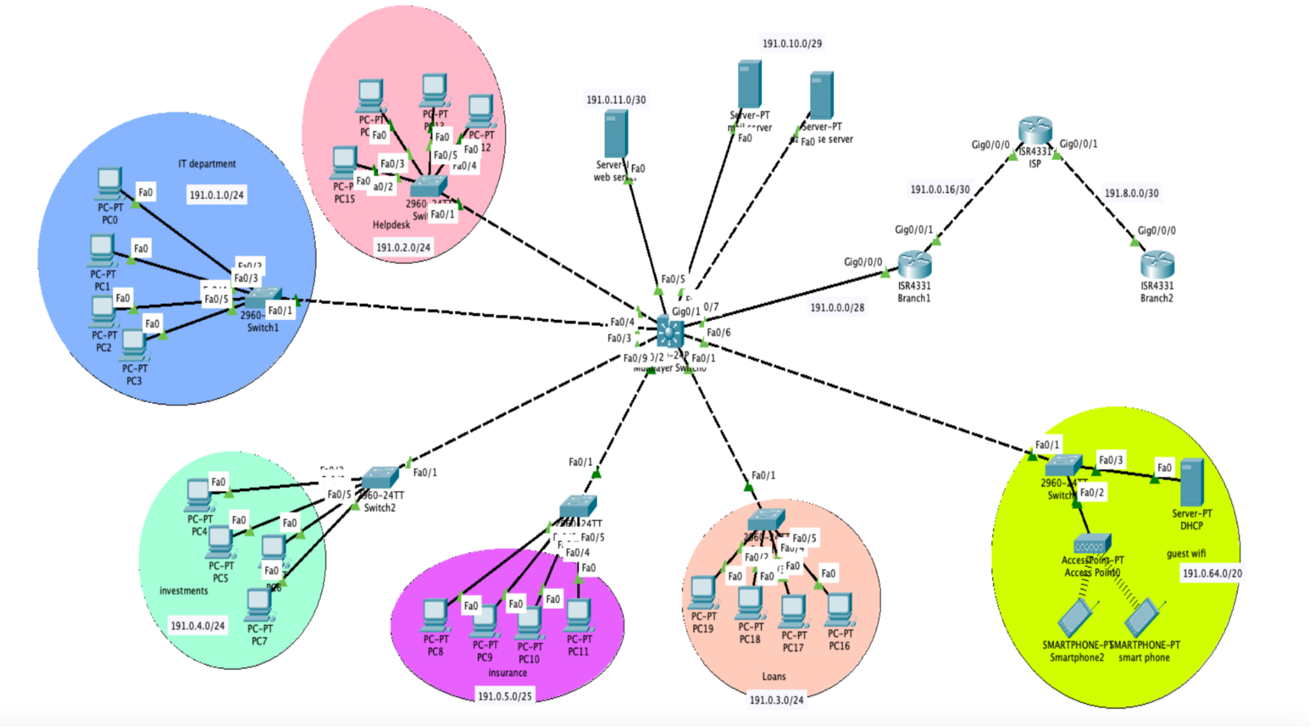
Sherif Gabr 900183120
Mina Ashraf 900182973

Computer Networks Project

Network Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
ISP router	Gig0/0/0	191.0.0.18	/30	
	Gig0/0/1	191.8.0.1	/30	
Branch 2 Router	Gig0/0/0	191.8.0.2	/30	
Branch 1 Router	Gig0/0/1	191.0.0.17	/30	
	Gig0/0/0	191.0.0.1	/28	
Multi Layered Switch	Gig0/1 (Branch1 Router)	191.0.0.2	/28	
	Fa0/3 (Vlan10 IT)	191.0.1.1	/24	
	Fa0/4 (Vlan20 Help Desk)	191.0.2.1	/24	
	Fa0/1 (Vlan30 Loans)	191.0.3.1	/24	

	Fa0/2 (Vlan40 Investments)	191.0.4.1	/24	
	Fa0/9 (Vlan60 Insurance)	191.0.5.1	/24	
	Fa0/6 (Vlan50 Guest)	191.0.64.1	/20	
	Fa0/8 (Email Server)	191.0.10.2	/29	191.0.10.1
	Fa0/7 (Database Server)	191.0.10.3	/29	191.0.10.1
	Fa0/5 (Web Server)	191.0.11.2	/30	191.0.11.1
PC0 (MLS-Fa0/3)	NIC	191.0.1.2	/24	191.0.1.1
PC1 (MLS-Fa0/3)	NIC	191.0.1.3	/24	191.0.1.1
PC2 (MLS-Fa0/3)	NIC	191.0.1.4	/24	191.0.1.1
PC3 (MLS-Fa0/3)	NIC	191.0.1.5	/24	191.0.1.1
PC12 (MLS-Fa0/4)	NIC	191.0.2.2	/24	191.0.2.1
PC13 (MLS-Fa0/4)	NIC	191.0.2.3	/24	191.0.2.1
PC14 (MLS-Fa0/4)	NIC	191.0.2.4	/24	191.0.2.1
PC15 (MLS-Fa0/4)	NIC	191.0.2.5	/24	191.0.2.1
PC16 (MLS-Fa0/1)	NIC	191.0.3.2	/24	191.0.3.1
PC17 (MLS-Fa0/1)	NIC	191.0.3.3	/24	191.0.3.1
PC18 (MLS-Fa0/1)	NIC	191.0.3.4	/24	191.0.3.1
PC19 (MLS-Fa0/1)	NIC	191.0.3.5	/24	191.0.3.1
PC4 (MLS-Fa0/2)	NIC	191.0.4.2	/24	191.0.4.1
PC5 (MLS-Fa0/2)	NIC	191.0.4.3	/24	191.0.4.1
PC6 (MLS-Fa0/2)	NIC	191.0.4.4	/24	191.0.4.1
PC7 (MLS-Fa0/2)	NIC	191.0.4.5	/24	191.0.4.1
PC8 (MLS-Fa0/9)	NIC	191.0.5.2	/24	191.0.5.1
PC9 (MLS-Fa0/9)	NIC	191.0.5.3	/24	191.0.5.1
PC10 (MLS-Fa0/9)	NIC	191.0.5.4	/24	191.0.5.1
PC11 (MLS-Fa0/9)	NIC	191.0.5.5	/24	191.0.5.1
DHCP Guest (MLS-Fa0/6)	NIC	191.0.64.2	/20	191.0.64.1
Guests	NIC	DYNAMIC	/20	191.0.64.1

Description:

The branch 1 bank contains 5 departments (IT, HelpDesk, Loans, Investments, and Insurance), 3 servers (Email, Database, and Web), and a guest wifi.

Branch 2 bank is abstracted as a single router.

Ideas Implemented:

- A multilayer switch is connected to the router of the branch.
- Each branch hosts is connected to a switch
- Each switch of each department is connected to an interface on the multilayer switch
- Each interface on the MLS is a VLAN with a different network address and different broadcast domain
- An access-list is implemented on the MLS to restrict access of the departments, servers, and guests depending on their permissions.
- All departments can communicate with each other using email, access the web server, and access the client's database
- The guests can only browse the web (http and https only)
- A wifi access point is used to connect users wirelessly to the network and each device gets a dynamic IP address from a DHCP server
- The Help Desk can access the Loans department, but not vice versa.
- The IT can access all departments
- Only the IT can access the other branch
- The connection to the other branch is encrypted using IPsec VPN

The Steps:

1. Add and configure the hosts for each of the 5 department (using static IPs) and connect to a switch (create a LAN)
2. Add a multilayer switch and connect all 5 switches to it
3. Create a different VLAN for each department and change mode to trunk
4. Add the 3 servers, assign a static IP, and connect it to the multilayer switch
5. The web server is on a different VLAN and is configured to issue http/https
6. The mail and DB servers are on the same VLAN and are configured to allow sending/receiving of emails and storing of data, respectively.
7. Add WIFI access point alongside a DHCP server, all connected to a switch connected to the multilayer switch, and change connection mode to trunk
8. Configure a gateway address for each VLAN connected to the multilayer switch
9. Implement an access-list to permit/deny traffic based on criteria of who can access the department, the servers, and the guests.
10. Connect the multilayer switch to a router (outer router of branch) and assign IP address to the interfaces (the connection should be on interface gig)
11. Connect 2 other routers in series to the branch router, representing the ISP and branch 2, respectively, and assign IPs to the interfaces.
12. Ensure branch 1 router can reach branch 2 router by doing static/dynamic routing (we did EIGRP routing)

13. Apply access-list on branch 1 router to restrict any department except the IT from accessing branch 2
14. Configure branch 1 router and branch 2 router to connect using the IPsec VPN

Questions:

1. Assume you forget to save your configuration; will you face any problem? If so, how can you fix this issue?

   Normally, it is best practice to execute “wr memory” or “copy running-config startup-config” to save the configuration locally, such that after a reboot, the configurations are the same. However, packet tracer saves the configurations automatically after saving the project, so executing “copy running-config startup-config” is not needed in that case. Therefore, not saving the project nor executing “wr” will result in the complete reset of the configurations, upon reboot.

2. How can you secure the server hosting the clients’ DB (*other than firewall*)?

   Alongside the different types of firewall protection, a server can be secured in a number of other methods.
   Firstly, the server can be connected to a router or a multi-layered switch, where an access-list is initialized. The access-list can specify the permitted IP hosts to connect and the denied hosts to connect. Also, the access-list can specify the type of connection to permit and deny, for example, ICMP, IP, HTTP, …etc. The access-list provides a good approach to customize and therefore secure who can connect to the server similar to firewalls, but this method comes with the cost of a router or multi-layered switch.
   Another method is to enable authentication on the server, whether it is password-based or key-based. This method ensures that if a user bypasses the access-list or firewall, they cannot do any harm on the server without having the correct credentials. So, it is more of a backup mechanism to ensure more security. Another method that is specific to database servers is ensuring the encryption of data. As a final security measure, if a user gets access to the data, it will be encrypted and therefore useless.

3. What is the type of access restriction used in the wireless router in your network?

   In a wireless router, we can set up access restrictions from the GUI of the router. In the access restriction, we can block specific URLs, keywords, and applications (HTTP, HTTPS, …etc.). Also, we have the flexibility to apply the restrictions to specific PCs on specific, predefined times. So, in our network, we need to block any traffic except for HTTP and HTTPS traffic coming from any source.

4. Which part will be affected in the network if we do not use a multilayer switch?

   The VLANs of the different departments will be affected, including the routing between them. Each department is on a different VLAN, all connected to the multilayer switch. The multilayered switch does the routing between them which includes the access restrictions of who can connect to who. Now by removing the multilayer switch, we need to add a router instead to ensure the same routing is implemented. From a functionality point of view, both will produce the same overall interaction between hosts. However, both are done in different ways. The router is more expensive and has many services that are not needed in the internal network of the branch, so it adds a higher overhead, especially considering the fact that with a multilayered switch, we gain the advantage of having the routing and switching on the same platform with low latency. Also, we lose the benefits of dividing the departments into different VLANs on the same LAN. A normal switch cannot be considered because it is a layer 2 device so it cannot do any routing.

Useful Commands:

- Standard Access List:

```
access-list access-list-number {permit|deny} {host|source source-wildcard|any}
interface <interface>
ip access-group number {in|out}
```

- Extended Access List:

```
access-list access-list-number {deny|permit} protocol source source-wildcard
destination destination-wildcard [eq port #]
interface <interface>
ip access-group number {in|out}
```

- Trunk VLAN:

```
vlan <number>
interface <interface>
switchport trunk encapsulation dot1q
switchport mode trunk
```

- Assign IP to VLAN:

```
interface vlan <number>

ip address <ip address> <subnet mask>
```

- Assign VLANs to interfaces:

```
interface fastEthernet <interface>
switchport mode access
switchport access vlan <number>
```

- Enable routing in MLS:

```
ip routing
```

- Dynamic Routing (EIGRP):

```
router eigrp autonomous_system_#
No auto-summary
network IP_network_# [subnet_mask]     (for all network interfaces connected)
```

- IPsec VPN:

```
access-list access-list-number permit ip {source wildcard} {destination wildcard}
crypto isakmp policy 10
   encryption aes 256
   authentication pre-share
   group 5
   exit
crypto isakmp key <password> address <other_int_ip_with_isp>
crypto ipsec transform-set <name> esp-aes 256 esp-sha-hmac
crypto map IPSEC-CRYPTOMAP <access-list-number> ipsec-isakmp
 set peer <other_int_ip_with_isp>
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set <name>
 match address <access-list-number>
interface <int_ip_with_isp>
 crypto map IPSEC-CRYPTOMAP
```

- Verify VPN tunnel:

```
show crypto ipsec sa
```

<u>Accounts of Routers:</u>

Username: Hall

Password: Access

<u>Access Lists on MLS:</u>

```
Standard IP access list 1
   10 deny 191.0.2.0 0.0.0.255
   20 deny 191.0.3.0 0.0.0.255 (7 match(es))
   30 deny 191.0.4.0 0.0.0.255
```

```
  40 deny 191.0.5.0 0.0.0.255
  50 deny 191.0.64.0 0.0.15.255
  60 permit any (3 match(es))
Standard IP access list 2
  10 deny 191.0.3.0 0.0.0.255 (5 match(es))
  20 deny 191.0.4.0 0.0.0.255
  30 deny 191.0.5.0 0.0.0.255
  40 deny 191.0.64.0 0.0.15.255
  50 permit any
Standard IP access list 3
  10 deny 191.0.4.0 0.0.0.255
  20 deny 191.0.5.0 0.0.0.255
  30 deny 191.0.64.0 0.0.15.255
  40 permit any (8 match(es))
Standard IP access list 4
  10 deny 191.0.2.0 0.0.0.255
  20 deny 191.0.3.0 0.0.0.255
  30 deny 191.0.4.0 0.0.0.255
  40 deny 191.0.64.0 0.0.15.255
  50 permit any
Standard IP access list 5
  10 deny 191.0.2.0 0.0.0.255
  20 deny 191.0.3.0 0.0.0.255
  30 deny 191.0.5.0 0.0.0.255
  40 deny 191.0.64.0 0.0.15.255
  50 permit any (10 match(es))
Extended IP access list 120
  10 permit tcp any any eq www (5 match(es))
  20 permit tcp any any eq 443

Extended IP access list 100
        10 deny ip 191.0.2.0 0.0.0.255 191.8.0.0 0.7.255.255
        20 deny ip 191.0.3.0 0.0.0.255 191.8.0.0 0.7.255.255
        30 deny ip 191.0.4.0 0.0.0.255 191.8.0.0 0.7.255.255
        40 deny ip 191.0.5.0 0.0.0.255 191.8.0.0 0.7.255.255
        50 deny ip 191.0.64.0 0.0.0.255 191.8.0.0 0.15.255.255
        60 permit ip any any
```

References:

- Access Lists and its configuration:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#standacl

https://networklessons.com/cisco/ccie-routing-switching/extended-access-list-example-on-cisco-router

- VLans and InterVLAN routing:

https://computernetworking747640215.wordpress.com/2018/07/05/vlan-configuration-on-a-cisco-switch-in-packet-tracer/

https://polar91.wordpress.com/2017/09/27/configure-multilayer-switch-on-packet-tracer/

- VPNS and Configuration:

https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

https://cybersecfaith.com/2020/11/01/setting-up-an-ipsec-vpn-using-cisco-packet-tracer/

- EIGRP (Dynamic Routing) and its configuration

https://networklessons.com/eigrp/introduction-to-eigrp

https://www.computernetworkingnotes.com/ccna-study-guide/eigrp-configuration-step-by-step-guide.html