Oisin Gibson - STUDENT

Friday, April 18, 2025

Secure Network Services

Network Company

Table of Contents

[Introduction 2](#_Toc195563532)

[IP Addressing 2](#_Toc195563533)

[Cisco setup 3](#_Toc195563534)

[Virtual Local Area Networks 4](#_Toc195563535)

[Web Server 5](#_Toc195563536)

[DNS Server 5](#_Toc195563537)

[Email Server 6](#_Toc195563538)

[Router Security 8](#_Toc195563539)

[Main Switch Security 9](#_Toc195563540)

[PC Firewalls 9](#_Toc195563541)

[Access Control Lists 11](#_Toc195563542)

[AAA Server 11](#_Toc195563543)

[Syslog Server 12](#_Toc195563544)

[Sniffer Tools 13](#_Toc195563545)

[RIP v2 15](#_Toc195563546)

[DHCP Snooping 16](#_Toc195563547)

[References 18](#_Toc195563548)

[Appendix 20](#_Toc195563549)

# Introduction

In today's digital landscape, a secure and efficient network infrastructure is essential. This report outlines the design, implementation, and security configuration of a network for Corona Fightback Solution, built using Cisco Packet Tracer. The network includes subnetting, VLAN segmentation, and various security protocols to ensure reliable connectivity and data protection.

Designed to support 200 staff members across multiple departments, the network uses a Class B address space (172.16.0.0/16), with each department assigned dedicated VLANs and subnets. Core services include application servers for research and marketing, an email server, and a web server accessible internally and externally.

Security is a central focus, with firewalls, ACLs, VLAN security, and encryption protocols in place to mitigate threats. Additional features beyond standard coursework were also implemented to improve network resilience.

This report covers the network topology, IP addressing, security features, and testing procedures, demonstrating the real-world application of network design and security best practices.

# IP Addressing

The project required the creation of an IP addressing table to ensure organized and sufficient IP allocation across six departments. A custom subnetting scheme was designed, assigning a unique subnet to each department and a dedicated one for essential services. This segmentation enhanced network performance, security, and management by reducing unnecessary inter-department traffic.(*IP Subnetting tutorial | How to subnet IPv4 addresses - YouTube*, no date)

To visualize the plan, an Excel spreadsheet was created detailing each subnet’s network address, subnet mask, usable IP range, and broadcast address, serving as a clear reference for implementation and troubleshooting.

For example, the Medical Research department was given the IP range 172.16.10.1 to 172.16.10.150, providing sufficient IPs while maintaining efficient use of address space. Rather than assigning IPs to every device, the first, middle, and last addresses in each subnet were used to demonstrate allocation—streamlining the process while illustrating the concept.

This structured approach ensured the network was scalable, manageable, and ready for future growth.

# Cisco setup

Using Cisco Packet Tracer (version 8.2.2.0400), a basic network topology was created. The design included multiple departments, each assigned the first, middle, and last IP addresses within their respective subnets.

Each department was connected to a switch, which in turn was linked to the main switch which then linked to the router. This setup ensured efficient communication and structured network segmentation.(*Small Organization Setup in Packet tracer | CCNA | Networkforyou*, 2022)

A diagram of a computer network

AI-generated content may be incorrect.

**Figure 1: Topology overview**

After establishing the foundational structure of the network, I assigned IP addresses to each device according to its respective department. Each device was configured with an IP address, default gateway, subnet mask, and DNS server IP. The network layout is illustrated below in **Figure 2**.A screenshot of a computer

AI-generated content may be incorrect.

**Figure 2: IP Configuration**

After configuring each device, I proceeded to the Main Router. At this stage, I assigned the default gateways for each department to their respective ports on the router, ensuring proper network segmentation and communication.(*How to assign IP address to Router Interface? | CCNA 200-301 | Networkforyou - YouTube*, 2023).

After assigning IP addresses to the ports, I proceeded to verify network connectivity between devices. To accomplish this, I selected a device from one end of the network, accessed the command prompt, and initiated a ping test to a device at the opposite end.

A screenshot of a computer program

AI-generated content may be incorrect.**F**

**Figure 3: Communication established**

# Virtual Local Area Networks

I configured VLANs to segment the physical network into multiple logical networks, assigning a unique VLAN ID to each department. For example, the Medical department was assigned VLAN 10, while Services was assigned VLAN 80, following a logical increment of 10 between VLANs for better organization and scalability.

This segmentation improved both the efficiency and security of the network. By isolating traffic within each VLAN, I was able to reduce unnecessary broadcast traffic and enhance overall performance. More importantly, sensitive data and critical systems are now isolated from less sensitive areas of the network, significantly reducing the risk of unauthorized access.

Additionally, VLANs allowed me to apply department-specific security policies, tailoring access control and firewall rules to the needs of each segment. While I initially followed a basic online tutorial for VLAN creation, I adapted the implementation to suit our specific organizational requirements. (*Configuring VLANS on Cisco Switches - YouTube*, 2017)

# Web Server

With device communication successfully established, I proceeded to set up the Web Server. This involved developing a simple company website and assigning a dedicated IP address to the Web Server. The website was accessible from the web browser of each device within the network, ensuring seamless internal access. (*How to configure HTTP service | Step-by-Step Guide: Setting up HTTP Service in Packet Tracer*, 2023)

A screenshot of a website

AI-generated content may be incorrect.

**Figure 4: Website setup**

# DNS Server

A Domain Name System (DNS) Server is responsible for translating human-friendly domain names into IP addresses, allowing users to access websites without needing to remember numerical addresses. In your network setup, the DNS Server was specifically used for providing access to the website by mapping its domain name to its corresponding IP address. This means that instead of entering an IP address in a web browser, users could simply type the website's domain name and be automatically directed to the correct server.

The way this works is straightforward: when a device requests access to the website, it sends a query to the DNS Server asking for the IP address associated with the domain name. The DNS Server then checks its records, retrieves the matching IP address, and sends it back to the requesting device. The device then uses this IP to establish a connection to the web server hosting the site. This process simplifies web access, making it more intuitive and user-friendly while reducing the chances of errors caused by manually entering an IP address. (*How to configure DNS Server | Step by step DNS server configuration*, 2024)

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 5: DNS**

# Email Server

I set up a shared email server to provide every user on the network with a personal email address. This allowed each member of the organization to communicate internally and externally through a centralized system.

Each user was manually added to the server, and email accounts were assigned accordingly. The setup ensured consistent communication across departments and simplified management by centralizing user email services.

While the configuration was based on a basic implementation, it effectively met the organization’s needs for reliable and accessible email communication. (*How to configure Email Server | Email Server configuration step by step in cisco packet tracer - YouTube*, 2023)

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 6: Email Server Set Up**

In order to test that the email server was working as expected I sent an email from the Receptionists department to the Medical Research department. I chose these departments as they are on opposite sides of the network.

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 7: Email Tester Working**

# Router Security

It was important for the main router to have security established. To do this I followed basic tutorials to install warning banners and enable secure passwords and establish authorized users.

A white background with black text

AI-generated content may be incorrect.

**Figure 8: Router security**

As shown in **Figure 8**, login banners—such as the MOTD (Message of the Day) and login banners—were configured on the network devices to display warning messages to users attempting access. While these banners do not provide direct security protection, they serve a critical legal and psychological role by clearly stating that access is restricted to authorized personnel only. This helps establish the organization's commitment to security and can serve as a deterrent to unauthorized users. In some jurisdictions, such warning banners may also have legal relevance, helping to support prosecution in cases of unauthorized access(*Configuration of MOTD | Login Banner | Cisco Packet Tracer*, 2023)

In addition to the use of banners, access control was enforced through user authentication mechanisms. A AAA (Authentication, Authorization, and Accounting) server was integrated with the router to ensure that only verified users could log into the system. The AAA model provides a centralized and scalable way of managing user credentials and policies. When users attempt to connect to the device, their credentials are validated against the AAA server, allowing for both secure authentication and activity tracking.

Alternatively, local authentication was also configured directly on the router’s CLI. This involved creating local user accounts with assigned usernames and passwords. These passwords were secured using cryptographic algorithms, such as MD5 hashing through the service password-encryption or secret command, making them significantly more difficult—if not impossible—to crack through conventional means. This adds an additional layer of protection against unauthorized access attempts(*How to Set Password on Cisco Router in Packet Tracer*, 2021)

Together, the use of warning banners, AAA authentication, and encrypted local credentials reinforces the overall security posture of the network, ensuring that access is tightly controlled and only granted to trusted users.

# Main Switch Security

The same security configuration process was also applied to the Main Switch to ensure a consistent and uniform security posture across all critical network devices. By implementing identical measures—such as login banners, user authentication via AAA or local credentials, and encrypted password storage—on both the Main Router and the Main Switch, the network was safeguarded from potential vulnerabilities that could arise from uneven security settings. This approach helps eliminate weak points in the infrastructure, ensuring that unauthorized access is prevented at every major access point. Standardizing security across both devices not only simplifies network management but also reinforces the overall integrity and reliability of the network’s access control policies.A black and white image of a person

AI-generated content may be incorrect.

**Figure 9: Switch security**

# PC Firewalls

Another security feature added to the network was the firewall configuration on individual PCs. This type of firewall acts as a local defense mechanism, allowing or blocking traffic based on specific rules set for each machine. While relatively simple in its implementation within Cisco Packet Tracer, it serves as an effective demonstration of host-based security.

The firewall was configured to permit or deny inbound traffic based on IP addresses. This means that each PC could control which other devices on the network were allowed to communicate with it, providing a layer of protection against unauthorized access or internal network threats.

To test this feature, the firewall was first applied to Medical PC1, where a rule was created to deny ICMP (ping) traffic from Medical PC120. As expected, Medical PC120 was no longer able to ping Medical PC1, confirming that the firewall was successfully filtering the traffic.

Similarly, on Marketing PC1, a firewall rule was set to deny ping requests from Medical PC1. Again, this rule worked as intended, blocking the ICMP packets and demonstrating the PC’s ability to control inbound communication on a per-device basis.

Although basic, this kind of configuration helps reinforce key security concepts like access control, traffic filtering, and segmentation within a network. In a real-world environment, host-based firewalls are commonly used in combination with network-level firewalls to provide defense in depth, ensuring that even if the network perimeter is breached, individual devices remain protected from unwanted access. (*Firewall Configuration using Cisco Packet Tracer | Network Security | Packet Tracer*, 2022)

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 10: Firewall set up on Medical PC1**

**A black screen with white text

AI-generated content may be incorrect.**

**Figure 11: Pinging Failure**

# Access Control Lists

An Access Control List (ACL) was configured as an example of traffic filtering between the Medical and Marketing departments. This involved entering a series of commands on the Main Switch, where the ACL was applied to control the flow of data based on predefined rules.

The ACL functioned as a gatekeeper, inspecting IP traffic and allowing or denying it based on the criteria set by the administrator. In this case, as illustrated in the figure below, the ACL was specifically designed to deny all IP traffic originating from the Medical department destined for the Marketing department. Meanwhile, all other IP traffic across the network was permitted.

This setup highlights how ACLs can be used to enforce network segmentation and security policies, helping to limit access between different parts of the network and reduce the risk of internal threats or unauthorized data sharing. (*CCNA DAY 42: Standard ACL Configuration Packet Tracer| How to Configure Standard Access Control List*, 2023)A close-up of a line

AI-generated content may be incorrect.

**Figure 12: Access Control List Sample**

# AAA Server

An Authentication, Authorization, and Accounting (AAA) Server was set up to manage and control access to network resources by enforcing centralized AAA policies. This setup ensures that only authorized users can access specific devices or services, while also tracking user activity and maintaining a centralized database of user credentials and access permissions.

In this network, the administrator holds the highest level of access privileges. The configuration was straightforward placing the AAA server on the network, assigning it an IP address, and then creating the appropriate username and password credentials relevant to the device being protected, in this case, the Main Router.

The router was then configured to authenticate users through the AAA server rather than relying on local credentials. This allows for more scalable and secure management of user access across the network.

To verify that the AAA server was functioning correctly, a login attempt was made on the Main Router. If the credentials were accepted and access was granted through the AAA server, the setup was confirmed to be successful.

This kind of setup is particularly valuable in larger or security-conscious environments, as it allows for centralized control, easier auditing, and stronger user accountability. (*RADIUS - AAA Configuration On Cisco Devices | Lab Packet Tracer | CCNA 200-301*, 2024)

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 13: AAA Server Set Up**

# Syslog Server

A Syslog Server was set up and connected to the Main Switch to give network admins a central place to collect and review logs from across the network. This makes it much easier to keep an eye on what’s happening, spot unusual behavior, and catch potential security issues early.

Getting it working on the switch was straightforward—it just involved pointing the logs to the Syslog Server’s IP address. Once that was done, the switch started sending system messages, like interface changes or security alerts, straight to the server.

As you can see in **Figure 14** below, the server is actively receiving and processing logs, giving the team a clear view of the network’s activity all in one place. It’s a simple setup, but uper effective for staying on top of things.(*How to Configure Syslog Server in Cisco Packet Tracer | Technical Hakim #SyslogConfiguration CCNA*, 2021)

A screenshot of a computer

AI-generated content may be incorrect.

**Figure 14: Syslog Sever activity**

# Sniffer Tools

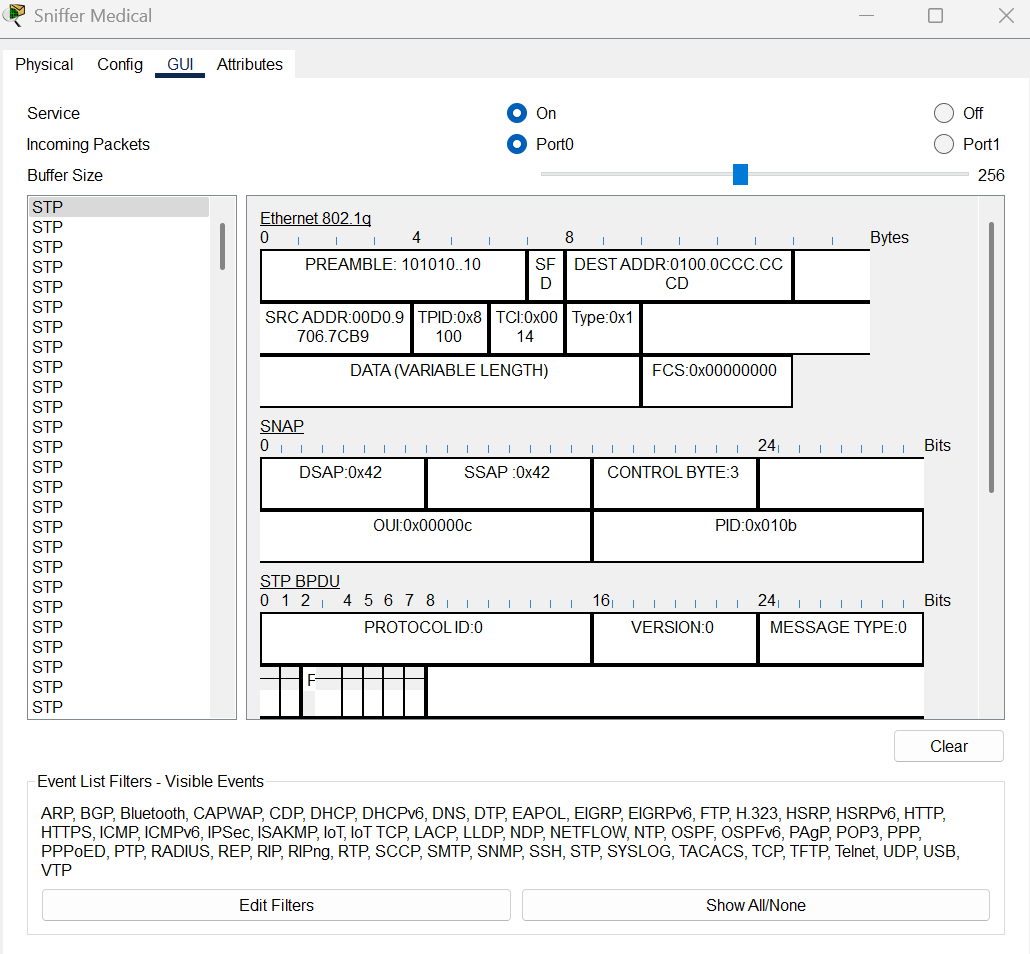
Sniffer tools were strategically placed between each department switch and the Main Switch, effectively allowing them to capture, monitor, and analyze real-time network traffic. By positioning these tools along the paths leading to the Main Router, they were able to observe the flow of data across critical segments of the network.

From a security standpoint, these tools play an essential role. They allow network administrators and security analysts to inspect communication patterns, spot unusual or suspicious behavior, and identify vulnerabilities in real-time. By capturing individual packets and displaying their contents—including source/destination IPs, protocols used, and metadata—these tools can reveal signs of unauthorized access attempts, malware activity, or misconfigured devices.

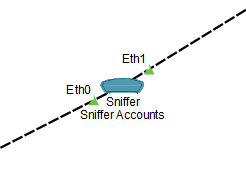
Sniffer tools also offer a hands-on way to learn about how different protocols operate on the network, making them valuable for both security monitoring and educational purposes. Whether it's analyzing DHCP handshakes, ARP broadcasts, or HTTP traffic, these insights help build a deeper understanding of how data travels across the network and where weaknesses might exist.

As for the setup, it was straightforward—simply placing the sniffer devices in-line between the switches and router and connecting the appropriate cables at both ends. Once in place, the devices began capturing packets immediately, providing full visibility into the traffic without disrupting network performance.

In a real-world environment, such tools are commonly used for intrusion detection, performance monitoring, and incident response, making them a key component of a proactive network security strategy. (*Using a sniffer in Packet Tracer*, 2019)



**Figure 15: Sniffer Tool Working**

****

**Figure 16: Sniffer Tool Placement**

# RIP v2

By implementing RIP version 2 (RIPv2), the network gains support for classless routing, which allows the use of subnet masks. This adds greater control and flexibility in IP address allocation, enabling more efficient use of address space and better network segmentation.

While RIPv2 doesn't offer robust built-in security features, it serves well in smaller networks like this one when combined with other security mechanisms. For example, when used alongside Access Control Lists (ACLs), RIPv2 can contribute to a more secure environment by limiting which devices or subnets can exchange routing information or access certain parts of the network. This layered approach helps enhance overall security despite the protocol’s simplicity. (*Configuring RipV2 in Packet Tracer*, 2016)

A screenshot of a computer program

AI-generated content may be incorrect.

**Figure 17: Router RIP**

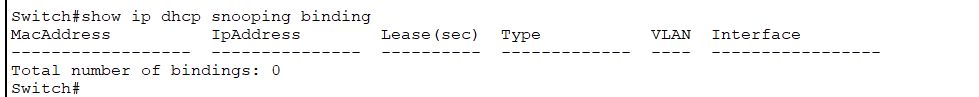
# DHCP Snooping

DHCP Snooping is an important security feature that was enabled on both the Main Router and Main Switch to protect the network from rogue DHCP servers and malicious IP configurations. It works by monitoring and filtering DHCP traffic at Layer 2, making sure only trusted devices can hand out IP addresses.

The setup involves marking certain ports as trusted—typically the ones connected to known DHCP servers—while all other ports are untrusted. Any suspicious DHCP messages on untrusted ports are blocked right away, helping prevent attacks like DHCP spoofing or man-in-the-middle threats.

DHCP Snooping also keeps a binding table that records valid client information, like MAC and IP addresses, VLANs, and ports. This not only boosts DHCP security but also supports other features like IP Source Guard and Dynamic ARP Inspection (DAI).

In short, DHCP Snooping helps create a more secure and trustworthy network by making sure only legitimate devices can assign IP addresses.(*►DHCP Spoofing Attack Explained Packet Tracer I IP dhcp snooping I Tons OF Network Fun*, 2023)



**Figure 18: DHCP Snooping Binding**

As seen in Figure – above, the DHCP Snooping binding table displays 0 bindings. This is because the IP addresses within the network were manually assigned rather than dynamically allocated by a DHCP server. This approach was intentionally chosen to demonstrate the full scope of the network, by manually selecting IP addresses from the beginning, middle, and end of the designated IP range.

While a DHCP server would typically be used in a real-world environment to streamline IP management and save time, the manual configuration method still allows for the implementation of essential DHCP-related security features, such as DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection. As such, the network retains the foundational protections expected in a DHCP-enabled setup, even without active DHCP traffic.

# References

*►DHCP Spoofing Attack Explained Packet Tracer I IP dhcp snooping I Tons OF Network Fun* (2023). Available at: https://www.youtube.com/watch?v=djJPo9U8Gsg (Accessed: 14 April 2025).

*CCNA DAY 42: Standard ACL Configuration Packet Tracer| How to Configure Standard Access Control List* (2023). Available at: https://www.youtube.com/watch?v=Bl6dZJq\_Wc0 (Accessed: 14 April 2025).

*Configuration of MOTD | Login Banner | Cisco Packet Tracer* (2023). Available at: https://www.youtube.com/watch?v=xfF4dmBIdds (Accessed: 14 April 2025).

*Configuring RipV2 in Packet Tracer* (2016). Available at: https://www.youtube.com/watch?v=2p0OWcoehnQ (Accessed: 14 April 2025).

*Configuring VLANS on Cisco Switches - YouTube* (2017). Available at: https://www.youtube.com/watch?v=c1R8dN8PCC0&ab\_channel=LearnTechTraining (Accessed: 11 April 2025).

*Firewall Configuration using Cisco Packet Tracer | Network Security | Packet Tracer* (2022). Available at: https://www.youtube.com/watch?v=yLOYd87z2jg (Accessed: 14 April 2025).

*How to assign IP address to Router Interface? | CCNA 200-301 | Networkforyou - YouTube* (2023). Available at: https://www.youtube.com/watch?v=-M4DhbQI7nE&ab\_channel=Networkforyou (Accessed: 4 April 2025).

*How to configure DNS Server | Step by step DNS server configuration* (2024). Available at: https://www.youtube.com/watch?v=CyEacSDD0V4 (Accessed: 5 April 2025).

*How to configure Email Server | Email Server configuration step by step in cisco packet tracer - YouTube* (2023). Available at: https://www.youtube.com/watch?v=y7v9EJyXo-Q&ab\_channel=ChiragBhalodia (Accessed: 11 April 2025).

*How to configure HTTP service | Step-by-Step Guide: Setting up HTTP Service in Packet Tracer* (2023). Available at: https://www.youtube.com/watch?v=eN4G7cyyoSo (Accessed: 4 April 2025).

*How to Configure Syslog Server in Cisco Packet Tracer | Technical Hakim #SyslogConfiguration CCNA* (2021). Available at: https://www.youtube.com/watch?v=aB1KJi7IkXw (Accessed: 14 April 2025).

*How to Set Password on Cisco Router in Packet Tracer* (2021). Available at: https://www.youtube.com/watch?v=-bVBKpnTGOg (Accessed: 14 April 2025).

*IP Subnetting tutorial | How to subnet IPv4 addresses - YouTube* (no date). Available at: https://www.youtube.com/watch?v=7hIbzlxbebc&ab\_channel=RichTechGuy (Accessed: 28 March 2025).

*RADIUS - AAA Configuration On Cisco Devices | Lab Packet Tracer | CCNA 200-301* (2024). Available at: https://www.youtube.com/watch?v=4xTQu7ULH3c (Accessed: 14 April 2025).

*Small Organization Setup in Packet tracer | CCNA | Networkforyou* (2022). Available at: https://www.youtube.com/watch?v=Teyqx0eb0zw (Accessed: 2 April 2025).

*Using a sniffer in Packet Tracer* (2019). Available at: https://www.youtube.com/watch?v=gsCSKQAVT2M (Accessed: 14 April 2025).

# Appendix

* Font: Arial
* Text Size: 12
* Reference Style: Harvard
* Word Count for Report (Not including Reference list): 3043
* Page Count: 21