

PROJECT DOCUMENTATION



ESOFT METRO CAMPUS

245, 3 De Fonseka Pl, Colombo 00400 (**Branch 1**)

No 5, 2nd Floor, Main Street, Trincomalee (**Branch 2**)

43 Baily Rd, Batticaloa (**Branch 3**)

Contact info : 0117 572 572 / 077 398 5759 / 0657 572 572

E-mail address : info@esoft.lk

Presented by :- MAM.Fahham

Contact number:- 0756175549

Email-address :- aroosfaham680@gmail.com

Table of Contents

PROJECT documentation	1
Project Introduction	4
Project Diagram.....	5
Subnetting.....	6
Devices used in diagram.....	8
Switches.....	9
Multilayer switches	10
Routers.....	11
Access point.....	12
Computers.....	13
Servers	14
Laptops	15
Printers.....	16
Smart phones	17
Ip phones.....	18
Cables	19
Protocols and configurations used in diagram	20
1.VLAN	21
2.Ether channel	22
3.Access point.....	23
4.Port security.....	25
NTP	26
FTP	27
VTP.....	28
STP	29

DHCP	30
AAA.....	31
HSRP	32
OSPF.....	34
TFTP	35
SNMP	36
VPN	Error! Bookmark not defined.
ICMP	37
IP Phone.....	Error! Bookmark not defined.
Project Estimation	38

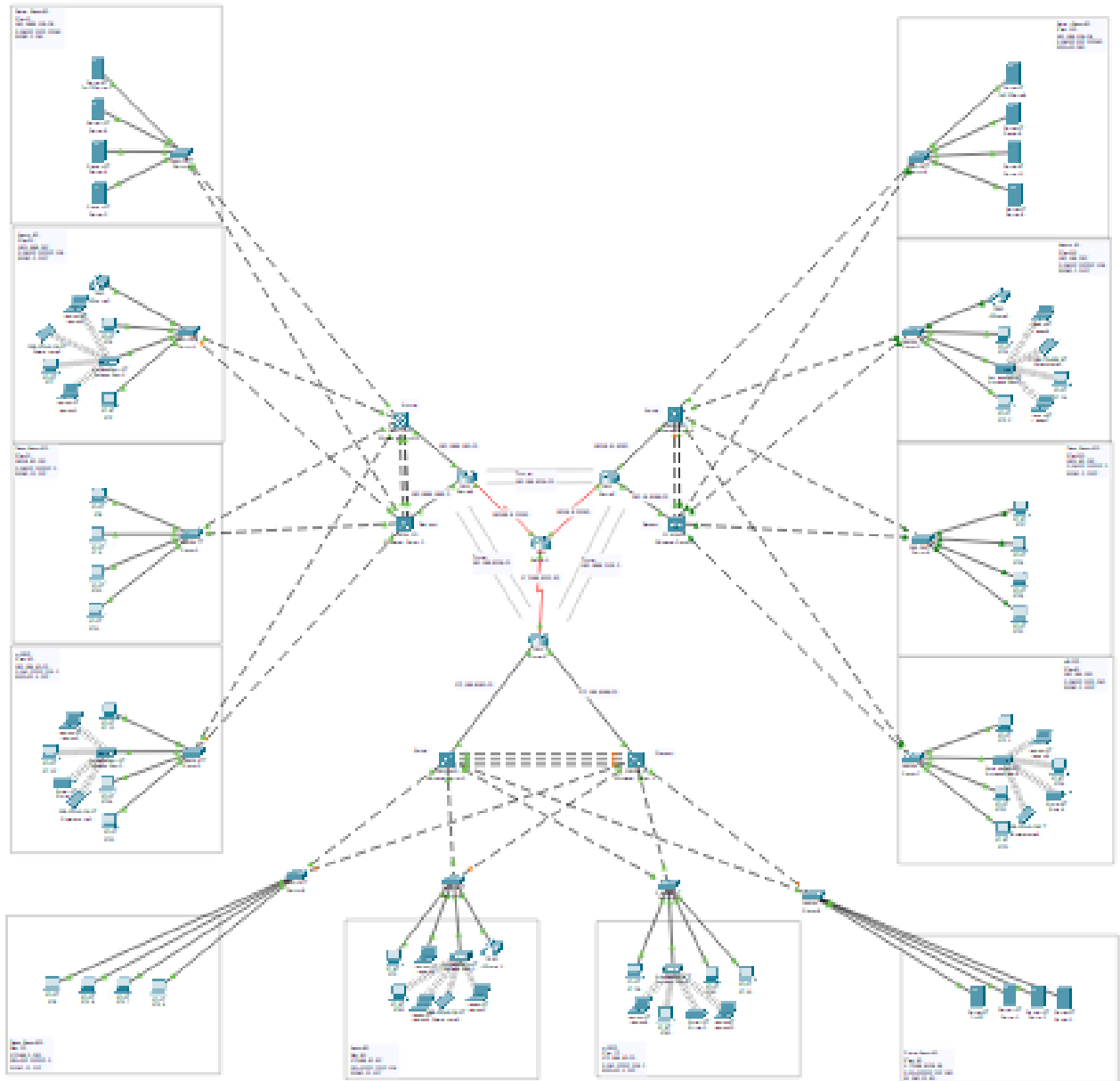
Project Introduction

Project Title : Esoft metro campus three branches network connectivity

The network connectivity at Esoft Metro Campus spans across three branches, forming a robust infrastructure that facilitates seamless communication, resource sharing, and collaboration among students, faculty, and administrative staff. Through a combination of wired and wireless connections, each branch is interconnected to ensure reliable access to online resources, academic materials, and administrative systems. This interconnected network fosters an environment conducive to learning, innovation, and academic excellence across all branches of Esoft Metro Campus.



Project Diagram



Subnetting

Branch 1

Departments	Network Ip	Subnet Mask	First Ip	Last Ip	Broadcast Ip
Classroom(600) Vlan 30	192.168.0.0	255.255.252.0	192.168.0.1	192.168.3.254	192.168.3.255
HR (350) Vlan 40	192.168.4.0	255.255.254.0	192.168.4.1	192.168.5.254	192.168.5.255
Admin (80) Vlan 20	192.168.6.0	255.255.255.128	192.168.6.1	192.168.6.126	192.168.6.127
Server Room (60) Vlan 10	192.168.6.128	255.255.255.192	192.168.6.129	192.168.6.190	192.168.6.191

Branch 2

Departments	Network Ip	Subnet Mask	First Ip	Last Ip	Broadcast Ip
Classroom(600) Vlan 30	172.168.0.0	255.255.252.0	172.168.0.1	172.168.3.254	172.168.3.255
HR (350) Vlan 40	172.168.4.0	255.255.254.0	172.168.4.1	172.168.5.254	172.168.5.255
Admin (80) Vlan 20	172.168.6.0	255.255.255.128	172.168.6.1	172.168.6.126	172.168.6.127
Server Room (60) Vlan 10	172.168.6.128	255.255.255.192	172.168.6.129	172.168.6.190	172.168.6.191

Branch 3

Departments	Network Ip	Subnet Mask	First Ip	Last Ip	Broadcast Ip
Classroom(600) Vlan 30	192.16.0.0	255.255.252.0	192.16.0.1	192.16.3.254	192.16.3.255
HR (350) Vlan 40	192.16.4.0	255.255.254.0	192.16.4.1	192.16.5.254	192.16.5.255
Admin (80) Vlan 20	192.16.6.0	255.255.255.128	192.16.6.1	192.16.6.126	192.16.6.127
Server Room (60) Vlan 10	192.16.6.128	255.255.255.192	192.16.6.129	192.16.6.190	192.16.6.191

Devices used in diagram

1. Switches
2. Multilayer switches
3. Routers
4. Access point
5. Computers
6. Servers
7. Laptops
8. Printers
9. Smart phones
10. Ip phones
11. Cables

Switches



Cisco Switch – 2960

- ❖ The Cisco Catalyst 2960 is a series of fixed- configuration, enterprise- class switches designed for small to medium- sized business networks. It's part of Cisco's expansive portfolio of network switches and offers a range of features and capabilities to support dependable and secure network connectivity.
- ❖ The Catalyst 2960 series switches give fast Ethernet and Gigabit Ethernet connectivity options, along with Power over Ethernet(PoE) support for bias similar as IP phones and wireless access points. These switches also offer advanced security features, quality of service(QoS) capabilities, and easy operation through Cisco's intuitive command- line interface(CLI) or web- grounded graphical stoner interface(GUI). The Catalyst 2960 switches are extensively used in colourful network surroundings to deliver high- performance and scalable network results.

Multilayer switches



Cisco MLS – 3560

- ❖ The multilayer switch (MLS) has 10gbe switch and Gigabit Ethernet switch. It's a network device which enables operation at multiple layers of the OSI model. By the way, the OSI model is a reference model for describing network dispatches. It has seven layers, including the physical layer (layer 1), data link layer (layer 2), network layer (layer 3) and so on. The multilayer switch performs functions up to nearly operation Layer (layer 7). For case, it can do the environment grounded access control, which is a point of layer 7. Unlike the traditional switches, multilayer switches also can bear the functions of routers at incredibly fast pets. In addition, the layer 3 switch is one type of multilayer switches and is veritably generally used.

Routers



Cisco Router – 1941

- ❖ The Cisco Router 1941 is a modular router designed for small to medium-sized businesses. It's part of the Cisco Integrated Services Router Generation 2(ISR G2) series. The router offers a range of features and capabilities, including high- performance data forwarding, security, and integrated services.
- ❖ It supports multiple WAN interfaces, similar as T1/ E1, xDSL, and Ethernet, furnishing inflexibility for connecting to different types of networks. The Cisco Router 1941 also includes intertwined services modules(ISMs) and enhanced high- speed WAN interface card(EHWIC) places, allowing for the expansion of functionality and performance as demanded. It's generally used for branch office connectivity, secure data transmission, and network services integration.

Access point



- ❖ Understand the significance of how a wireless access point enhances your network and what part it plays. Learn further about the different types of access point configurations.
- ❖ An access point(AP) is a term used for a network device that bridges wired and wireless networks. Consumer APs are frequently called a “ wireless routers ” because they generally also serve as both internet routers and firewalls. marketable and artificial APs tend towards minimum network routing capabilities and infrequently have firewalls.
- ❖ Most APs connect wireless networks using the Wi- Fi standard; still, ultramodern marketable and artificial APs decreasingly offer support for the Bluetooth and Thread wireless norms, as well. This allows marketable and artificial APs to support both mortal- centric and Internet of effects(IoT) bias.

Computers



PC (i5 6th Gen 8GB Ram , 256SSD and 1TB HDD 4GB nvidia geforce rtx 2050 graphics)

- ❖ A PC, or Personal Computer, is a protean electronic device used for colourful tasks like browsing, gaming, word processing, and more. It consists of factors like a central processing unit(CPU), memory, storehouse, and input/ affair bias. PCs run operating systems like Windows, macOS, or Linux and can be customized or upgraded to suit individual requirements. They are a abecedarian tool in ultramodern computing and are set up in homes, services, and institutions worldwide.

Servers



- ❖ A server is a computer program or device that provides a service to another computer program and its stoner, also known as the customer. In a data centre, the physical computer that a garçon program runs on is also constantly appertained to as a garçon. That machine might be a devoted server or it might be used for other purposes.
- ❖ In the client/ server programming model, a garçon program awaits and fulfils requests from customer programs, which might be running in the same, or other computers. A given operation in a computer might serve as a customer with requests for services from other programs and as a garçon of requests from other programs.

Laptops



HP INTEL CORE i7 13 Gen LAPTOP (8GB RAM, 512GB SSD, 15.6" FHD, WIN11, Intel UHD,MS OFFICE)

- ❖ A laptop is a movable computer that combines the factors of a desktop computer into a single, compact device. It includes a screen, keyboard, touchpad or mouse, and battery power source. Laptops are designed for protean use, allowing druggies to work, browse the internet, watch vids, and perform colourful tasks on the go. They're generally used for both particular and professional purposes due to their convenience and mobility

Printers



- ❖ A computer is an electronic device that takes input from the stoner, processes it, and gives the affair. A computer processes the data at a veritably high speed and with high delicacy. It processes the input according to the set of instructions handed to it by the stoner and gives the asked affair snappily.

- ❖ Introductory Functions of Computers are Inputting the Data, Processing the Input as per the Instructions handed, Storing the result and also furnishing the druggies with the asked affair.

Smart phones



- ❖ A smartphone is a mobile device that combines a PDA(particular digital adjunct) and a cellular phone. These bias have enhanced capabilities compared to cell phones; they let you do further than make phone calls and shoot textbook dispatches. Smartphones can browse the Internet and run programs like a computer. They've a touch screen that allows druggies to interact with over 7 million apps(November 2023), including those for particular and business use, games, social media, online shopping, and more. The picture shows the first interpretation of the Apple iPhone, a popular smartphone.

Ip phones



- ❖ (Internet Protocol phone) A telephone that's used with voice over IP(VoIP) telephone services. The IP phone entrapments directly into the Internet and converts voice into IP packets and vice versa. It has erected-in draft signalling and is used in confluence with an IP PBX in an enterprise or a hosted VoIP service. An IP phone can also be software installed in the stoner's PC for calls made at the computer(see softphone). See VoIP, hosted VoIP and IP telephony.

Cables



Cable (Gear IT Cat6 Outdoor Ethernet Cable, CCA Copper Clad, Waterproof, Direct Burial, In-Ground, UV Jacket, POE)

- ❖ Network lines are physical cables that connect bias in a computer network. They transmit data, allowing bias like computers, printers, and routers to communicate with each other. Common types include Ethernet lines(for wired connections) and fibre optical lines(for highspeed, long- distance connections). They come in colourful orders, with advanced orders supporting briskly data pets. duly installed lines are pivotal for a dependable and effective network connection

Protocols and configurations used in diagram

1. VLAN
2. Ether channel
3. Access point
4. Port security
5. NTP
6. FTP
7. VTP
8. STP
9. DHCP
- 10.AAA
- 11.HSRP
- 12.ospf
- 13.TFTP
- 14.SNMP
- 15.VPN
- 16.ICMP
- 17.IP Phone

1.VLAN

Virtual LAN(VLAN) is a conception in which we can divide the bias logically on subcaste 2(data link subcaste). Generally, subcaste 3 bias divide the broadcast sphere but the broadcast sphere can be divided by switches using the conception of VLAN.

A broadcast sphere is a network member in which if a device broadcast a packet also all the bias in the same broadcast sphere will admit it. The bias in the same broadcast sphere will admit all the broadcast packets but it's limited to switches only as routers don't forward out the broadcast packet. To further out the packets to different VLAN(from one VLAN to another) or broadcast disciplines, inter Vlan routing is demanded. Through VLAN, different small- sizesub-networks are created which are comparatively easy to handle.

IOS Command Line Interface

```
Switch(config)#do sh vl
```

VLAN	Name	Status	Ports
1	default	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
50	Classroom	active	
60	admin	active	
70	HR	active	
80	Severroom	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
60	enet	100060	1500	-	-	-	-	-	0	0
70	enet	100070	1500	-	-	-	-	-	0	0
80	enet	100080	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
------	------	------	-----	--------	--------	----------	-----	----------	--------	--------

2.Ether channel

EtherChannel is a port link aggregation technology in which multiple physical port links are grouped into one logical link. It's used to give high-speed links and redundancy. A outside of 8 links can be added up to form a single logical link.

EtherChannel, also known as Link Aggregation Control Protocol(LACP), is a fashion used in computer networks to combine multiple physical links between two network switches into a single logical link. This logical link provides increased bandwidth and redundancy, as well as bettered cargo balancing.

Two protocols can be used to dynamically configure an ether channel between switches.

1. **PAGP** (port aggregation protocol) = It's a cisco propriety protocol which is used in only cisco devices.
2. **LACP** (link aggregation control protocol) = It's an open standard protocol which is used in all devices.

```
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
,
```

```
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode passive
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode passive
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode passive
```

3.Access point

An access point is a device that allows you to connect wirelessly to a network, similar as the internet. It acts as a ground between your bias and the network, furnishing a wireless connection for your bias to pierce the network coffers.

Access Point1

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID faham

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase 12345678

User ID

Password

Encryption Type AES

Laptop1

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 24 Mbps

MAC Address 00E0.8F23.2E7D

SSID faham

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase 12345678

User ID

Password

Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.6.8

Subnet Mask 255.255.255.128

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address

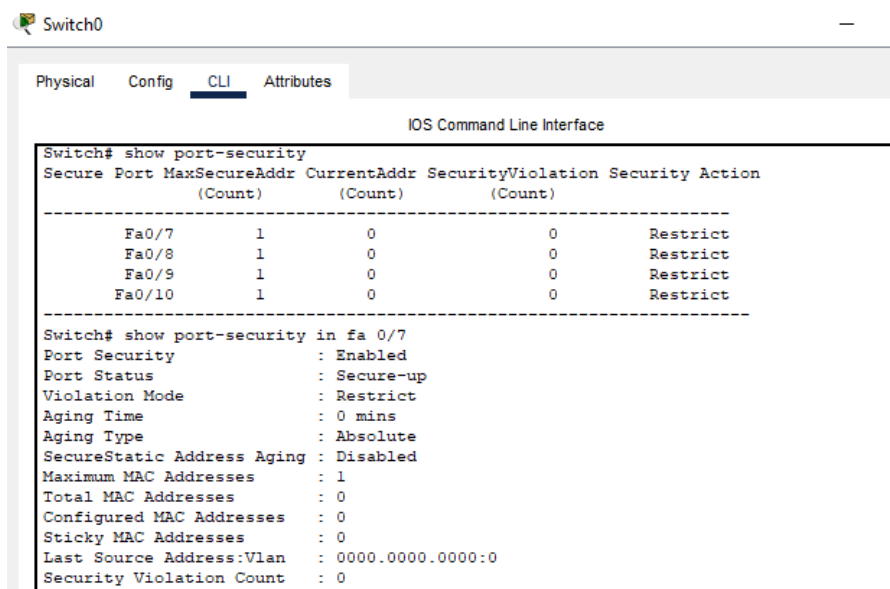
Link Local Address: FE80::2E0:8FFF:FE23:2E7D

4.Port security

Attackers' task is comparatively veritably easy when they can enter the network they want to attack. Ethernet LANs are veritably much vulnerable to attack as the switch anchorages are open to use by dereliction. colorful attacks similar as Dos attack at layer 2, address spoofing can take place. If the director has control over the network also obviously the network is safe. To take total control over the switch anchorages, the stoner can use a point called port- security. However, also the security will increase up to a great extent at layer 2, If ever help an unauthorized stoner to use these anchorages.

There 3 violations are

1. **Shutdown** : It put the port into error –disable state.
2. **Restrict** : Ignores all the traffic interface and count the violation.
3. **Protect** : Ignores all the traffic interface and doesn't count the violation

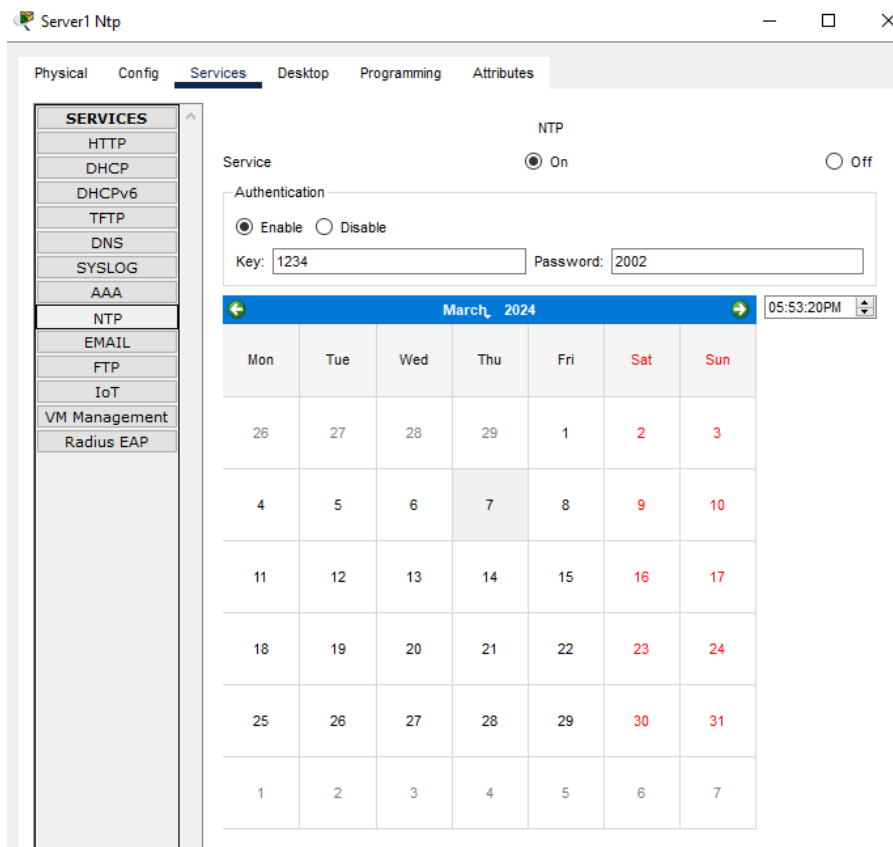


The screenshot shows a network switch interface with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the IOS Command Line Interface. The user has entered the command 'show port-security', which returns a table of port security status for ports Fa0/7, Fa0/8, Fa0/9, and Fa0/10. All ports are configured with 'Restrict' action and have 1 secure MAC address and 0 violations. A second command 'show port-security in fa 0/7' is entered, showing detailed configuration for Fa0/7: Port Security is Enabled, Port Status is Secure-up, Violation Mode is Restrict, Aging Time is 0 mins, Aging Type is Absolute, SecureStatic Address Aging is Disabled, Maximum MAC Addresses is 1, Total MAC Addresses is 0, Configured MAC Addresses is 0, Sticky MAC Addresses is 0, Last Source Address:Vlan is 0000.0000.0000:0, and Security Violation Count is 0.

```
Switch0
Physical Config CLI Attributes
IOS Command Line Interface
Switch# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
      (Count)      (Count)      (Count)
-----
Fa0/7      1          0          0          Restrict
Fa0/8      1          0          0          Restrict
Fa0/9      1          0          0          Restrict
Fa0/10     1          0          0          Restrict
-----
Switch# show port-security in fa 0/7
Port Security      : Enabled
Port Status       : Secure-up
Violation Mode     : Restrict
Aging Time        : 0 mins
Aging Type        : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

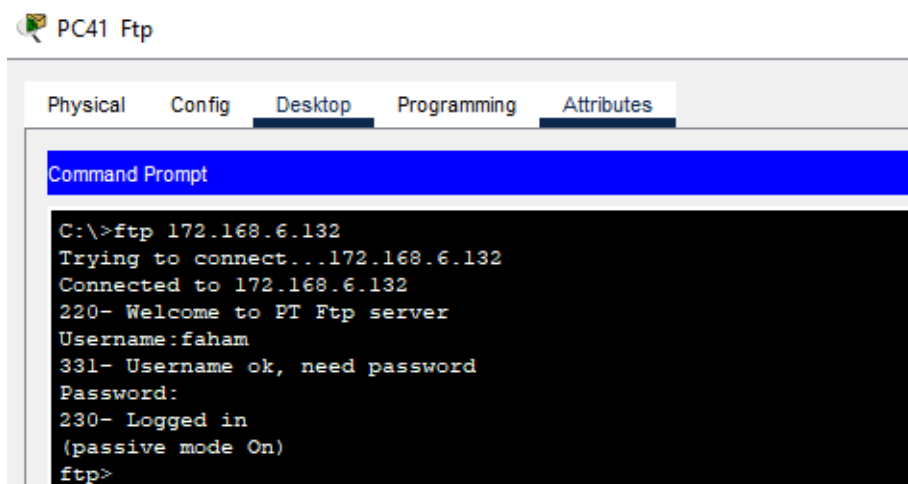
NTP

Network Time Protocol(NTP) is a protocol that helps the computers timepiece times to be accompanied in a network. This protocol is an operation protocol that's responsible for the synchronization of hosts on a TCP/ IP network. NTP was developed by David Mills in 1981 at the University of Delaware. This is needed in a communication medium so that a flawless connection is present between the computers.

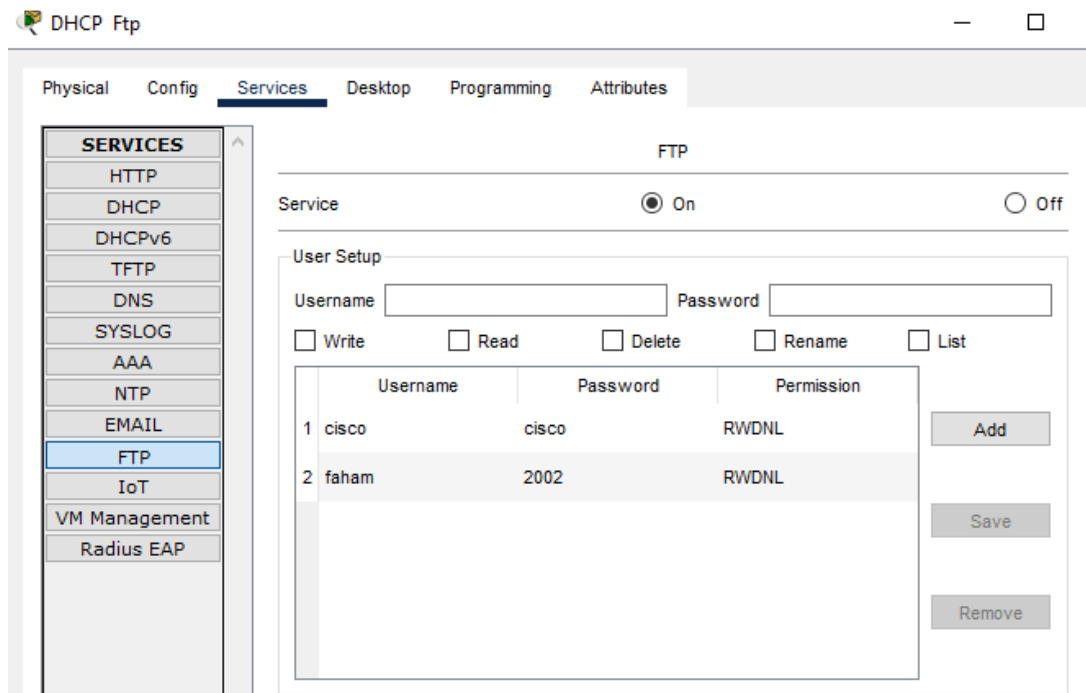


FTP

FTP is a standard communication protocol. There are colorful other protocols like HTTP which are used to transfer files between computers, but they warrant clarity and concentrate as compared to FTP. Also, the systems involved in connection are miscellaneous, i.e. they differ in operating systems, directories, structures, character sets, etc. The FTP secures the user from these differences and transfers data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default transfer format, in this, each character is decoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image transfer format is the default format for transferring double files.

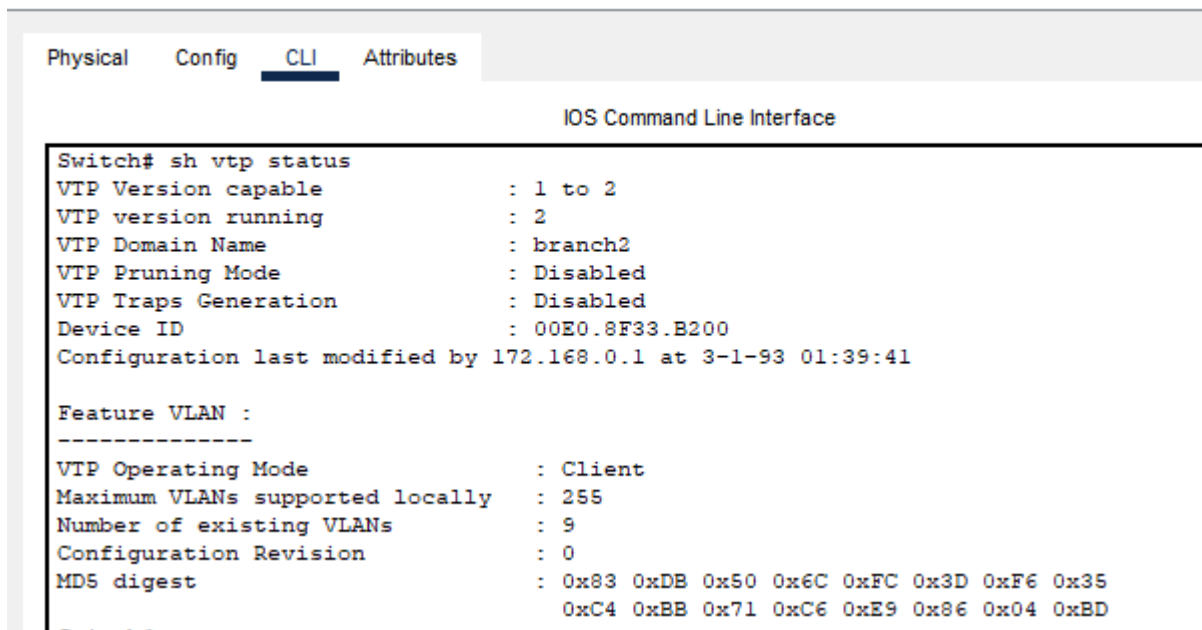


```
PC41 Ftp
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ftp 172.168.6.132
Trying to connect...172.168.6.132
Connected to 172.168.6.132
220- Welcome to PT Ftp server
Username:faham
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



VTP

To carry traffic of a VLAN, it must be first configured on the switch. Suppose, if the user wants to send a frame from source to destination and the shortest path between them contains 1000 switches. To process a frame of any VLAN, VLANs should be configured first so, have to configure the same VLANs on all the 1000 switches manually. It will not be possible for the administrator to do that. Here comes VTP to the rescue.



The screenshot shows the CLI interface of a switch named Switch8. The 'CLI' tab is selected. The command 'sh vtp status' has been entered, displaying the following output:

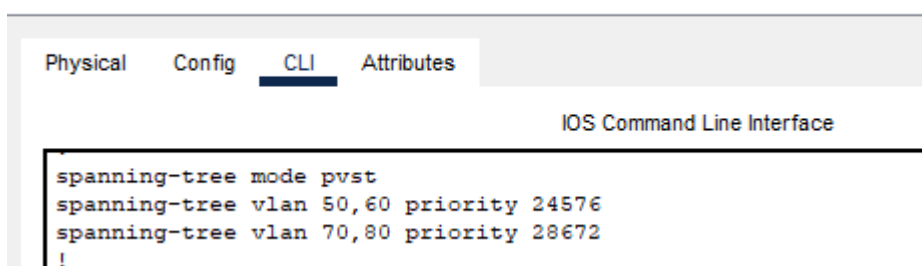
```
Switch# sh vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : branch2
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 00E0.8F33.B200
Configuration last modified by 172.168.0.1 at 3-1-93 01:39:41

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
Configuration Revision   : 0
MD5 digest               : 0x83 0xDB 0x50 0x6C 0xFC 0x3D 0xF6 0x35
                          0xC4 0xBB 0x71 0xC6 0xE9 0x86 0x04 0xBD
```

STP

Spanning Tree Protocol(STP) is used to make a loop free network by covering the network to track all the links and shut down the least spare bones.

Root ground is a switch in a single VLAN or whole topology(according to the type of STP standard used) which is responsible for distributing BPDUs and block the least spare harbourage.



The screenshot shows the CLI interface of a switch named Multilayer Switch0. The 'CLI' tab is selected. The following commands have been entered:

```
spanning-tree mode pvst
spanning-tree vlan 50,60 priority 24576
spanning-tree vlan 70,80 priority 28672
!
```

DHCP

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to bias(similar as computers, smartphones, and printers) on a network. rather of manually configuring each device with an IP address, DHCP allows bias to connect to a network and admit all necessary network information, like IP address, subnet mask, dereliction gateway, and DNS server addresses, automatically from a DHCP server.

This makes it easier to manage and maintain large networks, icing bias can communicate effectively without conflicts in their network settings. DHCP plays a pivotal part in ultramodern networks by simplifying the process of connecting bias and managing network coffers efficiently.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan 40	192.168....	0.0.0.0	192.168....	255.255....	508	0.0.0.0	0.0.0.0
vlan 30	192.168....	0.0.0.0	192.168....	255.255....	60	0.0.0.0	0.0.0.0
vlan 20	192.168....	0.0.0.0	192.168....	255.255....	124	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168....	255.255....	512	0.0.0.0	0.0.0.0

AAA

AAA consists of three factors that make access to a network more secure Authentication, Authorization, and Accounting(exertion monitoring/ charging), shortly appertained to as AAA. AAA is an effective network regulator that enables the authorized stoner to connect to the network with vindicated credentials to pierce computer coffers, determine what they're authorized to do, and track and record all exertion during access. What the AAA factors do can be epitomized as follows

1. Authentication : It verifies the identity of druggies or bias trying to pierce a network. This ensures that only authorized individualities or systems gain entry.
2. Authorization : Once authenticated, the AAA garçon determines what coffers or services a stoner or device is allowed to pierce. It sets warrants grounded on the stoner's profile or part.
3. Accounting : This tracks the operation of network coffers by a stoner or device. It logs information like login times, data transferred, and services used. This data can be useful for billing, auditing, or security purposes.

Server2 AAA

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

AAA

Service

☒ On
☐ Off

Radius Port

1645

Network Configuration

Client Name

Client IP

Secret

ServerType

Radius

	Client Name	Client IP	Server Type	Key	
1	MLS	172.168.6.129	Tacacs	12345	<div>Add</div> <div>Save</div> <div>Remove</div>
2	MLS2	172.168.6.130	Tacacs	12345	

User Setup

Username

Password


	Username	Password	
1	faham	12345	<div>Add</div>

HSRP

Hot Standby Router Protocol(HSRP) is a CISCO personal protocol, which provides redundancy for a original subnet. In HSRP, two or further routers gives an vision of a virtual router.

HSRP allows you to configure two or further routers as standby routers and only a single router as an active router at a time. All the routers in a single HSRP group shares a single MAC address and IP address, which acts as a dereliction gateway to the original network. The Active router is responsible for encouraging the traffic. However, the Standby router takes up all the liabilities of the active router and on the business, If it fails.

01.Active Router


 Multilayer Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
!
interface Vlan50
  mac-address 00e0.f9e5.a901
  ip address 172.168.0.1 255.255.252.0
  standby 50 ip 172.168.0.3
  standby 50 priority 110
  standby 50 preempt
!
interface Vlan60
  mac-address 00e0.f9e5.a902
  ip address 172.168.6.1 255.255.255.128
  standby 60 ip 172.168.6.3
  standby 60 priority 110
  standby 60 preempt
!
interface Vlan70
  mac-address 00e0.f9e5.a903
  ip address 172.168.4.1 255.255.254.0
  standby 70 ip 172.168.4.3
  standby 70 priority 110
  standby 70 preempt
!
interface Vlan80
  mac-address 00e0.f9e5.a904
  ip address 172.168.6.129 255.255.255.192
  standby 80 ip 172.168.6.131
  standby 80 priority 110
  standby 80 preempt
```

02.Stand by Router

 Multilayer Switch1

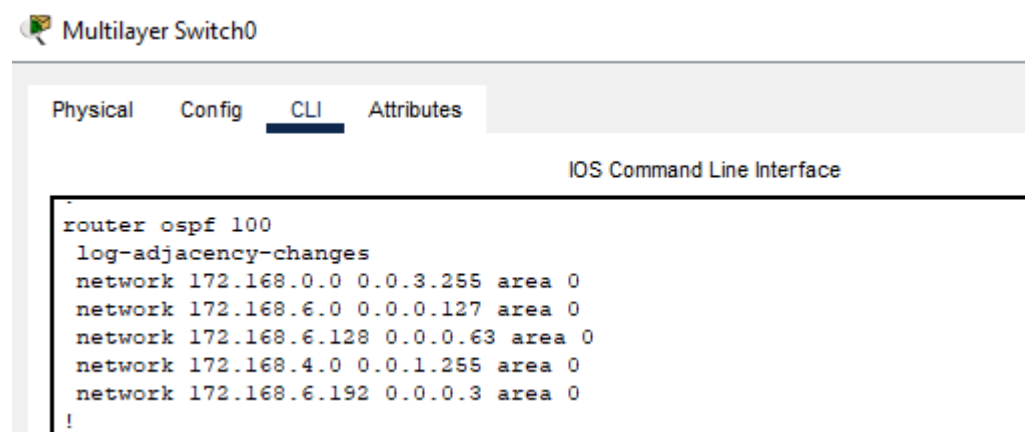
Physical Config CLI Attributes

IOS Command Line Interface

```
interface Vlan50
  mac-address 00d0.d36c.d301
  ip address 172.168.0.2 255.255.252.0
  ip helper-address 172.168.6.132
  standby 50 ip 172.168.0.3
  standby 50 preempt
!
interface Vlan60
  mac-address 00d0.d36c.d302
  ip address 172.168.6.2 255.255.255.128
  standby 60 ip 172.168.6.3
  standby 60 preempt
!
interface Vlan70
  mac-address 00d0.d36c.d303
  ip address 172.168.4.2 255.255.254.0
  standby 70 ip 172.168.4.3
  standby 70 preempt
!
interface Vlan80
  mac-address 00d0.d36c.d304
  ip address 172.168.6.130 255.255.255.192
  standby 80 ip 172.168.6.131
  standby 80 preempt
```

OSPF

Open Shortest Path First(OSPF) is a link- state routing protocol that's used to find the stylish path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force(IETF) as one of the Interior Gateway Protocol(IGP), i.e, the protocol which aims at moving the packet within a large independent system or routing sphere. It's a network subcaste protocol which works on protocol number 89 and uses announcement value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR) Provisory Designated Router(BDR).



Multilayer Switch0

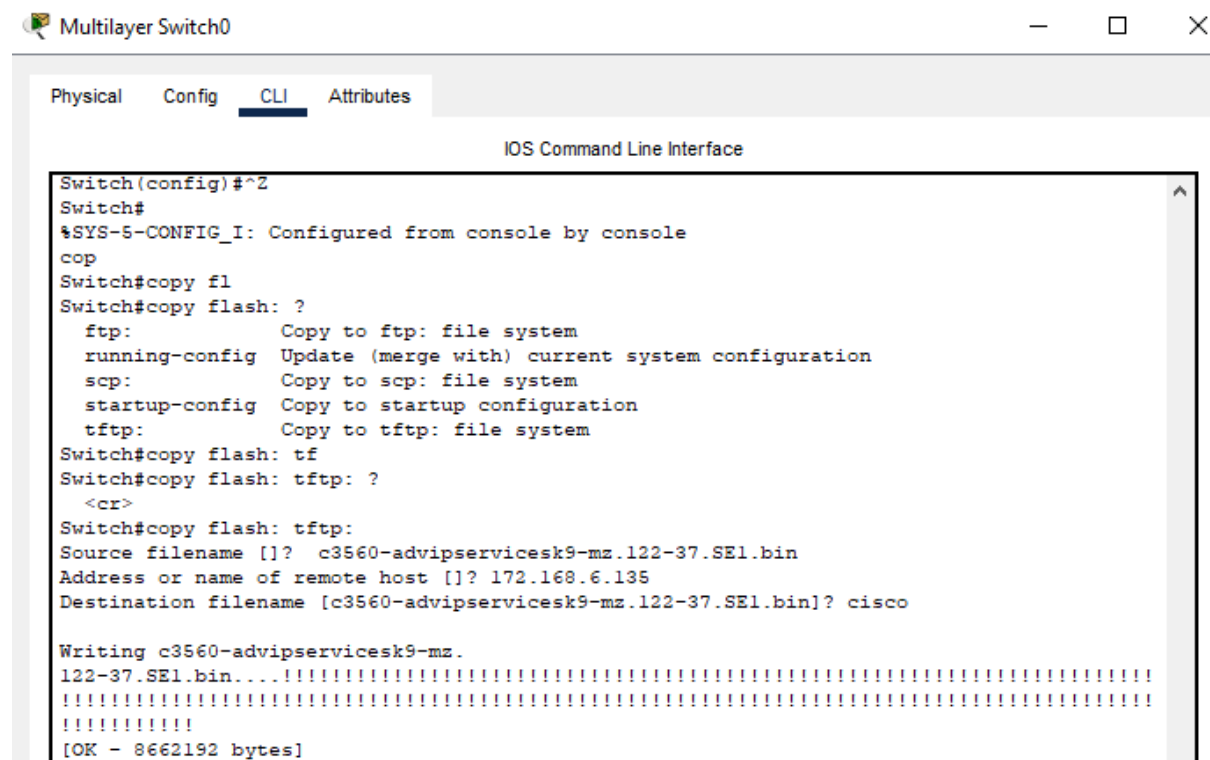
Physical Config CLI Attributes

IOS Command Line Interface

```
router ospf 100
log-adjacency-changes
network 172.168.0.0 0.0.3.255 area 0
network 172.168.6.0 0.0.0.127 area 0
network 172.168.6.128 0.0.0.63 area 0
network 172.168.4.0 0.0.1.255 area 0
network 172.168.6.192 0.0.0.3 area 0
!
```

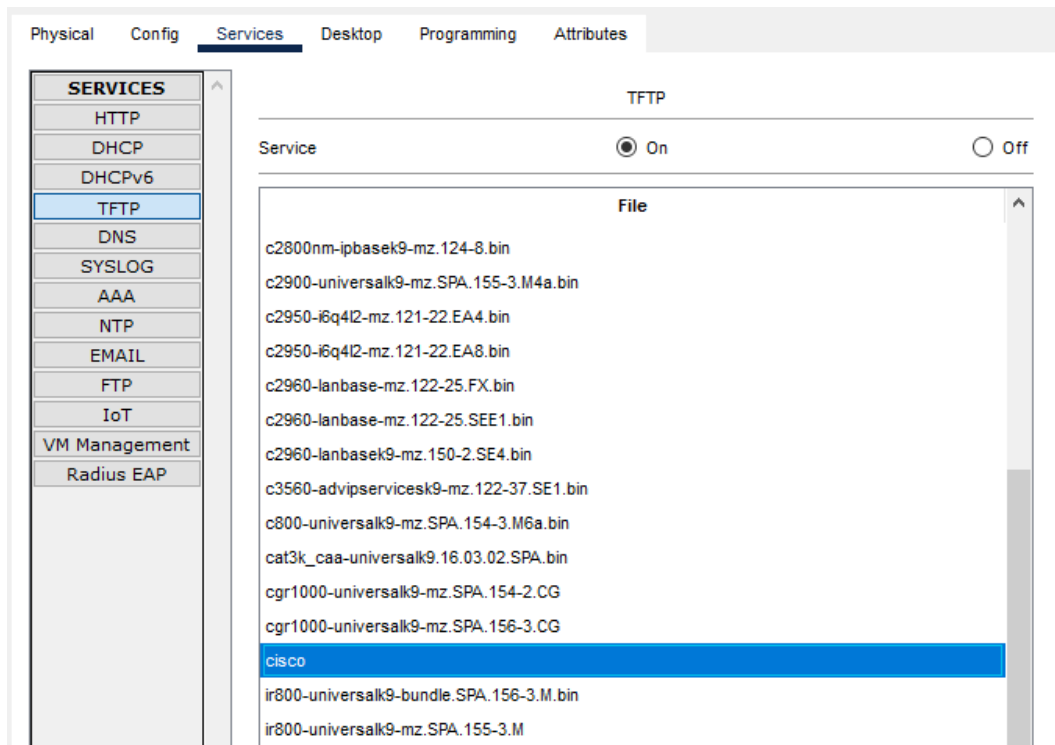
TFTP

The network is made up of colorful bias. These bias are moreover connected by ethernet or by any wireless means. The communication for transferring lines takes place between these connected bias. thus network protocols are needed. Network protocols are defined as rules that describe the format of data, transferring and entering of data between the bias connected in a network. The below composition covers in detail the Trivial train Transfer Protocol(TFTP).



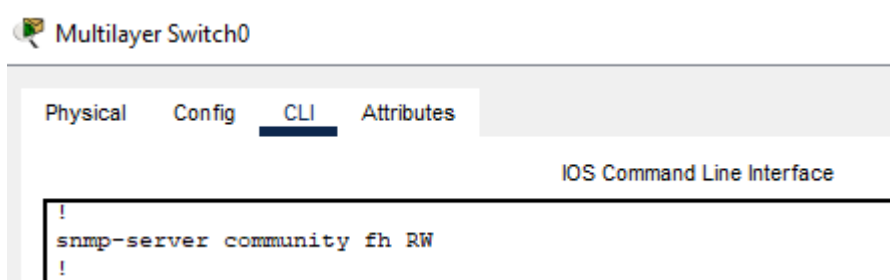
```
Multilayer Switch0
Physical Config CLI Attributes
IOS Command Line Interface
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
cop
Switch#copy fl
Switch#copy flash: ?
  ftp:          Copy to ftp: file system
  running-config Update (merge with) current system configuration
  scp:          Copy to scp: file system
  startup-config Copy to startup configuration
  tftp:         Copy to tftp: file system
Switch#copy flash: tf
Switch#copy flash: tftp: ?
  <cr>
Switch#copy flash: tftp:
Source filename []? c3560-advipservicesk9-mz.122-37.SE1.bin
Address or name of remote host []? 172.168.6.135
Destination filename [c3560-advipservicesk9-mz.122-37.SE1.bin]? cisco

Writing c3560-advipservicesk9-mz.
122-37.SE1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
[OK - 8662192 bytes]
```



SNMP

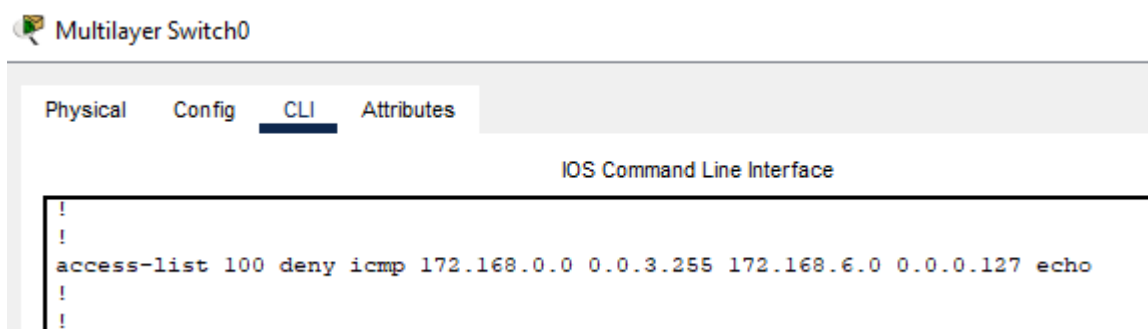
Simple Network Management Protocol(SNMP) is a extensively used protocol for network operation that provides a standardized frame for monitoring and managing network bias similar as routers, switches, waiters, and printers. It operates within the operation subcaste of the Internet protocol suite and allows network directors to manage network performance, find and break network problems, and plan for network growth.



ICMP

ICMP is used for reporting errors and operation queries. It's a supporting protocol and is used by network devices like routers for transferring error dispatches and operations information. For illustration, the requested service is not available or a host or router couldn't be reached.

Since the IP protocol lacks an error-reporting or error-correcting medium, information is communicated via a communication. For case, when a communication is transferred to its intended philanthropist, it may be interdicted along the route from the sender. The sender may believe that the communication has reached its destination if no one reports the problem. However, If a mediator reports the mistake.



Project Estimation

No	Devices	Quantity	Cost	Total cost \$	Total cost in LKR
1	Cisco 2811 router	4	\$1500	\$6000	1800000
2	Cisco 3560 mls	6	\$3000	\$1800	540000
3	Cisco 2960 switch	12	\$3500	\$42000	12600000
4	Server	12	\$700	\$8400	2520000
5	Access point	6	\$1000	\$6000	1800000
6	Laptop	15	\$700	\$10500	3150000
7	Desktop	36	\$600	\$21600	6480000
8	Ip phone	3	\$500	\$1500	450000
9	Printers	4	\$100	\$400	120000
10	Cable	500ft	\$10	\$5000	1500000
11	iPhone	3	\$800	\$2400	720000
Total in \$USD and LKR				\$105600	31680000