Abstract

ABCD Co-operative Society Limited is a **business or organization owned by and operated for the benefit of its members**. Profits or earnings are distributed among its members. The co-op can be a for-profit business or a non-profit organization. The co-op runs similarly to a corporation, because members purchase shares and elect a board of directors and officers. For the purposes of this project, the upgrade ABCD Co-operative Society Limited Computer Network and improve the reliability of this network. Currently they have simple network. This network no has any security features or File sharing technologies. So ABCD Co-operative Society Limited has a lot of problem with their internal network and bank area network. ABCD Co-operative Society Limited employees need to communicate and sharing some kind of sensitive data between ABCD Co-operative Society Limited office and ABCD Co-operative Society Limited bank. Overall, the existing system not configure secure file sharing technology or Connection between office and bank area. In this project include how to improve new network for ABCD Co-operative Society Limited. What are the hardware requirement and software requirements for this project, the protocols and technologies used in this project, and how much it cost. these details included in this project.

Table of Contents

List of Figures

List of Tables

List of Acronyms

DHCP – dynamic host configuration protocols

HSRP – Host standby Router Protocols

NTP – network Time protocol

VPN – virtual private network

VLAN – virtual local area network

ACL – Control access list

PAT – port address translation

SNMP – simple network management protocol

DDNS – dynamic Domain name service

SSH – secure shell

RDP - Remote Desktop Protocols

MIB - management Information base

QoS - Quality of Service

Background

To convince the reader that any conclusions drawn, and recommendations made at the end of the final report are valid, you need to show that you have a good understanding of the area in which you are working and are fully aware of any other working that has been done in related fields. You do that by presenting a summary of that work in this section. You do not need to copy out great chunks of other's work or spend a long time in reviewing this. This is the section where references will be most plentifully employed, both to demonstrate the level of reading you have undertaken and to save space. Rather than setting out other's work in detail in this section, you can summarize it briefly, and include a reference to the original which the reader can look at if necessary.

Panel will look for:

• How efficiently you have presented the information, using references rather than writing out lots of text.

• Quality of background work presented

• Completeness of coverage

• Level of understanding displayed

• Level of consideration of any wider contextual issues

Chapter 1 - Introduction

Introduction

ABCD Co-operative Society Limited is a organization that requires a reliable and secure network to carry out their daily operations. In order to achieve this, a well-designed network architecture should be implemented.

The network architecture should have 3 layers of security to prevent unauthorized access and protect sensitive data. This can be achieved through the use of firewalls, intrusion detection systems, and access control mechanisms. The network should also be designed with redundancy in mind to ensure maximum uptime and availability. This can be accomplished through the use of redundant routers, switches, and internet connections. To ensure reliable and ABCD Co-operative Society Limited fast network performance, the network should be designed with appropriate bandwidth allocation, Quality of Service (QoS) settings, and load balancing mechanisms.

As a network administrator, the task is to build a secure network for a ABCD Co-operative Society Limited. that can protect sensitive data and prevent unauthorized access to the organizations network. Building a secure network involves a range of processes, from assessing the organization needs and risks to designing and implementing security solutions that meet those needs. Furthermore, it is important to consider the scalability of the network to accommodate future growth and expansion. This can be achieved through the use of modular hardware and scalable software solutions.

Overall, by implementing a well-designed and secure network architecture, ABCD Co-operative Society Limited can ensure reliable and efficient network operations, which will ultimately lead to increased productivity and business success.

Project Background

ABCD Cooperative Society is a non-profit organization that provides financial and social services to its members. The organization has been growing steadily over the years and has expanded its services to multiple branches across different locations. With the increasing reliance on technology,

Harispathuwa Cooperative Society realizes the need for a reliable and secure network to carry out its daily operations.

The current network infrastructure of Harispathuwa Cooperative Society is outdated, unreliable, and lacks the necessary security features to protect the organization's data and systems. The network has been causing frequent downtime, slow response times, and security breaches, which have negatively impacted the organization's productivity and reputation. In addition, the organization's employees are struggling to access critical resources and collaborate efficiently due to the network's limitations.

To solve these issues, Harispathuwa Cooperative Society has decided to undertake a project to build a new network infrastructure that is reliable, secure, and scalable. The new network will be designed to support the organization's current needs and future growth while providing maximum uptime, performance, and security.

a new network architecture will be designed and implemented, which will include security features, redundancy mechanisms, and load-balancing techniques. The new network will also provide high-speed connectivity, Quality of Service (QoS) settings, and centralized management for efficient monitoring and troubleshooting.

The ultimate goal of this project is to help the ABCD Co-operative Society Limited to achieve a robust and reliable security posture that can defend against both known and emerging threats, and provide stakeholders with confidence that their critical assets are protected from harm.

Problem statement

Harispathuwa Cooperative Society is facing significant challenges with its existing network infrastructure, which is outdated, insecure, and unreliable. The network has been causing everyday downtime, slow response times, and security breaches, which have negatively impacted the organization's productivity and reputation. And also, the organization's employees are struggling to access critical resources and collaborate efficiently due to the network's limitations.

The current network infrastructure of Harispathuwa Cooperative Society lacks the necessary security features to protect the organization's data and systems. This can be impact in several security breaches, which have compromised sensitive information and put the organization at risk. The network is also unable to support the organization's current needs and future growth, leading to performance issues and poor user experience.

The existing network infrastructure of Harispathuwa Cooperative Society is unable to meet the organization's requirements for reliability, scalability, and security. This has led to a decrease in productivity, operational efficiency, and customer satisfaction. To address these challenges, the organization needs to undertake a project to build a new network infrastructure that is reliable, secure, and scalable.

Aim and Objectives

Aim:

To design and implement a new network infrastructure for Harispathuwa Cooperative Society that is reliable, secure, and scalable, to improve productivity, operational efficiency, customer satisfaction, and ensures maximum uptime, performance, and security.

Objectives

- To increase network capacity
- To improve network security
- To improve network speed
- To improve network efficiency
- To manage users
- To provide secure VPN connection between ABCD co-operative society limited office and bank
- To provide remote access service for network management. Administrator can access and configure network devices remotely
- To provide public WIFI network for users

- Conduct a comprehensive network analysis to identify the existing network's weaknesses and determine the requirements of the new network.

- To design a new network architecture that include the requirements of Harispathuwa Cooperative Society, including security features, redundancy mechanisms, load balancing techniques, high-speed connectivity, and centralized management.
- To ensure the new network infrastructure is reliable and provides maximum uptime, performance, and user experience, access control policies and mechanisms to protect sensitive information and prevent unauthorized access to the network and its resources.

Scope of the project

The scope of the project for Harispathuwa Cooperative Society is to design and implement a reliable secure and fast network infrastructure that can support the organization's day-to-day operations.

Chapter 2 - Literature review

Introduction paragraph

A literature review is a critical and thorough examination of the body of knowledge already published on a certain subject or issue. Finding, analyzing, and synthesizing published research studies, books, and other sources that are pertinent to the current research issue or topic are all part of this process.

A literature review often seeks to summarize the current body of knowledge on a given subject and to point out any gaps, discrepancies, or inconsistencies in the literature. Identifying major themes, concepts, theories, or approaches that have been applied in the literature and assessing their advantages and disadvantages may also be included.

CCNA Routing and Switching Complete study guide second edition

This book covers everything that I need to know to continue that project as well as how to configure that network using cisco Devices. that book provides how-to routers, switches, and other network devices configuration in practically [1].

VLAN and Network Management

The paper gives the details of VLAN technology and explains not only how it works, but also explains the different types of VLANs and where they should be in a network. Some real-world networks and some of the common problems associated with those traditional layouts are discussed. The author then integrates switches into those problem networks and examines the effect [2].

Windows Server Configuration

This book given us an introduction to the new operating system and overview of the new technology and capabilities.

01) Installing and managing windows server
02) Provide knowledge about configuration DNS, Active Directory, windows Deployment service and etc.

Networking with windows server provide VPN solution, Data Storage and users management services [3].

Firewall Technologies

Explores the firewall security and performance relationships for distributed systems. Experiments are conducted to set firewall security into seven different levels and to quantify their performance impacts. These firewall security levels are formulated, designed, implemented and tested, phase by phase, under an experimental environment in which all performed tests are evaluated and compared. Based on the test results, the impacts of the various firewall security levels on system performance with respect to transaction time and latency are measured and analyzed. It is interesting to note that the intuitive belief about security's relationship to performance, i.e. that more security would result in less performance, does not always hold in firewall testing. The results reveal that a significant impact of enhanced security on performance could only be observed under some particular scenarios, and thus their relationship is not necessarily inversely related. We also discuss the tradeoff between security and performance [4].

SolarWinds network Management Tools

SolarWinds network Monitoring tool is a one of fames network monitoring tool in world. This book tack about how to manage SolarWinds network management tool and what are the network management protocols such as TELENT, SSH, Syslog, RDP (Remote Desktop Protocols), MIB (management Information base) and etc [5].

Quality of service (QOS)

Software Defined Networking (SDN) promises to provide a powerful way to introduce Quality of Service (QoS) concepts in today’s communication networks. In SDN the behavior and the functionality of the network devices is programmatically modified using a single high-level program. Software Defined Networking (SDN) instantiation OpenFlow is designed according to these

properties. The realization of the Quality of Service (QoS) concepts becomes understandable with SDN in a convenient way. This paper focuses on the parameters of the existing architecture. Using QoS technology this network can prioritize deferent sections [6].

Hot Standby Protocol and configuration

The Hot Standby Router Protocol, HSRP, provides a mechanism that is designed to support non-disruptive failover of IP traffic in certain circumstances. In particular, the protocol protects against the failure of the first hop router when the source host cannot learn the IP address of the first hop router dynamically. The protocol is designed for use over multi-access, multicast, or broadcast capable LANs (e.g., Ethernet). HSRP is not intended as a replacement for existing dynamic router discovery mechanisms and those protocols should be used instead whenever possible. A large class of legacy host implementations that do not support dynamic discovery are capable of configuring a default router. HSRP provides failover services to those hosts. All of the routers participating in HSRP are assumed to be running appropriate IP routing protocols and have a consistent set of routes. The discussion of which protocols are appropriate and whether routing is consistent in any given situation is beyond the scope of this specification [7].

KIWI syslog server

Kiwi Syslog Server is a software application used for receiving, logging, and monitoring syslog messages from network devices, such as routers, switches, firewalls, and servers. It is developed by SolarWinds, a company that provides network management software. Kiwi Syslog Server can be installed on Windows operating systems and can receive syslog messages from devices that support the syslog protocol, which is a standard protocol used for sending system log messages. The software can also receive SNMP traps, Windows event log messages, and text log files [8] .

Truenas network storage

TrueNAS is a network-attached storage (NAS) operating system based on the open-source FreeNAS project. It is developed by iXsystems, a company that provides enterprise storage soluions.TrueNAS is designed to provide a high-performance and scalable storage solution for businesses and organizations. It supports various storage protocols, including NFS, SMB, iSCSI, and AFP, and can be configured as a file server, block storage, or object storage. The operating system also includes features such as data deduplication, compression, replication, and snapshots [9].

Pfsense firewall

It is inevitable that people will use Internet networks in their daily lives. Network access is governed by firewall access rules, which are intended to protect vital networks from outside threats. The firewall system is crucial in providing security to all internet users by guarding against malicious attacks and rule analysts. By regulating the links that may be made between two or more networks, the firewall system, which is situated between the private network and the public web, enforces the security access regulation. Every network should have a firewall, which only enables appropriate traffic flows. This firewall system's primary objective is to control network access to or from a secured network. There are certain issues with the firewall system procedure [10].

Tacacs radius and AAA

The network authentication, authorization, and accounting protocols TACACS (Terminal Access Controller Access-Control System) and RADIUS (Remote Authentication Dial-In User Service) are both utilized. (AAA).

TACACS and RADIUS servers give network equipment including routers, switches, and firewalls a centralized approach to managing user authentication and access control. In order to manage which users can access which network devices and which commands they are permitted to execute, they enable administrators to build up policies for user access to network resources [11].

Captive portal

The network authentication, authorization, and accounting protocols TACACS (Terminal Access Controller Access-Control System) and RADIUS (Remote Authentication Dial-In User Service) are both utilized. (AAA).

TACACS and RADIUS servers give network equipment including routers, switches, and firewalls a centralized approach to manage user authentication and access control. In order to manage which users can access which network devices and which commands they are permitted to execute, they enable administrators to build up policies for user access to network resources.

Any Hyper Text Transfer Protocol (HTTP) browser's access to the internet is controlled by a web page known as the captive portal. When attempting to access the internet over the wireless network, a user would be forwarded to a web page either only for authentication or for both authentication and payment. The Ethernet card's MAC address is used to identify authenticated users. An authentication

and authorization service for networks and network infrastructures is called Radius. This paper aims to show how to manage user authentication on a wireless network at the University of Mines and Technology (UMaT) using an open-source firewall called pfSense running the FreeBSD operating system with Captive Portal and Active Directory-AD [12].

Ntopng Network Traffic Monitoring Tools

Open-source network traffic monitoring software called ntopng offers real-time network analysis and visualization. It was created by ntop, a provider of network monitoring software.

The network stack's several layers, such as the application layer, transport layer, and network layer, can all be captured and analyzed by ntopng. It supports a large number of protocols, including VoIP, TCP, UDP, HTTP, and DNS. Various sorts of communication, including file transfers, audio, and video, can all be recognized by the software.

A web-based interface for real-time network traffic visualization is offered by ntopng. There are several views available on the interface, including a dashboard, traffic matrix, flow analysis, and geolocation. Additional capabilities of the software include network alarms and notifications, packet capture and replay, and connectivity with third-party technologies like Elasticsearch and Kafka.

The goal of ntopng is to offer both small and large networks a complete and simple solution for network traffic analysis. Network administrators and security specialists favor it because of its open-source nature, which enables customization and integration with other network tools [13].

Python for automation

This article is to provide the information about the python that who it is going to be used in Advanced system and making day by day new machines. As python was just a programing language in first and used to short the android and other languages and later on now its taking control all over the world by hand shaking with other elements like Machine Learning(ML) Systems and Artificial Intelligent(AI) systems, with the help of many Algorithms and tools technology they are overcoming to every phase of life but the strange part is that now the simple data is going to the changed in knowledge by using this python. As It is well known that history is well predictor of future and by taking data from past we are predicting future using this Advanced language in the mention below section have some knowledge about this technique [14].

Network Automation with python

A trend that has been influenced and improved by software defined networking Networks are built on standard programming languages and scripting techniques for managing and controlling network components. In order to speed up equipment configuration and make maintenance simpler, this paper presents some novel techniques for automating the configuration of network devices. By identifying and addressing security flaws, it also strengthens network stability and enhances network security. These approaches, which enable the unitary control of an expanding number of devices, are what networks will look like in the future [15].

Network Automation using python

The goal of this dissertation, which was completed as a requirement for the MSc in Cybersecurity program at the International Hellenic University, is to investigate the core network automation technologies and combine them in a python-based software application. The software's Graphical User Interface (GUI) allows users to perform both basic network automation tasks, such as backing up and restoring configuration files on multiple devices at once, and more complex operations, such as configuring security and configuration settings.The numerous options that the user has to connect to and configure network devices using Python and its libraries are displayed and discussed in the application's code as well as in the paper [16].

Zabbix network monitoring tool

An open-source network monitoring program called Zabbix offers real-time network utilization, availability, and security monitoring. It was created by Zabbix SIA, a provider of commercial monitoring solutions.

Servers, routers, switches, and apps are just a few of the network components and services that Zabbix can keep an eye on. It supports a number of protocols, including ICMP, TCP, UDP, SNMP, and others. Additionally, performance indicators like CPU consumption, memory usage, and network traffic can be tracked by the software.

The monitoring system can be configured and managed using the web-based interface provided by Zabbix. The interface has a number of capabilities, including dashboards, maps, and reports, which let network managers see how the network is doing and spot potential problems.

The scalability and flexibility of Zabbix are two of its main benefits. Both small and big networks can use the program, which can also be tailored to fit certain monitoring needs. Distributed monitoring is also supported by Zabbix, allowing numerous instances to be set up as a single monitoring system.

Zabbix is an all-around trustworthy and thorough network monitoring tool that can be used for a variety of applications, from small businesses to major corporations. Network administrators and IT specialists favor it because of its open-source status and adaptability [17].

Network topology architecture

The access layer, the distribution layer, and the core layer are the three layers that often make up tier-organized network topology architectures.

The layer nearest to end-user gadgets like computers, printers, and phones is called the access layer. Access layer tasks include connecting end-user devices, enforcing security rules, and carrying out fundamental traffic management duties. Switches and wireless access points are common components in the access layer.

Connectivity between switches at the access layer and the core layer is provided by the distribution layer. In addition to performing sophisticated traffic management and policy enforcement tasks, the distribution layer can offer services like access control and Quality of Service (QoS). Switches and routers on the layer 3 are devices that are frequently encountered in the distribution layer.

The core layer serves as the network's structural support and offers fast communication between distribution layer components. High-speed switches and routers often make up the core layer devices, which facilitate quick and dependable data transport between distribution layer devices [18].

- Vpn
- DHCP
- Spanning-tree
- Port security
- IoT devices
- Wireless configuration

Chapter 3 Analysis

Examining network traffic to identify patterns, solve issues, boost performance, and maintain security is known as network analysis. In order to understand how a network is functioning, how devices are connecting, and how data is moving through the network, traffic on the network has to be analyzed.

Analysis of the current system.

According to the current system the network architecture using start topology architecture in this architecture has many securities vulnerability and network failures. The current system has not firewall or any other security mechanism to secure harispathuwa cooperative internal network.

First, without a firewall, the network is exposed to a range of cyber risks, including malware infection, hacking attempts, and unauthorized access to confidential information. A firewall is a crucial security tool that can block unwanted access and manage network traffic coming into and going out of a network.

Second, poor network architecture could lead to network outages and poor network performance. In order to reduce the effects of hardware failures or network outages, redundancy and fault tolerance should be built into the network architecture.

Thirdly, the company is unable to manage the network infrastructure effectively in the absence of network monitoring tools and authentication systems. While authentication systems can aid in regulating access to network resources and preventing unwanted access, network monitoring technologies can assist in identifying possible network issues and helping to take proactive measures to address them.

Requirement

User/ Client requirement

- As a client an access control mechanism, firewall, and threat management applications are all components of a safe network structure that guards against online threats and illegal access to critical data.
- As a user provide reliable and effective network services, including email, file sharing, printing, and video conferencing, to help with the day-to-day operations of the company.

- As an administrator provide a user-friendly network management interface that makes it simple for administrators to continue to maintain tabs on and control the network infrastructure.
- offer a scalable and adaptable network architecture that is simple to grow with and adapt to changing business needs.
- the effective use of network resources, such bandwidth, to guarantee top performance and reduce downtime.

Functional Requirement

- Firewall: To protect the network from unauthorized access and online risks a firewall should be implemented.
- Network Monitoring Tools: To monitor network performance and detect any problems, network monitoring tools should be installed.
- Authentication system: Implementing an authentication system will help to guarantee that only authorized users may access the network.
- File sharing: To make it simple and secure for staff to share files, a secure file sharing system.
- wireless access points: wireless access points provide users to connect devices wirelessly.

Nonfunctional requirement

- Network Performance: The network must have sufficient bandwidth, latency, and dependability to support the organization's operations.
- Security: Access control, data protection, and threat management solutions that provide secure network for users
- Scalability: To support expansion and changing business requirements, the network infrastructure should be adaptable and scalable.
- Usability: The network infrastructure should be user-friendly and easy to manage, allowing administrators to easily monitor and manage the network.
- Availability: The network infrastructure should be highly available to minimize downtime and ensure optimal network performance.

Software specification

- Firewall software: A firewall software, such as pfsense
- Network Monitoring software: Zabbix, ntopng
- Authentication software: Active Directory, AAA, pfsense local database
- File sharing software: Truenass

Hardware specification

- Firewall: netgate firewall
- Switches: cisco switches
- Storage devices
- Servers
- Wireless access point
- Wireless Lan controller
- Wireless devices

Feasibility study

Time feasibility

The investigation of whether the planned project can be completed within the allotted time period is known as time feasibility.

It can be stated that the implementation of the new network infrastructure is viable in time. To ensure that the project is completed within the allotted time frame, the project team will create a comprehensive strategy and schedule, ensure resource availability, and have backup plans in place.

The ABCD cooperative network implementation is done withing the time line

2022	2023

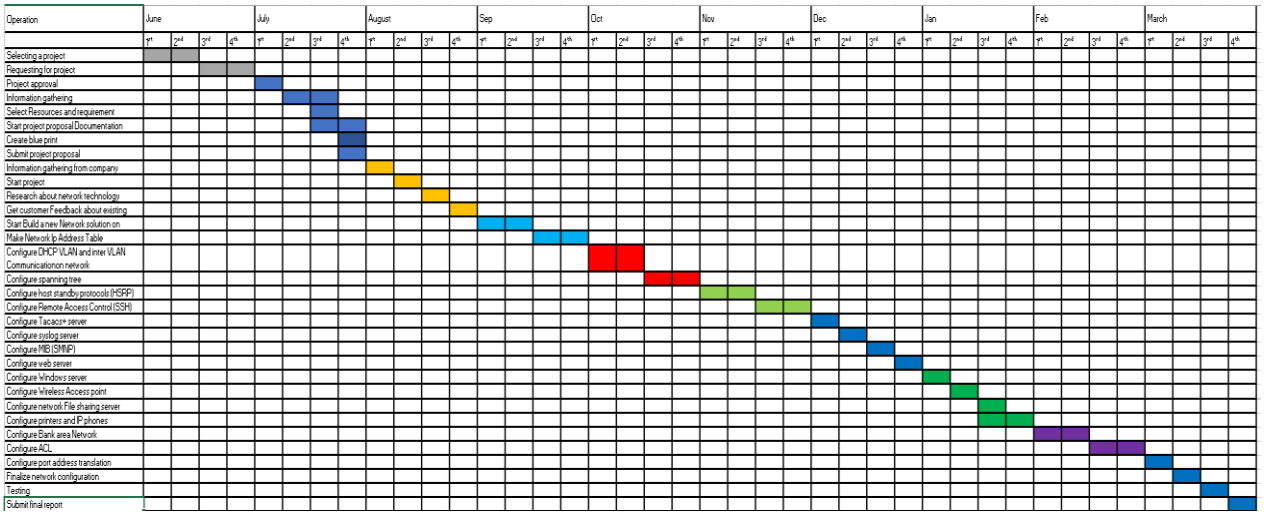


Figure 1:time plan

The available resources

Cost feasibility.

The investigation of whether the planned project can be completed with the money allocated is known as cost feasibility.

Table 1:budget and requirement

No:	Hardware Name	Per unit cost	Quantity	Total Cost
01	cisco catalyst 3650 24 poe+ 4x10g (layer 3 switch)	LKR 1,122,800	3	**LKR 3,368,400**
02	2960-24tt switch	LKR 332,500	3	**LKR 997,500**
03	Cables		500 m	**LKR 10000**
05	Wireless access point	LKR **145,250**	1	**LKR 145,250**
06	IP Phone (7960 series)	LKR 18,900	14	**LKR 264,600**
07	Printers	LKR 17500	4	**LKR 70,000**

08	Server and firewall hardware	200000		**LKR 200000**
No	Software Name	Per unit cost	Quantity	Total Cost
01	Windows servers 2022 Edition Stranded version	LKR 374,150	1	**LKR 374,150**
02	Zabbix	free	1	**Free**
04	KIWI syslog server	Free	1	**Free**
05	Pfsense	free	2	**free**
06	Truenass	Free	1	**Free**
No	Simulation software	Per unit cost	Quantity	Total Cost
01	Cisco packet tracer	Free	1	**Free**
02	GNS 3	Depend on a device image	1	**Depend on a device image**
03	Visio Drawing tool	free	1	**Free**
No	Other	Per unit cost	Quantity	Total cost
01	Training cost	LKR 70,000	2	LKR 140000
Sub Total				LKR 5,569,900

3.3.3. Scope feasibility

Scope Feasibility could be said that it is technically possible to build the new network infrastructure. The project team has the necessary skills and knowledge to complete the project within the specified

scope, and the project scope is clearly defined and achievable. In order to avoid scope variation, the project team will also work closely with the client to ensure that any changes to the scope are properly recorded, evaluated and approved.

Technical feasibility.

Technical feasibility is the assessment of whether the proposed project can be carried out with the technology and resources currently in use. The technical feasibility of the new network infrastructure for the ABCD Cooperative Society was examined and the following conclusions:

- The latest technology in the market can be used to implement the desired network infrastructure. Based on the client's needs and budget, the project team will research and choose the best technologies.
- The project team has the technical expertise to implement the suggested network infrastructure. The team can design, deploy and maintain the network infrastructure.
- It is possible to link the suggested network infrastructure with the customer's current IT systems, including servers, workstations and other hardware.

Economic feasibility

Methodology and planning artifact

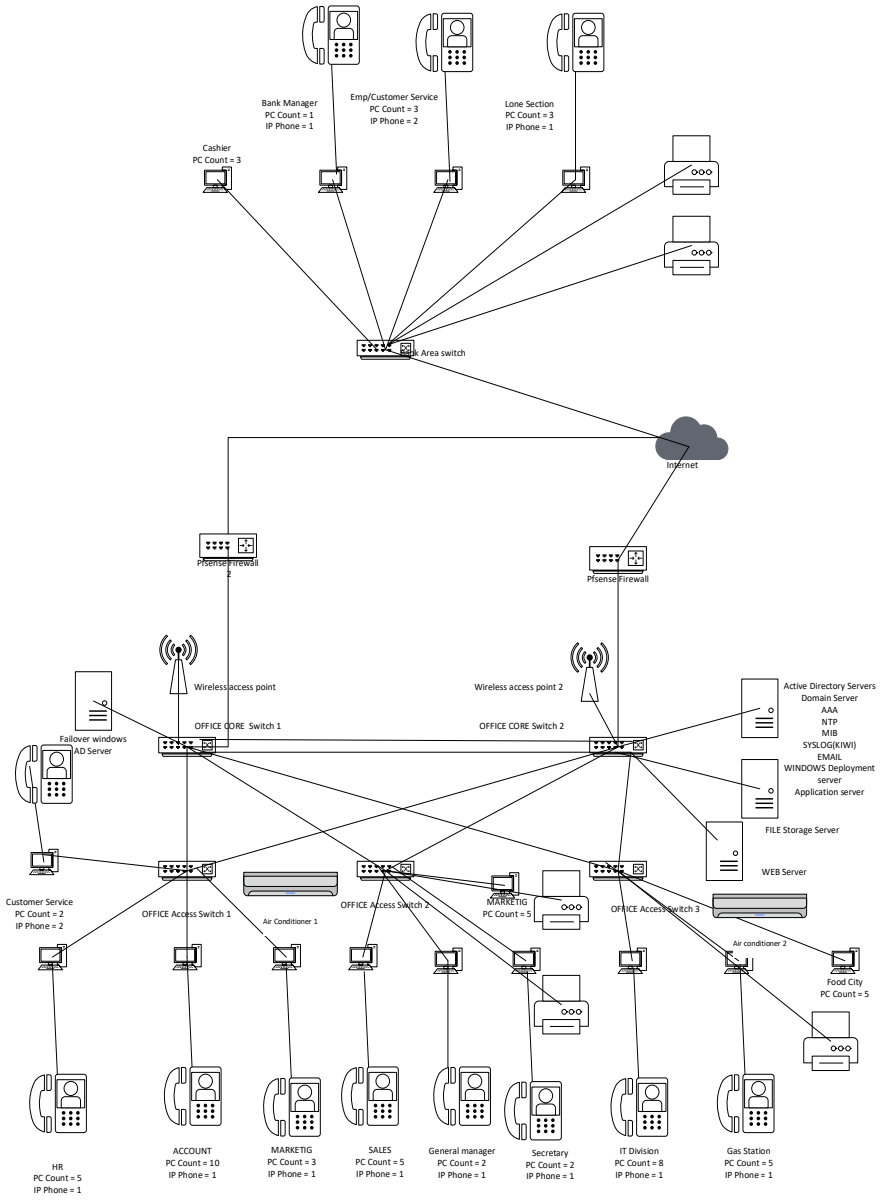
Methodology

The following phases make up the network lifecycle for the new network infrastructure project for ABCD Cooperative Society:

- Planning Phase: During this stage, the project team will collaborate with the client to gather requirements, specify project parameters, and create a project plan. Timelines, a budget and the distribution of resources are part of the project plan.
- Design Phase: During this stage, the project team will design the network infrastructure according to the client's needs and financial constraints. To meet the customer's needs, the team will choose the appropriate hardware, software and network protocols.
- The project team will install and configure the network infrastructure during the implementation phase. The group will test the network to make sure everything is working as it should.

- Operation phase: during this phase the network infrastructure will be put into operation. The project team will monitor the network, provide ongoing support and maintenance, and implement necessary improvements.
- Retirement phase: During this time, the network infrastructure will be replaced or retired if it is no longer suitable for customer demands or has outlived its usefulness.

Chapter 4 Design



Security and reliability are major parts when designing a network. So, in here use in very reliable architecture for developing this network and also use in lot of security technologies for protect that network.

This network architecture is called cisco two-layer architecture. this architecture has two deferent layers

01) Core layer
02) Access layer

core layer has a 2-cisco layer 3 switches and the Access layer has 3 cisco layer 2 switchers. When the core layer 1 switch will go down but the other core switch still works. so, this network hasn't any down time. to do this the administrator using Spanning tree protocols and standby protocols. And also, ABCD Co-operative Society Limited has a lot of deferent Department Using VLAN and VTP technologies I can divide into This Department in to Deferent VLAN And also ABCD Co-operative Society Limited need to sharing their Document withing the ABCD Co-operative Society Limited office and between ABCD Co-operative Society Limited bank and ABCD Co-operative Society Limited office in here I use Windows server and NAS (Network Attached Storage) for file sharing.

According to the diagram the administrator uses 2 pfsense firewall for implement this network. Therefor the administrator has failover firewall When the 1st firewall will go down but the other firewall still works. The administrator trying to increase network availability using failover switches firewall and servers.

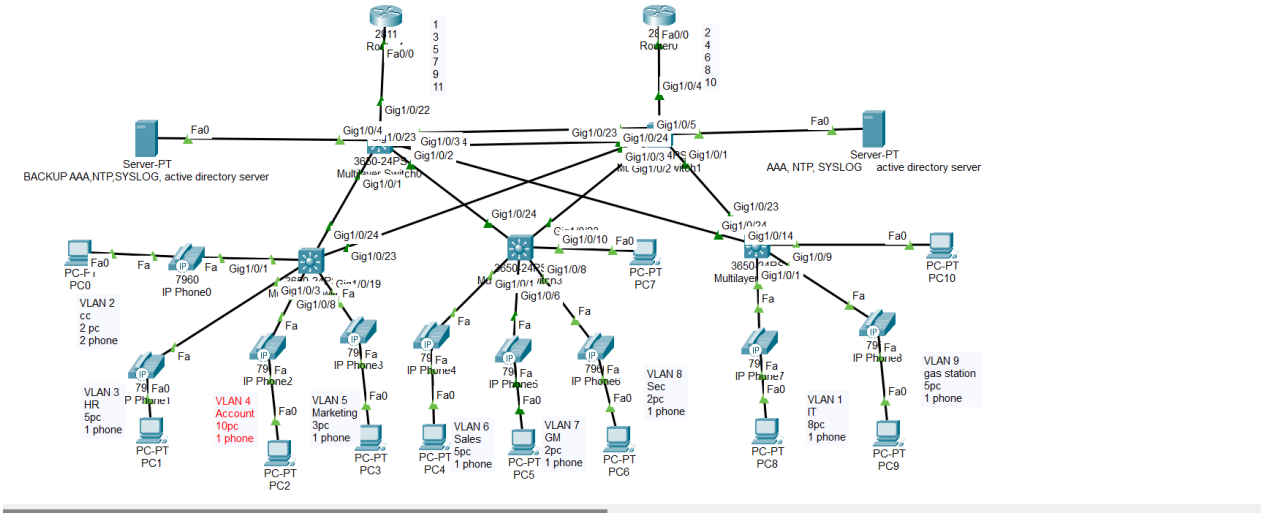


Figure 2:logical Diagram

In this section, the physical topology demonstrates the direction of the physical design implementation and illustrates the major points of the network upgrade, which includes the devices, locations, and cable installation.

In the main floor of the building, the main network and the two servers are in place. The core switches connect to the two servers. One server act like primary server and other server act like backup server.

The building is equipped with Category 5e cabling and wall plates in the offices

Within the building, managed switches are used. Managed switches give more control over LAN traffic and offer advanced features to control that traffic. It provides the ability to configure, manage, and monitor LAN and this gives greater control over how data travels over the network (spanning tree protocol) and who has access to it. In addition, managed switches use protocols such as the Simple Network Management Protocol, for monitoring the devices on the network. SNMP is a protocol that facilitates the exchange of management information between network devices. SNMP queries can determine the health of the network or the status of a particular device. By displaying this data in an easily understood format.

Department Name	Customer service	Human resource	Account	Marketing	sales	General manager	Secretary office	IT section	Gas station	Corp City	Voice
network	10.1.2.0	10.1.3.0	10.1.4.0	10.1.5.0	10.1.6.0	10.1.7.0	10.1.8.0	10.1.1.0	10.1.9.0	10.1.10.0	10.1.3.0
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255
VLAN ID	2	3	4	5	6	7	8	1	9	10	10
First usable ip address	10.1.2.1	10.1.3.1	10.1.4.1	10.1.5.1	10.1.6.1	10.1.7.1	10.1.8.1	10.1.1.1	10.1.9.1	10.1.10.1	10.1.3.1
Last usable ip address	10.1.2.254	10.1.3.254	10.1.4.254	10.1.5.254	10.1.6.254	10.1.7.254	10.1.8.254	10.1.1.254	10.1.9.254	10.1.10.254	10.1.3.254
Broadcast address	10.1.2.255	10.1.3.255	10.1.4.255	10.1.5.255	10.1.6.255	10.1.7.255	10.1.8.255	10.1.1.255	10.1.9.255	10.1.10.255	10.1.3.255
Default gateway	10.1.2.254	10.1.3.254	10.1.4.254	10.1.5.254	10.1.6.254	10.1.7.254	10.1.8.254	10.1.1.254	10.1.9.254	10.1.10.254	10.1.3.254

Figure 3:ip Allocation table

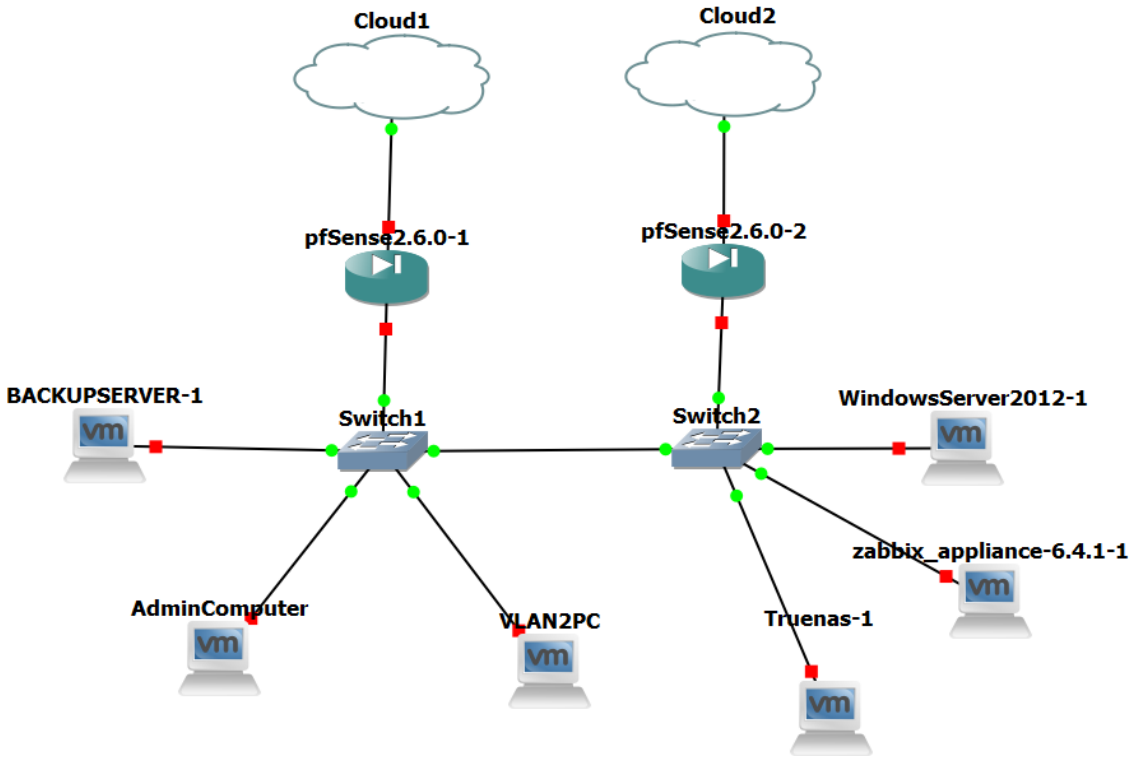


Figure 4:firewall and server Installation

This diagram demonstrate how servers and firewall are inter connect with each other according to diagram the topology has 2 pfsense firewall and 2 windows servers.

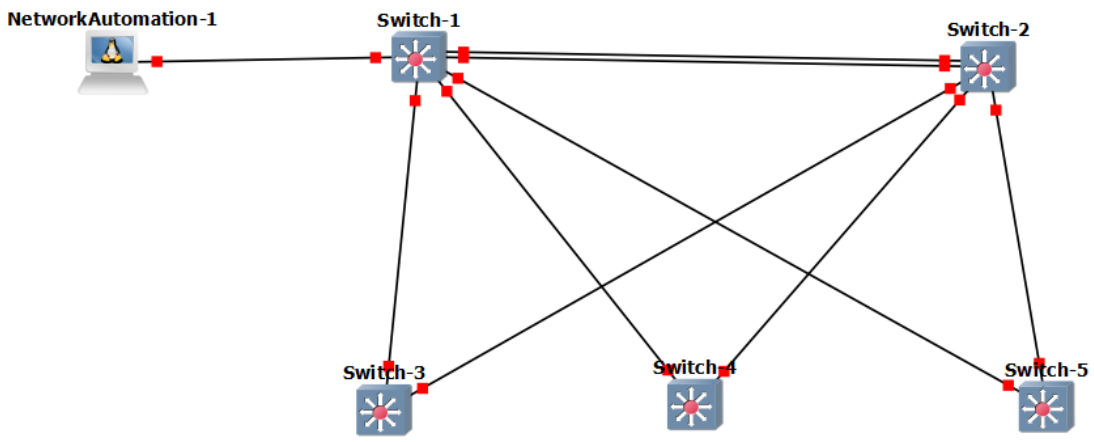


Figure 5:network Automation Diagram

This diagram is a text diagram used for network automation using python programming language

Chapter 5 Implementation

Implementation Environment

The physical environment in which the components will be installed, as well as the hardware and software components, will be included in the implementation environment of the new network infrastructure project for ABCD Cooperative Society.

Network equipment, including routers, switches, firewalls, and access points, as well as servers and storage devices, will be considered hardware components. These parts will be chosen and placed in the customer information center or other suitable locations according to the specifications acquired during the planning process.

Operating systems, network management software, security software, and other necessary programs shall be considered software components. To ensure that the network infrastructure works as it should, these components will be placed on the appropriate hardware devices.

Development Tools

Cisco packet tracer

Cisco Systems created a network simulation program called Cisco Packet Tracer (Packet Tracer) that allows users to replicate network configuration, design, and troubleshooting scenarios. It is frequently used by networking experts to test and verify network designs, as well as in educational settings for networking courses and training programs.

Users can drag and drop network devices, such as routers, switches, and computers, and connect them to mimic a network using Packet Tracer's graphical user interface (GUI). It also provides a command line interface (CLI) through which users can configure devices using Cisco IOS commands [19].

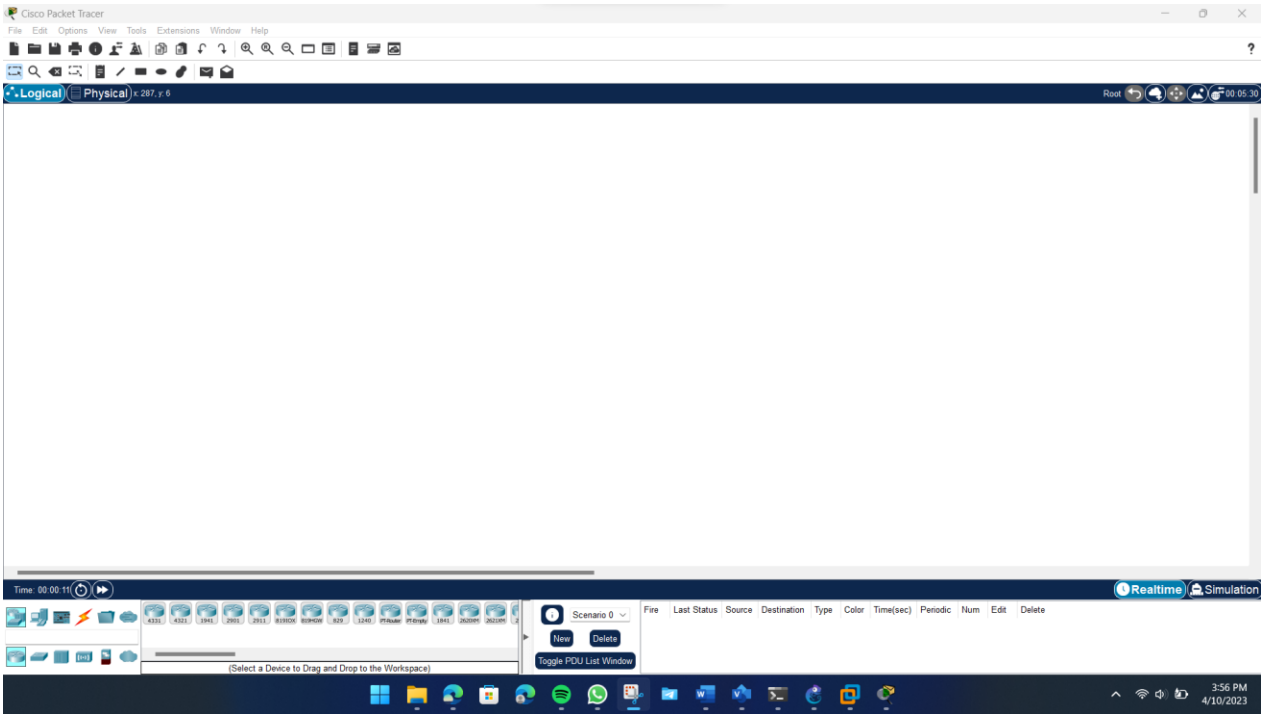


Figure 6:cisco packet tracer

GNS 3

The open-source network simulation and emulation tool GNS3 (Graphical Network Simulator 3) allows users to design complicated network topologies and test them in a virtual environment. Using it, users can build virtual networks that faithfully reproduce situations and configurations seen in the real world.

GNS3 provides a graphical user interface (GUI) that allows users to link together complex network topologies by dragging and dropping network components such as routers, switches, and firewalls. It also supports several different networks operating systems, including Juniper OS and Cisco IOS [20].

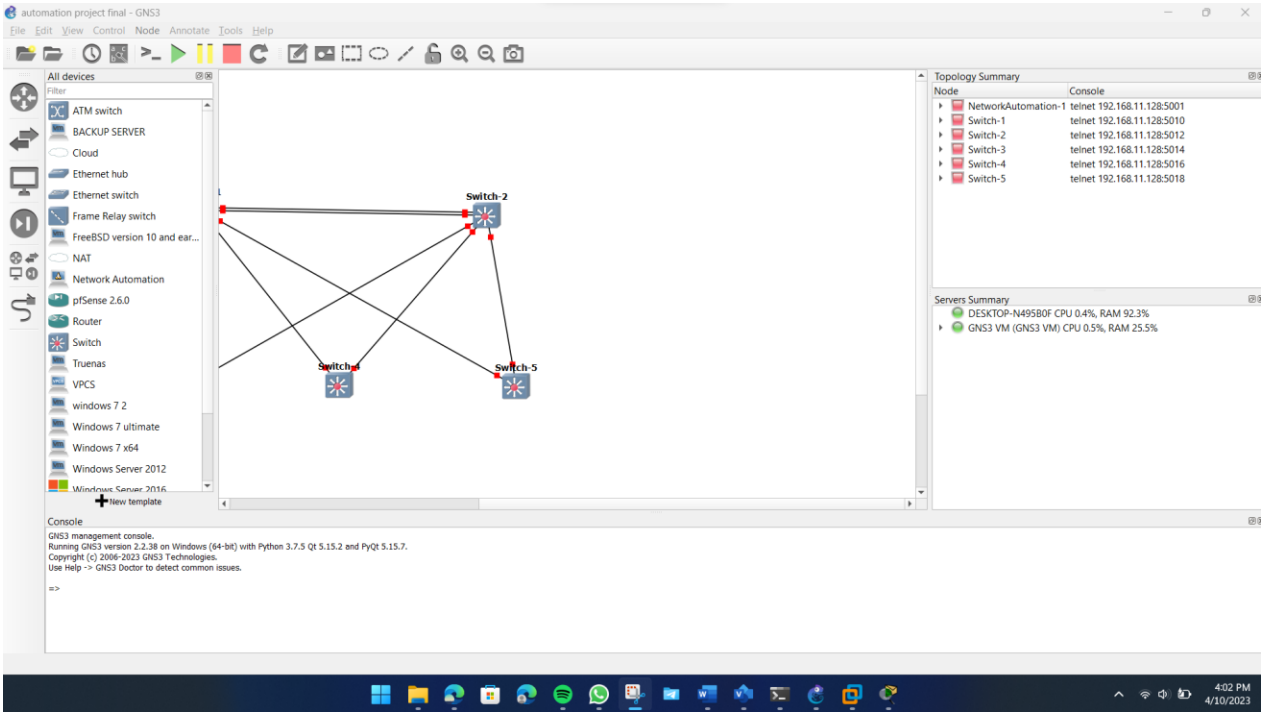


Figure 7:GNS 3

VMware workstation

With the support of the VMware Workstation virtualization program, users can run several different operating systems on a single physical machine. It allows users to create and control virtual machines (VMs) that can run multiple operating systems simultaneously, including Windows, Linux, and macOS.

VMware Workstation's easy-to-use interface allows users to create, customize, and manage virtual machines. It allows users to replicate multiple hardware configurations by supporting a wide variety of virtual hardware devices, including CPUs, RAM, hard drives, and network adapters.

In addition, VMware Workstation has capabilities such as snapshots that allow users to save the state of a virtual machine at a point in time and return to it later if needed [21].

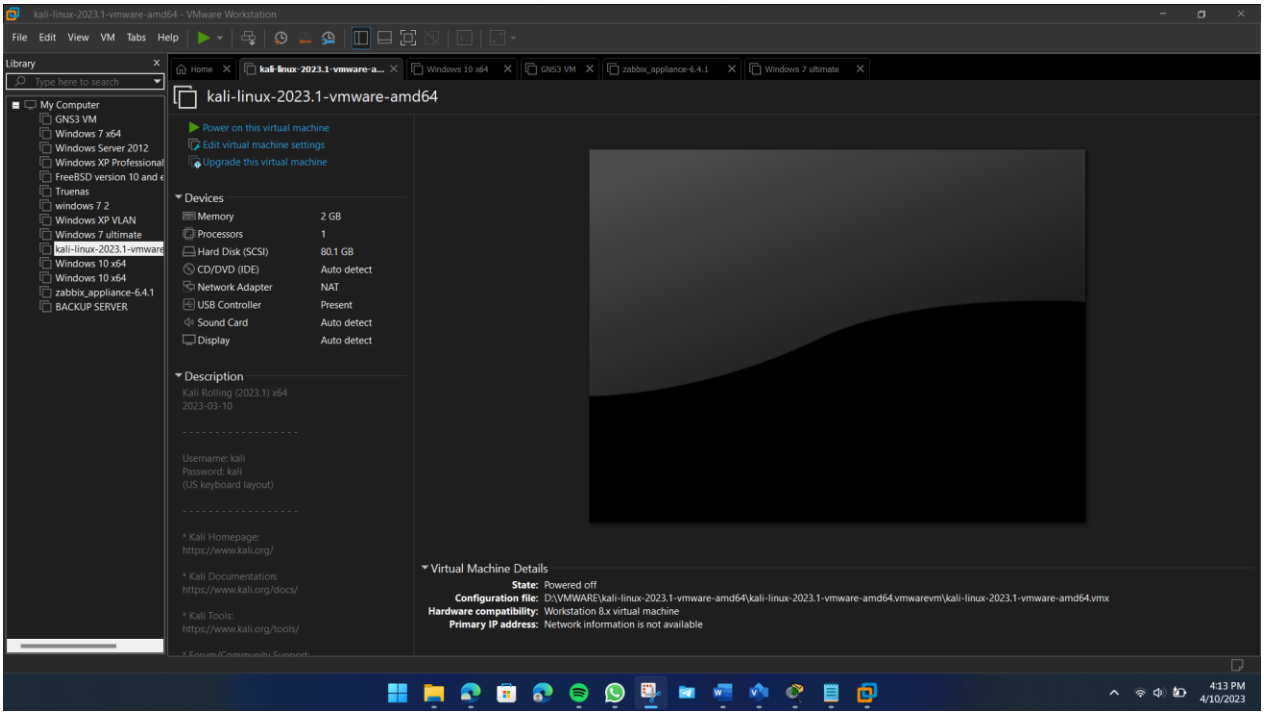


Figure 8:VMware Workstation pro

Major Configurations

Basic Configure in cisco network devices

Configuring cisco network devices has several steps to configure network devices but first the network administrator need connect to devices using a cable. And next the administrator need install terminal emulator for access cisco network device console. This console provides configuration command line to administrator then now administrator can configure cisco network Device such as Routers, switches

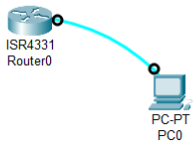


Figure 9:connect Network Devices though console cable

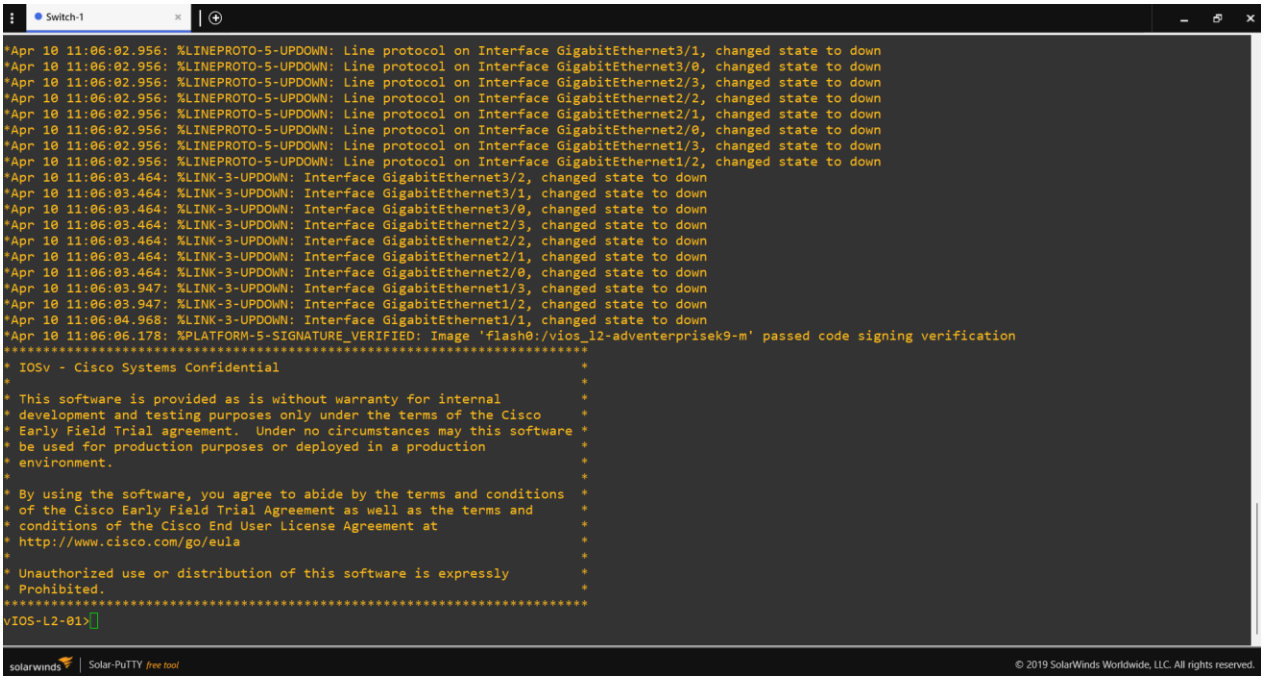


Figure 10:get access to device using terminal emulator (putty)

Configuration 2

Once connected, enter privileged EXEC mode by typing "enable"

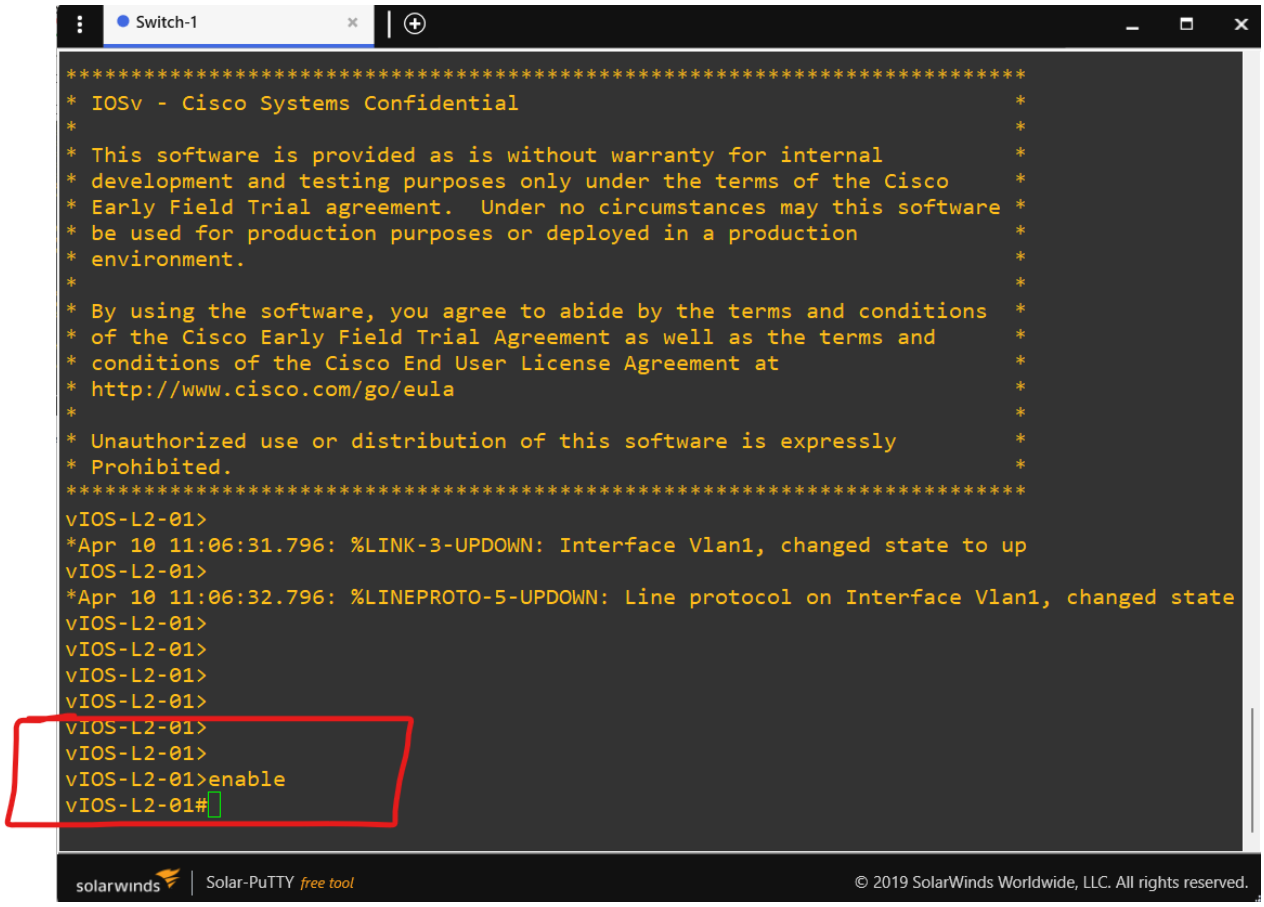


Figure 11:Enter enable Command to console

Configuration 3

After entering privilege mode user can't do configuration in privilege mode there for user need log in to global configuration mode using configure terminal command

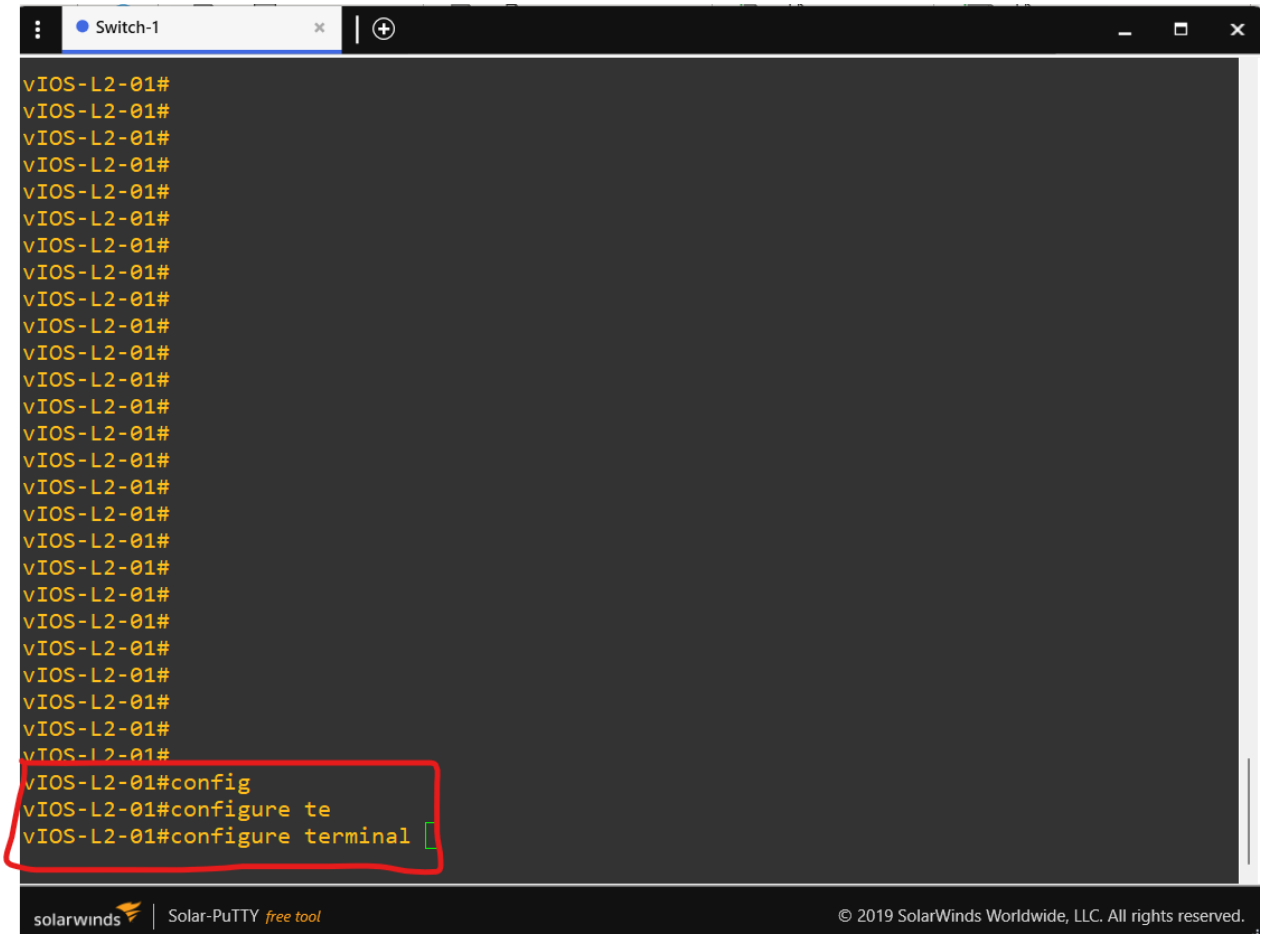


Figure 12:enter global configuration mode

After entering global configuration mode administrator can configure basic setting for devices such as hostname configuration and domain name configuration hostname used for identify the network devices in cooperation environment and also domain name used for an important configuration setting for Cisco routers that helps to ensure proper DNS configuration, device identification, name resolution, and security on the network.

Device Hostname configuration using **hostname** command

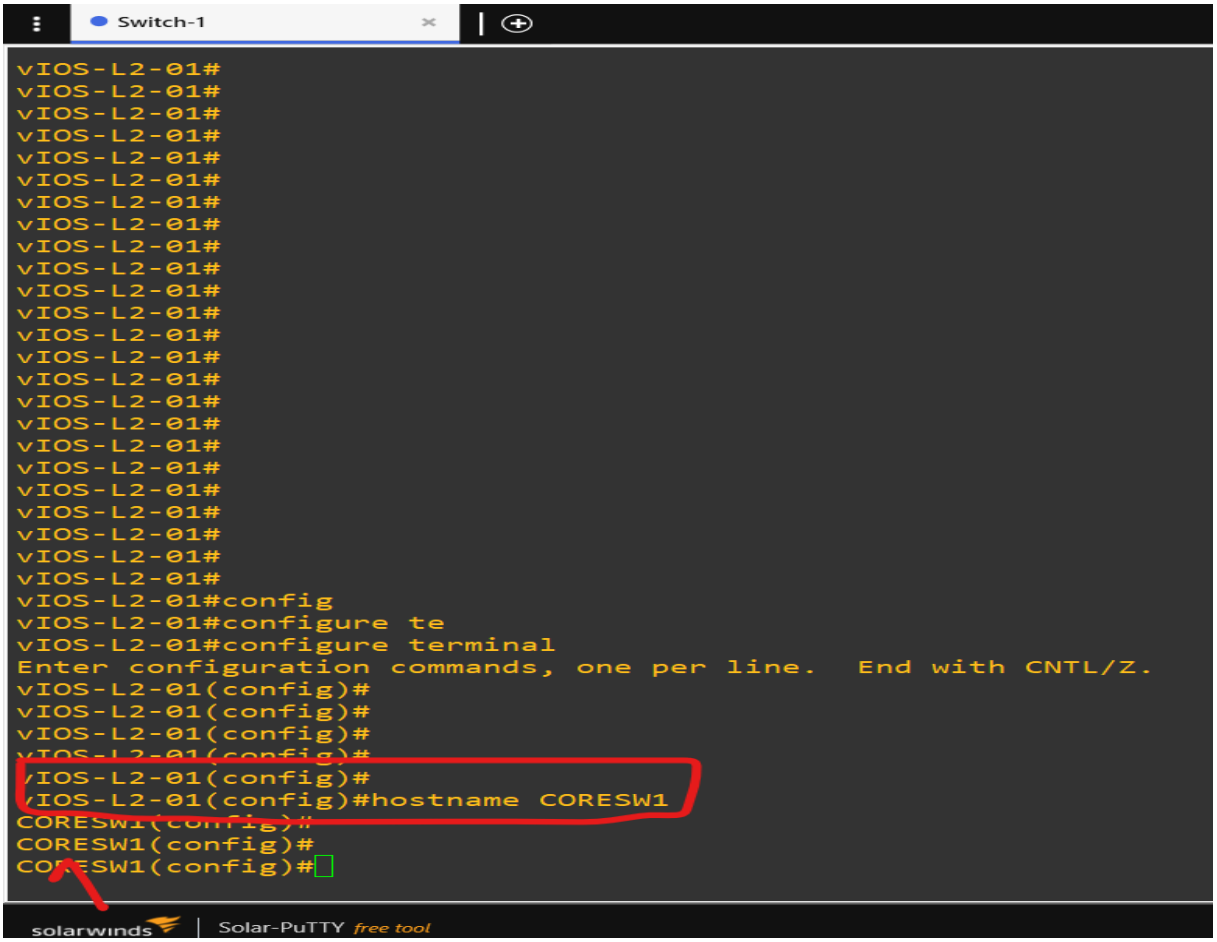


Figure 13:Device Hostname Configuration

According to the above picture the hostname {device name} command changes device hostname VIOS-L2-01 to CORESW1

Device domain name configuration using ip domain-name {device domain name} command

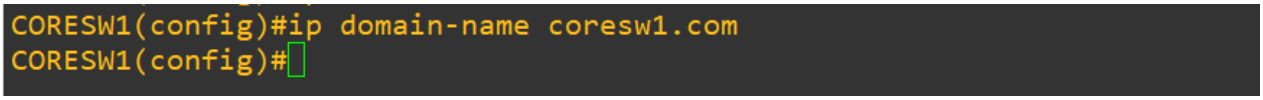


Figure 14:ip domain-name command

VLAN Configuration In cisco Devices

VLAN is Virtual Local Area Network that can connect multiple devices and machines in a single network, without having to place the devices in same geographical location.

According to ABCD corporation Network Diagram. The network administrator Decide divide this network into 11 VLANs. First VLAN Represent Default network and network administrators. The Second VLAN Describes customer service from now onwards third VLAN Used for Account, Fourth VLAN Used for Marketing.

VLAN 5= Sales

VLAN 6 = General manager

VLAN 7 = secretary office

VLAN 8 = IT section

VLAN 9 = GAZ station

VLAN 10 = corpcity

VLAN 11 = Voice

The administrator can configure VLAN using VLAN {vlan id} command and administrator can give name for VLAN using name {vlan name} command

Figure 15:VLAN command example

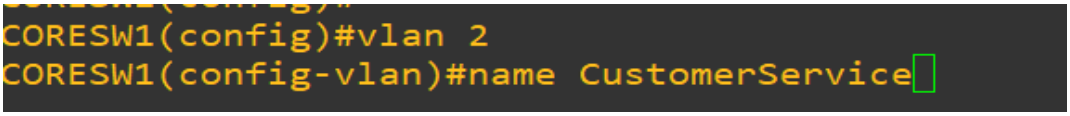


Figure 16:VLAN name configuration example

Final VLAN configuration in ABCD cooperative society CORESW1, CORESW2, ACCESS1, ACCESS2, ACCESS3 switches

```
CORE1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/4, Gig1/0/5, Gig1/0/6, Gig1/0/7
                                                Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/1/1
                                                Gig1/1/2, Gig1/1/3, Gig1/1/4
2    CustomerService                  active
3    HumanResource                    active
4    Account                          active
5    Marketing                        active
6    Sales                            active
7    GeneralManager                   active
8    SecretaryOffice                  active
9    GasStation                       active
10   CorpCity                         active
11   Voice                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 17:VLAN configuration

The Access layer switch ports are assigned into deferent Department Using Deferent VLAN ID

```
ACCESS1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/22, Gig1/1/1, Gig1/1/2, Gig1/1/3
                                                Gig1/1/4
2    CustomerService                  active    Gig1/0/1, Gig1/0/2
3    HumanResource                    active    Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/6
                                                Gig1/0/7
4    Account                          active    Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18
5    Marketing                        active    Gig1/0/19, Gig1/0/20, Gig1/0/21
6    Sales                            active
7    GeneralManager                   active
8    SecretaryOffice                  active
9    GasStation                       active
10   CorpCity                         active
11   Voice                            active    Gig1/0/1, Gig1/0/3, Gig1/0/8, Gig1/0/19
111  VLAN0111                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
```

```
ACCESS2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/1/1
                                                Gig1/1/2, Gig1/1/3, Gig1/1/4
2    CustomerService                  active
3    HumanResource                    active
4    Account                          active
5    Marketing                        active    Gig1/0/10, Gig1/0/11, Gig1/0/12, Gig1/0/13
                                                Gig1/0/14, Gig1/0/15
6    Sales                            active    Gig1/0/1, Gig1/0/2, Gig1/0/3, Gig1/0/4
                                                Gig1/0/5
7    GeneralManager                   active    Gig1/0/6, Gig1/0/7
8    SecretaryOffice                  active    Gig1/0/8, Gig1/0/9
9    GasStation                       active
10   CorpCity                         active
11   Voice                            active    Gig1/0/1, Gig1/0/6, Gig1/0/8
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
ACCESS3#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/1, Gig1/0/2, Gig1/0/3, Gig1/0/4
                                                Gig1/0/5, Gig1/0/6, Gig1/0/7, Gig1/0/8
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
2    CustomerService                  active
3    HumanResource                    active
4    Account                          active
5    Marketing                        active
6    Sales                            active
7    GeneralManager                   active
8    SecretaryOffice                  active
9    GasStation                       active    Gig1/0/9, Gig1/0/10, Gig1/0/11, Gig1/0/12
                                                Gig1/0/13
10   CorpCity                         active    Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
                                                Gig1/0/18
11   Voice                            active    Gig1/0/1, Gig1/0/9
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
 --More--
```

trunk port

In Cisco networks, trunk ports are used to carry traffic for many VLANs over a single physical link. When you need to transfer multiple VLANs between switches or on a router. According to network implementation the network administrator needs to configure trunks port between switches therefor the switches need to communicate with deferent VLANS. Configuration Example for Trunk port First administrator must need to select what are the connected links that is the administrator use int range command for select connected interfaces between switches. after selecting interfaces, the administrator need run switchport mode trunk command for trunk interfaces.

```
CORE1(config)#int range gi 1/0/1-4
CORE1(config-if-range)#
CORE1(config-if-range)#
CORE1(config-if-range)#
CORE1(config-if-range)#
CORE1(config-if-range)#sw
CORE1(config-if-range)#switchport mode trunk
```

Figure 18:example for configure trunk ports

After convert access port to trunk port the administrator can check what are the trunks ports in the switch using show interface trunk

```
CORE1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Gig1/0/1    on           802.1q         trunking      1
Gig1/0/2    on           802.1q         trunking      1
Gig1/0/3    on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-1005
Gig1/0/1    1-1005
Gig1/0/2    1-1005
Gig1/0/3    1-1005
```

Figure 19:core switch 1 trunk ports

```
CORE2#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Gig1/0/1    on           802.1q         trunking      1
Gig1/0/2    on           802.1q         trunking      1
Gig1/0/3    on           802.1q         trunking      1
Gig1/0/4    on           802.1q         trunking      1
```

Figure 21:core switch 2 trunk ports

```
ACCESS1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/23   on           802.1q         trunking      1
Gig1/0/24   on           802.1q         trunking      1
```

Figure 20:Access Switch 1 trunk port configuration

```
ACCESS2#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/23   on           802.1q         trunking      1
Gig1/0/24   on           802.1q         trunking      1
```

Figure22:Access Switch 2 trunk port configuration

```
ACCESS3#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/23   on           802.1q         trunking      1
Gig1/0/24   on           802.1q         trunking      1
```

Figure 23:Access Switch 3 trunk port configuration

VTP (VLAN TRUNKING PROTOCOL) modes

VTP stands for VLAN Trucking protocol this protocol is a cisco proprietary protocol used to distribute VLAN information across a network manly cisco has 3 main VTP modes in cisco networks.

01 server mode

02 client mode

03 transparent mode

According to the project the administrator decides used transparent mode for develop ABCD cooperative society network. The reason of selection Transparent VTP Transparent mode is considered the most secure VTP mode. This is because switches in Transparent mode do not participate in VTP updates and do not forward VTP updates to other switches

The switch configuration for VTP client and server modes must include the appropriate VTP domain name and password in order for it to participate in VTP updates. This indicates that an unauthorized switch could edit or delete VLANs and communicate this information to other switches in the VTP domain if added to the VTP domain and configured with the appropriate VTP domain name and password.

The administrator can stop any accidental or unauthorized modification to the VLAN configuration by configuring a switch to VTP Transparent mode. In this mode, the switch is guaranteed not to participate in VTP updates and will not broadcast VTP updates to other switches.

Which mean only change VLAN information in single switch and its not effected other switches therefor administrator need configure VLAN information in every switches manually

VTP mode and VTP domain Configuration example

First the administrator needs type vtp mode client command and next type vtp domain {domain name}

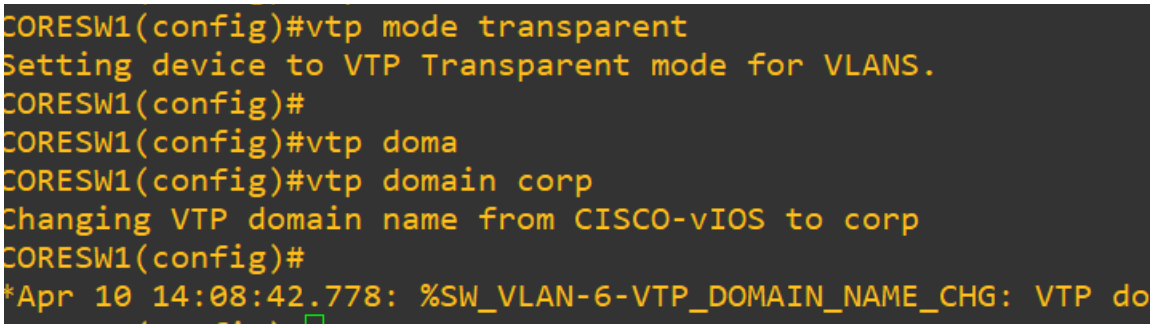


Figure 24:VTP configuration example

Once after all the configuration the administrator can check vtp status using **show vtp status** command

Example for show vtp status command

```
ACCESS1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : corp
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.C763.5800
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:20

Feature VLAN :
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 16
Configuration Revision            : 0
MD5 digest                        : 0x9D 0x6C 0xEC 0x32 0xC3 0x96 0x86 0x54
                                    0xE3 0x4F 0x9B 0xF9 0x9C 0xAF 0x90 0xEC
```

Figure 25:Example for show vtp status command

Spanning tree configuration

Spanning Tree Protocol (STP) is a protocol used in network bridging to prevent loops in a network topology. When a network topology has a loop, data can get stuck in an endless loop and network performance can degrade or even crash. STP works by creating a loop-free topology by blocking some of the network links to prevent loops.

According to the network topology in ABCD corporation internal network the ABCD cooperation has network loops in their internal network by blocking spanning tree protocol.

The Administrator can manage spanning tree loops in internal network when network administrator manage internal network loops the network can work effectively and efficiently also, the network administrator can use spanning tree for load balancing in internal network

The administrator can manage spanning tree using **spanning-tree vlan {vlan id} priority {value}** command.

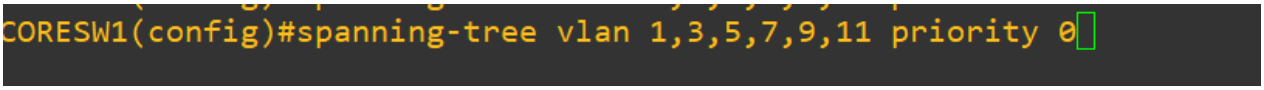


Figure 26:spanning Tree configuration example code

The spanning tree priory field determined which switch is root switch in the network topology. Each switch has a default priority value of 32768. Which switch has a lower priority value that device become a root switch or root bridge therefor the administrator can configure manually priority value and administrator can change what bridge is root bridge. The priority values must be increment in 4096 with valid ranging from 0 61440

The vlan id is of id of the which administrator want to configure the priority value

According to the above picture (figure 18) the administrator configure spanning tree for vlan 1,3,5,7,9,11 its priority value is 0 simply priority value 0 mean this bride is a root bridge for vlan 1,3,5,7,11

Example 2 for spanning tree

Figure 27:spanning tree configuration example code 2

According to the above picture vlan id 2,4,6,8,10 has priority 4096 that mean this bridge not root bridge for vlan 2,4,6,8,10,12

According to the ABCD internal network the network topology has two core switches. The network administrator need manage spanning tree in both core switches. The administrator decides manage spanning tree between core switches. Therefor core switch 1 contain VLAN 1,3,5,7,9,11 is a root VLANS and core switch 2 configure VLAN 2,4,6,8,10,12 are root VLAN for core switch 2

Configuration example for core switch 1

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 28:core switch 1 VLAN 1spanning tree configuration output

```
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    2
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    2  (priority 0 sys-id-ext 2)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 29:core switch 1 VLAN 2 spanning tree configuration output

```
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    3
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4099  (priority 4096 sys-id-ext 3)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 30:core switch 1 VLAN 3 spanning tree configuration output

```
VLAN0004
  Spanning tree enabled protocol ieee
  Root ID    Priority    4
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4  (priority 0 sys-id-ext 4)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 31:core switch 1 VLAN 4 spanning tree configuration output

```
VLAN0005
  Spanning tree enabled protocol ieee
  Root ID    Priority    5
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4101  (priority 4096 sys-id-ext 5)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

```
VLAN0008
  Spanning tree enabled protocol ieee
  Root ID    Priority    8
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8  (priority 0 sys-id-ext 8)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
```

Figure 33:core switch 1 VLAN 5 spanning tree configuration output

```
VLAN0007
  Spanning tree enabled protocol ieee
  Root ID    Priority    7
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4103  (priority 4096 sys-id-ext 7)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 35:core switch 1 VLAN 7 spanning tree configuration output

```
VLAN0009
  Spanning tree enabled protocol ieee
  Root ID    Priority    9
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4105  (priority 4096 sys-id-ext 9)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 37:core switch 1 VLAN 9 spanning tree configuration output

```
VLAN0011
  Spanning tree enabled protocol ieee
  Root ID    Priority    11
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4107  (priority 4096 sys-id-ext 11)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

```
VLAN0006
  Spanning tree enabled protocol ieee
  Root ID    Priority    6
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Br
```

Figure 32:core switch 1 VLAN 8 spanning tree configuration output

```
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 34core switch 1 VLAN 6 spanning tree configuration output

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     0007.ECAA.8EBA
             Cost        4
             Port        23(GigabitEthernet1/0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10  (priority 0 sys-id-ext 10)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/24         Altn BLK 4         128.24   P2p
Gi1/0/23         Root FWD 4         128.23   P2p
```

Figure 36:core switch 1 VLAN 10 spanning tree configuration output

```
VLAN0012
  Spanning tree enabled protocol ieee
  Root ID    Priority    12
             Address     000C.857C.220E
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32780  (priority 32768 sys-id-ext 12)
             Address     0002.17CC.3DED
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/6          Desg FWD 4         128.6    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/5          Desg FWD 4         128.5    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Po1              Root FWD 3         128.29   P2p
```

Example for Core switch 2 Spanning tree configuration

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     0002.17CC.3DED
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/5          Desg FWD 19        128.5    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Root FWD 3         128.29   P2p

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    2
             Address     000C.857C.220E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    2  (priority 0 sys-id-ext 2)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Desg FWD 3         128.29   P2p
```

Figure 40:spanning tree VLAN 1 and 2 output

```
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    3
             Address     0002.17CC.3DED
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4099  (priority 4096 sys-id-ext 3)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Root FWD 3         128.29   P2p

VLAN0004
  Spanning tree enabled protocol ieee
  Root ID    Priority    4
             Address     000C.857C.220E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4  (priority 0 sys-id-ext 4)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Desg FWD 3         128.29   P2p
```

Figure 41:spanning tree VLAN 3 and 4 output

```
VLAN0005
  Spanning tree enabled protocol ieee
  Root ID    Priority    5
             Address     0002.17CC.3DED
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4101  (priority 4096 sys-id-ext 5)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Root FWD 3         128.29   P2p

VLAN0006
  Spanning tree enabled protocol ieee
  Root ID    Priority    6
             Address     000C.857C.220E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    6  (priority 0 sys-id-ext 6)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Desg FWD 3         128.29   P2p
```

Figure 43:spanning tree VLAN 5 and 6 output

```
VLAN0007
  Spanning tree enabled protocol ieee
  Root ID    Priority    7
             Address     0002.17CC.3DED
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4103  (priority 4096 sys-id-ext 7)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Root FWD 3         128.29   P2p

VLAN0008
  Spanning tree enabled protocol ieee
  Root ID    Priority    8
             Address     000C.857C.220E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8  (priority 0 sys-id-ext 8)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Desg FWD 3         128.29   P2p
```

Figure 42:spanning tree VLAN 7 and 8 output

```
VLAN0009
  Spanning tree enabled protocol ieee
  Root ID    Priority    9
             Address     0002.17CC.3DED
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4105  (priority 4096 sys-id-ext 9)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Root FWD 3         128.29   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    10
             Address     000C.857C.220E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10  (priority 0 sys-id-ext 10)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Desg FWD 3         128.29   P2p
```

Figure 45:spanning tree VLAN 9 and 10 output

```
VLAN0011
  Spanning tree enabled protocol ieee
  Root ID    Priority    4107
             Address     0002.17CC.3DED
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4107  (priority 4096 sys-id-ext 11)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Po1              Root FWD 3         128.29   P2p

VLAN0012
  Spanning tree enabled protocol ieee
  Root ID    Priority    12
             Address     000C.857C.220E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    12  (priority 0 sys-id-ext 12)
             Address     000C.857C.220E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/6          Desg FWD 4         128.6    P2p
Po1              Desg FWD 3         128.29   P2p
```

Figure 44:spanning tree VLAN 11 and 12 output

Link Aggregation

Multiple physical connections between two devices can be aggregated into a single logical link using the link aggregation approach. This method is also known as Ethernet connection, port channeling and NIC teaming. Link aggregation provide Increased bandwidth, greater load balancing, and greater fault tolerance.

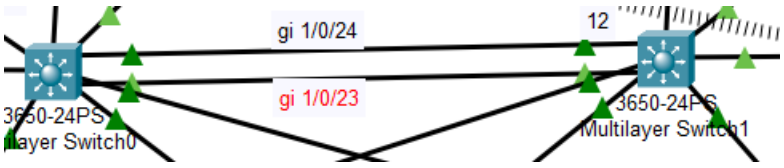


Figure 46:example for link aggregation

According to above image the administrator need configure link aggregation between switches (gi 1/0/23-24) link. Therefor administrator want to get console access for 1 switch first in bellow picture containing link aggregation configuration in switch one and two.

Before configure link aggregation the administrator must need select what links going to join

therefor administrator need run interface range gi 1/0/23-24 command.

```
CORE1(config)#interface range gigabitEthernet 1/0/23-24
CORE1(config-if-range)#
```

Figure 47:example for select interfaces

After entering interface configuration mode, the administrator needs to run channel-group {channel group id} active command for joining links.

```
CORE1(config-if-range)#channel-group 1 mode active
```

Figure 48:command for link aggregation

The "mode active" command tells the switch to actively initiate negotiations with the connected device to form a Link Aggregation group. In other words, the switch sends LACP (Link Aggregation Control Protocol) packets to the connected device to request the creation of the Link Aggregation group.

The group id 1 use for source-destination IP address load balancing and setting the interface to trunk mode

Once the Link Aggregation group has been created, you can configure additional options such switch port trunk and link types. These options can be configured using the "int port-channel {channel id}" command in global configuration mode. For example:

```
CORE1(config)#int port-channel 1
CORE1(config-if)#
CORE1(config-if)#
CORE1(config-if)#
CORE1(config-if)#sw
CORE1(config-if)#switchport mod
CORE1(config-if)#switchport mode tr
CORE1(config-if)#switchport mode trunk
```

Figure 49:example for int port-channel command

When all the Link Aggregation configuration done. but still has a one problem. That is a link type of the aggregation links. Most of the time this aggregation link has shr that mean this link support Harf

duplex. Therefor administrator need manually cover this shr link to point to point link for get full duplex.

Example for shr link type

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     0007.ECAA.8EBA
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Po1              Root FWD 3         128.29   Shr

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    2
             Address     0007.ECAA.8EBA
             Cost        3
             Port        29(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    2  (priority 0 sys-id-ext 2)
             Address     0009.7C75.711B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Po1              Root FWD 3         128.29   Shr
```

Figure 50:example for shr link type

Example Convert shr link to point to point link

First administrator needs to enter group channel with id next the administrator needs to type spanning-tree link type point-to-point

```
CORE1(config)#int port-channel 1
CORE1(config-if)#li
CORE1(config-if)#lin
CORE1(config-if)#spa
CORE1(config-if)#spanning-tree li
CORE1(config-if)#spanning-tree link-type po
CORE1(config-if)#spanning-tree link-type point-to-point
```

Figure 51:example for change link type shr to point to point

Assign ip address to VLAN interfaces

According to this project Assign an ip address to a VLAN interface for a few reasons one is the network administrator assigning and ip address to VLAN interface to enable remote management to switch using Telnet or SSH the administrator can connect to device using specific ip address and also VLAN interfaces are allows to network monitoring using SNMP protocols finally its also enables inter VLAN communication in layer 3 Switches

First of all, the administrator needs a specify what VLAN interface using interface vlan {vlan id} command

Next the administrator needs to specify ip address for VLAN interface using ip add {ip address} command

Finally, the administrator need turn on this interface using no shutdown command

Example for assign ip address to VLAN interface

```
vIOS-L2-01(config)#int vlan 1
vIOS-L2-01(config-if)#ip
*Apr 10 18:20:55.746: %LINK-3-UPDOWN: Interface Vlan1, changed stat
*Apr 10 18:20:56.746: %LINEPROTO-5-UPDOWN: Line protocol on Interfa
 to up
vIOS-L2-01(config-if)#ip add 10.1.1.1 255.255.255.0
vIOS-L2-01(config-if)#no shu
vIOS-L2-01(config-if)#no shutdown
vIOS-L2-01(config-if)#
```

Figure 52:Example for assign ip address to VLAN interface

Once assign ip address to VLAN interface the administrator can check these configurations are correctly configured using **show ip interface brief**

```
CORE1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  up                    up
GigabitEthernet1/0/23  unassigned      YES unset  up                    up
GigabitEthernet1/0/24  unassigned      YES unset  up                    up
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  10.1.1.252      YES manual up                    up
Vlan2                  10.1.2.252      YES manual up                    up
Vlan3                  10.1.3.252      YES manual up                    up
Vlan4                  10.1.4.252      YES manual up                    up
Vlan5                  10.1.5.252      YES manual up                    up
Vlan6                  10.1.6.252      YES manual up                    up
Vlan7                  10.1.7.252      YES manual up                    up
Vlan8                  10.1.8.252      YES manual up                    up
Vlan9                  10.1.9.252      YES manual up                    up
Vlan10                 10.1.10.252     YES manual up                    up
Vlan11                 10.1.11.252     YES manual up                    up
Vlan12                 10.1.12.252     YES manual up                    up
```

Figure 54:core switch 1 show ip int brief command example

```
CORE2#
CORE2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  up                    up
GigabitEthernet1/0/24  unassigned      YES unset  up                    up
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  10.1.1.251      YES manual up                    up
Vlan2                  10.1.2.251      YES manual up                    up
Vlan3                  10.1.3.251      YES manual up                    up
Vlan4                  10.1.4.251      YES manual up                    up
Vlan5                  10.1.5.251      YES manual up                    up
Vlan6                  10.1.6.251      YES manual up                    up
Vlan7                  10.1.7.251      YES manual up                    up
Vlan8                  10.1.8.251      YES manual up                    up
Vlan9                  10.1.9.251      YES manual up                    up
Vlan10                 10.1.10.251     YES manual up                    up
Vlan11                 10.1.11.251     YES manual up                    up
Vlan12                 10.1.12.251     YES manual up                    up
```

Figure 53:core switch 2 show ip int brief command example

```
--------
ACCESS1#show ip int bri
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  up                    up
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  up                    up
GigabitEthernet1/0/24  unassigned      YES unset  up                    up
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  10.1.1.240      YES manual up                    up
```

Figure 56:Access switch 1 show ip int brief command example

```
ACCESS2#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  up                    up
GigabitEthernet1/0/24  unassigned      YES unset  up                    up
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  10.1.1.241      YES manual up                    up
```

```
ACCESS3#show ip int bri
Interface              IP-Address      OK? Method Status                Protoc
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  up                    up
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  up                    up
GigabitEthernet1/0/24  unassigned      YES unset  up                    up
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  10.1.1.242      YES manual up                    up
```

Figure 57:Access switch 3 show ip int brief command example

HSRP (hot standby router protocol)

Redundancy for IP networks is provided by Cisco's proprietary protocol known as HSRP (Hot Standby Router Protocol). Intended to serve as a single virtual router and act as the default gateway for hosts on a LAN, HSRP allows multiple routers to share a virtual IP address.

According to the ABCD cooperation network need redundancy for their internal network therefor the administrator decides configure HSRP in core layer switches.

When configuring HSRP the administrator must need enter VLAN interface or interface id and administrator need to validate this interface active or standby manually

The host standby router protocol has virtual ip address this allows to multiple routers or switches to act like single virtual router on a LAN. This virtual ip also use as their default gateway.

HSRP Has two deferent routers one is Active Router and other one is standby router a situation where one router is assigned as an active router and another as a standby router. The standby router monitors the active router and takes over if the active router fails. The active router is responsible for forwarding packets delivered to the virtual IP address.

Each router participating in HSRP is assigned a priority value, with the router with the highest priority becoming the active router. This can be configured manually or dynamically using the router's IP addresses and interfaces.

Configuration Steps in HSRP

Configure HSRP in CoreSW1 interface VLAN 1

Select interface and Virtual ip address configuration in HSRP

```
core1(config)#int vlan 1
core1(config-if)#
core1(config-if)#stand
core1(config-if)#standby 1 ip 10.1.1.254
core1(config-if)#
```

Figure 58:core switch 1 Virtual ip address configuration in HSRP

Configure higher 200 priority value us **standby 1 priority 200** command

The priority 200 command decide this switch is VLAN 1 active switch because priority 200 is higher priority value

```
core1(config-if)#standby 1 priority 200
core1(config-if)#
core1(config-if)#
core1(config-if)#
```

Figure 59:set priority value to 200

Set preempt value using **standby 1 preempt** command

```
core1(config-if)#standby 1 preempt
core1(config-if)#
```

Figure 60:Set preempt value using standby 1 preempt command

Configure HSRP in CoreSW1 interface VLAN 1

Set virtual ip address for core switch 2 int VLAN 1

```
core2(config)#int vlan 1
core2(config-if)#
core2(config-if)#standby 1 ip 10.1.1.254
core2(config-if)#
```

Figure 61:Set virtual ip address for core switch 2 int VLAN 1

Set priority value to 100

```
core2(config-if)#standby 1 priority 100
```

Figure 62:Set priority value to 100

The priority value 100 is a default priority value of HSPRP this value is low value mare than 200 because this switch designated VLAN 1 standby switch/router

Finally, the administrator can check configuration using **show standby brief** command

```
CORE1(config-if)#do show standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl1         1    200 P Active   local           10.1.1.251      10.1.1.254
Vl2         1    100   Standby  10.1.2.251      local           10.1.2.254
Vl3         1    200 P Active   local           10.1.3.251      10.1.3.254
Vl4         1    100   Standby  10.1.4.251      local           10.1.4.254
Vl5         1    200 P Active   local           10.1.5.251      10.1.5.254
Vl6         1    100   Standby  10.1.6.251      local           10.1.6.254
Vl7         1    200 P Active   local           10.1.7.251      10.1.7.254
Vl8         1    100   Standby  10.1.8.251      local           10.1.8.254
Vl9         1    200 P Active   local           10.1.9.251      10.1.9.254
Vl10        1    100   Standby  10.1.10.251     local           10.1.10.254
Vl11        1    200 P Active   local           10.1.11.251     10.1.11.254
Vl12        1    100   Listen   10.1.12.251     10.1.12.251     10.1.12.254
```

Figure 64:core switch 1 standby brief command output

```
CORE2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl1         1    100   Standby  10.1.1.252      local           10.1.1.254
Vl2         1    200 P Active   local           10.1.2.252      10.1.2.254
Vl3         1    100   Standby  10.1.3.252      local           10.1.3.254
Vl4         1    200 P Active   local           10.1.4.252      10.1.4.254
Vl5         1    100   Standby  10.1.5.252      local           10.1.5.254
Vl6         1    200 P Active   local           10.1.6.252      10.1.6.254
Vl7         1    100   Standby  10.1.7.252      local           10.1.7.254
Vl8         1    200 P Active   local           10.1.8.252      10.1.8.254
Vl9         1    100   Standby  10.1.9.252      local           10.1.9.254
Vl10        1    200 P Active   local           10.1.10.252     10.1.10.254
Vl11        1    100   Standby  10.1.11.252     local           10.1.11.254
Vl12        1    200 P Active   local           10.1.12.252     10.1.12.254
```

Figure 63:core switch 2 standby brief command output

Port security

Port security is a security feature that can used for secure a computer network ports from unauthorized access and limiting number of devices that can connect to a specific port on a switch Port security mainly configure on network switches. Switches has a number of ports, and port security allows network administrators to control which devices are allowed connect to specific ports on the switch.

Enabling port security there are several methods used for port security

01) Mac address filtering
02) 802.1x authentication
03) VLAN assignment

Mac address filleting is a most commonly used technique that allows administrator to specify list of mac-address that allows to connect specific port.

According to the ABCD cooperative society network the administrator select mac address filleting method for enable network port security.

Port security configuration

First administrator need select specific **interface type int {int id}** command

```
ACCESS1(config)#int gi 1/0/1
```

Figure 65:select interface

Then administrator need enable port security using **switchport port security command**

```
ACCESS1(config-if)#switchport port-security
```

Figure 66:enable port security for switchport

Administrator can Specify the maximum number of allowed MAC addresses using bellow command.

switchport port-security maximum {value}

This command sets the maximum number of MAC addresses that can be learned on the port.

```
ACCESS1(config-if)#switchport port-security maximum 1
```

Figure 67:maximum mac address count

```
ACCESS1(config-if)#switchport port-security maximum 3
```

Figure 68:maximum mac address count

In above image the maximum number of mac address value is set to 3. This because According to the network diagram some switch ports connect with ip phone and computer. But the ip phone typically has two MAC addresses: one for the phone itself and one for the attached computer. The

third MAC address is reserved for the Voice VLAN. Therefore, the administrator needs to use 3 maximum number of mac address.

Finally, the administrator configures what are the allowed mac address using switchport **port-security mac-address sticky**

```
ACCESS1(config-if)#switchport port-security mac-address sticky
```

Figure 69:add mac address to switchport

The administrator can see which computers can access these ports using show port-security

```
ACCESS1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
     Gig1/0/1        3          1                0         Shutdown
---------------------------------------------------------------------
```

Figure 70:show port security command

Enable Ip routing

Based on their destination IP address, data packets are forwarded from one network to another using IP routing. Routers in a computer network are responsible for forwarding packets between various networks.

According to the network topology the administrator enables ip routing using **ip routing** command in core switches. These core switches are layer 3 swathes therefore this switch can communicate between deferent LAN like Router.

Ip Routing command example and text results

```
CORE1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 12 subnets
C       10.1.1.0 is directly connected, Vlan1
C       10.1.2.0 is directly connected, Vlan2
C       10.1.3.0 is directly connected, Vlan3
C       10.1.4.0 is directly connected, Vlan4
C       10.1.5.0 is directly connected, Vlan5
C       10.1.6.0 is directly connected, Vlan6
C       10.1.7.0 is directly connected, Vlan7
C       10.1.8.0 is directly connected, Vlan8
C       10.1.9.0 is directly connected, Vlan9
C       10.1.10.0 is directly connected, Vlan10
C       10.1.11.0 is directly connected, Vlan11
C       10.1.12.0 is directly connected, Vlan12
```

Figure 72: ip routing command result in core switch 1

```
CORE2#show ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 12 subnets
C       10.1.1.0 is directly connected, Vlan1
C       10.1.2.0 is directly connected, Vlan2
C       10.1.3.0 is directly connected, Vlan3
C       10.1.4.0 is directly connected, Vlan4
C       10.1.5.0 is directly connected, Vlan5
C       10.1.6.0 is directly connected, Vlan6
C       10.1.7.0 is directly connected, Vlan7
C       10.1.8.0 is directly connected, Vlan8
C       10.1.9.0 is directly connected, Vlan9
C       10.1.10.0 is directly connected, Vlan10
C       10.1.11.0 is directly connected, Vlan11
C       10.1.12.0 is directly connected, Vlan12
```

Figure 71:ip routing command result in core switch 2

AAA configuration

The security structure known as AAA, which stands for authentication, authorization, and accounting, is used in computer networks. The AAA framework is used to manage access to network resources securely and to monitor user activity when accessing those resources.

The administrator uses this technology in ABCD cooperative society network for monitor and manage networks.

First Administrator need enable AAA using **aaa new-model command**

```
vIOS-L2-01(config)#aaa new-model
```

Figure 73:Enable AAA

The administrator chooses TACACS+ server for authentication. This is a cisco propriety server and this server provide encryption method for secure user information.

The Administrator use TACACS+ for authentication and the local database as a backup, the configuration you provided will enable AAA authentication for privileged-level access on a Cisco device.

Example for TACACS+ configuration

```
vIOS-L2-01(config)#aaa authentication login default group tacacs+ local
```

Figure 74:TACACS+ configuration

```
vIOS-L2-01(config)#aaa authentication enable default group tacacs+ local
```

Figure 75:TACACS+ configuration 2

- aaa authentication: Set parameters for AAA authentication.
- enable – Indicates that this setting affects privilege level access.
- If no other authentication method is explicitly set, this specifies the default authentication method to be used.
- TACACS+ must be used for authentication, according to tacacs+.
- local - Indicates that in case TACACS+ authentication fails, the local database should be used as a backup alternative.

Administrator need create local user account if TACACS+ server failed therefor the administrator need run **username {username} privilege {privilege value} secret {password}** command.

```
vIOS-L2-01(config)#username abcd privilege 15 secret 1111
```

Figure 76:create local user account

The administrator need specify what is the server ip address then devices can learn what the authentication server

```
CORE1(config)#tacacs-server host 10.1.1.100 key cisco
```

Figure 77:specify TACACS server

```
!
aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ local
!
!
```

Figure 78:example for AAA configuration text result 1

```
!
!
username nim secret 5 $1$mERr$yZKBoxU.805LdhSXOw6y61
!
!
!
```

Figure 79:local user account configuration text result

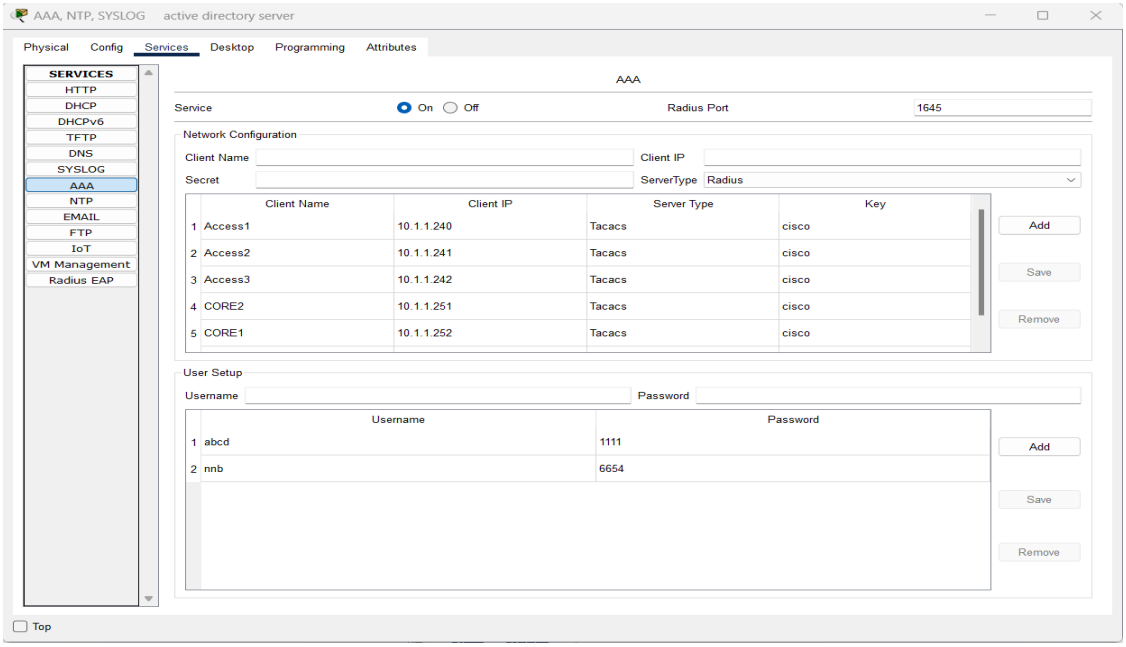


Figure 80:AAA server Configuration

SSH configuration

Secure Shell, also known as SSH, is a cryptographic network protocol used for secure remote access and control of computers, servers, and other networked devices. SSH allows secure network-based communication between two untrusted hosts.

According to the network the administrator configures SSH on network Devices this because the administrator can manage and access network devices remotely and secure.

First administrator need configure hostname and domain name for cisco devices

The administrator needs enabling SSH version 2 using **crypto key generate rsa** and the administrator need specifies the key length in bits, which in this case is 1024. the larger number of bits key length is stronger the encryption and authentication.

Example for Configure SSH

```
vIOS-L2-01(config)#crypto key generate rsa modulus 1024
```

Figure 81:example for enable SSH

Finally, the administrator need enable line vty for user login using line vty **{specific amount of one-time access}** commonly use **line vty 0 4** commands.

Example for line vty command

```
vIOS-L2-01(config-line)#line vty 0 4
vIOS-L2-01(config-line)#transport input ssh
```

Figure 82:example for SSH Configuration

After the configuration the administrator can log into devices remotely using TACACS+ authentication server.

Example for remotely access devices

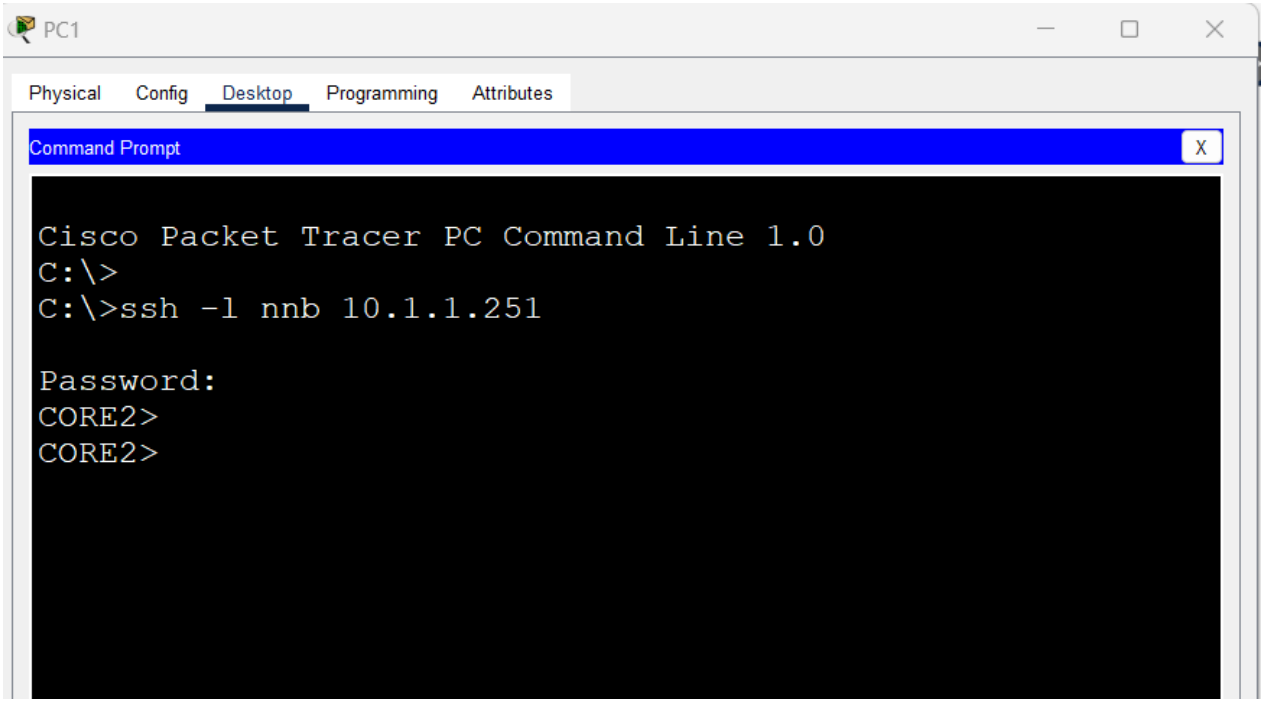


Figure 83:Example for SSH access

NTP (Network Time Protocol) configuration

A protocol called NTP (Network Time Protocol) is used to synchronize computer clocks over a network. A server that provides time synchronization for network clients is known as an NTP server.

According to the ABCD network implementation The Time is a very impotent for Debug Errors in Network Devices therefore the network administrator decided configure NTP server.

First administrator needs specific server for NTP. According to the network specification the administrator uses 10.1.1.100 server for NTP

Example for configuration NTP server

```
ACCESS1(config)#ntp server 10.1.1.101
```

Figure 84:NTP server configuration

Example for NTP Text Result

```
ACCESS1#show clock
16:44:45.937 UTC Fri Apr 14 2023
```

Figure 85:show clock command result

```
!
ntp server 10.1.1.101
!
end
```

Figure 86:NTP configuration result

WLC Wireless Lan Controller Configuration

The wireless LAN controller is called a WLC. It is a network device that controls wireless access points (APs) in an organization environment. The wireless infrastructure, including configuration, monitoring, and security policies. Using centralized Wireless LAN Controller.

According to the ABCD Network Topology it has two access point to control trough wireless LAN controller. This WLC manage access point authentication using radius server.

Configuration Steps in WLC

First administrator need must connect WLC to network after connecting administrator need configure its IP address, subnet mask, default gateway, and DNS settings.

Next administrator can access WLC though the web base application. Entering WLC Ip address in this example the administrator uses 10.1.12.20 ip address

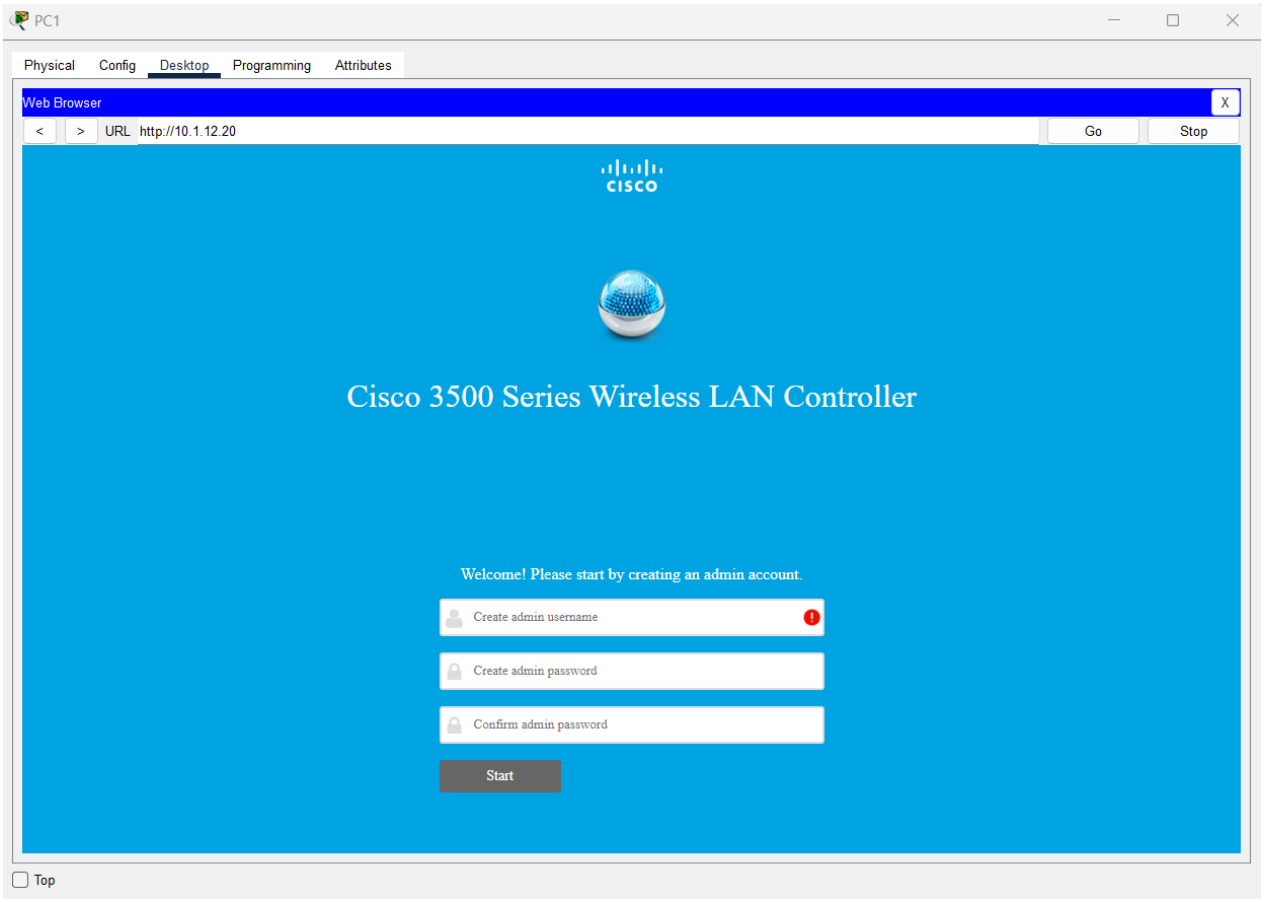


Figure 87:WLC configuration 1

In this phase administrator need must create user account for login wireless LAN controller

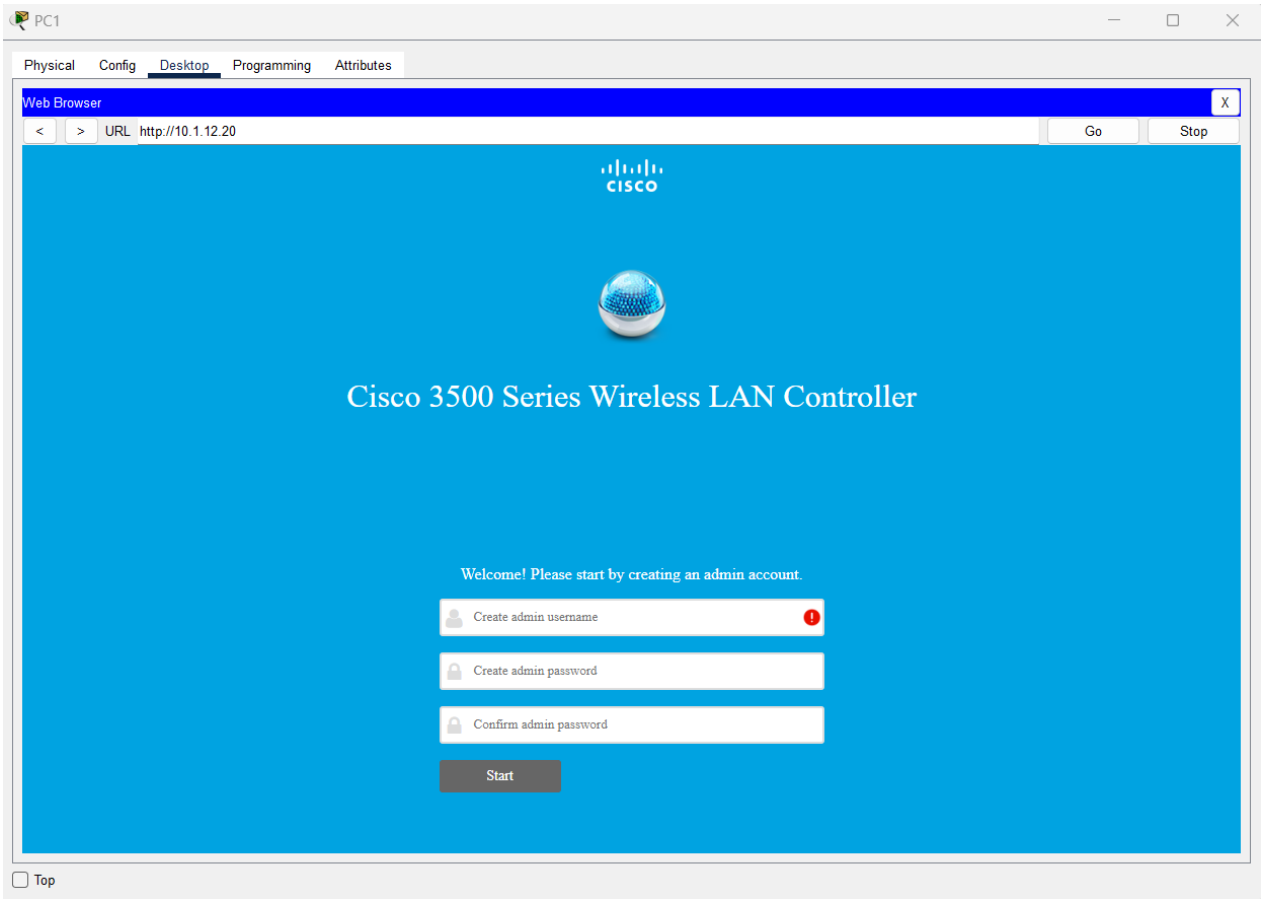
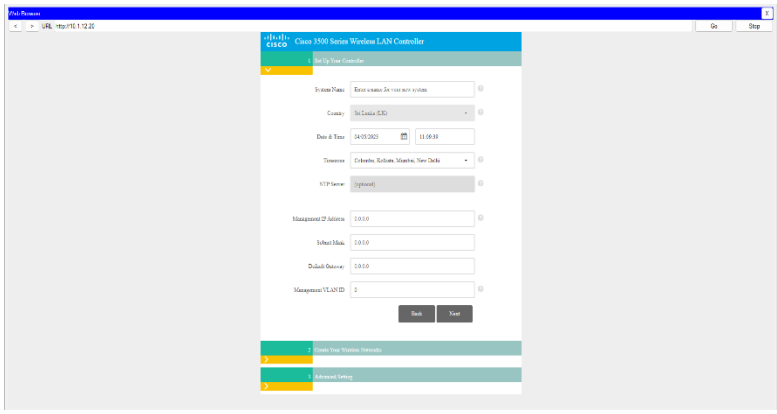
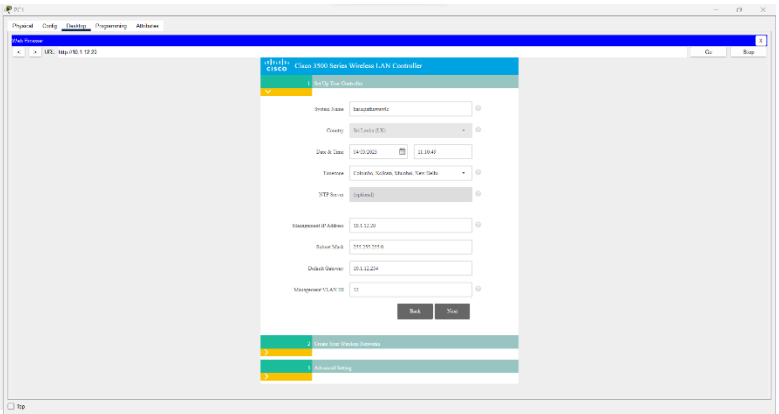


Figure 88:create new user for wireless LAN controller

After creating user account, the web browser pop up basic configuration in wireless Lan controller. In hear administrator need configure date and time, country, system name, WLC management ip address and subnet mask.





Then administrator need configure wireless local area network in this phase administrator create for employes custom wireless network.

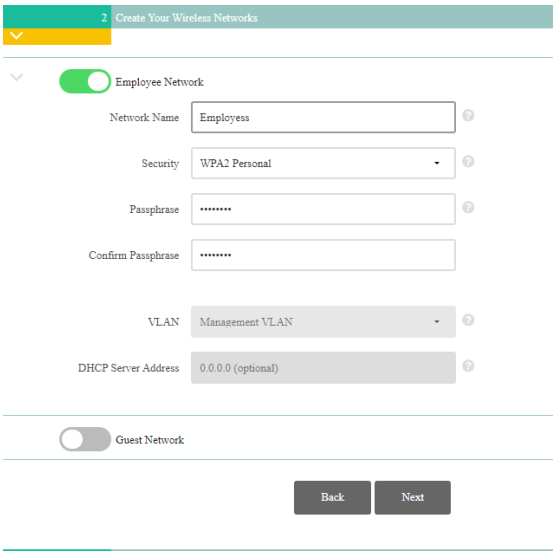


Figure 91:create custom wireless Local area network

Finally end the basic configuration the WLC need to reboot before reboot WLC administrator must need check configurations are correct or not if configuration are not correct administrator need go back and reconfigure WLC.

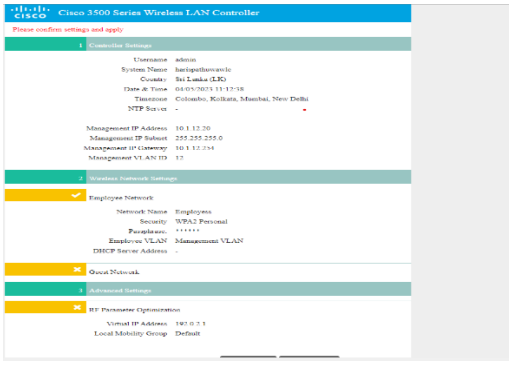


Figure 92:finally, text configuration is correct or not

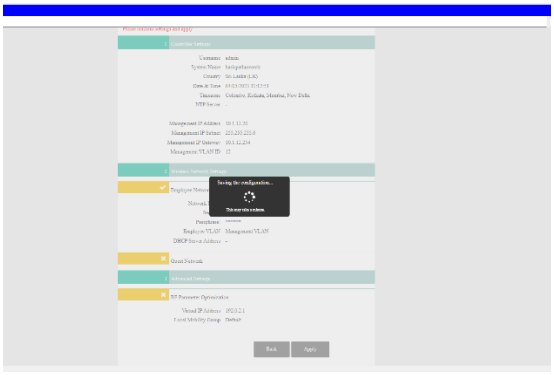


Figure 93:Reboot WLC

After reloading WLC, the administrator need log in again in this time the administrator can see WLC dash bord with contain some data about WLC

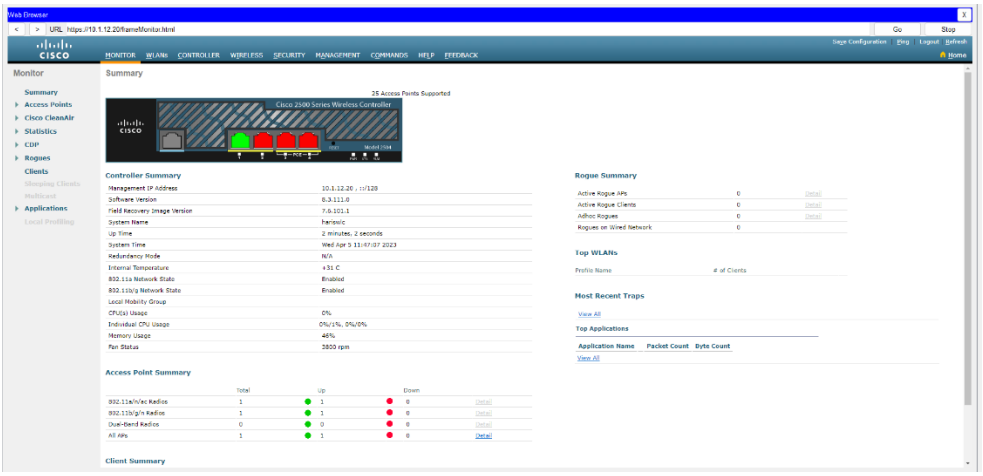


Figure 94:WLC Dash Board

Configure new Wireless Local Area network

Configuring new WLAN, it has several steps

First administrator need select WLANs tab

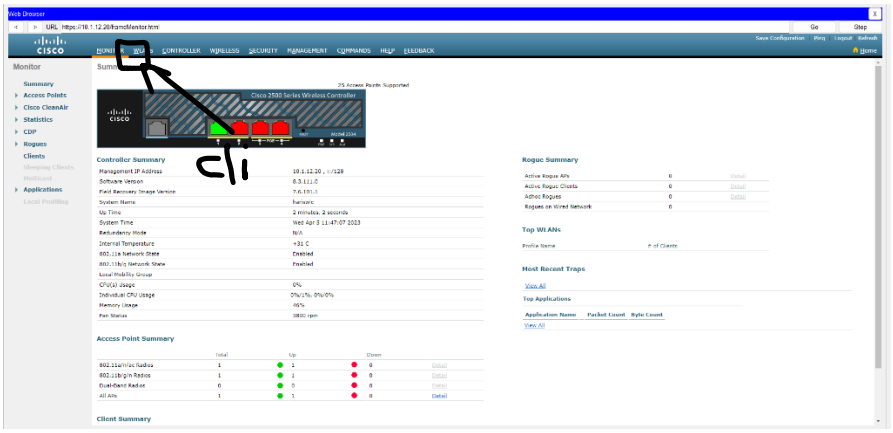


Figure 95:example for WLAN Configuration

Now administrator can see new web interface for configure WLAN

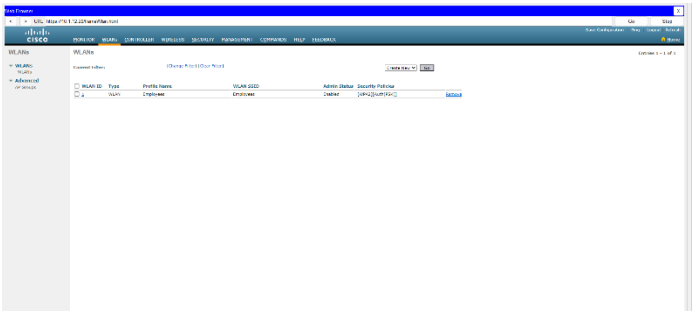


Figure 96:example for WLAN configuration

In bellow image has 1 pre-configured WLAN. This created by administrator during the basic configuration. Now administrator need add one more WLAN therefor administrator need click create new icon.

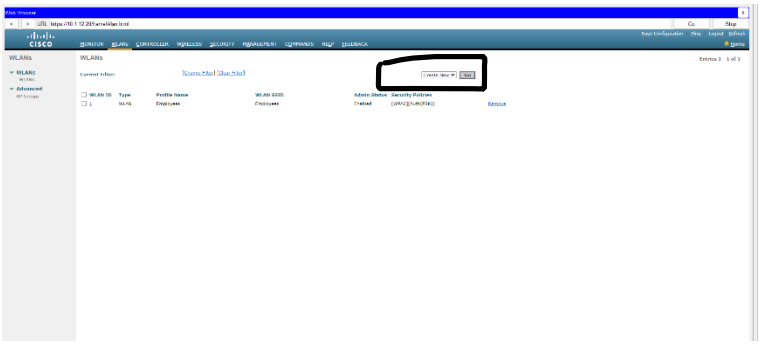


Figure 97:WLAN configuration example

Next administrator can create new WLAN typing WLAN profile name, SSID and WLAN ID after selecting these configuration administrators can click apply button for save the configuration next administrator can select authentication methods or set password for WLAN according to network.

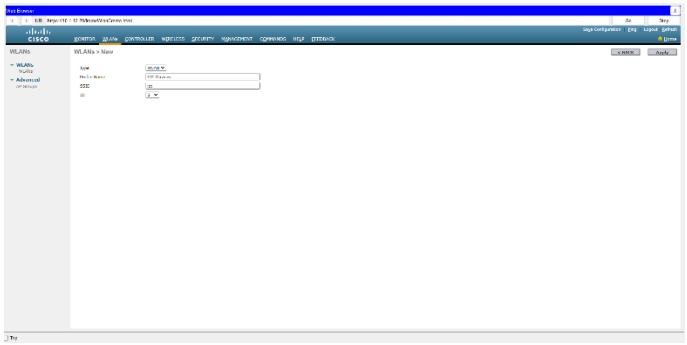


Figure 99:create new WLAN Profile

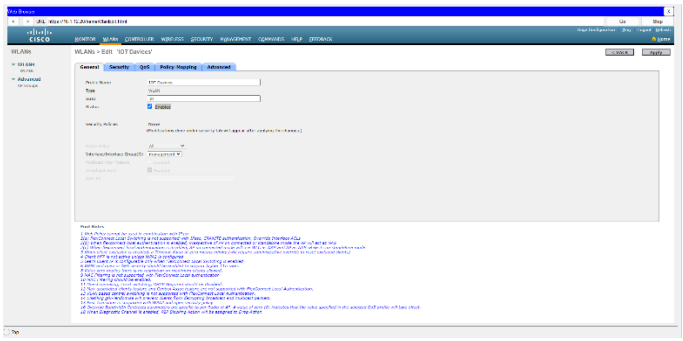


Figure 98:change Status to Enable

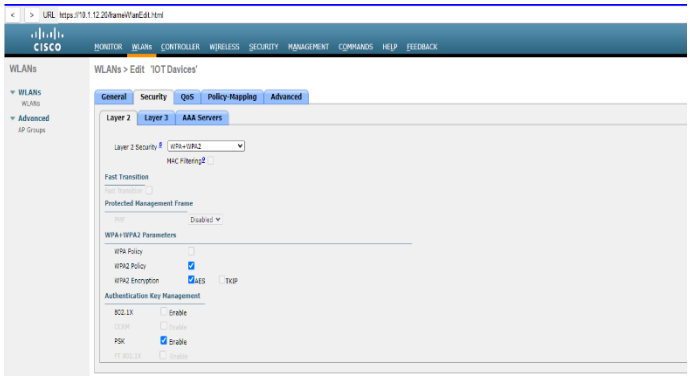


Figure 100:Select Authentication method or set password for WLAN

Configure Radius server for WLAN users

In a wireless networking, a Radius server is often used for authentication, permission, and accounting functions. A Radius server is used in the context of a Wireless LAN Controller (WLC) to authenticate wireless clients and grant them access to the wireless network.

Configuration steps

First the administrator need select security area in navigation bar after administrator need add new radius authentication server to WLC

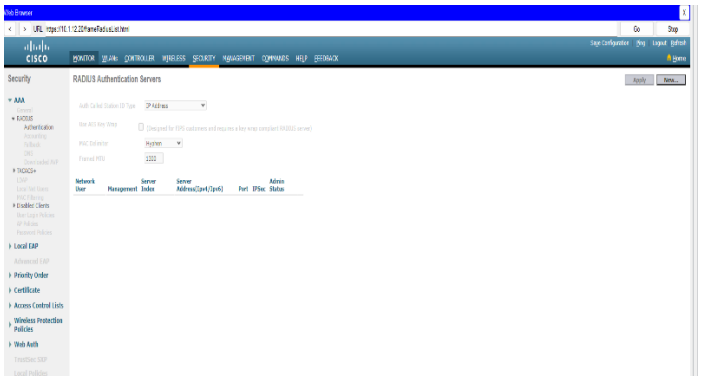


Figure 102:select Security tab in navigation bar

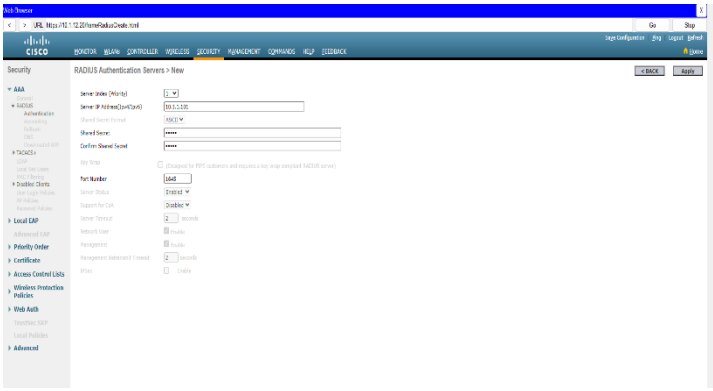


Figure 101:add new authentication server to WLC

New server configuration step has several configurations to do first administrator need enter server ip address next administrator need add shared key in radius server and port number.

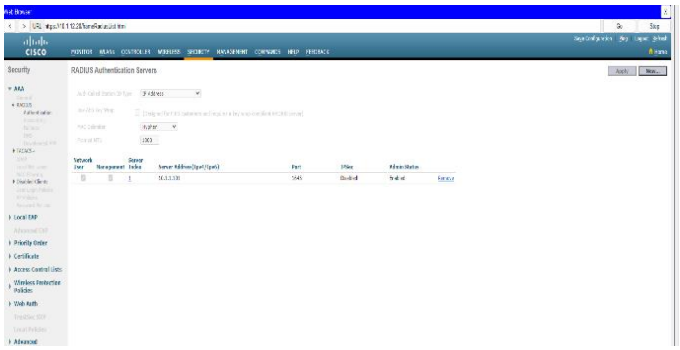


Figure 104:Example for WLAN Configuration

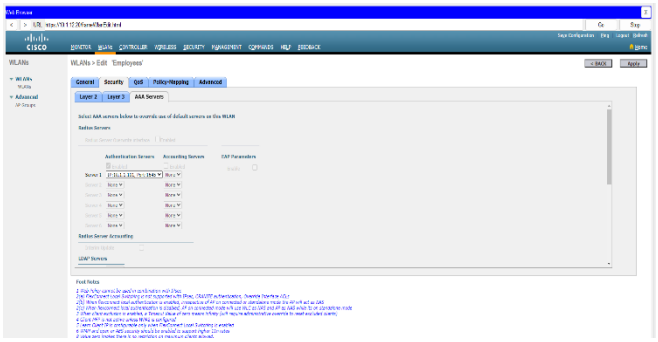


Figure 103:Ading radius server to Specific WLAN

Text result for WLAN Wireless Device configuration

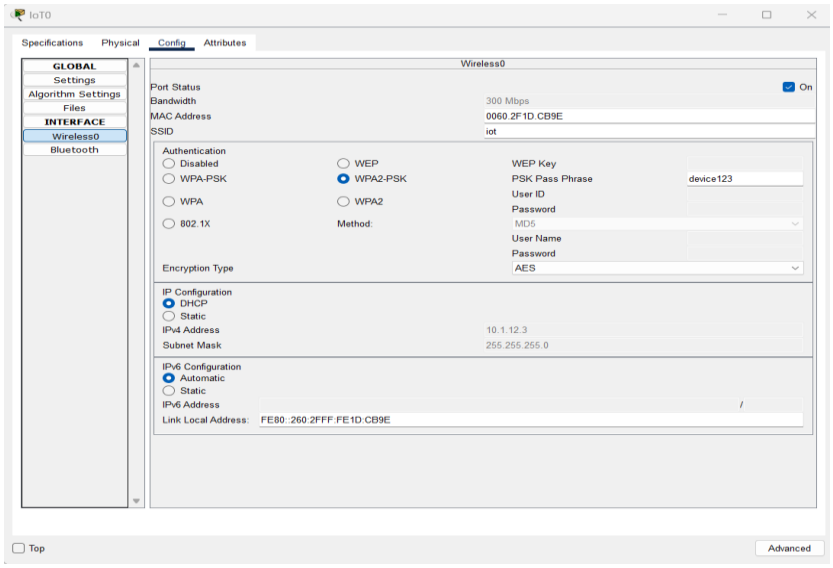


Figure 105:WLAN Wireless Device configuration

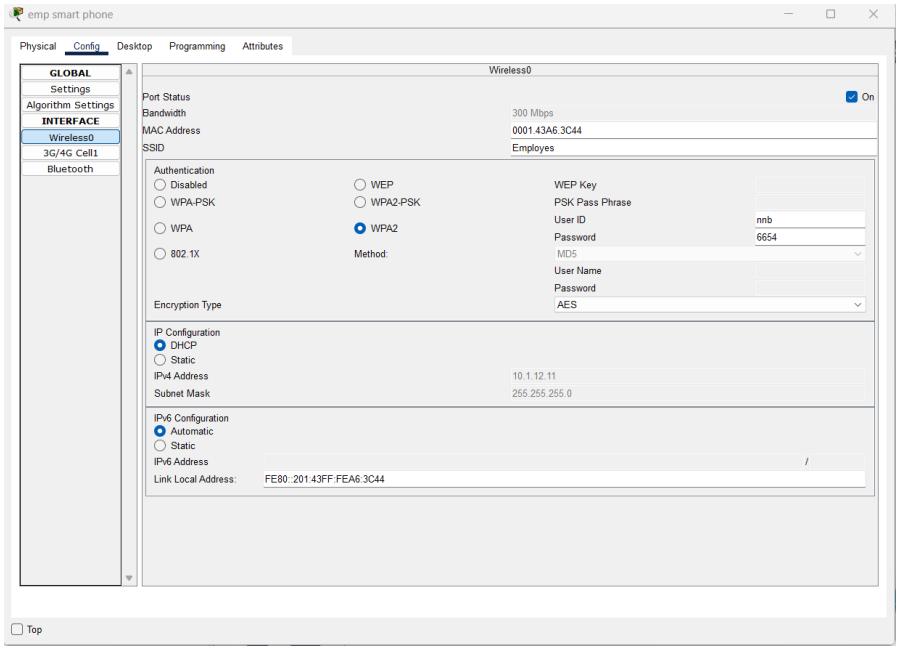


Figure 106:using authentication server login example

IoT (Internet of Things) server configuration

IoT server is a software platform that provide manage and communicate between IoT devices and network the IoT server generally act like central device that collect data from connected devices and process it. Also, it sends commands to devices as needed.

First of all, administrator need log in to IoT server web interface using Ip address for create new user. then the administrator can add IoT devices to IoT server finally server provide service to manage, process, and collect information on IoT devices

Configuration Example

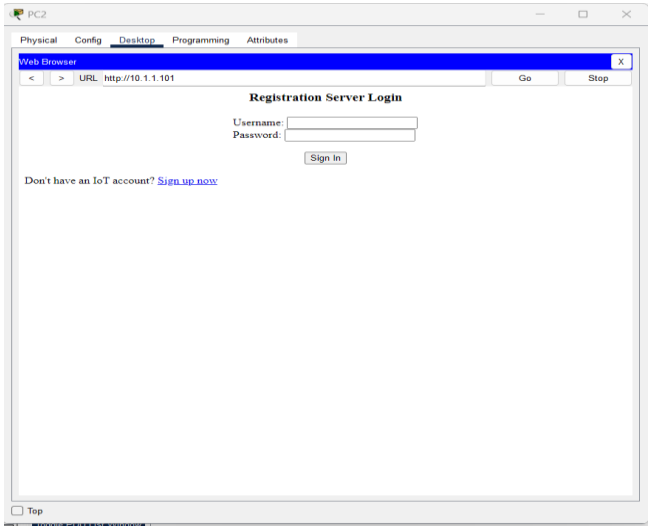


Figure 108:step 1 - create new user clicking sing up link

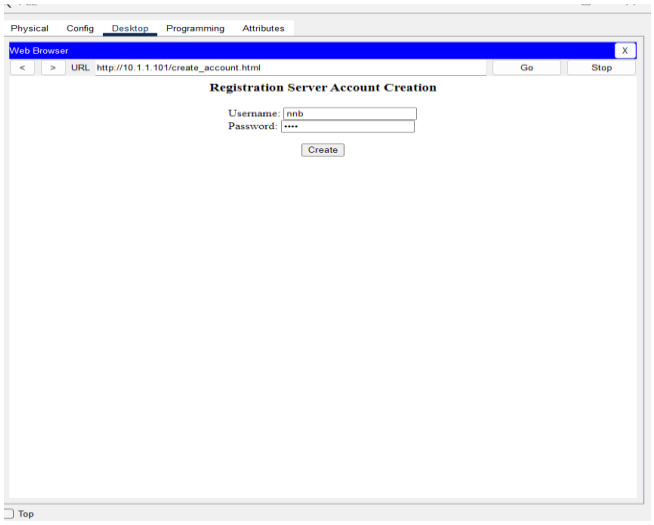


Figure 107:step 2 - create New User

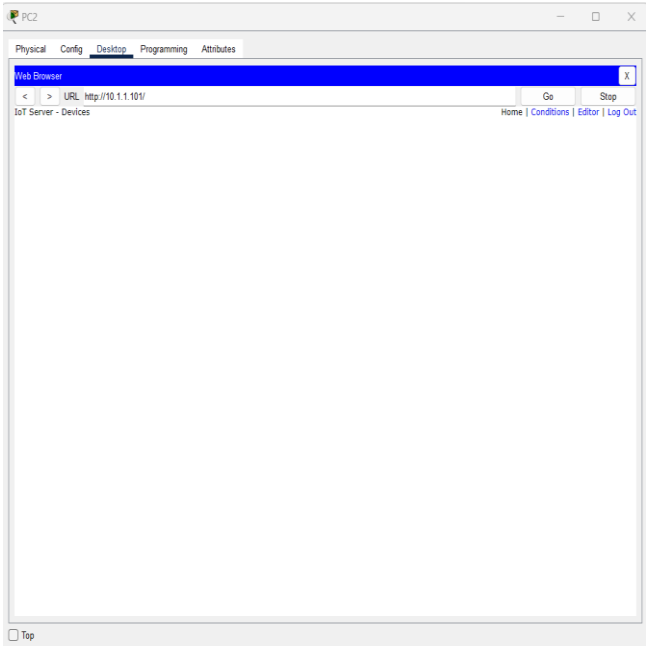


Figure 109:step 3 login to web interface using user credentials

After configuring IoT server the administrator need Connect the IoT devices to the IoT network. Configure the devices to communicate with the IoT server, such as setting the server IP address. according to the ABCD corporative society network that server ip address is 10.1.1.101 and it default gateway is 10.1.1.254 and also the administrator need configure server credential.

Configuration Steps on IoT devices

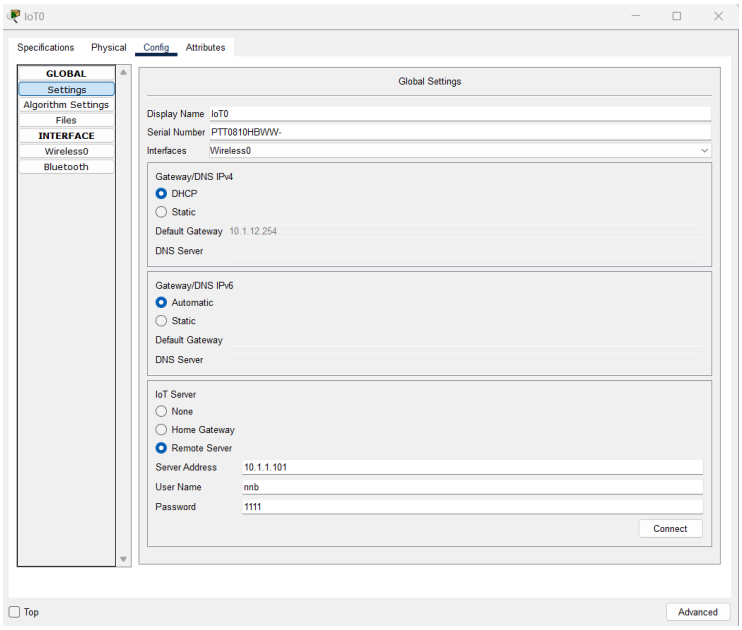


Figure 110:configure IoT Device Example 1

After IoT device configuration the administrator can see the IoT devices control panel trough IoT web server interface. using that interface administrator can manage all IoT device from a same place.

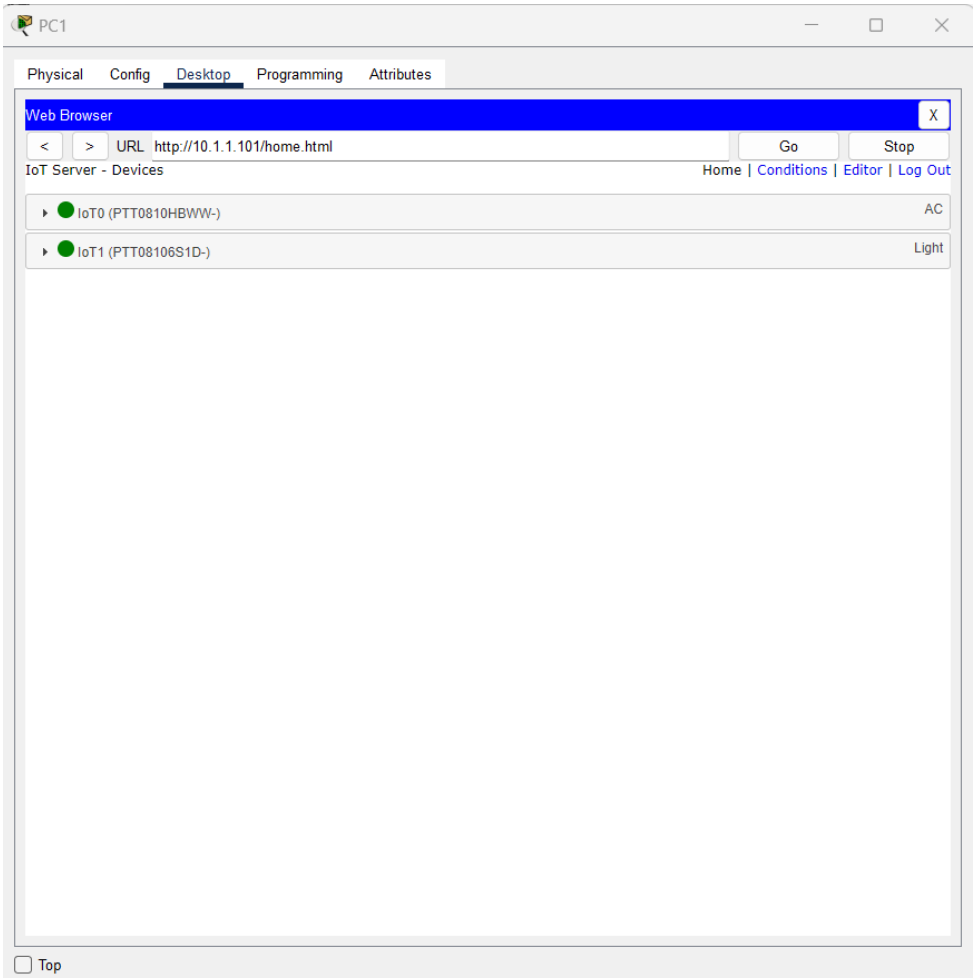


Figure 111:example for Web Interface

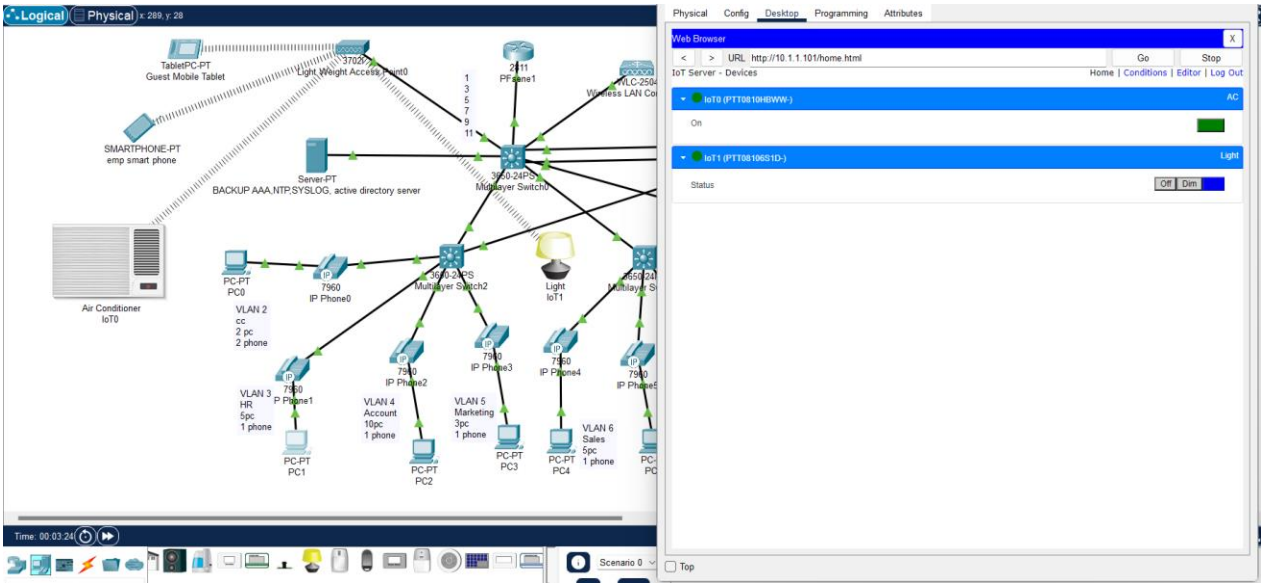


Figure 112:Example for change Devices status

IP phone configuration

Ip phones are provides several advantages over traditional analog phones. The ip phones us the internet or a company's private network to make calls and also, ip phones can be used anywhere with an internet connection.

According to the ABCD cooperative society network the users need communicate with customers and employees. To achieve this the administrator, configure ip phones for communication.

To start ip phone configuration administrator need connect ip phone and computer to switchport. Ip phone has two deferent Ethernet ports one for computer and other for switch.

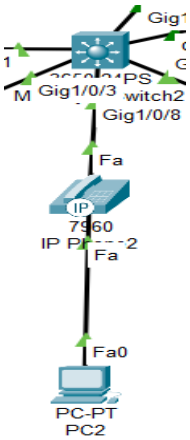


Figure 113:example for connecting Devices

Next Administrator need create new VLAN for Ip phone it because VLAN Allows for better security by isolating network traffic from deferent devices or group of devices and also voice traffic require high-quality and uninterrupted data transmission VLAN allows for QoS to be implemented on a network, ensuring that voice traffic is prioritized over data traffic.

```
vIOS-L2-01(config)#vlan 11
vIOS-L2-01(config-vlan)#name voice
vIOS-L2-01(config-vlan)#
```

Figure 114:Example for create VLAN

```
vIOS-L2-01(config-if)#int gi 0/0
vIOS-L2-01(config-if)#switchport voice vlan 11
vIOS-L2-01(config-if)#
```

Figure 115:Assign switchport to VLAN

```
ACCESS1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/22, Gig1/1/1, Gig1/1/2, Gig1/1/3
                                                Gig1/1/4
2    CustomerService                  active    Gig1/0/1, Gig1/0/2
3    HumanResource                    active    Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/6
                                                Gig1/0/7
4    Account                          active    Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18
5    Marketing                        active    Gig1/0/19, Gig1/0/20, Gig1/0/21
6    Sales                            active
7    GeneralManager                   active
8    SecretaryOffice                  active
9    GasStation                       active
10   CorpCity                         active
11   Voice                            active    Gig1/0/1, Gig1/0/3, Gig1/0/8, Gig1/0/19
111  VLAN0111                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 116:Example for Access switch 1 VLAN

Next administrator need Configure the network settings on the IP phone, including the IP address, subnet mask, default gateway, and DNS server. This can be done manually or automatically through DHCP.

```
 default-router 10.1.10.254
ip dhcp pool VLAN11
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.254
 option 150 ip 10.1.11.253
!
```

Figure 117: ip phone DHCP pool configuration

In above image the administrator need configuration network address default-gateway and option field that option field In VoIP, (Voice over IP) configurations, where IP phones must obtain configuration files from a TFTP server in order to function, option 150 is frequently used. When a device, such as an IP phone, asks the DHCP server for an IP address, the server usually includes the option in the configuration and transmits the IP address of the TFTP server along with the DHCP lease information.

Finally, administrator need register devices with it phone number

Example for ip phone configuration

Figure 118:Test result example for ip phone configuration

```
.
telephony-service
 max-ephones 10
 max-dn 10
 ip source-address 10.1.11.253 port 2000
 auto assign 1 to 10
!
ephone-dn 1
 number 1001
!
ephone-dn 2
 number 1002
!
ephone-dn 3
 number 1003
!
ephone-dn 4
 number 1004
!
ephone-dn 5
 number 1005
!
ephone-dn 6
 number 1006
!
ephone-dn 7
 number 1007
'
```

Figure 119:configure ip phone, phone number

SolarWinds Kiwi Syslog Server

Kiwi Syslog Server is a Syslog server and network monitoring tool that allows administrators to collect, view and analyze syslog messages from network devices such as routers, switches, firewalls, and servers. Syslog is a protocol used to send log messages and system events in a standardized format.

This syslog server is support debug networks and analyze network therefor the administrator decide use Kiwi syslog server for collocate network log messages

First administrator needs Download KIWI syslog server and install this server to administrator computer

installation steps

first administrator need read the agreement and agree with that agreement without administrator cannot install SolarWinds kiwi syslog server

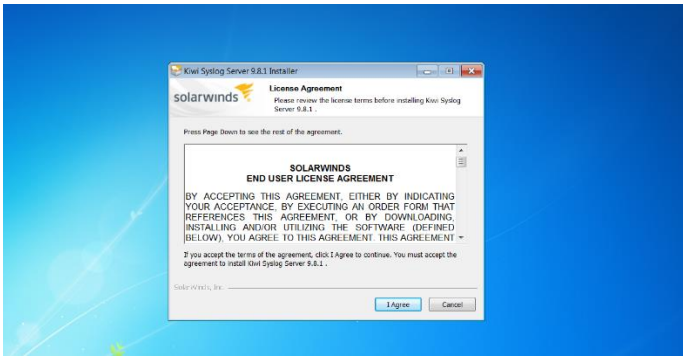


Figure 120:read and agree with user agreement

Decide on the operating system style: Choose between "server as service " or "server as an application" installation. When you install Kiwi Syslog Server, the "server as service" option installs kiwi syslog server as a windows service, allowing the program to run without the need for a user's login to windows this option also installs the kiwi syslog server manager which is used to control the service "server as an application" option allows to install kiwi server as a typical windows application requiring a user to login to windows before running the application.

According to the requirement the administrator choose server as a service operating system mode

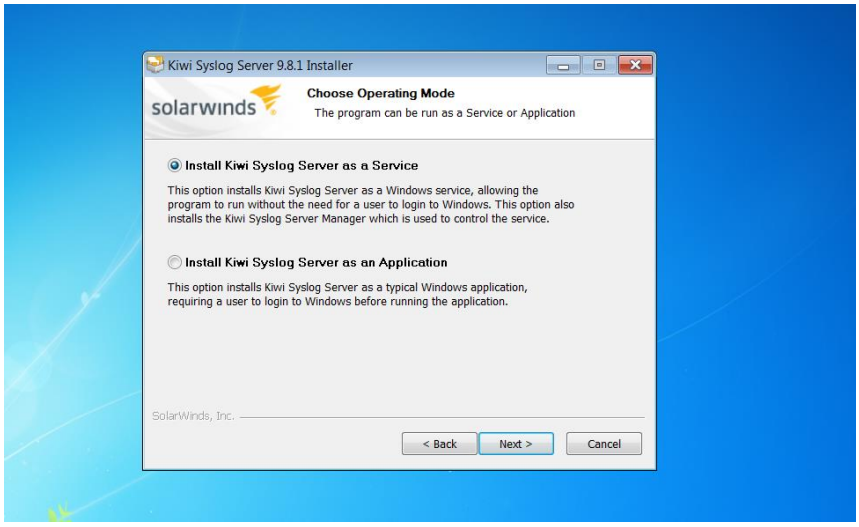


Figure 121:choose operating system mode

Service install option in hear administrator use local account therefore the administrator selects the local system option for installation

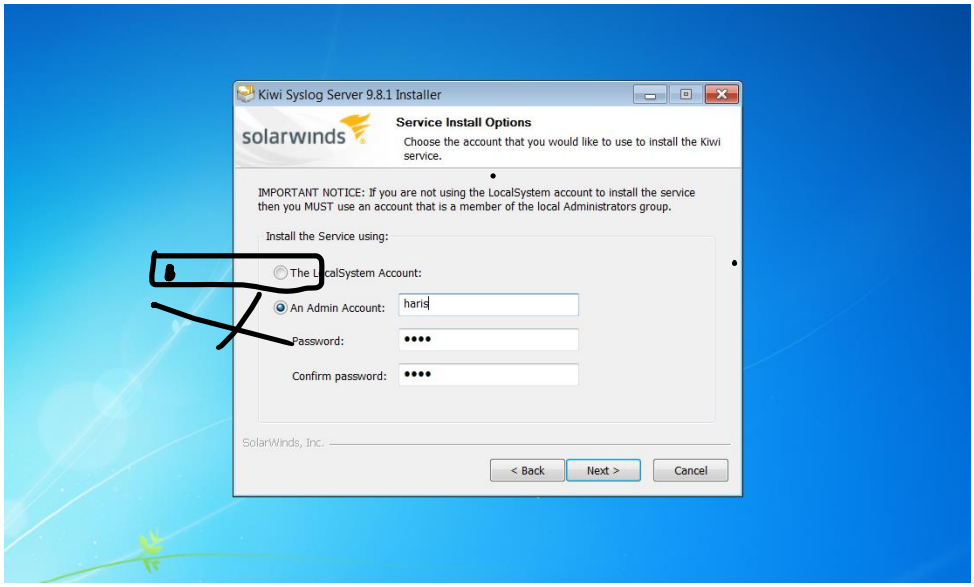


Figure 122:select service install option

According to the ABCD corporative society network the administrator install kiwi syslog web access configurator that will provide remote viewing filtering and highlight syslog events

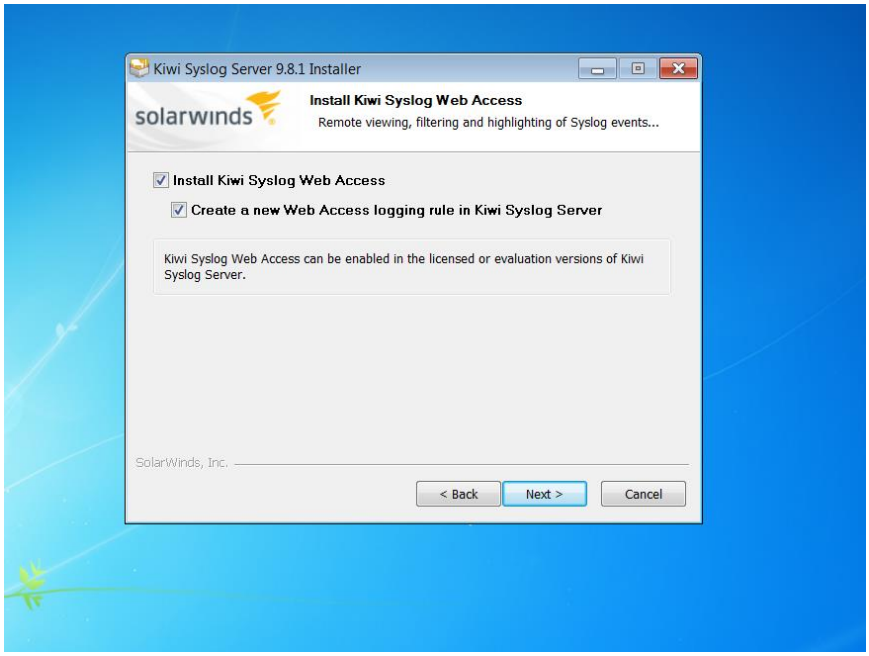


Figure 123:install kiwi syslog web access

Decide on the installation style: Choose between "Custom" or "Normal" installation. When you install Kiwi Syslog Server, the "Normal" option installs it with default settings, while the "Custom" option allows you to choose which features and components to install.

In that example the administrator select Normal mode for install a SolarWinds kiwi syslog server package.

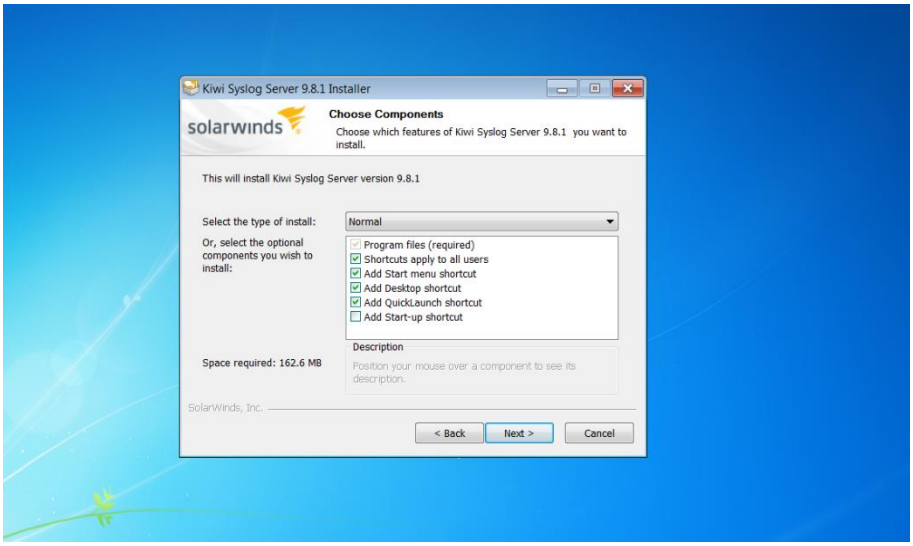


Figure 124:choose installation method

the installation directory of administrator choice: Choose the location to install Kiwi Syslog Server. Normally, the default directory is C:\Program Files (x86). the administrator chooses default location for install kiwi syslog server.

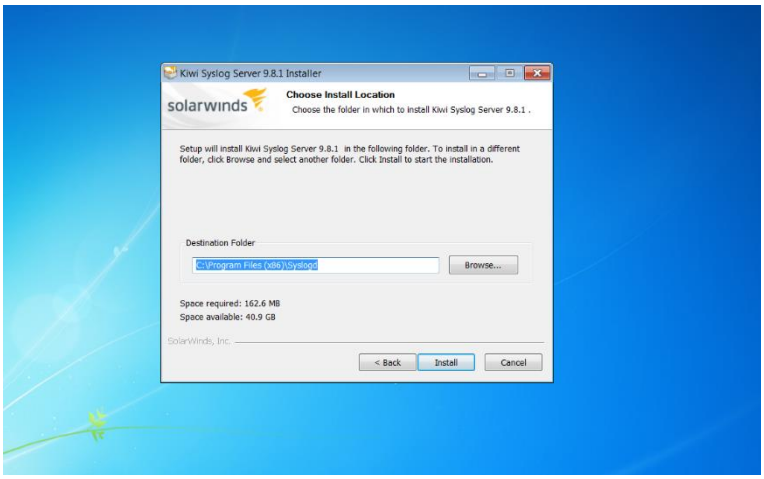


Figure 125:set kiwi syslog server install location

Administrator need install MySQL server for kiwi syslog server support that can install manually or automatically during the kiwi syslog install process according to that project the administrator installs that database server in manually therefore administrator no need installs database server for kiwi syslog server

installing kiwi syslog server

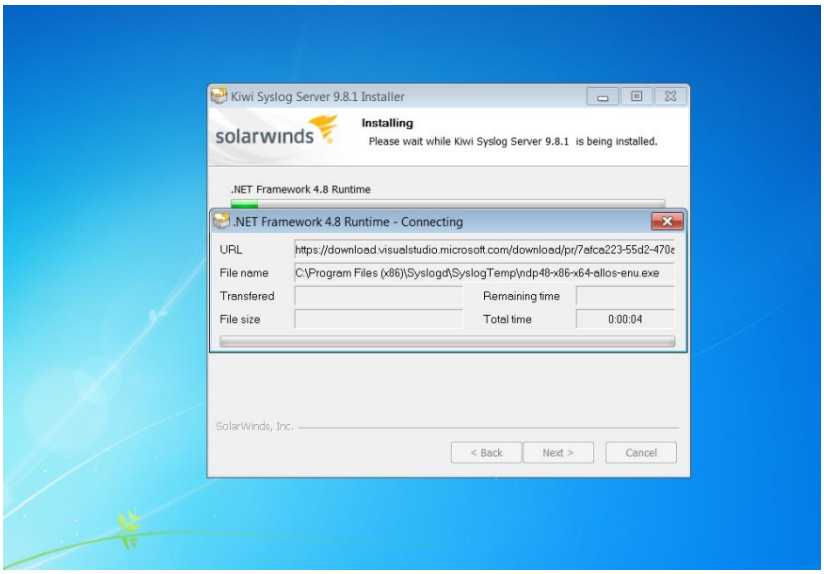


Figure 126:example for installing kiwi syslog server

Configure Kiwi Syslog Server settings, including network interfaces to use for listening, ports to use, and log retention options, after installation is complete.

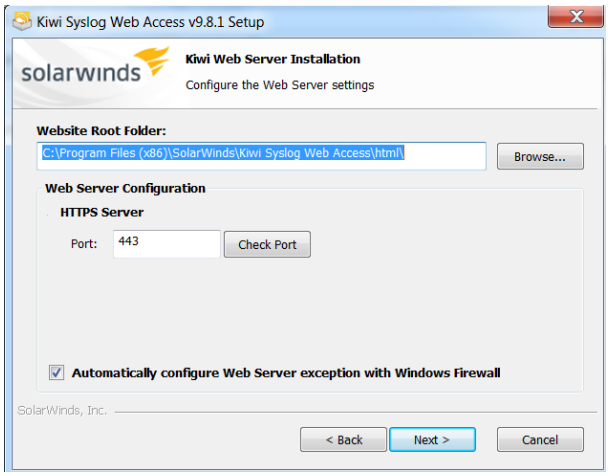


Figure 128:kiwi syslog web server installing example 1

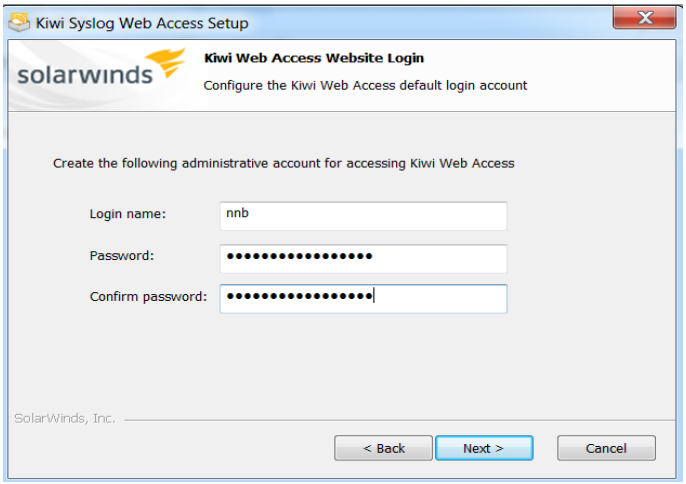


Figure 127:kiwi syslog web server installing example 2

After the installation process the administrator can use kiwi syslog server

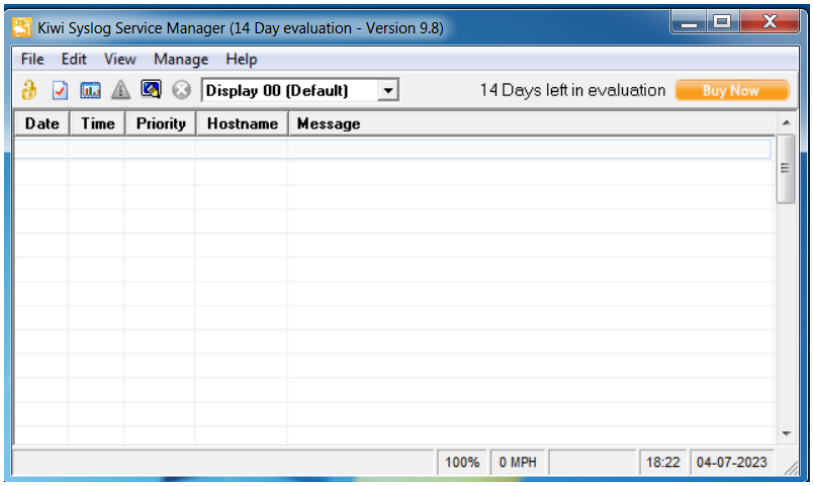


Figure 129:Kiwi syslog server Dash bord

Advertise kiwi syslog server in Cisco devices

```
vIOS-L2-01(config)#logging 10.1.1.20
vIOS-L2-01(config)#
*Apr 15 08:50:16.948: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.1.1.20 port 514 sta
rted - CLI initiated
vIOS-L2-01(config)#
```

Figure 130:configuration in core switch 1

Result of kiwi syslog server

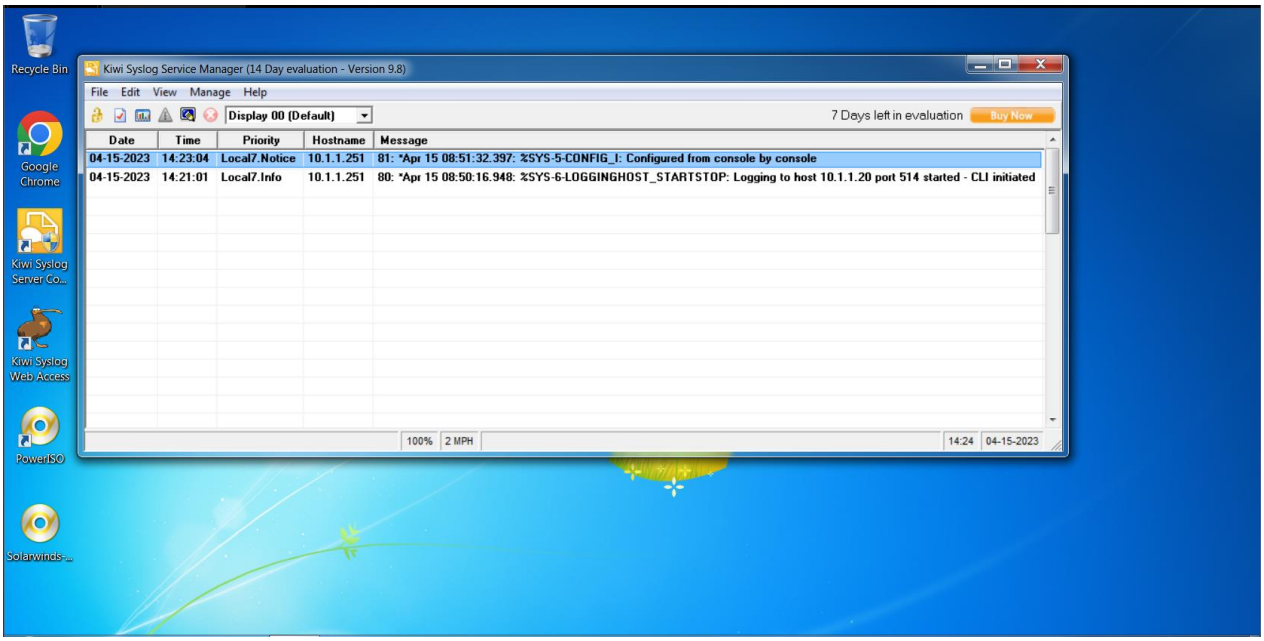


Figure 131:example for reed log messages

Windows server installation

Windows server is an operating system design specifically for used in server environments. the windows server provides features and tools for organization to run special application, deploy web sites, manage database, store and share files and manage network infrastructure such as printers, computers.

And also, windows server provides security features like advance firewall configuration

First administrator need get copy of the windows server install media which can be mounted as a virtual drive or burned to DVD as an ISO file

In hear administrator use Rufus application for create bootable device

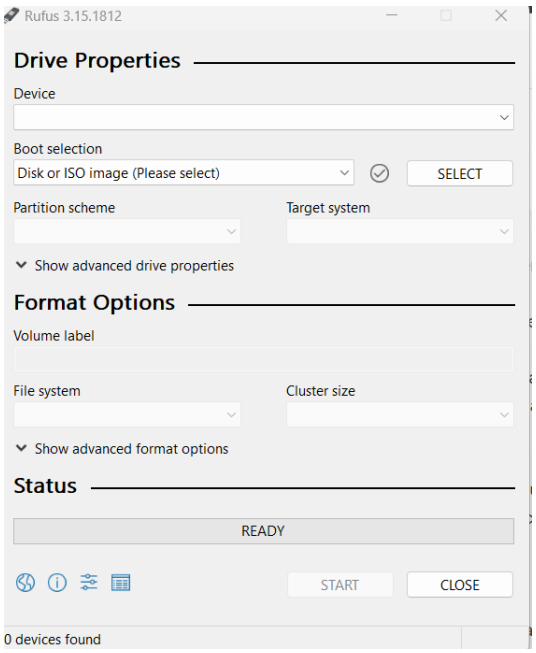
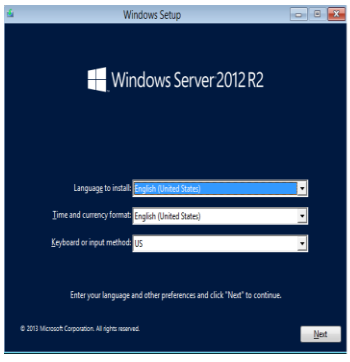


Figure 132:example for rufus software

Administrator need Power on the server and configure the BIOS to use the installation disk to boot. and Click "Install Now" after choosing the language and other regional options offered.



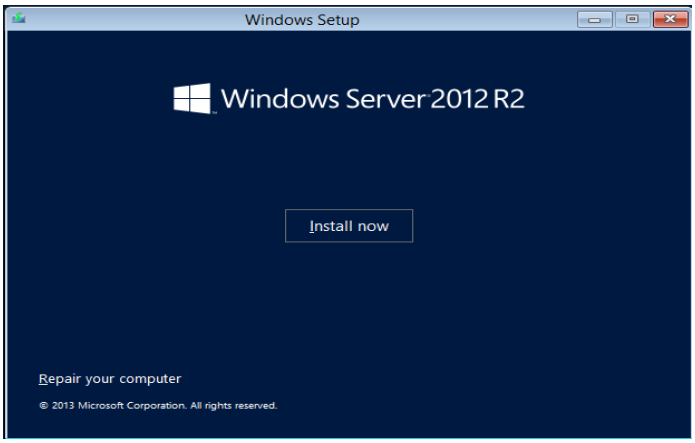


Figure 133:example for windows server configuration

Next administrator needs to enter windows product key and accept the license terms. After administrator Select the partition where administrator want to install Windows Server after choosing the installation type (such as "Server Core" or "Desktop Experience"). Partitions can also be added, removed or changed as needed.

According to the ABCD cooperative society network the administrator installed 2 deferent windows servers in one server for primary sever or root server and other server for backup server or standby server. In that primary server select Desktop server and other backup server use core server mode for installation.

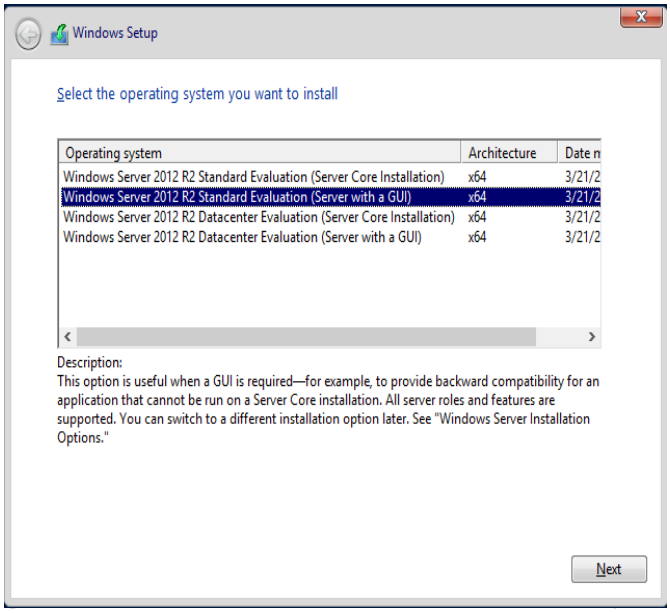


Figure 135:Select server operating system mode

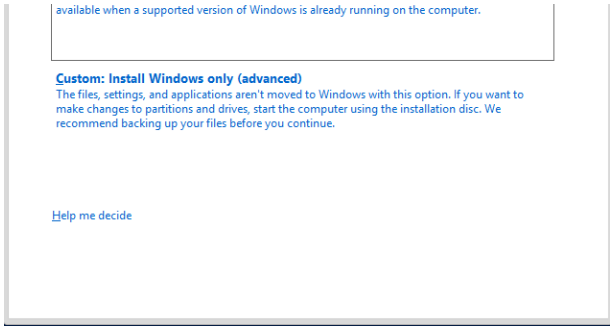


Figure 137:Select Installation type

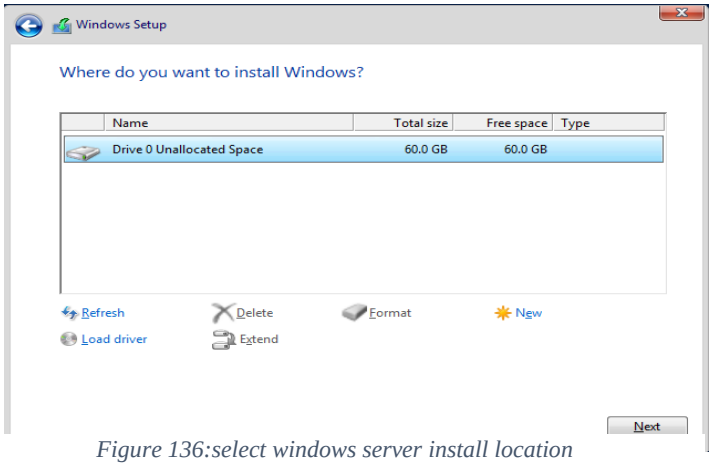


Figure 136:select windows server install location

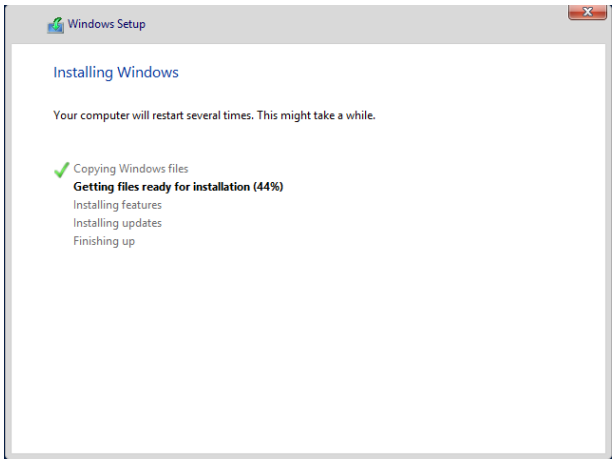


Figure 138:windows server installation example

To complete the installation, follow the instructions, the administrator need to provide the server's name and network settings, as well as the administrator password.

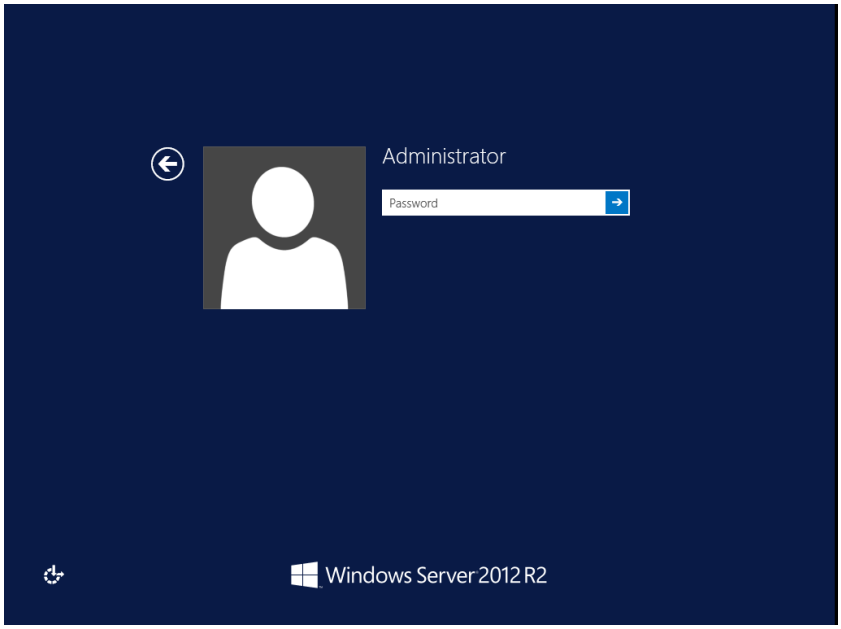


Figure 139:Login to windows server

Windows server user interface

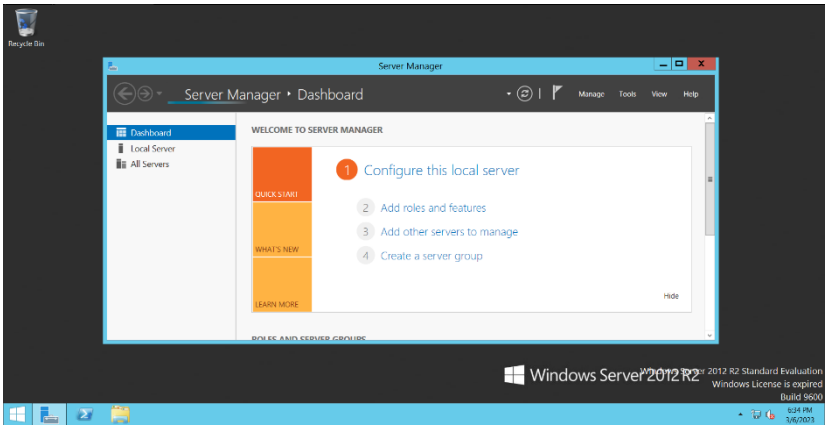


Figure 140:Windows server user interface

Active Directory configuration (AD Configuration)

Active directory found by Microsoft that technology used for managing and organizing users, computers and other network resources.

The windows server active directory needs several steps to configure AD server

First of all the administrator need install active directory domain services (AD DS) role on a windows server

First administrator need click add roles and features tab the administrator need install Active directory domain service

AD DS installation steps

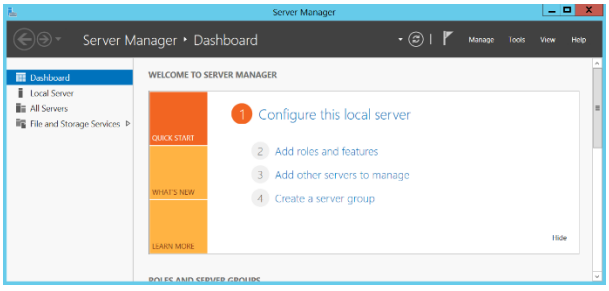


Figure 142:Step 1

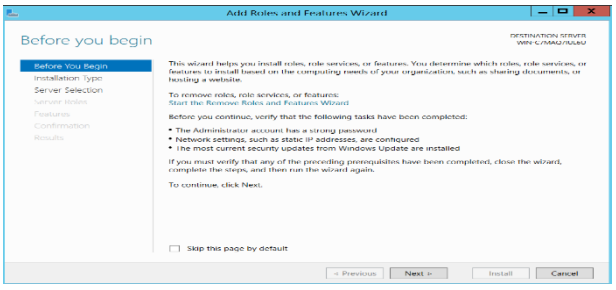


Figure 141:step 2

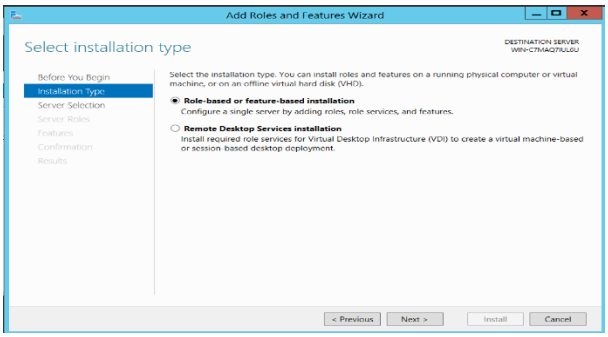


Figure 144:step 3

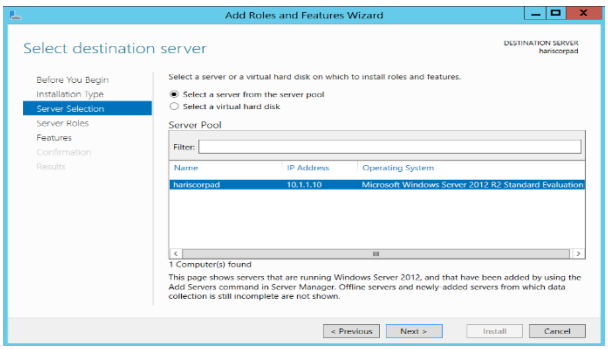


Figure 143:step 4 selects Windows server

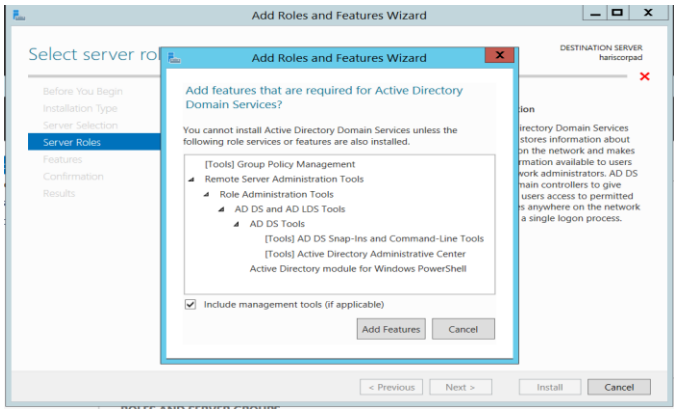


Figure 146:step 5

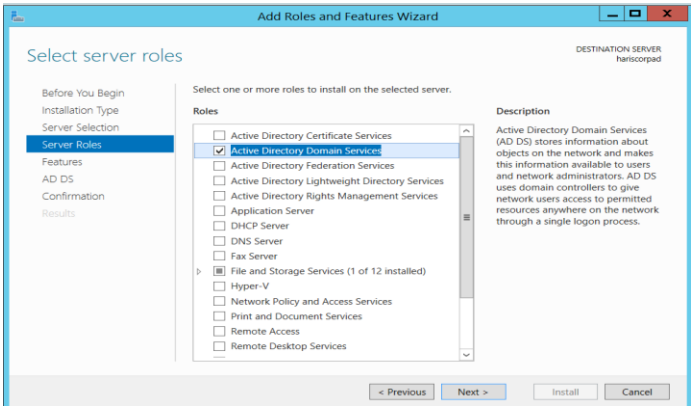


Figure 145:step 6 install select server roles

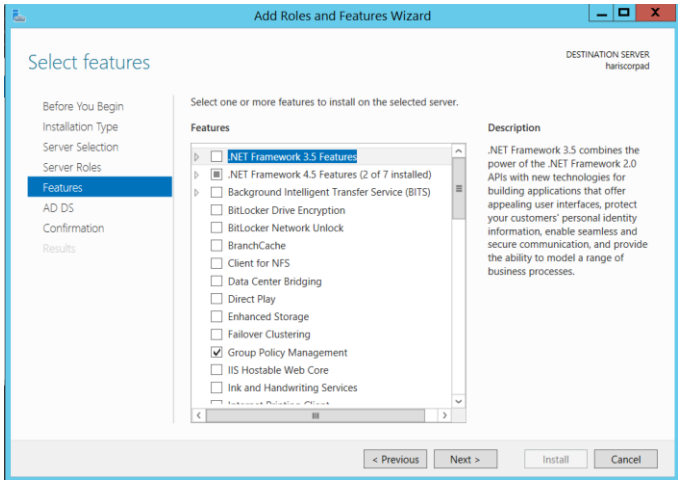


Figure 148:step 7 selects server features

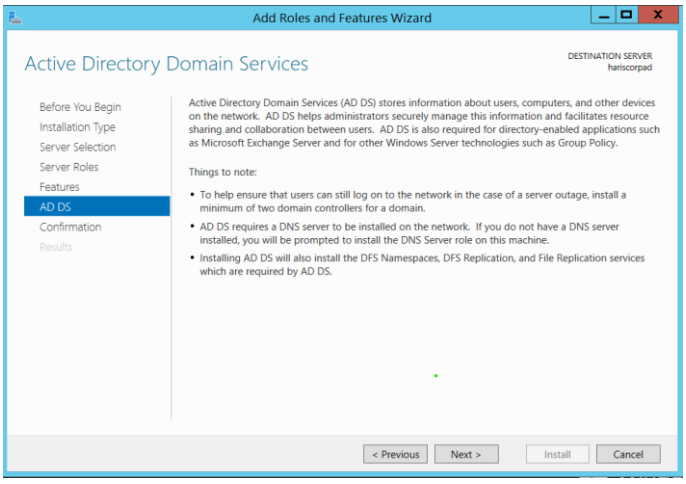
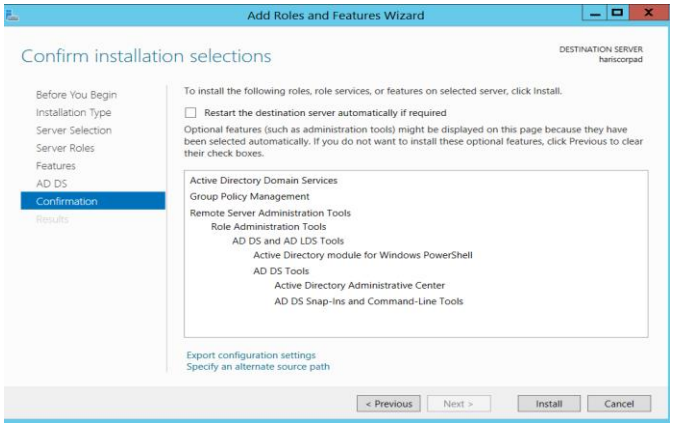


Figure 147:step 8



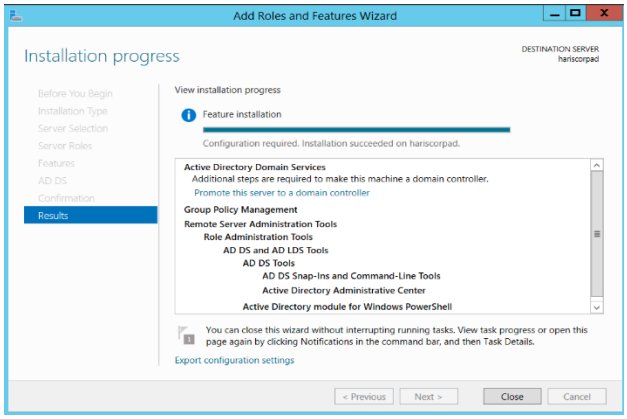


Figure 149:step 10 install server roles and features

Figure 150:install services

After the install AD DS roles, the administrator need run active directory configuration wizard to configure domain controller

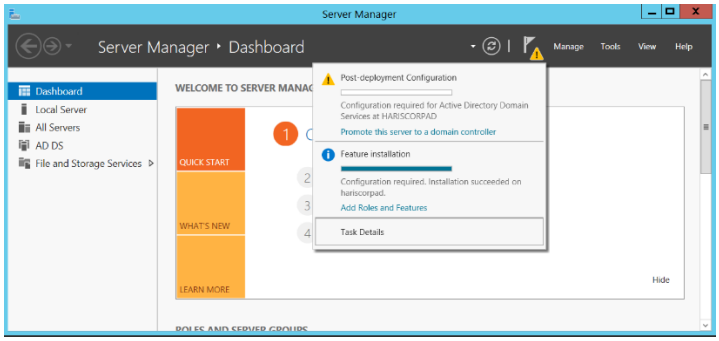


Figure 151:example for AD DS configuration wizard

First administrator need to provide a domain name which the name that will be used identify the active directory domain. According to the ABCD corporative society network the administrator decide ABCDcorp.com is a domain name for that server.

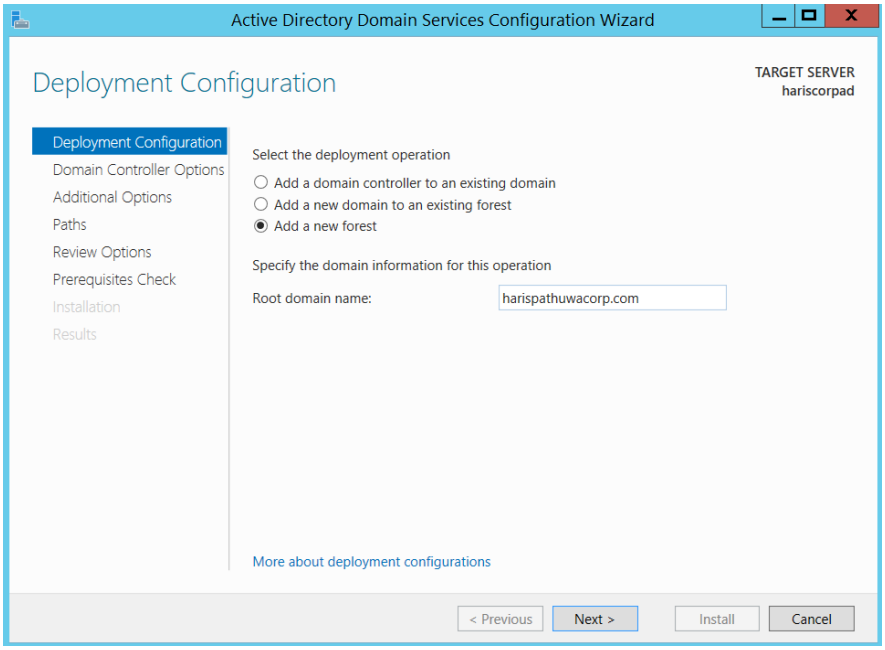


Figure 152:Active directory domain name configuration example

In above image the administrator creates new forest that because the ABCD cooperative network has not any forest.

The administrator need provide a NetBIOS name which is a short name used by older applications and services to identify a domain.

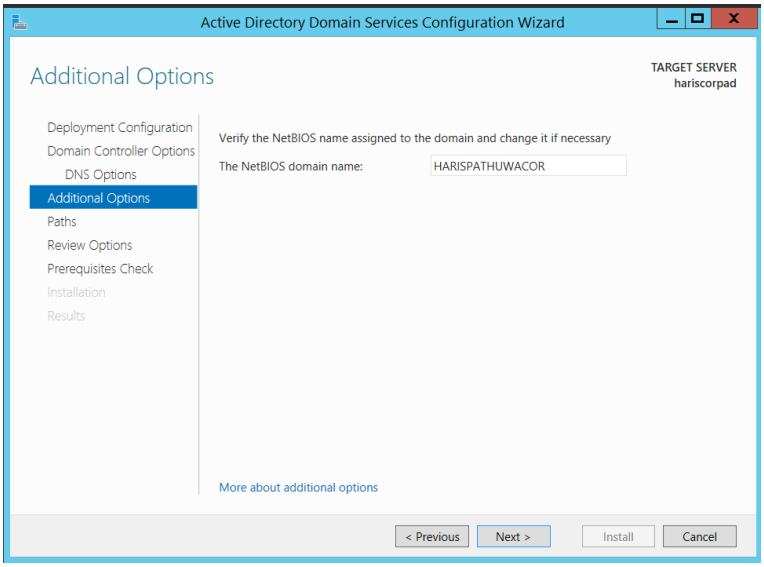


Figure 153:example for NetBIOS configuration

Next administrator need configure the DNS settings to ensure that domain controller can resolve host names and IP address on the network and also the administrator configure directory service restore Mode password used for boot a domain controller to perform certain maintains and recovery task.

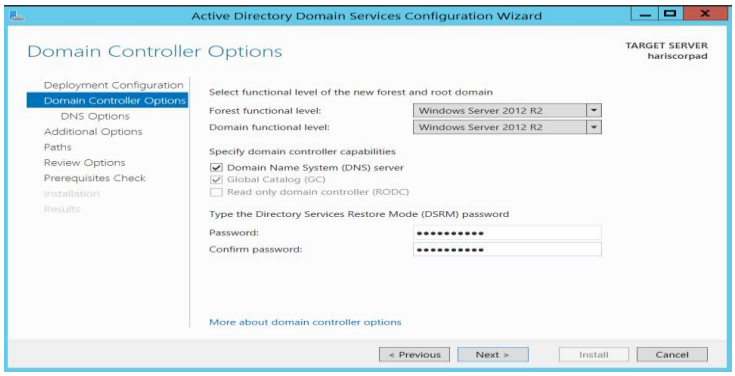


Figure 154:Example configuration for domain control options

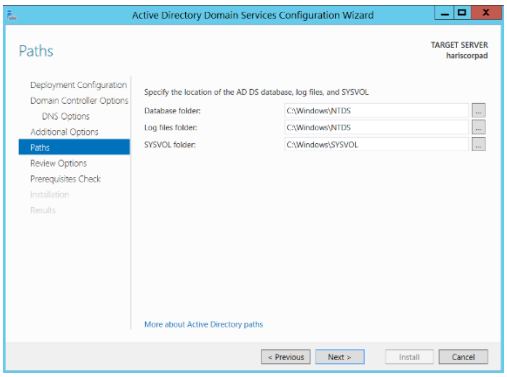


Figure 156:Specify AD DS Database

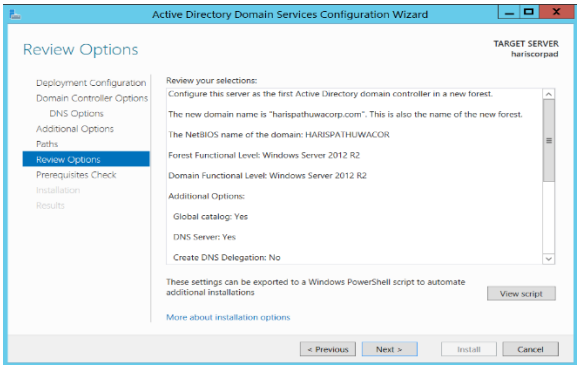


Figure 155:AD DS script configuration

Add computers to domain controller

Finally, administrator can add computers changing their system setting to use the domain controller for authentication and management.

First administrator needs go to computer management setting and administrator need click change setting button after administrator can specify domain name controller to pc

Configuration steps

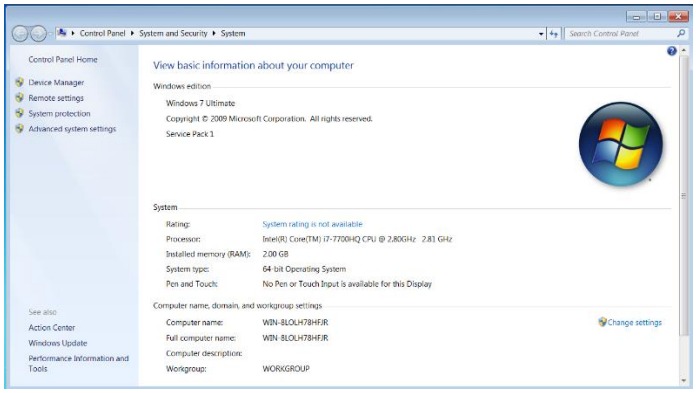


Figure 158:computer setting

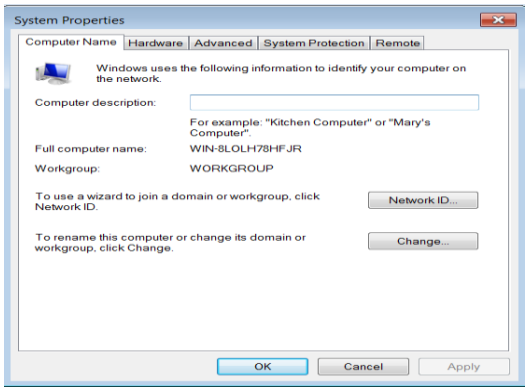


Figure 157:Change computer name and apply it

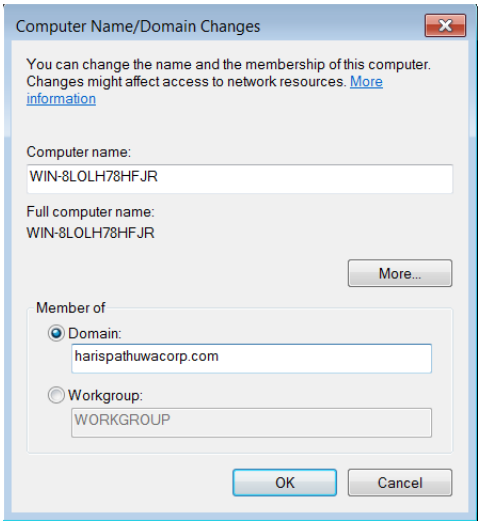


Figure 160:add computer to domain controller

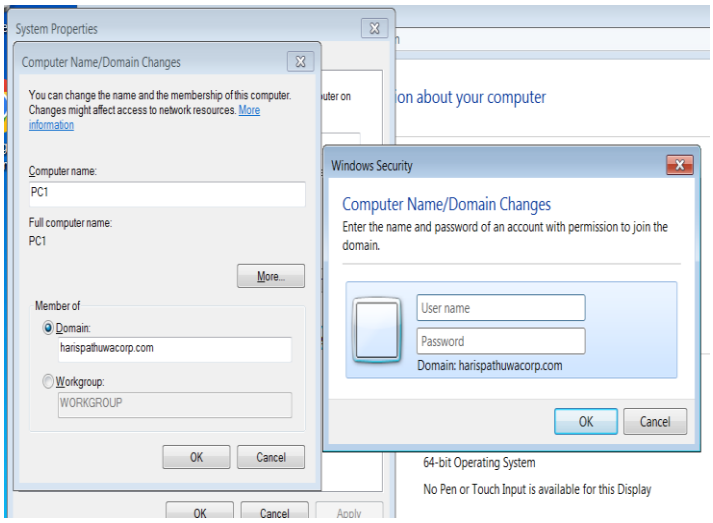


Figure 159:Enter Domain controller credentials

After the adding computer to domain controller administrator can check computer status from active directory users and computers management interface

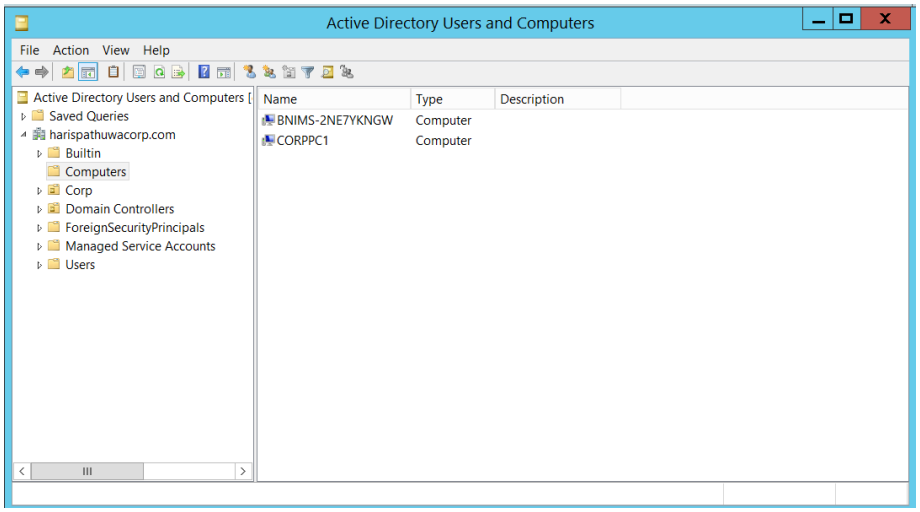


Figure 161:Example for active directory users and computers

Create organizational units

An organizational unit (OU) is a container within an Active Directory (AD) domain that can be used to group resources, such as user accounts, computer accounts, and other OUs, for ease of management.

When configuring OU administrator need log in to domain controller with an administrator account.

After login to domain controller administrator need open active directory users and computer console. Next administrator needs right click on the domain name and select **new** and click **organizational Unit** now administrator can create new organization unit Entering OU name.

Configuration Example for Organizational Unit.

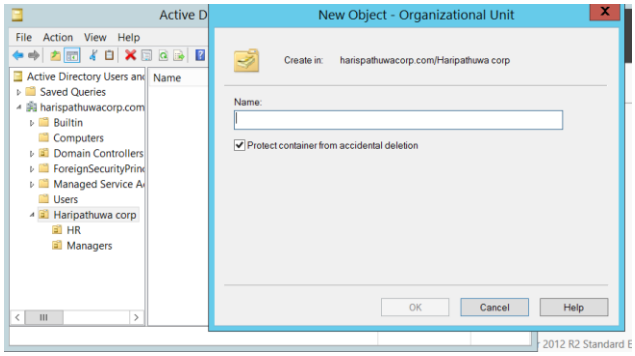


Figure 163:create New OU

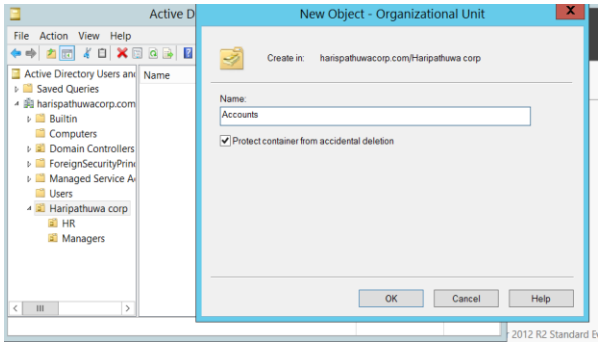


Figure 162:create New OU

Create new user account

Active Directory (AD) should be used to create user accounts and groups in order to control who has access to which network resources. Before configuring User Accounts, the administrator need login to active directory server.

After login to domain controller administrator need open active directory users and computer console. Next administrator needs right click on the domain name and select **new** and click **create new user account** now administrator can create new user account enter the required information for user such as first name, last name, and password also administrator can add department, job title and office location if administrator need.

According to the ABCD corporative society the administrator need configure password chousing user must change password at next time check box that provide Users will not be able to access their account until they have created a new password when they are forced to change it at their next login. This ensures that even if a third party manages to obtain the user's login information, they will not be able to regain access to the account after the password has been changed.

Configuration Steps

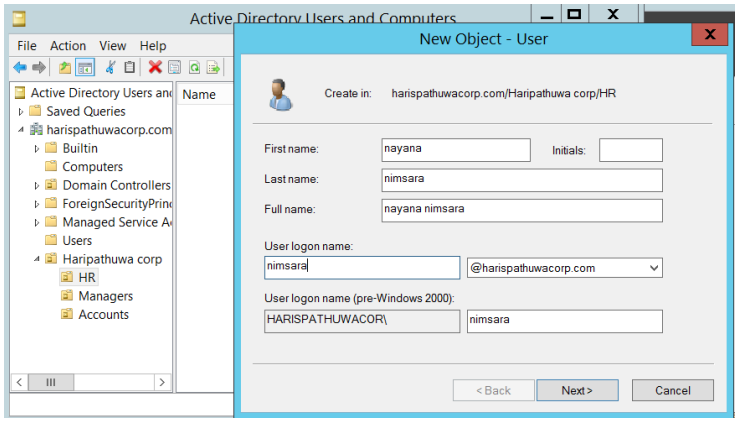


Figure 165:step 1 for create new user account in domain controller

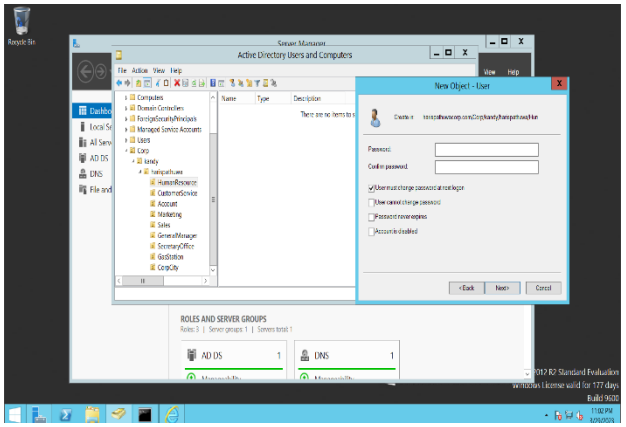


Figure 164:step 2 for create new user account password with user must change password at next logon setting

After the creating user account user can login to the system using login user name and password but in first login user need setup new password for account that because the administrator add user account password with user must change password at next logon setting.

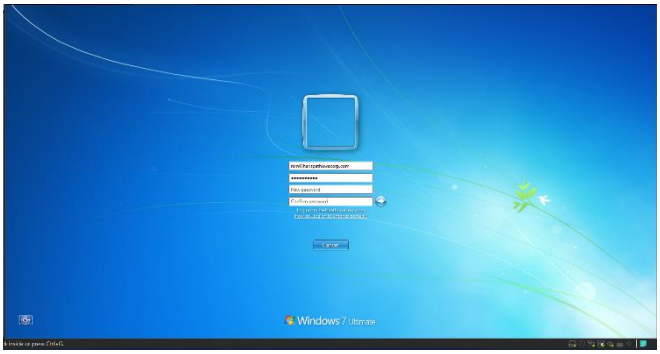


Figure 166:First Time user Login

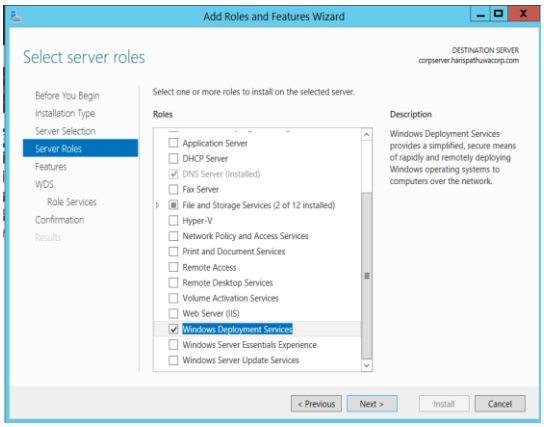
Windows Deployment server configuration

A server feature in Windows Server called Windows Deployment Services (WDS) allows administrators to remotely install Windows operating systems on workstations.

Configuring the WDS Server Role Click Add Roles and Roles in the Server Manager once it has opened. The WDS server feature can be installed by following the instructions.

Open the WDS console after installing the WDS feature to configure WDS. Select Configure Server by right-clicking the server. The server setup wizard must be followed. You must select the PXE server settings, DHCP server settings, and the location where the operating system files will be saved.

Steps of Windows Deployment server configuration



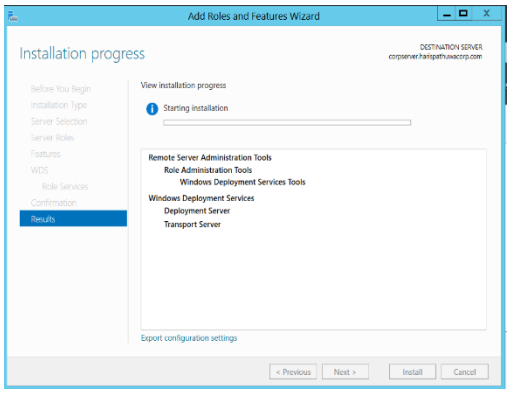


Figure 167;install Windows Deployment server

Figure 168:Select window deployment server Roles for installation

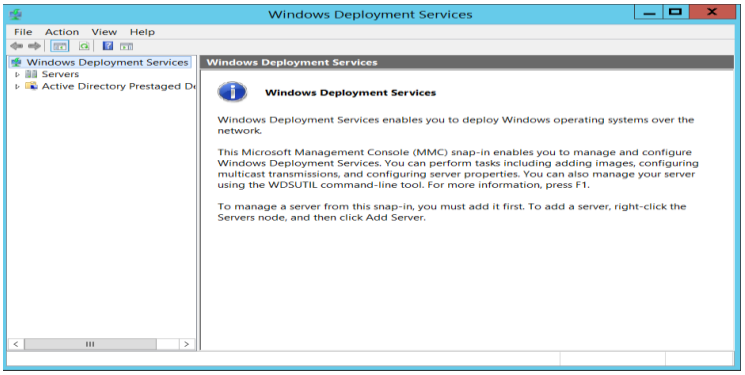


Figure 169:windows Deployment server console

Failover windows server configuration

A backup server called a failover server often called a standby server or a redundant server, is created to take over the workload of a primary server in the event of a failure.

First The administrator needs create server cluster

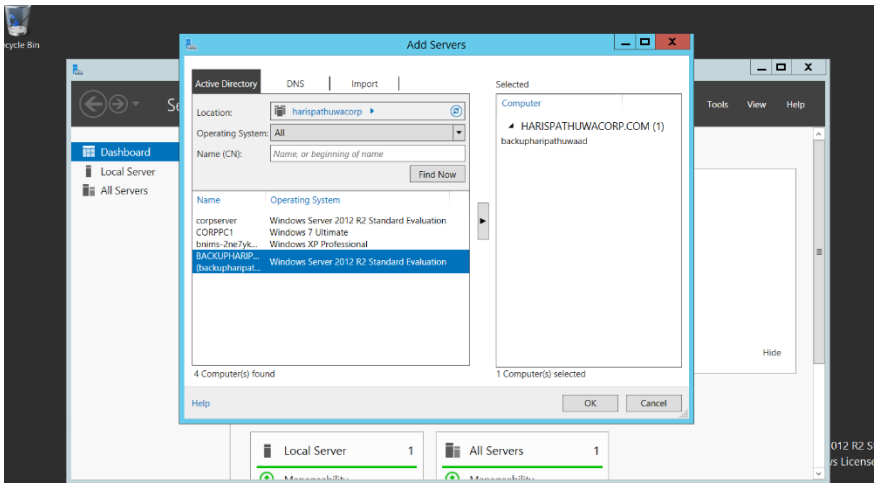
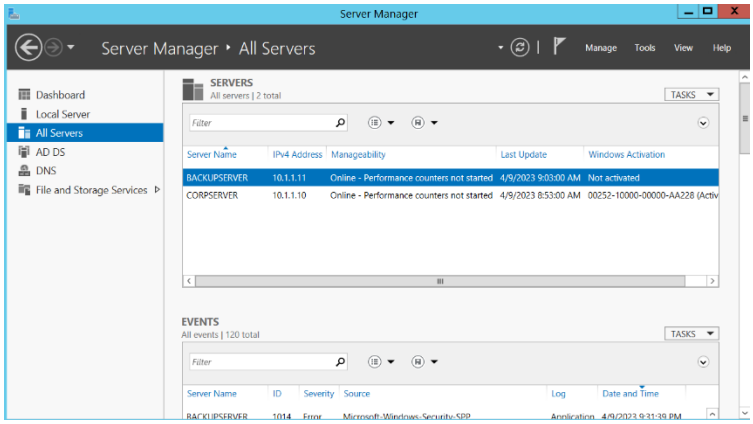


Figure 170:create server cluster



Windows has a feature called Group Policy that allows administrators to centrally control and manage user and computer settings across a network.

The administrator need create new group policy by right clicking on "**group policy objects**" folder and select "**new**" give the GPO name and click ok. The administrator can edit GPO write click on the GPO and select EDIT. The ABCD cooperative society network administrator need edit these group policies according to the network requirement. Also, after configuring GPO The administrator need LINK group policies to OU (organizational Unit).

GPO Configuration example

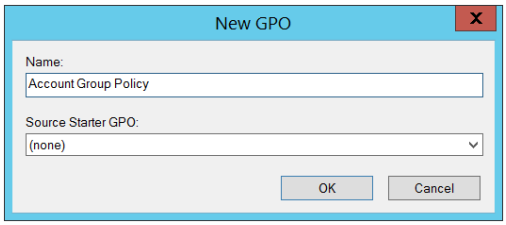


Figure 172:Create New GPO

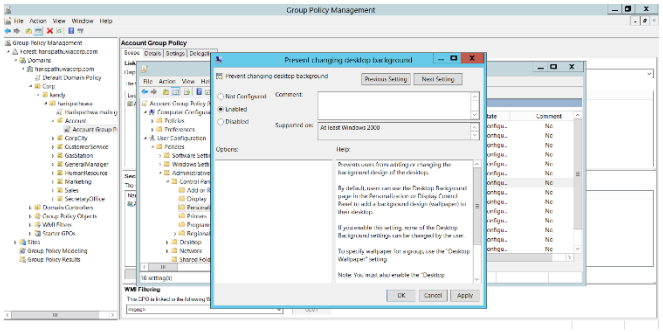


Figure 171:Edit Group policies

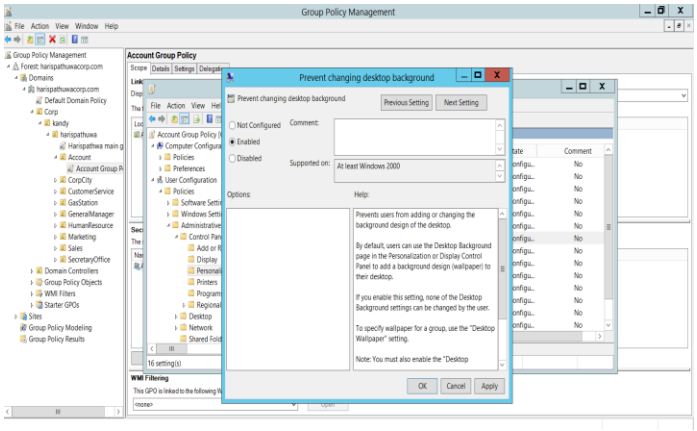


Figure 174:create GPO for prevent change wallpaper

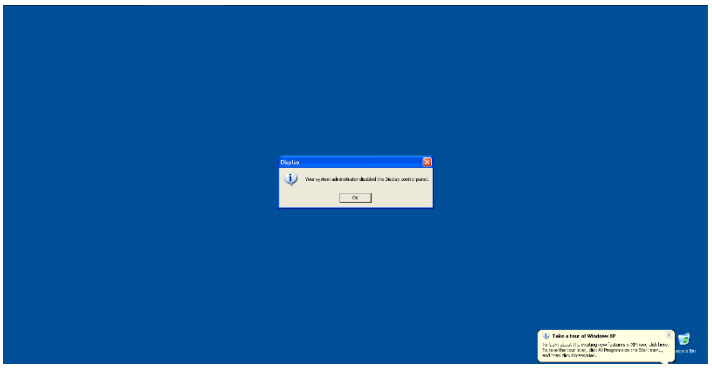


Figure 173GPO Results

Pfsense firewall configuration

A router and firewall software distribution based on the FreeBSD operating system is called pfSense. It has capabilities such as a captive portal for guest access, traffic configuration, and many other security-related features and is intended to be used as a firewall, router, or VPN gateway.

The administrator chooses that firewall for ABCD cooperative society network that because

That firewall flexible and ease of use, making it a popular for small and medium business and also that firewall need very small amount of pc requirement for run that firewall.

Pfsense install process

Pfsense install process may very depend on the hardware platform. First administrator needs to download latest pfsense from the pfsense official website next administrator need create bootable

installation media for run pfsense. During the installing process administrator need go through the installation process once administrator have configured the partition according to ABCD cooperative network it has only one hard drive therefor administrator can select default partition mode for installation process. Once installation process is completed administrator need reboot the system and remove installation media form pfsense hardware. Finally, administrator need connect with pfsense using web browser and administrator need follow startup wizard to set up firewall rules interfaces and other settings.

Example screenshots for pfsense installation.

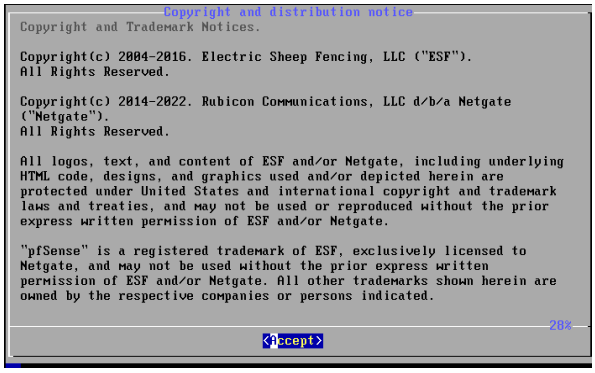


Figure 176:pfsense user agreement

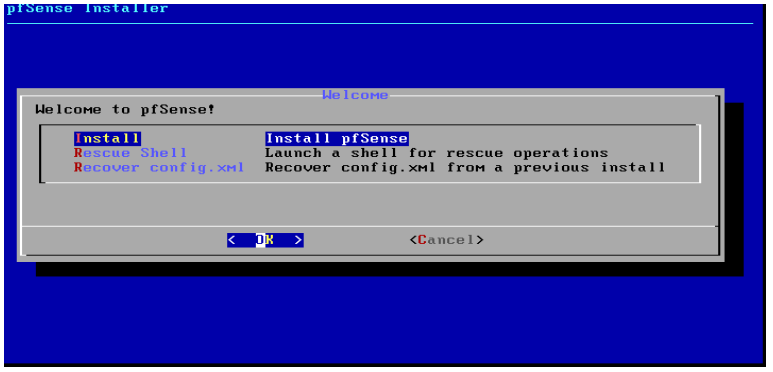


Figure 175:start installation process

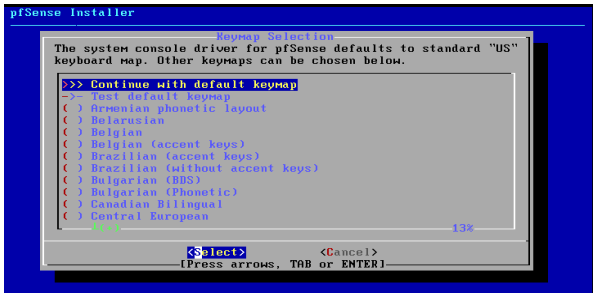


Figure 178:select key map

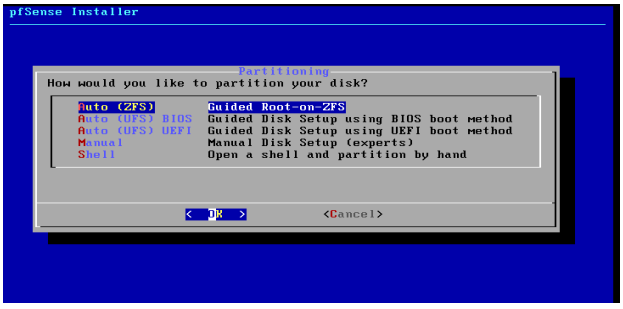


Figure 177:select portions type

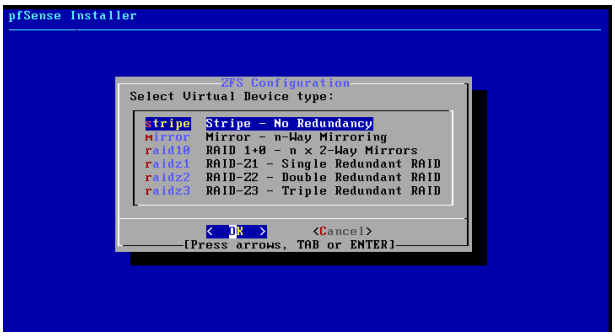


Figure 179:selects ZFS configuration type

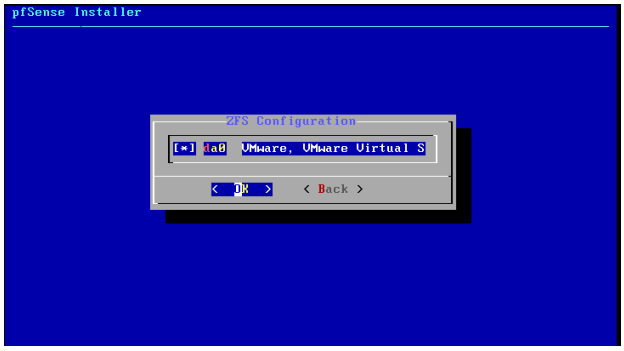


Figure 181:select Hard disk

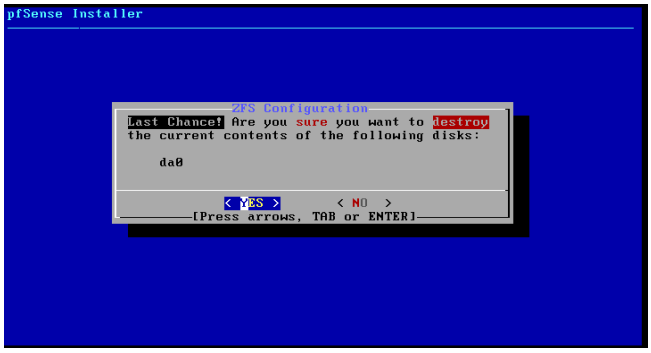


Figure 180:format entire hard disk

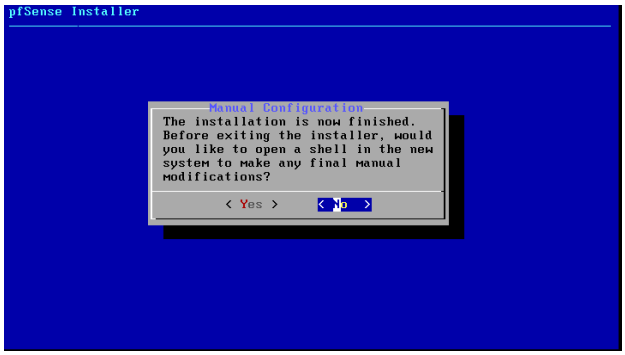


Figure 182;End installation process

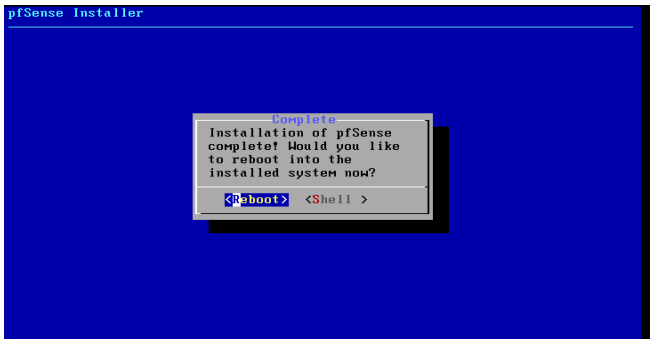


Figure 183:reboot pfsense system

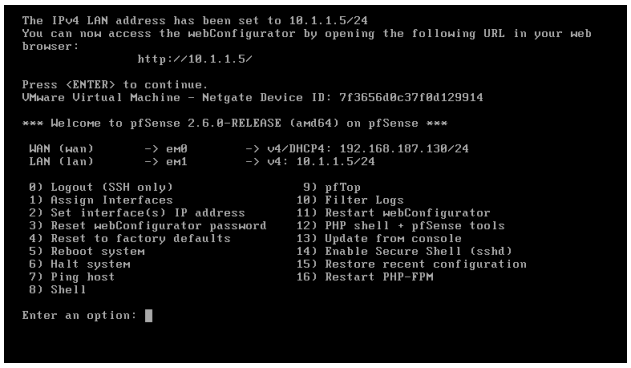


Figure 185:configure pfsense Lan interface

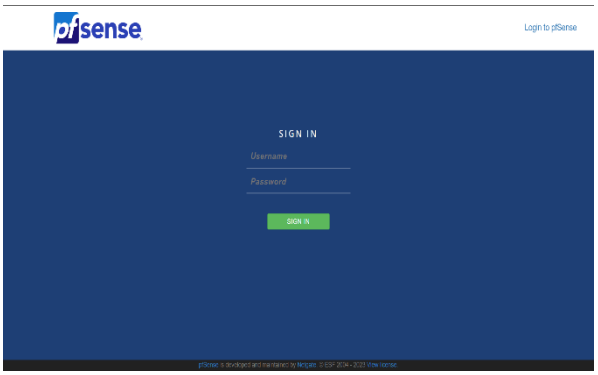


Figure 184:access pfsense web interface

Pfsense basic wizard configuration

According to basic pfsense configuration the administrator need connect admin computer to the pfsense hardware using an Ethernet Cable and open a web browser and administrator need type pfsense LAN ip address. According to the ABCD corporative society the administrator need type 10.1.1.5 ip address for access pfsense web interface. After the access web interface, the administrator need enter default username and password {admin, pfsense}. After enter password and username the administrator will need to enter LAN interface ip address, subnet mask, for LAN interface. Next administrator need enter DNS server Address provide by ISP and local DNS server Ip address. Finally finish wizard configuration administrator need save and reload the system.

Pfsense basic configuration example

Figure 187:Pfsense Login web Interface

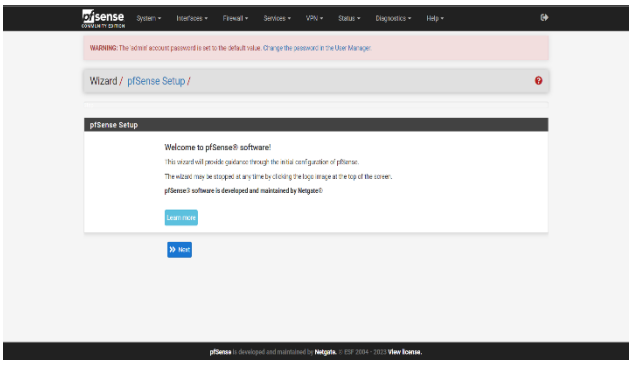


Figure 186:pfsense basic configuration Step 1

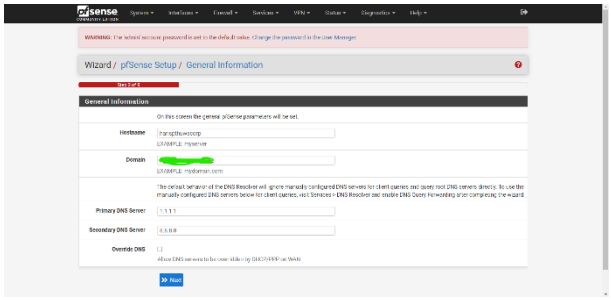


Figure 189:configure pfsense hostname and DNS

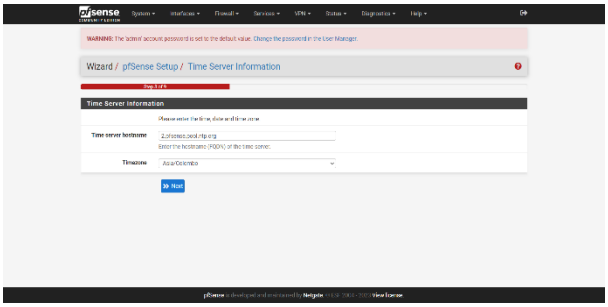


Figure 188:configure pfsense time zone

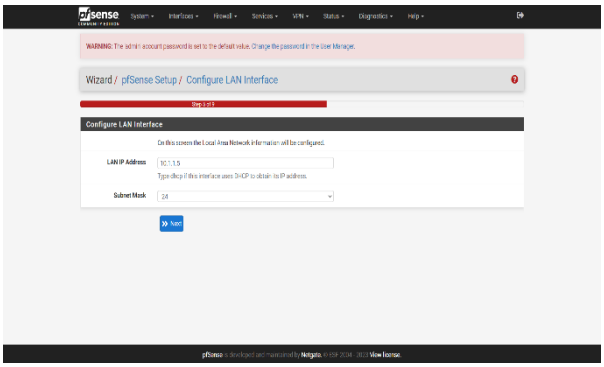


Figure 191:Configure LAN ip address

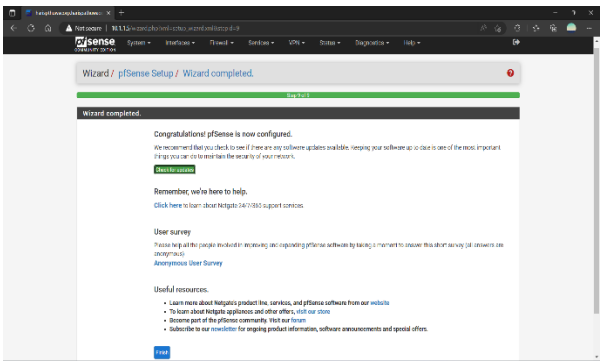


Figure 190:Save and reload pfsense configuration

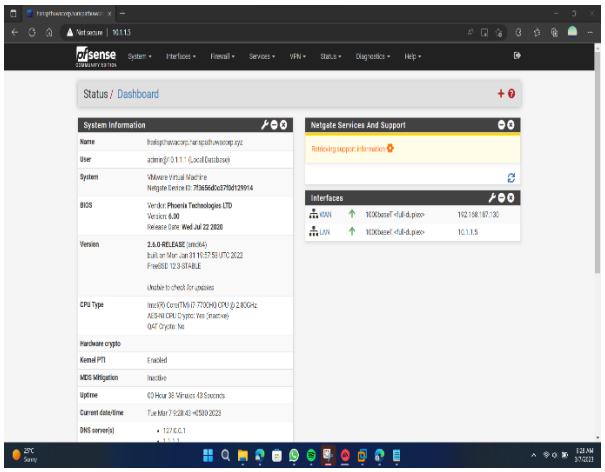


Figure 192:after configure basic wizard

Pfsense add new port number for web interface access

Administrator need use specific port number for access web interface that because administrator need avoiding conflicts with other services by default pfsense use 443 for HTTPS web access but the ABCD corporative society has internal web server therefor administrator need change web configurator port number in that network administrator use 10443 port number for access pfsense web interface. And also, that configuration provide by making it harder for attackers to locate and target the web interface, changing the default port number for accessing the web interface can help increase security. This strategy is called "security through obscurity".

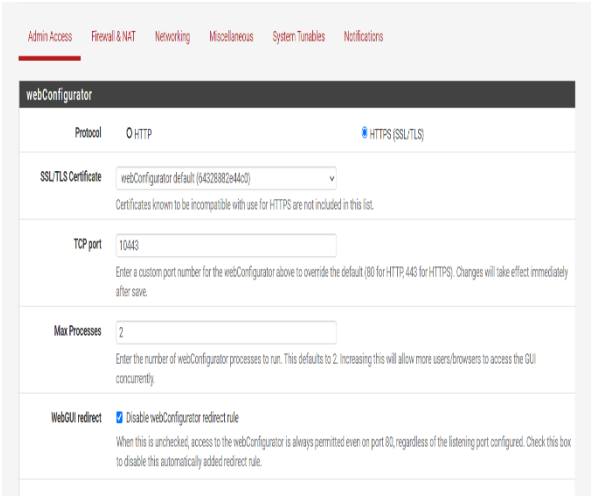


Figure 194:web interface port configuration

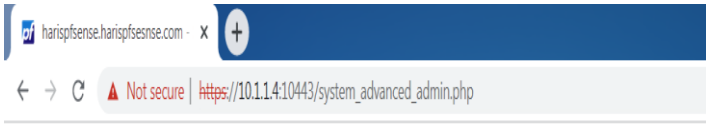


Figure 193:example for web interface port configuration

Captive portal configuration

Captive portal is a feature in pfsense that allows network administrator to provide controlled access to ABCD cooperative society network resource by requiring users to authenticate or agree to a term of service be for being granted access.

Click on the "Enable captive portal" checkbox to enable the feature.

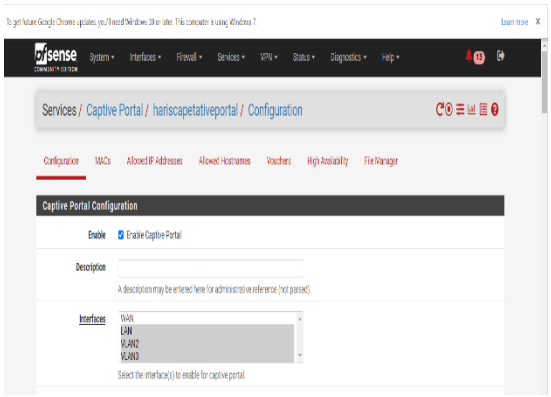


Figure 195:Enable Captative portal in pfsense

Administrator need configure authentication server selecting under the general setting section according to the ABCD cooperative society network the administrator use local authentication database that because the ABCD cooperative society network used less than hundred uses therefore administrator decide no need radius or other authentication system for this network.

Configure local database authentication system example

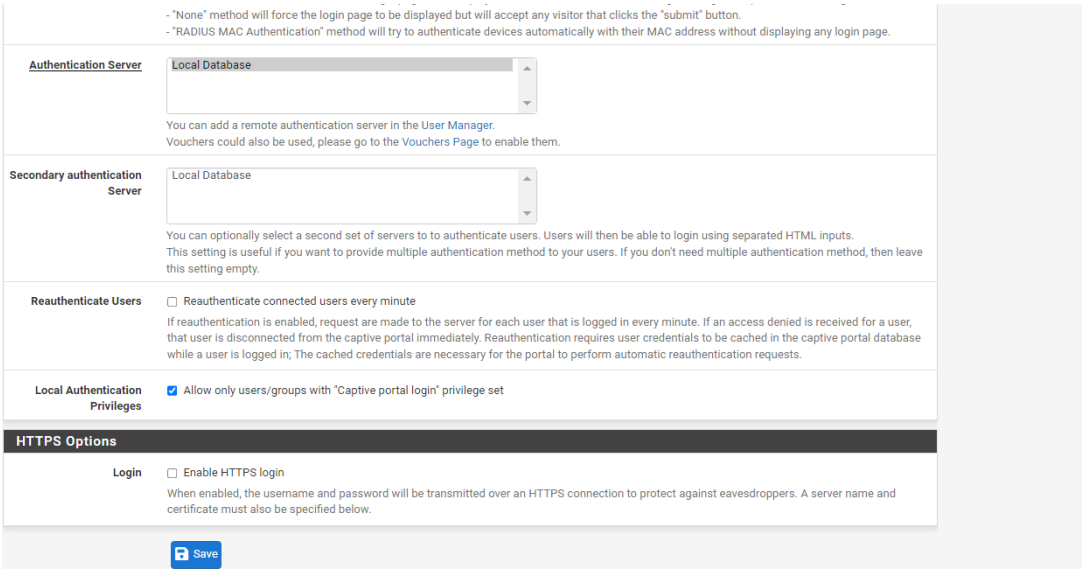


Figure 196:Configure local database authentication system example

Under the **allowed ip addresses** section you can configure a list of IP addresses that will allowed to bypass the Captive Portal authentication process and be granted immediate access to the network.

According to the ABCD cooperative society network the administrator decide windows server ip address to bypass because user need authenticate with windows server active directory service before user access computer devices.

Example for allowed ip address Tab

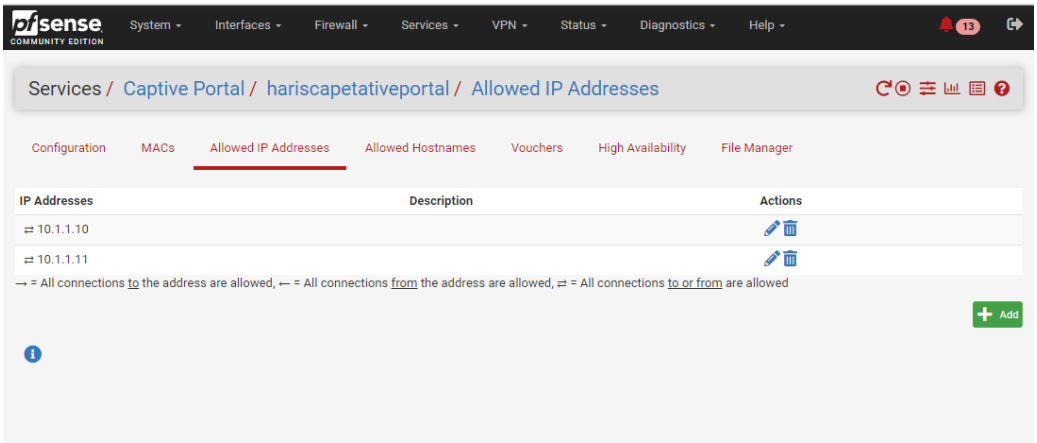


Figure 197:Example for allowed ip address Tab

Finally, administrator can click save button

After configure captive portal user need enter username and password without users cannot access network services such as internet

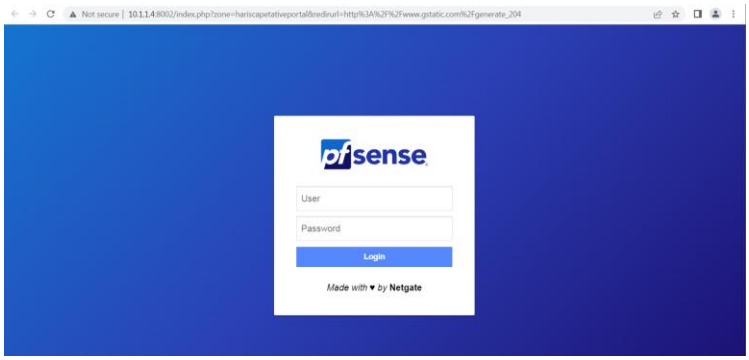


Figure 198:pfsense captive portal login

Create captive portal user account

First administrator need log into pfsense web interface using administrator username and password after log in to pfsense web interface administrator need navigate to system → user manager tab. Now administrator can create new user clicking add button. During the create new user account administrator need specify username and password for user account and also administrator need select **captive portal login** under the **effective privilege** section

Example for create new captive portal user account

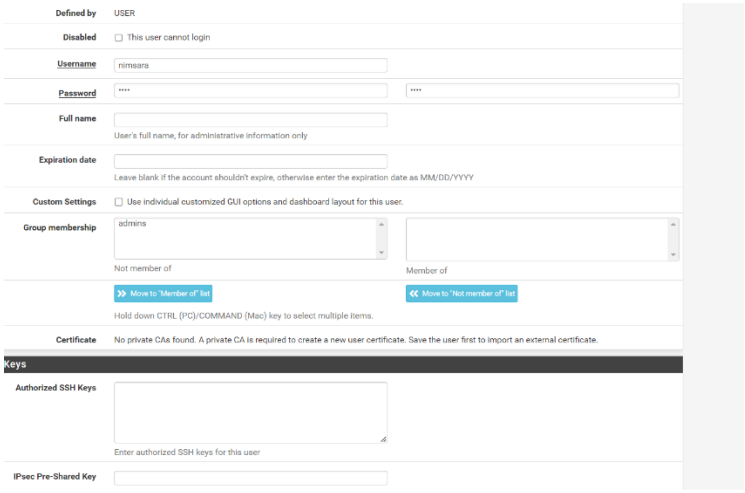


Figure 200:create new user account

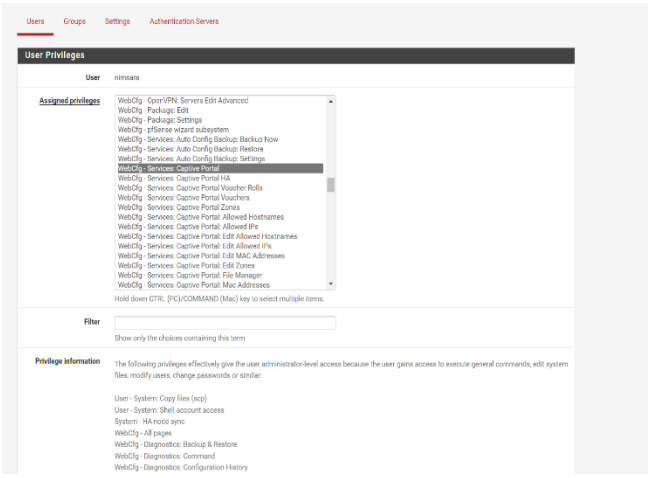


Figure 199:add captive portal permission to user

Ntopng

Ntopng is an open-source network traffic monitoring and analysis tool that provide real time visibility in to network traffic and usage. Ntopng also use troubleshot network issue. Ntopng also capable for monitor and capture traffic form multiple interfaces and that can provide detailed about network and traffic and graphs that helps to identify usage of their network.

Installation steps in Ntopng

administrator need download and install Ntopng package from pfsense web interface. first administrator need go to system>package>search package {Ntopng} and click install button for install package.

Once page is installed administrator need configure ntopng accessing services>ntopng tab then administrator need configure ip address and port number for the ntopng web interface after the enabling ntopng the administrator can access ntopng using it ip address and port number. The administrator will be prompted to log in using the ntopng admin password and username.

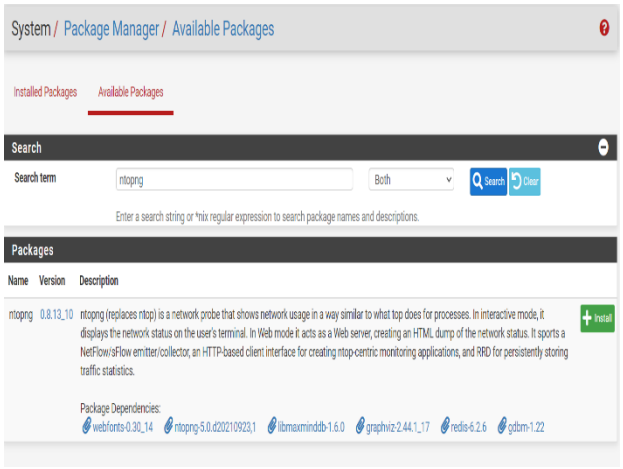


Figure 202:search ntopng package for installing

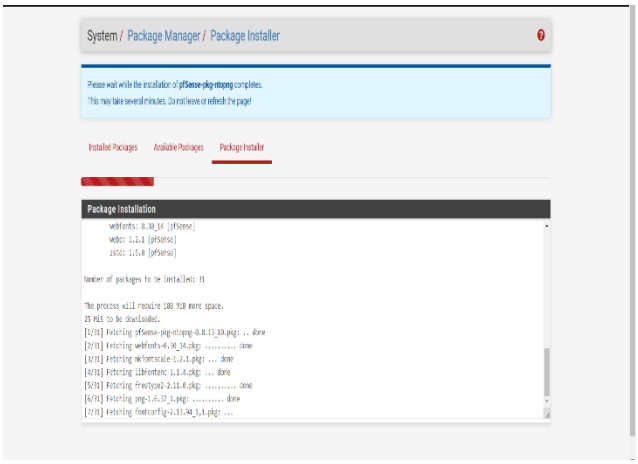


Figure 201:install ntopng package

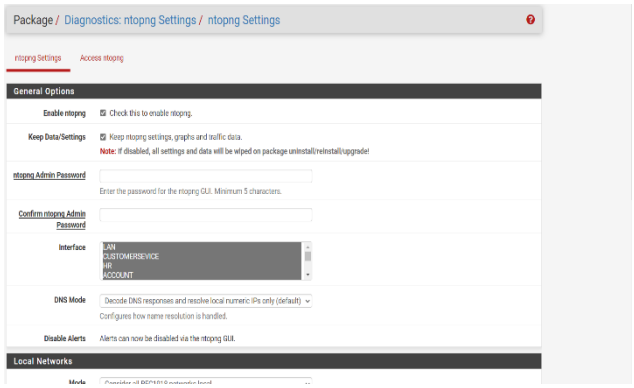


Figure 204:enable ntopng package

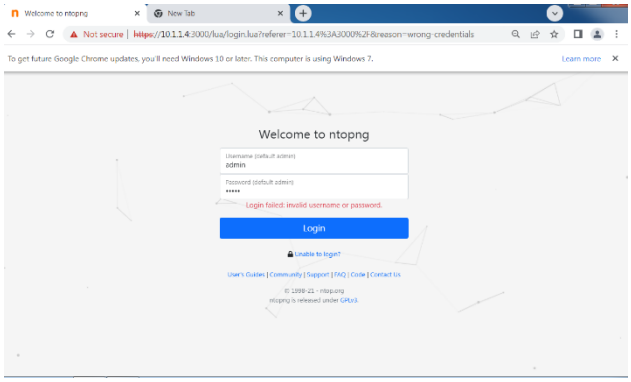


Figure 203:ntopng logging page

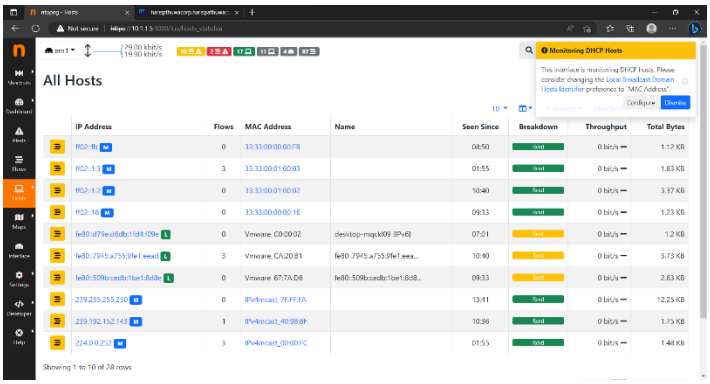


Figure 205:ntopng Monitoring Dashboard

Pfsense VLAN configuration

According to the ABCD cooperative network has VLAN configuration in a network therefor administrator need configure VLAN in pfsense firewall

Example for VLAN Configuration

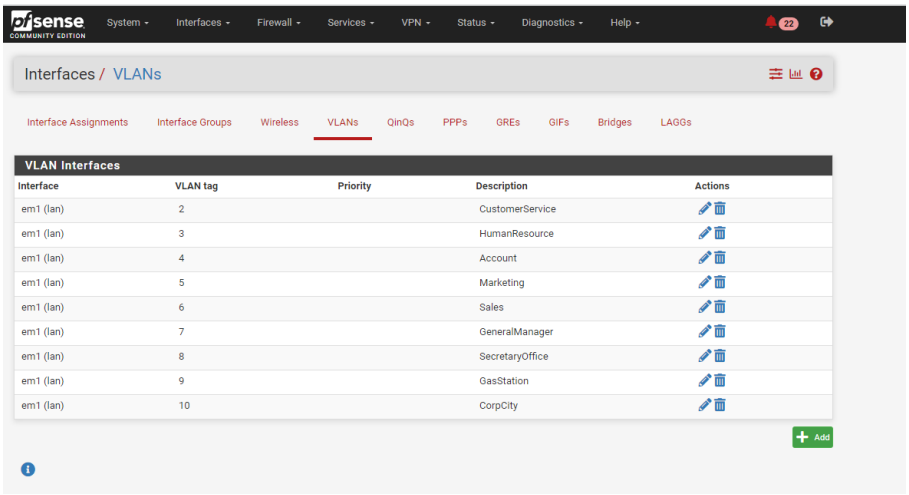


Figure 206:Example for VLAN Configuration

Pfsense DHCP server Configuration

DHCP stand for dynamic host configuration protocol. That is network protocol it enables assign ip address automatically to network devices. Such as laptop, computers, and tablets computers.

According to the ABCD corporative society network administrator need allow DHCP for manage ip address allocation efficiently and reducing the possibility of conflicts between devices that use the same ip address.

The DHCP server on the network responds with an available ip address and other configuration parameters, such as subnet mask, default-gateway and DNS server address according to the ABCD corporative society network DNS server values are one is google DNS server and Other one is Active directory servers. Also, the administrator configures default gateway according to the network VLAN virtual ip address.

Example for DHCP configuration in pfsense firewall

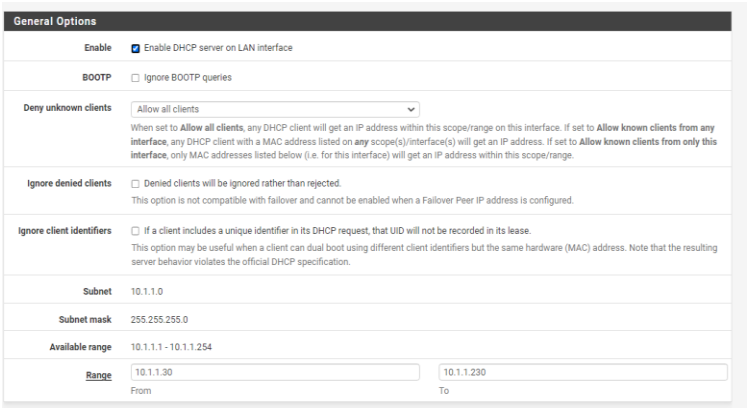


Figure 208:example for DHCP configuration

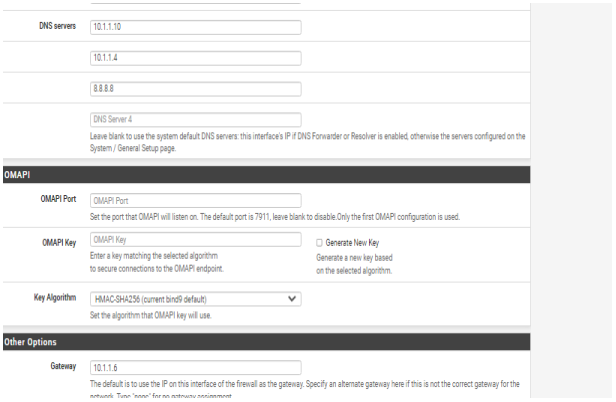


Figure 207:Configure DNS and default gateway

In above pictures administrator configure range of ip address DNS server and ip default gateway

Pfsense high availability configuration

In the event of a hardware failure or network outage, pfSense high availability (HA) capability ensures network redundancy and continuous operation.

According to the ABCD cooperative society network administrator need configure 2 firewalls. When one firewall failed the other firewall need continues operation. Using that kind of machoism, the administrator can improve network availability.

Configuration steps in pfsense high availability

First administrator needs done basic configuration in both firewalls. Next administrator needs CARP (Common address redundancy protocol) used to manage virtual ip address shared by two pfsense devices

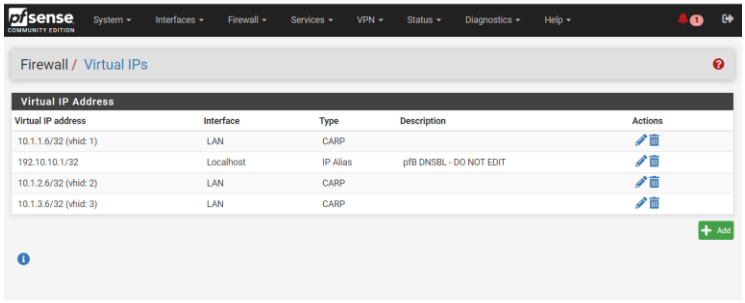


Figure 209:Virtual ip configuration

Next administrator need ensure both pfsense firewall has same configuration before enable synchronization. The administrator can enable synchronization going to system>high availability sync and selecting the synchronization option.

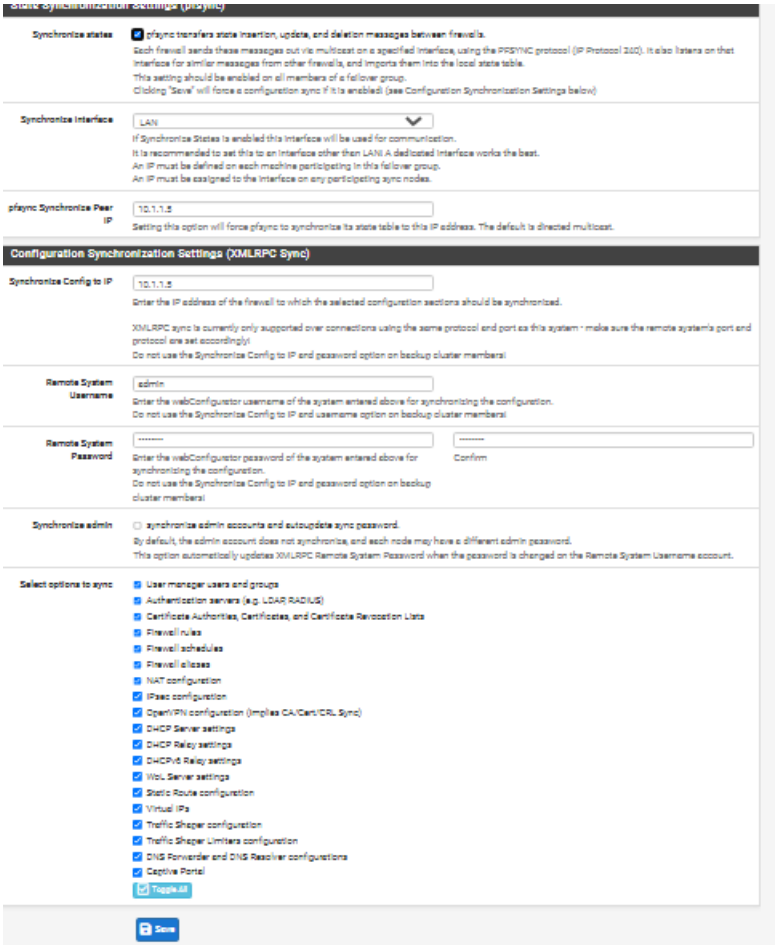


Figure 210;Example for configure high availability

Master and backup firewall configuration example

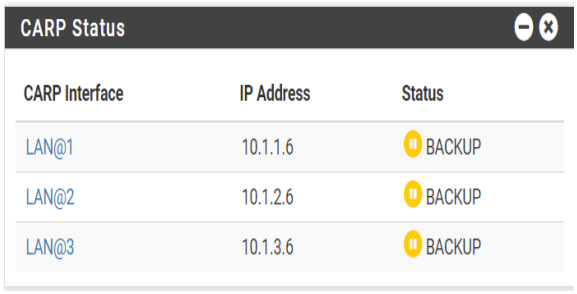


Figure 212:backup firewall

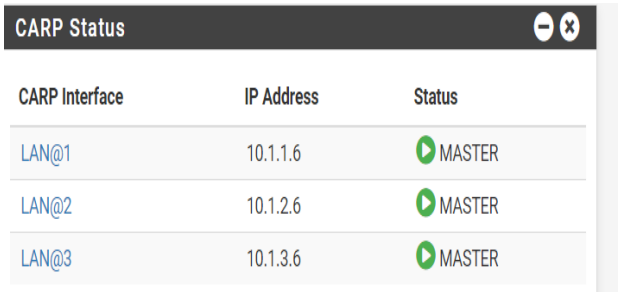


Figure 211:Master firewall

Firewall rules configuration

Firewall rules are a set of policy that provide how traffic allowed or deny on a network. According to ABCD cooperative network the administrator need allow and blocked traffic using pfsense firewall.

First administrator need allow all traffic for a LAN networks after the allowing traffic administrator must need block pfsense web interface and ntopng interface from other VLAN once block traffic from web interfaces administrator need block private ip address ranges that improve security in a network the other most important configuration is block web sites according to the ABCD cooperative society network solution that configuration prevent users from accessing authorized websites. Finally, administrator need configure block ip address list for particular Lan that because the administrator use class full ip range that can be vulnerable to network because administrator need to block that ip address manually creating Aliases.

Configuration example

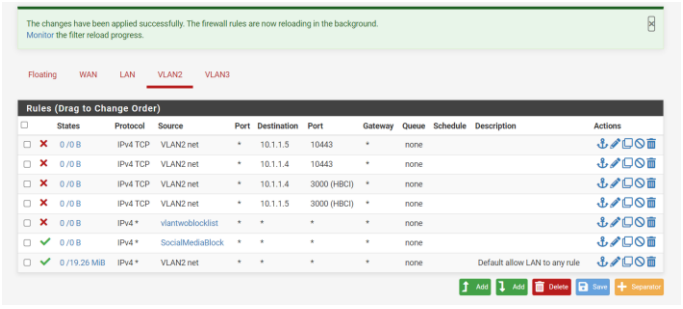


Figure 214:example for firewall rules configuration

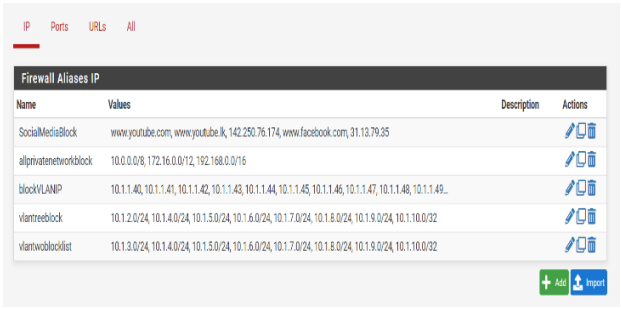


Figure 213;example for Aliases list

IDS Intrusion Detection system and IPS intrusion prevention system

IDS Intrusion Detection System

IDS, or intrusion detection system. It is a type of security technology used to monitor network activity and find potential security risks. And also, Network traffic patterns are analyzed and compared to signatures of malicious activity recognized by the IDS software. There are Security risks such as malware, viruses, worms, network scans, and intrusion attempts can be found with IDS but IDS system cannot prevent system from security risk. IDS only can alert about security threats.

Pfsense IDS Installation and configuration

In pfsense IDS system can be configure using snort IDS package. Snort is a widely used open-source IDS system that system can analyze traffic detect type of security threats including malware, network scans, and intrusions attempts.

Steps of snort install in pfsense

Install the snort packages first administrator need select system tab in navigation bar next administrator need select package manager once select package manager administrator need search snort package in pfsense package manager. Then administrator need install snort package to pfsense system.

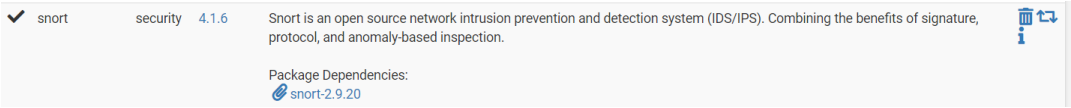


Figure 215:example for snort installation

The snort need configure interface where administrator need enable IDS according to the ABCD cooperative society network administrator need enable snort for all interfaces that because the ABCD cooperative society has more sensitive information in their servers and local computer.

First administrator need enable interface in snort interface configuration.

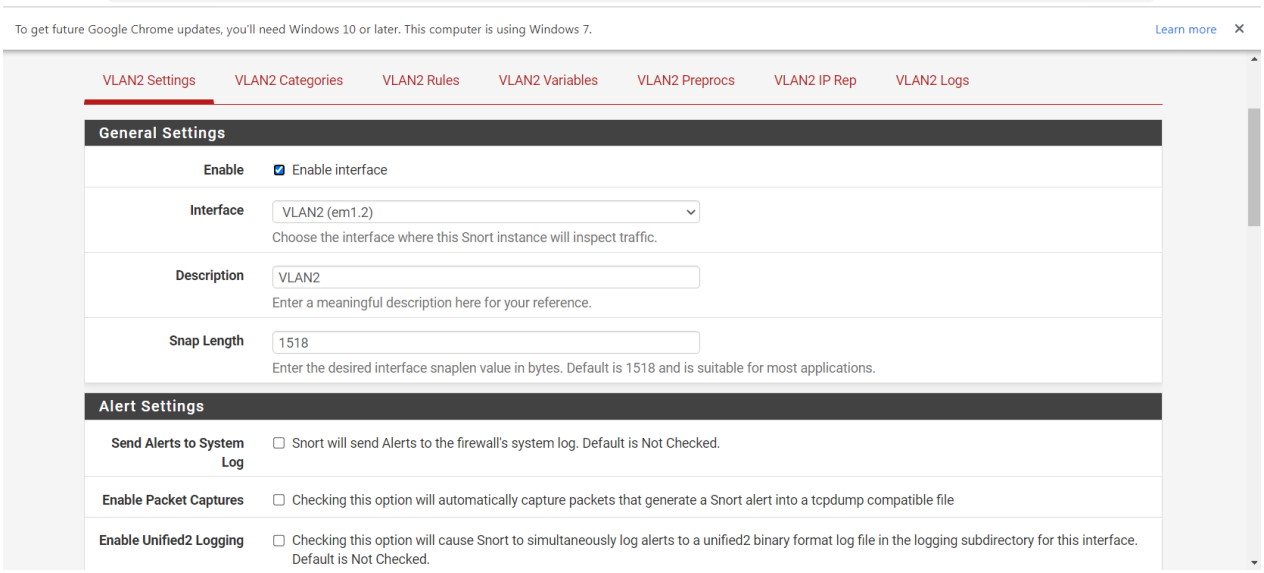


Figure 216:Enable Snort interface

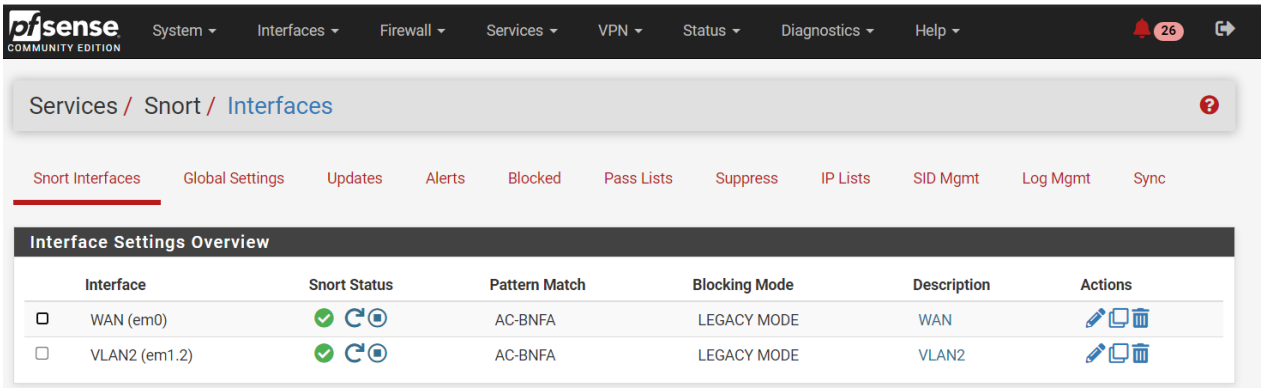


Figure 217:example for snort interface configuration

Next administrator need configure snort rules the administrator can use default rules or download additional rules official web site and administrator need update that rules clicking services>snort>update rules button.

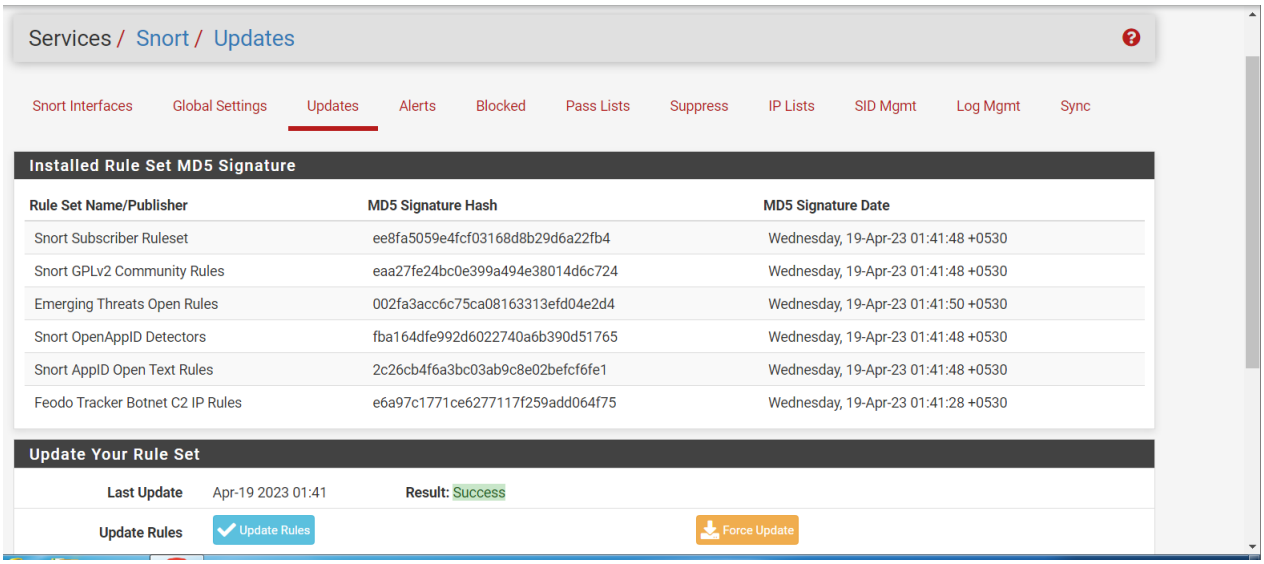


Figure 218:Example for update security rules in snort

Finally, the administrator can enable snort IDS configuring Services>snort and click enable button

According to the that IDS system administrator can enable IPS protection enabling block host configuration in that configuration can automatically block unauthorized computers in local area and WAN network.

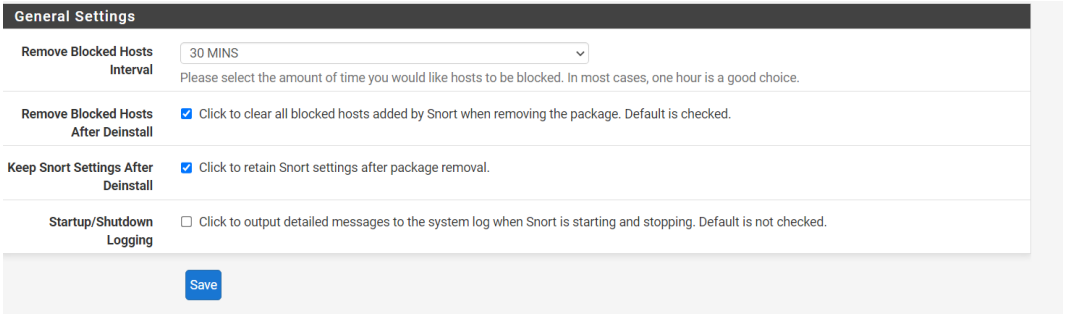


Figure 219:configure IPS setting in snort

Configure PF blocker

PF blocker is a package for pfsense. That provide an easy-to-use interface for configuring and managing IP blocklist. That package provide verity range ip address for block such as tor service ip address, other malicious ip address, DNS Black list, county ip address block and many more features. That package can improve ABCD cooperative society internal network security.

Installation steps in pfblockerNG

First administrator need install pfblocker from package pfsense package manager next administrator need administrator need select block list from Services>pblocker>feeds tab to configures block list. And administrator can change or modify that block list if administrator needed.

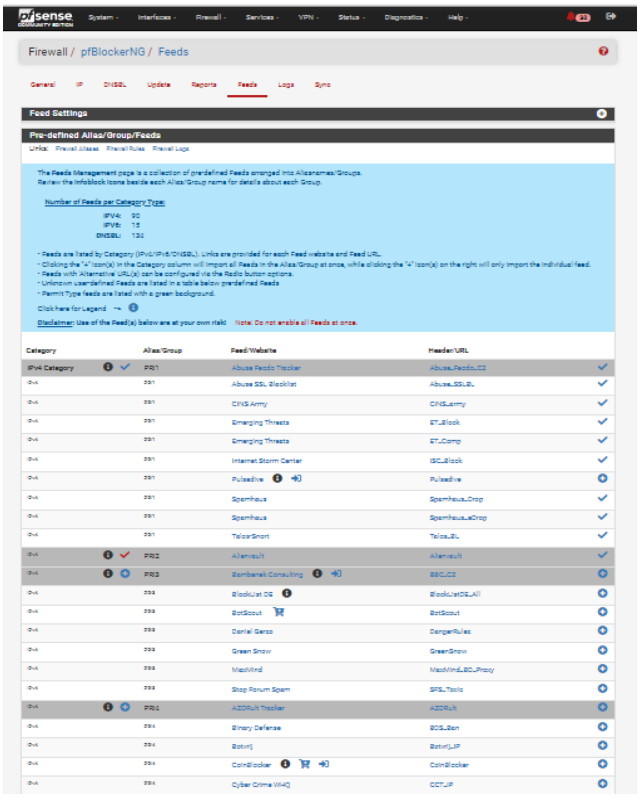


Figure 220:pfblocker feed configuration example

Finally, administrator need save pfblocker configuration

Install Network Monitoring Tool

According to ABCD cooperative society network administrator need monitor some network devices in a single place first administrator decide used SolarWinds network performance tools for monitor ABCD cooperative society network but NPM is very expensive network monitoring tool. Therefor the administrator changes the network monitoring tools for another network monitoring tool. according to ABCD cooperative society network monitoring task the administrator decides choose Zabbix monitoring system for monitor network devices and computers.

Installation steps in Zabbix network monitoring tools

First administrator need visit official web site and download Zabbix. Then administrator install in a Linux base operation system it can be ubuntu or another operating system. Once done the installation step the administrator need setup username and password for Zabbix network monitoring tool. Next administrator need add static ip address for access for Zabbix, after configuring basic step in Zabbix the administrator needs restart the database services and network services for run Zabbix without any issue. Finally, administrator can login in to Zabbix web interface using Zabbix ip address.

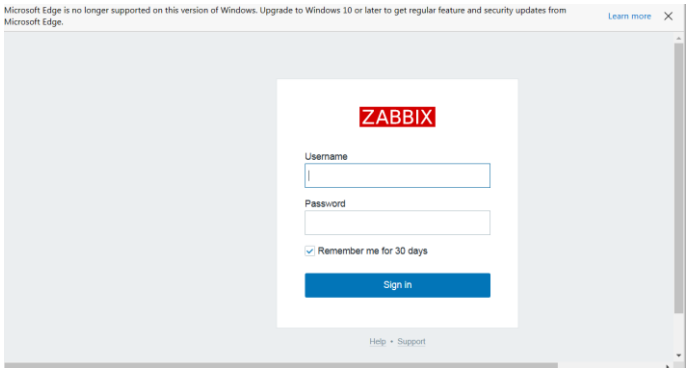


Figure 221:example for Zabbix

Example for Zabbix dash bord

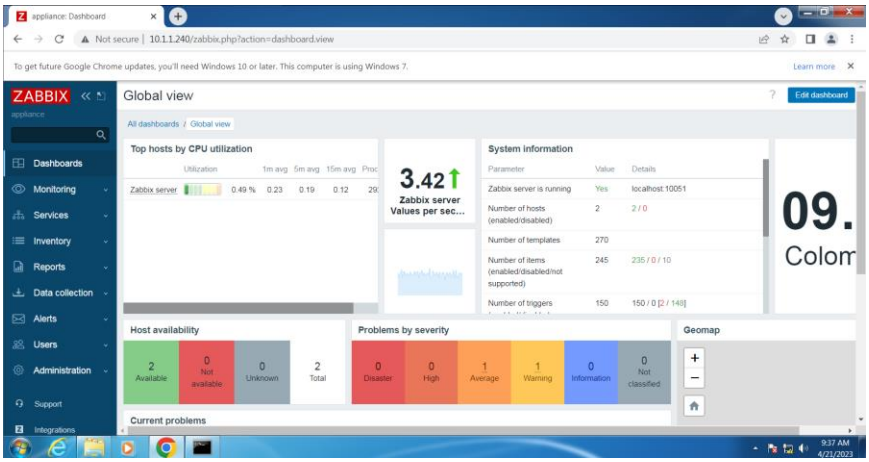


Figure 222:Zabbix dash bord

Install and configure Zabbix argent application on a network device Devices. That application needs small amount of storage from network devices and end devices. That application runs on the

monitored host and sends data to the Zabbix server for processing and analysis. The agent can be used to collect various metrics such as CPU usage, memory usage, network traffic, disk space and more. And also, that agent application support range of operating system such as Linux, windows, and macOS.

Example for agent application install in local computer

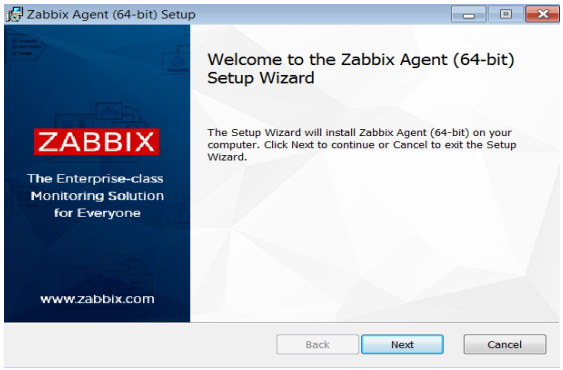


Figure 224:start Zabbix step wizard

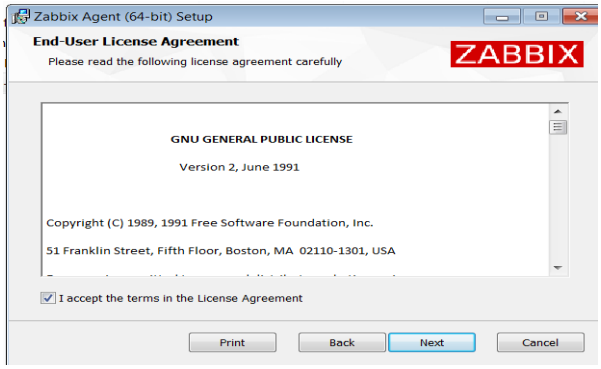


Figure 223:accept Zabbix user agreement

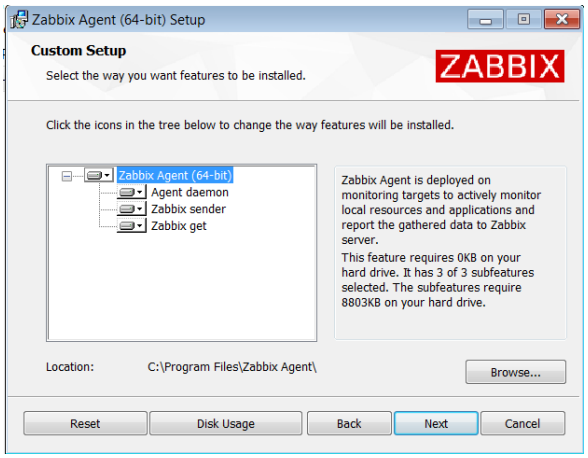


Figure 226:setup installation location and installation packages

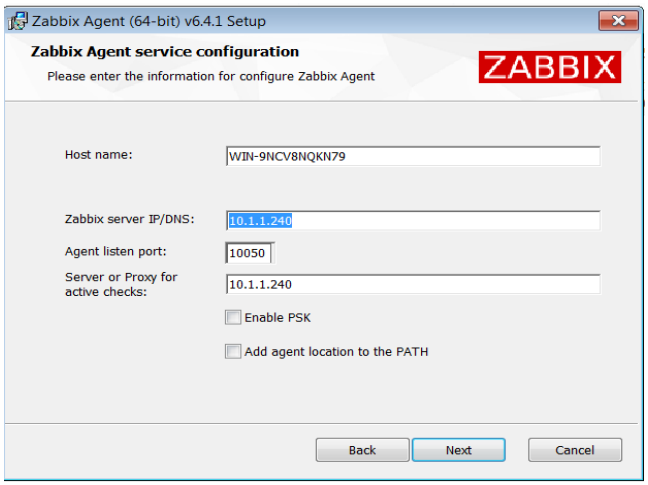


Figure 225:configure device hostname and Zabbix server ip address

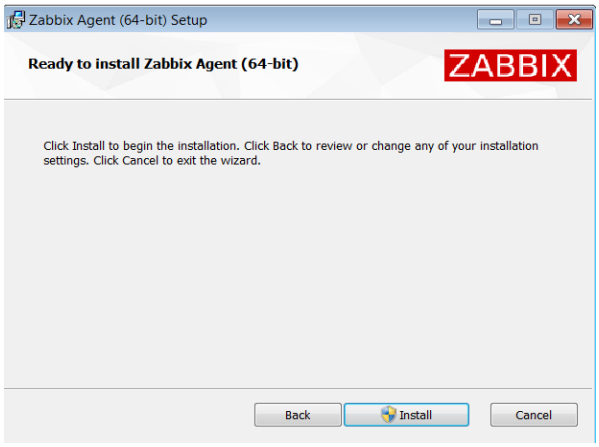
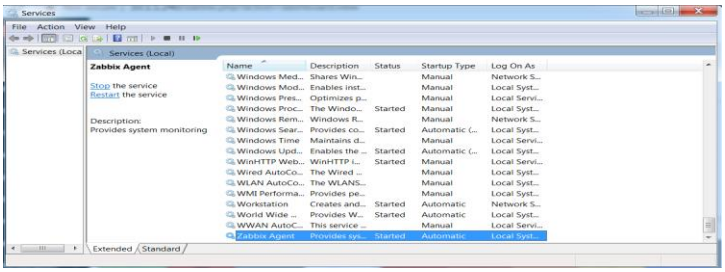


Figure 227:start install Zabbix agent application

Finally, administrator need check Zabbix agent application running or not therefor administrator need go to windows search bar>run>services.msc.



Add Monitoring Devices to Zabbix.

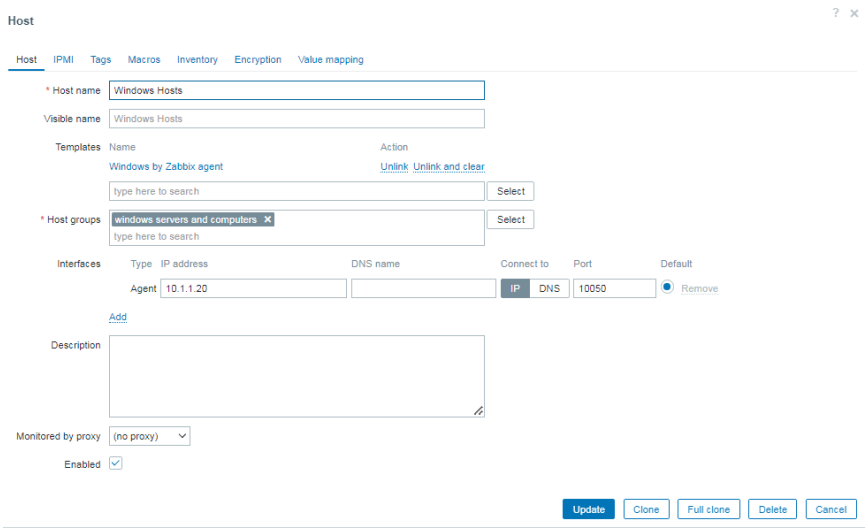


Figure 228: Add Monitoring Devices to Zabbix.

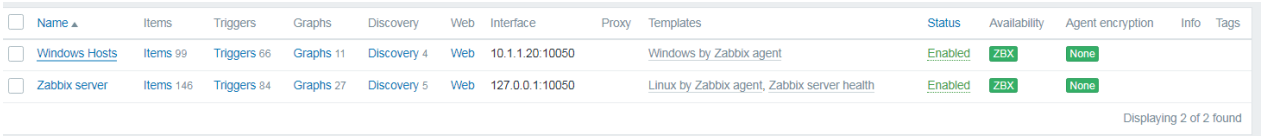


Figure 229:device configuration in Zabbix

Zabbix provide information and status about devices then administrator can troubleshoot manage and provide secure environment for users using Zabbix network monitoring tools.

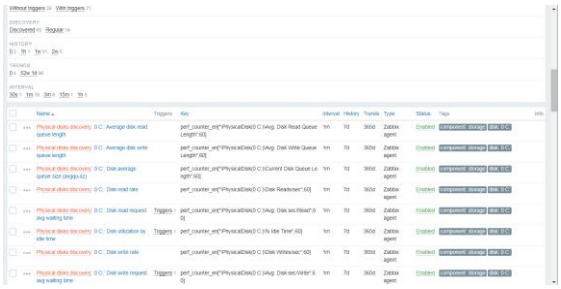


Figure 230: example for manage and monitor network devices

VPN Tunnel

VPN stand for Virtual private network. That allows users to securely connect to internet or private network over a public network and also VPN provide data encryption between user devices and internet or private network.

According to the ABCD cooperative society network administrator need configure remote access VPN for ABCD cooperative society. Remote access VPN allows remote users to securely access private network from outside the ABCD cooperative society employees. the work from home users is commonly used that technology in ABCD cooperative society.

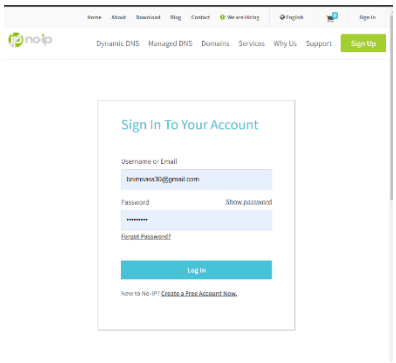
According to the ABCD cooperative society user requirement the administrator decide use open VPN client for configure VPN tunnel between network and employees.

First administrator needs static ip or dynamic DNS for configure VPN tunnel. In that example the administrator uses dynamic DNS for configure VPN tunnel.

“This is a demo VPN configuration one therefor DDNS is enough.”

Dynamic DNS configuration

First administrator need check free DDNS provide services in that example the administrator uses No-ip DDNS for configure that DDNS service. First administrator need login in to service and create new Domain name. then administrator can configure DDNS in pfsense. According to the pfsense configuration administrator need connect that DDNS service to pfsense.



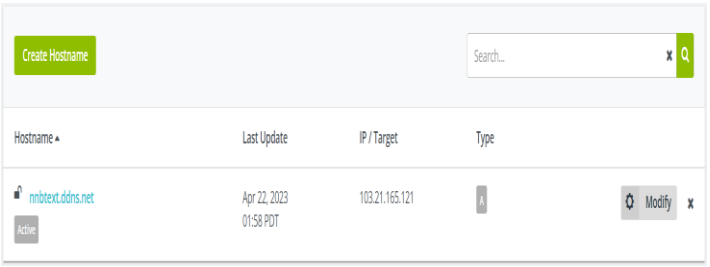
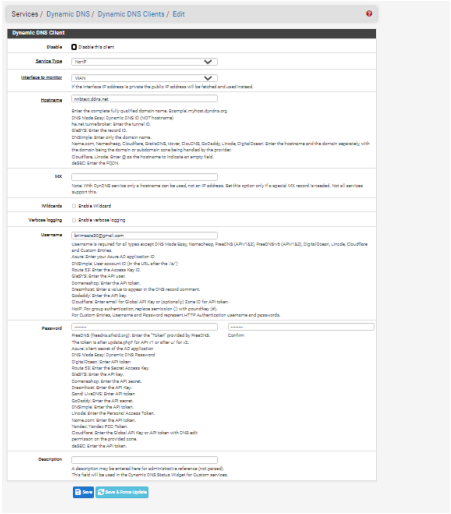


Figure 232:connetc c Domain or host name to my public ip address



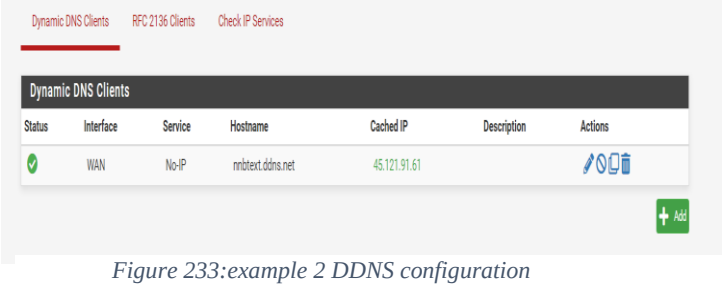


Figure 233:example 2 DDNS configuration

Figure 234:Example for DDNS configuration

Next administrator need create configure OPEN VPN wizard in that wizard administrator need configure what network or network devices are allows to the access users and that phase administrator need configure basic and advance configuration in VPN such as Description Of VPN, server mode, device mode, protocols, backend authentication, encryption method and etc.

According to the ABCD cooperative society network the administrator select local authentication database for authenticate VPN user also administrator use TCP IPV4 and IPV6 on all interface protocol that provide TCP configuration for VPN service. And the administrator provides TLS configuration for VPN that provide enhance security of an open VPN connection by requiring both parties to have a common key before pear can perform TLS handshake. And also, administrator need enable data encryption algorithm for secure data.

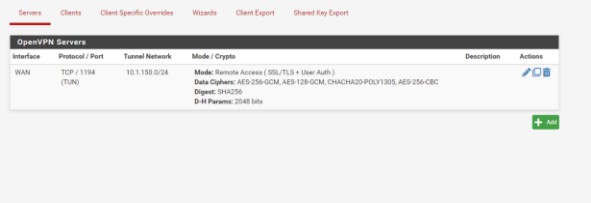


Figure 235:configuration example for open VPN

File Storage Server

Truenas is an open-source network storage operating system that allows administrators to store and manage data on a networked storage system. Truenas has many features such as data synchronization, remote access, snapshot and backup functionality. That also support multiple file sharing protocol.

Truenas has free and commercial versions. According to ABCD cooperative society network the administrator decide choose free version that because the free version has important function server such as malware protection. That free version functionalities are enough to ABCD cooperative society network users to continue their day-to-day works.

Configure Truenas server steps

First administrator needs download Truenas iso image file then administrator need install that Truenas server in a NAS device that can be computer or any other related devices for NAS server. After installing Truenas the administrator can access share and manage Truenas server using username and password which configured by administrator. In that example administrator use root for username and 1111 for password.

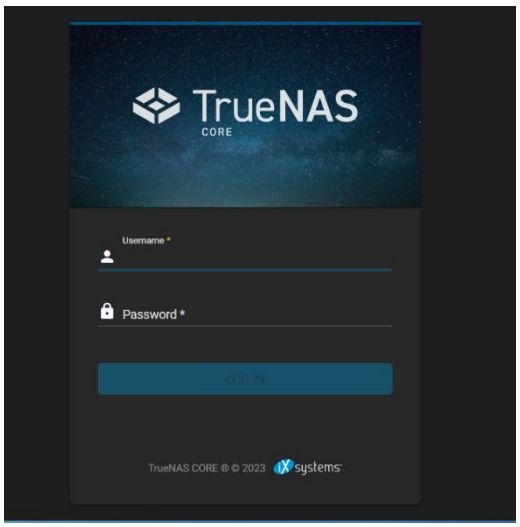


Figure 237:Truenas user logging page

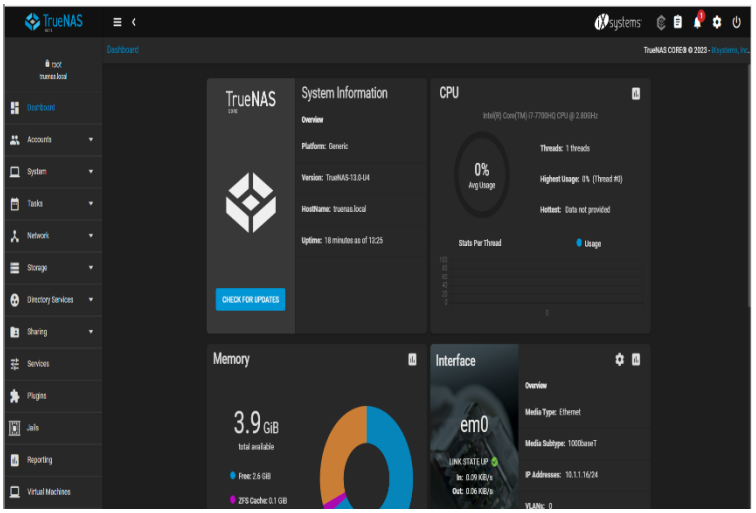


Figure 236:Truenas dashboard

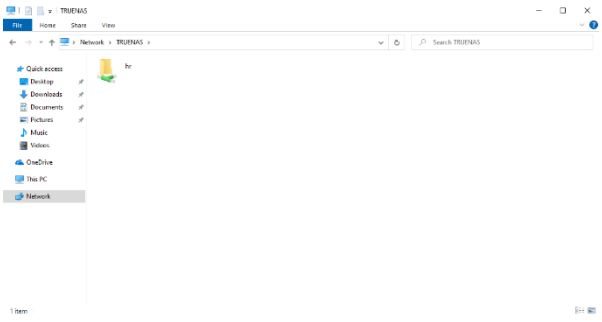


Figure 239:access file server using username and password

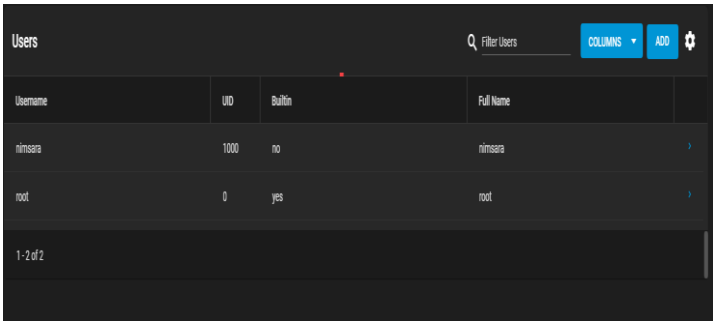


Figure 238:add users to Truenas server

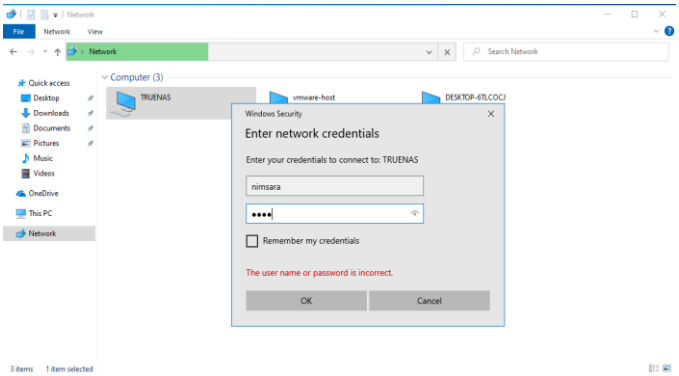


Figure 240:enter username and password for access file server

Network automation configuration

Automate network using python

The administrator can automate ABCD cooperative society network that provide easy management, fast configuration process, and monitoring. The network automation involves using programming or scripting language to write code that can perform task. According to the ABCD cooperative society network the administrator use python programming language for automate some function on that network.

The goal of network automation is to increase network efficiency, reduce error, and save it professionals' time.

Example for network automation according to ABCD cooperative society

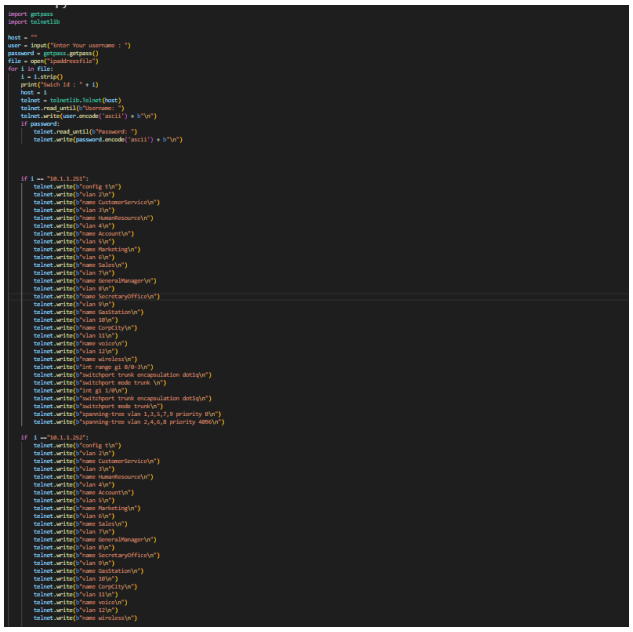


Figure 242:example source code 1

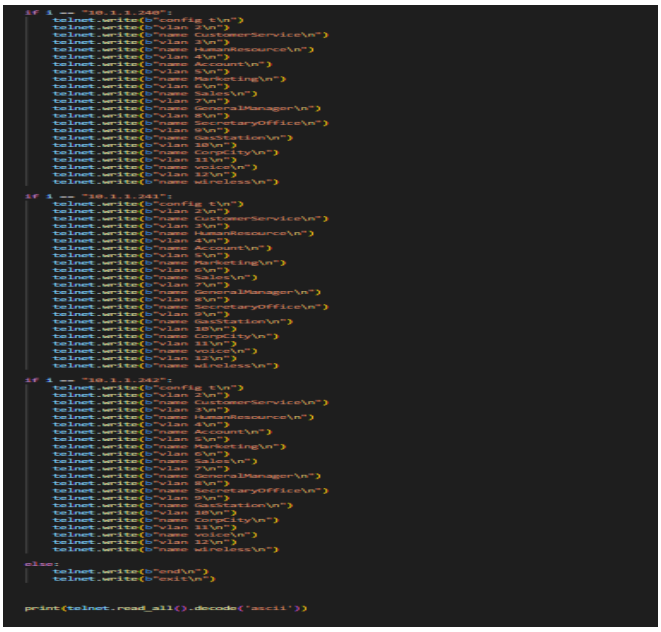


Figure 241:example source code 2

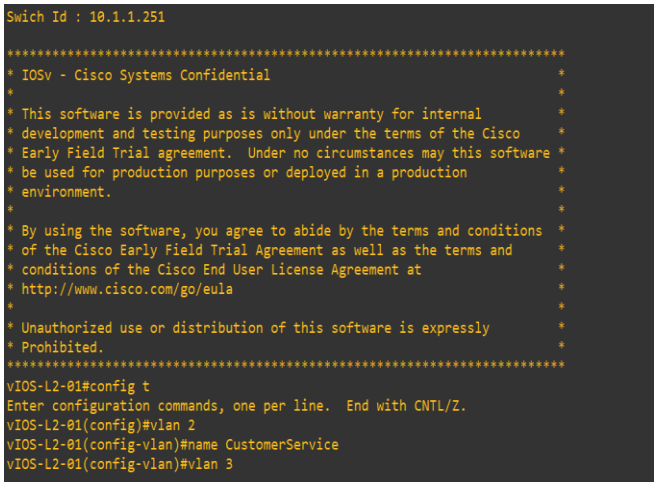


Figure 243:example for running python code

According to the bellow figures the administrator use getpass and telnetlib library for implement network automation python code

Getpass library support get password from switches local database and telnetlib support connecting switches using telent if administrator can use netmiko library that allows connect with devices using SSH

Chapter 6 Evaluation

You must include test plan and test cases for this task.

Introductory paragraph

Network Testing

The network testing, I the process of assessing the functionality, evaluating performance and reliability or dependability of computer network. Network testing include various testing method of the network, hardware, software, protocol and network services to ensure the specific requirement and performance as expected.

The main task of network testing is identified and fix any potential issues or problem that may existing in the network. Also, network testing provide ability to testing deferent type of traffic such as data, voice and video as well as its security and scalability.

Techniques of network Testing

There is various method for network testing such as [22].

- Manual testing
- Automated testing
- Blackbox testing
- Whitebox testing

Manual testing is a traditional network testing method. In that testing method humans are manually verify the network performance, functionality, and security. That technique used various tests such as ping test, traceroute, port scans.

Automated testing more efficient method of network testing that uses software tools automated the testing process.

Black box testing: This is a testing method where the tester is not aware of the inner workings of the network. Without considering the internal structure of the network, the tester evaluates the performance of the network based on its inputs and outputs.

White box testing: This is a testing method where the tester is fully aware of how the network works internally. Based on the internal structure of the network, the tester evaluates the performance of the network.

Types of networking Testing

there are deferent type of network testing each network testing method support to ensure network security, performance and reliability in a network. There has some comment network testing such as.

- Performance testing
- Functional testing
- Security testing
- Compatibility testing
- Load testing

Performance testing test ability to handle a specific workload in a network under the deferent condition. Such as network latency and resource limitation.

Functional testing focus on testing the network functionality in that testing method administrator can include ability to send and receive data, support specific protocols, and handle deferent type of traffic.

Security testing method used for identify the security vulnerability and security loopholes in the network that provide security from unauthorized access, detect intrusions, and protect sensitive data.

Compatibility testing focus on identify network compatibility with various network hardware, software and devices. That compatible testing ensures that network compatible with new devices and new technologies without effecting its performance.

Load testing check how much network load can handle that testing type includes high traffic load bottlenecks, capacity limitation and performance issue.

Test Plan and Test Cases

Test Plan

The network test plan ensures basic network setup including the installation and configuration cisco switches, client devices, firewall, monitoring tools, IDS, files server and other devices and network mechanisms. To goal of that text plan is ensure that the network properly work and meet client requirement without any issue.

Test objective in ABCD cooperative society network

- verify cisco switches are properly installed and configured
- verify pfsense firewall properly installed and configured
- verify snort properly installed and configured
- verify windows server properly installed and configured
- verify Truenas file server properly installed and configured
- verify that client devices can connect to network and access internet
- verify that network is secure and protected against unauthorized access
- verify the network has reliable connection with network
- verify that network can handle workload
- verify that network can performed day-to-day works without any issue

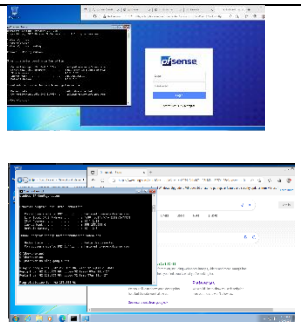
Test environment

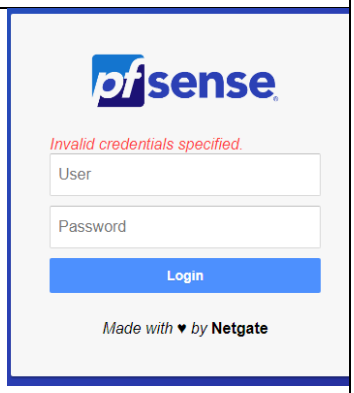
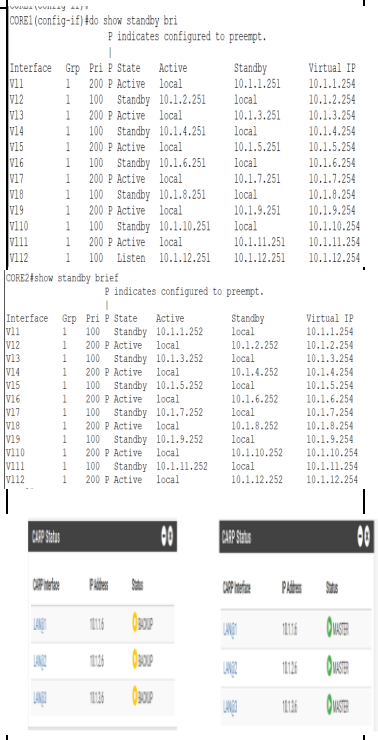
- Cisco catalyst 3650-24-layer switches
- Pfsense firewall
- Client Devices
- Ethernet ports and cable
- Internet connectivity
- Network reliability
- Network performance
- Network security

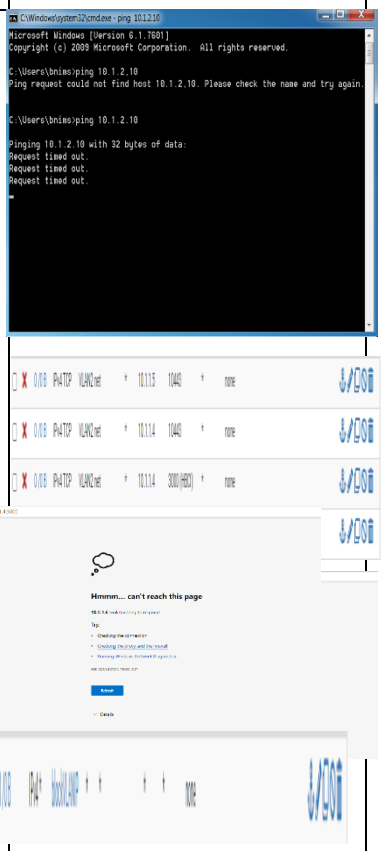
Text procedures

- Install and configure cisco switches according to the ABCD cooperative society network.
- Connect client devices to network.
- Configure firewall according to the user/client requirement.
- Configure windows server according to the user/client requirement.
- Configure Truenas file server according to the user/client requirement.
- Text network reliability
- Text network security by attempting to access network from an unauthorized device.
- Verify network connectivity using QOS (quality of service) that can handle voice and data traffic without degradation.

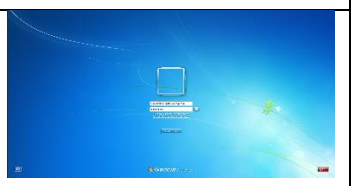
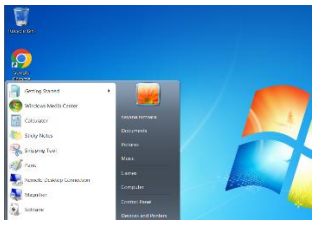
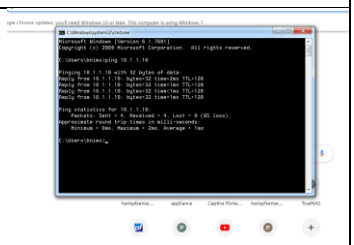
Network test Cases

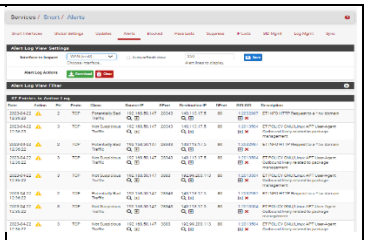
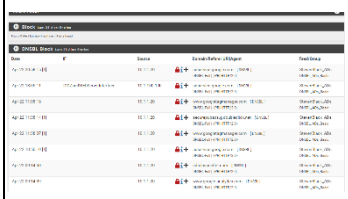
Test ID	Text object	Test steps/description	Text steps	Text result	Screenshot
HT001	Network connectivity text To verify the client devices can access internet	1Cisco switches and firewall properly configured. 2Client devices are connected to switches using ethernet cable. 3The client devices obtain an ip address	Check client devices obtain an ip address using DHCP. Check the client can access web site.	Success	

		using DHCP server			
HT002	Verify internet security users cannot access network resources without login	1The administrator need configure captive portal and authenticates users	Check captive portal using wrong user name and password	Success	
HT003	Configuration failover technologies for core layer switches, firewall and windows server	1Cisco switches are used HSRP (Hot standby protocol) for one switch failed other switch can manage network resources without any down time in a network. 2 firewalls use high availability protocols for archive	Check redundancy protocols working properly.	Success	

		redundancy in a network 3 the windows server has backup server for archive that redundancy protocol that server is manage FSMO rules			
HT004	Text firewall rules are working or not	According to the network first administrator block firewall interface from other VLAN the web interface only allows LAN one administrators. 2 this rule only allow ntopng interface for LAN users. Other users cannot access	Check Firewall rules are working properly trying to ping in other VLAN ip address	All access lists are working properly Other VLAN can't pfsense and ntopng web interface	

		ntopng interface from their LAN 3 that rule allow ip address block according to network the administrator use class full ip address for every VLAN that because the lot of ip address are blocked that can be security vulnerability for network therefor the network administrator only allow used ip address for each VLAN other VLAN Ip address now allow to use in network.			

		4 Next rules contain block pinging local ip address that allow to security feature for network.			
HT005	Check user can login using windows server active directory credential				 
HT005	Check active directory server is active or not	According to the network the administrator configures active directory server for manage internal network user account	Ping windows server and text windows server active or not		

HT 004	Check snort is working properly	Snort is an open-source IDS system that allow to improve network security from hackers that contain black list and white list. That also allowed automatically blocked hackers source ip address and prevent attacks from outside network.	Check logs in snort	Success	
HT006	Text pfblocker rules are working properly	Pfblocker contain pre define set of firewall rules that helps to administrator increase interval network security using rules and lists	Check pfblocker log pfblocker rules are working or not	In the log message area show log messages about block network such as advertisement web site, and tor services	

User Feedback

The administrator gets user feedback from ABCD cooperative society network users. According to user feedback the administrator collect feedback from 11 users according to the feedback for most users are provide positive feedback about network.

The first question is user are satisfied or no network performance

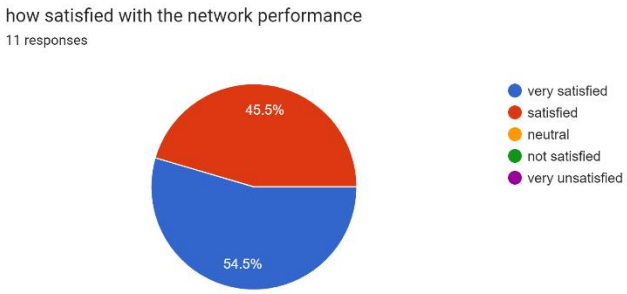


Figure 244:feedback question 1

According to the above image the 6 (54.5%) users are satisfied network performance no any unsatisfied users therefore that network performed very well.

The next questions about network outages connectivity issue.

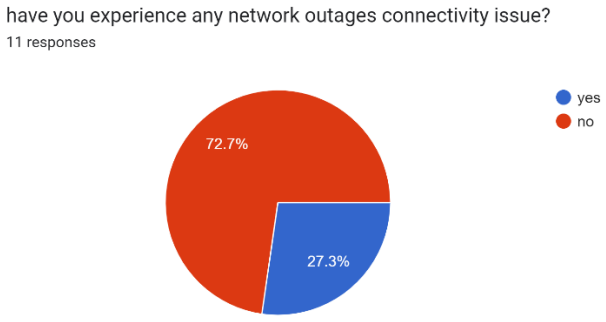


Figure 245:feedback question 2

According to above image 72.7% users are given feedback no any network outages connectivity issue.

The next question how about network speed the 50% users are says network speed is fast.

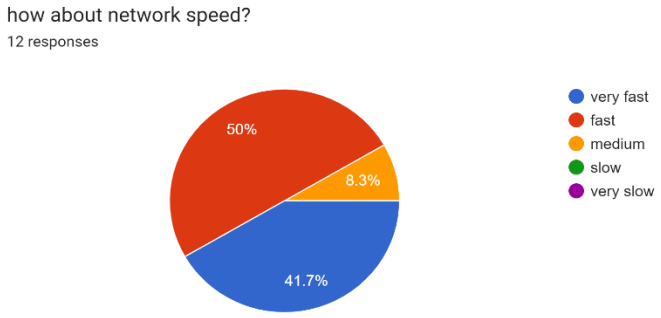


Figure 246:question 3

The fourth question ask about captative portal the 50% users say it's easy to use and 41% user are saying it's very easy to use. Furthermore 8.3% users say it's not easy to use.

The next question asks about network resources and application.

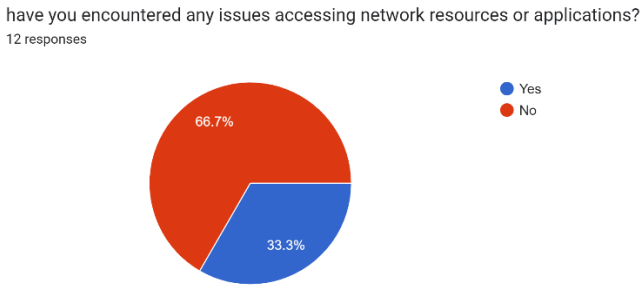
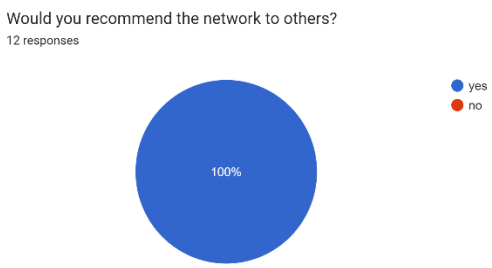


Figure 247:question 5

According to the question 5 image the most users are using network resources without any errors or issues 66.7% users say no any issue in network resources 33.3 users say they have some issue using network resource.

Next question the administrator ask about the network is recommended to another user. According bellow chart the all users say yes.



The final question is what is the experience with network

Chapter 7 Conclusion

You must include CONCLUSION from your project. (Summaries the project and your solution in one or two paragraphs.

Conclusion

ABCD Co-operative Society Limited is trying to secure their internal network as well as external network for doing their day-to-day work easily and securely.

Critical evaluation

The administrator wishes use dual wan dual ISP routers for configure that network. that routers will provide redundancy for network.

Limitation

The Administrator developed that project using simulation tools and virtualization tools such as GNS3, cisco packet tracer, VMWARE workstation. This software has shortcoming therefor some function not work properly.

Future work

In order to further work administrator, enhance the security features using application and, next gen Firewall that support to this network in the future as it provides full overall network protection.
Using fiber optics cable to further speed up this network and Convert computers computer network

adapters into gigabit network cards to increase the efficiency of the computer, administrator use dual ISP wan interface routers for increase ISP service and balance internet speed.

Lesson learnt.

Finally, I learned a lot doing this project such as basic computer network, how to improve network security, how build repairable network, authentication methods, security methods used in network, how build a VPN connectivity between branches or users, why we need VPN connectivity etc.

References

Bibliography

[1] T. Lammle, "CCNA," in *CCNA complete study guide*, John Wiley & Sons,, 2016, p. 899.

[2] V. Rajaravivarma, "Virtual local area network technology and applications," in *Virtual local area network technology and applications*, Cookeville, IEEE.

[3] v. boricha, "Windows server configuration," in *mastering windows server 2019*, birminham, packt publishing ltd, 2019, p. 498.

[4] M. lyu and L. lau, "Firewall security: policies, testing and performance evaluation," in *Firewall security: policies, testing and performance evaluation*, Taipei, LEEE, 2007.

[5] B. hale, network managment back to the bacis, Solarwinds.

[6] M. A. Hossain, M. N. A. Sheikh, H. Monishanker , S. Biswas and M. . A. I. Arman, Quality of Service in Software DefinedNetworking, Global Journals, 2018.

[7] T. Li, B. Cole, P. Morton and D. Li, " Cisco Hot Standby Router Protocol (HSRP)," Cisco, [Online]. Available: https://www.rfc-editor.org/rfc/rfc2281.html. [Accessed 10 04 2023].

[8] "Documentation for Kiwi syslog server," solawinds, [Online]. Available: https://documentation.solarwinds.com/en/success_center/kss/content/kss_gsg_overview.htm. [Accessed 10 04 2023].

[9] "TrueNAS: Open Storage," ixsystems, [Online]. Available: https://www.truenas.com/docs/. [Accessed 10 04 2023].

[10] P. SenthilKumar and M. Muthukumar, "A Study on Firewall System, Scheduling and Routing using pfsense Scheme," netgate, 15 12 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8997167/authors#authors. [Accessed 10 04 2022].

[11] W. Stackpole, "Centralized Authentication Services (RADIUS, TACACS, DIAMETER)," 2003. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/noe0849385858-15/centralized-authentication-services-radius-tacacs-diameter-william-stackpole-cissp. [Accessed 10 04 2023].

[12] L. F. Aryeh, M Asante and A. E. Y. Danso, "Securing Wireless Network Using pfSense Captive Portal with Radius Authentication – A Case Study at UMaT," GHANA JOURNAL OF TECHNOLOGY, 2016. [Online]. Available: http://www2.umat.edu.gh/gjt/index.php/gjt/article/view/21. [Accessed 10 04 2023].

[13] L. Deri, M. Martinelli and A. Cardigliano, "Realtime High-Speed Network Traffic Monitoring," 9–14, November 2014. [Online]. Available: https://www.usenix.org/system/files/conference/lisa14/lisa14-paper-deri.pdf. [Accessed 10 04 2023].

[14] T. R. Yarlagadda, "Python Engineering Automation to Advance Artificial Intelligence and Machine Learning Systems," INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY , 12 03 2021. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3797347. [Accessed 10 04 2023].

[15] P. MIHĂILĂ, T. BĂLAN, R. CURPEN and F. SANDU, "Network Automation and Abstraction using Python," MACRo 2017 - 6th International Conference on Recent Achievements , 19 10 2017. [Online]. Available: http://archive.sciendo.com/MACRO/macro.2017.2.issue-1/macro-2017-0011/macro-2017-0011.pdf. [Accessed 10 04 2023].

[16] G. Milios, "Network Automation using Python," International Hellenic University, 09 09 2021. [Online]. Available: https://repository.ihu.edu.gr/xmlui/handle/11544/29802. [Accessed 10 04 2023].

[17] R. olpus, zabbix 8.1 network monitoring, olton: packt publishing ltd, 2010.

[18] "Network Topology Architectures," ipcisco, [Online]. Available: https://ipcisco.com/lesson/network-topology-architectures/. [Accessed 10 04 2023].

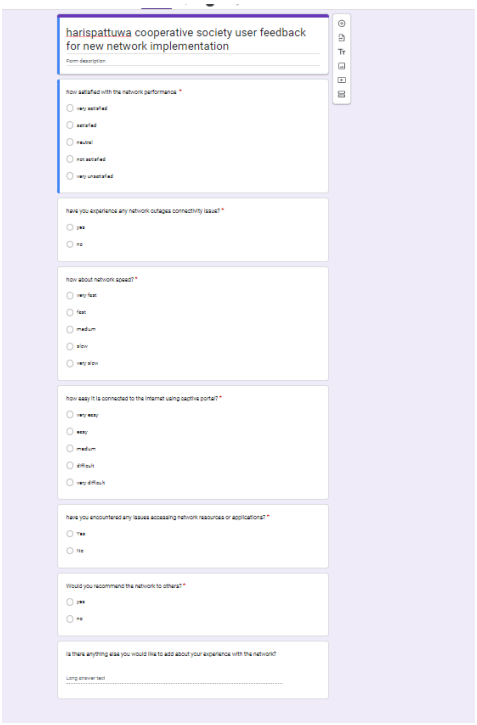
[19] "Cisco Packet Tracer," cisco, [Online]. Available: https://www.netacad.com/courses/packet-tracer. [Accessed 10 04 2023].

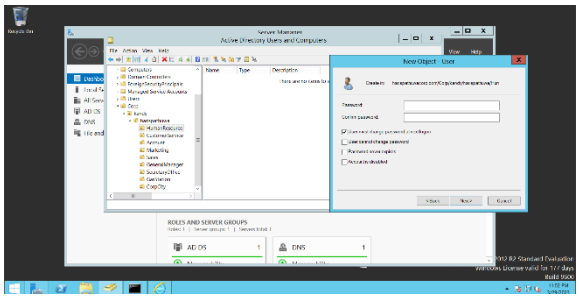
[20] "Getting Started with GNS3," GNS3, [Online]. Available: https://docs.gns3.com/docs/. [Accessed 10 04 2023].

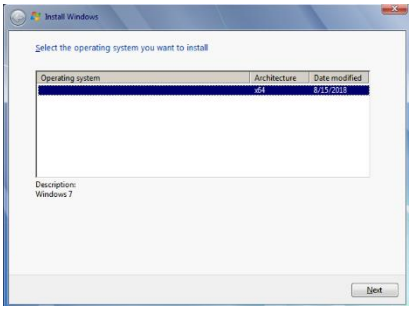
[21] "VMware Workstation Pro," VMware , [Online]. Available: https://www.vmware.com/products/workstation-pro.html. [Accessed 10 04 2023].

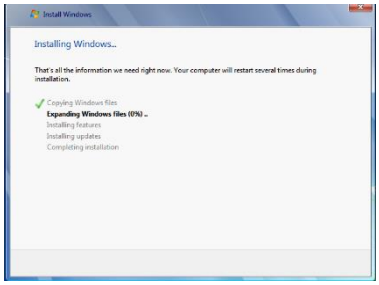
[22] A. Lamberti, "Network Testing: How to Test Network Performance," obkio, 01 03 2023. [Online]. Available: https://obkio.com/blog/network-testing/. [Accessed 15 04 2023].

Appendices


harispattuwa cooperative society user feedback for new network implementation
Form description
how satisfied with the network performance *
very satisfied
satisfied
neutral
not satisfied
very unsatisfied
have you experience any network outages connectivity issue? *
yes
no
how about network speed? *
very fast
fast
medium
slow
very slow
how easy it is connected to the internet using captive portal? *
very easy
easy
medium
difficult
very difficult
have you encountered any issues accessing network resources or applications? *
Yes
No
Would you recommend the network to others? *
yes
no
Is there anything else you would like to add about your experience with the network?
Long answer text


Server Manager
Active Directory Users and Computers
New Object - User
ROLES AND SERVER GROUPS
AD DS
DNS


Install Windows
Select the operating system you want to install
Operating system
Architecture
Date modified
x64
8/15/2013
Description:
Windows 7
Next


Install Windows
Installing Windows...
That's all the information we need right now. Your computer will restart several times during installation.
Copying Windows files
Expanding Windows files (0%) ...
Installing features
Installing updates
Completing installation