EAST WEST UNIVERSITY

Department of Computer Science and Engineering

CSE499

INTERNSHIP REPORT ON

Network Monitoring, Implementation and Software Design

Submitted By

Hussain Muhammad Khalid

ID: 2014-2-60-053

Supervised By

Dr. Md. Nawab Yousuf Ali

Associate Professor

Department of Computer Science and Engineering

East West University

An Internship Report Presented to the Department of Computer Science and Engineering in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science (B.Sc.) in Computer Science and Engineering, East West University, Dhaka - 1212

Performed at

Energypac®

25, Energy Center, Tejgaon I/A, Dhaka-1208

Internship Attended: 20th January, 2019 – 19th April, 2019

Date of submission: 22nd September, 2019

Declaration

I, Hussain Muhammad Khalid (ID: 2014-2-60-053) hereby, declare that this report was compiled by me based on the experience and knowledge I gained from undergoing the industrial training at Energypac IT for partial fulfilment of the requirement for the completion of the B.Sc. in Computer Science and Engineering as required in the syllabus approved by the senate of East West University, Dhaka – 1212, Bangladesh.

Signature

. . . . . .

(Hussain Muhammad Khalid)

ID: 2014-2-60-053

LETTER OF TRANSMITTAL

12th June, 2019

Dr. Md. Nawab Yousuf Ali
Associate Professor
Department of Computer Science and Engineering
East West University, Dhaka-1212, Bangladesh.

Subject: Submission of Internship Report.

Dear Sir,
It gives me immense pleasure to submit my report on Internship at Energypac.It ia great achievement to work under your active supervision. In this report, I have tried to describe my experience, project works, and achievements and so on.

As part of my internship, I have served in Energypac IT for three months where I have not only gained real life work experience but understood how important is to maintain regulatory and functionality in professional field. As a document of my effort during the internship period I have conducted all the planning, research and project works that I have done during my internship periods, specially their requirement, functionalities and technical specification.

I shall be highly obliged if you are kind enough to receive this report and provide your valuablae judgment. I sincerely hope that this report will meet your expectation and will serve its purpose.

Sincerely Yours,

Hussain Muhammad Khalid
ID: 2014-2-60-053
Department of Computer Science and Engineering
East West University, Dhaka-1212, Bangladesh.

LETTER OF ACCEPTANCE

This Internship Report entitled "Network Monitoring, Implementation and Software Design", submitted by Hussain Muhammad Khalid (ID: 2014-2-60-053) to the Department of Computer Science and Engineering, East West University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 12th September, 2019.

. . . . . **(Internship Supervisor)**

Dr. Md. Nawab Yousuf Ali
Associate Professor
Department of Computer Science and Engineering
East West University, Dhaka-1212, Bangladesh.

. . . . . **(Chairperson)**

Dr. Taskeed Jabid
Associate Professor and Chairperson
Department of Computer Science and Engineering
East West University, Dhaka-1212, Bangladesh.

Acknowledgement

As it is true for everyone, I have also arrived at this point of achieving a goal in my life through various interactions and help from the others. However, written words are often elusive and harbor diverse interpretations even in one's mother language. Therefore, I would like to make efforts to find best words to express my thankfulness other than simply listing those people who have contributed to my intern itself in an essential way. This work was carried out in the Department of Computer Science and Engineering at **East West University, Bangladesh.**

First of all, I would like to express my deepest gratitude to the almighty for His blessings on me. Next, my special thanks go to my supervisor, **Dr. Md. Nawab Yousuf Ali**, without his guidance this would not have been possible. His encouragements, visionaries and thoughtful comments and suggestions, unforgettable support at every stage of my B.Sc. study were simply appreciating and essential.

We would like to thank **Md. Atiqur Rahman, IT manager** as my organizational supervisor. I am also grateful to **Md. Emran Rony, IT officer** for his overall support and his valuable suggestions.

I am very great full to all **The Faculty Members** of CSE Department who taught me every way. They taught me that knowing the subject matter is more important than grade.

Last but not the least, we would like to thank my parents for their unending support, encouragement and prayers.

ABSTRACT

This report brings out a detailed picture on my role as an intern of Technical Evangelist team at Energypac Bangladesh from 19th January, 2019 – 20th April, 2019. The organizational structure of Energypac, key values and responsibilities of the Technical Evangelist team and the major research and project I have assigned during my internship period are described in the report.

I am going to report my work on Network Implementation and monitoring on a corporate office environment and how to maintain it properly. In this Internship I had worked on Network Performance Monitoring System by using TNM and TNI Network Monitoring Software. I had also worked how to create subdomain and server configuration.

Also I am going to describe how router and servers are interconnected with each other, I also learn how different type of server working process and how they maintained in an office environment.

In Energypac they mainly use some in house build in and developed software for their daily office propose. I am going to describe about an E-ticket system software design under, which software they are using for request individual Day Off, Early Leave or Vacation.

Table of Contents

Chapter 1

Introduction

A data network or computer network is a communication network that allows computers to exchange data with one another. Two devices are said to be networked when a device id able to exchange information with another device. Network basics include switches and routers, which can help business share applications, speed information access, and enhance customer service. If a company's head office is connected with its branch offices located at different cities then it is easy to control branches using communication network. It can also provide security so that unauthorized user can't have access to the system. Only authorized users are allowed to use different servers like mail server, database server, file server etc. A backup server will provide backup of all documents and files.

1.1 Overview

Now a day's Data communication and networking may be the fastest growing technologies in the world. Computer and Computer networks and Internet Services are found in nearly every business and industry around us. But just 30 years ago situation was not like that. As an underdevelopment country we don't have trained people and unexpected actions from our Government.

We now stand at a critical turning point in the use of technology to extend and empower our human network. The globalization of the Internet has succeeded faster than anything. Other things is rapidly changing to keep up with the evolution of global network. In the next stage of our development, innovators will use the internet as a starting point for their efforts.

In this Internship I had worked on Network Performance Monitoring System by using TNM and TNI Network Monitoring Software. These two tools are very cool to use and provide best performance. I had also worked how to create subdomain and server configuration.

1.2 Objective of the Report

The main objectives of this report are as follows:

- To learn about types of network and network classification.
- To learn how to install VLAN and Networking configuration.
- To know about DNS Server, Web Server and hoe to configure DNS Server and Web Server.
- To know about the Network Monitoring with TNM and TNI and others monitoring software.
- I have learn C# and design an E-ticket system software for a project purpose.

1.3 Reason Behind Choosing Internship

Internship is known as to gain sensible experiences from the different organizations that will help a lot to make a relation between the theoretical and practical knowledge. Internship is not only a four credit course for the students graduating from East West University but it also gives knowledge about how works goes on in an organization.

As a student of CSE, I have done some networking courses but this is insufficient to know the computer networking properly because it's a vast area of the modern technology. As a result to get a sound knowledge about computer networking, I was interested to do this internship.

1.4 Summary of the Report

The objective of this Internship is to develop an efficient knowledge in Network Monitoring Performance and acquire real life software knowledge.

The 1st Chapter, I have described the aim and objective and an overall view that I am going to implement throughout these internship work.

The 2nd Chapter, I will describing about Network classification, how they work, its importance etc.

The 3rd Chapter, is describing how to install VLAN and how to setup network.

The 4th Chapter, mainly discuss about DNS Server and Web Server and also DNS and Web Server configuration.

The 5th Chapter, is describe about Network Monitoring with Total Network Monitoring software and will describing about Networking Error Solving. A computer Network may fail to function properly for many different reasons and we discuss about this problem in this chapter.

The 6th Chapter, is the Conclusion & Future Work.

Chapter 2

Computer Network

A computer network is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

2.1 Computer Networks

A network consists of two or more computers or devices that are linked in order to share resources (such as printers, CD-ROMs etc.), exchanges files or allow electronic communication. The computers or Devices on a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beams.

2.2 Types of Networks

There are three basic types of networks included:

1. LAN
2. MAN
3. WAN

2.2.1 Local Area Network (LAN):

A Network is said to be Local Area Network (LAN) if it is confined relatively to a small area. It is generally limited to a building or a geographical area, expanding not more than a mile apart to other computers. Figure 1 shows the construction of a LAN.

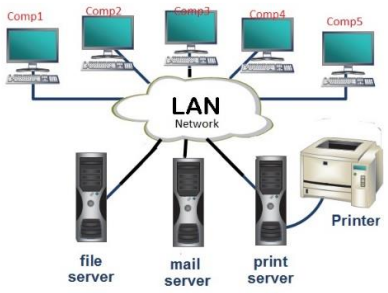


Fig 1: LAN

2.2.2 Metropolitan Area Network (MAN):

Metropolitan Area Network (MAN) covers large geographic areas, such as cities. Often used by local libraries and government agencies often to connect to citizens and private industries. Figure 2 shows the construction of a MAN.

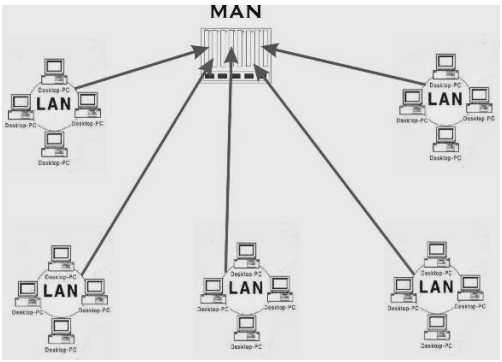


Fig 2: MAN

2.2.3 Wide Area Network (WAN):

Wide Area Networks (Wan) connect large geographic areas, such as London, UK or the ant countries of the world. In this type of network dedicated transoceanic cabling or satellite uplinks may be used. Figure 3 shows the construction of a WAN.

Fig 3: WAN

2.3 Equipment's

2.3.1 Router:

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. The most familiar type of IP routers are home and small office routers that simply forward IP packets between the home computers and the Internet.

Fig 4: Cisco Router 1841-K9

2.3.2 Switch:

A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device. A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Switches for Ethernet are the most common form of network switch. The first Ethernet switch was introduced by Kaplan in 1990. Switches also exist for other types of networks including Fiber Channel, Asynchronous Transfer Mode, and InfiniBand.

Fig 5: Avaya ERS 2550T-PWR Network Switch

2.3.3 Firewall:

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

The term firewall originally referred to a wall intended to confine a fire within a building. Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment. The term was applied in the late 1980s to network technology that emerged when the Internet was fairly new in terms of its global use and connectivity. The predecessors to firewalls for network security were the routers used in the late 1980s, because they separated networks from one another, thus halting the spread of problems from one network to another. Figure 6 shows the working process of a Firewall.

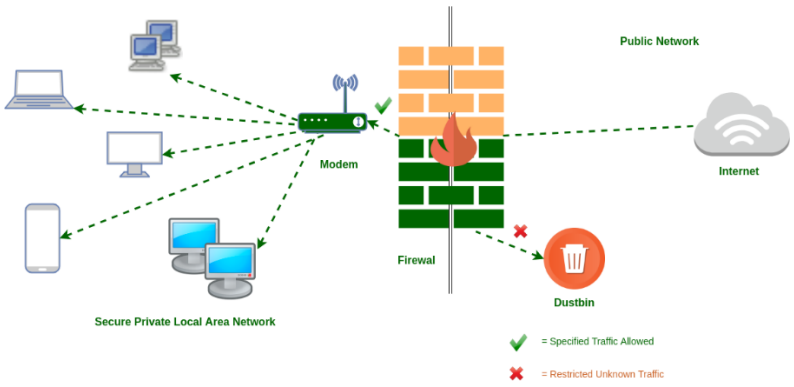


Fig 6: Firewall Working Process

2.4 Server:

A server is a computer designed to process requests and deliver data to another computer over the internet or a local network. The word server is understood by most to mean a web server where web pages can be accessed over the internet through a client like a web browser. However, there are several types of servers, including local ones like file servers that store data within an intranet network.

Although any computer running the necessary software can function as a server, the most typical use of the word references the enormous, high-powered machines that function as the pumps pushing and pulling data from the internet.

2.4.1 DNS Server:

A DNS server is a type of name server that manages, maintains and processes Internet domain names and their associated records. In other words, a DNS server is the primary component that implements the DNS (Domain Name System) protocol and provisions domain name resolution services to Web hosts and clients on an IP-based network. A DNS server stores a database of different domain names, network names, Internet hosts, DNS records and other related data. The most basic function of a DNS server is to translate a domain name into its respective IP address.

2.4.2 Mail Server:

Email servers facilitate the sending and receiving of email messages. If you have an email client on your computer, the software is connecting to an IMAP or POP server to download your messages to your computer, and an SMTP server to send messages back through the email server.

2.4.3 Proxy Server:

Proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems.

2.4.4 Web Server:

A web server show pages and runs apps through web browsers. The server your browser is connected to right now be a web server that's delivering this page and any images you see on it. The client program, in this case, is most likely a browser like Internet Explorer, Chrome, Firefox, Opera, or Safari. Web servers are used for all sorts of things in addition to delivering simple text and images, such as for uploading and backing up files online through a cloud storage service or online backup service.

2.4.5 Database Server:

The term database server may refer to both hardware and software used to run a database, according to the context. As software, a database server is the back-end portion of a database application, following the traditional client-server model. This back-end portion is sometimes called the instance. It may also refer to the physical computer used to host the database. When mentioned in this context, the database server is typically a dedicated higher-end computer that hosts the database.

2.4.6 FTP Server:

FTP servers support the moving of files through File Transfer Protocol tools. FTP servers are accessible remotely via FTP client programs, which connect directly to the file share on the server, either through the server's built-in FTP capabilities or with a dedicated FTP server program.

2.4.7 Backup Server:

A backup server is a type of server that enables the backup of data, files, applications and/or databases on a specialized in-house or remote server. It combines hardware and software technologies that provide backup storage and retrieval services to connected computers, servers or related devices.

2.5 Existing System:

I have studied on the Network setup of Energypac Corporation where in terms of usability their set ups are meant to be works like other system. Their systems are as following:

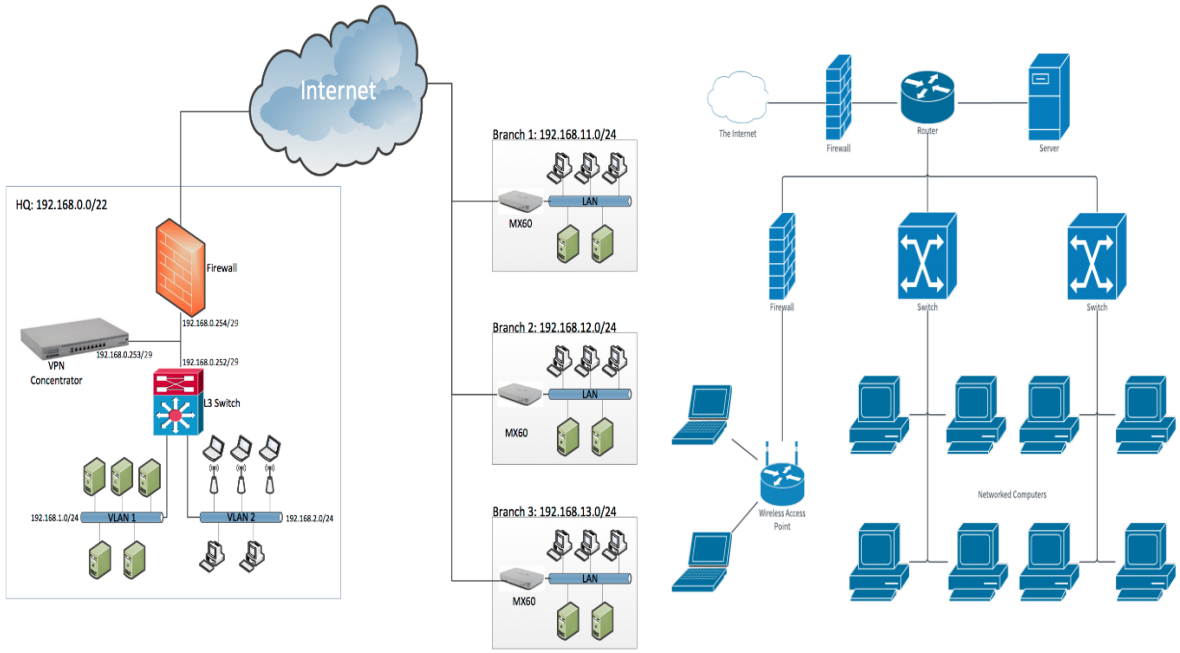


Fig 7: Networking Model

In Energypac they have well decorated Networking Model. There are four different floor in the building and in each floor there are different Server placed. Each department have its own server. It would help a lot to avoid complication. They don't use VPN but there are Backup Servers which ensure that if any server is down for a while it doesn't affect the whole network. There are Mail Server, FTP Server, Software Server and Firewall keeps the system secure form malicious and hacking attack. All branches aren't connected with each other.

2.6 Internet Protocol Address:

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using

128 bits for the IP address, was developed in 1995, and standardized in December 1998.[4] In July 2017, a final definition of the protocol was published. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6. The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., 192.168.1.15/24, which is equivalent to the historically used subnet mask 255.255.255.0. IP address can be divided into two types:

- Public IP address / Real address
- Private IP address

2.7 IP Address Classes and Formats:

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	2,147,483,648 (2^{31})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	1,073,741,824 (2^{30})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	536,870,912 (2^{29})	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	240.0.0.0	255.255.255.255

Class A
In a Class A network, the first eight bits, or the first dotted decimal, is the network part of the address, with the remaining part of the address being the host part of the address. There are 128 possible Class A networks.

0.0.0.0 to 127.0.0.0

However, any address that begins with 127. Is considered a loopback address.

Example for a Class A IP address:
2.134.213.2

Class B
In a Class B network, the first 16 bits are the network part of the address. All Class B networks have their first bit set to 1 and the second bit set to 0. In dotted decimal notation, that makes 128.0.0.0 to 191.255.0.0 as Class B networks. There are 16,384 possible Class B networks.

Example for a Class B IP address:
135.58.24.17

Class C
In a Class C network, the first two bits are set to 1, and the third bit is set to 0. That makes the first 24 bits of the address the network address and the remainder as the host address. Class C network addresses range from 192.0.0.0 to 223.255.255.0. There are over 2 million possible Class C networks.

Example for a Class C IP address:
192.168.178.1

Class D
Class D addresses are used for multicasting applications. Unlike the previous classes, the Class D is not used for "normal" networking operations. Class D addresses have their first three bits set to "1" and their fourth bit set to "0". Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address space, since all the hosts within a group share the group's IP address for receiver purposes.
Example for a Class D IP address:
227.21.6.173

Class E
Class E networks are defined by having the first four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is used as a broadcast address.

Example for a Class D IP address:
243.164.89.28

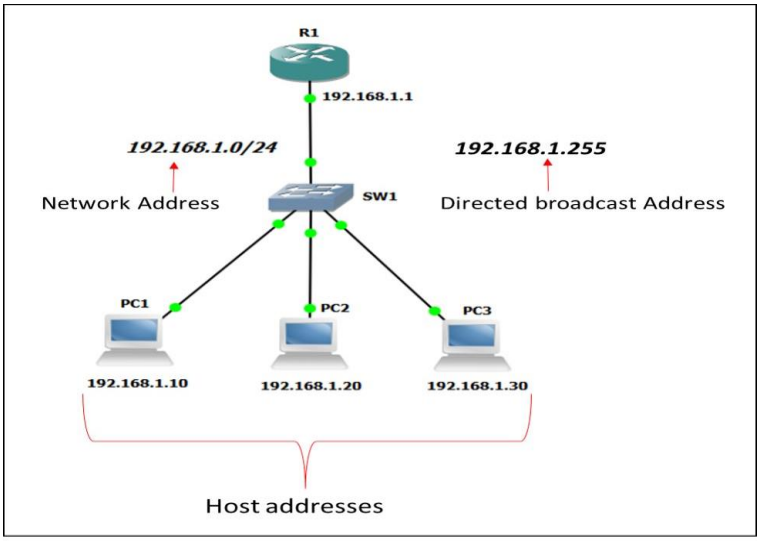
2.8 Network and Host Addressing:

Internet addresses are allocated by the InterNIC (http://www.internic.net), the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions. The next section explains how networks can be divided using subnet masks.



Three types of IP addresses in a network

2.8.1 Public IP Address:

A public IP address is an IP address that your home or business router receives from your ISP. Public IP addresses are required for any publicly accessible network hardware such as a home router and the servers that host websites. Public IP addresses differentiate the devices that are plugged into the public internet. Each device that accesses the internet uses a unique IP address. A public IP address is sometimes called an Internet IP.

2.8.2 Private IP Address:

A private IP address is an IP address that's reserved for internal use behind a router or other Network Address Translation (NAT) device, apart from the public. Private IP addresses are in contrast to public IP addresses, which are public and can't be used within a home or business network. Sometimes a private IP address is also referred to as a local IP address.

The Internet Assigned Numbers Authority (IANA) reserves the following IP address blocks for use as private IP addresses:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

The first set of IP addresses allow for over 16 million addresses, the second for over 1 million, and over 65,000 for the last range.

Another range of private IP addresses is 169.254.0.0 to 169.254.255.255, but those addresses are for Automatic Private IP Addressing (APIPA) use only.

In 2012, the IANA allocated 4 million addresses of 100.64.0.0/10 for use in carrier-grade NAT environments.

2.8.3 Broadcast Address:

A broadcast address is a network address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. A message sent to a broadcast address may be received by all network-attached hosts. For network layer communications, a broadcast address may be an IP address. In Ethernet networks, it can be a MAC address. The broadcast address for an IPv4 host can be obtained by taking the bit complement of the subnet mask and then performing a bitwise OR operation with the host's IP address. In other words, take the host's IP address, and set to '1' any bit positions which hold a '0' in the subnet mask. For example, for broadcasting a packet to an

Entire IPv4 subnet using the private IP address space 172.16.0.0/12, which has the subnet mask 255.240.0.0, the broadcast address is 172.16.0.0 OR 0.15.255.255 = 172.31.255.255.

2.9 Sub Netting:

Subnetting is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduces the size of the broadcast domain.

Consider the following example:

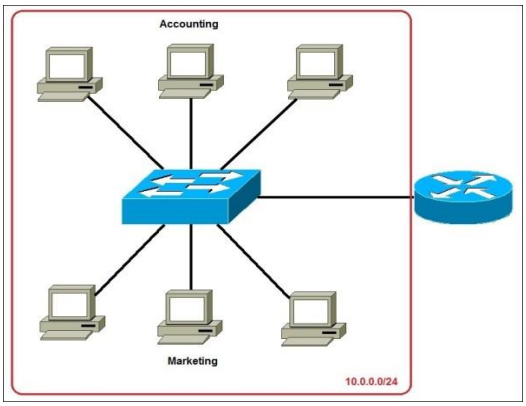


Fig 8

In the picture above we have one huge network: 10.0.0.0/24. All hosts on the network are in the same subnet, which has following disadvantages:

- A single broadcast domain – all hosts are in the same broadcast domain. A broadcast sent by any device on the network will be processed by all hosts, creating lots of unnecessary traffic.
- Network security – each device can reach any other device on the network, which can present security problems. For example, a server containing sensitive information shouldn't be in the same network as a user workstation.
- Organizational problems – in a large networks, different departments are usually grouped into different subnets. For example, you can group all devices from the Accounting department in the same subnet and then give access to sensitive financial data only to hosts from that subnet.

The network above could be sub netted like this Fig 9:

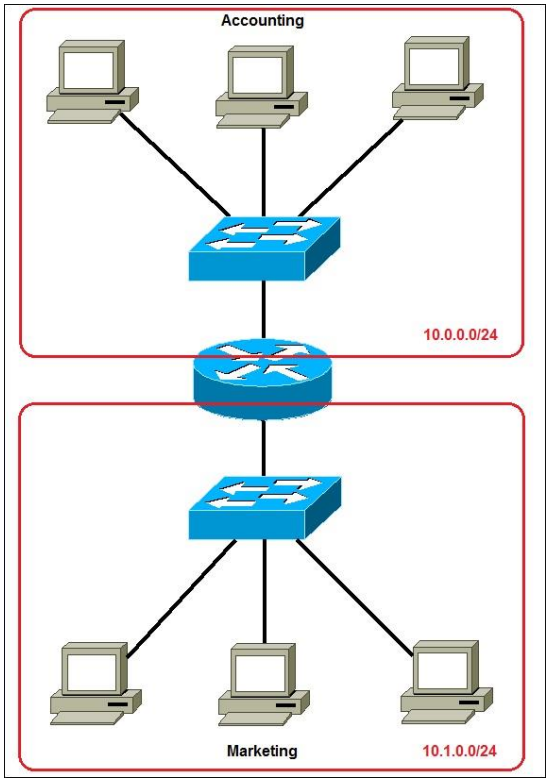


Fig 9

Now, two subnets were created for different departments: 10.0.0.0/24 for Accounting and 10.1.0.0/24 for Marketing. Devices in each subnet are now in a different broadcast domain. This will reduce the amount of traffic flowing on the network and allow us to implement packet filtering on the router.

2.10 Subnet Mask:

A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets). Systems within the same subnet

Can communicate directly with each other, while systems on different subnets must communicate through a router.
A subnet mask hides (or masks) the network part of a system's IP address and leaves only the host part as the machine identifier. It uses the same format as an IPv4 address — four sections of one to three numbers, separated by dots. Each section of the subnet mask can contain a number from 0 to 255, just like an IP address. For example, a typical subnet mask for a Class C IP address is:

255.255.255.0

In the example above, the first three sections are full (255 out of 255), meaning the IP addresses of devices within the subnet mask must be identical in the first three sections. The last section of each computer's IP address can be anything from 0 to 255. If the subnet mask is defined as 255.255.255.0, the IP addresses 10.0.1.99 and 10.0.1.100 are in the same subnet, but 10.0.2.100 is not.

A subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used).

If your computer is connected to a network, you can view the network's subnet mask number in the Network control panel (Windows) or System Preference (macOS). Most home networks use the default subnet mask of 255.255.255.0. However, an office network may be configured with a different subnet mask such as 255.255.255.192, which limits the number of IP addresses to 64.

Large networks with several thousand machines may use a subnet mask of 255.255.0.0. This is the default subnet mask used by Class B networks and provides up to 65,536 IP addresses (256 x 256). The largest Class A networks use a subnet mask of 255.0.0.0, allowing for up to 16,777,216 IP addresses (256 x 256 x 256).

Chapter 3

Implementation of VLAN

A virtual LAN (**VLAN**) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.

3.1 Virtual Local Area Network:

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area. VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

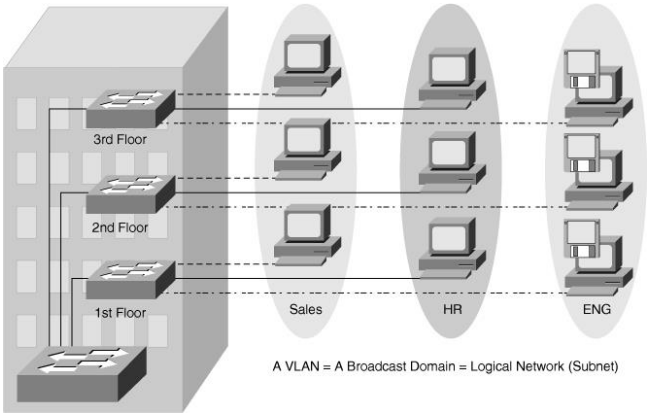


Fig 10: VLANs Multiple Switches and Multiple Floors

Types of VLANs include Protocol based, static and dynamic VLANs:

- A Protocol VLAN- which has traffic handled based on its protocol. A switch will segregate or forward traffic based on the traffics protocol.
- Static VLAN- also referred to as port-based VLAN, needs a network administrator to assign the ports on a network switch to a virtual network; while:

- Dynamic VLAN- allows a network administrator just to define network membership based on device characteristics, as opposed to switch port location.

3.2 VLAN Model in Energypac:

Energypac has a mix setup for its employees sitting arrangement which includes Marketing, Accounts, Sales, IT and HR department all together in the same place. Some part of the Marketing department sit in the first floor and few sit in the top floor of the same building. Now to create a secure data sharing traditional LAN is not applicable. So they has decided to implement Virtual Local Area Networking into its office which will allow them to utilize optimum technological advancement.

To create VLAN name on a catalyst switch 3560G enter following configuration command on the terminal:

Creates VLAN Command: vlan 2 name name

3560G>

3560G>en

3560G#config t

3560G (config)#vlan

3560G (config-vlan)#vlan 2

3560G (config-vlan)#name marketing

3560G (config-vlan)#^z

To see the VLAN database use the show vlan command.

3.3 VLAN Memberships:

Two types of VLAN membership methods exists and they are Static and Dynamic.

The difference between static and dynamic VLANs are given below.

• **Static VLANs:** In a static VLAN, the network administrator creates a VLAN and then assigns switch ports to the VLAN. Static VLANs are also called port-based VLANs. The association with the VLAN does not change until the administrator changes the port assignment. End-user devices become the members of VLAN based on the physical switch port to which they are connected.

The ports on a single switch can be assigned multiple VLANs. Even though two devices are connected to different ports on a same switch, traffic will not pass between them if the connected ports are on different VLANs. We need a layer 3 device (typically a Router) to enable communication between two VLANs.

• **Dynamic VLANs:** In a dynamic VLAN, the switch automatically assigns the port to a VLAN using information from the user device like MAC address, IP address etc. When a device is connected to a switch port the switch queries a database to establish VLAN membership. A network administrator must configure VLAN database of a VLAN Membership Policy Server (VMPS).

Dynamic VLANs support instant movability of end devices. When we move a device from a port on one switch to a port on another switch, the dynamic VLANs will automatically configure the membership of the VLAN.

To configure the port we need to follow the following procedure:

3560G (config-if)#int f0/2

3560G (config-if)#switchport access vlan 2

3560G (config-if)#int f0/3

3560G (config-if)# switchport access vlan 3

3560G (config-if)# int f0/4

3560G (config-if)# switchport access vlan 4

3560G (config-if)# int f0/5

3560G (config-if)# switchport access vlan 5

3560G (config-if)#^z

To verify the configuration use the show vlan command on the terminal.

3.4 Uses of Trunk Link:

A Trunk link is a point-to-point link between two network devices. Trunk link carry more than one VLAN. With VLAN trucking, we can extend our configured VLAN across the entire network. Remember, sending information from an access link on one VLAN to another VLAN is not possible without the additional device a router or an external layer 2 bridge connected between the VLAN.

A Trunk link can transport multiple VLANs traffic through a single switch port. A trunk link is not assigned to a specific VLAN.

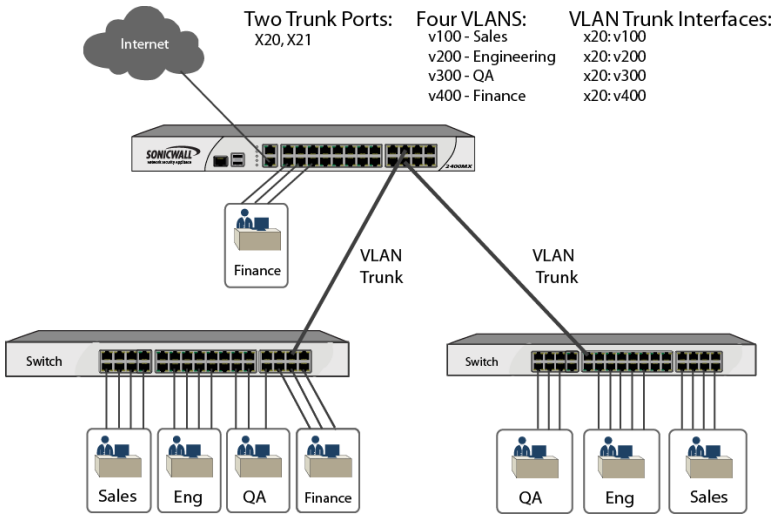


Fig 11: Use of Trunk link to connect switches

Configuration of trunk ports are shown below:

3560G#config t

3560G (config)# int f0/12

3560G (config-if)# switchport model trunk

3560G (config-if)#^z

3560G#

3.5 VLAN Trunk Protocol:

VLAN Trucking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network. To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over 802.1Q, and ISL trunks. VTP is available on most of the Cisco Catalyst Family products. Using VTP, each Catalyst Family Switch advertises the following on its trunk ports:

- Management domain
- Configuration revision number
- Known VLANs and their specific parameters

A configuration of VTP is given below:

3560G (config)#vtp mode server

3560G (config)#vtp domain transcom

3560G (config)#vtp password *******

3560G (config)#vlan 2

3560G (config)#name Marketing

3560G (config)#vlan 3

3560G (config)#name Sales

By using the show vlan brief command we can verify our configuration.

3.6 Routing Between VLANs:

Each VLAN is its own subnet and broadcast domain, which means that frames broadcast onto the network are only switched between the ports within the same VLAN. For inter-VLAN communication, a layer 3 device (usually a router) is needed. This layer 3 device needs to have an IP address in each subnet (VLAN) and have a connected route to each of those subnets. The hosts in each subnet can use the router's IP addresses as their default gateway. This logical diagram explains a simple inter VLAN routing scenario. The scenario can be expanded to include a multi-switch environment if you first configure and test inter-switch connectivity across the network before you configure the routing capability. For such a scenario that uses a Catalyst 3550, refer to Configuring Inter VLAN Routing with Catalyst 3550 Series Switches.

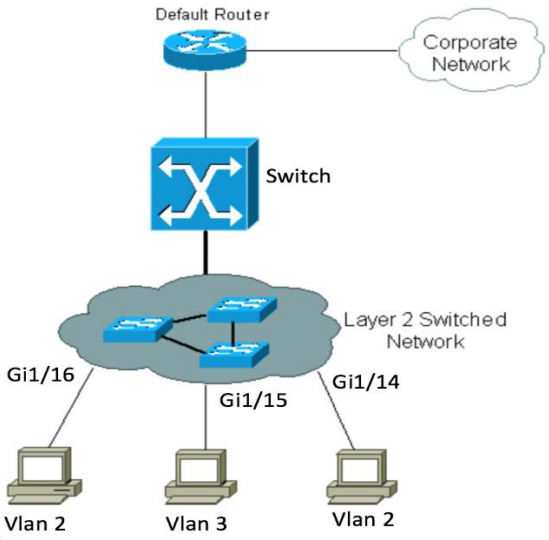


Fig 12: Router connection of all VLANs together allowing inter VLAN communication

Step-by-Step Instructions

We have to complete these steps in order to configure a switch to perform interVLAN routing.

Enable routing on the switch with the IP routing command. Even if IP routing was previously enabled, this step ensures that it is activated.

```
Switch#vlan database

Switch (vlan)#vlan 2
VLAN 2 added:
   Name: VLAN0002

Switch (vlan)#vlan 3
VLAN 3 added:
   Name: VLAN0003

Switch (vlan)#vlan 10
VLAN 10 added:
   Name: VLAN0010

Switch (vlan)#exit
APPLY completed.
Exiting....


Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch (config)#interface Vlan2

Switch (config-if)#ip address 10.1.2.1 255.255.255.0

Switch (config-if)#no shutdown


Switch (config)#interface FastEthernet 0/1

Switch (config-if)#no switchport

Switch (config-if)#ip address 200.1.1.1 255.255.255.0

Switch (config-if)#no shutdown
```

Configure the default route for the switch.

```
Switch (config)#ip route 0.0.0.0 0.0.0.0 200.1.1.2
```

Chapter 4

Network and Server Configuration

Network configuration is the process of setting a network's controls, flow and operation to support the network communication of an organization and/or network owner. This broad term incorporates multiple configuration and setup processes on network hardware, software and other supporting devices and components.

4.1 Schematic Network Diagram:

Schematic diagrams showing the network configurations of the three vascular patterning models. These have been re-arranged from the original figures to aid comparison between models. Activation or repression is shown with solid lines. Dashed lines indicate transport of auxin into and out of the cell, with the arrowhead indicating whether it promotes or inhibits auxin accumulation within that cell. Figure 13 shows an office Networking Diagram.

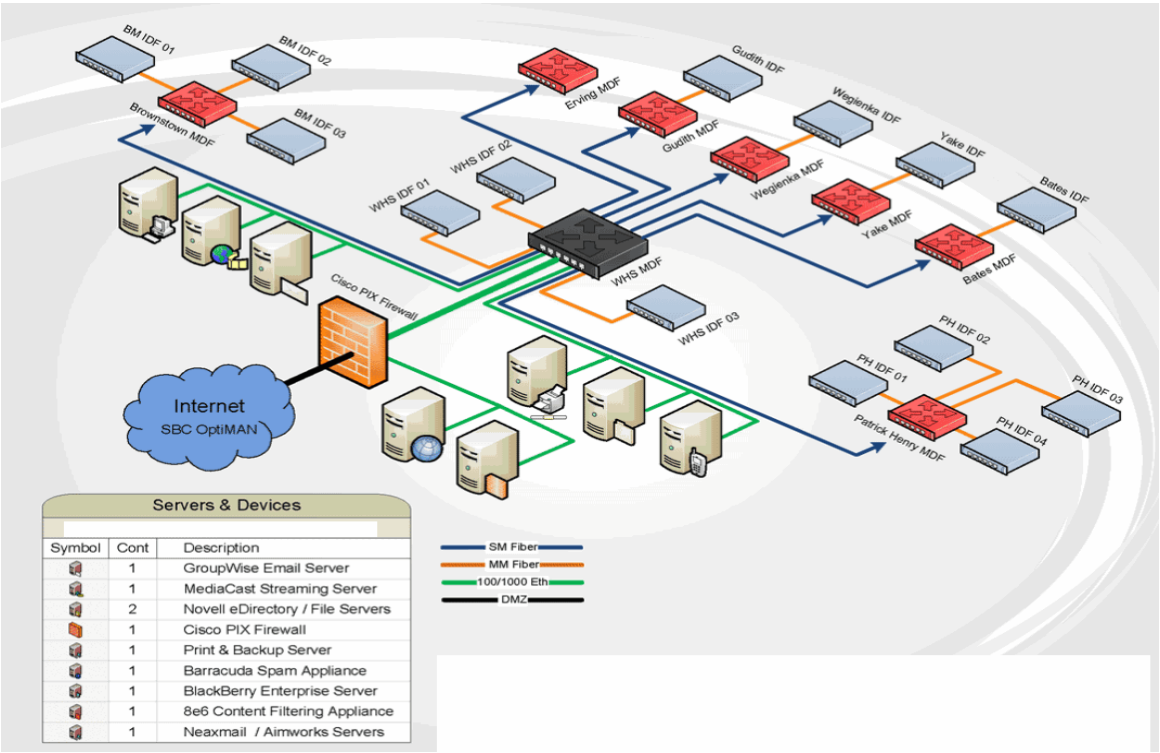


Fig 13

4.2 Router and Switch Configuration of the Network:

4.2.1 Core Routing Configuration:

Step 1: Establish a HyperTerminal session to router R1.

Step 2: Enter privileged EXEC mode.

Router>enable

Router#

Step 3: Enter global configuration mode.

Router#configure

terminal Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Step 4: Configure the router name as R1.

Enter the command hostname R1 at the prompt.

Router(config)#

hostname R1 R1(config)#

Step 5: Disable DNS lookup.

Disable DNS lookup with the no ip domain-lookup command.

R1(config)#no ip domain-lookup

R1(config)#

Step 6: Configure the EXEC mode password.

Configure the EXEC mode password using the enable secret password command. Use class for the password.

R1(config)#enable secret class

R1(config)#

Step 7: Configure a message-of-the-day banner. Configure a message-of-the-day banner using the banner motd command.

R1(config)#banner motd & Enter TEXT message. End with the character '&'.
****

!!!AUTHORIZED ACCESS ONLY!!!

****

&

R1(config)#

Step 8: Configure the console password on the router. Use cisco as the password. When you are finished, exit from line configuration mode.

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#

Step 9: Configure the password for the virtual terminal lines. Use cisco as the password. When you are finished, exit from line configuration mode.

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#

Step 10: Configure the FastEthernet0/0 interface. Configure the FastEthernet0/0 interface with the IP address 192.168.1.1/24.

R1(config)#interface fastethernet 0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shutdown %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#

Step 11: Configure the Serial0/0/0 interface. Configure the Serial0/0/0 interface with the IP address 192.168.2.1/24. Set the clock rate to 64000.

R1(config-if)#interface serial 0/0/0

R1(config-if)#ip address 192.168.2.1 255.255.255.0

R1(config-if)#clock rate 64000

R1(config-if)#no shutdown

R1(config-if)#

Step 12: Return to privileged EXEC mode. Use the end command to return to privileged EXEC mode.

R1(config-if)#end

R1#

Step 13: Save the R1 configuration. Save the R1 configuration using the copy running-config startup-config command.

R1#copy running-config startup-config Building configuration... [OK]

R1#

4.2.2 Backup Routing Configuration:

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#line vty 0

R1(config-line)#password redhat

R1(config-line)#login

R1(config-line)#exit

R1(config)#line console 0

R1(config-line)#password redhat123

R1(config-line)#login

R1(config-line)#exit

R1(config)#int fa0/0

R1(config-if)#ip address 1.0.0.1 255.0.0.0

R1(config-if)#no shut

R1#show run

```
Building configuration...

Current configuration : 552 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 1.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
line con 0
password redhat123
```

login

!

line aux 0

!

line vty 0

password redhat

login

line vty 1 4

login

!

end

4.3 Server Configuration:

4.3.1 DNS Server:

Bind can be easily installed with most Linux distributions - it's available in their repositories. You can also compile it from the source code.

To install BIND 9 from the repositories, enter in super user mode and run:

apt-get install bind9

And you now have bind installed on your machine. You can start and stop it at any time with the "start" and "stop" commands.

Stopping Bind

/etc/init.d/bind9 stop

Starting Bind

/etc/init.d/bind9 start

How to "chroot" Bind

The first step of the Bind configuration is to "chroot" it. This means that bind will not be executed with root privileges, but as a separate user, which is limited to see only its folder tree. This is done for security purposes - if someone manages to exploit a BIND vulnerability, he will not be able to do much damage, since BIND's folder structure will act as root folder.

Here we will show you how to chroot bind to the "var/lib/named" folder. The first thing to do is to edit the /etc/default/bind9 file. We will tell the bind daemon to run this file as the user "bind", who has no privileges. This is how the file should look like:

The /etc/default/bind9 file:

```
OPTIONS="-u bind -t /var/lib/named"
# Set RESOLVCONF=no to not run resolvconf
RESOLVCONF=yes
```

Now, we will have to create the specific folder in the /var/lib directory.

```
mkdir -p /var/lib/named/etc
mkdir /var/lib/named/dev
mkdir -p /var/lib/named/var/cache/bind
mkdir -p /var/lib/named/var/run/bind/run
```

This will create all the necessary folders for BIND to work without a problem in the "var/lib/named" folder. The next step is to copy BIND's configuration file. The file is located in the "/etc/bind" folder, and we will have to move it to the "/var/lib/named/etc" folder.

```
cp /etc/bind /var/lib/named/etc
```

Once we have the configuration file in its new location, it's time to create a symlink to it, since this will be very useful for future BIND updates.

```
ln -s /var/lib/named/etc/bind /etc/bind
```

Now BIND will be running without a problem in the chroot jail. However, it will still need access to several files in order to function properly, for example - the /dev/null. You can create all of them with the following commands:

```
mknod /var/lib/named/dev/null c 1 3
mknod /var/lib/named/dev/random c 1 8
chmod 666 /var/lib/named/dev/null /var/lib/named/dev/random
chown -R bind:bind /var/lib/named/var/*
chown -R bind:bind /var/lib/named/etc/bind
```

The final step is to configure the systemlog to send log and error messages to the correct location. For this, you will have to add the following line:

```
SYSLOGD="-a /var/lib/named/dev/log"
```

to the "/etc/default/syslogd" file. Here is how the file should look after that:

A syslogd file for a chrooted BIND

```
#
# Top configuration file for syslogd
#

#
# Full documentation of possible arguments are found in the manpage
# syslogd(8).
#
```

```
#
# For remote UDP logging use SYSLOGD="-r"
#
SYSLOGD="-a /var/lib/named/dev/log"
```

Now, restart syslogd and BIND and check "/var/log/syslog" for any errors.

Restart syslogd and start BIND

```
/etc/init.d/sysklogd restart
/etc/init.d/bind9 start
```

Configuring BIND

Once you have installed and chrooted BIND, it's time to start using it. The first thing that you need to do is add a DNS zone for your domain name. To do this, you will need to edit the "named.local.conf" file.

```
vi /etc/bind/named.conf.local
```

In there, you can add the following text to create a DNS zone for the "my-best-server.com".

```
zone "my-best-server.com" {
type master;
file "/etc/bind/zones/my-best-server.com.db";
};
```

The next step is to edit the actual DNS zone

```
mkdir /etc/bind/zones
vi /etc/bind/zones/my-best-server.com .db
```

The last command will show the actual DNS zone. Now add other , or change the ones shown here with your custom ones.

Two steps are left - to configure the DNS forwarder and the self-resolving setting.

To configure the DNS forwarder, we will have to edit the "named.conf.options".

```
vi /etc/bind/named.conf.options
```

In the file, look for the "forwarders" line and enter the IP of your IPS DNS server in the place of the default one.

```
forwarders{
123.123.123.123;
};
```

This way, if your DNS server cannot resolve a request, it will forward it to the ISP DNS server, not failing the request.

The last thing that we need to do is to make the DNS server resolve itself. To do this, we will have to modify the resolv.conf file.

```
vi /etc/resolv.conf
```

In there, enter the name of your domain name and your IP address.

search my-best-server.com
nameserver 192.168.0.100

4.3.2 Web Server:

For a minimum HTTP server installation, issue the following command.

```
# yum install httpd
```

If you want a more complete installation, you can install the "Web Server" package group.

```
# yum groupinstall "Web Server"
```

Make sure the "/etc/hosts" file contains references for the loopback address and the hostname.

```
127.0.0.1      localhost localhost.localdomain localhost4 localhost4.localdomain4
192.168.122.89 rhce1.localdomain rhce1
```

Turn on the HTTP server and make sure it starts automatically on reboot.

```
# service httpd start
# chkconfig httpd on
```

Create the following directories as locations for two virtual hosts. I've also created a test file in both document roots.

```
# mkdir -p /www/mysite1.com/logs
# mkdir -p /www/mysite1.com/html
# echo "MySite1.com Test file" > /www/mysite1.com/html/test.txt
# mkdir -p /www/mysite2.com/logs
# mkdir -p /www/mysite2.com/html
# echo "MySite2.com Test file" > /www/mysite2.com/html/test.txt
```

If you are using SELinux, make sure the directories and their contents are assigned the correct context.

```
# semanage fcontext -a -t httpd_sys_content_t "/www(/.*)?"
# restorecon -F -R -v /www
```

Virtual hosts are defined in the "/etc/httpd/conf/httpd.conf" file. The definition of the two virtual hosts are shown below.

```
NameVirtualHost *:80

<VirtualHost *:80>
```

```
    ServerName www.mysite1.com
    Serveralias mysite1.com
    DocumentRoot /www/mysite1.com/html
    ErrorLog /www/mysite1.com/logs/mysite1.com-error_log
</VirtualHost>

<VirtualHost *:80>
    ServerName www.mysite2.com
    Serveralias mysite2.com
    DocumentRoot /www/mysite2.com/html
    ErrorLog /www/mysite2.com/logs/mysite2.com-error_log
</VirtualHost>
```

Reload or restart the httpd service for the changes to take effect.

```
# service httpd reload
# # OR
# service httpd restart
```

Provided the DNS, or hosts file, resolves the names "mysite1.com" and "mysite2.com" to the IP address of the web server, pages under the document roots will now display for each virtual host. To test this you can alter your hosts file with the following entries.

```
127.0.0.1 mysite1.com mysite1
127.0.0.1 mysite2.com mysite2
```

You should now see the correct test page under each of the following URLs on the web server.

```
http://mysite1.com/test.txt
http://mysite2.com/test.txt
```

Using the virtual hosts we created previous, create a new directory called "private" and place a file in it.

```
# mkdir /www/mysite1.com/html/private
# echo "MySite1.com Private Test file" > /www/mysite1.com/html/private/test.txt
```

Create a ".htpasswd" file containing a username/password, then add a second entry.

```
# cd /www/mysite1.com/html/private
# htpasswd -cmb .htpasswd user1 password1
# htpasswd -mb .htpasswd user2 password2
```

Edit the "/etc/httpd/conf/httpd.conf" file with an entry such as the following.

```
<Directory "/www/mysite1.com/html/private">
  AuthType basic
  AuthName "Private Access"
  AuthUserFile "/www/mysite1.com/html/private/.htpasswd"
```

```
   Require valid-user
   Order allow,deny
   Allow from all
</Directory>
```

Reload or restart the httpd service for the changes to take effect.

```
# service httpd reload
# # OR
# service httpd restart
```

We should now be prompted for a username/password when trying to access the following file.

```
http://mysite1.com/private/test.txt
```

When the proxy server is active, the following directives specify various caching options. They are normally disabled:

#CacheRoot /var/cache/httpd
#CacheSize 5
#CacheGcInterval 4
#CacheMaxExpire 24
#CacheLastModifiedFactor 0.1
#CacheDefaultExpire 1
#NoCache a_domain.com another_domain.edu joes.garage_sale.com

The Listen directive lets your bind Apache to a specific IP address or port, in addition to the default IP address and port. It is generally disabled:

#Listen 3000
#Listen 12.34.56.78:80

The <VirtualHost> and </VirtualHost> tags enclose a series of options that establish a virtual host, useful if your system has multiple IP addresses. The options can include any of the options described in this subsection. The tags and options are normally disabled:

#<VirtualHost host.some_domain.com>
#ServerAdmin webmaster@host.some_domain.com
#DocumentRoot /www/docs/host.some_domain.com
#ServerName host.some_domain.com
#ErrorLog logs/host.some_domain.com-error_log
#TransferLog logs/host.some_domain.com-access_log
#</VirtualHost>

Chapter 5

Network Monitoring & Error Solving

Network monitoring is a computer network's systematic effort to detect slow or failing network components, such as overloaded or crashed/frozen servers, failing routers, failed switches or other problematic devices. In the event of a network failure or similar outage, the network monitoring system alerts the network administrator (NA). Network monitoring is a subset of network management.

5.1 Introduction:

In today's world, the term network monitoring is widespread throughout the IT industry. Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.

Important aspects of network monitoring:

- Monitoring the essentials
- Optimizing the monitoring interval
- Selecting the right protocol
- Setting thresholds

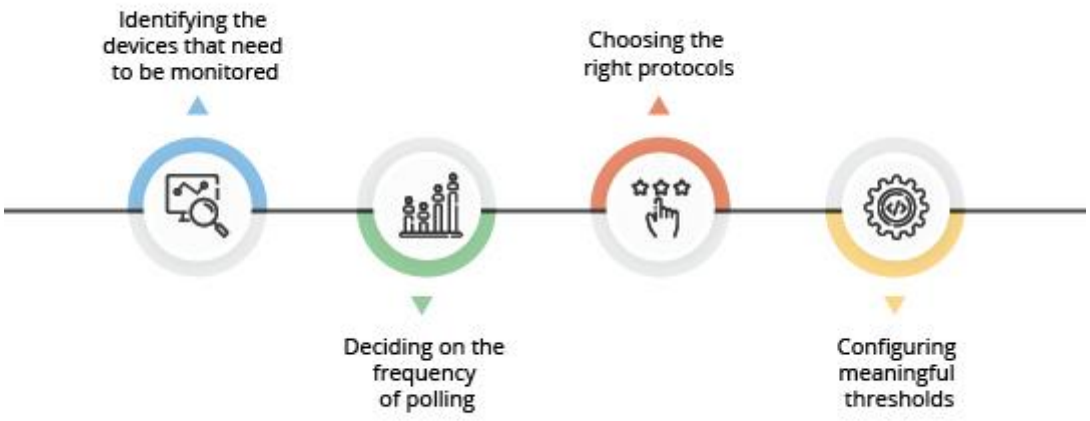


Fig 14

5.2 Monitoring the Essentials:

Faulty network devices impact network performance. This can be eliminated through early detection and this is why continuous monitoring of network and related devices is essential. In effective network monitoring, the first step is to identify the devices and the related performance metrics to be monitored. The second step is determining the monitoring interval. Devices like desktops and printers are not critical and do not require frequent monitoring whereas servers, routers and switches perform business critical tasks but at the same time have specific parameters that can be selectively monitored. Fig 15 shows the inter connectivity of devices with Network Monitoring Software.

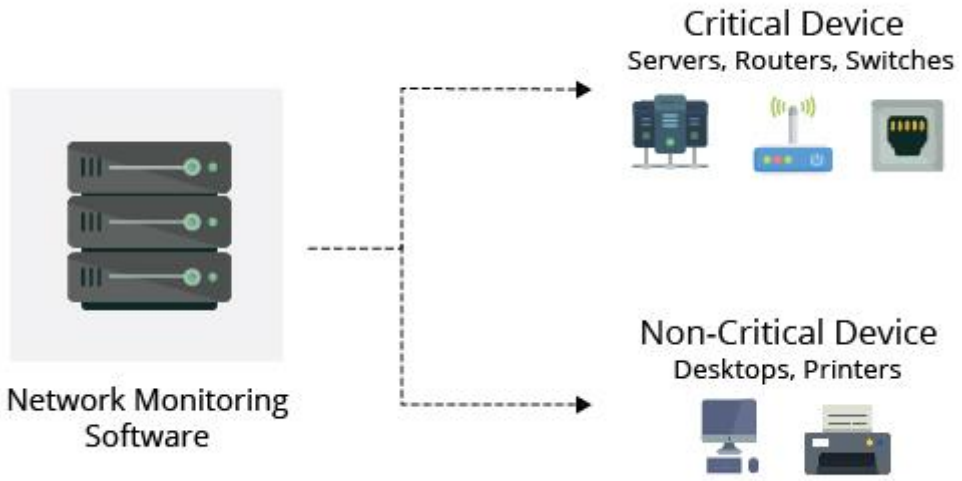


Fig 15

5.3 Monitoring Interval:

Monitoring interval determines the frequency at which the network devices and its related metrics are polled to identify the performance and availability status. Setting up monitoring intervals can help to take the load off the network monitoring system and in turn, your resources. The interval depends on the type of network device or parameter being monitored. Availability status of devices have to be monitored the least interval of time preferably every minute. CPU and Memory stats can be monitored once in every 5 minutes. The monitoring interval for other metrics like Disk utilization can be extended and is sufficient if it is polled once every 15 minutes. Monitoring every device at the least interval will only add unnecessary load to the network and is not quite necessary.

5.4 Server and Nodes Monitoring:

5.4.1 Server Monitoring:

Enterprises run multiple servers to deliver business critical services for their end users. Some of them include database servers, core app servers, caching servers, web servers, and more. Performance of each

Of these servers are critical because even if one of the servers fail, then it impacts the delivery of business critical services. Therefore it is imperative to know any performance issues proactively so that

they are identified at the early stage and fixed before they turn big and pose a threat to business. Server monitoring tools help in monitoring servers as well as the entire infrastructure. They also provide intensive reports on capacity planning to maintain the network without any hassle. Server Monitoring is the process of monitoring a server's system resources like CPU Usage, Memory Consumption, I/O, Network, Disk Usage, Process etc. Server Monitoring also helps in capacity planning by understanding the server's system resource usage. A server monitor software helps in automating the process of server monitoring. Server performance monitoring also helps in identifying other performance related issues like resource utilization, app downtime and response time.

Why is it important to monitor server performance?

- To monitor server availability and data loss.
- To monitor the responsiveness of the server.
- To know the server capacity, user load and speed of the server.
- To detect and prevent any issues that might affect the server proactively.

5.4.2 Nodes Monitoring:

Nodes Monitoring refers to the system or process to check the weather an IP address is down or not. It helps to find out the running nodes that is up. It also helps to notify the IP address that is down.

The realm of Network Monitoring Tools, Software and Vendors is Huge, to say the least. New software, tools and utilities are being launched almost every year to compete in an ever changing marketplace of IT monitoring and server monitoring.

There are different types of monitoring tools. Most of them are free. We can easily download a tool from internet and can make it use to monitoring the total network.

Some Network Monitoring Tool’s name are given below:

1. SolarWinds Network Performance Monitor
2. ManageEngine OpManager
3. Zabbix
4. Incinga
5. Datadog
6. Logic Monitor
7. OP5 Monitor
8. Fiddler
9. Pandora FMS
10. Nagios
11. The Dude
12. OpenNMS
13. NetworkMiner
14. Monitors
15. WirelessNetView

5.5 Error Solving:

5.5.1 Introduction:

Troubleshooting is a form of problem solving, often applied to repair failed products or processes on a machine or a system. It is a logical, systematic search for the source of a problem in order to solve it, and make the product or process operational again. Troubleshooting is needed to identify the symptoms. Determining the most likely cause is a process of elimination eliminating potential causes of a problem. Finally, troubleshooting requires confirmation that the solution restores the product or process to its working state.

In general, troubleshooting is the identification or diagnosis of "trouble" in the management flow of a system caused by a failure of some kind. The problem is initially described as symptoms of malfunction, and troubleshooting is the process of determining and remedying the causes of these symptoms.

5.5.2 Networking Problems and Mistakes to Avoid:

Computer networks connect the home both to the outside world and between devices within the home. Networks provide internet access, the ability to share files and printers, additional home entertainment options, and so on. Though home networking technology has advanced considerably and has become much easier to use, home network technology can pose challenges. Where does one start when first setting up a home network? Things often don't work right the first time, so how do troubleshoot? Sometimes, people settle for an inferior setup and never realize the full potential of their home network.

5.5.3 Can’t Decide Which Network Gear if Need:

Networks can be built with different combinations of hardware and software. The sheer number of choices can be overwhelming to beginners and may decide on the first solution they find. However, setups that meet the needs of some families just won't cut it for others.

5.5.4 Network Won’t Reach Certain Areas:

In many homes, networks wireless and wired won't conveniently reach all of the areas a person might need access. Stringing network cables to distant rooms of the home can prove impractical, for example, and even with wireless networks Wi-Fi radio signals may not reach corner bedrooms, a study or a porch.

Be strategic when planning where your modem or router is located in the home, and be ready to make a few concessions in your network installation plan. Thousands of home network layouts exist, can be something different.

5.5.5 Computers Can’t Get On The Internet:

Even when all of the devices in a home can communicate with each other, they may still fail to reach websites on the internet. This, too, is a common problem when first installing a home network.

After a simple check of the key network components, will be surfing again in no time.

5.5.6 Computers Can’t See Each Other On The Network:

One have finished connecting all your network gear, but nothing works. Devices can't see each other or connect to the printer, for example. Maybe the printer itself is offline.

No error messages are being displayed. You're developing a sneaking suspicion that your network is laughing at you.

Take a step-by-step approach to this problem, and your network will be up and running soon. There are lots of resources and tutorials on Livewire, including methods for connecting two computers, setting up an ad-hoc wireless network.

5.5.7 Devices Won't Join The Network:

Many home networks have a will have a computer or device such as an iPad that will not connect to the network. The device could be a specialized piece of hardware like a game console, or it could be a lone wireless computer trying to join a wired network. It could even be a computer running an old version of Windows or running Linux. Whatever the situation, extra care and attention may be required to get your device to play well with others.

5.5.8 Network Is Too Slow:

For several reasons, a home network might not run fast enough to keep up with a family's needs. They may experience very slow web downloads, sluggish or unplayable network games, interminable delays in online chatting/IM applications, and have difficulty streaming content like videos or music. This is known as network latency and the problem can be frustratingly difficult to pin down.

5.5.9 Network Connections Drop Unexpectedly:

A home network may operate flawlessly for a day, a week or a month, but suddenly, at the most inopportune time, something breaks. You may have been happily listening to an internet radio station, streaming a TV show, or playing a networked game at home, and then…nothing. What happened? There are several possibilities. Don't be surprised if this happens.

5.5.10 Network Is Not Secure:

Many home networks suffer from a lack of sufficient security, which is a risk to your data privacy. Too many homeowners fail to take a few essential steps to protect their network from attacks by outsiders. Network attacks and hacks are real threats; they happen every day and affect real families.

5.5.11 IP Address Conflict (Address Already in Use):

If a computer is set up with a static IP address that's being used by some other device on the network, the computer (and possibly also the other device) will be unable to use the network.

An example is two or more devices using the IP address 192.168.1.115.

In some cases, this problem can even occur with DHCP addressing.

5.5.12 Connected With Limited Access:

A technical glitch in Windows can cause this error message to appear when making certain types of wireless connections, which is why Microsoft provided a fix for it in a service pack update for Windows Vista systems.

You might still find this error in other versions of Windows too, though. It can also occur on a home network for other reasons that might require you to reset your router or connect and then disconnect from the wireless connection.

5.6 Troubleshooting Network Routing Problem:

5.6.1 Mac Address Restrictions:

MAC address filtering allows you to define a list of devices and only allow those devices on your Wi-Fi network. That's the theory, anyway. In practice, this protection is tedious to set up and easy to breach.

This is one of the Wi-Fi router features that will give you a false sense of security. Just using WPA2 encryption is enough. Some people like using MAC address filtering, but it's not a security feature. Each device you own comes with a unique media access control address (MAC address) that identifies it on a network. Normally, a router allows any device to connect — as long as it knows the appropriate passphrase. With MAC address filtering a router will first compare a device's MAC address against an approved list of MAC addresses and only allow a device onto the Wi-Fi network if its MAC address has been specifically approved.

Your router probably allows you to configure a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network.

5.6.2 Loose or Disconnected Cables:

Fiber optic cable was once reserved for high-performance needs, but today it's turning up in all kinds of networks. If you're familiar with copper cable, you'll quickly discover that fiber optic cable is a completely different animal. Not only is the installation process different for fiber, but also the troubleshooting process. Fiber optic cable is also far more fragile than copper cable, so there are more potential causes of trouble. I'll discuss common fiber optic cable problems and how to diagnose and repair them.

5.6.3 Overheating or Overloading:

Electronic components by nature produce heat and do not operate properly when subjected to the heat they create. A common failure of others is to not provide proper displacement of the heat created by these components. We find all too often that pieces of electronic equipment are placed in cabinetry, closets, and other enclosures without proper ventilation or cooling, and in some cases no ventilation or cooling at all.

All parts of a control system need to communicate at correct intervals to keep the system alive and healthy. What many inexperienced techs don't know is that there are specifications pertaining to the maximum number of a certain type of device that can be on a communications loop prior to malfunction occurring. We find far too often that others do not obey these rules, overload a communications chain with too many devices inevitably results in a system malfunction. The irony here is that most control systems offer hubs, repeaters and similar components that can increase the number of devices able to communicate on a single loop.

Chapter 6

Conclusion & Future Work

Technology is perhaps the most significant change agent in the world today, as it helps to create a world in which national borders, geographic distance and physical limitations become less relevant and present ever-diminishing obstacles. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe. As the internet connects the people and promotes unfettered communications, it presents the platform on which to run business, to address emergencies, to inform individuals and to support, education, science and government. It is incredible how quickly the internet became an integral part of our daily life. The complex interconnection of electronics devices and media that comprise the network is transparent to the millions of users who make it a valued and personal part of their life.

My Internship is nothing but to go one step ahead in the professional life. Internship is the bridge between theoretical knowledge and practical knowledge.

Different kinds of practical experience were gathered while performing the job during the internship period. During this intern period there were lots of constrain but it was solved through authentic determination and as per the proper guidance by the employee of Energypac.

Linux was originally developed as a free operating system. It is actually easier to install Linux to computer than Windows. It is a leading operating system on server. Linux has been used to configure server which is more secured and extensive. I have configured DNS Server and Web Server in this report. DNS is naming system in the internet so that people can easily identify the desired server. www.cisco.com , is much easier for people to remember than 10.0.0.0 which is the actual numeric address for this server. The World Wide Web is based on IP addresses, which are usually difficult to remember but DNS converted IP address to name.

A Web server is a program that, using the client/server mode. Apache is used by 60.6% of all the websites. This apache is an open source server application. There are a lot of benefits and advantages that are provided from the server.

Eventually Energypac is a well decorated and a renowned company of our country. Their Network implementation and the applications at such a level that employees and the users are all fully satisfied.

References

1. https://en.wikipedia.org/wiki/Network_switch
   (Last Access: 16/07/2019)
2. https://www.lifewire.com/servers-in-computer-networking-817380
   (Last Access: 12/08/2019)
3. https://www.paessler.com/it-explained/ip-address
   (Last Access: 12/08/2019)
4. https://support.microsoft.com/en-us/help/164015/understanding-tcp-ip-addressing-and-subnetting-basics (Last Access: 15/08/2019)
5. https://searchnetworking.techtarget.com/definition/virtual-LAN
   (Last Access: 18/08/2019)
6. http://www.omnisecu.com/cisco-certified-network-associate-ccna/vlan-membership-types.php (Last Access: 16/07/2019)
7. https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html (Last Access: 15/08/2019)
8. https://www.slashroot.in/backup-and-restore-router-configuration-file-using-tftp-server-packet-tracer-cisco-ccna (Last Access: 21/07/2019)
9. https://www.ntchosting.com/encyclopedia/dns/server-setup/#Configuring_BIND
   (Last Access: 21/07/2019)
10. https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html
    (Last Access: 22/08/2019)
11. https://www.pcwdld.com/best-network-monitoring-tools-and-software
    (Last Access: 15/07/2019)
12. https://www.lifewire.com/top-home-networking-problems-and-mistakes-817736
    (Last Access: 12/08/2019)
13. https://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/ (Last Access: 22/08/2019)