Evaluation of Design and Security of the Network Infrastructure of a UK-Based SME

Daniel Jones
Arden University, Manchester Campus, Manchester, United Kingdom
dan_jones7@outlook.com

Abstract

This paper evaluates various aspects of design and security of the network infrastructure of an SME in the UK. It signifies how the best practices in network deployment from the literature can be used to acquire an efficient and secure communication network. The paper includes comparative analyses of a wide range of components of the network infrastructure, and different types of network diagrams. The paper also discusses various aspects of monitoring of the network infrastructure, highlights the critical parameters to gauge network performance, and demonstrates the use of different monitoring tools. The last section of this paper discusses security in the context of network infrastructure of the SME. It discusses various theoretical aspects of security, identifies various threats that could be posed to the SMEs, and a range of logical and physical countermeasures to protect against security threats and attacks. This paper can be helpful for the researchers and practitioners interested in the design and security of the network infrastructure of the SMEs. This paper can also act as a guideline for the users to apply the best practices from the literature to their own network deployment and management.

Keywords: Logical Network Design, Physical Network Design, Network Services, Network Monitoring, Security

Article Number: IOARP-JCN03-002
IOARP Journal of Communication and Networks
Volume 3, Issue 1, December 2023
Appeared on Digital Library: 15 January 2024

1. Introduction

The term Computer Networks derives from 'the merging of computers and communications' [1] in which Computer Systems are interconnected but separate systems. If two computers can exchange information, they are interconnected. The connection has a variety of techniques, including copper wire, fibber optic cabling, and microwaves, infrared and through satellites. Table 1 shows the area network classifications for typical location and distance this gives a good representation of business requirements.

Table 1: Network Classification [1]

Area Network	Distance	Standard Location
PAN	1M	Square Meter
LAN	10M	Room
	100M	Building
	1KM	Campus
MAN	10KM	City
WAN	100KM	Country
	1000KM	Continent
The Internet	10,000KM	Planet

1.1. A network to solve data inconsistency issues

The consistency becomes compromised when data gets saved. Duplicated files can include customer information, such as names and addresses. This duplicate data is redundant; therefore, the information becomes unreliable because the data can be changed in one file but not the other.
A solution to the inconsistency of data is to create a file server '… a file server is a computer responsible for the central storage and management of data files so that all the computers on the same network can access the files' [2].

A file server can be beneficial to any business because of the functionalities. The key benefits include:

- Remote Access - information can be accessed remotely without being at the office.
- Centralized Management of Permissions – allows the data to be secured and only accessible to the employees, maintaining data confidentiality.
- Data Security and Backup – backing up data to a file server maintain data integrity, should a computer failure occur.
- Data Recovery – data that gets deleted accidentally can be easily retrieved, often into newer versions.
- Employee Monitoring – support gets provided where all employees can be monitored, tracking their activities.
- Increase User Control – administrations of the file server can generate a new user and delete a former employee quickly without the worry of any unauthorized access.

1.2. A network to solve security issues

A NAC solution provides support to the visibility of the network and 'access management to policy enforcement on devices and users of corporate networks' [3]. Mobile devices have grown significantly accessing corporate networks which increase security risks. Providing the NAC is critical to strengthening the company security infrastructure. 'A NAC system can deny network access to noncompliant devices, place them in a quarantine area or give them only restricted access to computing resources…' [3]. Table 2

presents an overview of the capabilities of Network Access Control.

Table 2: NAC Capabilities

Capability	Overview
Policy Lifecycle Management	Policies are enforced
Profiling and Visibility	Users and their devices are recognised and profiled
Guest Network Access	A self-service portal with a guest management control
Security Posture Check	Users, devices and operating systems evaluated for security compliance
Incidence Response	The network that mitigates by enforcing security policies
Bidirectional Integration	Security and network integrated with other solutions

The article has been accepted, authors will be required to hand-in a final version of their article, pay the relevant fees where applicable, and submit a Copyright Transfer for the rest of this paper is organized as follows. Section 2 discusses logical and physical network design for the SME, including the choice of cabling and devices to be used.

2. Network Design

2.1. Logical Network Design

Ethernet cable is the main link from the router to the computer. An Ethernet cable has RJ45 standard connectors with a boot covering the release clip. These cables are connected to the wall-mounted Ethernet ports then to the Network Interface Card (NIC) in the computer. A NIC has an external network socket for the Ethernet cable which is connected directly to the motherboard.

The network topology helps to design a logical illustration of the network based on company requirements. The SME requires multiple workstations for their offices in the building, across two floors. They require seven workstations for the upper floor and three on the ground floor; one for dispatch and one each for the directors.

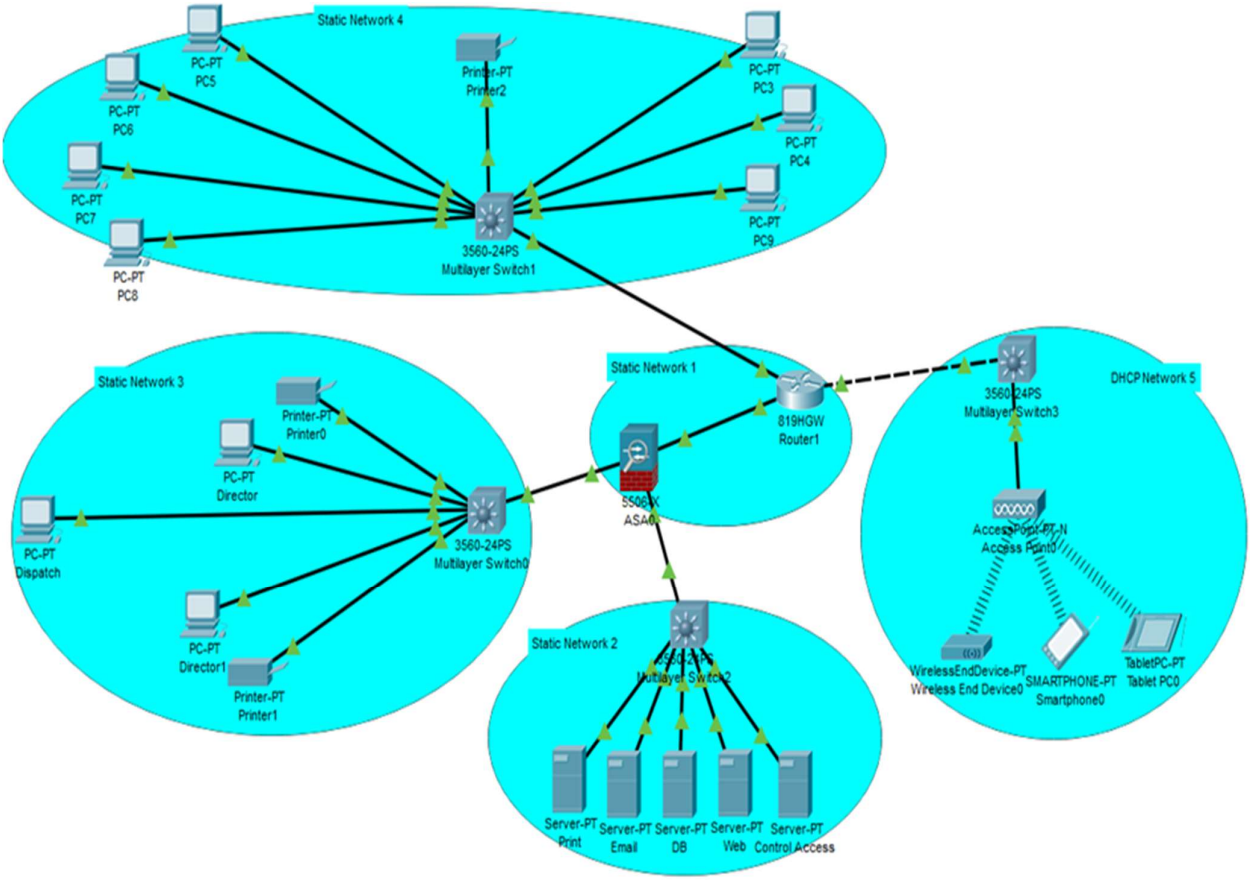

Figure 1: Logical Network Topology based on the business's requirements.

2.2. Cabling Requirements

Cables are a way of sending and receiving data allowing the client to access information. The Electronic Industries Association (EIA) and the Telecommunications Industry Association (TIA) define the standards of cables. The latest category (Cat) is Cat6 which supports Gigabit Ethernet and can accommodate 10 Gigabit Ethernet but over a limited distance of approximately 164 feet per cable.

The cable Cat6e measures 305m in length. This quantity will provide business expansion. The cable has no connectors, this an ideal product to individually create cable paths.

A pack of 100 unshielded twisted pair (UTP) male RJ45 connectors which are Cat6 ready and a pack of 10 RJ45 snag-less boots will also be required. Cat6A single gang dual-port faceplates and surface mounting single gang back boxes will be necessary for the walls. The Ethernet cabling will be connected to the wall gangs and into the computer's NIC.

The cabling estimate based on a two-floor building approximately measures L 13m x W 9m x H 5.7m.

Table 3: Estimated accessories, cable length and cable quantity

Product	Quantity
Cat6A single gang dual-port faceplate	12
Surface mounting single gang back box	12
Cat6e Cable (305m) Approximate cable length required = 137.5m	1
Cat6A RJ45 Connectors (100 pieces per pack)	1
RJ45 Snag-less Boots (10 pack)	10

Cable Length(m)	Quantity
11	3
7	1
5	9
3	13
1.5	9

2.3. Physical Network Design

The following key will be used to represent the component in the physical network design for the SME.

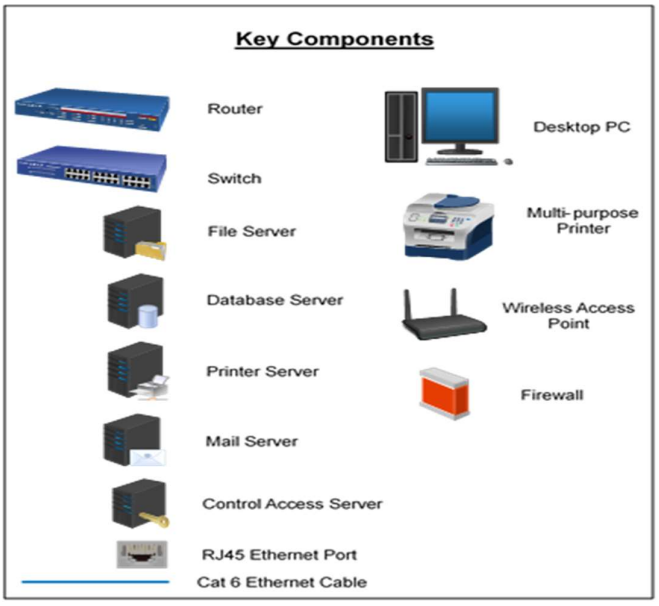

Figure 2: Key to identify components in the Physical Network Diagram

Figures 3 and 4 provide the physical network diagram for the first and second floor of the company.

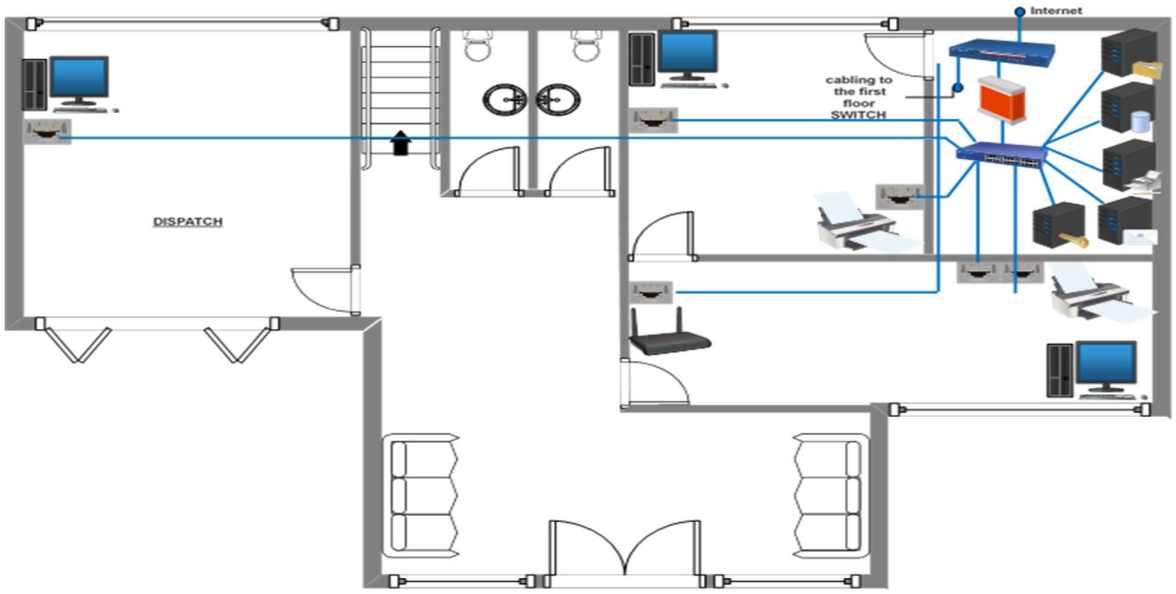

Figure 3: Ground floor physical network diagram showing a server room connected to the workstations and other network devices.

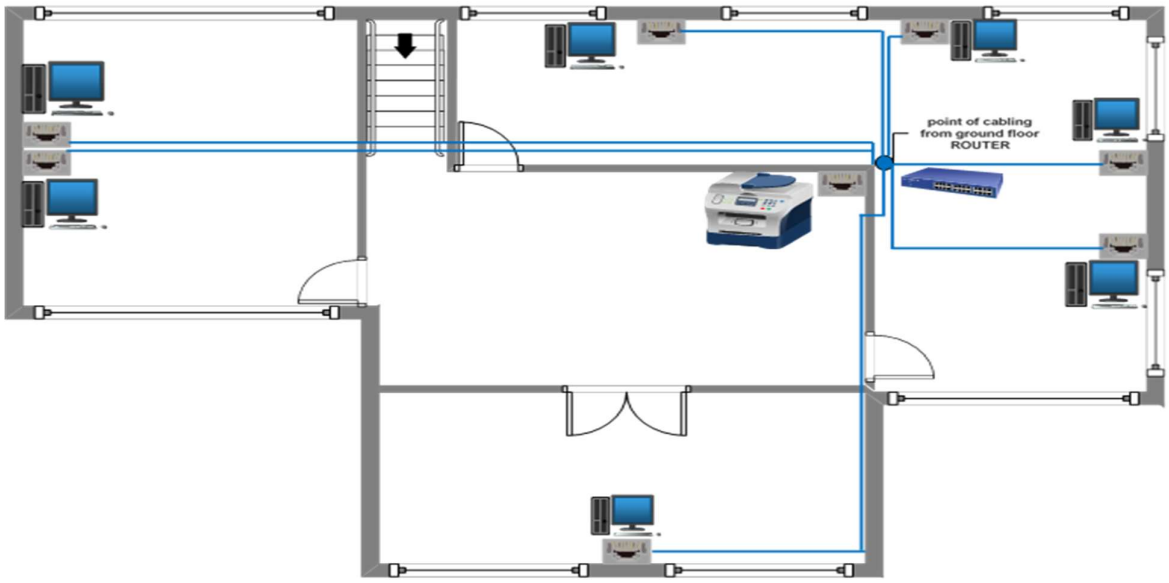

Figure 4: First-floor physical network diagram showing the connectivity of the workstations using Ethernet cabling.

2.4. Infrastructure Devices Used

This section provides information and discusses the devices that will be part of the infrastructure for the SME.

2.4.1. Routers

A router uses the third layer of the Open Systems Interconnection (OSI) model, defined as the Network Layer. 'Their main job is to forward packets based upon a routing table' [4]. They act as a gateway between two networks. The router controls the sending and receiving of data using Internet Protocol (IP)

addressing.

Routers are static and dynamic. An administrator sets up and configures the routing table manually, whereas a dynamic router is automatic. Dynamic routers are more sophisticated over a static router as '… they examine the information from other routers and make packet-by-packet decisions about how to send data across the network' [5].

Modern-day routers have the option of having a firewall pre-installed into the hardware. These are Integrated Service Routers (ISR). An alternative for the bigger network and businesses requiring high performing, large bandwidth applications is Aggregation Service Routers (AGR).

2.4.2. Switches

A network switch uses the second layer of the OSI model, defined as the Access Layer. These devices can connect multiple hosts to a network. To avoid data being sent and received to the wrong destination, a switch uses frames, Media Access Control (MAC) addressing '… the switch receives and decodes the frames to read the physical (MAC) address portion of the message' [6]. Like a routing table, a switch also has a table for MAC addresses. This table contains the active ports and the hosts MAC addresses.

A circuit is created to prevent a collision '… between the source and destination ports. This circuit provides a dedicated channel of all which the host connected to the various ports on the switch can communicate' [6].

A switch commonly contains 24 Ethernet ports to connect to the Internet. A wired network provides better security, reliability, is easy to use, and speed is consistent over a distance.

2.4.3. Servers

A server 'serves' data to all computers on a network. They store, retrieve and send data over the network. Servers connected to the Internet, process requests 24/7. Different types of server that each have a role, purpose, and functionality:

- Web Servers – serves web-related content such as HTML, CSS, and JavaScript.
- Mail Server - relays mail to the client
- File Server – web servers related to a file server because they follow the same protocols for storing and sharing files
- Database Server – data stored structurally, and indexed for quick responses to requests
- Print Server – accepts and sends applications to print documents
- Three different server variations:
- Tower Server - look like a desktop computer by providing basic levels of performance and less maintenance required.
- Rack Server – bay designed where devices can stack on top of each other. These bays can accommodate the server, storage devices, and security appliances. Several servers installed such as applications, email, database, software, and storage. They are more expensive than a tower server but offer greater flexibility and functionality.
- Blade Server – latest development, and offer higher processing power, take up less energy and space. A chassis is explicitly designed for blade servers as they share hardware elements with other blades, to reduce cost and gain efficiency.

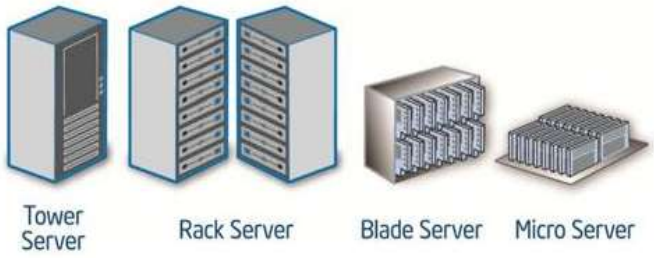

Figure 5: Server Variations [7]

2.4.4. Firewalls

A firewall is a Network Security device that monitors incoming and outgoing network traffic…' [8]. Based on a set of rules. Traffic can be blocked or allowed depending on the rules that are defined. Firewalls have evolved into threat specific capability while keeping the critical functions of a firewall because the malware and attacks are becoming increasingly sophisticated and can easily bypass older developments. The next-generation firewalls 'provide a holistic solution to filtering out dangers' [9].

Firewalls monitor ingoing and outgoing traffic information as they regularly update regarding applications and websites. They '… provide reliable protection to your PC &System' [10]. It is recommended to have a web application and network-wide firewall protection for home and business use**.**

Downtime significantly reduces because data on the server is accessible after the credentials get imported. Servers allow remote access and improved collaboration within a business by updating and syncing calendars within seconds. Servers are more powerful than a desktop computer server as they have higher processing power, larger storage capacities and seamless run times.

2.4.5. Wireless Access Points (WAP)

The wireless access points 'creates a wireless local area network (WLAN), usually in an office or large building' [11]. The wired Ethernet sends data to the access point and converted into a wireless signal frequency of 2.4 GHz are 5 GHz. 'It sends and receives wireless traffic to and from nearby wireless clients' [12].

Nearly all devices have wireless capabilities. The benefits of having access points, encourage employees to Bring Your Own Device (BYOD) which can save the company on maintenance costs and upgrades. BYOD is generally mobile, so employees do not have to be at their desk; they can use the canteen or use their device in a meeting.

2.5. Comparison of Products for Each Infrastructure Device

All products selected will be chosen with expansion in mind because businesses are likely to expand and would require extending their network. By selecting products that are beyond the current business's requirements, they will be able to save money by spreading their network.

2.5.1. Router Comparison

Two routers selected belong to the company Cisco who specialize in networking hardware and other IT services. The routers are capable for a small-medium enterprise (SME) and suitable, should the company look to expand the business or upgrade the network. They are both ISR routers.

Table 4: A comparison between two routers

	Cisco ISR 4331 UC Bundle, PVDM4-32, UC License, CUBEE10	**Cisco ISR 1100 8P Dual GE WAN w/LTE Adv SMS/GPS 802.11ac -E Wi-Fi**
Price	£1917.43	£899.31
Ethernet LAN Data Rates	10, 100, 1000 Mbits/s	10, 100, 1000 Mbits/s
LAN Ports	5	8
USB Ports	2x (2.0)	1x (3.1)
RS232	2	0
Mobile Network	Not Supported	4G LTE
WLAN	N/A	Dual Band (2.4GHz/5GHz)
Data Rate WLAN	N/A	867 Mbit/s
Wi-Fi Standard	N/A	IEEE 802.11ac
Network Standards	IEEE 802.1Q, IEEE 802.1ag IEEE 802.3, IEEE 802.3ah	IEEE 802.3, IEEE 802.3ab IEEE 802.3af, IEEE 802.3at IEEE 802.3u
Web Based Management	Yes	Yes
Support	Yes	No
Firewall	Yes	Yes
Security Algorithms	3DES, AES	3DES, 802.1x, RADIUS, AES, DES
Flash Memory	4000 MB	
Internal Memory	4 GB	
Memory Card Size	16 GB	

2.5.2. Server Comparison

The two servers selected are both capable of an SME. The Fujitsu is a rack-type server where the HPE ProLiant is a tower server.

Table 5: A comparison between two routers

	Fujitsu PRIMERGY RX2510 M2 E5-2620v4	**HPE ProLient Micro Server Gen10 X3216**
Price	£1872.95	£263.23
Processor Frequency	2.1GHz	1.6GHz
Processor Family	Intel Xenon E5 v4	AMD Opteron
Processor Cores	8	2
System Bus Rate	8 GT/s	
Hard Drive Size	3.5”	3.5”
Hard Drive Interface	Serial ATA III	Serial ATA

Internal Memory	16 GB	8 GB
Memory Type	DDR4-SDRAM	DDR4-SDRAM
USB Ports	1x (2.0), 4x (3.1)	3x (2.0), 4x (3.1)
RAID Levels	0,1,5,6,10,50,60	0,1,10
Storage Capacity	4TB	16TB
Ethernet LAN	1	2
Ethernet Interface Type	Gigabit	Gigabit
Ethernet LAN Ports	1	2
Chassis Type	Rack (1U)	Ultra-Micro Tower

2.5.3. Switch Comparison

The two switches are a product of Cisco with similar pricing but with some different specifications.

Table 6: A comparison between two switches

	Cisco Catalyst 3850 **WS-C3850-24P-L**	**IE4010 4x 1G SFP** **IE-4010-4S24P**
Price	£2646.51	£2485.26
Switch Type	Managed	Managed
LAN Ports	24	24
VLAN Support	Yes	Yes
MAC Address Table	24000	16000
Security Algorithms	802.1x, RADIUS	802.1x, RADIUS, FIPS, 140-2, SNMP, SSH
Switching Capacity	88 Gbit/s	56 Gbit/s
Multicast Support	Yes	Yes
Network Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3at	IEEE 802.3, IEEE 802.3af, IEEE 802.3at
Other Protocols	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, SSH, CLI	IPv4, IPv6, VTPv2, NTP, UDLD, CDP, LLDP, HTTP
Flash Memory	2 GB	128 MB
Internal Memory	4 GB	1 GB
Memory Type	DRAM	GB DRAM
DHCP Server	No	Yes
USB Port	1 (2.0)	1 (2.0)
Switch Layer	L2/L3	L2/L3

2.5.4. Firewall Comparison

As routers mainly have a firewall already adopted, it is a good practice to have further firewalls added to the topology to secure the LAN further. The firewall selected is from Cisco's 5500 series.

Table 7: A comparison between two firewalls

	Cisco ASA 5525-X with SW ASA5525-CU-K9	**Cisco ASA 5525-X with SW ASA5525-K9**
Price	£5044.42	£3134.74
Ethernet LAN Ports	9	9
Firewall Throughput	2048 Mbit/s	2000 Mbit/s
VPN Throughput	300 Mbit/s	300 Mbit/s
VLANs	200	200
Management Protocols	HTTP, SMTP, FTP, IMAPv4, BitTorrent, DNS	HTTP, SMTP, FTP, IMAPv4, BitTorrent, DNS
USB Ports (2.0)	2	2
Internal Memory	12288 MB	8192 MB
Security Algorithms	3DES, AES	3DES
Features	Firewall protection, VPN support, VLAN support, High Availability, IPsec	Firewall protection, VPN support, VLAN support, High Availability, IPsec
Memory	8GB	8GB

2.5.5. WAP Comparison

Wi-Fi can have protocols set where all employees can access the network and depending on the hierarchy within the business; they can obtain sensitive information.

Table 8: A comparison between two WAP

	Cisco AIR-AP3802P-E_K9C	**Cisco AIR-CAP1602I-EK910**
Price	£683.04	£2505.09
Ethernet LAN Data Rates	100, 1000, 2500, 5000 Mbits/s	10, 100, 1000 Mbits/s
Wi-Fi Data Rates	2600Mbit/s	
Data Transfer Rate	5200Mbit/s	300Mbit/s
Frequency Band	2.412-2.472, 5.18-5.32, 5.5-5.6, 5.64-5.7GHz	2.4, 5GHz
Channel Bandwidth	160MHz	
Channel Quantity	29	
Antenna Type	External	Integrated
Wi-Fi Standard	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac Wave 2	IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11h, IEEE 802.11d
Network Standards	IEEE 802.3bz, IEEE 802.11a, IEEE 802.11ac, IEEE 802.11b, IEEE 802.11d, IEEE 802.11g, IEEE 802.11h, IEEE 802.11i,	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h, IEEE 802.11n, IEEE 802.3af

	IEEE 802.11n, IEEE 802.1x IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3at, IEEE 802.3u	
Security Algorithms	802.1x, RADIUS, AES, EAP, EAP-FAST, EAP-PEAP, EAP-SIM, EAP-TLS, EAP-TTLS, MSCHAPv2, WPA, WPA2	3DES, 802.1x, RADIUS, AES, DES

3. Network Monitoring in the SME

Network monitoring monitors network devices and detects failing components of that network. These components can include servers overloaded, crashing routers and switches failing. The network administrator (NA) is alerted through the network monitor system. Tools and software applications are commonly used to monitor networks because they can detect the full functionality of properly connected networks and Web servers. The software constantly monitors the network health and reliability, seeking for trends which are tracked, with parameters logged. The parameters include:

- Transmission rates (throughput)
- Error rates
- Use time percentages
- Uptime/downtime
- User response time
- Automated inputs and requests

Network fault management processes initiate when set parameters reach the limit. A basic monitoring tool used is 'Ping' accessible in the 'cmd prompt'. This tool tests the time it takes to reach a host of an IP address. As network traffic has increased and will continue to grow, a basic monitoring tool is not enough to monitor the network performance. Tools and software packages with sophisticated algorithms to monitor network performance are available.

The network monitoring tools combine with tools that can scan the network. These tools now offer a real-time breakdown of the live network. Examples of companies who provide network monitoring are Zabbix, Spiceworks, and Paessler PRTG but the number one in network management is SolarWinds [13] who offer an abundance of tools and software for management of networks, systems, and databases. They provide support globally and have open an academy to become a SolarWinds Certified Professional.

SolarWinds are based in Austin, Texas, the USA with 2500 employees worldwide. They provide '… powerful and affordable IT infrastructure management software' [14]. As a company they work to:

- Understand IT
- Build for IT
- Make IT simple
- Make IT work
- Solve IT

Their products can manage and monitor the performance of any IT infrastructure regardless of size and complexity, on-premises, in the cloud or hybrid models. They engage with different technology professionals, e.g., DevOps and managed service providers (MSA) to understand current and future challenges.

Downtime reduces by providing multi-vendor monitoring. Hop-By-Hop path analysis can be performed to check devices and applications inside AND outside the network using a feature called NetPath. The NA proves the networks mean-time-to-innocence-fast. All the data is collected and correlated for fast troubleshooting. Everything in the network is analyzed and provided in timelines, graphs, and charts.

SolarWinds NPM current version is at 12.4, and the key features include:

- Multi-vendor
- Deeper visibility int the network
- Intelligent maps
- NetPath and PerfStack for troubleshooting
- Smarter scalability for larger environments
- Advanced alerting

NPM SL100 is the recommended license SME because they only have a small number of users but will allow for expansion of the network up to 100 elements.

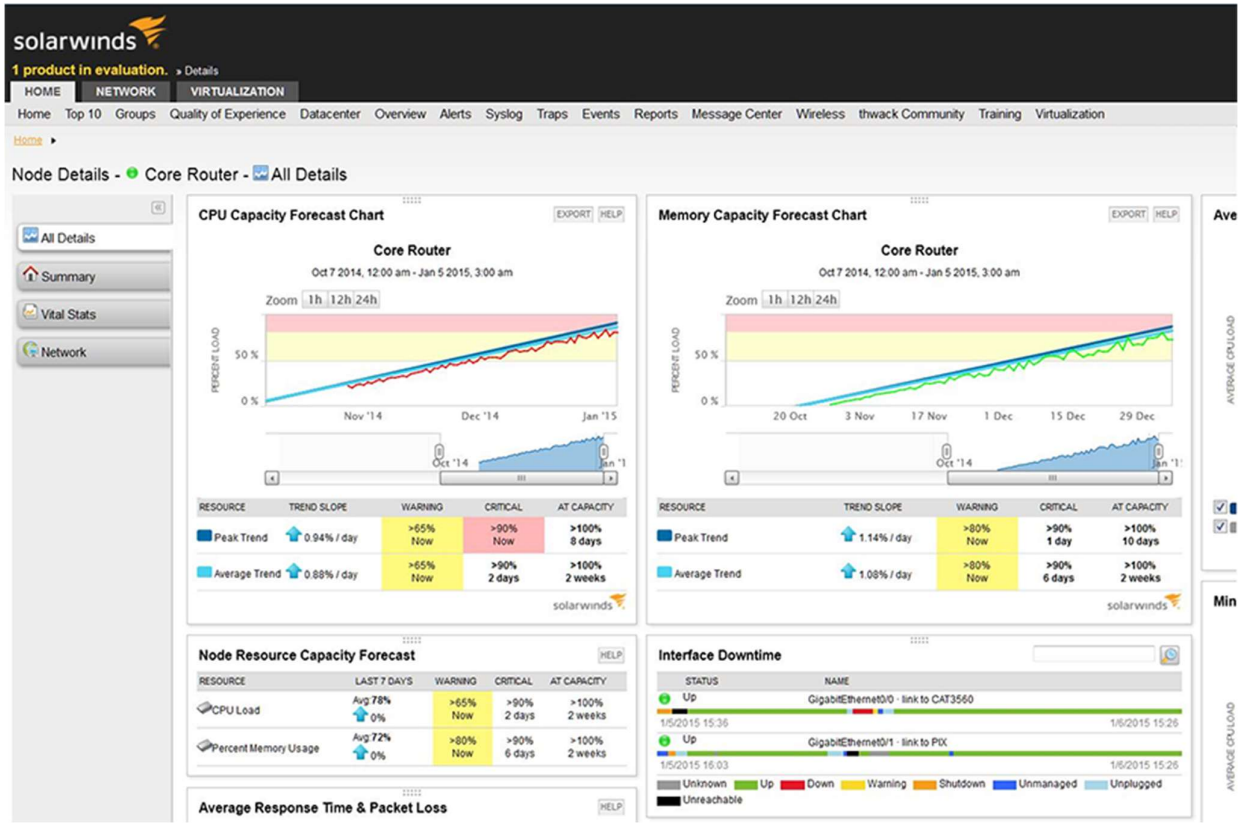

Figure 6: Solar Winds Network Dashboard (Solar Winds, n.d.)

4. Security in SME

4.1. Security and Cryptography

In data communication and networking, security is undeniably essential and a must for anybody using a network. Cryptography is '… the science and art of transforming messages to make them secure and immune to attack' [15, p. 931]. What this provides is confidentiality, integrity, and authentication, including the authenticity of a message between sender and receiver.

The process of cryptography starts with plaintext. This plaintext transforms into ciphertext through an encryption algorithm which then sends the message receiver where a decryption algorithm converts it back into plaintext.

Encryption and decryption algorithms are known as cyphers which are different categorised algorithms. As an algorithm, the cypher operates on a key which is a number or set of digits. Without this key, a message is not able to be encrypted or decrypted.

Two modern symmetric-key cyphers used are Data Encryption Standard (DES) and Advanced Encryption Standard (AES). These encryption standards class as block cyphers '… because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks' [14, p 941].

DES worked on a 64bit key and was deemed too small, the formation of TripleDES (3DES) increased the key size to 168bits, but the process was too slow. AES is a computer round cypher designed with three key sizes, 128, 192 and 256bits which was developed to speed up the process.

4.2. Security Threats

Security threats can come at any time. The standard security threats use a variety of ways to access a network and gain confidential information such as usernames, password, and accounting information.

The most common threat is the computer virus. A virus infects a host computer then spreads to connected computers on the network looking to retrieve data, shut down systems and even delete information.

A Trojan horse '… refers to tricking someone into inviting an attacker into a security protected area' [16]. It is a piece of attacking code or software that maliciously tricks the user by hiding behind a program. They often hide behind fake advertisements throughout the Internet. They record keystrokes, hijack webcams and steal sensitive information.

Phishing is another security threat that can cause serious harm to a person or business. Phishing aims to obtain data such as usernames, passwords, and accounting information by sending messages through social engineering.

Other threats to the SME in question may include:

- Adware and spyware
- Computer Worm
- DOS and DDOS attack
- Rootkit
- Man-in-the-middle-attacks (MITMA)

4.3. Physical and Logical Countermeasures

It is the responsibility of the CEO who deals with security. The CEO should make their staff aware of the principles of network security. A Security protocols such as IPsec is a requirement as they work in the OSI model to help with the integrity, confidentiality, and authentication of the network. The following table shows the countermeasures in the context of security for the SME.

Table 9: Physical and logical ways of securing a network

Physical Access Measures	**Logical Access Measures**
Lockable server room	Anti-virus software
Detection sensors: - **Heat** - **Smoke**	Software updates and patches
Provide CCTV inside and outside the building	Access rights - User segmentation
Place vulnerable devices into the server room	Regular backups
Use (cost permitted) rack-mounted servers	User IDs and password - Authentication - Two-factor authentication (2FA) - Token authentication
Locks on all offices in the building - **Access card**	Connect firewalls near vulnerable devices

- **Biometric system**	
Disable removable media: - **USB ports**	Provide hard disk encryption and if available use biometrics for mobile devices
Remove/disable unused computers	Intrusive Detection System (IDS)
Keep backups locked in the server room	Intrusive Prevention System (IPS)
	Honeypot – provides purpose-built vulnerabilities on the network for would-be hackers, once trapped the NA can administer a block

5. Conclusion

An SME based in the UK, as an example, a quality communication network will rely heavily on the mix of devices chosen to fulfil Business communication needs. It is essential that the right devices are chosen for the business to enable communication through their network efficiently and effectively, with speed, and promptly, matching the business profile. As discussed, the performance of the network devices needs to be monitored in an efficient, systematic manner, providing the business with the necessary tools to push forward in their sector, while maintaining a high level of essential security and unique identification.

The paper indicates how to set up a network infrastructure for an SME within a building over two floors with relevant information for a novice or a general DIYer looking to set up a network. The readers get an insight into the type of equipment typically used in networking infrastructure and their purpose to enable a fully functioning and secure network for a business.

References

[1] Tanenbaum, A. S. & Wetherall, D. J., Introduction. In: *Computer Networks.* 5 ed. Essex: Pearson Education Limited, pp. 1-88, 2014.

[2] Rouse, M.,File Server, 2015 [Online] Available at: https://searchnetworking.techtarget.com/definition/file-server.

[3] Cisco,. What Is Network Access Control?, 2019. [Online] Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html.

[4] Learn Cisco,. Exploring the Functions of Routing, 2012.[Online] Available at: http://www.learncisco.net/courses/icnd-1/lan-connections/functions-of-routing.html.

[5] Scottish Qualifications Authority,. Functions of Routers, 2008. [Online] Available at: https://www.sqa.org.uk/e-learning/NetTechDC02CD/page_47.htm.

[6] Cisco & Cisco Router, Network Switch,. Network Switches: Functions & Types of Switches, 2011[Online] Available at: http://ciscorouterswitch.over-blog.com/article-network-switches-functions-types-of-switches-94061458.html.

[7] Rouse, M. & Zaharoff, S,. Microserver, 2014 [Online] Available at: https://internetofthingsagenda.techtarget.com/definition/microserver.

[8] Cisco,. What Is a Firewall?, 2018 [Online] Available at: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html.

[9] Kaspersky Lab,. What Is a Firewall?., 2018 [Online] Available at: https://www.kaspersky.co.uk/resource-center/definitions/firewall.

[10] TPro,. What is a firewall and why do we need it?, 2015 [Online] Available at: https://www.itro.com.au/what-is-a-firewall-and-why-do-we-need-it/.

[11] Linksys,. What is an Access Point and How is it Different from a Range Extender?, 2016 [Online] Available at: https://www.linksys.com/us/r/resource-center/what-is-a-wifi-access-point/.

[12] Netgear,. What is a wireless access point?, 2013 [Online] Available at: https://kb.netgear.com/235/What-is-a-wireless-access-point.

[13] SolarWinds, n.d. [Online] Available at: https://www.solarwinds.com/ [Accessed 28 March, 2019].

[14] SolarWinds,. SolarWinds: We Make IT Look Easy, 2018[Online] Available at: https://www.solarwinds.com/company/home.

[15] Forouzan, B. A,. Cryptography. In: Data Communications and Networking, Singapore: McGraw-Hill, pp. 923 – 960, 2007.

[16] SecurityTrails Team,. Top 10 Common Network Security Threats Explained,2018. [Online] Available at: https://securitytrails.com/blog/top-10-common-network-security-threats-explained.