

FINAL YEAR INTERNSHIP REPORT ON COMPUTER NETWORKING

BY

MD. APPLE MAHMUD

ID No: 172-15-10099

This Report Presented in Partial Fulfillment of the Requirements
for the Degree of Bachelor of Science in Computer Science and
Engineering

Supervised by

Md. SazzadurAhamed

Senior Lecturer

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

22 JULY

APPROVAL

This Project/internship titled “**Computer Networking**”, submitted by **MD: SAZZADURAHMED**, ID No: 172-15-10099 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on July 22, 2020.

BOARD OF EXAMINERS



Dr. Syed Akhter Hossain
Professor and Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Subhenur Latif
Assistant Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

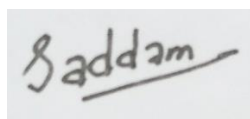
Internal Examiner



Raja Tariqul Hasan Tusher
Senior Lecturer

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md. Saddam Hossain
Assistant Professor

Department of Computer Science and Engineering
United International University

External Examiner

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Md. Sazzadur Ahamed, Computer Networking, Department of CSE** at Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

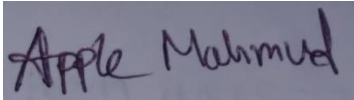
Supervised by:



Md. Sazzadur Ahamed

Senior Lecturer
Department of CSE
Daffodil International University

Submitted by:



Md. Apple Mahmud

Id Number: 172-15-10099
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Md. SazzadurAhamed, Senior Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “Networking” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to the Almighty Allah and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

Computer Networks have come to be an essential tool in many aspects: human communication, gathering, trade and sharing of information, dispensed work environments, access to faraway assets (data and computing power) and many more. Starting from an historical overview, this paper will provide an introduction to the underlying ideas and technologies. The second half of will pay attention on the most frequently used network technology these days (Ethernet and TCP/IP) and supply an introduction to the conversation mechanisms used.

As a networking professional, I will domesticate industry-supported skills and credentials that I will be in a position to transfer to future employment opportunities. With the CCNA certification, I will be in a position to display and promote the truth that I have the necessary skills to do job efficiently and you are certified by means of the leader in Network Technologies.

TABLE OF CONTENTS

CONTENTS	PAGE
Approval	i-ii
Declaration of the Student	ii
Acknowledgement	iii
Abstract	iv
CHAPTER 1:	
INTRODUCTION	
1.1 Introduction to Networks	1
1.2 Networking Types	2
1.3 Internship Objectives	3
1.4 Introduction of Company	3
1.5 Report Layout	3
CHAPTER 2:	
IP ADDRESSING AND SUBNETS	
2.1 IP address	4-5
2.2 Private and Public IP addresses	5
2.3 Subnetting	6-7
2.4 Variable Length Subnet Masks (VLSM)	7-10
CHAPTER 3:	
INTRODUCTION TO CISCO DEVICES	
3.1 Introduction to Router and Switch	11-12
3.2 Configuring DNS & DHCP	12-20
3.3 Password Recovery	21-22

CHAPTER 4:

INTRODUCTION TO IP ROUTING

4.1	IP Routing	23
4.2	Static and Dynamic Routing Protocols	23-
4.3	ACL (Access Control Protocol)	24-36

CHAPTER 5:

SWITCHING AND SPANNING TREE PROTOCOL

5.1	Ether Channel	37-39
5.2	Port Security	39-40
5.3	STP	40-47

CHAPTER 6:

VLANs AND VTP

6.1	Virtual LANs (VLANs)	48-50
6.2	VLAN Trunking Protocol (VTP)	50-54
6.3	Inter-VLAN Routing	54-55

CHAPTER 7:

NETWORK SECURITY

7.1	Network Security	56-58
7.2	Cisco Firewalls	58-60
7.3	Layer 2 Security	60-65

CHAPTER 8:

FUTURE OPPERTUNITY & CONCLUTION

8.1	Conclusion of Internship	66
8.2	Future Opportunity for Career	66

**APPENDIX
REFERENCE**

67-69

LIST OF FIGURES

FIGURE	PAGE
Figure 2.2.1: Subnetting Ex	6-7
Figure 2.4.1: Variable Length Subnet Masking	8
Figure 3.1.1: Shows the front panel of the router.	11
Figure 3.1.2: Shows the front panel of the switch.	12
Figure 3.2.1: Configuration DHCP on Router	13
Figure 3.2.2: Server Configuration.	15
Figure 3.2.3: DHCP Configuration on Desktop.	16
Figure 3.2.4: Configuration Static IP address on Desktop.	17
Figure 3.2.5: Configuration Static IP address on Desktop.	18
Figure 3.2.6: Configuration Static IP address on Desktop.	19
Figure 3.2.7: Configuration DNS server.	20
Figure 4.2.1: Configuration Static Routing Protocol.	24
Figure 4.2.2: Configuration Dynamic Routing Protocol.	28
Figure 4.2.3: Configuration Border Gateway Protocols	31
Figure 4.2.4: A Protocol for Configuration ACL	34
Figure 5.1.1: EtherChannel or link aggregation	37
Figure 5.1.2: EtherChannel allows spanning tree	38
Figure 5.3.1: Spanning tree protocol	41
Figure 6.1.1: VLAN configuration.	49-50
Figure 6.2.1: VTP server configuration	52
Figure 6.3.1: Inter VLAN routing	55
Figure 7.1.1: Computer Network	57
Figure 7.3.1: Port Security.	62
Figure 7.3.2: How Trunk link work	64

CHAPTER 1

INTRODUCTION

1.1 Introduction of Network

Networking is referred as connecting computer systems electronically for the motive of sharing information. Resources like files, applications, printers and software program are frequent facts shared during a networking. The advantage of networking is often considered sincerely in phrases of security, efficiency, manageability and fee effectiveness because it allows collaboration between customers during a huge range. Basically, community consists of hardware component like computer, hubs, switches, routers and other units which shape the community infrastructure. These are the gadgets that play an important position in records transfer from one area to a different the usage of unique science like radio waves and wires. There are many sorts of community handy within the networking industries and therefore the commonest network are Local Area Network (LAN) and Wide Area Network (WAN). LAN community is formed from two or greater computer systems connected together during a short distance generally reception , office constructions or school. WAN may be a network that covers wider location than LAN and typically covers cities, international locations and therefore the total world. Several predominant LAN are often join collectively to shape a WAN. As countless devices are connected to network, it's essential to make sure data collision does not happened when this units attempt to use facts channel simultaneously. a group of policies called Carrier Sense Multiple Access / Collision detection are wont to become conscious of and stop.

Before you learn Cisco Internetworking, it's important to know what a network is and therefore the importance of networks themselves. Simply put, a network may be a collection of interconnected devices (such as computers, printers, etc.) we will tell also networking is that the exercise of linking two or more computing units together for the explanation for sharing data. Networks are built with a combine of pc hardware and pc software.

1.2 Networking Types

As you recognize a network may be a collection of devices connected together. There are three sorts of networks

- **Local Area Network (LAN)**
- **Metropolitan Area Network (MAN)**
- **Wide Area Network (WAN)**

Local Area Network (LAN): LAN or Local Area Network connects community units in such a way that private pc and workstations can share data, tools and programs. The team of computers and devices are linked collectively with the help of a switch, or stack of switches, employing a personal addressing scheme as described by means of the TCP/IP protocol. Private addresses are special in reference to other computer systems on the nearby network. Routers are determined at the boundary of a LAN, connecting them to the larger WAN.

Metropolitan Area Network (MAN): MAN or Metropolitan area Network covers a bigger area than that of a LAN and smaller area as in contrast to WAN. It connects two or greater computer systems that are apart however resides within the equal or distinct cities. It covers a huge geographical vicinity and should additionally function an ISP (Internet Service Provider). MAN is meant for clients who need a high-speed connectivity. Speeds of MAN tiers in phrases of Mbps. It's difficult to diagram and preserve a Metropolitan Area Network.

Wide Area Network (WAN): WAN or Wide Area Network may be a laptop network that extends over a huge geographic area , although it's going to be constrained inside the bounds of a nation or country. A WAN need to be a connection of LAN connecting to different LAN's through smart phone strains and radio waves and may additionally be confined to workplace (a company or an organization) or available to the general public . The science is high speed and incredibly highly-priced.

1.3 Internship Objectives

I have finished my internship within the period of 3 months. As I already finished my internship

And my next target is to build my career in “**Networking**”. Initially I started **CCNA** course. My intern company goal is to build and train me, directly for job markets requirements. Now this days in Bangladesh and there are many opportunities for networking sector So, I can say in Bangladesh & outside of Bangladesh, I have good chance to get jobs. If I’m able to delivery my 3 month period experience in perfectly then I will able to get good jobs and also successful achieved my life goals. In future I have a plan to open my own firm in Bangladesh.

1.4 Introduction of Company

New Horizons is an Information Technology (IT) institute in **Momtaz Plaza 3rd Floor, Road No 4, Dhaka 1205, Dhaka**. Since it is a training institute they provide training on some IT related topics like Web design & development, Web graphics, Software development, Web applications, Database solutions, Domain and hosting services.

1.5 Report Layout

My report, I mentioned basic concepts of CCNA that I learn through this 3 month period of time. In “**chapter 1**” I discusses about basic introduction of internship, my motivation and objectives of my life. I also provide a short description of my interned company. In the “**chapter 2**” I provide a brief description about my interned IT **Company and their services**. In “**chapter 3**” I brief describe about what was my task, roles and activities in period of internship. Every works that I have done I write on it and given an example of that I done.

CHAPTER 2

IP ADDRESSING AND SUBNETS

2.1 IP Addressing

An Internet Protocol address (IP address) may be a numerical label assigned to each machine connected to a pc community that creates use of the web Protocol for communication. An IP tackle serves two predominant functions: host or community interface identification and area addressing.

- **Bit** – a touch may be a single digit with a fee of 0 or 1.
- **Byte** –Eight bits synthesis a byte.
- **Octet** – An octet is additionally made from eight bits. Throughout this chapter the phrases byte and octet are interchangeable.
- **Network Address** – This refers to a foreign network in terms of routing. All hosts within the faraway community fall inside this address.

An IP address is 32 bits long . to form the address simpler to read, it's divided into 4 sections of 8 bits every divided via a period. Each section is therefore, 1 byte (also referred to as octet) long. To similarly make it simpler to look at and remember, the binary numbers are converted to decimal.

- **Class A** – the primary byte (8 bits) is that the network component and therefore the remaining three bytes (24 bits) are host component (network.host.host.host). This class is for an internetwork with small number of networks and enormous number of hosts per networks
- **Class B** – the primary two bytes (16 bits) are the network component and therefore the remaining three bytes are host components (network.network.host.host). This class bridges the gap between Class A and sophistication C by providing for medium number of networks with medium number of hosts.

- **Class C** –The first three bytes (24 bits) are the network component and therefore the last byte (8 bits) is that the host components (network.network.network.host). This class provides for giant number of networks with fewer hosts per network.
- **Class D** – Used for multicasting.
- **Class E** – Reserved addresses

2.2 Public And Private IP Address

Public IP address

A public IP address is that the address that's assigned to a computer system to permit direct get admission to over the web . A internet server, electronic message server and any server system at once handy from the web are candidate for a public IP address. A public IP tackle is globally unique, and may only be assigned to a singular device.

Private IP Address

A private IP address is that the address area allocated through InterNIC to allow organizations to make their own private network. There are three IP blocks (1 classification A, 1 B and 1 category C) reserved for a personal use. The computers, capsules and smart phones sitting at the rear of your home, and therefore the pc systems within organizations are normally assigned private IP addresses. A community printer living in your domestic is assigned a personal tackle in order that only your family can print to your local printer.

2.3 Subnetting

Subnetting is that 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 published domain

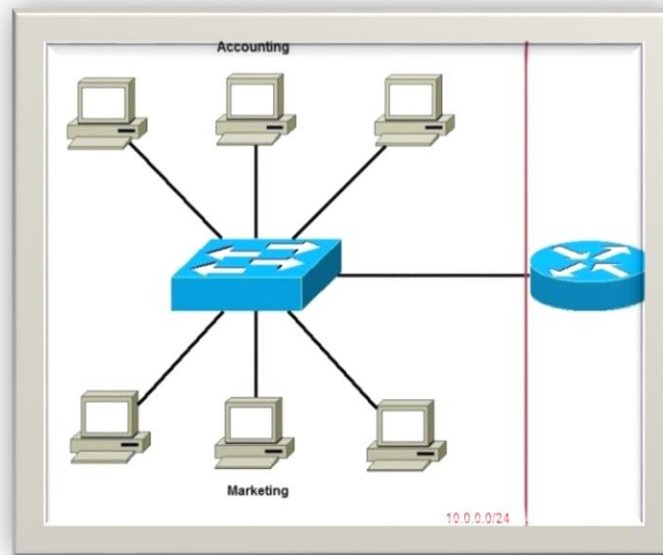


Figure 2.2.1: Subnetting Ex.

In the picture above we have got one huge network: 10.0.0.0/24. All hosts on the network are within an equivalent subnet, which has the next disadvantages:

A single broadcast domain – all hosts are within an equivalent broadcast domain. A broadcast sent by any device on the network are getting to be processed by all hosts, creating many unnecessary traffic. **Network security** – each device can reach the opposite device on the network, which can present security problems. as an example, a server containing sensitive information shouldn't be within an equivalent network as user's workstations. **Organizational problems** – during an outsized networks, different departments are usually grouped into different subnets. as an example, you will be ready to group all devices from the Accounting department within an equivalent subnet then give access to sensitive financial data only to hosts from that subnet. The network above could also be subnetted like this:

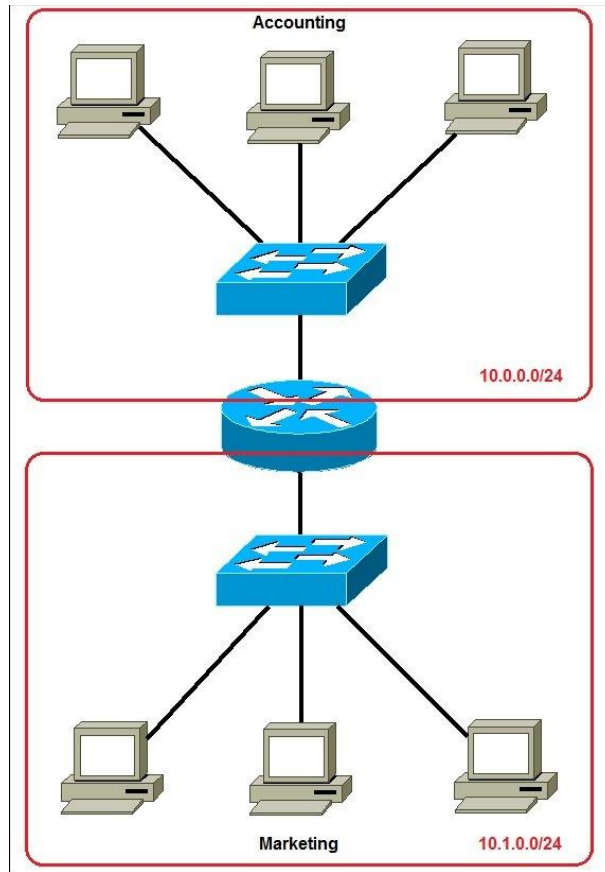


Figure 2.2.2: Subnetting Ex.

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

2.4 Variable Length Subnet Masks (VLSM)

Variable Length Subnet Masking – VLSM – might be a way that permits network administrators to divide an IP address space into subnets of varied sizes, unlike simple same-size Subnetting. Variable Length Subnet Mask (VLSM) during how, means

subnetting a subnet. For further simplification, VLSM is to break IP addresses into subnets (multiple layers) and assign them according to the individual needs of a network. It's going to even be called a classless IP addressing. A classful addressing follows the ultimate rule that has been proven to amount to IP address wastage.

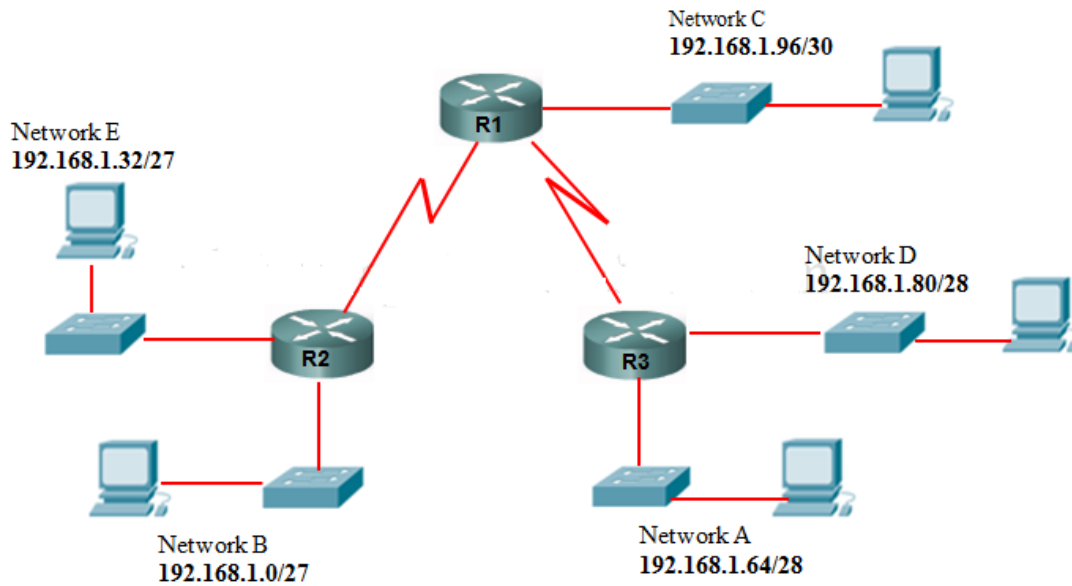


Figure 2.4.1: Variable Length Subnet Masking

The first thing to seem out for is that the number of subnets and number of hosts. during this case, an ISP allocated 192.168.1.0/24. Class C

HQ = 50 host

RO1 = 30 hosts

RO2 = 10 hosts

2 WAN links We will attempt to subnet 192.168.1.0 /24 to sooth this network which allows a complete number of 254 hosts i like to recommend you get conversant in this table below. I never leave home without it!

Table 2.4.1: Subnet extraction table.

Remember the cram table:-

Bit Value	128	64	32	16	8	4	2	1
Bits Borrowed	1	2	3	4	5	6	7	8
Subnet mask	128	192	224	240	248	252	254	255
Subnet Prefix /CIDR	/25	/26	/27	/28	/29	/30		

Let's begin with HQ with 50 hosts, using the table above:

We'll borrow 2 bits with the value of 64. This is often the closest we will get for 50 hosts.

HQ – 192.168.1.0 /26 Network address

HQ = 192.168.1.1 Gateway address

192.168.1.2, First usable address

192.168.1.62- Last usable address. Total address space -192.168.1.2 to 192.168.1.62

192.168.1.63 are going to be the printed address (remember to order the primary and last address for the Network and Broadcast)

HQ Network Mask 255.255.255.192 – we got the 192 by adding the bit value from the left to the worth we borrowed = 128+64=192

HQ address will appear as if this 192.168.1.0 /26

RO1= 30 hosts

We'll borrow 3 bits with the value of 32; this again is that the closest we will get to the amount of host needed.

RO1 address will start from 192.168.1.64 – Network address

Now we will add 64 to 32 we had to borrow before = 32+64 = 96

RO1 = 192.168.1.65 Gateway address

192.168.1.66 – First usable IP address

192.168.1.94 – Last usable IP address

192.168.1.95 Broadcast address – total address space – 192.168.1.66 –192.168.1. 94

Network Mask 255.255.255.224 I.e. 128+64+32=224 or 192.168.1.64/27

RO2 = 192.168.1.96 Network address

We borrow 4 bits with the worth of 16. That's the closest we will go.

$96+16=112$ So, 192.168.1.97- Gateway address

192.168.1.98 – First usable address

192.168.1.110 – Last usable address

192.168.1.111 broadcast

Total host address space – 192.168.1.98 to 192.168.1.110

Network Mask 255.255.255.240 or 192.168.1.96 /28

WAN links = we are borrowing 6 bit with value of $4=112 + 4 =116$

WAN links from HQ to RO1 Network address are going to be 192.168.1.112 /30:

HQ se0/0 = 192.168.1.113

RO1 se0/0= 192.168.1.114

Mask for both links= 255.255.255.252 (we got 252 by adding the bits value we borrowed i.e

$124 +64 +32 +16+ 8 +4=252$

WAN Link 2= $112+4=116$

WAN Link from HQ to RO2 Network address = 192.168.1.116 /30

HQ = 192.168.1.117 subnet mask 255.255.255.252

RO2 = 192.168.1.118 Subnet mask 255.255.255.252

CHAPTER 3

INTRODUCTION TO CISCO DEVICES

3.1 Cisco Integrated Services Router (ISR) Cisco provides various series and models of routers geared towards differing types of customer and requirements. variety of them just do routing whereas others provide another functions like Wireless connectivity, security measures and Voice-over-IP services. Cisco ISR series routers are provide a variety of services.. the sooner CCNA exams used to concentrate on Cisco 2500 and 2600 routers that are replaced by ISR 1800 and 2800/2900 series routers. 2500 and 2600 routers to the end of his life, and now cannot be purchased from Cisco. Figure 3-1 shows a component of the backplane of a Cisco 1841 router with important parts labeled. These parts are described in fig 3-1.

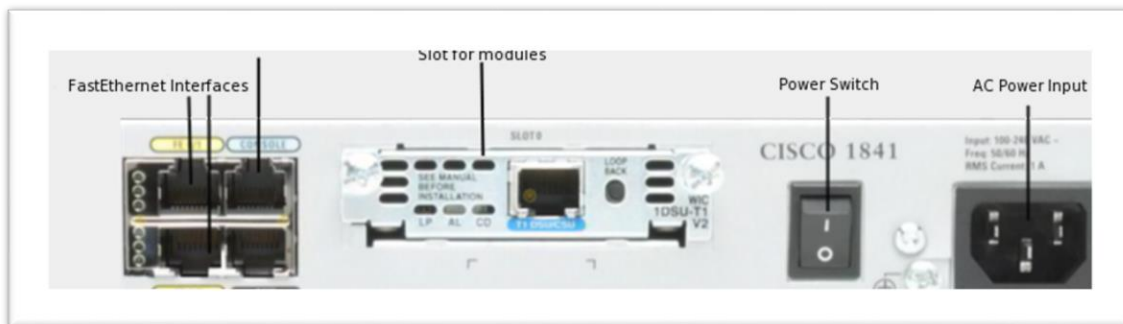


Figure 3.1.1: Shows the front panel of the router.

Cisco Catalyst Switches Cisco provides an honest range of switches under its Catalyst brand. The Catalyst brand encompasses many series of switches with each series targeting a specific part or size of a network. The CCNA exam focuses on the 2960 series of switches within the Catalyst brand. 2960 switches are low-cost wiring closet switches that you simply simply would expect to be used at the Access layer (remember the Cisco Hierarchical model) for providing network connectivity to hosts

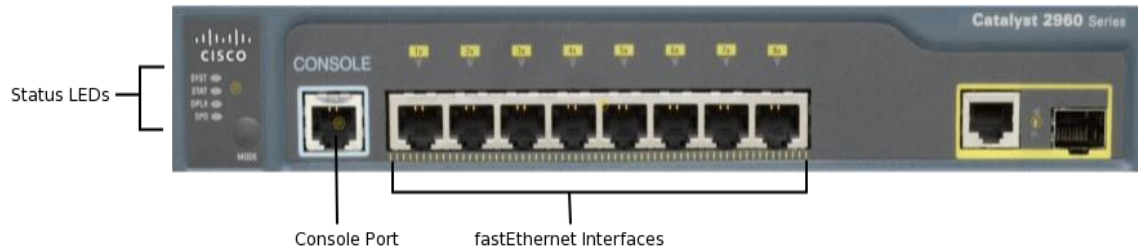
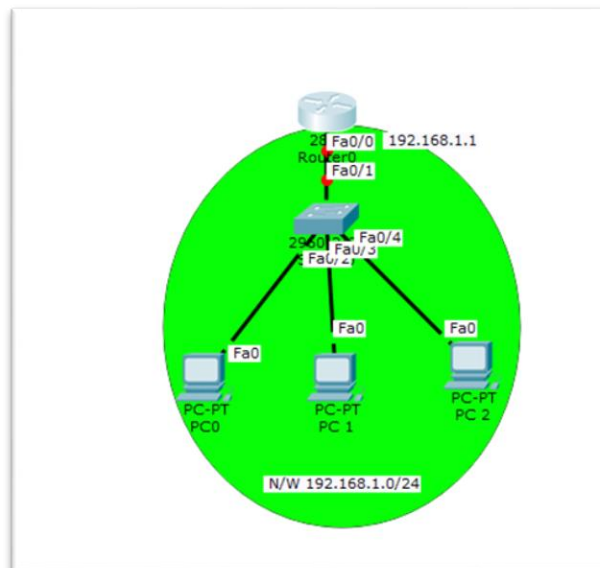


Figure 3.1.2: Shows the front panel of the switch.

3.2 Configuring DHCP & DNS

Configuring DHCP DHCP server both on a router and on a generic server in Cisco Packet Tracer. In both cases, configuration is straightforward as long as you've got a basic knowledge of IP addressing. On thereto then! Configuring DHCP server on a Router.

Build the network topology:



On the router, configure interface fa0/0 to act because the default gateway for our LAN.

```
Router>enable
```

```
Router#config terminal
```

```
Router(config)#int fa0/0
```

```
Router(config-if)#ip add 192.168.1.1 255.255.255.0
```

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

```
Router(config-if)#exit Router(config-if)#exit
```

Configure the DHCP server on the router. IP addresses assigned to the host server, we'll define a dieicasipi pool, a default gateway for the LAN and DNS server.

```
Router(config)#
```

```
Router(config)#ip dhcp pool LAN
```

```
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
```

```
Router(dhcp-config)#default-router 192.168.1.1
```

```
Router(dhcp-config)#dns-server 192.168.1.1
```

Ip dhcp configuration, we can add an extended-address command when the clients address 192.168.1.1 192.168.1.1 through the router can be configured to exclude the router addresses. Except IP DHCP - The address command cannot store permanently assigned addresses on key hosts.

Now go to each PC and IP Configuration tab, enable dieicasipi. Each PC an IP address, default gateway and DNS server to be prepared to get in,

Click PC1-> Desktop-> IP Configuration then Enable DHCP:

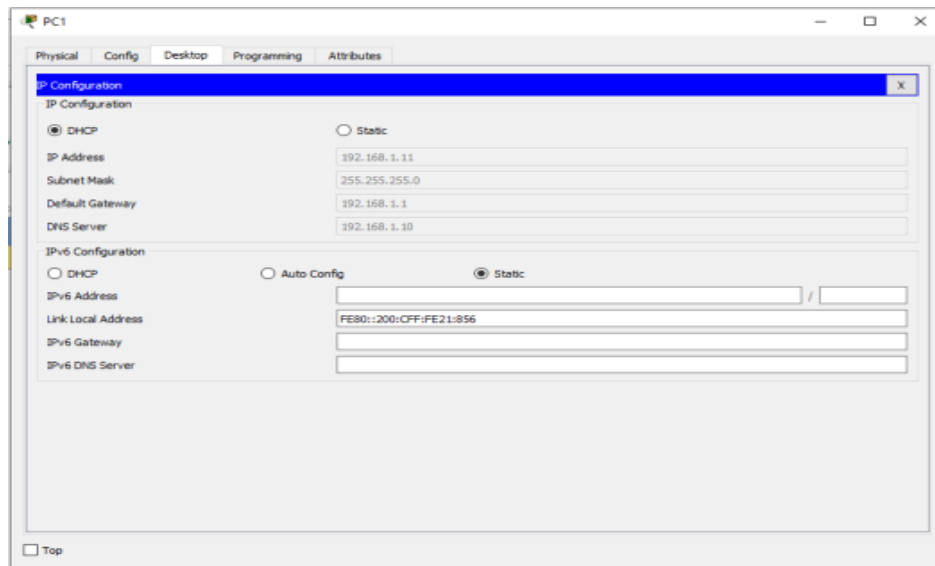
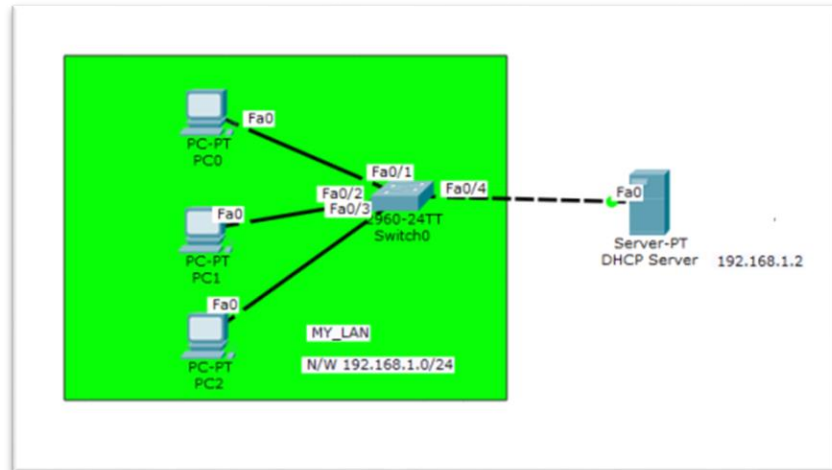


Figure 3.2.1: Configuration DHCP on Router

Get it for other PCs. A router is now engaged in the generic server to let things like:

Create a network topology in packet tracer



Configure the server address fixed EP (192.18.1.2/24).

Configure the generic server DHCP Service.

To do this, click on the server, then click the Services tab. You can choose the menu dhcp. Proceed then DHCP Network parameters can be defined as the following: Pool name: LAN

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.2

Start IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Maximum Number of users: 256

Save and then click Add. dhcp entry has been included in the list.

The server configuration includes:

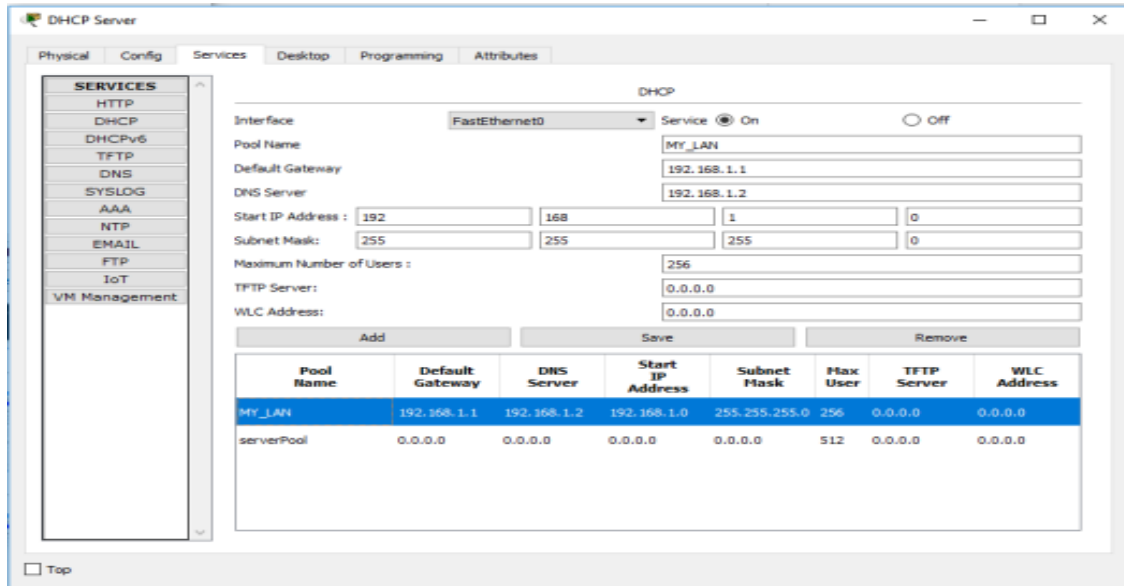


Figure 3.2.2: Server Configuration.

ON the bottom in DHCP service

Finally, enable the configuration of each PC dhcp. The PC will be configured automatically. Here is that the DHCP configuration on PC1:

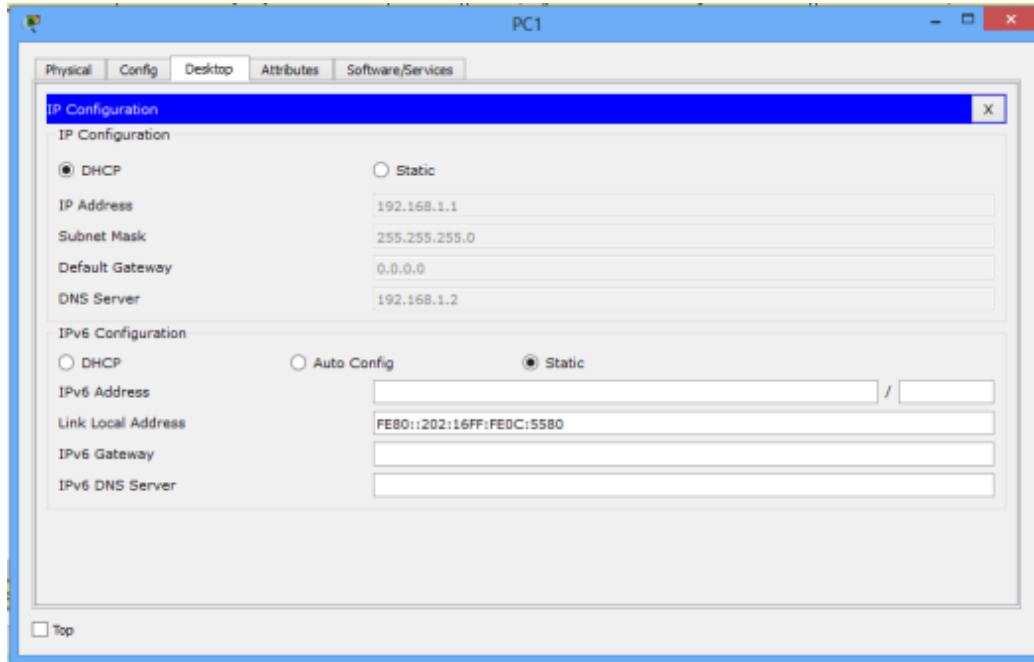
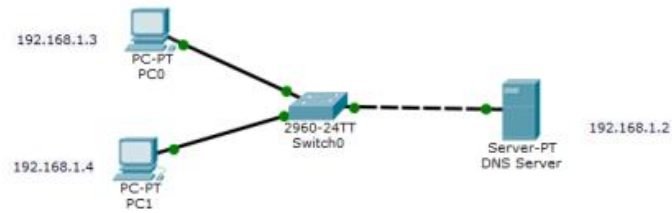


Figure 3.2.3: DHCP Configuration on Desktop.

Configuring DNS A Domain Name System (DNS) server to resolve host names to IP addresses. Although we are able to access a network using the IP address of the host, DNS lets us use domain names are easy to recall. For example, if you type `http://www.google.com` `http://208.117.229.214` than typing easier to access Google websites. In both cases, you can access the Google website is definitely easier to use the name. Now, a host using a DNS service before, we first need to configure a DNS server. For example, once you type in the URL in your browser to `http://www.google.com`, then the DNS server will ask for the IP address of the host `http://www.google.com`. DNS server IP address and the IP address of the host that will solve `http://www.google.com` will answer.

Create the network topology.



Configure the PC and server IP addresses are fixed.

IP Address: 192.168.1.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1

DNS Server: 192.168.1.2

Server

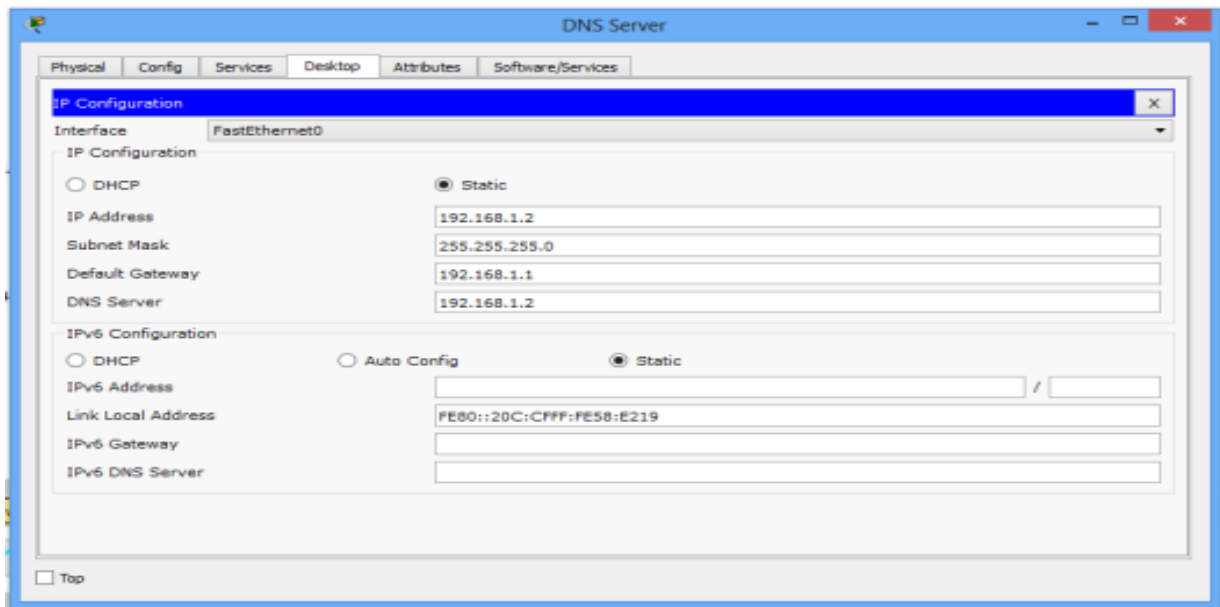


Figure 3.2.4: Configuration Static IP address on Desktop.

PC0

IP add: 192.168.1.3 **Subnet mask:** 255.255.255.0

Default gateway: 192.168.1.1 **DNS server:** 192.168.1.2

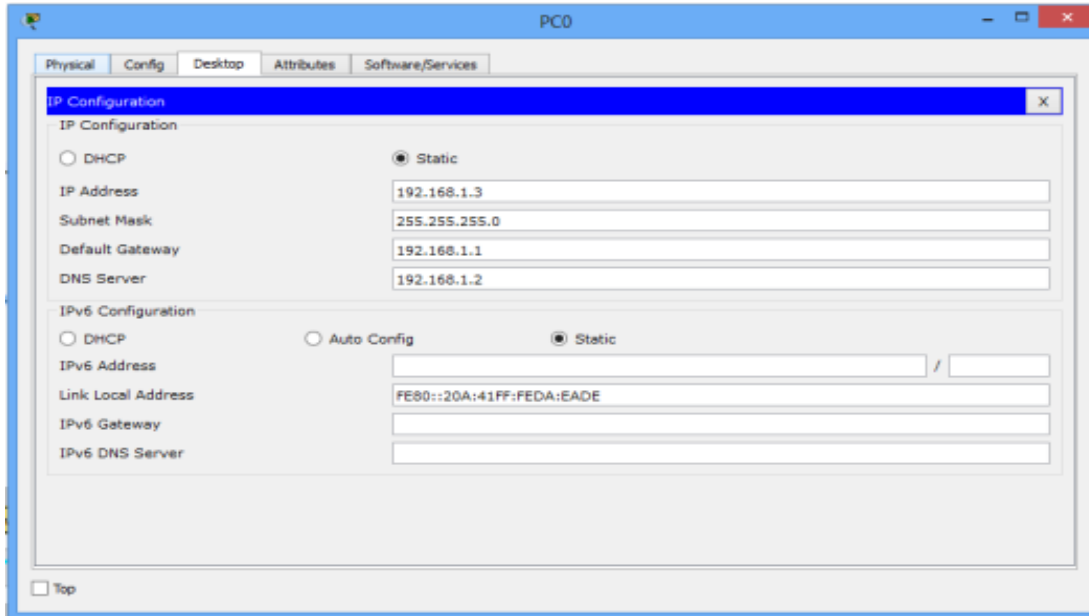


Figure 3.2.5: Configuration Static IP address on Desktop.

PC1 IP address: 192.168.1.4 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 DNS Server: 192.168.1.2

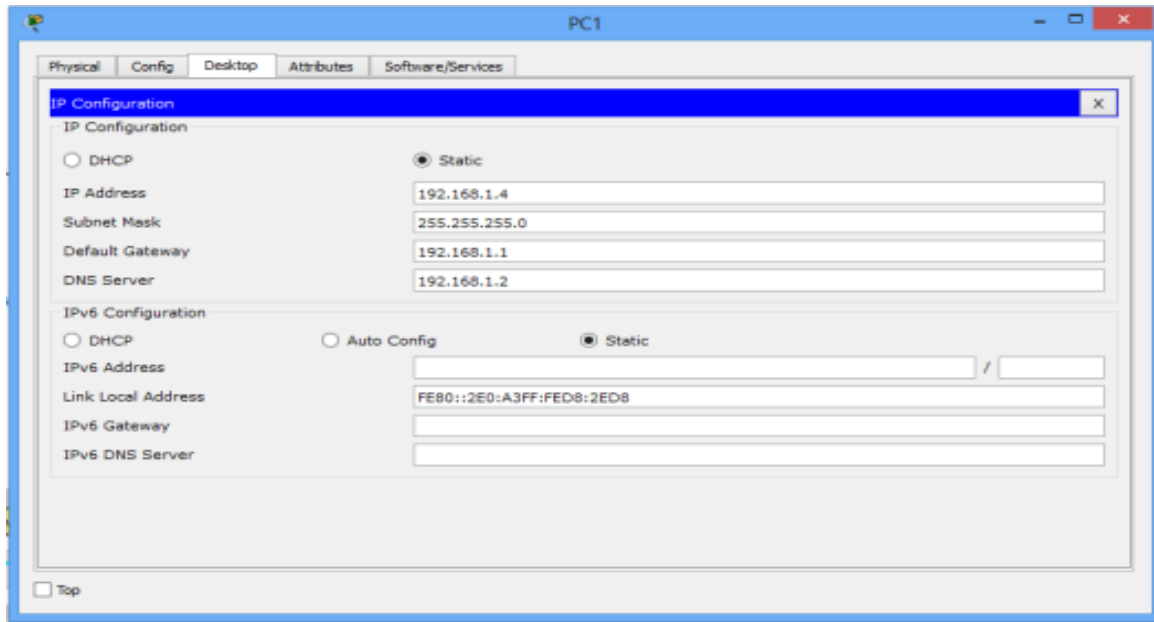


Figure 3.2.6: Configuration Static IP address on Desktop.

Configure the PC and server IP addresses are fixed.

IP address: 192.168.1.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 DNS Server: 192.168.1.2

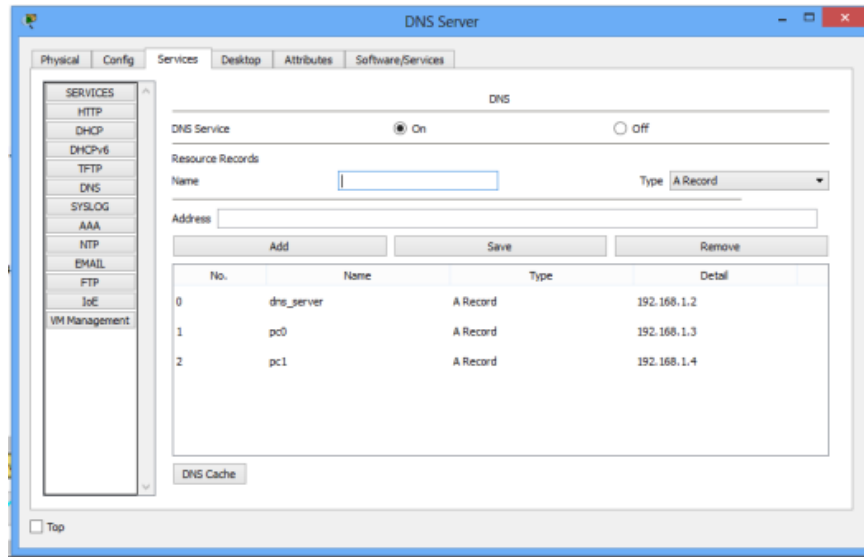
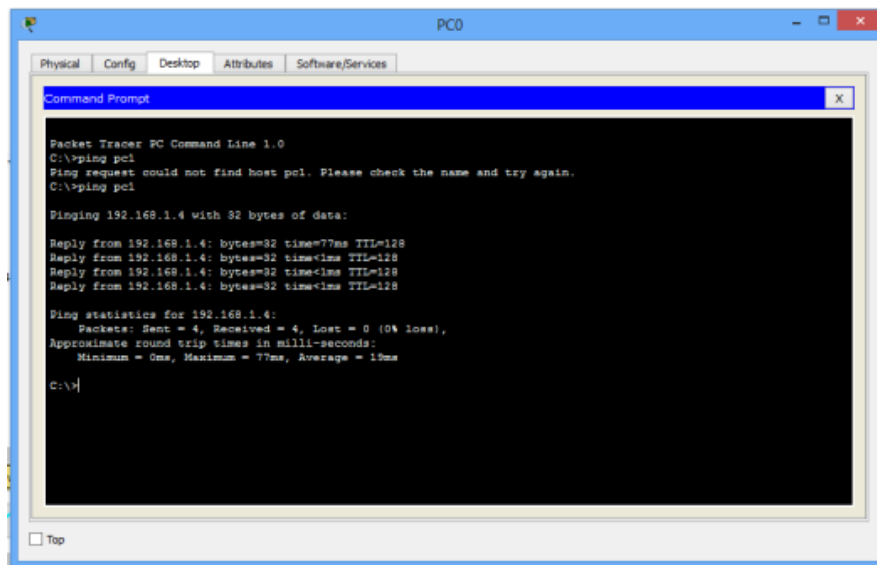


Figure 3.2.7: Configuration DNS server.

Experiment Name - IP resolution. Instead of using the IP address of the host name to Ping. If the DNS service is on each IP configuration is correct, then it should be done Ping. For example, PC 1 PC 1. Ping should be achieved.



3.3 Password Recovery on a Cisco Router

When working with iOS-based devices, forgotten passwords and locked out of your own devices are not unusual. Password recovery method differs from device to device, but the most common procedure for the Cisco router password recovery has. Cisco switches can be somewhat different for the passwords to be restored and is covered on CCNA, so these categories shows the router password recovery procedure.

Step1: We've set the password before you can retrieve your password

```
Router>enable
Router#configure terminal
Router(config)#hostname Newhorizons
Newhorizons(config)#line console 0
Newhorizons(config-line)#pass cisco123
Newhorizons(config-line)#login
Newhorizons(config-line)#exit
Newhorizons(config)#line aux 0
Newhorizons(config-line)#pass cisco456
Newhorizons(config-line)#login
Newhorizons(config-line)#exit
Newhorizons(config)#line vty 0 4
Newhorizons(config-line)#pass cisco789
Newhorizons(config-line)#login
Newhorizons(config-line)#exit
Newhorizons(config)#service password-encryption
Newhorizons(config)#enable secret cisco
Router0 Newhorizons(config)#exit
```

Step2: We need to verify that the password is set by using this command

```
Newhorizons#sh run
Newhorizons#copy running-config startup-config
Newhorizons#write
```

Step3: And now we have the password recovery or re-set for our router version, because the password of an article will be saved and the router at boot time, we router to reset, and when we **Ctrl+Break/Pause** Use this

```
rommon 1 > confreg 0x2142
rommon 2 > reset
Router>enable
Router#show version
Router#conf t

Router(config)#line con 0
Router(config-line)#no pass
Router(config-line)#exit
Router(config)#line aux 0
Router(config-line)#no pass
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#no pass
Router(config-line)#exit
Router(config)#no enable pas
Router(config)#no enable secret
Router(config)#exit
```

CHAPTER 4

INTRODUCTION TO IP ROUTING

4.1 IP Routing

Previous chapter, we learn to configure a Cisco router to connect to the network because it can be managed remotely and in other things. The time has finally come for routers to do one of the most important things - IP routing time. You already know that routers monitor the destination IP address of a packet and take it to the destination.

There is three types of IP Routing

- Static Routing
- Dynamic Routing
- Default Routing

4.2 Static Routing Protocol

Routing permanent fixtures and forwarding table that routes are often configured as a fixed route. These routes are generally not changed, and often only one or very few destinations are included in the route. To create a static route to the routing table, the router you must defined as at least stabilize and with a hop address to be added. If the next-hop address is accessible to the routing table, static route forwarding table is inserted. For the entire static route for transit traffic is shifted to the next HAP address. Routing table once installed, you can specify options which include the static route to route defines additional information. All stable options are optional.

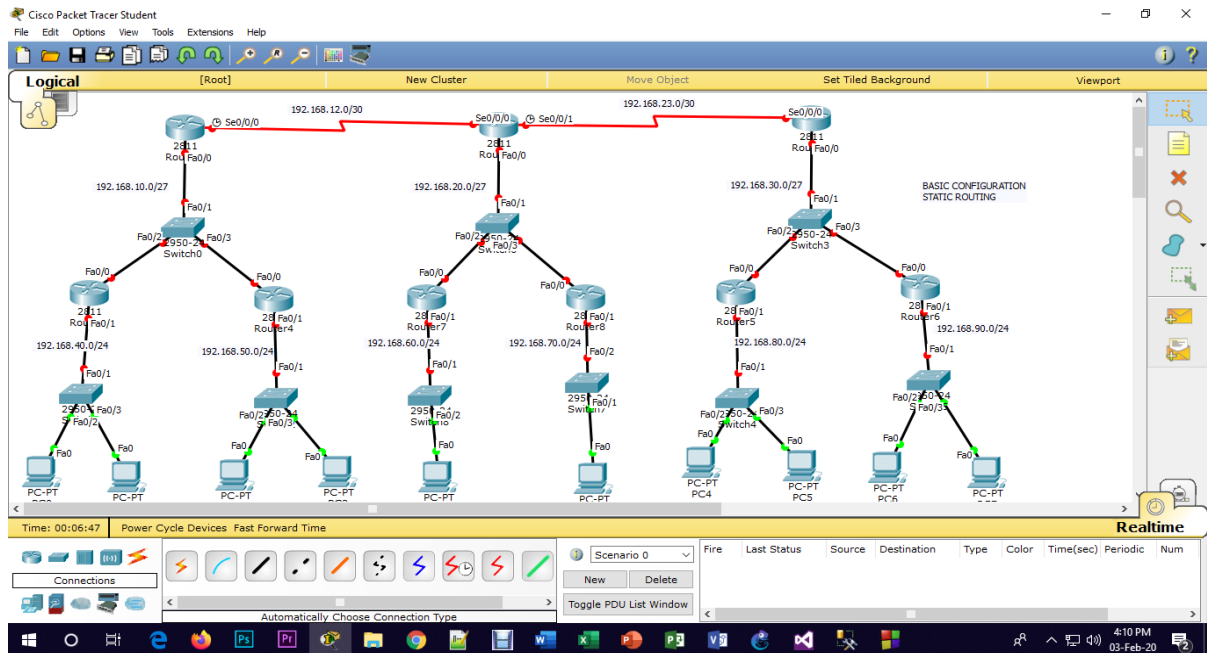


Figure 4.2.1: Configuration Static Routing Protocol.

For Route 1

Router>en

Router#conf t

Router(config)#hostname R1

R1(config)#int s0/0/0

R1(config-if)#no shutdown

R1(config-if)#ip address 192.168.12.1 255.255.255.252

R1(config-if)#exit

R1(config)#int f0/0

R1(config-if)#no shutdown

R1(config-if)#ip address 192.168.10.1 255.255.255.0

R1(config-if)#exit

The same process for next router

For Router 2

```
Router>en
```

```
Router#conf t
```

```
Router(config)#int s0/0/0
```

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

```
Router(config-if)#ip address 192.168.12.2 255.255.255.252
```

```
Router(config-if)#int s0/0/1
```

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

```
Router(config-if)#ip address 192.168.23.1 255.255.255.252
```

```
Router(config-if)#int f0/0
```

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

```
Router(config-if)#ip address 192.168.20.1 255.255.255.0
```

```
Router(config-if)#exit
```

For Router 3

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#int s0/0/0
```

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

```
Router(config-if)#ip address 192.168.23.2 255.255.255.252
```

```
Router(config-if)#int f0/0
```

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

```
Router(config-if)#ip address 192.168.30.1 255.255.255.0
```

```
Router(config-if)#exit
```

This is how configure static router

Dynamic Routing Protocols

Dynamic routing allows routing of data in a networking strategy that could be. Unlike static routing, dynamic routing enables routers to choose a path that is compatible with real-time changes in the layout of the logical network. In dynamic routing, dynamic routing protocol router for routing the operating table, responsible for maintenance and updating. In static routing, this is done manually by the supervisor. Multiple algorithms and protocols that are used in dynamic routing. Most Popular Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Dynamic routing is the easiest and simplest way to configure large networks, choose the easiest route, route identification, and remote networks to discover the changes to be more intuitive. However, they decided to divide the routers update routing takes more bandwidth; the CPU routers and routing protocols as a result of additional RAM might be overloaded. Finally, the static routing, dynamic routing is slightly higher than secured.

Dynamic Routing Protocols has 2 Types:

- IGP (Interior gateway Routing Protocols)
Same Domain
EX: RIP, EIGRP, OSPF
- EGP (Exterior gateway Routing Protocols)
Different Domain
EX: BGP

IGP (Interior gateway Routing Protocols)

IGP Protocols has 3 types:

- Distance Vector Routing Protocols
Hop Count. (RIP)
- Link-state Routing Protocols
Interface Bandwidth (OSPF)
- Advanced Distance Vector Routing Protocols / Hybrid Routing Protocols

Interface:

- 1.Bandwith
- 2.Load
- 3.Delay
- 4.Relaibility
- 5.MTU (Maximum Transfer Unit)

EIGRP

Here I will configure Routing Information Protocols (RIP)

It's open standard Protocol of IGP(Interior Gateway Protocol)

Characteristics:

RIP Version 2

- Metric Cost = Hop Count
- Information Sharing = Multicast (224.0.0.9)
- Convergence = Medium
- Classless & VLSM = Yes
- Version = RIP Version 1, RIP Version 2
- Hello timer = 30 sec
- Hold timer = 180 sec
- Authentication = NO
- Maximum Hop Count = 16 HOP
- 10.Protocol Number = 519
- Algorithm = Bellmanford
- AD (Administrative Distance) Value = 120

Convergence Types

- Very Fast
- Fast
- Medium
- Slow
- Very Slow

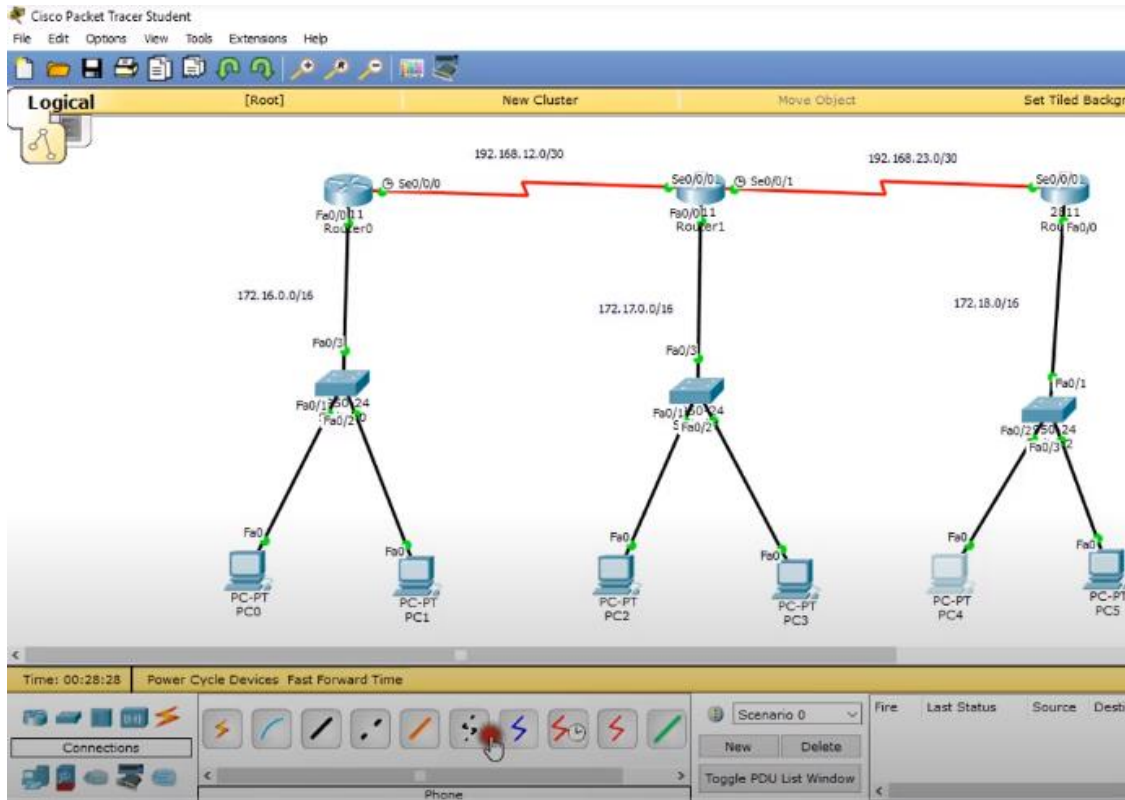


Figure 4.2.2: Configuration Dynamic Routing Protocol.

For Router 1:

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#int s0/0/0
```

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

```
Router(config-if)#ip address 192.168.12.1 255.255.255.252
```

```
Router(config-if)#int f0/0
```

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

```
Router(config-if)#ip address 172.16.0
```

```
Router(config-if)#ip address 172.16.0.1 255.255.0.0
```

For Router 2:

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#int s0/0/0
```

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

```
Router(config-if)#ip address 192.168.12.2 255.255.255.252
```

```
Router(config-if)#int s0/0/1
```

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

```
Router(config-if)#ip address 192.168.23.1 255.255.255.252
```

```
Router(config-if)#int f0/0
```

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

```
Router(config-if)#ip address 172.17.0.1 255.255.0.0
```

For Router 3:

```
Router2 Router>enable
```

```
Router#conf t
```

```
Router(config)#int s0/0/0
```

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

```
Router(config-if)#ip address 192.168.23.2 255.255.255.252
```

```
Router(config-if)#int f0/0
```

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

```
Router(config-if)#ip address 172.18.0.1 255.255.0.0
```

Now we have to show the version of RIP and we have to identify the network

For Router 1:

```
Router(config-if)#do sh ip route
```

```
Router(config-if)#exit
```

```
Router(config)#router rip
```

```
Router(config-router)#version 2
```

```
Router(config-router)#network 172.16.0.0
```

```
Router(config-router)#network 192.168.12.0
```

```
Router(config-router)#exit
```

For Router 2:

```
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.12.0
Router(config-router)#network 192.168.23.0
Router(config-router)#network 172.17.0.0
Router(config-router)#exit
```

For Router 3:

```
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.23.0
Router(config-router)#network 172.18.0.0
Router(config-router)#exit
```

If we want to see which protocol use here then you have to write this command in priviliged moder of any router

```
Router#show ip protocols
```

Border Gateway Protocols(BGP) is OPEN STANDARD Protocol
EGP(Exterior Gateway Protocol)

Characteristics of BGP:

- Metric Cost = 11 Attributes(weights, local preference, locally injected route, AS path length, Origin, MED, IGP metrics, Neighbors Types,Oldest Neighbors,Highest Neighbors-ID,Highest Neighbors IP)
- Information Sharing = Unicast
- Convergence = Very Slow
- Classless & VLSM = Yes
- Types = 2 types (1.Ibgp 2.Ebgp)
- keep Alive = 30 Sec
- Dead timer = 60 Sec
- Authentication = Yes
- Maximum Hop Count = UNLIMITED
- 10.Protocol Number =TCP/179
- 11.AD(Administrative Distance) Value = IBGP(200) EBGP (20)

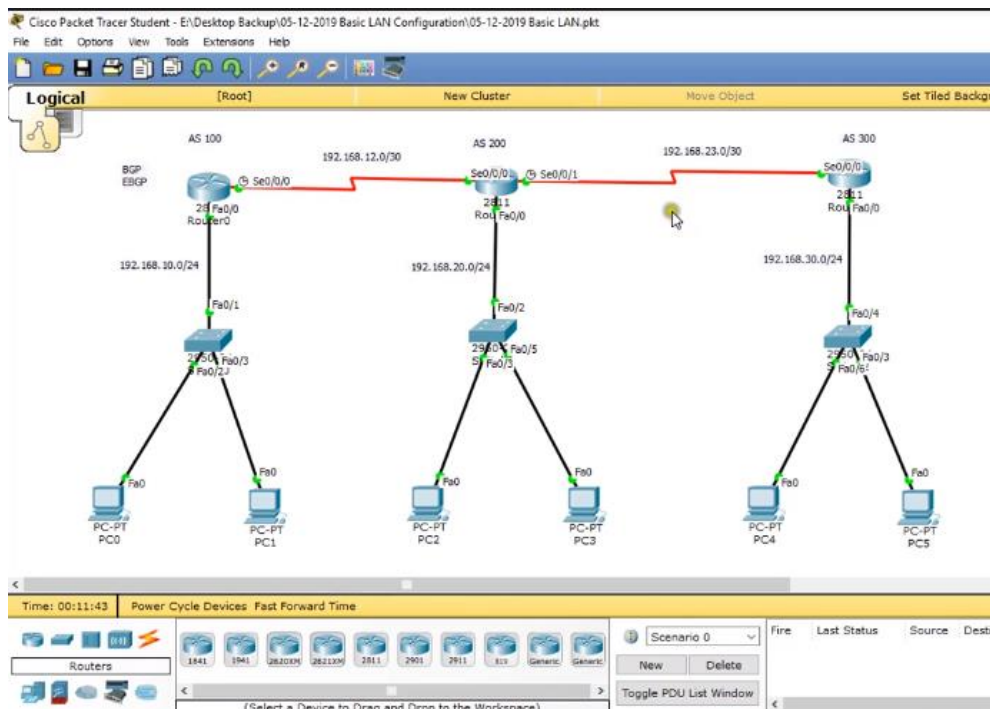


Figure 4.2.3: Configuration Border Gateway Protocols.

For Router 1:

```
R1>enable
```

```
R1#sh ip proto
```

```
R1#sh ip int br
```

```
R1#conf t
```

```
R1(config)#no router eigrp 10
```

Same command for the next router.

For Router 2:

```
R2>en
```

```
R2#conf t
```

```
R2(config)#do sh ip int br
```

```
R2(config)#no router eigrp 10
```

For Router 3:

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#no router eigrp 10
```

For Router 1:

```
R1(config)#do sh ip route
```

```
R1(config)#router bgp ?
```

```
R1(config)#router bgp 100
```

```
R1(config-router)#bgp router-id 1.1.1.1
```

```
R1(config-router)#neighbor 192.168.12.2 remote-as 200
```

```
R1(config-router)#network 192.168.12.0 mask 255.255.255.252
```

```
R1(config-router)#network 192.168.10.0 mask 255.255.255.0
```

```
R1(config-router)#exit
```

For Router 2:

```
R2>enable
```

```
R2#conf t
```

```
R2(config)#router bgp 200
```

```
R2(config-router)#bgp router-id
```

```
R2(config-router)#bgp router-id 2.2.2.2
```

```
R2(config-router)#neighbor 192.168.12.1 remote-as 100
```

```
R2(config-router)#neighbor 192.168.23.2 remote-as 300
```

```
R2(config-router)#network 192.168.12.0 mask 255.255.255.252
```

```
R2(config-router)#network 192.168.23.0 mask 255.255.255.252
```

```
R2(config-router)#network 192.168.20.0 mask 255.255.255.0
```

```
R2(config-router)#exit
```

For Router 3:

```
Router>en
```

```
Router#conf t
```

```
Router(config)#router bgp 300
```

```
Router(config-router)#bgp router-id 3.3.3.3
```

```
Router(config-router)#neighbor 192.168.23.1 remote-as 200
```

```
Router(config-router)#network 192.168.23.0 mask 255.255.255.252
```

```
Router(config-router)#network 192.168.30.0 mask 255.255.255.0
```

```
Router(config-router)#exit
```

For Router 1: you can show the summary to write this command

```
R1(config)#do sh ip route
```

```
R1>en
```

```
R1#show ip route
```

```
R1#sh ip bgp
```

```
R1#sh ip bgp summary
```

4.3 ACL Protocol

Here I will make a list for ACL (Access Control List)

Conditions 1:

- Student dept cannot access to HR
- All other traffic will be allowed

Standard ACL

- Implemented in destination router
- Destination gateway interface
- Range (1-99)

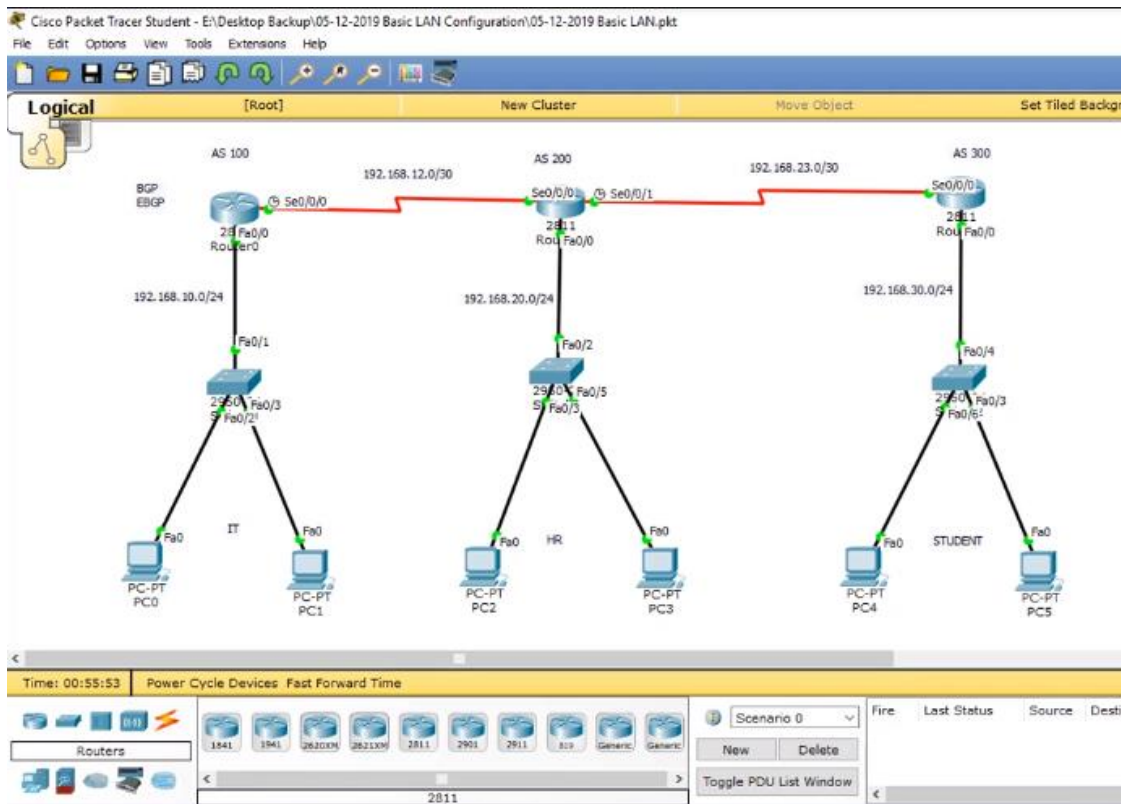


Figure 4.2.4: A Protocol for Configuration ACL

```
R2(config)# access-list 10 deny 192.168.30.0 0.0.0.255
R2(config)# access-list 10 permit any
R2(config)# int f0/0
R2(config-if)# ip access-group 10 out
R2(config-if)# exit
R2(config)# access-list 20 permit host 192.168.30.2
R2(config)# access-list 20 deny 192.168.30.0 0.0.0.255
R2(config)# access-list 20 permit any
R2(config)# int f0/0
R2(config-if)# ip access-group 20 out
R2(config-if)# exit
```

Conditions 3:

- STUDENT dept. pc 192.168.30.2 & pc 192.168.30.3 can not access to HR dept.
- Others network of STUDENT dept can access to HR dept.
- All other Traffic will be allowed.

```
R2(config)# access-list 30 deny host 192.168.30.2
R2(config)# access-list 30 deny host 192.168.30.3
R2(config)# access-list 30 permit any
R2(config)# int f0/0
R2(config-if)# ip access-group 30 out
R2(config-if)# exit
```

Extended ACL

- Implemented in Source Router
- Range (100-199)
- Source Gateway Interface

Conditions 1:

1. STUDENT dept. cannot access to HR dept.
2. All other Traffic will be allowed.

```
R3(config)# access-list 100 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
R3(config)# access-list 100 permit ip any any
```

```
R3(config)# int f0/0
```

```
R3(config-if)# ip access-group 100 in
```

```
R3(config-if)# exit
```

Conditions 2:

- STUDENT dept. pc 192.168.30.2 can only access to HR dept.
- Others network of STUDENT dept can not access to HR dept.
- All other Traffic will be allowed.

```
R3(config)# access-list 110 permit ip host 192.168.30.2 192.168.20.0 0.0.0.255
```

```
R3(config)# access-list 110 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
R3(config)# access-list 110 permit ip any any
```

```
R3(config)# int f0/0
```

```
R3(config-if)# ip access-group 110 in
```

```
R3(config-if)# exit
```

CHAPTER 5

SWITCHING AND SPANNING TREE PROTOCOL

5.1 EtherChannel:

Ethernet Switch Ethernet switch with higher realized bandwidth used in the process can be understood as a collection of links to ports or etherchannel. Together to interconnect switches, and other devices when connected to a switch, consolidation is often useful links. No more than one network adapter that allows you to connect to the server after a switch or switch interconnection of two distribution etherchannel be able to use later. When Ethernet switches interconnect multiple physical interfaces are used to help improve the operation of the etherchannel. traditional network function more traditional Layer 2 loops avoid unnecessary spanning-tree protocol link block, which etherchannels that it links the reduction of traffic using the balance on the balance; This helps to improve the efficient use of bandwidth. Switch-port regarded as a logical bundle etherchannel spanning tree and bandwidth increased to reflect the cost by adjusting spanning tree.

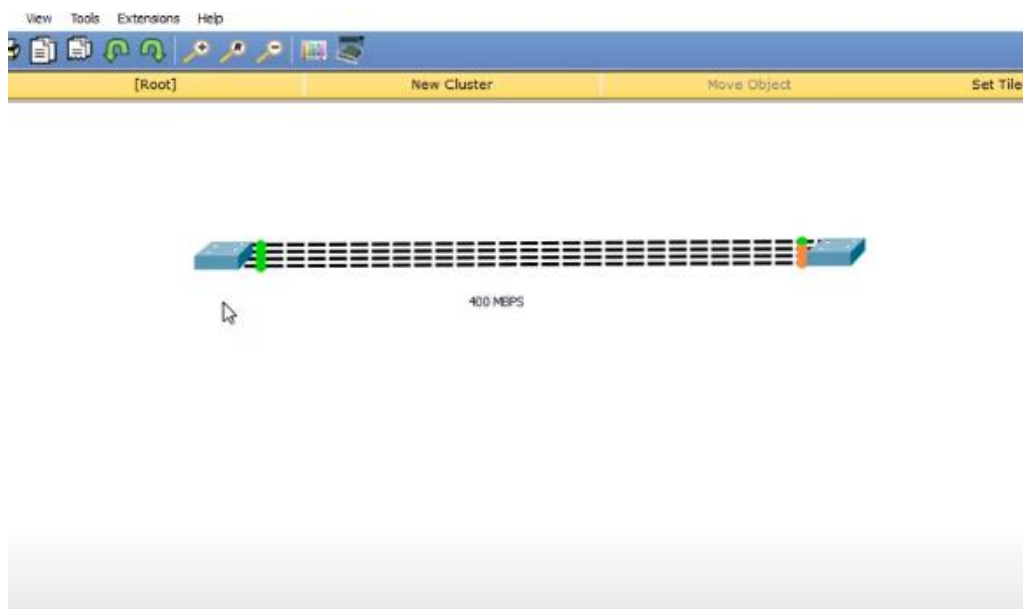


Figure 5.1.1: EtherChannel or link aggregation

Spanning trees block a redundant port link to prevent loops.

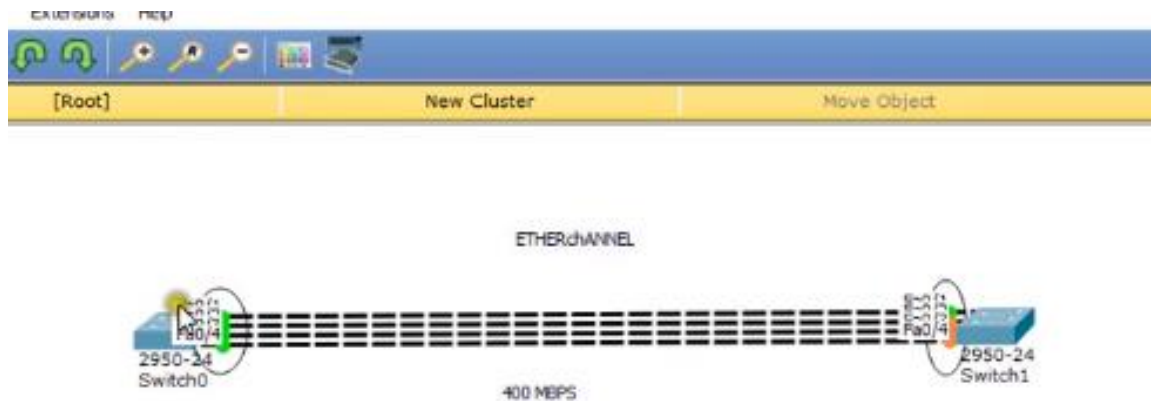


Figure 5.1.2: EtherChannel allows spanning tree

EtherChannel broad tree as two popular port and both ports are considered to be linked to the physical storage mode enables you to manage.

How It's Works

An Ethernet channel group, if no physical link fails, the Ethernet channel bandwidth loses only the link provided. However, if it comes to a copy of the physical link will be added dynamically Ethernet. As a logical switch port etherchannelbundle spanning tree shows and bandwidths increased to reflect the cost by adjusting spanning tree. Together to bundle multiple physical Ethernet ports, you want to use the channel-group command, it is a logical interface allows the port-channel. This is an access port or a port-channel to a trunk port. You can enable Cisco Catalyst Switch with eight 10/100 ports with a port-channel can collect in total, can be found if you are able to collect eight Gigabit port or bundle. A switch can have multiple ports channels.

EtherChannel Protocol

- Port aggregation Protocol(PAgP)
This Cisco-owned port channel protocol negotiation
- Link Aggregation Protocol (LACP 802.3ad)
It has exactly the same purpose as PAgP but it's private

5.2 Port Security:Port Security unknown devices to stop forwarding packets to help protect the network. When the dynamic locked down any link address is released. Port Security feature provides the following benefits:

- You can also limit the amount of the portMAC addresses. Identical MAC address (a protected packet) is provided with forward packets; All other packets (unsecure packet) is limited.
- You can enable each port on the port security.
- Two port security traffic filtering methods, dynamic and static locking by locking. These methods can be used together.

Dynamic locking:The maximum number that can be learned in a port to the Mac addresses. The maximum number of MAC addresses on the platform, and it is the software release notes.After the limit has been reached does not seem to have learned more MAC address. Only a authorizeframes including the Mac address has been forwarded.

Note:If you want to make a port at the MAC address lines, dynamic entries is set to 0, the fixed addresses in the list with only Mac to Mac only allow packets.

Locking dynamic addresses are converted into stable locking address. Dynamically locked MAC addresses if they are not met with another packet of old age.Set in outing value. By dynamically locked MAC addresses learning in another port. Mac does not seem appropriate for the age fixed addresses.

Static locking: You can manually specify a list of addresses to a port, Mac stable. Dynamic locked addresses are converted into stable locking address.

You'll need to enter this command to configure

```
Switch>en
Switch#sh mac-add
Switch#conf tearminal
Switch(config)#int f0/1
Switch (config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#int f0/1
Switch(config-if)#no shutdown
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

5.3 Spanning tree protocol: spanning Tree Protocol (STP), the switch is made from the local area network (LAN), loop-free topology ensures. Disrupt the normal activity of a network failure cannot link so a lot of redundant links should be switched worst quality. Physical switching loops, which may introduce arbitrary redundant links. STP loops and prevents errors related to the body to allow for additional work.

Spanning Tree Protocol standard as IEEE 802.1D. Several operations were launched to increase the quality of the STP Cisco, which was included as the WP AP802.1w Rapid Span Tree Protocol (RSTP).

During this chapter, we Tree Protocol (STP) configuration and verification commands to specialization, as Cisco switch was applied. Figure 1 Cisco Catalyst 3550 switch, including three that have been used in the topology.

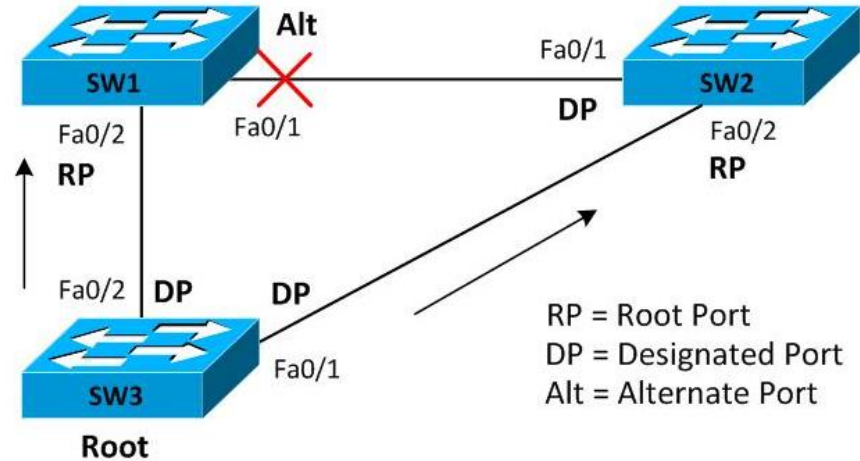


Figure 5.3.1:Spanning tree protocol

There are three trunk links in above:

- SW1 Fa0/1 – SW2 Fa0/1
- SW2 Fa0/2 – SW3 Fa0/1
- SW3 Fa0/2 – SW1 Fa0/2

Three switches were connected to each other and it was going to, and with the additional configuration dynamictrunks Protocol (DTP) was discussed by the three trunk dynamically. Let's check the trunk SW1 has been successfully established.

SW1#show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	n-isl	trunking	1
Fa0/2	desirable	n-isl	trunking	1

<Output omitted for brevity>

SW2 and SW3 to verify successful deployment of the trunk can be used in the same order. As shown in the following output modes are three broad tree will be configured Cisco switch.

```

SW1(config)#spanning-tree
mode
mst Multiple spanning tree mode
pvst Per-Vlan spanning tree mode
rapid-pvst Per-Vlan rapid spanning tree mode

```

By default, the Cisco Catalyst 3550 used to create this scene PVST internal switch mode is decorated tree. PVST cross-VLAN spanning tree protocol, and this is the mode IEEE 802.1 D STP for each VLAN.

Below is the output of the command shows a spanning tree that shows spanning tree on SW1 pvst running mode.

SW3#show spanning-tree summary

```

Switch is in pvst mode
Root bridge for: none
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

```

<Output omitted for brevity>

The first phase involves the expansion of the Foundation, the switch in the direction of the tree. Rock Bottom Bridge won the elections with ID switch. Standard bridge ID is an 8-byte value byte priority 2 and 6 bytes for the Mac is made possible by a unique address on a switch bridge ID unique look you can use the command show-spanning-tree bridge ID.

SW1#show spanning-tree bridge id

VLAN0001 8001.0016.c831.9000

SW2#show spanning-tree bridge id

VLAN0001 8001.000f.24b7.1400

SW3#show spanning-tree bridge id

VLAN0001 8001.000f.233b.8a80

Won the elections with the ID switch on the bridge is very cheap. In our view, the bridge ID SW 3 is very cheap, so it should be switched to the Foundation. You can change the priority appears at the bottom of the switch VLAN of the Foundation have an impact on the election, however, we view Mr. ta have kept the default priority.

SW3(config)#spanning-tree vlan 1 pri

SW3(config)#spanning-tree vlan 1 priority ?

<0-61440> bridge priority in increments of 4096

You can see the command based on spanning-tree root bridge ID matches the ID SW3, indicating that the basic switch. Please note that the following command in the output priority is shown as a decimal value to 32769 hexadecimal is equal to 8001 was shown as part of the bridge ID.

SW3#show spanning-tree root

```
Root Hello Max Fwd
Vlan      Root ID      RootCost HelloTime  MaxAge FwdDly  Root Port
-----
VLAN0001  32769 000f.233b.8a80  0   2   20  15
```

The next step is for each route of convergence STP port (RP), which is the only port in which to spend a minimum amount returned to their roots.

All outbound interfaces based on a wide range of switches trail tree path cost is calculated by adding the cost. This set the scene for fast Ethernet interfaces default cost of 19.

The route is the main port of the switch, there is no basis for it itself; The root switch ports assigned to the port. SW1 is fixed with FH / 2 because the main port while SW2 has F / 2 because the root port.

The last major step for each category defined port (DP) set. When multiple switches are connected to the same department, then it may switch the interface to spend the least amount of return on the basis of the path segment. Our scenario has three segments and a single designated port has been determined for each as shown in the figure. The show spanning-tree command executed on SW1, SW2, and SW3 validates these facts.

SW1#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 000f.233b.8a80

Cost 19

Port 2 (FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0016.c831.9000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/1	Altn	BLK	19	128.1		P2p
-------	------	-----	----	-------	--	-----

Fa0/2	Root	FWD	19	128.2		P2p
-------	------	-----	----	-------	--	-----

SW3#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 000f.233b.8a80

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 000f.233b.8a80

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Fa0/1	Desg	FWD	19	128.1		P2p
Fa0/2	Desg	FWD	19	128.2		P2p

SW2 of us FA0 / 2 ports on the price change from the default of 19 to 39, and let's look at how the role is changing. Instant FA0 / 2 to SW2 Foundation is the main port switch provides the path SW3 lease expenses.

SW2>enable

SW2#configure terminal

Enter configuration commands, one per line. CNTL / Z will end up with.

SW2(config)#interface FastEthernet0/2

SW2(config-if)#spanning-tree cost 39

SW2(config-if)#end

SW2#

After the conversion, re-conversion of the plant to be expanded, based on the switch SW2 SW1 through 3 for the indirect chooses the way to achieve it because of the cost of the shortest path to be seen as the cost of 38.

WW2 direct path FA / 2 should now be switched to the Su-39 has spent 3K- and it's not the easiest way of spending. SW 2, 4 / 1 as the root port forwarding to keep state and FA 2/2, as shown here, would be blocked..

SW2#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 000f.233b.8a80

Cost 38

Port 1 (FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 000f.24b7.1400

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/1	Root	FWD	19	128.1		P2p
-------	------	-----	----	-------	--	-----

Fa0/2	Altn	BLK	39	128.2		P2p
-------	------	-----	----	-------	--	-----

You should proceed and run show spanning-tree command on SW1 and SW3 further to search out out how the spanning tree topology changed after re-convergence.

CHAPTER 6

VLANs AND VTP

6.1 Virtual LANs (VLANs):

VLAN (Virtual Local Network) may be logically separate IP subnet, multiple IP networks work and to attend to the same subnet-switched network. VLAN may be a logical broadcast domain can be extended multiple physical LAN segment. A wide range of network administrators to reduce the level 2 broadcast domains to boost the performance of virtual local-area networks (VLAN) to configure switches. Using VLAN, a network administrator logical functions or applications without the physical location of users through the relevant stations will be able to group together.

Each VLAN separate LAN and act as one or more switches that span. This allows the host device to behave in such a way so that they are in the same network.

VLANs to drive traffic in a layer 3 device (router) are required. VLAN has three major functions:

- Limit the size of broadcast domains
- Improve network performance
- Provides a level of security

How it's works.

Let us use the real-world conditions; Tired of the building, including an office or department altitude to think about the organization. A few years later, the company has expanded and now includes three buildings. The network continues to be identical, but the office and the computers that are displayed throughout the building.

HR offices and other departments on the same floor, and the building is opposite to the floor. However, network administrators will want to make sure that each office computer to share the same security measures and bandwidth controls.

Create a large LAN and wire each department work together to form a large and must be involved in the management of the network will not be easy.

This is where the VLANs comes to switching, the companies of their offices and departments, regardless of their use and their specific security requirements and to manage bandwidth in a positive way that will facilitate the easier. Select the network administrator for a switched VLANlogically network devices, which allow a group to create their own independent networks (VLAN) act like they are in another VLANs whether a standard infrastructure sharing. When you configure a VLAN, for the first time, users will be able to give its name to explain the role. Study the fig below for more details:

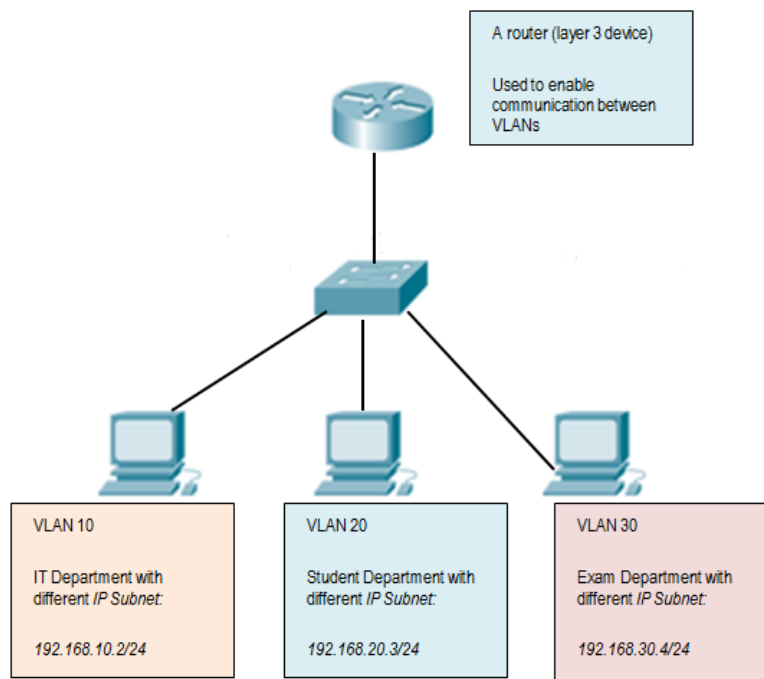


Figure 6.1.1: VLAN configuration.

In summary:

- VLAN is LAN network and it's an independent.
- ii. VLAN code and allow the individual school computers, even though they share a common structure does.
- iii. For general detection, will be given the name of VLAN

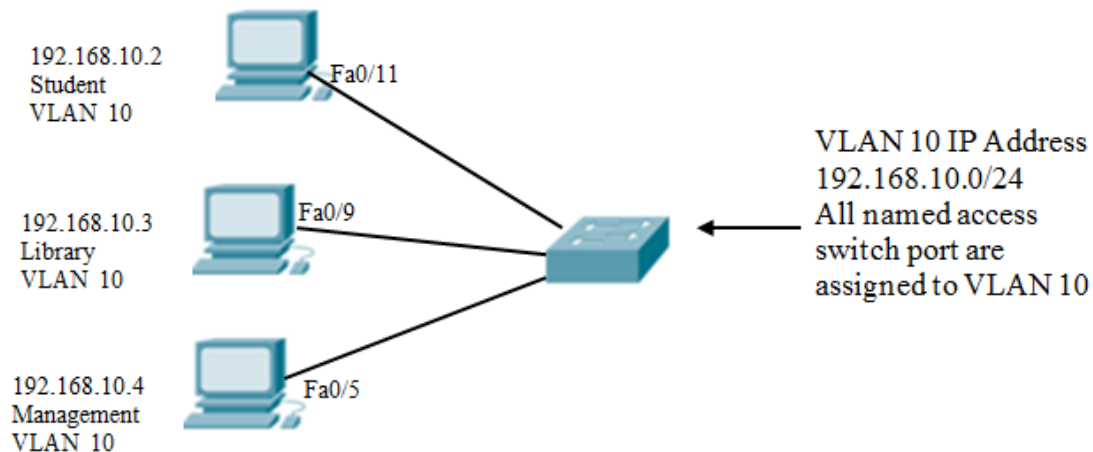


Figure 6.1.2: VLAN configuration

- VLAN = 10 for the PC VLAN define a subnet address has been assigned the
- VLAN configure, assign ports on VLAN
- An IP subnet address assigned to the PC firing.

Advantages of VLAN:

Security – Sensitive data protection is different from the rest of the network, reducing the possibility of security violations.

Higher performance – Multiple logical workgroup (broadcast domain), the Layer 2 network to network segmentation, and performance increases by reducing unnecessary traffic.

Cost reduction – Less need for expensive network upgrades cost savings and as a result of the network.

6.2 VLAN Trunking Protocol (VTP)

The first days of networking, networks VLAN was difficult to apply. Each network switch for each VLAN was configured manually. Switched Network to manage a larger size will not be a better job, this issue was made to simplify procedures for the VLANtrunking.

VTP Concept

VLAN Trimming Protocol (VTP) may be the primary goal of which is owned by Cisco. Across a switched network to configure and manage VLAN. And promotion helps VTP

Switch to the other network configuration VLAN maintain continuity. A domain is a message protocol VTP. VLAN featured, delete and change the name of the trunk frame using layer 2. It helps others, the changes concentration. Switch in the network. To manage your VLAN a VTP a switch to configure the server role your network configuration. Server (s) will share information with others VLAN by switching network, which is of course identical to the domain name.

Only normal-range VTP. VLAN (VLAN ID 1 to 1005) learns. VTP primary role is to take care of a consistent configuration across VLAN network administration domain. VLAN configuration is stored in the database Vlan.dat VTP. VLAN name. After the establishment of a trunk switch, are exchanged between VTP. ads. Switch. Switch to the server and client is both Exchange and monitor advertising VLAN each other to make sure the information is accurate records. VTP advertisement won't be exchanged if the trunk between the switches is inactive.

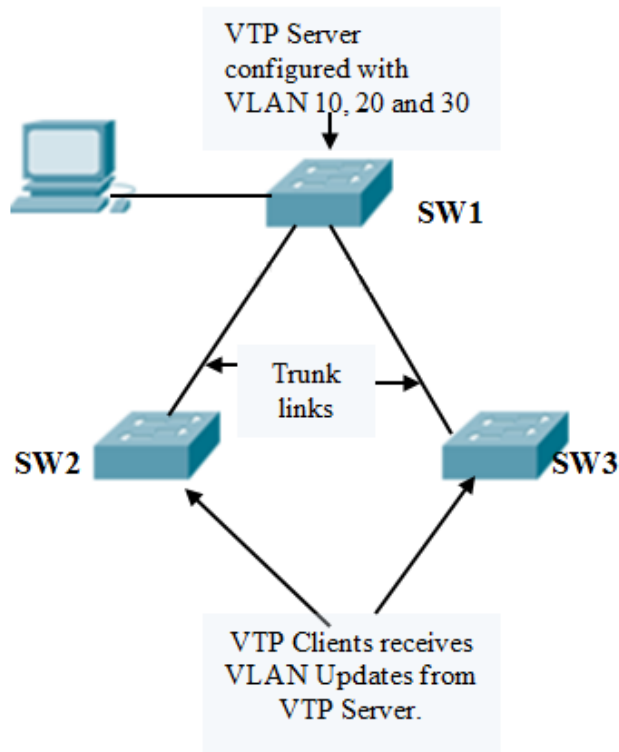


Figure 6.2.1: VTP server configuration

How to Configure VTP on a Cisco switch

The following command is used to configure a switch (S1) as VTP server:

```
Sw1#config t
```

```
Sw1(config)#vtp mode server
```

```
Sw1(config)#exit
```

Configure switch (Sw2 and Sw3) as VTP client:

```
Sw2#config t
```

```
Sw2(config)#vtp mode client
```

```
Sw2(config)#exit
```

VTP domain name and password to configure:

VTP in the exchange will be switched for short advertisements, in the switch

The network includes the same domain and the same password should be used:

VTP Domain

```
Sw1#config t
```

```
Sw1(config)#vtp domain lab
```

```
Sw1(config)#exit
```

```
VTP password
```

```
Sw1#config t
```

```
Sw1(config)#vtp password orbit123
```

```
Sw1(config)#exit
```

Configure the same username and password for clients. Make sure to change the configuration. VTP mode and to check whether the domain S-1 shows the command status VTP has been configured correctly.

```
Sw1#show vtp status
VTP Version: 2
Configuration Revision: 0
Maximum VLANs supported locally: 64
Number of existing VLANs: 5
VTP Operating Mode: Server
VTP Domain Name: lab
VTP Pruning Mode: Disabled
VTP V2 Mode: Disabled
VTP Traps Generation: Disabled
MD5 digest: 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

S1 and S2 for sure same

VTP to verify password, use the command show VTP password.

```
Sw1#show vtp password
```

```
VTP Password: orbit123
```

```
S1#
```

6.3 Inter-VLAN Routing

We have a router or layer 3 device employing a VLAN different VLAN network traffic to be forwarded to the process as defined in the Inter-VLAN routing it. The previous pages, we have learned about how to configure a network switch VLAN. VLAN- varied devices connected to each other to allow you to talk; you want to connect to a router. As we learned from each VLAN a unique broadcast domain, so the computers on separate VLAN By default, the ability to speak. There are several ways to allow the computer to communicate; Inter-VLAN routing to each. One way is to hold inter-VLAN routing infrastructure that connects the router switch. VLANs unique IP subnet with the network.

This configuration is a multi-subnet routing process that enables multi-VLAN environment. Inter-VLAN routing to facilitate the recruitment router, the router interfaces is connected to a separate VLAN. This VLANs communicate with each other via a router device.

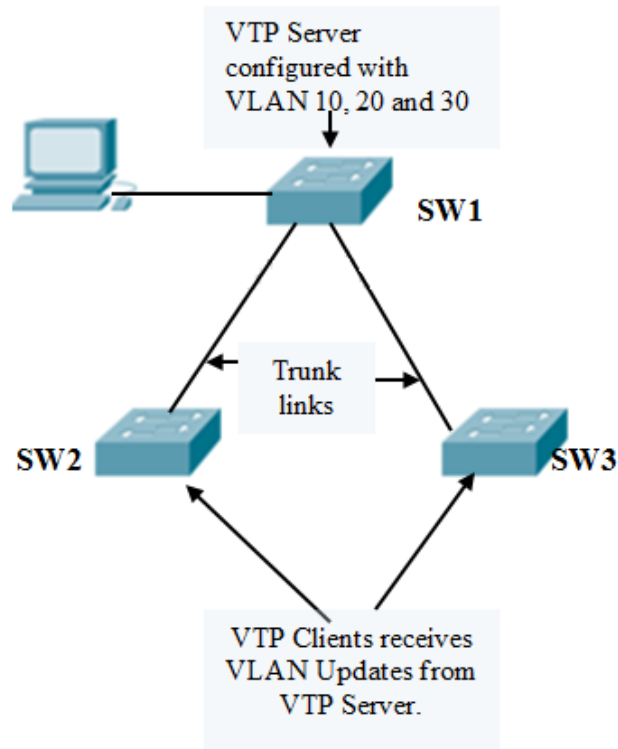


Figure 6.3.1: Inter VLAN routing

1. VLAN 10 VLAN on PC1 and PC3 to gain traffic through the router R1 flows 20.
2. PC1 and PC3, and a variety of different VLAN subnet IP address.
3. R1 router and a separate interface for each VLAN configure

Summary of the routing VLANs

- Inter-VLAN routing a stick to appoint an external router via the router uses to pass traffic between VLANs.
- Encapsulation 802.1Q trunk of a stick and a router for each VLAN sub-interface is configured.

CHAPTER 7

NETWORK SEVURITY

7.1 Network Security

Where there is an electric network, wired or wireless; there is a threat. Some people in a home or office network easily with this fear that keeps them hanging on the drive, or a hacker can access anything neighbors. The network has been developed for the protection of potential threats and the constant electronic monitoring of network systems and security for any network administrator should be the ultimate priority. If objection network security, privacy and sense of loss can be serious consequences, such as theft. It was the greatest concern is the network security to protect against unauthorized access to wireless connections to ensure that. Nowadays business transactions are done through internet, Also, mobile commerce and wireless networks, increasing security solutions to integrate smoothly, more transparent and more flexible to the demand.

The network attack has now increased. To use the basic tools and basic attacks that hackers days BASIC computer programming language and have knowledge of networking. Computer crimes they did not participate before they are able to do so.

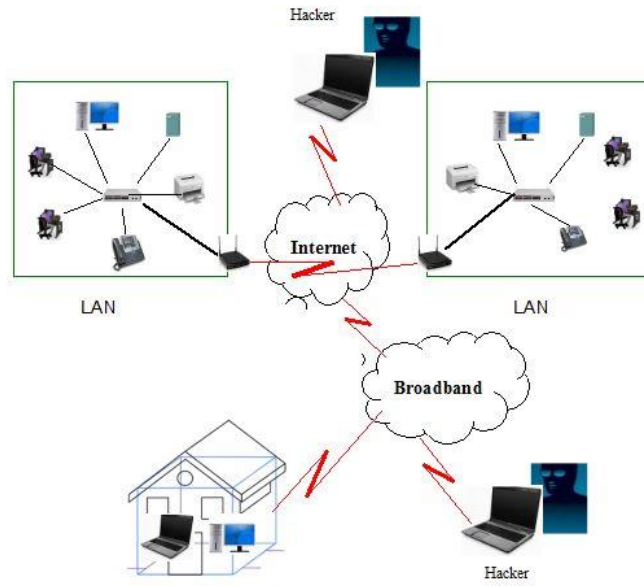


Figure 7.1.1: Computer Network

Types of Network Threats and Attacks

Threats, attacks and the absorption of a variety of styles to increase the size of terms is used to describe people involved. A number of the most common terms are as follows:

- White hat– These network vulnerability an attacker who is looking for systems or networks, according to the owners of the weaknesses of the system so they can be fixed. They are in principle hostile misuse of the computer system. A white hat generally focuses on the protection of IT systems.
- Hacker– It is a general term which can be used to record any programming expertise. These are usually to describe a person employed as a negative, which is thanks to network resources with malicious intent tries to grasp unauthorized access.
- Black hat or Cracker- White Hat Alternatively, the term of the person or the computer systems and programming skills, knowledge of their systems or networks to prevent use for which they are not authorized to use them to explain is employed, of course, it's usually in the end is to make profits.

- Phreaker: This term generally describes a person who is not allowed to perform a task in the bid led to the phone network. Freakier free Long-haul calls illegal to create or join a network device, usually through a pay phone.
- Spammer: It is often a large amount of email messages is used to describe what might have remained intact. Scammers often used to control the virus for help messages and the use of home computers.
- Phisher: MasterCard number or other sensitive information such as passwords in order to use e-mail or other means. Fisher sensitive information that may be a legitimate need to masquerades as a trusted party.

7.2 Cisco Firewalls:

Firewalls carefully analyze incoming traffic supported pre-established rules and filter traffic coming from unsecured or suspicious sources to forestall attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. for instance, "Source address 172.18.1.1 is allowed to achieve destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so people within the house are only allowed to access certain rooms (destination ports), looking on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a specific set of rooms (specific ports).

Types of firewalls

A firewall can be either software or hardware, it's better to keep both. A software firewall is a program that can be installed on each computer, and the port numbers and applications, traffic control, when a physical firewall and gateway installed in your network can be a part of the kit.

Packet-filtering firewall, firewall, the most common style, the test packets, and if they do not match the long-term protection rules forbid them to go through. This check the packet source and destination IP addresses of the firewall. Packets firewall in an "authorized" to access the network, it is reliable, however, coincides with the rules.

Packet-filtering firewall is divided into two sections: the state and the state. stateless firewall test packets independently of the other 1, and the lack of context makes them easy targets for hackers. In contrast, the state information about packets to be passed before the firewall remembers, and is considered to be more secure. However, packet-filtering firewall effective, they ultimately provide the basic protection and can be very limited - for example, that they cannot determine the contents of the request will reach the adverse effects. If malicious requests from a reliable source address were allowed to tell if a database is deleted, then the firewall will not approach it any sense. The next-generation firewall and proxy firewall is better equipped to detect such threats.

Next-generation firewalls (NGFW) Encrypted traffic inspection, penetration prevention measures, such as anti-virus, and many others, with the additional functionality of firewall technology combine traditional. Most significantly, the deep packet inspection (DPI) is included. Basic firewall keeps track of only the title of the packet, the data packet inspection, deep packet inspection to more effectively identify the user packets with corrupted data, classification, or is able to stop.

Proxy firewalls

Filter appliance at the network traffic. In contrast to the basic firewall, the proxy acts as the intermediary between the two parts of the system. The client must send an invitation to the firewall, where it is evaluated against the collection of security rules, and so allowed or blocked. Most significantly, the proxy firewall, such as HTTP and FTP protocols layer 7, and the traffic monitoring to detect malicious traffic and the use of deep packet inspection both.

Network address translation (NAT) firewalls

Unique IP addresses to multiple devices, including network address individual without revealing to connect to the Internet using a single IP address Allow. As a result, scanning a network for IP addresses cannot capture the specific details of the attackers, attack provides greater protection. NAT firewall proxy firewall, similar to a group that acts as an intermediary between the computer and external traffic.

Stateful multilayer inspection (SMLI) firewalls

Network, transport and application level packet filtering, and compare them with known, trusted packet. NGFW such as firewall, packet SMLI are individually tested and only pass each level, and allow them to pass. Contact the firewall status (the name refers to) check to see if the test packets

7.3 Layer 2 Security

Network security is only strong as the weakest link, because, because, if successfully exploited enough for the entry of a liability for a weak link in the data link layer of the reference model layer 2 or collaboration. We were able to protect our network from external threats, it is equally important to protect the internal network, because a number of threats has been derived from the internal. Like routers, Cisco switches have its own set of security requirements. If true, then switches to the weak areas can be protected.

The attacker, who wants to gain access to an organization's network is a convenient entry point for access to the switch. With access to a switch, an attacker can attack all kinds of networks. In order to protect the network perimeter security, not only in the network will not be enough to stop the attack because it is derived from. For example, malicious attackers looking for great business critical servers to Mac and IP address to evade. Continue to produce even rogue access can access the points established.

Port Security

Who is a switch port that connects to the network can access the Cisco switch port security feature to restrict what you can use. This feature allowed the port to access the systems to detect MAC address limited and is engaged. Configure a switch port for you to stay safe and there is no MAC address which can specify port allowed to access. Protected switch port MAC addresses assigned to the port, the source MAC addresses out of the loop does not forward frames. Port Security MAC address for the port you manually set or a limited number of incoming frames allowing switch for Mac allows you to enable addressing. In only a limited amount of allowed MAC addresses on a port, you can ensure that only 1 port can connect, connect to a network hub or switch to prevent any unauthorized expansion. When a secure port receives a frame, the frame source MAC address and port security related to the list of MAC addresses are compared. The secure MAC addresses can be configured manually or automatically, or at the port is configured to be learned. Source Mac Address in a frame separate from the list of protected addresses or port if the port is closed to throw frames from unauthorized host. Administratively able to secure the port until the default behavior is to pack up. How do you respond to security violations configure it depends on the behavior of the port.

The switch port this image FA0 / 1, only the incoming frames on a Mac's source MAC address is the only Mac to the source MAC address or other frames Mac on the side of the other of the frame source MAC address of the traffic will block allow Similarly, port F 0/2 B of the Mac will allow traffic with a source MAC address. The port on a Mac, including all other sources mac address block will, the fact that despite the fact that the Mac port Fax / 1 and approved, it's port-Fi / two friends has been blocked because the protected (approved) Mac addresses the individual switch ports specified.

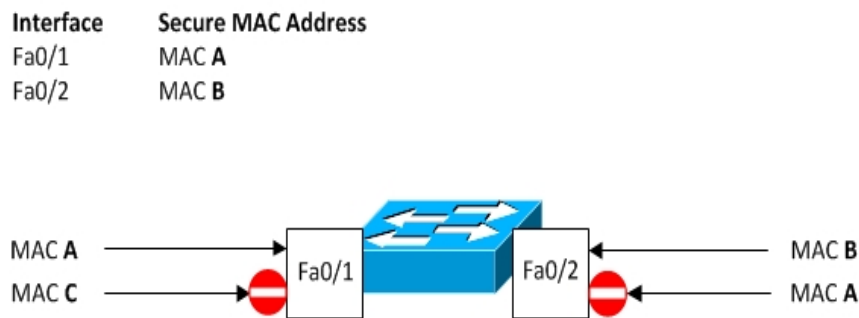


Figure 7.3.1: Port Security.

I co-host of the packet to exclude unauthorized address to pack instead of a port to configure port security feature will suggest. Pack up the port if port security is not an attack, but that it is still possible for the excessive traffic load port is disabled. Port security can be a useful feature, because it protects you from the port to the Mac address and MAC address is a lot more to connect to a port allowed to determine. However, if the hacker knows that it is allowed at any MAC address, however, he will have access to the network of the stall. For a user to connect a hub to connect additional hosts decisions LAN port security prevents unauthorized expansion.

Extension of this type of forest, only a Mac will allow you to protect the port. Also, if you're worried about port security bypass incognito mac address, the IEEE 802.1X authentication process, consider applying. Let's see how we secure MAC address to a specific port on a switch, including the ability to configure. The interface of the other device using the MAC address of the port is incorrect plug-in will be disabled

If the administrator has been deleted by the state.

```
Switch#configure terminal
```

```
Switch(config)#interface Fa0/0
```

```
Switch(config-if)#switchport mode access
```

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

```
Switch(config-if)#switchport port-security mac-address 1234.5678.9ABC
```

VLAN Hopping

VLANs isolate network traffic from several VLAN maintenance easier, improve performance and provide protection. You will remember that the router for inter-VLAN communication is not possible without the rumors. However, the router does not exceed the first time a method called VLAN hopping VLAN traffic to allow viewing by other VLAN. Attackers are some situations that can smooth the data and passwords and other sensitive information can be collected. A trunk port configured incorrectly attack works by taking advantage of a mistake. As you have learned, all VLAN trunk ports (1 - 4094) from the same physical link to the turn traffic. The trunk links running across the data frames with the IEEE 802.1 Q or ISL VLAN encapsulated related to a frame so determines.

As shown in the image, which we'll discuss a basic VLAN hopping attack by a rogue trunk link. During this attack, the attacker takes advantage of the switch to the default auto-tracking configuration. The attacker first switches a zero-turn access to it and so a system, perhaps a laptop computer to configure a switch as it turned out turn the system on a 802.1 Q or ISL capable NIC with a fitted, if sometimes NIC comes with the appropriate software to use and try to make it possible.

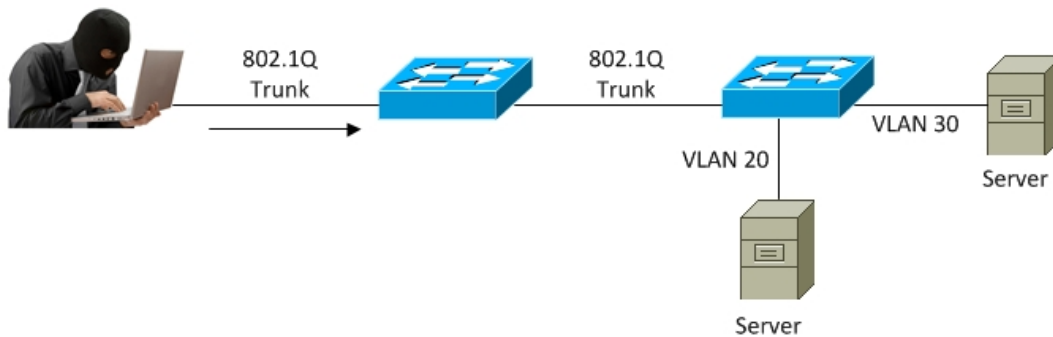


Figure 7.3.2:How Trunk link work

Dynamic attacker tracking Protocol (DTP) messages with a contact switch, the switch should be considered more of a switch, which tries to mislead Trunk. If the attacker successfully established a trunk system and switch between trunk port, then the attacker can get access to on affiliates or any VLAN. In order to be successful, this attack requires a switch port that supports trunking as desired or Ottawa. The attacker is on top of the results which may be a member of the VLAN switches Trunk and jumped on the VLAN can send and receive traffic.

One of these simple but effective VLAN hopping either way attack was launched: the attacker from host to host VTP message is generated that can determine a trunk. Once the trunk once established, invasive of another server on another host VLAN sort of tagged along with VLAN can send and receive traffic, the switch delivers the packet destination.

- Trucking is a genuine rogue switch and turned on the switch to the victims to set up a trunk. The attacker then switch to target rogue VLAN can access the switch.

If you need trunking switch port, switch port without using the command without any compromise DTP should be disabled and the trunk interface configuration mode and command mode using switch port trucking should be configured manually.

CHAPTER 8

FUTURE OPPERTUNITY & CONCLUTION

8.1 Conclusion of Internship

Bangladesh is developing Country. The Government of Bangladesh announce in 2011, our country will be fully digital within 2021. For this, Government of Bangladesh take many **necessary steps to grow Information technology (IT) Industries. This Concept name “Digital Bangladesh”.**

For computer science student book knowledge is important but practical knowledge gives us more confident. **“New HorizonsIT” has an important role in creation of “Digital Bangladesh” I thankful to “New Horizons” that they give me chance to working with them and I gained lot of experience at “Networking”. After finished intern I got a chance to working with acosmetic brand in Bangladesh. Now I’m implementing the knowledge that I got from theInternship.**

In future I have a plan to give a IT firm in Bangladesh.

8.2 Future Opportunity for Career

In Networking I have a great opportunity in future. In our country Networking future is also Bright. In every day, networking demand is increasing. There are lots of company in Bangladesh hiring networking expert. South Asia biggest IT exporter currently India. Bangladesh also want to **contribute in this sectors. That’s why Bangladesh government announced “Vision 2021” as a**

Digital Bangladesh. Networking expert also includes in this sectors of increasing demand rapidly.

APPENDIX

Introduction

The internship consists of learning and understanding the actual activity of words, applications and implementation of theories of the study. It's a workspace for university students and before entering the labor market to understand the real work environment. This is a real opportunity for students to adapt to future professional life.

Learning in entire Internship

I learned the things discussed below when practicing New Horizons computer learning center.

Discipline

In my entire internship, I learned the discipline which is very important. I learned to Be disciplined in the business environment. How to follow the hours of work and the office and maintained I learned from my job. It is very important that I have also encountered the discipline.

Team Work

Teamwork is very important for all types of work. No service can be provided better without all together teamwork. Better synchronization is also knowing how to understand the team members and how to follow them for better work environment.

Understanding Responsibilities

All types of work have responsibilities and must be met. Faced with a given situation and manage it using the skill. The older members of the team made me understand this and supported

me for Satisfy the responsibilities of the job in the situation. I learned a lot from my senior's.

To be Professional

To have a better service, perfection must be at work. And it's impossible to have Perfection at work without professional and appropriate attitude. That was totally taught by the **seniors'**.

APPENDIX A

COMPANY INFORMATION

New Horizons Computer Learning Center is based in Dhaka, Bangladesh. They have in markets in 35 years. Growing every year. It also has the technology to provide creative solutions. To the challenges of your business. New Horizons IT is a private company incorporated under the Law of 1994. Provides a centralized automated solution for your business and industry. In function of the Size and scope of the partners, offers different products and services to meet your needs. New Horizons provides the best and customized solutions for organization. New Horizons expert group provide solution that helps the customer's environment to use it in a maximum scale.

COMPANY HEAD OFFICE

New Horizons

Computer training school in Dhaka

Address: Momtaz Plaza (3rd Floor, House 7 Road No 4, Dhaka 1205

Phone: 01783-366877

REFERENCE

[1] Available at url://www.google.com, Last visited January 01, 2020 2.00 pm

[2] Available at url://www.bing.com, Last visited February 01, 2020 11.00 am

