COMPUTER NETWORKS PROJECT

Contents

Part 1: Design and Implement a VLSM Addressing Scheme.

HOSTS: Indicates the number of usable IP addresses available for hosts within that specific network segment or VLAN.

NETWORK ID: Specifies the network address that identifies the beginning of the IP subnet for that VLAN or link.

SUBNET MASK: Defines the subnet mask in dotted decimal notation, which determines the size of the network and the number of available host IP addresses within that subnet.

FIRST ADDRESS: Represents the first usable IP address within the subnet that can be assigned to a device (e.g., a router interface or an end-user device).

LAST ADDRESS: Denotes the last usable IP address within the subnet that can be assigned to a device.

BROADCAST: Shows the broadcast address for the subnet. This address is used to send data to all devices within that specific subnet.

	HOSTS	NETWORK ID	SUBNET MASK	FIRST ADDRESS	LAST ADDRESS	BROADCAST
VLAN 100	61	10.1.0.0	255.255.255.192	10.1.0.1	10.1.0.62	10.1.0.63
VLAN 700	31	10.1.0.64	255.255.255.192	10.1.0.65	10.1.0.126	10.1.0.127
VLAN 200	30	10.1.0.128	255.255.255.224	10.1.0.129	10.1.0.158	10.1.0.159
VLAN 600	29	10.1.0.160	255.255.255.224	10.1.0.161	10.1.0.190	10.1.0.191
VLAN 800	25	10.1.0.192	255.255.255.224	10.1.0.193	10.1.0.222	10.1.0.223
VLAN 400	20	10.1.0.224	255.255.255.224	10.1.0.225	10.1.0.254	10.1.1.255
VLAN 500	15	10.1.1.0	255.255.255.224	10.1.1.1	10.1.1.30	10.1.1.31
VLAN 25	12	10.1.1.32	255.255.255.240	10.1.1.33	10.1.1.46	10.1.1.47
SWS TO MIU GW	7	10.1.1.48	255.255.255.240	10.1.1.49	10.1.1.62	10.1.1.63
MAIN MLS TO MIU GW	2	10.1.1.64	255.255.255.252	10.1.1.65	10.1.1.66	10.1.1.67
N MLS TO MIU GW	2	10.1.1.68	255.255.255.252	10.1.1.69	10.1.1.70	10.1.1.71
S TO GW	2	10.1.1.72	255.255.255.252	10.1.1.73	10.1.1.74	10.1.1.75
R TO GW	2	10.1.1.76	255.255.255.252	10.1.1.77	10.1.1.78	10.1.1.79

Part 2: Build the Network and Configure Basic Device Settings and Interface Addressing.

```
MIU-GW#show running-config
Building configuration...

Current configuration : 3557 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname MIU-GW
!
!
!
enable secret 5 $1$mERr$rieJ5nEP8XfGN.NvipeTy1
!
!
ip dhcp excluded-address 10.1.0.1 10.1.0.3
ip dhcp excluded-address 10.1.0.33 10.1.0.35
ip dhcp excluded-address 10.1.0.129 10.1.0.131
!
ip dhcp pool VLAN100
 --More-- |
```

```
Router>ENABLE
Router#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#security password min-
00:00:40: %OSPF-5-ADJCHG: Process 100, Nbr 3.3.3.3 on GigabitEthernet0/2/0 from LOADING to FULL,
Loading Done
lengt
00:00:45: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on GigabitEthernet0/1/0 from LOA
Router(config)#security password min-length 10
Router(config)#line console 0
Router(config-line)#password MIU1234567
Router(config-line)#Login
Router(config-line)#exit
Router(config)#enable secret CSC1234567
Router(config)#banner motd^unauthorised access^
                         ^
% Invalid input detected at '^' marker.

Router(config)#banner motd #unauthorized access#
Router(config)#
```

```
show running-config
Building configuration...

Current configuration : 3754 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Main-Mls
!
!
enable secret 5 $1$mERr$rieJ5nEP8XfGN.NvipeTy1
!
!
ip dhcp excluded-address 10.1.0.1 10.1.0.3
ip dhcp excluded-address 10.1.0.129 10.1.0.131
ip dhcp excluded-address 10.1.1.33 10.1.1.35
!
ip dhcp pool VLAN100
 network 10.1.0.0 255.255.255.192
 default-router 10.1.0.1
 --More-- |
```

Part 3: Configure Network Infrastructure Settings (VLANs, Trunking, Inter-VLAN Routing EtherChannel)

To enable communication between PCs in different VLANs, we define the VLANs on the Multi-Layer Switches (MLS). For each VLAN, a Switched Virtual Interface (SVI) is configured, which is then assigned an IP address and corresponding subnet mask. This SVI functions as the default gateway for devices within that specific VLAN. To facilitate shared VLAN information and allow routers and servers to access multiple VLANs, physical interfaces (such as GigabitEthernet0/1 and GigabitEthernet0/2) are combined into a logical channel port by trunking therefore extending the VLAN across the network. The switchport mode trunk command is then applied, forcing the interface into trunking mode, which allows it to carry traffic for multiple VLANs.

Main-mls		
G 1/1/1	10.1.1.65	255.255.255.252
Vlan 100	10.1.0.1	255.255.255.192
Vlan 200	10.1.0.129	255.255.255.224
s-mls		
G 1/1/1	10.1.1.73	255.255.255.252
Vlan 25	10.1.1.33	255.255.255.240
Vlan 400	10.1.0.225	255.255.255.224
n-mls		
G 1/1/1	10.1.1.69	255.255.255.252
Vlan 500	10.1.1.1	255.255.255.224
Vlan 600	10.1.0.161	255.255.255.224
r-mls		
G 1/0/5	10.1.1.77	255.255.255.252
Vlan 700	10.1.0.65	255.255.255.192
Vlan 800	10.1.0.193	255.255.255.224
Miu-miu gw		
G 0/0	209.165.200.226	255.255.255.240
G 0/1	10.1.1.78	255.255.255.252
G 0/0/0	10.1.1.50	255.255.255.252
G 0/1/0	10.1.1.66	255.255.255.252
G 0/2/0	10.1.1.74	255.255.255.252
G 0/3/0	10.1.1.70	255.255.255.252

```
Switch>en
Switch>enable
Switch#confi
Switch#configure
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inter
Switch(config)#interface r
Switch(config)#interface range g
Switch(config)#interface range gigabitEthernet 0/1-2
interface range not validated - command rejected
Switch(config)#interface range gigabitEthernet 1/0/1-2
Switch(config-if-range)#channel-g
Switch(config-if-range)#channel-group mode active
```

Those command lines were repeated for every vlan to create port channels

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Po2, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, 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
100  VLAN0100                          active    Fa0/3
200  VLAN0200                          active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Part 4: Configure Routing Protocols.

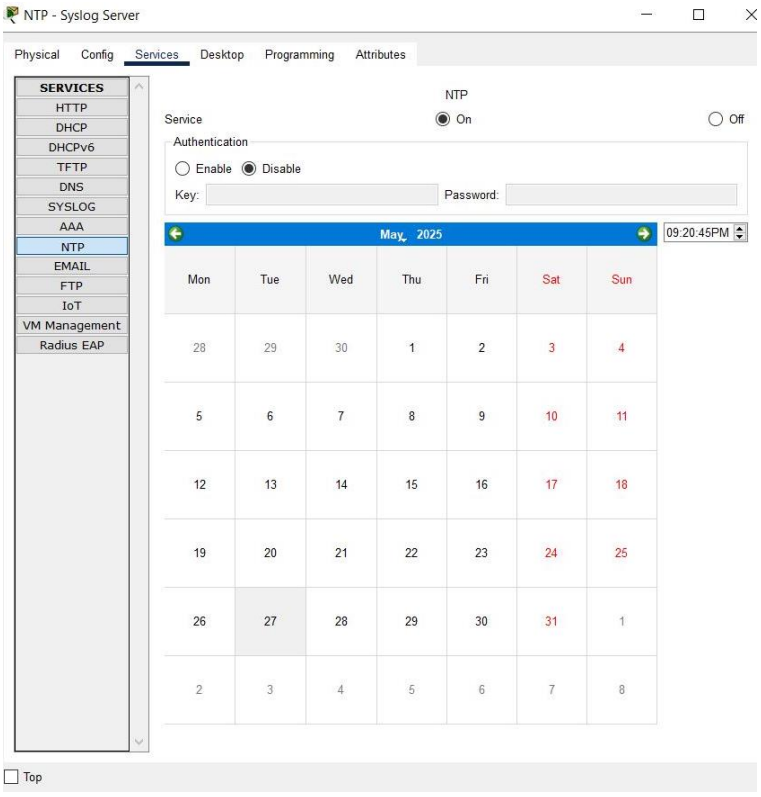
This process involves configuring IPv4 routing protocols to achieve rapid network convergence. We begin with OSPFv2 setup by enabling the process, assigning Router IDs, advertising networks, and then configuring passive interfaces and default route. EIGRP is configured by the same steps. The purpose of this operation is establishing bi-directional route redistribution between OSPFv2 and EIGRP. Finally, static default routes are implemented on edge routers pointing to the ISP with corresponding static routes configured on the ISP to direct traffic back to the internal network.

Part 5: Configure DHCP Server.

We are required to configure the DHCP address to exclude the first three usable IP addresses from being assigned from each of their pools. For the DHP pool configuration the DHCP server we had to define the DHCP pools for the VLANs of the building so then it would automatically assign IP addresses, default gateway and DNS server information to all hosts located in the Main building and S building. The next step is to configure the routers of the Main-MLS and S-MLS to act as DHCP relay agent then attempt to require an IP address from the provided PCs to verify the server and its relay configurations. For the next step, we exclude the first five usable IP addresses from their configured address pools and then verify that it works correctly achieving network connectivity.

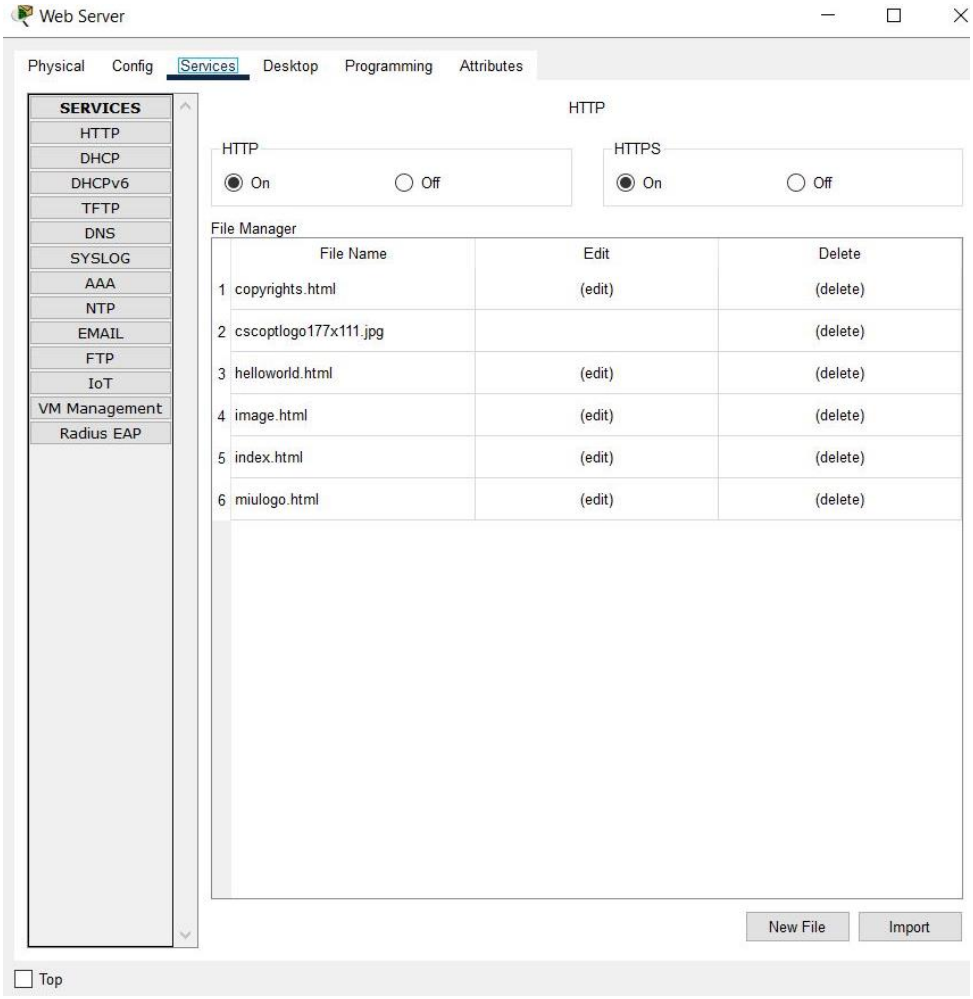
Part 7: Configure Network Management Features.

We have to configure all our devices to use an NTP server to synchronize their clock with a Network Time Protocol (NTP) to ensure a consistent timestamp across the network.



Enabling authentication is for security protocol which prevents malicious time sources from providing incorrect time.

Then, we make sure the syslog server is ‘on’ so it would listen to syslog messages. Next, we configure te web server to display the main web page with domain name miu.edu.eg that features MIU logo as the main page content



For the email server we have to configure it to fully support both sending and receiving of email messaging under the miu.edu.eg domain. For the last step of this part we should configure the DNS server to accurately resolve the domain name to the correct IP address of our web server.

Part 8: Configure and Verify a Site-to-Site IPsec VPN.

Assuming that the routers can see each other through the EtherChannel we have to confirm that the internal network have an appropriate routing path to their respective gateways. We should be looking for successful ping between the interfaces and gateways and internal networks to their gateways