Bradley De’Ath

DEA18001355

April 21, 2020

Network Planning, Design and Implementation

SCDT43 – assignment 2

Table of Contents

[Document Overview 1](#_Toc37258859)

[Network Plan and Design 1](#_Toc37258860)

[Topology Design 1](#_Toc37258861)

[Layout Plan & Hardware Costs 3](#_Toc37258862)

[The Switch 4](#_Toc37258863)

[The Router 4](#_Toc37258864)

[The Server 4](#_Toc37258865)

[The Wireless Access Point 4](#_Toc37258866)

[Prototype Model 5](#_Toc37258867)

[Performance Testing 5](#_Toc37258868)

[Cyber Security Risk Assessment 6](#_Toc37258869)

[Asset Prioritization 6](#_Toc37258870)

[Potential Risks 6](#_Toc37258871)

[Phishing 6](#_Toc37258872)

[Broken Access Control 7](#_Toc37258873)

[Testing Appendix 8](#_Toc37258874)

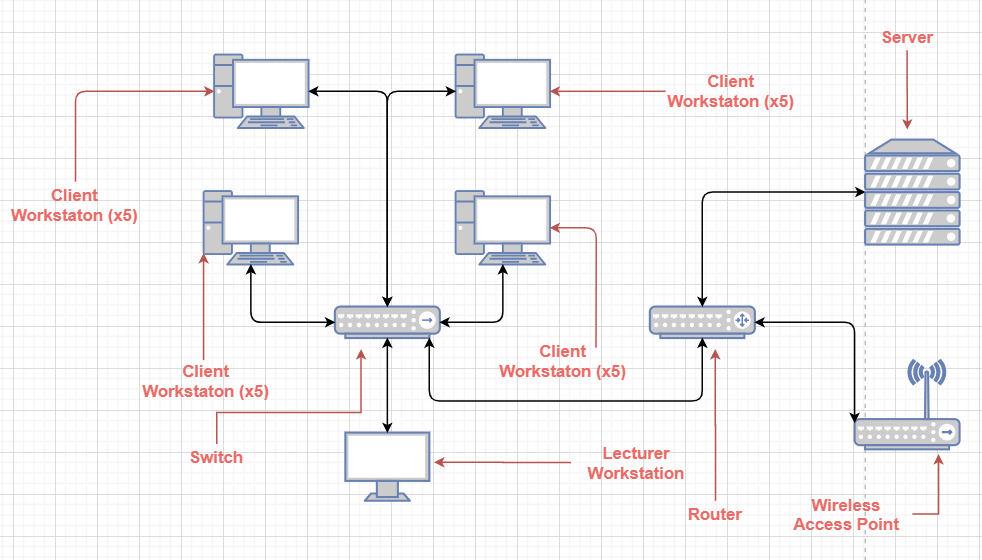
[Bibliography 11](#_Toc37258875)

# Document Overview

The Aim of this documentation is to provide detailed information on the proposed new closed network for University Centre Somerset’s Cyber Security Lab. With Analysis of design decisions such as the chosen topology and design, along with evaluation of the cyber security capabilities and how they can help protect against damaging cyber-attacks. Along with the working prototype developed in Packet Tracer, testing has been documented on how aspects of the network run in comparison to the laid out requirements.

# Network Plan and Design

## Topology Design



The Above diagram shows the basic design for the Cyber security Lab, with the layout being modelled on the star topology.

The topology of a network is how the elements and hardware that make up a network are arranged, meaning that is an important factor for how the network operates. It has been observed that topologies can be one of the leading factors when determining a network’s reliability **(Kumar et al., 1993)**, with different topologies managing traffic and connections in different ways.

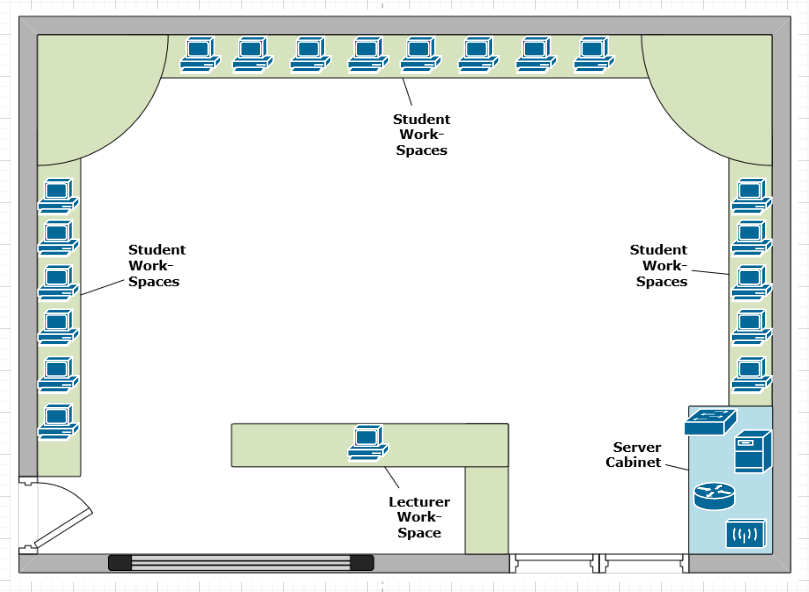
Being one of the most commonly used, the Star topology’s main focus is on separate connections to nodes for different devices. These star topologies are designed similar to that of an actual star, with serval protruding points to connect the devices. As can be seen in the above diagram, the switch acts as the central point of the star, with connections to each of the workstations and to the router branching off to form the star style. The data from this these protrusions all flows through the switch, making it a central funnel to manage all of the content that flows on the network **(Faircloth, 2013)**.

This topology is efficient due to how it manages failures in connections, in the event that one device off the switch fails, the usability and connections of the others are not compromised **(DelCoco et al., 1992)**. This allows for the network and those using it to continue functioning even in times of partial failure. This is one of the main benefits to using this topology over others that cannot handles downtime as well, such as with the ring topology: unlike with the Star, the ring is far less adaptable to devices suffering downtime.

As seen in the diagram above, the ring topology has all of the devices on the network interconnected to form a loop, meaning that any data traffic needs to potentially pass through several unnecessary devices until it reaches the intended recipient. This method of passing data can lead to slowdowns on the network, as more traffic is going around the network at any one time when it could be sent directly to the recipient.

However, even with the implementation and upkeep of the ring topology being cheaper than the star alternative **(Bisht and Singh, 2015)**, the impact that downtime can have on users of ring is far greater. Where operations can continue relatively normal on star-based networks; due to each device acting as a node for traffic, if a single device in the chain goes down in the ring topology it can potentially prevent any traffic on the network from successfully transferring **(Orava and Ramfelt, 2008)**.

## Layout Plan & Hardware Costs



The above diagram shows how the hardware for the network would be implemented into the Cyber Security Lab, based on the simple room plan provided.

The main reason for this chosen layout Is due the requirement of all networking equipment being located in the server cabinet. If items such as the router or switch were located elsewhere in the room, it would not meet the requirement, as well as add potentially more work for the upkeep and management of the network. With the important hardware being scattered around the room, they are no longer centralised, and so tasks such as checking temperature or fixing hardware require each item to be located rather than easily accessible from a single point.

The layout of the workstations is based on the simple room plan, with the 19 devices spread out across the 3 computer spaces around the sides of the room, the users are able to still have their space while all fitting into the single room, while not having the network need to spread outside of the allocated space.

As can be seen in the diagrams above, there are several pieces of hardware that are needed in the network to ensure that it works both efficiently and correctly. Due to this, if hardware is used that isn’t of a high enough standard, the network may suffer performance issues and so not meet the standards set for the Cyber security lab. This means that having high quality yet affordable hardware is the best option to ensuring that the network is both efficient and achievable. The hardware selections and their prices are below:

### The Switch

In the requirements for the network, a total of 20 workstations are needed as well as one router, all 21 of these devices need to be able to connect to the switch for the star topology to be successful, and so that is why I have chosen this model. The Cisco Catalyst 2960-24TT-L Switch (Priced at £1,185.76) has a total of 24 ethernet connection ports, meaning that all of 21 devices can be connected to the singular switch, allowing for expansion as needed **(Cisco Catalyst 2960-24TT-L Switch, n.d.)**. While it is unlikely that too big of an expansion would be needed for the network, the switches allow for switch-to-switch connections, meaning that another node can simply be plugged in and connect to the wider network.

### The Router

In a network, the router acts as a node for managing how information is distributed, making it a vital piece of the overall structure. The chosen router (Cisco Systems C1941-SEC-SRE/K9) allows for easy connection between the main switch and other key components such as the server. Due to the use of a wireless access point elsewhere on the network, the additional costs for a built-in-wireless router were not needed, resulting in a cost of £1,258.35 for the chosen router **(Cisco 1941 Series Integrated Services Routers Data sheet, n.d.)**.

### The Server

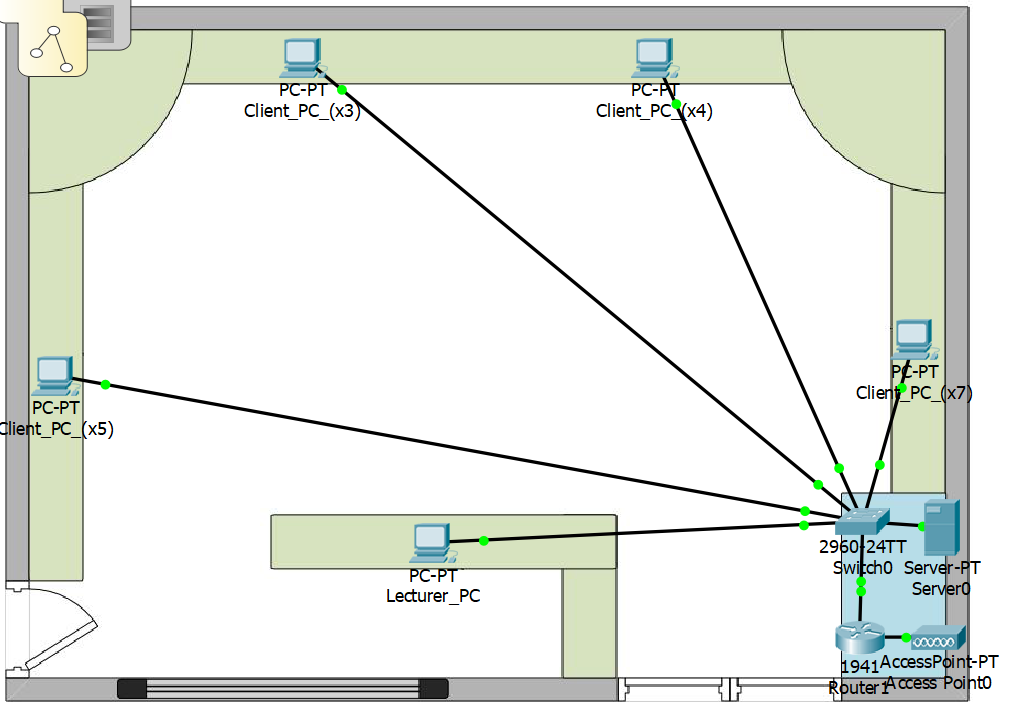
As stated in the requirements, there are several services that need to be provided to the network from a single server. DHCP, DNS and File & Email Servers are all runnable from the chosen server (SNTC 24X7X4OS Cisco Edge 340 Generic. 2G Mem.32G SSD.1), allowing for all requirements to be met without the need to pay for a more advanced server model: leaving the server costs to £6,029.16 **(Cisco Servers, n.d.)**.

Active directory is another tool that is listed as a requirement for this server, due to its functionality in managing access/permissions to items on the network. Along with the group policy which allows for better management of user accounts on the network, the services that this server can run allows for better control over network security.

### The Wireless Access Point

Costing £245.24, the chosen wireless access point for the network (Cisco Systems AIR-AP1141N-E-K9 Cisco Aironet 1140 Access Point 300Mbps WLAN Access Point) is able to provide a wireless connection for devices to the new network. The ability to provide a wireless connection was one of the main requirements for the network, and with this access point several devices are able to connect without the need for a wireless router, reducing the cost **(Cisco Aironet 1140 Series Access Point Data Sheet, n.d.)**.

# Prototype Model



## Performance Testing

Below shows testing proof of the prototype network meeting the requirements for the Cyber Security Lab:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Test No.** | **Test** | **Test Description** | **Expected Result** | **Actual Result** | **Screenshot** |
| **1** | Lecturer Ping | The Lecturer’s workstation is able to communicate with the client workstations | Success | Success | Testing Appendix: Figure 2 |
| **2** | Workstation Ping | The Client workstations are able to communicate with the lecturer’s workstation | Success | Success | Testing Appendix: Figure 1 |
| **3** | Wireless Connection | Devices can connect to the network wirelessly | Success | Success | Testing Appendix: Figure 3 |
| **4** | DHCP Server | The Network’s server has DHCP capabilities | Success | Success | Testing Appendix: Figure 4 |
| **5** | DNS Server | The Network’s server has DNS capabilities | Success | Success | Testing Appendix: Figure 5 |
| **6** | File Server | The Network’s Sever has a file repository | Success | Success | Testing Appendix: Figures 6 & 7 |
| **7** | Email Server | The Network has an Email Server | Success | Success | Testing Appendix: Figure 8 |

# Cyber Security Risk Assessment

## Asset Prioritisation

While keeping all devices on a network properly protected is important for cyber security, it is also important to identify which parts of the network are in more crucial need of protection. Due to both the cost and the information stored within it, it can be argued that the server is the most important and liable asset of the network, making it essential to provide it with proper security and protection. Whereas the user workstations simply access the information such as user logins and the email accounts, these services are directly stored within the server linking their functionality to the functionality of the server. If this server is compromised, as too are these services that run off it, preventing the network from functioning properly as well as compromising the personal data on it. This means that the server is the network asset that should have its cyber security prioritised, as where other pieces of hardware can be replaced without too much change to the network’s functions, if the data on the server is lost then more work will be required to restore the network to its previous state.

This is especially evident with the personal information that may be linked to user accounts stored on the server. While within the Security Lab there is unlikely to be information linked to user’s payment credentials, which is one of the leading sources of Identify Theft **(Teraguchi et al., 2004)**, important information such as names and logon credentials are susceptible to being lost or stolen if the sever is compromised. In the even that this information is lost, it is unlikely to affect the day-to-day operations of the university as new accounts can be created, but anything users had saved and registered to those accounts is at risk to being lost – potentially impacting students’ abilities to continue their education.

## Potential Risks

### Phishing

One of the most common cyber security threats are phishing attacks. These attacks are where a malicious attack is disguised as an email to trick the recipient into allowing access to private information. Through taking the form of a potentially trustworthy email, users are more likely to interact with the content sent to them **(Dhamija et al., 2006)**. With the sender of the email seeming like someone trustworthy or important, the recipient may be more inclined to download any files that have been sent under the false pretence of it being trustworthy, whereas they have instead allowed the network to be compromised by an unknown entity.

This type of attack can become more advanced in the form of **Spear Phishing**. These more intricate attacks rely on better knowledge of the intended target, such as posing as other members of an organisation. These Spear Phishing attacks are most specially engineered for a single target that could provide value data once access has been gained, as opposed to a widespread attack intended to target several recipients simultaneously **(Wang et al., 2012)**.

While Phishing is one of the oldest and most common attacks, they require the recipient to have an internet connection for the scam emails to be viewable. With the Cyber Security Lab’s requirement of being a closed-off network with no access to the wider college LAN, emails from outside of the network would be unable to be received, and so could not pose a threat to the systems running there.

### Broken Access Control

It is important on a network that information is only able to be accessed by those intended, meaning that it isn’t freely available to those who do not have the correct authorisation. Broken Access Control is one of the largest cyber security risks **(OWASP Top Ten, 2017)**, with a large reason being that many attackers may not need high level computer knowledge for these attacks to succeed. With the attacks relying on poor management of user access on a network, once a vulnerability is discovered, most users would be able to make use of it and gain access to content they are not supposed to **(Owasp.org, 2017)**.

Any valuable or personal information is susceptible to theft in the event of Broken Access Control. If users’ personal details are stored in an admin account and someone without admin privileges is able to gain access, the information can easily be taken and redistributed, putting the owners of the information at risk of crimes such as Identify Theft.

Unlike with Phishing, the Cyber security Lab is susceptible to Broken Access Control, and if it were to suffer from an attack, the network could be compromised. The best method of avoiding these attacks is to ensure that all user accounts on the network have the proper access level and authorisation. Through the use of the DNS and mail servers implemented in the prototype of the network, proper accounts can be set up with passwords that can be accessed by induvial rather than by workstation, meaning that without the proper username and password, users will be unable certain data and content on the network **(Ferraiolo et al., 2003)**.

One of the resources included in the prototype network, Microsoft Active Directory, is designed to help prevent these sort of attacks through properly managing permissions **(Azure Active Directory | Microsoft Azure, n.d.)**. With the ability to manually set which user accounts have access to which network resources, the control of users’ authorisation can easily be monitored and updated from a single interface, making it easier to keep content access governed.

# Testing Appendix

Figure 1 : Client PC pinging Lecturer PC

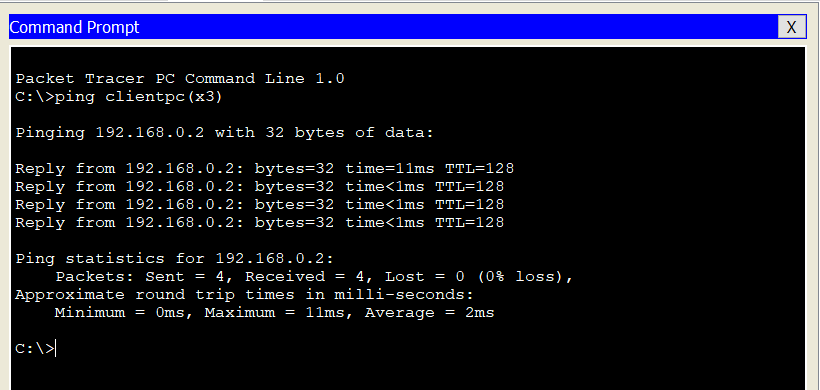


Figure 2 : Lecturer PC pinging Client PC

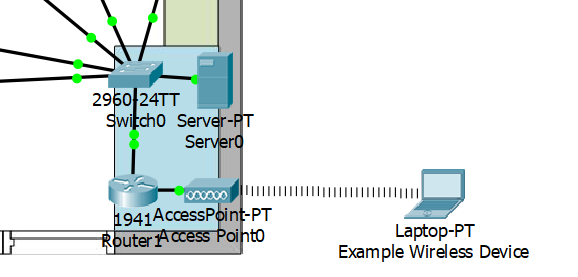
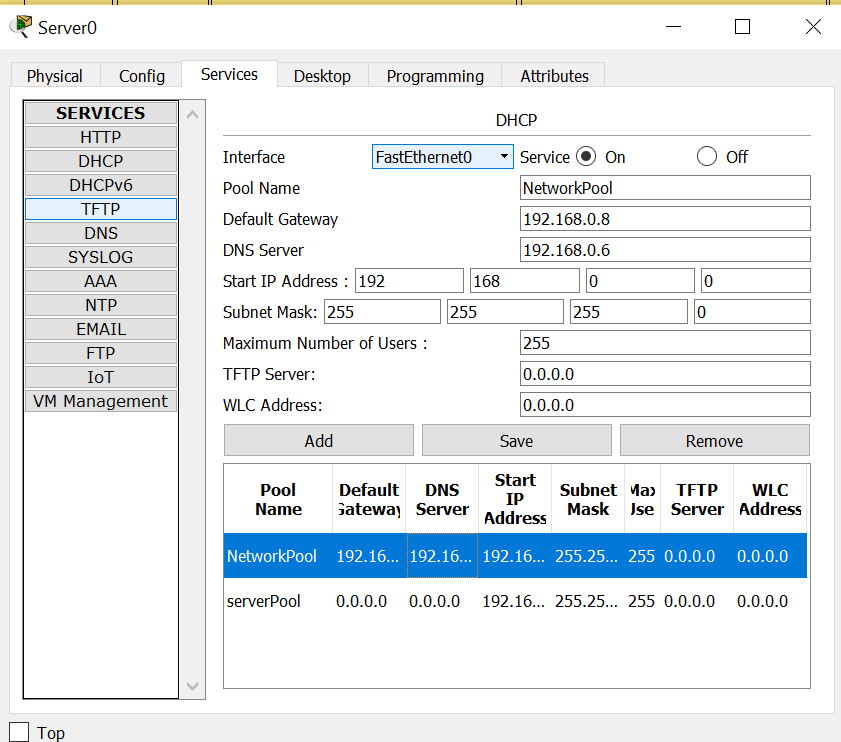
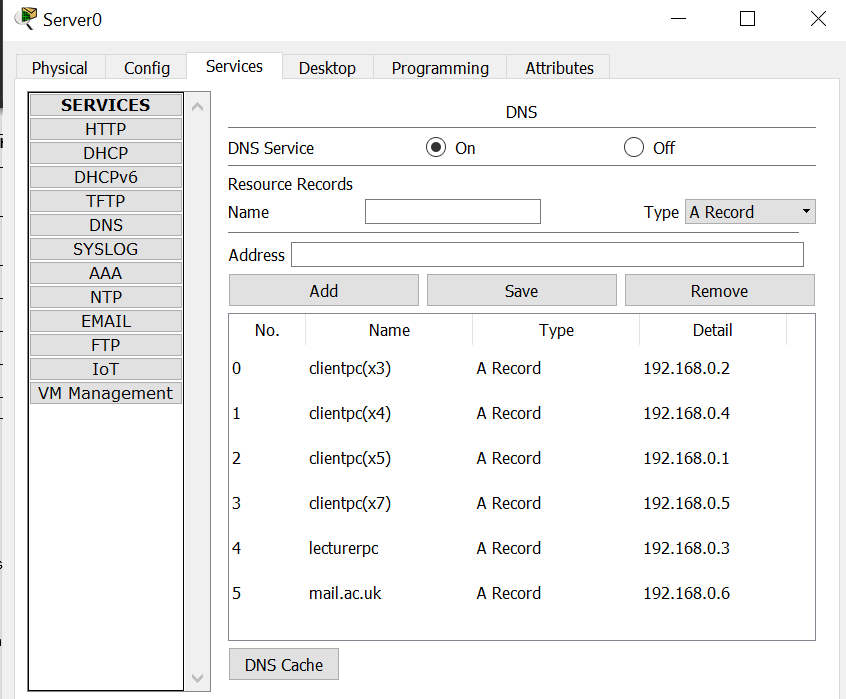


Figure 5 : DNS settings on the Network Server

Figure 4 : DHCP settings on the Network Server

Figure 3 : Example Wireless Device connecting to Network

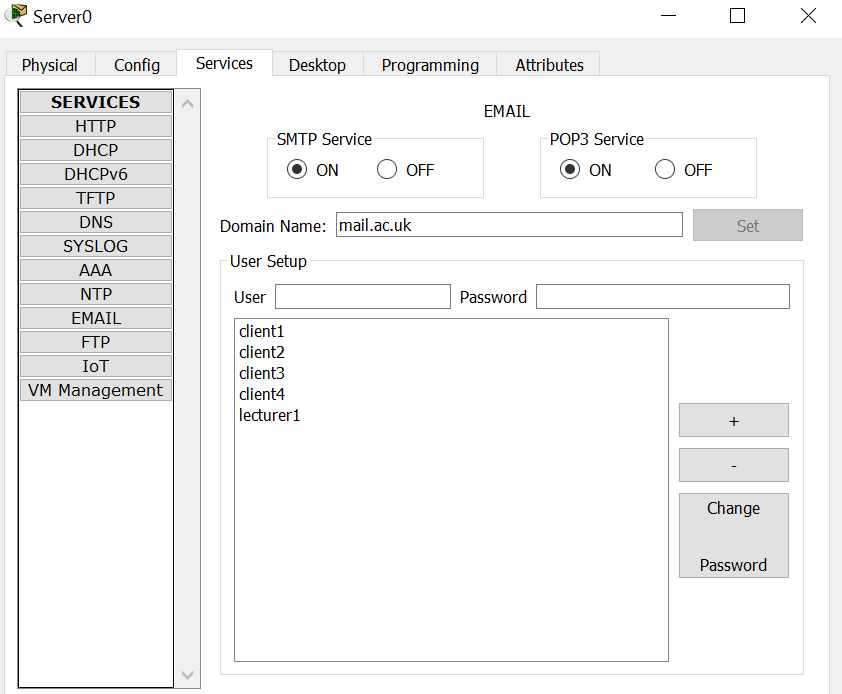
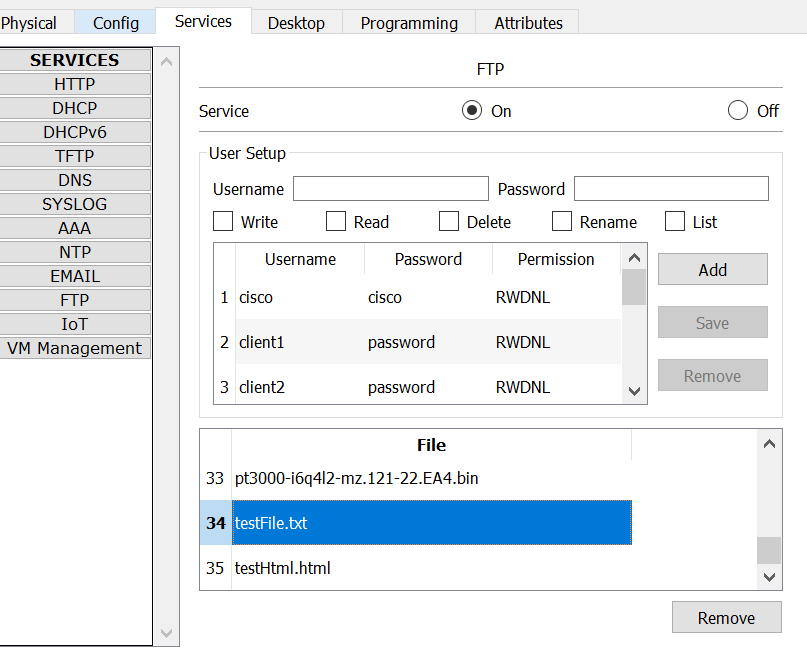


Figure 8 : Files added to File Server

Figure 7 : Email service viewed from client PC

Figure 6 : Email Server settings on the Network Server

# Bibliography

Kumar, A., Pathak, R.M. and Gupta, M.C., 1993, March. Genetic algorithm based approach for designing computer network topology. In *Proceedings of the 1993 ACM conference on Computer science* (pp. 358-365).

Faircloth, J. (2013). *Enterprise Applications Administration*. Elsevier Science.

DelCoco, R.J., Kroeger, B.W. and Kurtz, J.J., Westinghouse Electric Corp, 1992. *Local area network with star topology and ring protocol*. U.S. Patent 5,127,067.

Bisht, N. and Singh, S., 2015. Analytical study of different network topologies. *International Research Journal of Engineering and Technology (IRJET)*, *2*(01), pp.88-90.

Orava, F. and Ramfelt, L. (2008). *Method of sending information through a tree and ring topology of a network system*. US7391771B2.

Cisco. n.d. *Cisco Catalyst 2960-24TT-L Switch*. [online] Available at: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-24tt-l-switch/model.html> [Accessed 7 April 2020].

Suzuki, K. and Jibiki, M., NEC Corp, 2006. *Router and network connecting method*. U.S. Patent Application 10/547,464.

Cisco. n.d. *Cisco 1941 Series Integrated Services Routers Data Sheet*. [online] Available at: <https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data\_sheet\_c78\_556319.html> [Accessed 8 April 2020].

Apps.cisco.com. n.d. *Cisco Servers*. [online] Available at: <https://apps.cisco.com/ccw/cpc/guest/content/ucsContentMain/ucsHome> [Accessed 8 April 2020].

Cisco. n.d. *Cisco Aironet 1140 Series Access Point Data Sheet*. [online] Available at: <https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/datasheet\_c78-502793.html> [Accessed 8 April 2020].

Dhamija, R., Tygar, J.D. and Hearst, M., 2006, April. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).

Wang, J., Herath, T., Chen, R., Vishwanath, A. and Rao, H.R., 2012. Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE transactions on professional communication*, *55*(4), pp.345-362.

Owasp.org. 2019. *OWASP Top Ten*. [online] Available at: <https://owasp.org/www-project-top-ten/> [Accessed 8 April 2020].

Owasp.org. (n.d.). *A5-Broken Access Control | OWASP*. [online] Available at: https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_A5-Broken\_Access\_Control [Accessed 8 April. 2020].

Ferraiolo, D., Kuhn, D.R. and Chandramouli, R., 2003. *Role-based access control*. Artech House.

Teraguchi, N.C.R.L.Y. and Mitchell, J.C., 2004. Client-side defense against web-based identity theft. *Computer Science Department, Stanford University. Available: http://crypto. stanford. edu/SpoofGuard/webspoof. pdf*.

Azure.microsoft.com. n.d. *Azure Active Directory | Microsoft Azure*. [online] Available at: <https://azure.microsoft.com/en-gb/services/active-directory/> [Accessed 8 April 2020].