National College of Ireland

Project Submission Sheet

Student Name:	Matthew Browne		
Student ID:	x21174415@student.ncirl.ie		
Program:	MSc/PGD in Cybersecurity	**Year:**	1
Module:	Network Security and Penetration Testing (H9NSPT)		
Lecturer:	Michael Pantridge MSc/PGD		
Submission Due Date:	15th August 2025		
Project Title:	Network Security and Penetration Testing CA2		
Word Count:	9370		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the library. To use other authors' written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:	Matthew Browne
Date:	15th August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Network Security and Penetration Testing (H9NSPT)

Your Name/Student Number	Course	Date
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	05/08/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Continuous Assessment Name	Network Security and Penetration Testing CA2
Student Name	Matthew Browne
Student ID	x21174415
Student Email	x21174415@student.ncirl.ie

Network Security and Penetration Testing (H9NSPT) CA2

Matthew Browne
Microsoft MVP & CITP
E-mail: *x21174415@student.ncirl.ie*

Contents

1.0 Abstract

Based on the requirements of our continues assessment we were required to undertake and demonstrate research techniques into defining a sample complex network setup for home, business or enterprise use, as part of this I was required to gather information pertaining to my network configuration alongside showcasing a design diagram of my network configuration. The network configuration should typically contain a router, a switch, access points, firewalls alongside any additional components such as laptops, desktops, servers, these are just some of the peripherals that were up for discussion as part of my paper. The goal of the exercise was to be able to articulate and explain the different elements that go into a complex network topology.

For my continues assessment I had the opportunity to choose the network, so I chose my home network as I believe it lives up to a complex standard incorporating many elements of a traditional business or enterprise network. Accompanying this I was to research three different attack vectors which could potentially be used to compromise my network or at least different sections or portions of it , alongside the comparison study of the attack vectors I was to showcase what type of mitigation techniques could be used to protect against the attack vectors while encompassing a summary of findings and conclusion and potential next steps.

1.1/1.2 Executive Summary & Scope

My report presents a realistic view on a typical small to medium sized enterprise network or at least the components that go into creating a similar network, the idea behind my paper is to use something I have actually setup based on industry experience and expertise. The scope of the assignment was to focus more on giving a rounded view into my network architecture , focusing on things like dhcp server's , dns server's , layer 3 switching , static and dynamic ip addressing , potential reserved address in the dhcp scope and even the switch , port and vlan configurations all while discussing the potential firewall configurations and setup , the focus was also on how to show this configuration in a diagram , using tools like draw.io I was able to create an accurate depiction of my network calling out specific like , workstations , servers , core networking , guest networking , lab networking , network storage devices and more all of these devices combine to bring together my network configuration and map.

1.3 Objectives

The objective alongside simulating , representing , showcasing and explaining the topology of the network and its contents was to call out three recent attack vectors and discuss their potential impacts on networks like mine in doing so by way of comparison to recent exploits which are publicly available which could be used to compromise the network and its associated devices , the other objective was to call out and discuss mitigation techniques which could be used not just in my network but in enterprise and home networks across the world , in other words looking at the attack vectors seeing how they fit into the overall viewpoint and discussing the mitigation techniques which can be used to prevent these types of breaches and compromises.

1.4 Network Descriptor

Describing networks can be both easy and difficult to begin we first have to understand the difference between networks both home and enterprise networks can be differentiated using different factors for example a home network will be part of a workgroup normally an enterprise network will be part of a domain , while this is not always exclusive you can have in some situation home networks being part of a domain but normally this is reserved for business or enterprise , next in understanding how computers work and differentiating them in both setups , Home networks normally do not have any management server where as enterprise networks will typically have at least one.

1.5 Justification for Choice

The reasoning behind choosing my own home network versus studying a enterprise network was simple , my home network and its creation was based on my experience and knowledge across information security backed by 300+ Certifications and a QQI Level 8 in computer networks and cloud infrastructure , I chose my home network as its just as complex as a enterprise network based on the article written by Trend net my home network could be classed as an enterprise network , why might this be the cause because my home network has more then one server , users login to my home network using a specified Active Directory username and password , alongside this I have group policies on my domain controllers controlling servers and workstation on my network , I've also incorporated logs across systems which include switches , firewalls , routers and data which traverses through my network is stored on central shares such as file servers and more , qualifying my network as a small to medium sized enterprise network. Alongside this for a home network to be classed as an enterprise network it also has to have some other specific characteristics such as you may have a dedicated virtual private network or perhaps you may have layer three switching which allows for a high configuration additional to this you may have power over ethernet switches which allows for the connection of wireless access points , all of which are usually found in an enterprise network , similar to what I currently have in my home network.

1.6 Network Setup Definition

Network setups can be classified in multiple ways and often this id down to different characteristics things like building size , scalability , security , network performance , speeds required and cost all contributed and determine the scale and size of your network , when we look at size it can be anything from 1-20 devices this would normally be categorized as a home network , where security plays a key role this can often be integrated into your router configuration when using home based networking equipment , business and enterprise's normally use dedicated firewalls , intrusion detection and prevention systems alongside proxy servers all of which differentiate them from home networks , network performance is another thing where in a typical home network you may just have your router emitting 2.4 , and 5 Ghz channels this is normally not considered

enterprise level even if you are using the higher scaled encryption methods for securing your local area network and your wireless area network business and enterprises often look to Wi-Fi 6 and Wi-Fi 7 speeds over wireless connections , chances are there using enterprise grade equipment from manufacturers like , cisco , juniper , Fortinet , dell ubiquity , Aruba , Omada and so on often these won't be found in your average household ultimately network setup and definition can also come down to cost as well consumer grade equipment is normally not destined to last anything more than a couple of years where as business and or enterprise grade equipment could last in excess of 2 decades depending on manufacturer and quality , so in truth the definition of a network setup is not solely defined on one single characteristic it's a combination of multiple requirements. [1]

Home Vs Work Comparison

If we take a look at the comparison of a home vs work network, we can see the following

Requirement	Home	Work
The main purpose	Small scale personal devices are used for browsing, watching movies,	Large scale usually for achieving business workflows and operations
Hardware Types	Usually, a consumer router	Usually enterprise switches, routers, firewalls and servers
IP Address Management	Automatic DHCP from consumer router	Both Automatic and Manual Ip addressing normally segregated networks with custom access control lists and routing.
Login Types	Local username and passwords none managed	Centralized username and passwords managed by Active Directory
Security Configuration types	Usually WPA2/3 for personal devices with little to no configurations	Usually Enterprise level security configurations, access controls, intrusion detection and prevention systems and so on.
Access internal and external	Usually achieved only through port forwarding.	Usually achieved through virtual private networks, remote desktops and other secure protocols
Maintenance	Usually very little oversight or requirements such as enabling automatic updates on computer and ISP provided router.	Usually managed by multiple IT teams or a IT Administrator, regular updates, Monitoring and Maintenance and completed.

1.7 Researched network types

1.7.1 Home Networks

Based on my readings from "Advancing the State of Home Networking" I was able to understand that most home networks cannot handle complex tasks, most of them contain a mix of devices which often have compatibility issues and rely heavily on automatic updates. Privacy from a home networking point of view is reliant on the out of the box internet service providers built in configurations , due to the nature of home networking being ad-hock we can see that the amount of manual oversight required can often lead to very disorganized and unmanageable in comparison with work networks , the capabilities and understanding from a user's point of view often leads to miss understandings in how much capabilities there networks can actually handle lastly due to sheer volume of technical controls required to manage devices from a home network this often leads to users being unable to define specific policies making them reliant on vendors for their security needs. In home networks we were able to see from the research that often connectivity issues and complex setups lead to user frustration this is mostly the case in unmanaged networks. We were also able to see that while home networking products are being bought users would frequently return them due to their complexities even if the products were working. Alongside this, due to the sheer volume of providers in a home network users would often spend time on contacting incorrect providers to get resolutions to problems despite self-help guides being available. [2] [3]

1.7.2 Work Networks

Based on my readings from "Constructing, Configuring, and Hardening a Medium-sized Business Network Infrastructure " [4] I was able understand that most enterprise and or work networks as an individual or business you need to focus on understanding the network design and architecture principal and protocols play a key role in this , technologies and protocols like Nat , Dhcp , Routing and switching all combine to incorporate as part of the overall design and configurations not understanding the fundamentals of how the design is put together is what can cause gaps in the overall security all combine to provide for a more focused view on the actual steps of setting up these processes of starting your network and architecture configurations things like purchasing hardware reasoning behind it , configuring the software defined networks , knowing what your Ip addressing and or pools are going to look like subnets , masks , address ranges , reservations alongside knowing how and where to implement firewalls were all key elements in knowing the differences between personal vs work environment. The paper also looked at how teams can face limitations in hardware reliability , throughput and performance on networks and latency among other things , it also spoke about how connectivity and troubleshooting can contribute to complex networks , from the paper I was able to get a grasp on what the practical elements of networks setup in an enterprise environment would look like and how to integrate that along with my own theoretical knowledge for building out and identifying gaps in my own enterprise version of a corporate environment.

Both home and work network investigations and analysis provided different perspectives and topics to understand but both followed guiding principles, and they were to understand the fundamentals of networking and creation of architectures.

1.8 Network Setup Aspects

Some not all of the key network elements for setting up a home network will be to consider things like placements of network comms cabinets , will there be a requirement to mount the network cabinets to the walls or ceiling , next what will the network cabinet size you will need to get will you have a small medium or large sized cabinet these come in form factors like 9U , 16u , 36u [5] and so on , The kind of equipment that will be feeding into the cabinet will often dictate the sizing , next thing as a Networking specialist you will need to think about the speed required will you need a Cat5 or Cat6 cable connection , understanding where patching will take place at this point will be paramount , networks require a level of redundancy and backups considerations into weather you will have one or maybe two internet connections present on the premises will also dictate the level of hardware required , often companies opt to have dual connections and in some cases have these networks segregated example , your primary connection might be your eir or virgin media , your secondary connection might be your star link or Vodafone , ensuring proper backup and redundancy is in place is key as you will want a failover connection in my case I use eir as the primary internet connection and star link as the secondary connection.

This brings us onto the next point will you require a failover , a failover internet connection is where systems switch from one provider to another seamlessly without any intervention on the user or individuals part this normally consists of your enterprise IT Administrator configurating this using a dedicate firewall allowing for dual wan connectivity and failover , with cost being a key factor for both home and enterprise networks often you will find that home users opt for a simple setup where as enterprise users will normally have an architecture behind it. So for the network setup to recap we have spoken about the cabinet size the internet connections the cabling speeds , the redundancy requirements , and the internet service providers (ISP) for short the next thing will be the requirement of some layer 3 switching and the use of software defined networking in these , layer 3 switches often incorporate many different tolling and abilities some of these tooling's will allow you to control network ports on switches , create virtual networks , tag ports , and create specific allowed and blocked lists controlling access between networks.

1.9 Network Setup Process

Setting up a network can be difficult to define due to the level of complexities , Microsoft [6]makes this easier by defining the process and the setup procedures if your setting up a small business network , this can be broken down into 6 stages this can be broken down into planning what do you actually want to achieve for your network configuration , preparation what kind of hardware and software elements are you going to design or integrate , configuration what sort of pools , ip addressing , domains and workgroups might you create alongside securing the different elements such as access control lists , firewall rules , policies and more , you might also want to initiate some testing and redundancy as part of the overall design and then you will need to think about maintaining the network.

Some of the things you need to consider are your goals versus what you currently have in place things like topology such as routers switches and access points all combine to guide your decisions as these are cost factors , the ability to be able to purchase all at once versus expanding over time is a huge contribution factor , the other thing is the quality of the hardware your going to use this is a case of consumer vs enterprise grade again another important factor to consider things like lifespan and quality are also important , Microsoft defines the core requirements as networking such as Ip addressing , switching routers , Active directory domains or workgroups and file sharing servers or network attached storage devices all of these will contribute toward costs of setting up the network.

The next thing you need to look at when setting up and configuring your network are things like the cabling standards and throughputs knowing if you're going to need to use power over ethernet switching or layer 2 and 3 switches without any poe functionality. Lastly, you're going to need to think about security, things like intrusion detection systems, firewalls and intrusion prevention systems all factor in as part of the network architecture and design understanding how you want to secure your network configurations will be critical to its operations.

2.0 Network characteristics

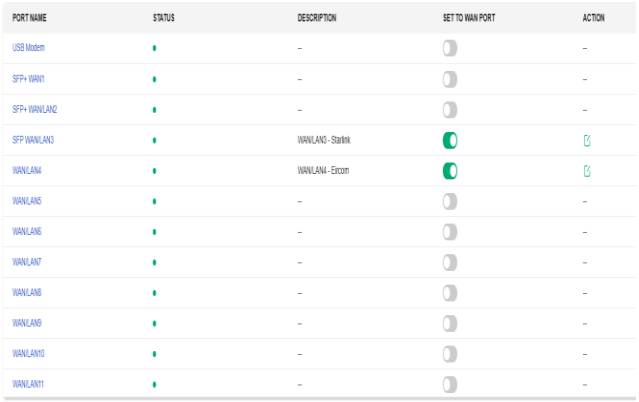
My network consists of multiple layers Routers, firewalls, switches, access points, patch panels, servers and Network attached storage devices. All of which comprise my full network configuration alongside this my network also consists of multiple virtualized networks with the abilities of software defined networks I don't just have a single network, but I have multiple networks performing different operations. My network operates using 2 different internet service provider connections one from Eircom which is a fibre connection for primary link one from Starlink which is a satellite connection for my secondary link both internet service provider connections have static Ip addresses and both internet service providers have failover so if one goes down the other kicks in.

Additional to this I have multiple Vlan ID'S, scopes , dhcp reservations and access control lists and firewall rules between the networks ensuring scalable , secure controlled environments , this all supported my decision to use my network as an example as it goes beyond your standard home network.

2.1 Router Configuration Layer

Device Name	IP Address	Model	Version Number	Mac Address	Reference Link

Omada Router	192.68.0.1	ER8411 v1.0	1.3.1 Build 20250515 Rel.63712	B0-19-21-44-48-3E	https://www.tp-link.com/ae/business-networking/vpn-router/er8411/
Starlink Router	192.1678.0.3	Starlink Router (Gen 3)	2025.07.21.mr60152.1	n/a	https://www.starlink.com/

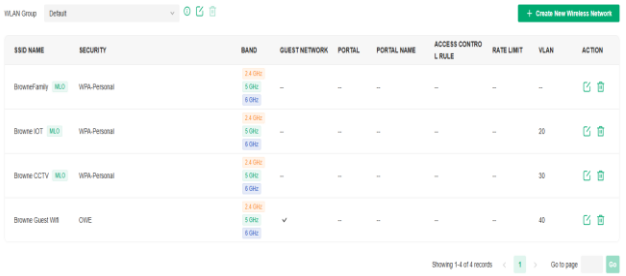


2.2 Virtual Network Lan Configuration Layer's

Network Name/IP Pool	VLAN ID	Description for use
Lab Network is 192.168.50.1/24	Vlan ID 50	This network is used for lab testing scenarios
IOT Network is 192.168.20.1/24	Vlan ID 20	This network is used for IOT Devices
Guest Network is 192.168.40.1/24	Vlan ID 40	This network is used for Guests connecting into the network
CCTV Network is 192.168.30.1/24	Vlan ID 30	This network is used for CCTV Cameras
Home Network is 192.168.0.1/24	Vlan ID 1	This network is core network for standard devices

2.3 Virtual Network WLan Configuration Layer's

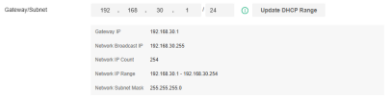
SSID Name	Network Name/IP Pool	VLAN ID	Bands Supported	Description for use
Browne IOT	IOT Network is 192.168.20.1/24	Vlan ID 20	2.4 GHz 5 GHz 6 GHz	This network is used for IOT Devices
Browne Guest Wi-Fi	Guest Network is 192.168.40.1/24	Vlan ID 40	2.4 GHz 5 GHz 6 GHz	This network is used for Guests connecting into the network
Browne CCTV	CCTV Network is 192.168.30.1/24	Vlan ID 30	2.4 GHz 5 GHz 6 GHz	This network is used for CCTV Cameras
Browne Family	Home Network is 192.168.0.1/24	Vlan ID 1	2.4 GHz 5 GHz 6 GHz	This network is core network for standard devices



2.4 Virtual Networks Lan configuration detailed.

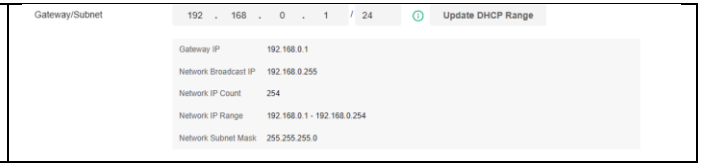
2.4.1 CCTV Network

Vlan ID	30
Gateway IP:	192.168.30.1
Network Broadcast IP	192.168.30.255
Network IP Count	254
Network IP Range	192.168.30.1 - 192.168.30.254
Network Subnet Mask	255.255.255.0
Image	

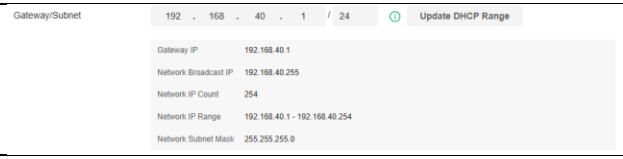


2.4.2 Core Network

Vlan ID	1
Gateway IP:	192.168.0.1
Network Broadcast IP	192.168.0.255
Network IP Count	254
Network IP Range	192.168.0.1 - 192.168.0.254
Network Subnet Mask	255.255.255.0

Image	

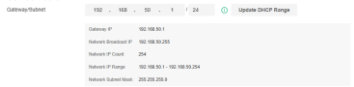
2.4.3 Guest Network

Vlan ID	40
Gateway IP:	192.168.40.1
Network Broadcast IP	192.168.40.255
Network IP Count	254
Network IP Range	192.168.40.1 - 192.168.40.254
Network Subnet Mask	255.255.255.0
Image	

2.4.4 IOT Network

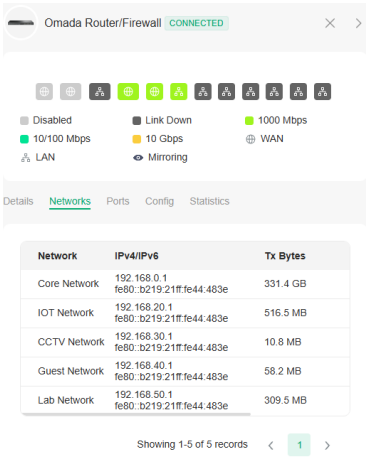
Vlan ID	20
Gateway IP:	192.168.20.1
Network Broadcast IP	192.168.20.255
Network IP Count	254
Network IP Range	192.168.20.1 - 192.168.20.254
Network Subnet Mask	255.255.255.0
Image	

2.4.5 Lab Network

Vlan ID	50
Gateway IP:	192.168.50.1
Network Broadcast IP	192.168.50.255
Network IP Count	254
Network IP Range	192.168.50.1 - 192.168.50.254
Network Subnet Mask	255.255.255.0
Image	

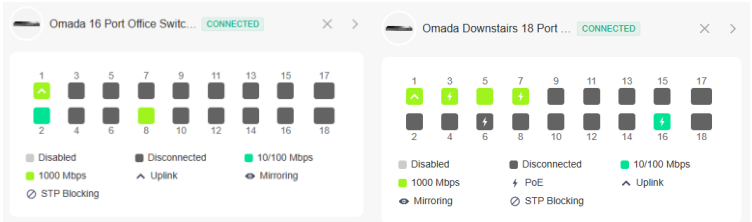
2.4.6 Firewall Configuration Layer

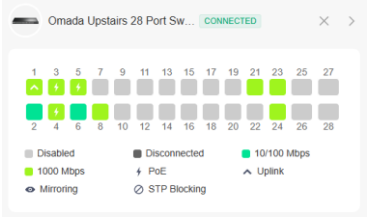
Device Name	IP Address	Model	Version Number	Mac Address	Refference Link
Omada Router/Firewall	192.168.0.1	ER8411 v1.0	1.3.1 Build 20250515 Rel.63712	B0-19-21-44-48-3E	https://www.tp-link.com/ae/business-networking/vpn-router/er8411/



2.4.7 Switch Configuration Layer

Device Name	IP Address	Model	Version Number	Mac Address	Refference Link
Omada 16 Port Office Switch (Non-POE)	192.168.0.119	SG2218 v1.20	1.20.9 Build 20250307 Rel.72554	00-31-92-76-3F-EE	https://www.omadanetworks.com/ae/business-networking/omada-switch-smart/sg2218/
Omada Downstairs 18 Port Switch (POE)	192.168.0.8	SG2218P v1.20	1.20.9 Build 20250307 Rel.72554	5C-62-8B-73-A4-74	https://www.omadanetworks.com/us/business-networking/omada-switch-access/sg2218p/
Omada Upstairs 28 Port Switch (POE)	192.168.0.149	TL-SG3428MP v5.0	5.0.16 Build 20250430 Rel.43731	AC-15-A2-06-4F-CD	https://www.tp-link.com/us/business-networking/managed-switch/tl-sg3428mp/





2.4.8 Access Point Configuration Layer

Device Name	IP Address	Model	Version Number	Mac Address	Reference Link
AP-Utility Old	192.168.0.120	EAP225(EU) v3.0	5.1.6 Build 20240313 Rel. 43415	90-9A-4A-D2-AD-CE	https://www.tp-link.com/uk/service-provider/business-wireless/eap225/
AP 2nd TV-Room Old	192.168.0.5	EAP225(EU) v3.0	5.1.6 Build 20240313 Rel. 43415	90-9A-4A-D2-AE-C6	https://www.tp-link.com/uk/service-provider/business-wireless/eap225/
AP Garden	192.168.0.2	EAP225-Outdoor (EU) v1.0	5.1.6 Build 20240313 Rel. 43415	60-A4-B7-E4-B0-E2	https://www.omadanetworks.com/ae/business-networking/omada-wifi-outdoor/eap225-outdoor/
AP 1st TV-Room New	192.168.0.153	EAP653(EU) v1.0	1.1.3 Build 20250326 Rel. 59878	A8-6E-84-57-40-2A	https://www.tp-link.com/uk/business-networking/omada-sdn-access-point/eap653/
AP Hallway New	192.168.0.210	EAP653(EU) v1.0	1.1.3 Build 20250326 Rel. 59878	F0-09-0D-02-7C-DC	https://www.tp-link.com/uk/business-networking/omada-sdn-access-point/eap653/
AP Kitchen New	192.168.0.152	EAP653(EU) v1.0	1.1.3 Build 20250326 Rel. 59878	A8-6E-84-57-3D-E2	https://www.tp-link.com/uk/business-networking/omada-sdn-access-point/eap653/
AP Office New	192.168.0.209	EAP653(EU) v1.0	1.1.3 Build 20250326 Rel. 59878	F0-09-0D-70-99-58	https://www.tp-link.com/uk/business-networking/omada-sdn-access-point/eap653/

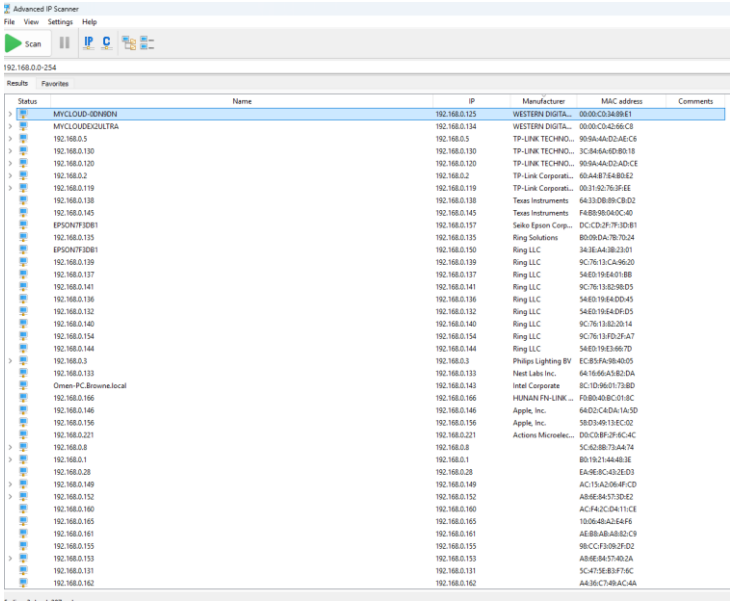
2.4.9 Storage Devices (Nas)

Device Name	IP Address	Model	Version Number	Mac Address	Refference Link
MYCLOUD-0DN9DN	192.168.0.125	MYCLOUD-0DN9DN	?	00:00:C0:34:89:E1	https://support-en.wd.com/app/products/product-detailweb/p/1369
MYCLOUDEX2ULTRA	192.168.0.134	MYCLOUDEX2ULTRA	?	00:00:C0:42:66:C8	https://support-en.wd.com/app/products/product-detailweb/p/130

2.5 Summary table Peripheral Devices on networks (Sample)

Device Name	IP Address	Mac Address	Manufacturer	model	Os version	Release date	Main service application	Refference
Driveway Camera	192.168.0.139	9C:76:13:CA:96:20	Ring LLC	Spotlight Cam Plus Plug-In	cam-1.24.13800	28 July 2025	CCTV Camera	https://ring.com/eu/en/products/battery-doorbell-pro
Front Door Camera	192.168.0.137	54:E0:19:E4:01:BB	Ring LLC	Battery Video Doorbell Pro	cam-1.24.13800	22 July 2025	CCTV Camera	https://ring.com/eu/en/products/battery-doorbell-pro
Garden Front Camera	192.168.0.141	9C:76:13:82:98:D5	Ring LLC	Spotlight Cam Plus Plug-In	cam-1.24.13800	28 July 2025	CCTV Camera	https://ring.com/eu/en/products/spotlight-cam-plus-plug-in
Garden Left Camera	192.168.0.136	54:E0:19:E4:DD:45	Ring LLC	Spotlight Cam Plus Plug-In	cam-1.24.13800	28 July 2025	CCTV Camera	https://ring.com/eu/en/products/spotlight-cam-plus-plug-in
Garden Middle Camera	192.168.0.132	54:E0:19:E4:DF:D5	Ring LLC	Spotlight Cam Plus Plug-In	cam-1.24.13800	28 July 2025	CCTV Camera	https://ring.com/eu/en/products/spotlight-cam-plus-plug-in
Garden Right Camera	192.168.0.140	9C:76:13:82:20:14	Ring LLC	Spotlight Cam Plus Plug-In	cam-1.24.13800	28 July 2025	CCTV Camera	https://ring.com/eu/en/products/spotlight-cam-plus-plug-in
Hallway Downstairs Camera	192.168.0.154	9C:76:13:FD:2F:A7	Ring LLC	Indoor Camera 2nd Gen	cm-17.1.1200	28 March 2025	CCTV Camera	https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in
Hallway Upstairs Camera	192.168.0.144	54:E0:19:E3:66:7D	Ring LLC	Indoor Camera 2nd Gen	cm-17.1.1200	28 March 2025	CCTV Camera	https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in
Kitchen Camera	192.168.0.135	B0:09:DA:7B:70:24	Ring LLC	Indoor Camera 2nd Gen	cm-17.1.1200	28 March 2025	CCTV Camera	https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in
Pink TV Room Camera	192.168.0.121	4C:60:BA:52:2E:88	Ring LLC	Indoor Camera 2nd Gen	cm-17.1.1200	28 March 2025	CCTV Camera	https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in
Purple TV Room Camera	192.168.0.122	5C:47:5E:B3:F7:6C	Ring LLC	Indoor Camera 2nd Gen	cm-17.1.1200	28 March 2025	CCTV Camera	https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in

Utility Room Camera	192.168.0.123	F0:09:0D:70:99:58	Ring LLC	Indoor Camera 2nd Gen	cm-17.1.1200	28 March 2025	CCTV Camera	https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in
Philips Light controls	192.168.0.3	EC:B5:FA:98:40:05	Philips Lighting BV	Lighting Controls	1972076030	21 July 2025	Lighting Controls	https://www.philips-hue.com/en-gb/p/hue-bridge/8719514342583
Nest Thermostat	192.168.0.133	64:16:66:A5:B2:DA	Nest Labs Inc.	Heating Controls	Version 6.4-5	14 July 2025	Heating Controls	https://store.google.com/ie/product/nest_learning_thermostat_3rd_gen?hl=en-GB&pli=1
Omen-PC.Browne.local	192.168.0.143	8C:1D:96:01:73:BD	Intel Corporate	System Model OMEN 30L Desktop GT13-0xxx	Microsoft Windows 11 Pro Version 10.0. 26100 Build 26100	May 2020	Windows Personal Computer	https://support.hp.com/us-en/document/ish_5054198-5054246-16

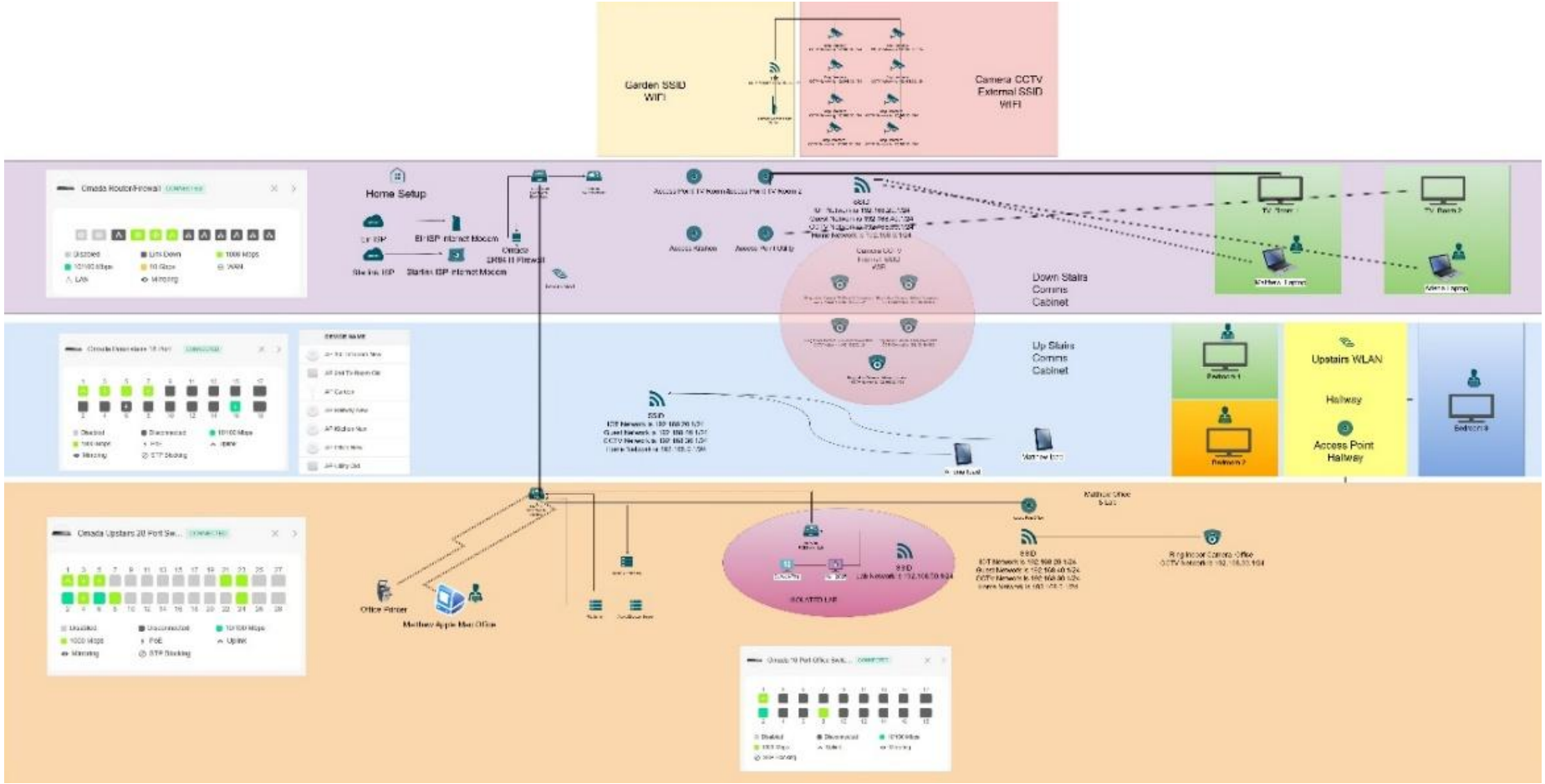


2.5.1 Network Type/Purpose

The Purpose of my network is to be able to allow me to manage devices at scale this includes devices such as windows operating systems, televisions, tablets, laptops and storage devices. With my network I am also to ensure redundancy via two internet connections ensuring we always stay online , the ability to have more than one virtualized network also allows me to expand and secure my networks having purposely built networks for camera's internet of things devices , core network for day to day devices and more , being able to manage desktops and laptops in an Active Directory environment at scale allows me to manage the device configurations , networking and security policies ensuring my devices stay secure permanently. I also have the ability to ensure our family's storage and precious pictures , documents and files stay secure through storage servers and Raid configurations all of this compiles to bring together my network and configuration in an enterprise like manner.

2.5.2 Network Diagram

Diagram Of Full Network: For this I used Draw.io to create the diagram which is an open-source diagram tool used by IT Professionals to draw out their diagrams.



2.5.3 Network Assumptions

Based on the large footprint of my network which includes Core networking like my three switches 2 of which are power over ethernet , my integrated router/firewall , my dual Cabinets one for downstairs and one for upstairs , and my many virtualized software defined networks such as Lab Network is 192.168.50.1/24 for configuring and testing out things in my lab , my IOT Network is 192.168.20.1/24 , for ensuring things like my robot vacuum , lawnmower , lighting and fridge all stay secure on the network. The ability to have an isolated network for both Guests and CCTV cameras allow me to ensure that segregation is occurring and keeps my networks from being open to attackers ensuring confidentiality, integrity and availability across systems. Lastly with the assumption that my Home Network, which is 192.168.0.1/24 has its on network as well I am able to separate out the different functions across a broad range of systems and networks.

2.6 My Chosen Attack Vectors and Mitigation Strategies

Based on the review of my current infrastructure and networking components I was able to identify three different realistic attack approaches that could be conducted if an attacker wanted to exploit my network for vulnerabilities and gain access to different systems , this represents a realistic approach in terms of real world scenarios each example included a real world scenario of where this actually happened.

2.6.1 Example one Scenario Chosen, (IOT Devices)

Due to the nature of internet of things devices these are often a primary target for attackers as they can sometimes allow an attacker to gain access to a network and do some reconnaissance and or discovery these can be considered both hardware and software appliances and would have various levels of protection required.

2.6.2 Example two Scenario Chosen, (Access Points)

where attackers may be able to gain unauthorized access are by spoofing my access point SSID’s or using an Evil twin and rouge access points, this would essentially allow an attacker to intercept my traffic as I would be connecting to the wrong access point its important to state that these would and could also be covered under hardware and software best practices.

2.6.3 Example three Scenario Chosen (Western Digital)

where attackers might be doing reconnaissance work on a network if they discover vulnerable network storage devices such as that of the western digital EX2 Ultra or Home they may look to use public vulnerabilities based on their firmware (Hardware) or default login credential’s (Software) to steal or hold Ransome a person’s files.

Attack Method/Vector	Reasoning/Justification	Differentiator's/Comparison
Exploitation of IOT Devices	Due to the nature of IOT devices as these are things like , robot hoovers and mops , robot lawnmowers , fridges and freezers , washers and dryers often these are devices which are just connected to individuals and business networks , there normally setup using the quickest method and once online there normally forgotten about in terms of updates and upgrades as these devices can often be setup with minimal authentication methods and supports the pose some of the highest risks	Due to the nature of IOT devices in comparison to both access points and network attached storage devices these devices are usually weak devices with very little to no security attackers will often target these as there exposed to the internet and often not maintained or managed centrally , essentially in terms of the CIA Triad attackers are attacking the integrity/Availability of the IOT devices.
Access point impersonation	Due to the nature of access point's and the abilities for places like coffee shops , airports , shopping centers and more wanting to provide free wifi networks like public hotspots to the public often these form as prime targets to allow attackers to duplicate an mimic real world systems e.g. some users could think their connecting to a secure reliable connection but in fact there actually connected to rogue or spoofed access points , attackers are getting to good they can often replicate the landing pages for these devices and end up stealing users information.	Due to the nature of access points and users wanting to get access to high speed wifi often in areas of low network coverage for 4g , 5g networks users will use these open networks to gain access to social media platforms to conduct there media presence this plays straight into attackers abilities to be able to exploit the user behavior , mainly attackers focus on wireless protocols here to conduct there reconnaissance and credential stealing , this is a significant different to prying on vulnerable devices or storage systems rather the attacker is goading individuals and playing on their behaviors as would be expected in situations with little network coverage.
Network attached storage device exploitation	Due to the nature of network attached storage devices and server storage solutions individuals and businesses are often storing large quantities of data in these storage solutions just like what my western digital home and ultra Nas's do , these are primary target for attackers to hold ransom as they propose an ability for them to have financial gain should they be able to extort money from business and individuals.	Due to the nature of what is usually stored and how its stored both business and individuals store their data usually on Network attached storage devices like WD or even Storage servers if attackers can exploit these devices there able to gain significant advantage over these users allowing them to extort money from them and holding them to ransom this differentiates this type attack from the other two it focuses on data integrity and confidentiality as if the attackers gain access they can control the outcome if the individual or business does not have preventative measures put in.

2.7 Table Summary Characteristics of Each Attack Type/Vector

2.7.1 Device Type	2.7.2 Motives	2.7.3 Attack Technique	2.7.4 Targeted Devices	2.7.5 Attack Vulnerabilities	2.7.8 Attack Exploits	2.7.9 Cve Number/ Exploit Detail	2.7.10 Real World Incident Example	2.7.11 Ways to Mitigate At Home and At Work
IOT Devices such as the below are all open to exploitation from attackers. • Ring Cameras • Nest Thermostats • Lighting such as Philips Hue • Samsung Family Hub Fridge/Freezer	Some attackers may want to gain internal access to systems so they can hold them ransom. Some attackers may want to use IOT devices for botnet purposes such as attacking other networks and systems. Some attackers may want to steal the Data and post it to the darknet/web.	Attackers may use default credentials such as those posted in manuals and manufacturer documentation. They may try to brute force these credentials and they may try to use outdated firmware that have exploits publicly available.	Systems like my ring cameras, Philips hue bridge and nest thermostat are all viable options for attacking as they could be used to attack other systems.	Some of the common vulnerabilities used in the attacks can be weak default passwords. Exploitation of older firmware versions and sometimes unencrypted communications methods may also be used to gain access to systems.	Hue Zigbee buffer overflows are often used to make devices unavailable. Mirai malware is a classic example of what an attacker could use to get your devices to attack others.	2020, 6007,	In 2016 Mirai Botnet was able to disable key platforms like X and Netflix using hijacked IOT Devices. [7]	Ensuring you have properly configured segmentation in your network and access controls lists are one preventative method. Turning off and disabling inter Vlan routing between Vlans will also prevent attackers from traversing across systems. Ensuring you keep devices updated and on regular maintenance schedules are some good ways to be proactive in your defenses and mitigation methodologies. Turning off public internet access to specific devices where not required and ensuring your devices remain behind a firewall or only placed in a DMZ where required is a potential preventative method.

Access points such as the below or all open to exploitation for attackers as each manufacturer posts default login credentials in their guides. • Aruba • Cisco • Omada • Juniper	Utilizing man in the middle attacks and session hijacking is often a favorited method. Attackers may want to get access to important credentials so that they can steal, copy , manipulate and change data within your environment. Attackers may want to retrieve key information such as financial credit cards or Personal identifiable information and this is why Man in the middle attacks can be so compromising to individuals.	Evil Twin attack using rogue access points or spoofed access points. Lateral movement between networks and Vlan's such as traversing across network subnets.	Access points such as The EAP 653 from Tplink Omada enterprise range can be a primary target for attackers among others. Any windows laptop Any windows desktop Any device with a wifi chipset/card.	Weak Wi-Fi encryption methods such as using standard wep configurations or easy to guess passwords or even open source unsecured wifi SSID's can all lead to a potential compromise.	KRACK or WPA2 Key Reinstallation Attacks	2017, 13077, 13088,	Key Reinstallation Attacks [8]	Ensuring you're using the latest WPA3 or enterprise level encryption across your Wifi SSID's. Enable security measures such as using Omada's rogue ap detection options as part of the setup and configuration within the controller. Turning Off SSID'S that do not need to be broadcasted aka enabling hidden networks.
Network-attached storage devices such as western digital are a primary target for attackers for Ex filtering data and exposing it for sale across the dark web. • WD My Cloud Ultra • WD My Cloud Home • Other Third-Party networks have attached storage devices.	Attackers may want to hold your files for a ransom until the ransom is paid. Attackers may want to delete your files to cause harm on purpose. Attackers may use your file storage for evil purposes such as planting incriminating material on your storage solutions.	Attackers will look for exposed unsecured access to panels such as browsing http access instead of https. Attackers may use dictionary attacks to target logins and brute force their way in. Attackers may also try to inject malicious payloads into the admin login page to brute force their way in and gain access.	Usually, attackers target these kinds of attacks on network-attached storage devices and storage servers.	If a network attached storage device is public facing attackers may look to access the web panels. Attackers may also look for devices with unpatched firmware and exploit these. By not ensuring your account is secure for your login s attackers may aim to circumvent 2FA authentication.	Authentication bypass tooling Incorrectly set login controls and restrictions. Brute force account attacks.	2018, 17153, Authentication Bypassing 2022, 22947, Access controls	Western digital Mass Nass wipe, this was where devices around the world got reset and wiped. [9]	The way of securing and ensuring your systems and data remaining safe were to: Turn of any non-required ports and remote access tooling to the Nas. Keep the Nas patched and update regularly. Putting the Nas behind a firewall and blocking any external access to it bar what's required. Have an independent backup solution to the Nas.

3.0 General Recommendations for Attack Prevention Methodologies

Based on my reading of the "National Security Agency" best practices document some of the key recommendations for attack preventions were to ensure software remained updated for both firmware's and operating systems, leveraging modern hardware and software security Av products, removing the use of simple unsecured passwords and authentication replaces these with more modern authentication such as MFA and 2FA. Remembering to practice safe data and backup hygiene is a must , ensuring you also exercise sound judgement in terms of limiting data access between systems and utilizing encrypted means of communications this means to ensure you see the lock symbol and https instead of http on websites and in general practicing safe behavior both online and offline these were just some of the attack prevention methodologies that could be used.

3.1 Best Practices

It's evident best practices and guidelines are something many home users do not follow and sometimes businesses , this is clear from the way in which home networks are setup , the "National Security Agency" [10] doe have an open source basic guide for home users this discusses the different elements that make up a home users environment such as their laptops , desktops , browser , routers , smart speakers and so on all of these are just some of the devices users can operate in their home but it's how the user operates them and secures them they should take notice of , things like using WPA2/3 for secure wifi access potentially including child safety nets such as fileting the connections on specific SSID's this shows potential for ensuring users secure there access to Wi-Fi connections and also filter out unsuitable content on their wifi networks. Another option is to ensure you have more then one copy of your data , data backup is not something that individuals remember to do remembering things like the CIA Triad is key when ensuring your important files remain safe. Limiting your IOT device access to the internet is also another key thing ensuring that these devices only have access to what they need to have access to is key to ensuring they remain secure , updating things like software and firmware versions prevent them from easily exploitable and is something users should do by default.

Another must do by individuals in a home setting environment and work environment is the recommendation of turning on automatic updates without these desktops and laptops operating systems remain open to vulnerabilities , keeping the operating system updated is important element and prevents them from being exploitable. Key to keeping your operating systems updated you need to do the same with your networking equipment this prevents them from being abused by external actors ensuring that your using the latest firmware , separating out network access from internal trusted devices and external unknown devices is key to ensuring that you minimize vulnerabilities. Wi-Fi security is a key element of any home network ensuring that you isolate and segment these from each other is important keeping your IOT and Camera network separate this is because IOT devices are often considered less secure than Camera's and they should not be able to interconnect or interact between each other.

A key area in which best practices should be followed is around firewall configuration and setup , this applies to both home and work networking solutions and security safeguards ensuring that proper policies and security solutioning such as Edr Mde and Av are implemented is key this prevents systems from being breached and exploited if they are connected to any external networks such as the world wide web. Security products have become a key element of both network types ensuring you have the right product and safeguards implemented is also key preventing against malware, ransomware and spyware is key in terms of ensuring your systems and devices remain safe when connected to the internet. Knowing when to implement standard vs admin accounts is another key element this prevents escalation of privileges so that standard users cannot perform admin tasks these should be separated out to allow for maximum safeguards. While all of these are valid best practices for both home and work networks it ultimately comes down to exercising good judgement in design and architecture of systems, this should be noted when setting up and configuring them taking into consideration some of the best practices outlined in the document.

3.2 Guidelines

Following guideline like the "National Security Agency" best practices for securing your home network allows individuals to understand where they should be focusing their efforts for securing their home networks , it focuses on secure router configurations and placements of devices on the network , it also focuses on how devices should be secured and the required maintenance levels for devices on a home network. It looks at the best practices around Wi-Fi security and ensuring individuals follow basic security hygiene, it explains how segmentation and separation across the home networks ensures bad actors cannot traverse across systems therefore providing more robustness for systems. It reminds users the importance of data backup and having more than one copy of data across systems and devices for redundancy purposes, it also looks at how individuals can limit their use of admin credentials where not needed to prevent malicious actors from elevating permissions on devices providing for simpler cyber hygiene. [11]

Following guidelines like the "Nist Cybersecurity Framework CSF 2.0" allows an organization or enterprise network to organize risks into categories enabling them to prioritize the risks and conduct risk reduction exercises , the do this by building out profiles on there systems for e.g. current vs target it enables to create maturity assessments allowing them to actually gauge where they currently stand and create a roadmap to where they want to be. Understanding where each responsibility lies how to they can create a clear governance roadmap to where they need to be helps them to clear easy win tasks and focus on more technical requirements. Nist also allow companies to create a continues improvement framework which means they can track and eliminate security threats there for improving there overall security posture , this is significantly relevant in terms of mitigating and preventing threats on networks. By using guidelines like Nist it allows the organization to utilizing a common language and effort that all cybersecurity professionals should understand and be able to implement to alleviate threats to the organizations networks. [12]

In essence both guidelines offer best practices to enterprise environments and home environments , there key focus on risk based eliminations and eradication ensuring that a more layered and proactive approach is taken to cyber hygiene and standards. While they

both offer similar approaches it can be assumed that there guiding principles are closely aligned while maintaining a separation based on both size and control factors if we take a quick look at the comparisons we can see the differences. The key takeaway for me for both of these documents was organizations should focus more on a structured and more resilient alignment toward Nist 2.0 framework and Home users should focus more on security hygiene , both came across with a single and compelling theme and that was applying layered security but in a consistent manner weather at home or at work , doing this will allow users and organization to reduce there overall attack surface across devices , systems and login's.

Key Theme	Organizational (NIST CSF 2.0)	Home Network (NSA CSI 2023)
Risk controls	Based on business requirements and standard operating procedures.	Standard network isolation recommendations out of the box configurations.
Management	Focuses on using a Tiered approach.	Focuses Soley on limiting Admin elevations.
Configurations	Focuses on hardening systems as a whole bigger picture thinking.	Focuses Soley on basic security hygiene e.g. default logins for devices rou software.
Access	Focuses on centralized access and prevention controls lean towards full governance with administration oversight.	Focuses on basic controls built into web logins, multifactor authentication an
Defenses	Enterprise level controls such as Edr, Mde, Enterprise AV Soc and Siem.	Focuses on Basic Firewall and disk encryption built into systems.
Improvements	Centrally Managed governed by Cab processes.	Setting up basic automatic updates built in patching nothing centrally manage

3.3 Legislation/ Standards

So, what does this all mean in terms of standards and legislations, it means that frameworks like Nist are focusing more on risk based outcomes essentially allowing organizations to tailor their controls based on there business requirements and how mature they are rather then strict controls based on regulatory requirements. Then if we look at the NSA recommendations we can see that its guiding users towards more basic security hygiene following simple practices which will allow them to secure there systems using built in tooling to devices e.g. strong Wi-Fi password essentially giving them a baseline rather then a regulatory requirement. We can see from the Nist documentation that its adopting an approach of interlinking between standards allowing organizations a more simplified approach to meeting multiple regulatory requirements and frameworks one such example is the " EU Cyber Resilience Act" [13] interlinking between Nist guidelines and best practices. Some of the guidelines and standards such as Nis2 , Dora and ISO/IEC 27002 all form clear standards which organizations and individuals should map back to these should be implemented in various organization settings where deemed appropriate.

3.4 Implications/Consequences

Due to the nature of Cyber Governance and more and more organizations making there people accountable for risks its now turned to a legal requirement in some countries and states as laws around cyber regulations are becoming more and more specialized e.g. Dora governance covers risk over financial services now in the European union some of the implications for not ensuring you have the relevant policies and procedures in place can be fines in excessive amounts or maybe event prison sentences. It also wont be surprising to see if best practice guidelines for home users with those such as the NSA could become the norm in future years as Cybersecurity for home users may also become a national risk factor for countries and nation states around the world.

3.6 Main findings

It's evident that home networks are a key requirement for users , yet they seem to be very difficult to manage if adding devices in an Ad-Hoc style often this has caused confusion for end users because the technical needs of the home users and the actual understanding of how a network is comprised often differs in a real world scenario and this can often lead to a very fragmented setup meaning individuals would need to re-think how they look at there home networking setups and needs. Its often evident that home users expose significant amounts of personal data due to the lack of security around there devices this is evident when they continue to setup and connect IOT devices to their networks and forgetting any additional security configurations , utilizing public forms as a means for technical support in a home network setup often leads users to getting unsolicited advice which can damage their setup. Its also evident that some home users prefer to offload there storage needs to cloud services providers instead of utilising home network attached storage devices , this is due to the complexities around setup and configurations and the end users not understanding or having the mindset to setup and configure these devices.

In comparison with there counterpart for work networks , work networks often consist of at least one managements servers , this is normally used for user account and security policy configurations , alongside this this allows for a centralized management of systems on a network , group policies allow IT Administrators to control all devices ensuring they stay secure and compliant in support of this most work and enterprise networks bake in security as part of the configuration utilizing items like firewall's , proxy servers , intrusion detection systems and intrusion prevention systems all allow for a more unified secure setup in comparison to a home network which is usually add-hoc. The differences between home vs work networks can also be seen in the scalability while users in home environments continue to add devices to there network often work networks are segmented , segregated and managed centrally using specific scopes and subnets , the same cant be said for home networks as normally there all thrown onto the one network.

3.7 Limitations

Although all these guidelines, best practices and principles represent a requirement for governance , controls , safeguards and enforcement mechanisms for utilizing frameworks it is evident that in the case of Nist controls and guidance that they are more flexible rather than directive , Nist in particular looks and what an individual or organization should look to achieve rather then how they would actually achieve the controls this essentially leads to confusion around implementing the compliance requirements for both individuals and organizations , due to the lack of limitations around how the guidance documents for both Nist and NSA can be perceived it should be noted that there guidelines more than regulatory requirements this can also lead to confusion for implementation unless organization's higher individuals with these expertise. It's also evident that the Nsa guidelines are just that guidelines they're not enforceable actions more their advisory guidelines due to the fact that these don't serve a purpose beyond baselines for individuals it evident that they could be ignored and may only provide for personal recommendations not absolute law. Its also evident from the documents that both

documents while one is more advanced than the other still imply that the individual or organization would need a substantial level of technical acumen often this is not found unless the individual in question has a high level of comprehensive experience around cybersecurity , this two can lead to minimal implementation and can cause a serious limitation around home and enterprise networking especially in terms of implementation in real world environments due to a lack of proficiency and financial availabilities access to experience resourcing to setup the control for both users or organization. It was also evident from the documentation that more work would be required if you were to map back each recommendation and best practice this also adds significant cost to what is an already expensive process for individuals and organization its realistic to assume that this limitation could be a serious problem to evaluating the threat landscape for an enterprise network and architecture design and development alongside being a barrier for individuals looking to setup scalable secure networks. The Nsa's documentation is also very presumptive in terms of user behavior it assumes the user has a technical mindset whereas the user may just be a parent , guardian , or adult who has basic information technology knowledge due to the human nature of most individuals is should assume that not every individual has the same technical acumen and this could certainly be a barrier and or limitation that being said the Nsa's guidance also doesn't support step by step guidance for individuals so its relevant to say that human factors will certainly undermine even the best of intentions here it should focus far more on providing actionable guidance with baseline settings for individuals. All in all, both documents serve as a guideline, that's what they have in common but what they also have in common is the level of technical depth that would be required to understand and implement both frameworks and guiding principles.

3.8 Conclusions

The assessment and research piece between the three attack vectors chosen IOT, Wi-Fi and Nas all showcased the need for individuals and businesses to ensure they follow best practices in the design and architecture phases of their home and work networks. It also showed the differences between networks setups this showed us that even if a network both business and home was following both best practices and recommendations it would likely still face some risks from vulnerabilities not yet discovered.

While we can always implement the best in both security hardware vendor technologies like intrusion detection systems , prevention systems and firewalls from providers like Palo , Fortinet , Cisco and TP-Link Omada alongside configuration of Edr , Mde and AV products with our software and hardware firewalls what remains critical at the end is the user understanding and training essentially the human element of operating and configuring systems. After reviewing the different elements its still easy to see how a Pentest activities may showcase some additional exposures to vulnerabilities and therefore showing us that you can only mitigate to a point security doesn't have a single golden bullet rather a layered defense strategy to prevent attacks and exploits.

4.0 Next steps

For my continues assessment if I had more time with it, I would have spent more time on diving further into various guidelines and best practices I researched as part of my assessment , one area I found really interesting was going through the documentation for both Nist and the national security agency both of these provided for interesting reading on the basics of setting up networks , securing the components and devices and interlapping between different frameworks and guidelines. I also found the exploration of trying to identify how the three attack vectors I chose on IOT, Wi-Fi and Nas could all be used as examples of where you could conduct a security gap analysis on your network. I would have liked to do a more in-depth analysis on the three to discover how each of the principles and guidelines could have been used to better map the baselines and requirements in both a home and enterprise networks. I also found the review of how Edr, Mde and soc and Siem tooling could be used to mitigate threats really interesting this could have served as a benchmark into understanding more how these platforms contribute toward securing the networks this would have been another interesting topic to dissect and delve into as part of the overall research paper. Another area I'm always keen on is discovering the role of education in terms of educating enterprises and end users this is something I felt you could have done a full research paper alone on, the educations around networking architecture, tooling, best practices and risk and compliance around limitations and averse effects which could occur due to bad practices , it was really evident to me throughout the research that creating roadmaps and mapping back security controls to each of the recommendations would have been important in mitigating threats this is something I could have also delved more into , lastly I would have really enjoyed looking more into the regulations side of cybersecurity best practices this would have helped me understand more about how you could ensure networks remain secure and complaint across enterprise and home networking architecture another key components of how the research could have been brought to a more conclusive ending if I could have mapped back the three technologies chosen versus how they differ in different scenarios e.g. Home Vs Work.

References

[1] trendnet.com, ""What Is the Difference Between a Home Network and an Enterprise Network?," Trendnet.com.," trendnet.com, June 2023. [Online]. Available: https://www.trendnet.com/press/resource-library/home-vs-enterprise-networks. [Accessed 2 August 2025].

[2] D. Wetherall, R. Mahajan, R. E. Grinter and K. W. Edwards, "Advancing the State of Home Networking," ResearchGate, June 2011. [Online]. Available: https://www.researchgate.net/publication/220421482_Advancing_the_State_of_Home_Networking. [Accessed 31 July 2025].

[3] Microsoft , "https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/set-up-your-small-business-network," Microsoft , 15 January 2025. [Online]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/set-up-your-small-business-network. [Accessed 2 August 2025].

[4] N. Briglia and C. R. Duell, “Constructing, Configuring, and Hardening a Medium-sized Business Network Infrastructure,” ResearchGate, April 2023. [Online]. Available: https://www.researchgate.net/publication/370288088_Constructing_Configuring_and_Hardening_a_Medium-sized_Business_Network_Infrastructure. [Accessed 31 July 2025].

[5] Server Room Environments, “https://www.serverroomenvironments.co.uk/server-rack-size-guide?srsltid=AfmBOorgesszYPl3cAea13UDDQKjXM7X2aF3ioL0yn6_jIrqDRziKQxz,” Server Room Environments, March 2021. [Online]. Available: https://www.serverroomenvironments.co.uk/server-rack-size-guide?srsltid=AfmBOorgesszYPl3cAea13UDDQKjXM7X2aF3ioL0yn6_jIrqDRziKQxz . [Accessed 31 July 2025].

[6] Microsoft , “https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/set-up-your-small-business-network,” Microsoft , 15 1 2025. [Online]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/set-up-your-small-business-network. [Accessed 1 August 2025].

[7] B. Krebs, “https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/,” 21 October 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/. [Accessed 2 August 2025].

[8] M. Vanhoef and I. DistriNet, “https://www.krackattacks.com/,” 16 October 2017. [Online]. Available: https://www.krackattacks.com/. [Accessed 2 August 2025].

[9] NIST, “https://nvd.nist.gov/vuln/detail/CVE-2022-22947,” NIST, 4 March 2022. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-22947. [Accessed 2 August 2025].

[10] “https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF,” National Security Agency (NSA), 22 February 203. [Online]. Available: https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF. [Accessed 1 August 2025].

[11] National Security Agency, “https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF,” National Security Agency, February 2023. [Online]. Available: https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF. [Accessed 4 August 2025].

[12] National Institute of Standards and Technology, “https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf,” National Institute of Standards and Technology, 26 February 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [Accessed 3 August 2025].

[13] European Commission , “https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act,” European Commission , 6 March 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. [Accessed 4 August 2025].

[14] TPLINK, “eap653,” TPLINK, [Online]. Available: https://www.tp-link.com/uk/business-networking/omada-sdn-access-point/eap653/ . [Accessed 2 August 2025].

[15] TPLINK, “eap225,” TPLINK, [Online]. Available: https://www.omadanetworks.com/ae/business-networking/omada-wifi-outdoor/eap225-outdoor/ . [Accessed 2 August 2025].

[16] Ring , “battery-doorbell-pro,” Ring , [Online]. Available: https://ring.com/eu/en/products/battery-doorbell-pro. [Accessed 2 August 2025].

[17] Ring , “spotlight-cam-plus-plug-in,” Ring , [Online]. Available: https://ring.com/eu/en/products/spotlight-cam-plus-plug-in . [Accessed 2 August 2025].

[18] Ring , “mini-indoor-security-camera-plug-in,” Ring , [Online]. Available: https://ring.com/eu/en/products/mini-indoor-security-camera-plug-in . [Accessed 2 August 2025].

[19] “hue bridge,” Philips , [Online]. Available: https://www.philips-hue.com/en-gb/p/hue-bridge/8719514342583 . [Accessed 2 August 2025].

[20] Google Nest, Google Nest , [Online]. Available: https://store.google.com/ie/product/nest_learning_thermostat_3rd_gen?hl=en-GB&pli=1 . [Accessed 2 August 2025].

[21] Western Digital , “https://support-en.wd.com/app/products/product-detailweb/p/130,” Western Digital , [Online]. Available: https://support-en.wd.com/app/products/product-detailweb/p/130 . [Accessed 2 August 2025].

[22] Western Digital , “https://support-en.wd.com/app/products/product-detailweb/p/1369,” Western Digital , [Online]. Available: https://support-en.wd.com/app/products/product-detailweb/p/1369 . [Accessed 2 August 2025].