global services*, eng, 2020.

[43] OPC Foundation, *Unified architecture*, Accessed 2024-09-06. [Online]. Available: `https://opcfoundation.org/about/opc-technologies/opc-ua/`.

[44] TP-Link, *Tl-sf1048 48-port 10/100mbps rackmount switch*, Accessed 2024-04-06. [Online]. Available: `https://www.tp-link.com/us/business-networking/unmanaged-switch/tl-sf1048/`.

[45] Juniper Networks, *Acx5000 line of universal metro routers datasheets*, Accessed 2024-30-05. [Online]. Available: `https://www.juniper.net/us/en/products/routers/acx-series/acx5000-line-of-universal-metro-routers-datasheet.html`.

[46] Nokia, *7220 interconnect router for data center fabric*, Accessed 2024-30-05. [Online]. Available: `https://www.nokia.com/networks/data-center/data-center-fabric/7220-interconnect-router/`.

[47] Cisco Systems, Inc., *Cisco 900 series integrated services routers*, Accessed 2024-30-05. [Online]. Available: `https://www.cisco.com/site/us/en/products/networking/sdwan-routers/900-series-integrated-services-routers/index.html`.

[48] TP-Link, *Er8411 omada vpn router with 10g ports*, Accessed 2024-09-06. [Online]. Available: `https://www.tp-link.com/uk/business-networking/omada-sdn-router/er8411/`.

[49] R. Moskowitz, D. Karrenberg, Y. Rekhter, E. Lear and G. J. de Groot, *Address Allocation for Private Internets*, RFC 1918, Feb. 1996. DOI: 10.17487/RFC1918. [Online]. Available: https://www.rfc-editor.org/info/rfc1918.

[50] Netthreat, *Sonicwall nsa 6700*, Accessed 2024-21-06. [Online]. Available: https://www.sonicwallonline.co.uk/firewalls/nsa-series/sonicwall-nsa-6700.html.

[51] J. Villanueva, *An introductory guide to intrusion detection systems*, Accessed 2024-21-06. [Online]. Available: https://techgenix.com/ids-intrusion-detection-system-guide/.

[52] Microsoft, *Azure dedicated host*, Accessed 2024-21-06. [Online]. Available: https://azure.microsoft.com/en-gb/products/virtual-machines/dedicated-host.

[53] D. A. Ltd, *Enterprise cbrs and private lte/5g the convergence of private cellular and wi-fi a disruptive analysis thought-leadership paper*, Accessed 2024-28-05. [Online]. Available: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/2021/enterprise-cbrs-and-private-lte5g-the-convergence-of-private-cellular-and-wi-fi.pdf.

[54] I. Romanov, *Cost of private 5g and private lte networks: What should business choose*, Accessed 2024-14-06. [Online]. Available: https://www.uctel.co.uk/blog/%d1%81ost-of-private-5g-and-private-lte-networks-what-should-business-choose.

[55] A. Clark and F. Rankl, *Building broadband and mobile infrastructure*, https://researchbriefings.files.parliament.uk/documents/CBP-9156/CBP-9156.pdf, Commons Library Research Briefing, CBP 9156, Mar. 2024.

[56] I. Romanov, *When will 4g be phased out in the uk — is 4g still relevant today?* Accessed 2024-14-06. [Online]. Available: `hhttps://www.uctel.co.uk/blog/when-will-4g-be-phased-out-in-the-uk-is-4g-still-relevant-today`.

[57] A. Greenberg, J. R. Hamilton, N. Jain, S. Kandula, C. Kim, P. Lahiri, D. A. Maltz, P. Patel and S. Sengupta, 'Vl2: A scalable and flexible data center network,' in *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication*, ser. SIGCOMM '09, Barcelona, Spain: Association for Computing Machinery, 2009, pp. 51–62, ISBN: 9781605585949. DOI: `10.1145/1592568.1592576`. [Online]. Available: `https://doi.org/10.1145/1592568.1592576`.

[58] K. K. S. Wai, 'Network-level redundancy for campus lan,' *International Journal of Trend in Scientific Research and Development*, 2019.

[59] J. D. Fernandez and A. E. Fernandez, 'Scada systems: Vulnerabilities and remediation,' *J. Comput. Sci. Coll.*, vol. 20, no. 4, pp. 160–168, Apr. 2005, ISSN: 1937-4771.

[60] G. Thomas, 'Introduction to subnetting,' *The extension A Technical Supplement to Control network*, vol. 1, no. 8, 2000.

[61] C. W. Kok and M. S. Beg, 'Simple ip subnet vlan implementation,' in *Proceedings. Ninth IEEE International Conference on Networks, ICON 2001.*, IEEE, 2001, pp. 160–165.

[62] B. Ford, P. Srisuresh and D. Kegel, 'Peer-to-peer communication across network address translators.,' in *USENIX Annual Technical Conference, General Track*, 2005, pp. 179–192.

[63] M. Wen, Q. Li, K. J. Kim, D. López-Pérez, O. A. Dobre, H. V. Poor, P. Popovski and T. A. Tsiftsis, 'Private 5g networks: Concepts, architectures, and research landscape,'

IEEE Journal of Selected Topics in Signal Processing, vol. 16, no. 1, pp. 7–25, 2022. DOI: 10.1109/JSTSP.2021.3137669.

[64] M. Feilner, *OpenVPN: Building and integrating virtual private networks*. Packt Publishing Ltd, 2006.

[65] A. Calvagna, G. Morabito and A. La Corte, 'Wifi bridge: Wireless mobility framework supporting session continuity,' in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003).*, 2003, pp. 79–86. DOI: 10.1109/PERCOM.2003.1192729.

[66] J. SALTER, *Point-to-point wi-fi bridging between buildings—the cheap and easy way*, Accessed 2024-28-05. [Online]. Available: https://arstechnica.com/gadgets/2021/08/point-to-point-wi-fi-bridging-between-buildings-the-cheap-and-easy-way/.

[67] F. Grijpink, A. Ménard, H. Sigurdsson and N. Vucevic, *The road to 5g: The inevitable growth of infrastructure cost*, Accessed 2024-14-06. [Online]. Available: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost.

[68] Ofcom, *Enabling 5g in the uk*, Accessed 2024-13-06. [Online]. Available: https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/spectrum-management/enabling-5g-uk.pdf.

[69] J. Rogerson and K. Thomas, *How fast is 5g?* Accessed 2024-13-06. [Online]. Available: https://5g.co.uk/guides/how-fast-is-5g/.

[70] P. Song, J. Lee and L. Mukhanov, 'A case study on latency, bandwidth and energy efficiency of mobile 5g and youtube edge service in london. why the 5g ecosystem and energy efficiency matter?' *arXiv preprint arXiv:2310.14090*, 2023.

[71] Vodafone, *5g ultra*, Accessed 2024-13-06. [Online]. Available: https://www.vodafone.co.uk/network/5g.

[72] R. Dunne, *How fast are 4g and 5g*, Accessed 2024-13-06. [Online]. Available: https://www.techradar.com/broadband/5g-broadband.

[73] R. Dunne, *5g home broadband: What is it and how much do deals cost?* Accessed 2024-13-06. [Online]. Available: https://www.techradar.com/broadband/5g-broadband.

[74] B. Raman and K. Chebrolu, 'Experiences in using wifi for rural internet in india,' *Communications Magazine, IEEE*, vol. 45, pp. 104–110, Feb. 2007. DOI: 10.1109/MCOM.2007.284545.

[75] M. A. Hadidi, J. S. Al-Azzeh, R. Odarchenko, S. Gnatyuk and A. Abakumova, 'Adaptive regulation of radiated power radio transmitting devices in modern cellular network depending on climatic conditions,' *Contemporary engineering sciences*, vol. 9, pp. 473–485, 2016. DOI: 10.12988/CES.2016.629.

[76] C. Shao, D. Hui, R. Pazhyannur, F. Bari, R. Zhang and S. Matsushima, *IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP)*, RFC 7494, Apr. 2015. DOI: 10.17487/RFC7494. [Online]. Available: https://www.rfc-editor.org/info/rfc7494.

[77] SRFS Teleinfra, *Omni-directional vs. directional antenna*, Accessed 2024-14-06. [Online]. Available: https://www.srfsteleinfra.in/omni-directional-vs-directional-antenna/.

[78] Cisco Systems, Inc., *Omni antenna vs. directional antenna*, Accessed 2024-14-06. [Online]. Available: `https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html`.

[79] 4g.co.uk, *4g and 5g frequency bands*, Accessed 2024-14-06. [Online]. Available: `https://www.4g.co.uk/4g-frequencies-uk-need-know/`.

[80] tp-link, *Eap225-outdoor ac1200 wireless mu-mimo gigabit indoor/outdoor access point*, Accessed 2024-20-06. [Online]. Available: `https://www.tp-link.com/uk/business-networking/omada-sdn-access-point/eap225-outdoor/`.

[81] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala and H. Al-Shahwani, 'Exploring the top five evolving threats in cybersecurity: An in-depth overview,' *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 57–63, Mar. 2023. DOI: `10.58496/MJCS/2023/010`. [Online]. Available: `https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/44`.

[82] Y. Chung, S. Choi, Y. Lee, N. Park and D. Won, 'An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks,' *National Library of Medicine*, vol. 16, no. 10, 2016. DOI: `10.3390/s16101653`.

[83] 'Information technology - security techniques - information security management systems - requirements (iso/iec 27001:2013),' BSI, Tech. Rep., Mar. 2017.

[84] OWASP Foundation, *Owasp risk rating methodology*, Accessed = 2024-06-17. [Online]. Available: `https://owasp.org/www-community/OWASP_Risk_Rating_Methodology`.

[85] C. P. Pfleeger, S. L. Pfleeger and J. Margulies, *Security in Computing, 5th Edition*. Pearson, 2015.

[86] CableLabs, *A comparative introduction to 4g and 5g authentication*, Accessed = 2024-06-18. [Online]. Available: `https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication`.

[87] S. R. Hussain, O. Chowdhury, S. Mehnaz and E. Bertino, 'Lteinspector: A systematic approach for adversarial testing of 4g lte,' in *Network and Distributed System Security Symposium*, 2018. [Online]. Available: `https://api.semanticscholar.org/CorpusID:3387805`.

[88] M. Wazid, A. K. Das, S. Shetty, P. Gope and J. Rodrigues, 'Security in 5g-enabled internet of things communication: Issues, challenges and future research roadmap,' *IEEE Access*, vol. PP, pp. 1–1, Dec. 2020. DOI: `10.1109/ACCESS.2020.3047895`.

[89] C. Jost, *Security features for non-public networks*, Accessed = 2024-06-18. [Online]. Available: `https://www.3gpp.org/technologies/sec-npn`.

[90] G. K. Chalamasetty, P. Mandal and T.-L. Tseng, 'Secure scada communication network for detecting and preventing cyber-attacks on power systems,' in *2016 Clemson University Power Systems Conference (PSC)*, 2016, pp. 1–7. DOI: `10.1109/PSC.2016.7462865`.

[91] NSCC, *Authentication methods: Choosing the right type*, Accessed 2024-20-06. [Online]. Available: `https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type`.

[92] 'Data protection act 2018 chapter 12,' Crown and database right, Tech. Rep., May 2018.

[93] 'Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation),' THE EUROPEAN PARLIAMENT and COUNCIL, Tech. Rep., Apr. 2016.

[94] Information Commissioner's Office, *A guide to the data protection principles*, Accessed 2024-18-06. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/.

[95] UK Government, *The security of network & information systems regulations*, Accessed 2024-18-06. [Online]. Available: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018.

[96] UK Government, *Cyber laws updated to boost uk's resilience against online attacks*, Accessed 2024-18-06. [Online]. Available: https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks.

[97] Jisc, *Networking, computers and the law*, Accessed 2024-18-06. [Online]. Available: https://www.jisc.ac.uk/guides/networking-computers-and-the-law.

[98] *Investigatory powers act 2016*, https://www.legislation.gov.uk/ukpga/2016/25/section/1, Accessed: 18 June 2024, 2016.

[99] UK Parliament, *Human rights act 1998*, https://www.legislation.gov.uk/ukpga/1998/42/contents, Accessed: 2024-06-18, 1998.

[100] *The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018*, UK Statutory Instruments, Made 8th March 2018, coming into force in accordance with regulation 1, 2018. [Online]. Available: https://www.legislation.gov.uk/uksi/2018/356/made.

[101] L. Fisher, 'Pollution kills fish,' *Scientific American*, vol. 160, no. 3, pp. 144–146, 1939.

[102] British Broadcasting Corporation, *How much raw sewage is released into rivers and the sea, and what are the rules?* Accessed 2024-20-06. [Online]. Available: `https://www.bbc.co.uk/news/explainers-62631320`.

[103] C. A. Ezeigweneme, A. A. Umoh, V. I. Ilojianya and A. O. Adegbite, 'Telecommunications energy efficiency: Optimizing network infrastructure for sustainability,' *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 26–40, 2024.

[104] A. Abou el Kalam, 'Securing scada and critical industrial systems: From needs to security mechanisms,' *International Journal of Critical Infrastructure Protection*, vol. 32, p. 100 394, 2021, ISSN: 1874-5482. DOI: `https://doi.org/10.1016/j.ijcip.2020.100394`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S1874548220300585`.