Edge Hill University

The Department of Computer Science

CIS2706 Computer Networks

Coursework 1 – Network Design Report

2024/2025

Fahad Nasir 25788311

Bradley Roberts 25740423

Thomas Mason 26040247

Matthew Partington 25709488

Table of Contents

Introduction: 3
The Scope: 3
Functional Objectives of the scenario: 4
Network Requirement Analysis 4
Users and user requirements 4
Network and Service Requirements 5
The Storage, Reliability and Security Requirements 6
Hardware and Infrastructure Requirements 7
Assumptions 7
Logical Design 8
Logical network diagram 8
Logical Design Diagram 9
IP Addressing Plan 10
References 24

Guidelines:

1. All the explanation should be with proper references in Harvard Style.
2. The figures/tables should be captioned and embedded in the text.
3. The text should be justified and not left aligned and in the same font.
4. The structure of the report should be professional as in the template.

Contribution Table:

Fahad Nasir	Percentage of Contribution 25%
Bradley Roberts	Percentage of Contribution 22.5%
Thomas Mason	Percentage of Contribution 30%
Matthew Partington	Percentage of Contribution 22.5%

Introduction:

In this assignment we will be creating a case-study based design report, this means we will be given a case study and then must design, explain, and show how the designed network will meet the requirements of the company. In this case, the company we will be designing the network for is WLA, this is a small company with 18 employees based in Ormskirk, they provide asbestos containing materials to both large-scale commercial contracts and domestic contracts. The company requires the network for its singular head office in Ormskirk which will have laptops and PCs needing to be connected to the network as well as other possible mobile devices such as mobile phones. The company is also split into 3 divisions so security requirements should also be put in place to ensure better security of the company and that employees within each division only have access to the data they require.

The Scope:

Network Scope:

This network design is for a small company with a singular office and 18 employees; therefore, the network only must cover one floor and only accommodate 18 employees, however it is better if the network is able to accommodate more so the company can grow so the network should be able to accommodate more than this.

Network Scope	Details
Location	Ormskirk
Main Office	The company has a single office with 1 floor and 18 employees
Wi-Fi usage	Employees will require access to the internet and network on all their work devices, including mobile devices, therefore the Wi-Fi is required so they are able to access the internet and network from anywhere in the office on all their mobile devices. The Wi-Fi must be able to cover the entire office.
Devices	The company will be using PCs, laptops, mobile phones, and possibly printers.
Network Scaling	The network must be able to be expanded in the future when required to accommodate a larger network with more devices.

Functional Objectives of the scenario:

The proposed network design will need to functional and meet all the functional objectives to function as intended for the business and be usable as a network.

Secure Communication: The network needs to be able handle of the traffic that will be travelling over the network while the employees are using the network for the business, However, this sensitive data travelling on the network must be secure. This means that the network must be secure from unauthorised users trying to gain access to the network so they can access the network traffic and steal data, as well as secure data on the network from users already on the network to keep the companies network data safe.

Seamless Communication: In order not to affect the operation of the business, the network must provide seamless communication for anyone using the network. This means that employees won't be hindered due to slow connection on the network, having to wait for data to send over the network, or communication problems with other devices on the network such as printers or computers.

Resource Sharing: Any device that needs to be able to connect to the network should be able to connect such as printers, scanners, databases and any other machine or data that would need to be remotely accessed.

Centralized monitoring and network management: Using one network for the whole office of WLA means that the network is easily monitored and all suspicious activity on the network can be detected and addressed quickly, Furthermore, managing one centralized network will be more efficient and reduce downtime.

(Ahmed, 2024)

Network Requirement Analysis

Users and user requirements

General Office Staff:

General Office employees do daily day to day activities. The user requirements are access to shared files, printers and databases. A network is also needed for doing daily communications via email and doing online tasks. (Parker, 2012)

Contracts Managers and Administrators:

The Contracts Managers and Administrators at WLA are vital for managing projects and making successful operations. The requirements needed are secure storage and practical tools to communicate with external workers. (Parker, 2012)

Accounts Team:

The Accounts Team manages finance using calculation tools. User requirements for the accounting team is storing data in a secure place and accessing tools easily. (Parker, 2012)

Field Technicians:

Field technicians operate mostly outside of the workplace. Technicians require secure remote access to systems via VPN and stable connectivity to perform tasks. (Parker, 2012)

IT Support Staff:

IT Support Staff manages the network. Support Staff require tools for monitoring, troubleshooting, and updating the network without interrupting employees. (Parker, 2012)

Network and Service Requirements

Network Requirements

Top Priority Core:

Making sure that Router2, Multilayer Switch2, and servers File Server, Backup Server work without delay. Setting up multiple connections or backups plans for important network systems. Allowing a computing plan of new devices (eg, PCs in General Office or Accounts) without redesigning. (CISCO, 2025)

For further development, implementing a programmable networking structure. Using VLANs setup the computer network and traffic is for departments General Office, Accounts, and Contracts Manager. To prevent unauthorised access, using strong encryption and secure setups on access points (0, 1, 2). Setting up Router2 and Multilayer Switch2 to allow communication in-between VLANs traffic control. (CISCO, 2025)

Medium Priority Core:

Using DHCP Servers to randomly assign IP addresses, which makes simple device management connections across VLANs. To enable wireless signals from Access Points 0, 1, and 2 are strong logical traffic connections. Implementing Quality of Service (QoS) on Multilayer Switch 2 to arrange traffic for critical services such as file sharing and backups. (CISCO, 2025)

Low Priority Core:

Using network monitoring tools eg SNMP to monitor performance and identify problems with key devices such as Multilayer Switch2 and servers. Enabling cloud backup storage to improve backup and capacity.
To use networking devices and configurations to use IPv4 and IPv6. (CISCO, 2025) (Jackson, 2022)

Service Requirements

Critical Services:
Vital files and documents are stored systematically and accessible to all users. Making regular backups of critical data to restore in the case of a failure or theft. (Cisco, 2024)

Automating the use of IP addresses use to improve management while decreasing manual configuration errors. Allowing interaction between VLANs while maintaining security controls. (Cisco, 2024)

Non-Critical Services:

Supplying essential printing facilities to employees in the General Office VLAN. The host websites or applications internally employees needed. (Cisco, 2024)

Value-Added Services:

Providing guests with limited access to the internet via VLAN on Access Points to keep guest traffic separate from internal activities. Assisting VoIP communications for departments such as Accounts, if required. (Cisco, 2024)

The Storage, Reliability and Security Requirements

Storage Requirements

Top Priority – Implement a network with enough storage to hold all the businesses and customers data. This of course will require multiple terabytes of storage and therefore will need multiple methods of storage such as NAS(Network attached storage), Local device drives and cloud storage. (Bigelow, Lutkevich and Kranz, 2022)

Medium Priority – Implement data backup of the network storage on an intermittent schedule, this ensures all the data is not lost if a data breach occurs, if data is corrupted or for instance all the physical devices are destroyed. The cloud storage ensures all the data will not be lost if the drives are physically destroyed and the separate drives are used to ensure quick retrieval of data if the current data drive loses the prospective data.

Least Priority – Ensure enough cloud storage is available for remote use, this allows employees to access the businesses data remotely so that in the event of being unable to attend the office they can carry on working from home or whiles travelling.

Reliability Requirements

High Priority - This is a simple but effective measure to ensure the reliability of the network, it ensures that the network is regularly maintained and update to ensure peak performance, security patches and constant improvements to the current network's productivity.

Medium Priority – If a HSRP were to be implemented then this would majorly improve the reliability of the Network, this is because if the main router were to fail in any way the backup router would step in so that the network can operate as if nothing had happened, this is what you call a failover system. (Cisco, 2023)

Low Priority – Another requirement to ensure the reliability of this network is as previously mentioned data backup, this ensures that in the event of data loss that the backup storage is instantly ready to be accessed so that business can carry on as usual.

Security Requirements

Top Priority—To improve the security of this network, access controls would be important. Access controls ensure that users without privileges cannot access sensitive data that can be used maliciously against the company or its customers.

Medium Priority – Another form of data security would be data encryption, this ensures that whiles data is sent from device to device if it was intercepted it would be accessed by the intruder.

Low Priority – Lastly software such as firewalls or anti-virus could be implemented to improve security even more as unwanted communication would be controlled/prohibited and the anti-virus ensures if any malware is on the computer or viruses then these can be recognised and deleted as soon as possible. (Anon, 2022)

Hardware and Infrastructure Requirements

1. Network Devices

- **Switches (3 Units)**: Connect devices within the office network, each representing each department.
- **Router (2 Unit)**: Connect the office to the internet and handle communication between departments securely.
- **Wireless Router (3 Units)**: These routers provide wired and wireless access to the network.
- **Multi-layer Switch(1 Unit)**: This device allows in-depth networking concepts like VLAN routing while acting as both a router and a switch.
- **DHCP Server(1 Unit)**: Gives all devices on the network a unique IP Address.

2. Storage Devices

- **Network Attached Storage (NAS) Server (1 Unit)**: Centralize file storage with secure access for each division which will be represented using a server which represents the NAS storage.
- **Backup Cloud server (1 Units)**: Implement a cloud server that simulates cloud storage to maintain on-site and off-site backups of critical data.
- **Devices(Multiple Units)**:Personal data and work will be stored in the physical device of the employee.

3. Security Hardware

- **Access Control Devices (e.g., Control the access of files) (1 Unit)**: Restrict physical access to network equipment by restricting which IP addresses can access the data.
- **Firewall (1 Unit)**: Protect the network by blocking unauthorized access.

Purpose:

- Each device ensures the network is secure, reliable, and functional for all 18 employees while meeting the company's division-based data segregation requirements.

Assumptions

- Vlan is logically inserted and signals via a multilayer switch.
- All devices are supported by ipv4 and ipv6 range for each vlan configuration.
- IP addresses are assigned with subnets for usage.

- Wireless devices are connected via access points with WPA3 encryption security system.
- Routers and firewall have the capability to handle NAT and secure VLAN configurations.
- The DHCP server is configured with IP addresses for static devices.
- ISP provide stable internet connections to the network design.
- Physical security is used to restrict access to network hardware components.
- They are no third-party services to handle the inside network usage.
  Listing assumptions to the design phase. (LINKEDIN, 2024)

Logical Design

The Logical Design outlines how the data is transmitted across the network in relation to the organization's requirements via communication in between VLANs such as the Server Room, Accounts Office, and Manager Office. By dividing up the network with VLANs and assigning unique subnets, the designed data runs smoothly, securely, and quickly in the system. (GEEKSFORGEEKS, 2024)

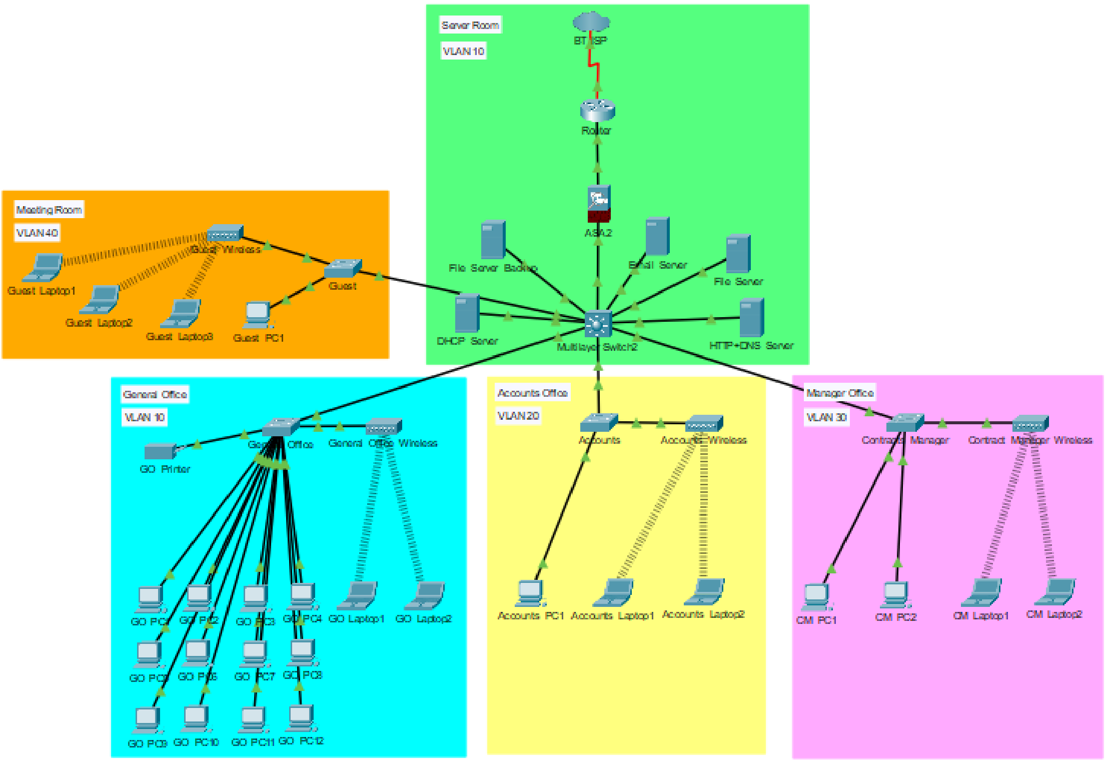
The network architecture is designed by using logical systems for networks. Network components connect VLANs addresses data patterns. Services such as DHCP, DNS, and NAT, are logically linked to secure network operations. (CISCO, 2025)

Logical Design outlines services, such as DHCP, DNS, NAT, equipment, network structure, and IP addresses to meet requirements. It provides VLANs, data flow, and the key components required for a secure network. (CISCO, 2025)

Logical network diagram

Addressing strategy (CISCO, 2025)
Subnetting – Each Vlan has its own IP range e.g. 192.168.10.5.
Static IP is used in gateways, servers, and critical devices.
Dynamic IP is assigning user devices via DHCP server.
NAT router is managing internet access to devices.
DNS- Local DNS server with back up to public DNS (8.8.8.8).
IP ranges from IPV4 to IPV6 for each VLAN.

Logical Design Diagram



VLAN Configuration (GEEKSFORGEEKS, 2024)

VLAN 10 (Server Room, General Office)

VLAN 20 (Accounts Office)

VLAN 30 (Manager Office)

VLAN 40 (Meeting Room)

The diagram includes different VLANs for segmenting network traffic.

Hardware Components

- Core Router is connecting BT ISP for WAN access.
- Multilayer Switch 2 is a central device for VLAN connection inside a router.
- ASA Firewall (ASA2) secures a network from an external attack via installing firewall.

Servers (CISCO, 2025)

File servers for storing files in meeting room, general office, accounts and managing office. Email servers manage email communications in between wla organisation and clients. DHCP Server randomly assigns IP addresses to devices. HTTP and DNS server Provides web services and domain name resolution. Access point connects devices in each vlan.

Software Requirements (CISCO, 2025)

Operating System Windows Server for files, email, and DHCP servers.

Linux operating system for HTTP and DNS servers.

Network Management Tools for monitoring and managing VLANs and traffic activity.

Security Tools are for Firewall configurations and monitoring devices.
Antivirus protection is used for client devices to be protected from a virus.

LAN Topology- Star topology with a central switch. VLANs make sures that traffic is sorted and active. Each office space has a dedicated access point and wired devices connected to the switch. (CISCO, 2025)

WAN Links (CISCO, 2025)

BT ISP is the primary connection to the Internet. Router handles WAN connections and communication between internal and external networks.

Services

DHCP Service assigns IP addresses to devices. DNS Services sorts hostnames to IP addresses. Email servers manage email communications in between wla organisation and clients. File servers for storing files in meeting room, general office, accounts and managing office. Wireless Access is available on all VLANs via APs. (CISCO, 2025)

IP Addressing Plan

Table 1: IP Table

Device/Hosts	IP Address	Network mask	Default Gateway
Accounts PC1	192.168.20.12	255.255.255.0	192.168.20.1
General Office PC1	192.168.10.37	255.255.255.0	192.168.10.1
Contract Manager PC1	192.168.30.14	255.255.255.0	192.168.30.1
Guest PC1	192.168.40.10	255.255.255.0	192.168.40.1

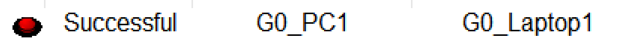
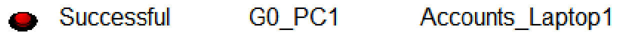
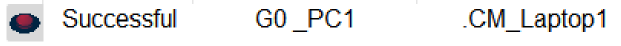
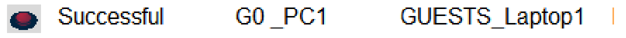
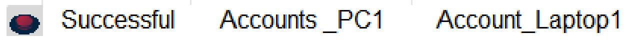
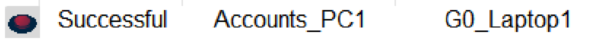
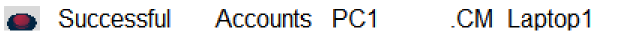
Table 2: IP Table

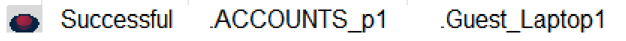
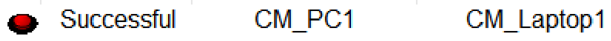
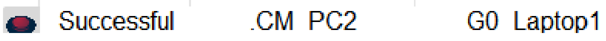
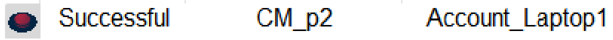
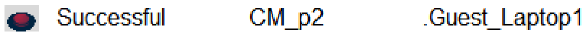
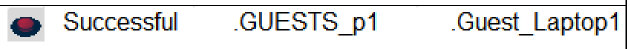
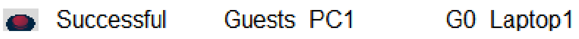
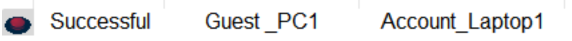
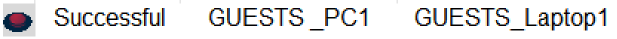
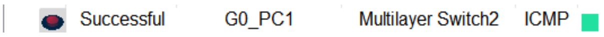
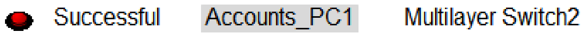
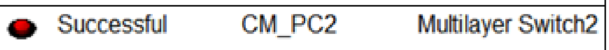
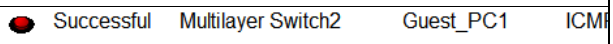
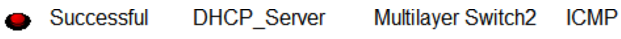
Device	IP Address	Network mask	Default Gateway
File_Server_Backup	192.168.10.5	255.255.255.0	192.168.10.1
DCHP_Server	192.168.10.2	255.255.255.0	192.168.10.1

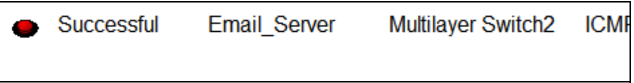
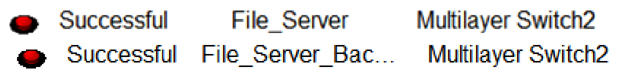
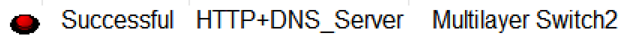
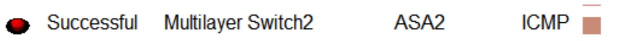
Email_Server	192.168.10.6	255.255.255.0	192.168.10.1
File_Server	192.168.10.3	255.255.255.0	192.168.10.1
HTTP+DNS_Server	192.168.10.4	255.255.255.0	192.168.10.1
MRPC1	192.168.40.10	255.255.255.0	192.168.40.1
Guest Laptop3	192.168.40.13	255.255.255.0	192.168.40.1
Guest Laptop2	192.168.40.12	255.255.255.0	192.168.40.1
Guest Laptop1	192.168.40.11	255.255.255.0	192.168.40.1
GOPrinter	192.168.10.33	255.255.255.0	192.168.10.1
GOlaptop1	192.168.10.35	255.255.255.0	192.168.10.1
GOlaptop2	192.168.10.34	255.255.255.0	192.168.10.1
GOPC1	192.168.10.37	255.255.255.0	192.168.10.1
GOPC2	192.168.10.13	255.255.255.0	192.168.10.1
GOPC3	192.168.10.28	255.255.255.0	192.168.10.1

GOPC4	192.168.10.31	255.255.255.0	192.168.10.1
GOPC5	192.168.10.21	255.255.255.0	192.168.10.1
GOPC6	192.168.10.41	255.255.255.0	192.168.10.1
GOPC7	192.168.10.10	255.255.255.0	192.168.10.1
GOPC8	192.168.10.22	255.255.255.0	192.168.10.1
GOPC9	192.168.10.27	255.255.255.0	192.168.10.1
GOPC10	192.168.10.14	255.255.255.0	192.168.10.1
GOPC11	192.168.10.25	255.255.255.0	192.168.10.1
GOPC12	192.168.10.40	255.255.255.0	192.168.10.1

Accounts PC1	192.168.20.12	255.255.255.0	192.168.20.1
Accounts Laptop1	192.168.20.10	255.255.255.0	192.168.20.1
Accounts Laptop2	192.168.20.11	255.255.255.0	192.168.20.1
CM PC1	192.168.30.14	255.255.255.0	192.168.30.1
CM PC2	192.168.30.13	255.255.255.0	192.168.30.1
CM PC3	192.168.30.11	255.255.255.0	192.168.30.1
CM PC4	192.168.30.12	255.255.255.0	192.168.30.1

Ping Trace	Description	Screenshot
VLAN 10	Vlan 10 to Vlan 10(GO _PC1) Pings to GO_Laptop1.	 ● Successful G0_PC1 G0_Laptop1
VLAN 10	Vlan 10 to Vlan 20GO _PC1) Pings to accounts_Laptop1.	 ● Successful G0_PC1 Accounts_Laptop1
VLAN 10	Vlan 10 to Vlan 30GO _PC1) Pings to cm_Laptop1.	 ● Successful G0 _PC1 .CM_Laptop1
VLAN 10	Vlan 10 to Vlan 40GO _PC1) Pings to Guest_Laptop1Guest_Laptop1.	 ● Successful G0 _PC1 GUESTS_Laptop1
VLAN 20	Vlan 20 to Vlan 20(Accounts_PC1) pings to accounts_Laptop1.	 ● Successful Accounts _PC1 Account_Laptop1
VLAN 20	Vlan 20 to Vlan 10(Accounts_PC1) pings to GO_Laptop1.	 ● Successful Accounts_PC1 G0_Laptop1
VLAN 20	Vlan 20 to Vlan 30(Accounts_PC1) pings to cm_Laptop1.	 ● Successful Accounts PC1 .CM Laptop1

VLAN 20	Vlan 20 to Vlan 40(Accounts_PC1) pings to Guest_Laptop1	 ● Successful .ACCOUNTS_p1 .Guest_Laptop1
VLAN 30	Vlan 30 to Vlan 30(CM_PC1)pings to cm_Laptop1.	 ● Successful CM_PC1 CM_Laptop1
VLAN 30	Vlan 30 to Vlan 10(CM_PC2)pings to GO_Laptop1.	 ● Successful .CM PC2 G0 Laptop1
VLAN 30	Vlan 30 to Vlan 20(CM_PC2) Pings to accounts_Laptop1.	 ● Successful CM_p2 Account_Laptop1
VLAN 30	Vlan 30 to Vlan 40(CM_PC2) pings to Guest_Laptop1	 ● Successful CM_p2 .Guest_Laptop1
VLAN 40	Vlan 40 to Vlan 40(Guest _PC1)pings to Guest_Laptop1.	 ● Successful .GUESTS_p1 .Guest_Laptop1
VLAN 40	Vlan 40 to Vlan 10(Guest _PC1)pings to GO_Laptop1.	 ● Successful Guests PC1 G0 Laptop1
VLAN 40	Vlan 40 to Vlan 20(Guest _PC1)pings to accounts_Laptop1.	 ● Successful Guest _PC1 Account_Laptop1
VLAN 40	Vlan 40 to Vlan 30 (Guest _PC1)pings to guest_Laptop1.	 ● Successful GUESTS _PC1 GUESTS_Laptop1
VLAN 10 (Server Room, General Office) GO _PC1	VLAN 10 PINGS TO THE multilayer Switch. (GO _PC1)	 ● Successful G0_PC1 Multilayer Switch2 ICMP 🟩
VLAN 20 (Accounts Office) Accounts_PC1	VLAN 20 PINGS TO THE multilayer Switch. (Accounts_PC1)	 ● Successful Accounts_PC1 Multilayer Switch2
VLAN 30 (Manager Office) CM_PC2	VLAN 30 PINGS TO THE multilayer Switch. (CM_PC2)	 ● Successful CM_PC2 Multilayer Switch2
VLAN 40 (Meeting Room) Guest _PC1	VLAN 40 PINGS TO THE multilayer Switch. (Guest _PC1)	 ● Successful Multilayer Switch2 Guest_PC1 ICMP
DCHP_Server	DCHP_Server pings to the multilayer Switch.	 ● Successful DHCP_Server Multilayer Switch2 ICMP

Email_Server	Email_Server pings to the multilayer Switch.	 ● Successful Email_Server Multilayer Switch2 ICMP
File_Server	File_Server pings to the multilayer Switch.	 ● Successful File_Server Multilayer Switch2 ● Successful File_Server_Bac… Multilayer Switch2
HTTP+DNS_Server	HTTP+DNS_Server pings to the multilayer Switch.	 ● Successful HTTP+DNS_Server Multilayer Switch2
ASA	ASA pings to the multilayer Switch.	 ● Successful Multilayer Switch2 ASA2 ICMP ■

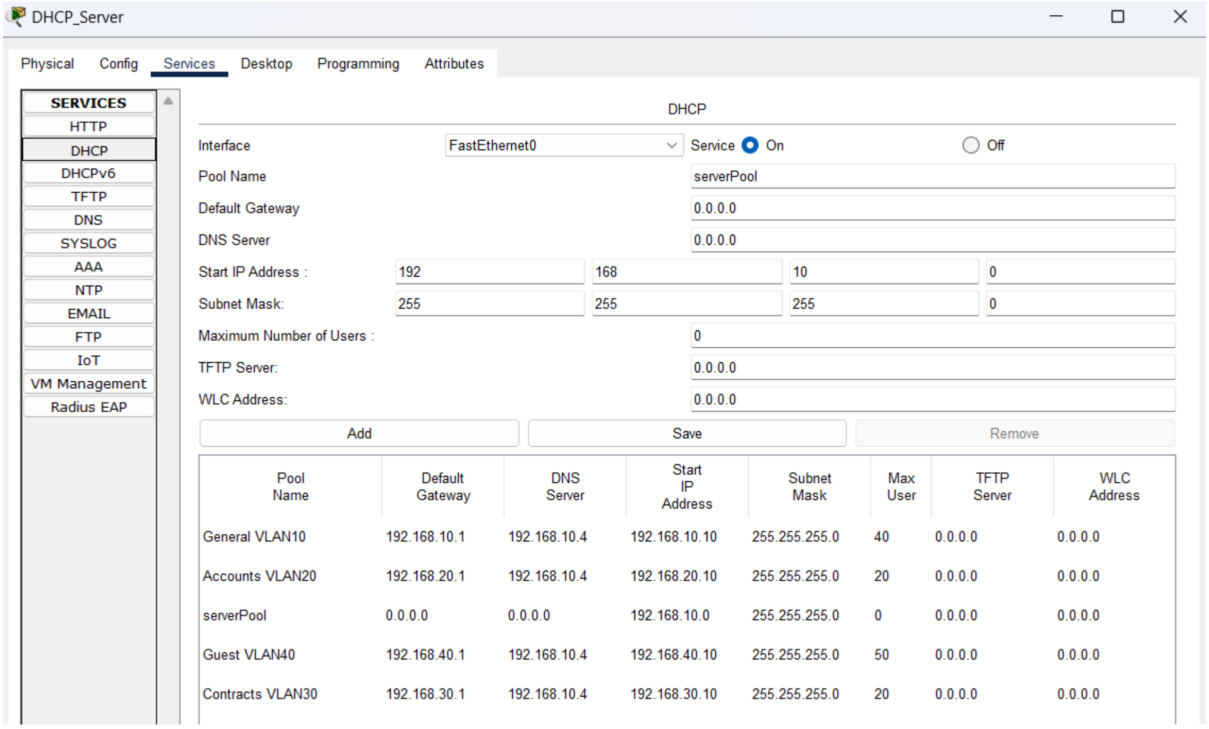
Clearly describe the use of NAT and VLAN if any.

VLANs allow the segmentation of a single network into multiple departments/VLANs inside a single network, for example in our network we had multiple departments with their own VLAN which are Server room, Meeting room, General office, Accounts Office and the Manager Office. To allow each VLAN to communicate with each other we had implement a three-layer switch. (Harmoush, 2016)

Screenshots of Network Setup.

Servers:

Image 1, DCHP Server Setup:



DHCP_Server

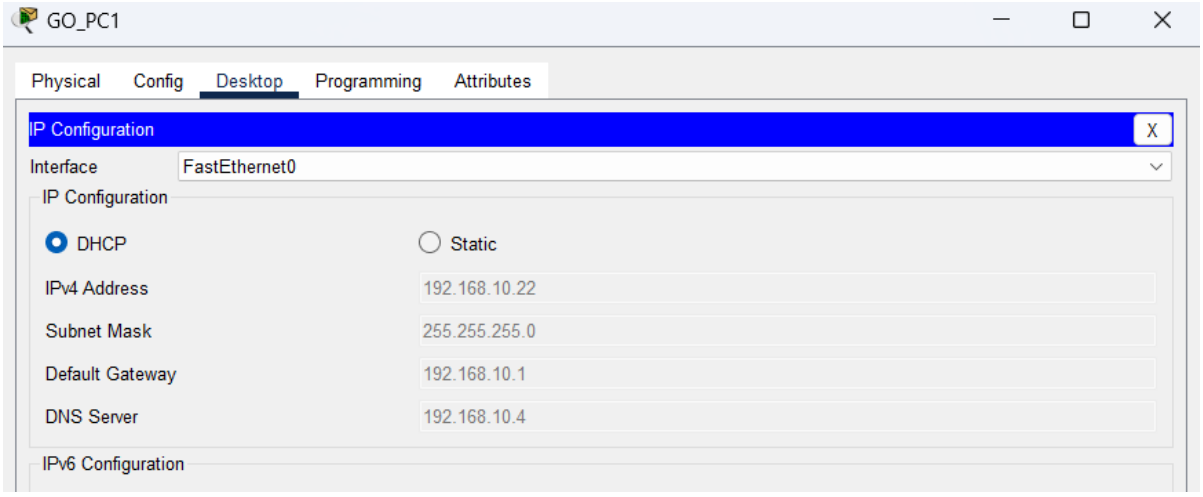
DHCP

Interface: FastEthernet0 — Service ● On ○ Off

Pool Name	serverPool
Default Gateway	0.0.0.0
DNS Server	0.0.0.0
Start IP Address :	192 . 168 . 10 . 0
Subnet Mask:	255 . 255 . 255 . 0
Maximum Number of Users :	0
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
General VLAN10	192.168.10.1	192.168.10.4	192.168.10.10	255.255.255.0	40	0.0.0.0	0.0.0.0
Accounts VLAN20	192.168.20.1	192.168.10.4	192.168.20.10	255.255.255.0	20	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.10.0	255.255.255.0	0	0.0.0.0	0.0.0.0
Guest VLAN40	192.168.40.1	192.168.10.4	192.168.40.10	255.255.255.0	50	0.0.0.0	0.0.0.0
Contracts VLAN30	192.168.30.1	192.168.10.4	192.168.30.10	255.255.255.0	20	0.0.0.0	0.0.0.0

Image 2, example of DCHP working on GO_PC1 and Accounts_Laptop1:



GO_PC1

IP Configuration

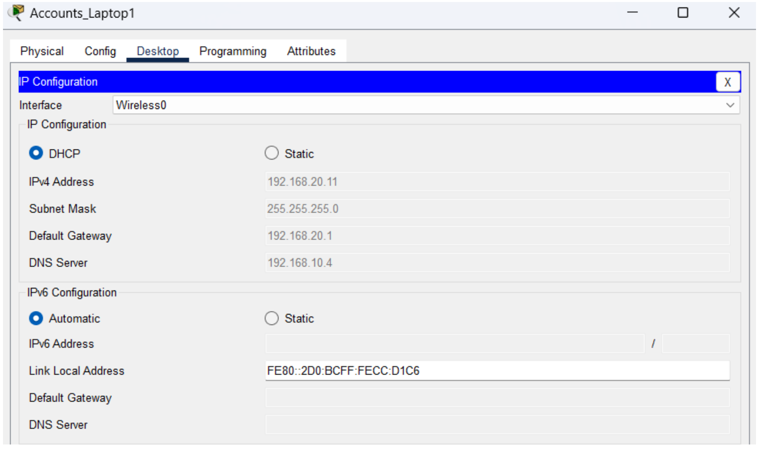
Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address	192.168.10.22
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	192.168.10.4

IPv6 Configuration



Accounts_Laptop1

IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static

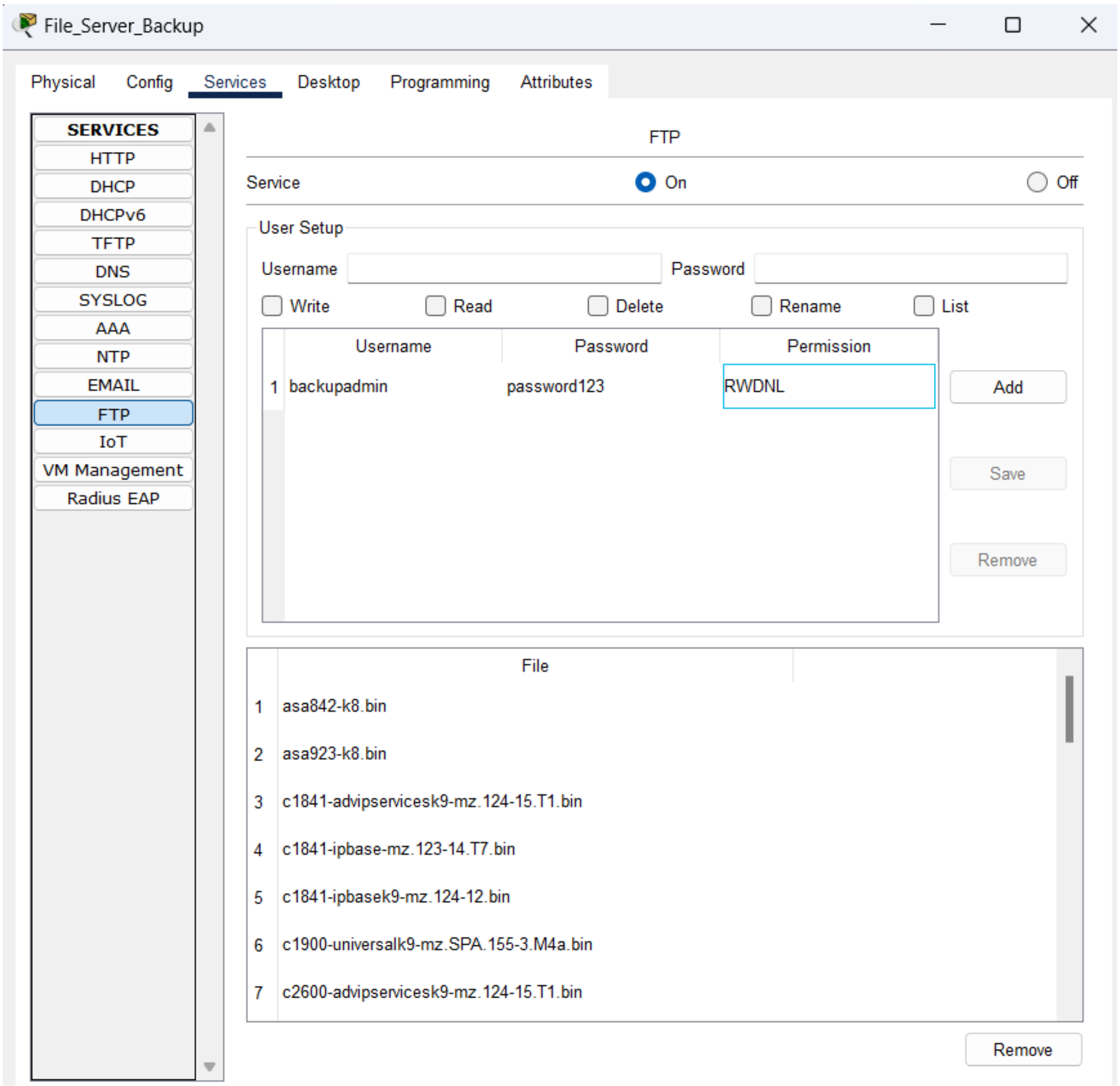
IPv4 Address	192.168.20.11
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	192.168.10.4

IPv6 Configuration

● Automatic ○ Static

IPv6 Address	/
Link Local Address	FE80::2D0:BCFF:FECC:D1C6
Default Gateway	
DNS Server	

Image 3, FTP Server Setup:



FTP

Service ● On ○ Off

User Setup

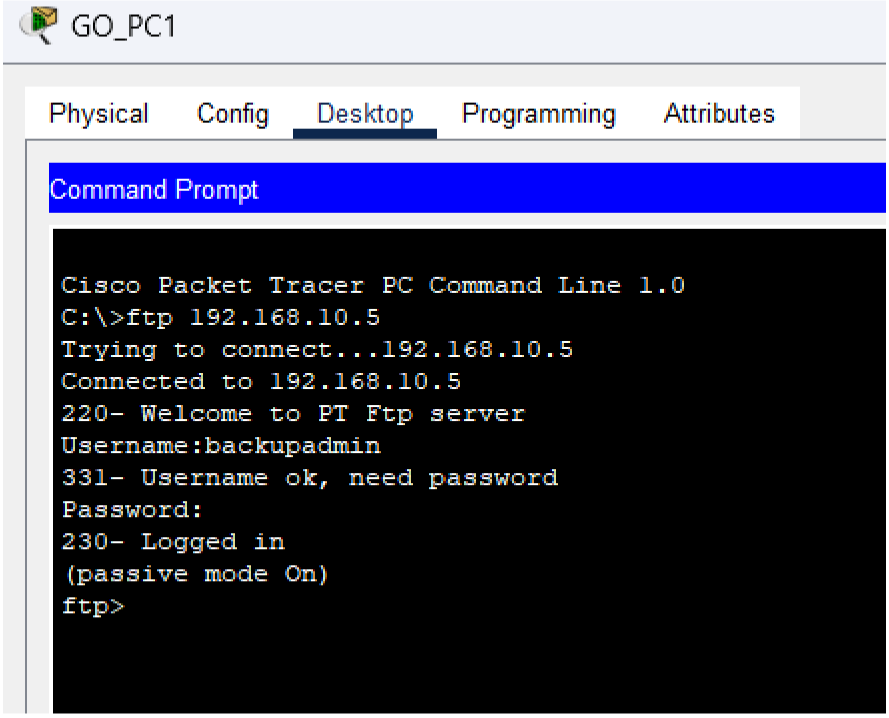
Username Password

□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	backupadmin	password123	RWDNL

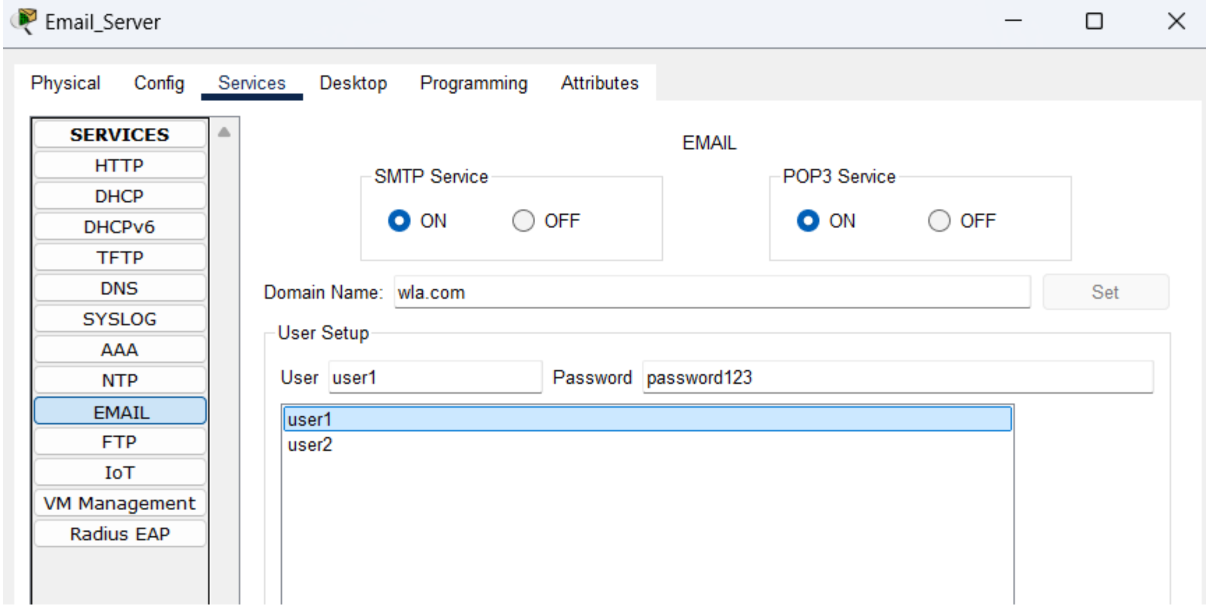
	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin
7	c2600-advipservicesk9-mz.124-15.T1.bin

Image 4, example of FTP Server Backup working on GO_PC1



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.10.5
Trying to connect...192.168.10.5
Connected to 192.168.10.5
220- Welcome to PT Ftp server
Username:backupadmin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Image 5, Email Server Setup:



SMTP Service ● ON ○ OFF

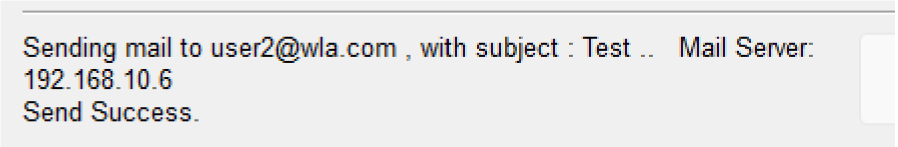
POP3 Service ● ON ○ OFF

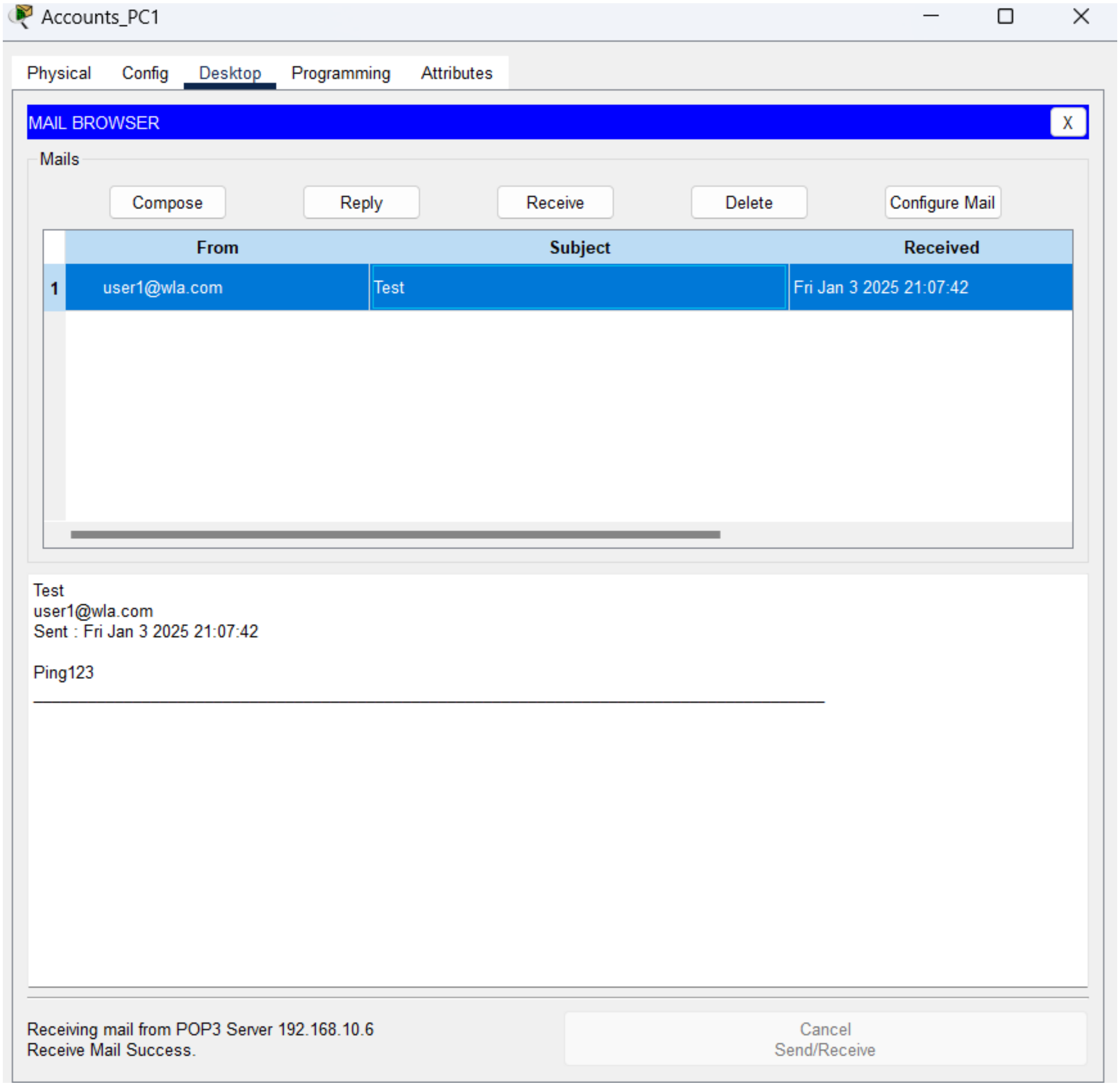
Domain Name: wla.com

User user1 Password password123

user1
user2

Image 6, Sending Email from User 1 to User 2:


Sending mail to user2@wla.com , with subject : Test .. Mail Server: 192.168.10.6
Send Success.



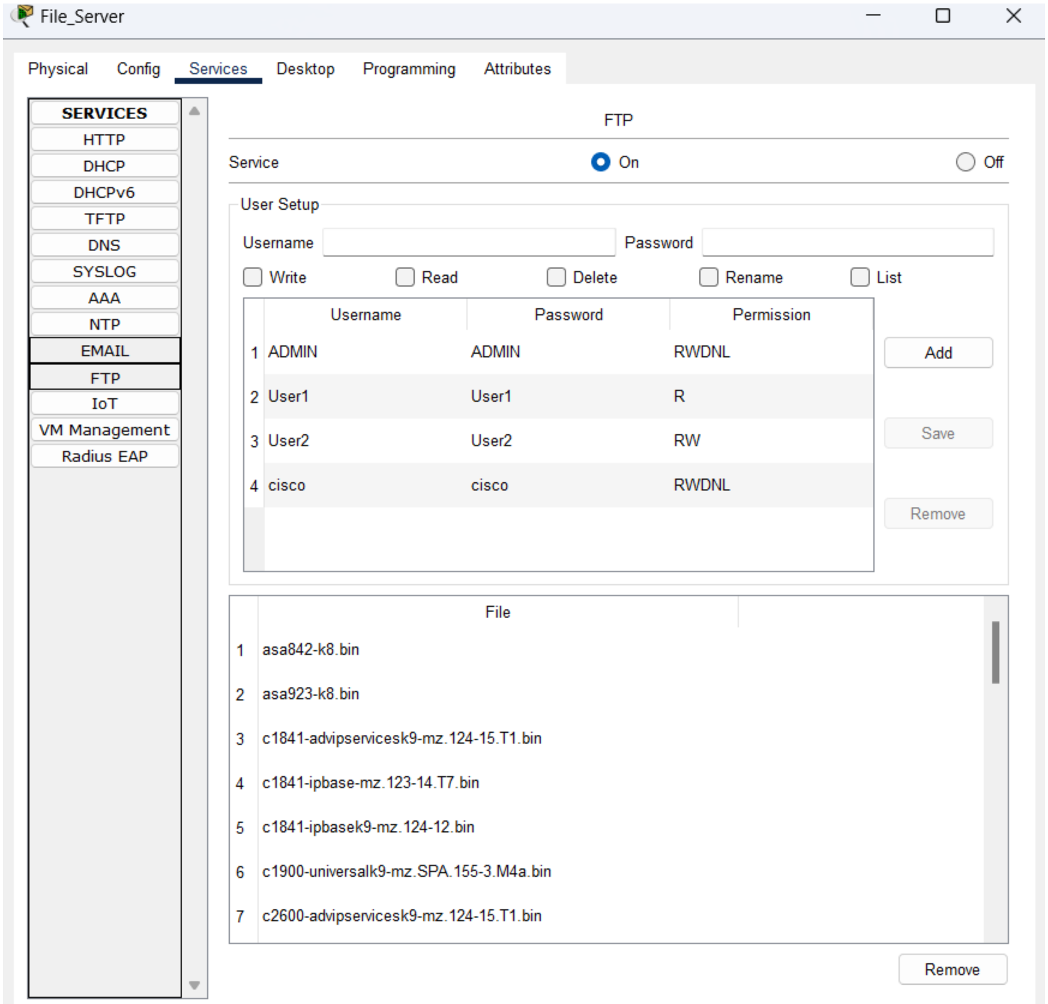
	From	Subject	Received
1	user1@wla.com	Test	Fri Jan 3 2025 21:07:42

Test
user1@wla.com
Sent : Fri Jan 3 2025 21:07:42

Ping123

Receiving mail from POP3 Server 192.168.10.6
Receive Mail Success.

Image 7, FTP File Server Setup:



Service ● On ○ Off

User Setup

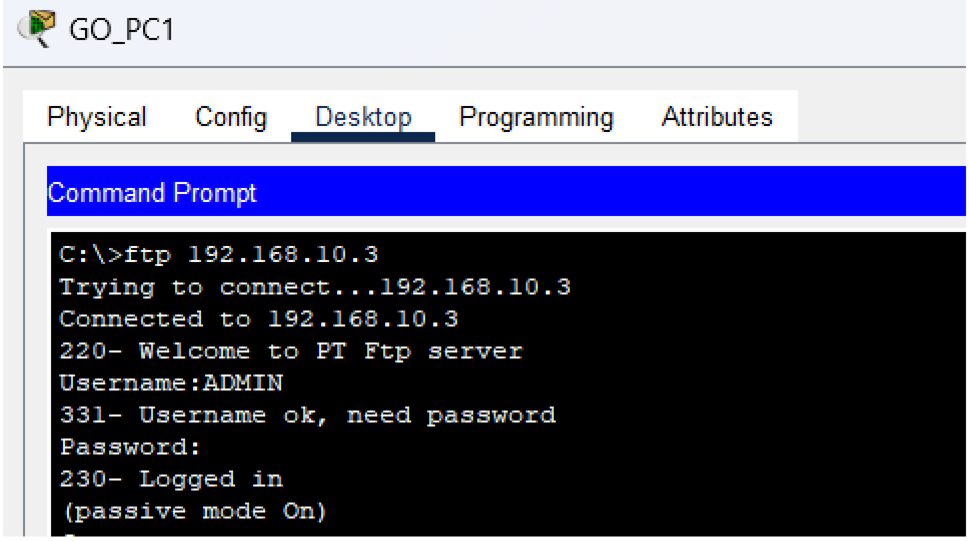
Username Password

□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	ADMIN	ADMIN	RWDNL
2	User1	User1	R
3	User2	User2	RW
4	cisco	cisco	RWDNL

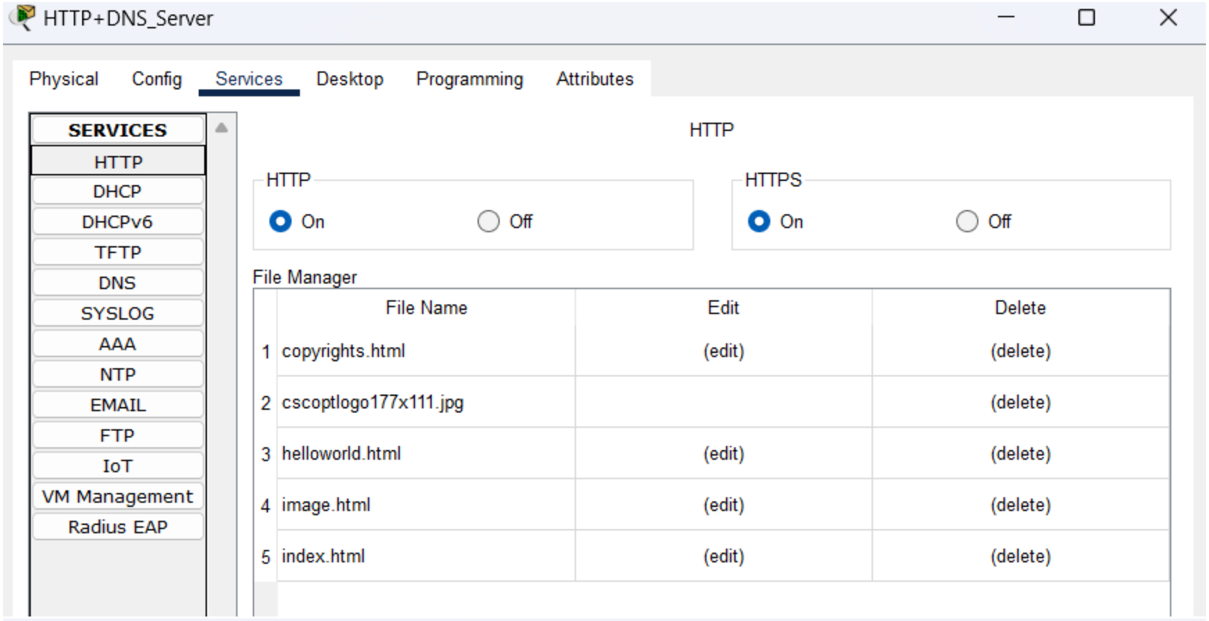
	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin
7	c2600-advipservicesk9-mz.124-15.T1.bin

Image 8, example of FTP File Server working on GO_PC1



```
C:\>ftp 192.168.10.3
Trying to connect...192.168.10.3
Connected to 192.168.10.3
220- Welcome to PT Ftp server
Username:ADMIN
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

Image 9, example of HTTP on HHTP+DNS Server.



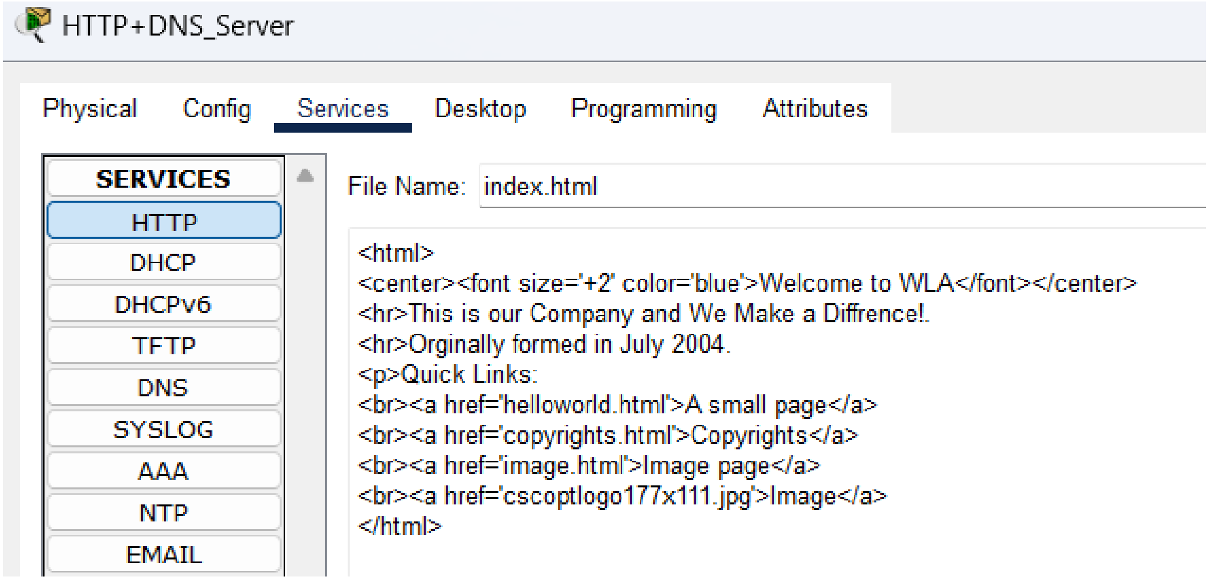
HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

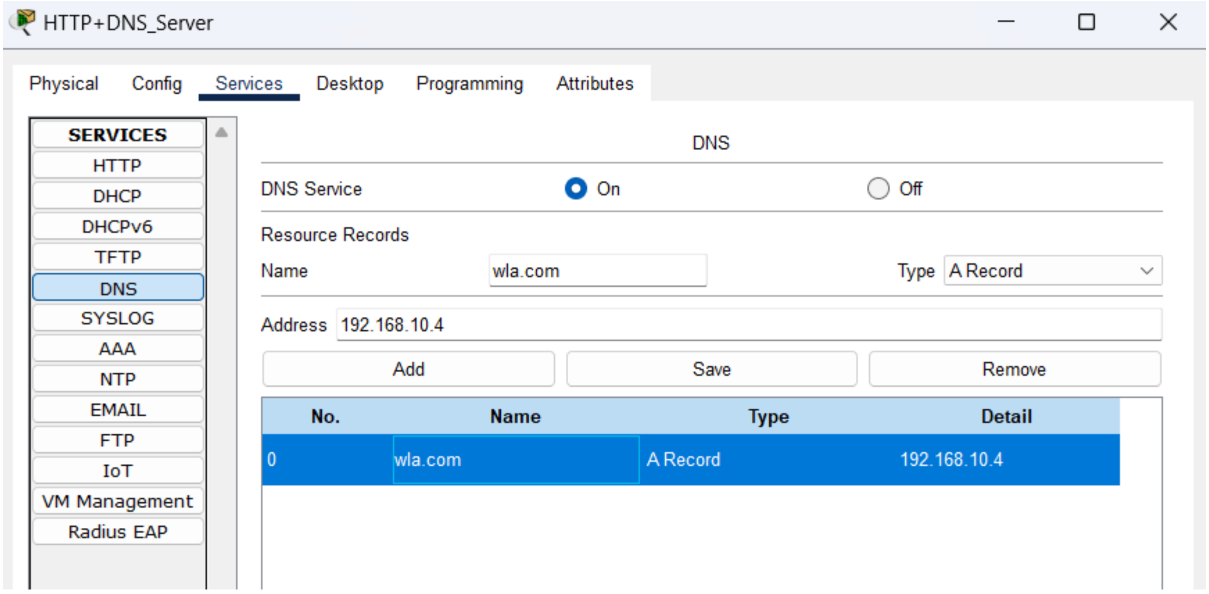
	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)



File Name: index.html

```
<html>
<center><font size='+2' color='blue'>Welcome to WLA</font></center>
<hr>This is our Company and We Make a Diffrence!.
<hr>Orginally formed in July 2004.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

Image 10, example off DNS working on HTTP+DNS Server.



DNS Service ● On ○ Off

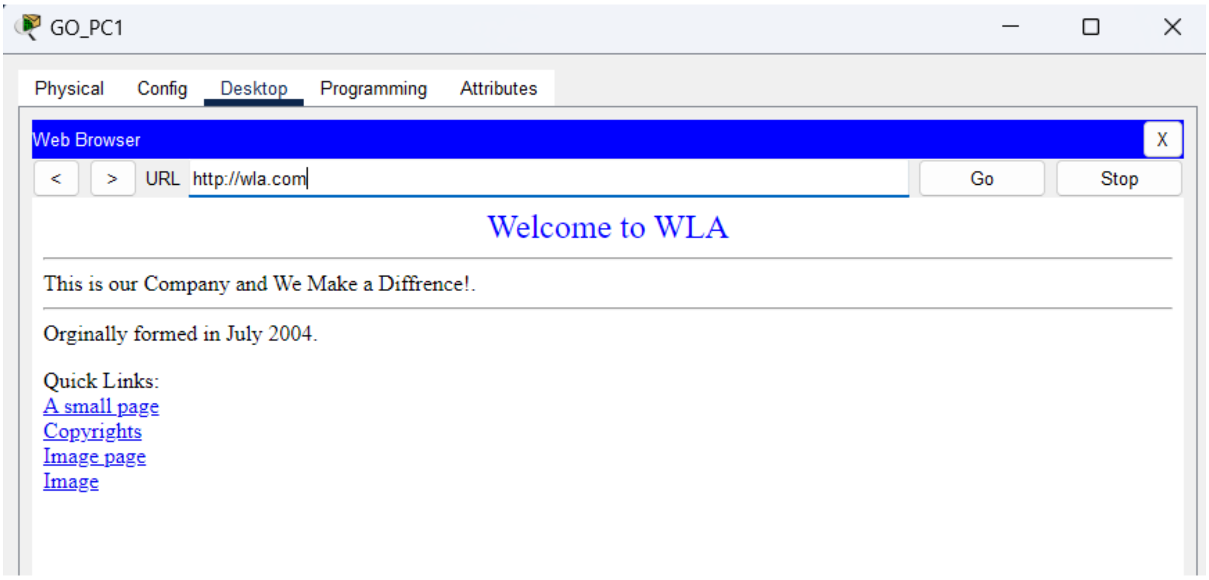
Resource Records

Name wla.com Type A Record

Address 192.168.10.4

No.	Name	Type	Detail
0	wla.com	A Record	192.168.10.4

Image 11, example of HTTP+DNS Server working on GO_PC1



URL http://wla.com

Welcome to WLA

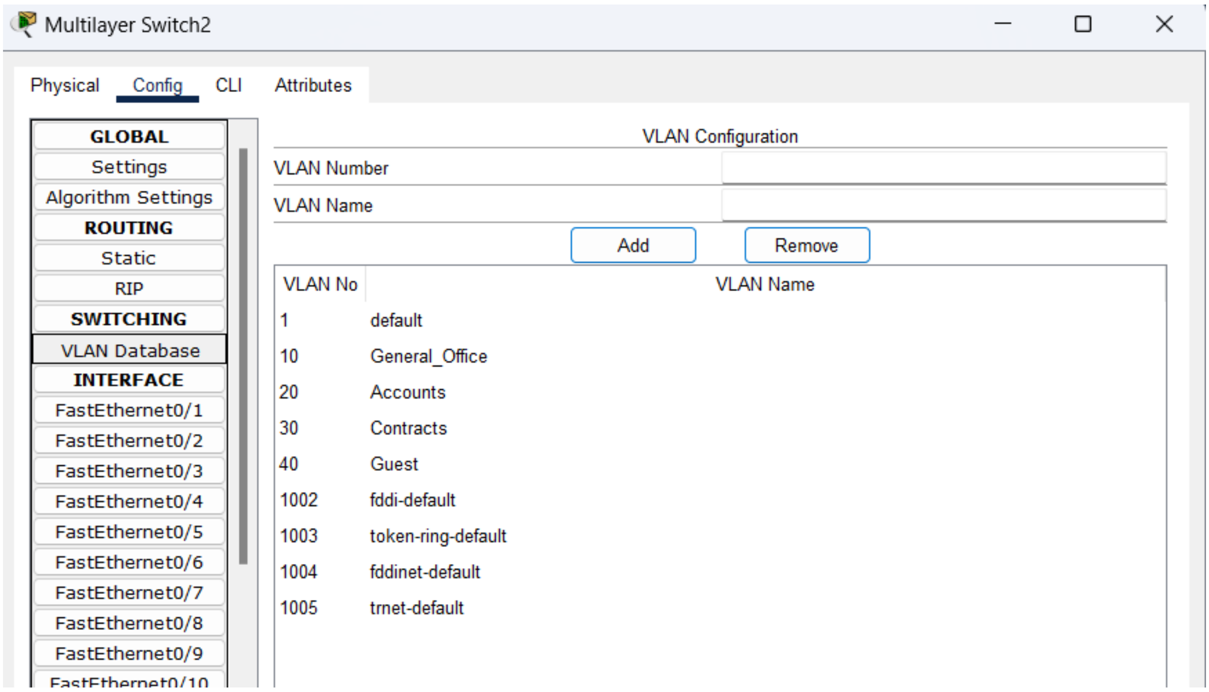
This is our Company and We Make a Diffrence!.

Orginally formed in July 2004.

Quick Links:
A small page
Copyrights
Image page
Image

Multilayer Switch Setup

Image 12, VLAN Setup on Multilayer Switch



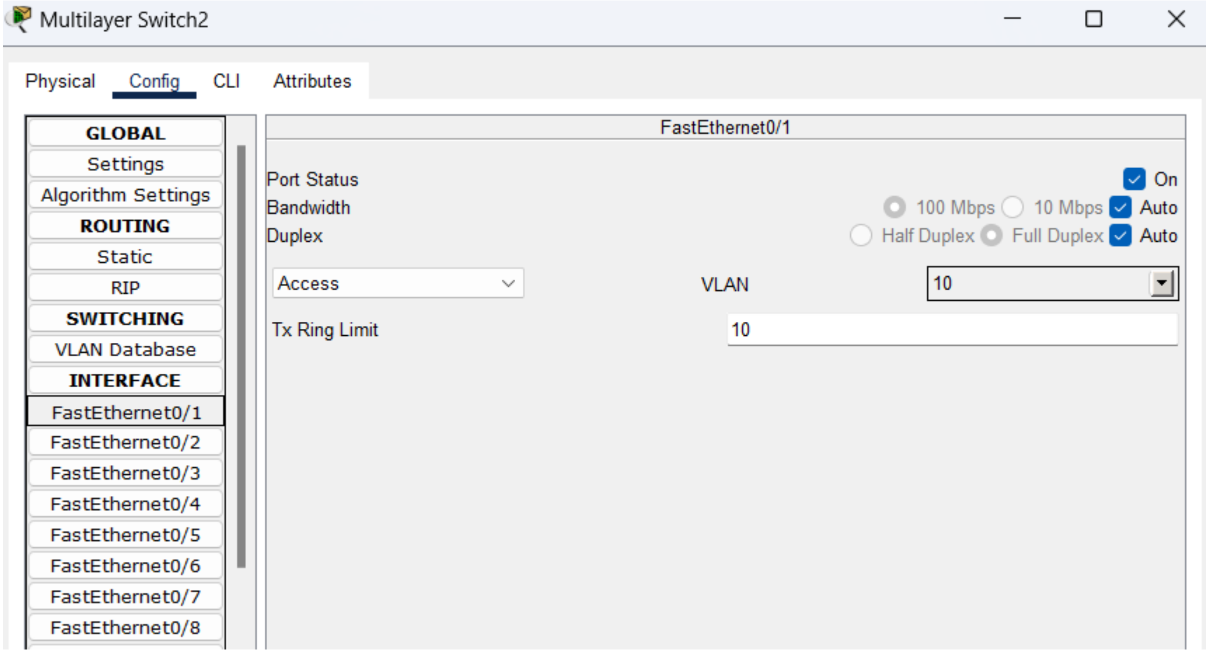
VLAN Configuration

VLAN Number

VLAN Name

VLAN No	VLAN Name
1	default
10	General_Office
20	Accounts
30	Contracts
40	Guest
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Image 13, Example of VLAN Setup on Ethernet 1.



FastEthernet0/1

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

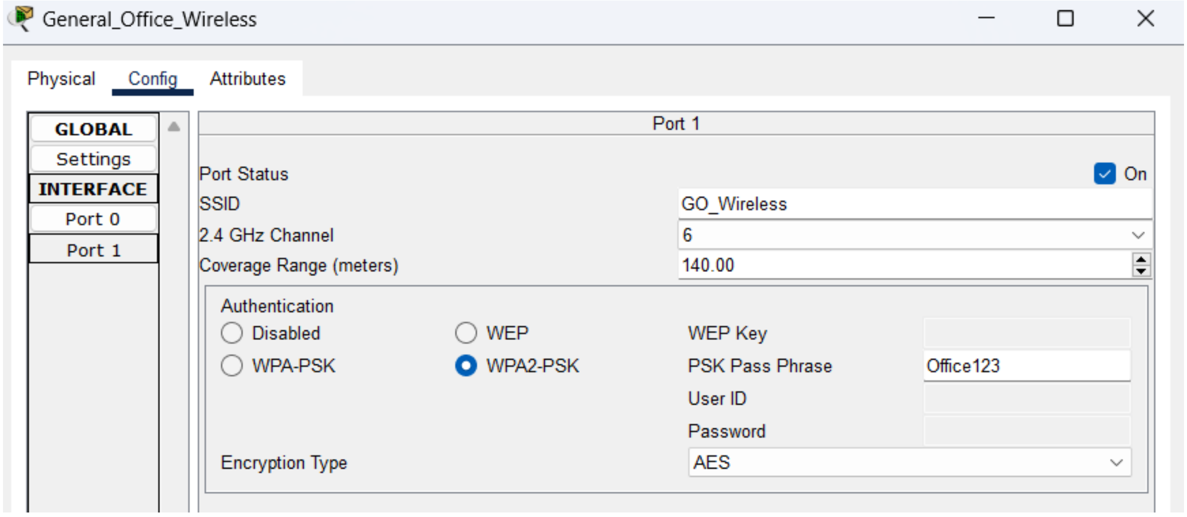
Access

VLAN 10

Tx Ring Limit 10

Wireless Access Point

Image 14, Setup Example of Wireless Accesspoint



General_Office_Wireless

Port 1

Port Status ☑ On

SSID: GO_Wireless

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: Office123

User ID:

Password:

Encryption Type: AES

References

Cisco, 2024. *Configuring VLANs*. [Online]
Available at: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html
[Accessed 21 12 20224].

CISCO, 2025. *Network Requirements for Secure Access*. [Online]
Available at: https://docs.sse.cisco.com/sse-user-guide/docs/network-requirements-for-secure-access
[Accessed 05 01 2025].

GEEKSFORGEEKS, 2024. *configuring-and-verifying-vlans-in-cisco*. [Online]
Available at: https://www.geeksforgeeks.org/configuring-and-verifying-vlans-in-cisco/
[Accessed 05 01 2025].

LINKEDIN, 2024. *What are the best tools and methods for documenting design assumptions?*. [Online]
Available at: https://www.linkedin.com/advice/3/what-best-tools-methods-documenting-design
[Accessed 23 23 12].

Parker, J., 2012. *Business, User, and System Requirements*. [Online]
Available at: https://enfocussolutions.com/business-user-and-system-requirements/
[Accessed 05 01 2024].

ANON, 2022. Basic Firewall Configuration in Cisco Packet Tracer. *GeeksforGeeks* [online]. Available from: https://www.geeksforgeeks.org/basic-firewall-configuration-in-cisco-packet-tracer/.

BIGELOW, S., LUTKEVICH, B., and KRANZ, G., 2022. What is Network-Attached Storage (NAS) and How Does it Work? *SearchStorage* [online]. Available from: https://www.techtarget.com/searchstorage/definition/network-attached-storage.

CISCO, 2023. Hot Standby Router Protocol Features and Functionality. *Cisco* [online]. Available from: https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html.

HARMOUSH, E., 2016. Routing Between VLANs – Practical Networking .net. *Practical Networking .net* [online]. Available from: https://www.practicalnetworking.net/stand-alone/routing-between-vlans/.

Ahmed, F. (2024). The Power of Wireless Connectivity: Empowering Seamless Communication and Data Exchange. [online]

Available from: https://daisyuk.tech/resource/the-power-of-wireless-connectivity-

Jackson, K. (2022). *What is SNMP? How Does SNMP Work? | Fortra*. [online] www.fortra.com.

Available from: https://www.fortra.com/resources/articles/snmp-basics-what-it-and-