AUC

THE AMERICAN UNIVERSITY IN CAIRO

Networks Project

Names: Joseph Hany Boulis, Abdelrahman Shaaban

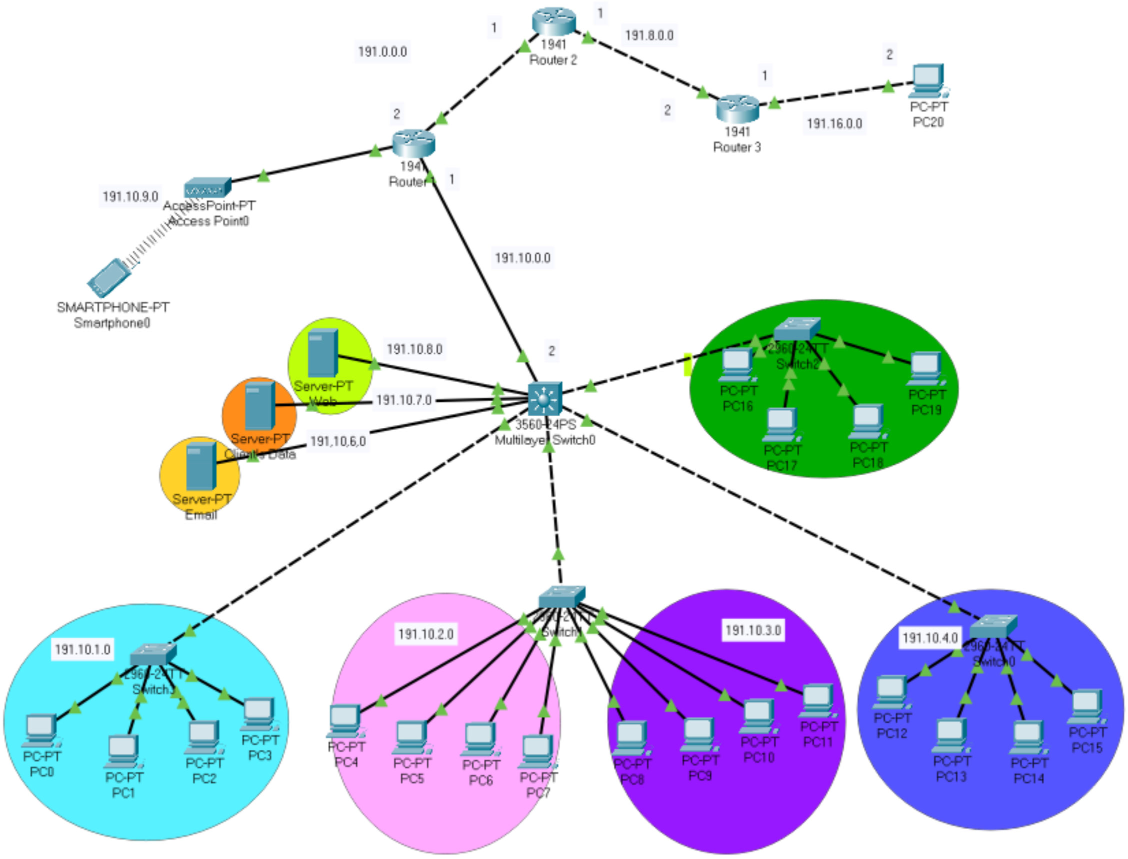
SIDs: 900182870, 900183004

Routing table

Device	IP	Subnet Mask		
PC0	191.10.1.2	255.255.255.0	Vlan 191.10.1.1	
PC1	191.10.1.3	255.255.255.0	Vlan 191.10.1.1	
PC2	191.10.1.4	255.255.255.0	Vlan 191.10.1.1	
PC3	191.10.1.5	255.255.255.0	Vlan 191.10.1.1	
PC4	191.10.2.2	255.255.255.0	Vlan 191.10.2.1	
PC5	191.10.2.3	255.255.255.0	Vlan 191.10.2.1	
PC6	191.10.2.4	255.255.255.0	Vlan 191.10.2.1	
PC7	191.10.2.5	255.255.255.0	Vlan 191.10.2.1	
PC8	191.10.3.2	255.255.255.0	Vlan 191.10.3.1	
PC9	191.10.3.3	255.255.255.0	Vlan 191.10.3.1	
PC10	191.10.3.4	255.255.255.0	Vlan 191.10.3.1	
PC11	191.10.3.5	255.255.255.0	Vlan 191.10.3.1	
PC12	191.10.4.2	255.255.255.0	Vlan 191.10.4.1	
PC13	191.10.4.3	255.255.255.0	Vlan 191.10.4.1	
PC14	191.10.4.4	255.255.255.0	Vlan 191.10.4.1	
PC15	191.10.4.5	255.255.255.0	Vlan 191.10.4.1	
PC16	191.10.5.2	255.255.255.0	Vlan 191.10.5.1	
PC17	191.10.5.3	255.255.255.0	Vlan 191.10.5.1	
PC18	191.10.5.4	255.255.255.0	Vlan 191.10.5.1	
PC19	191.10.5.5	255.255.255.0	Vlan 191.10.5.1	

Server 1 (Email)	191.10.6.2	255.255.255.0	Vlan 191.10.6.1	
Server 2 (Client’s Data)	191.10.7.2	255.255.255.0	Vlan 191.10.7.1	
Server 3 (Web)	191.10.8.2	255.255.255.0	Vlan 191.10.8.1	
Router 1	191.10.0.1	255.255.255.0		Gig0/0
	191.0.0.2	255.248.0.0		Gig0/1
Router 2	191.0.0.1	255.248.0.0		Gig0/0
	191.8.0.1	255.248.0.0		Gig0/1
Router 3	191.8.0.2	255.248.0.0		Gig0/0
	191.16.0.1	255.255.0.0		Gig0/1
PC20	191.16.0.2	255.255.0.0	191.16.0.1	
AP0	191.10.9.2	255.255.255.0	191.10.9.1	f0/9 (vlan 9)

Networks Topology



Description of the architecture:

In order to construct our architecture, we followed the following design requirements:

1) Security

   In order to fulfill the requirement of the security, we adopted the following:

   - Using the VLAN approach and Layer 3 switch allowed more control over implementing the security policies and creating fully-independent Vlans that have restrictions on accessing each other based on the access list.
   - Using VPN to communicate with the second branch and troubleshooting its devices by the IT department provides more protection on the system’s online privacy.
   - Using Firewall on each server to protect it against any access by unauthorized users.

- Creating an isolated Guest-WiFi network that is independent of the branch's main network (Multilayer Switch) allows more protection against the servers' attacks.

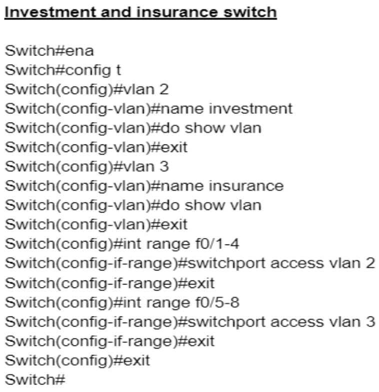
2) Performance

   In order to fulfill this requirements, we used the multilayer switch instead of a router which gives us the following benefits:
   - Provides high-speed scalability with low latency.
   - Move traffic at wire speed and also provide layer 3 routing.
   - Gain the benefits of both switching and routing on the same platform.
   - Allows administrators in the bank to collapse the network, create fewer layers, while still maintaining the same level of redundancy.

3) Cost
   - The cost of the multilayer switch is lower than the router which achieves an acceptable cost for the whole network.
   - We used one common switch for two VLANs since they do not interact with each other in the first place. Thus, we saved the cost of an extra switch.

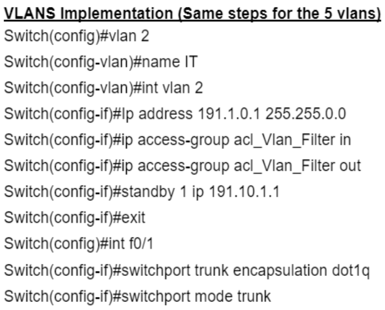
<u>Documenting the commands and screenshots for each implemented functionality:</u>

1) Below is the implementation of the proposed topology, creating the vlans in the multilayer switch, trunking between the multilayer switch' s ports and each department's switches, configuring the servers, and enabling the routing in the multilayer switch. The main purpose of adding a switch for each department is to consider the case of more than 4 hosts in the department "The Extendability".
   In addition, you can find below how the VLANs are divided into groups as each VLAN was considered as an access list group with an 'in' and 'out' ports to be used as filters to restrict the flow of the network traffic through it based on the logic of the access lists, tha.



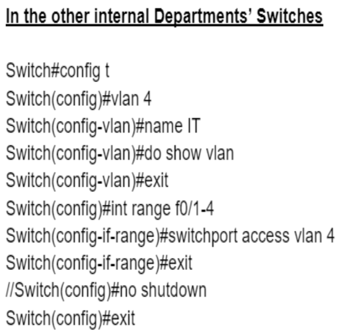
Investment and insurance switch

```
Switch#ena
Switch#config t
Switch(config)#vlan 2
Switch(config-vlan)#name investment
Switch(config-vlan)#do show vlan
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name insurance
Switch(config-vlan)#do show vlan
Switch(config-vlan)#exit
Switch(config)#int range f0/1-4
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#int range f0/5-8
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
```



VLANS Implementation (Same steps for the 5 vlans)

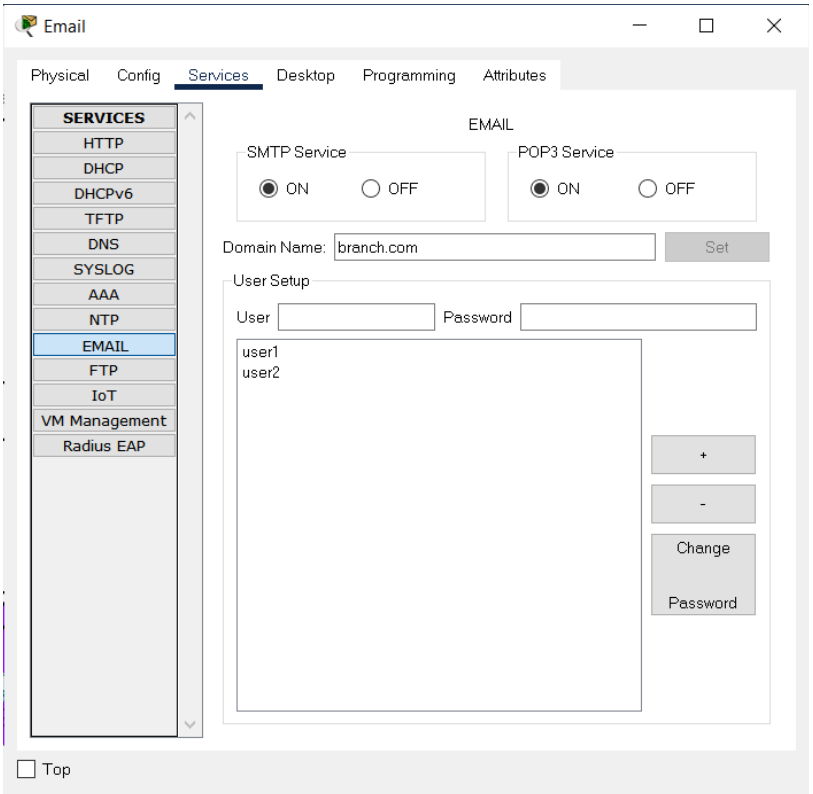
```
Switch(config)#vlan 2
Switch(config-vlan)#name IT
Switch(config-vlan)#int vlan 2
Switch(config-if)#Ip address 191.1.0.1 255.255.0.0
Switch(config-if)#ip access-group acl_Vlan_Filter in
Switch(config-if)#ip access-group acl_Vlan_Filter out
Switch(config-if)#standby 1 ip 191.10.1.1
Switch(config-if)#exit
Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```



In the other internal Departments' Switches

```
Switch#config t
Switch(config)#vlan 4
Switch(config-vlan)#name IT
Switch(config-vlan)#do show vlan
Switch(config-vlan)#exit
Switch(config)#int range f0/1-4
Switch(config-if-range)#switchport access vlan 4
Switch(config-if-range)#exit
//Switch(config)#no shutdown
Switch(config)#exit
```

2) Setting up the Email service in the email server:



EMAIL

SMTP Service: ● ON ○ OFF

POP3 Service: ● ON ○ OFF

Domain Name: branch.com

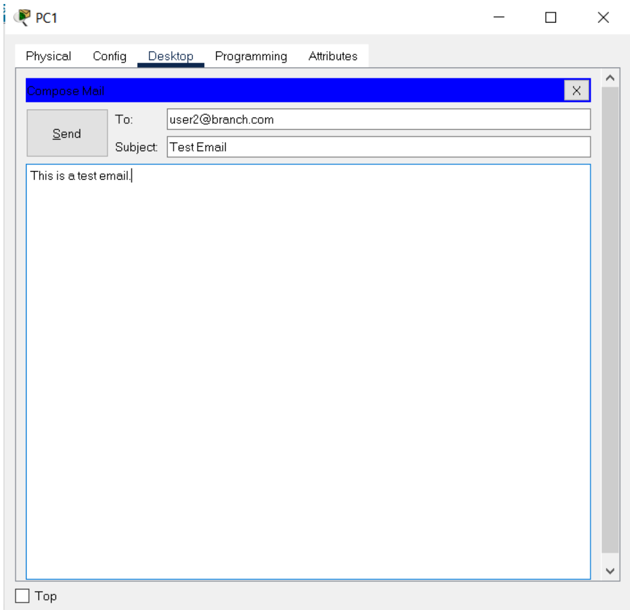
User Setup

User

Password

user1
user2

Sending a message from and to two local PCs in the same vlan:

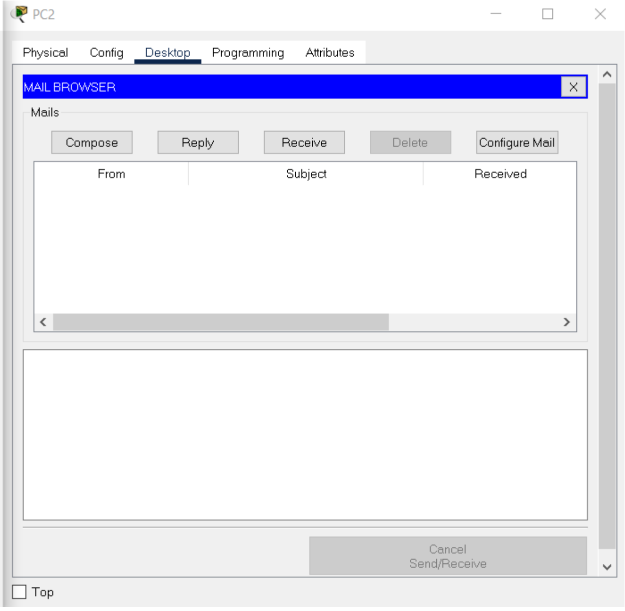


Compose Mail

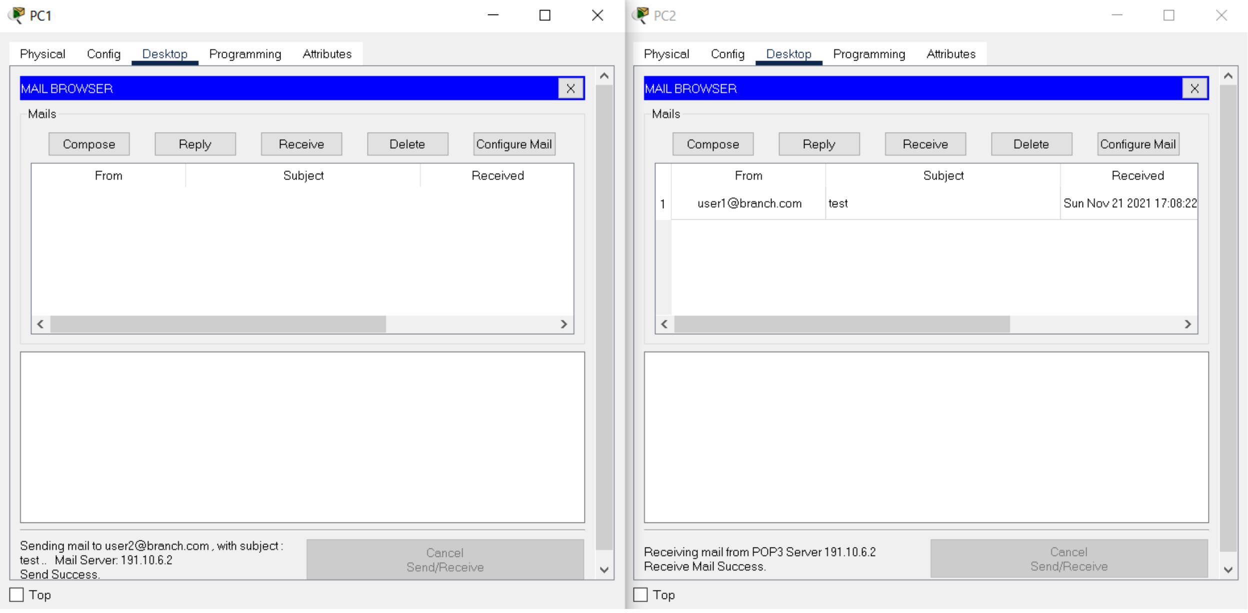
To: user2@branch.com

Subject: Test Email

This is a test email.



The below screenshot shows that the message has been received successfully by PC2:



PC1:

From	Subject	Received

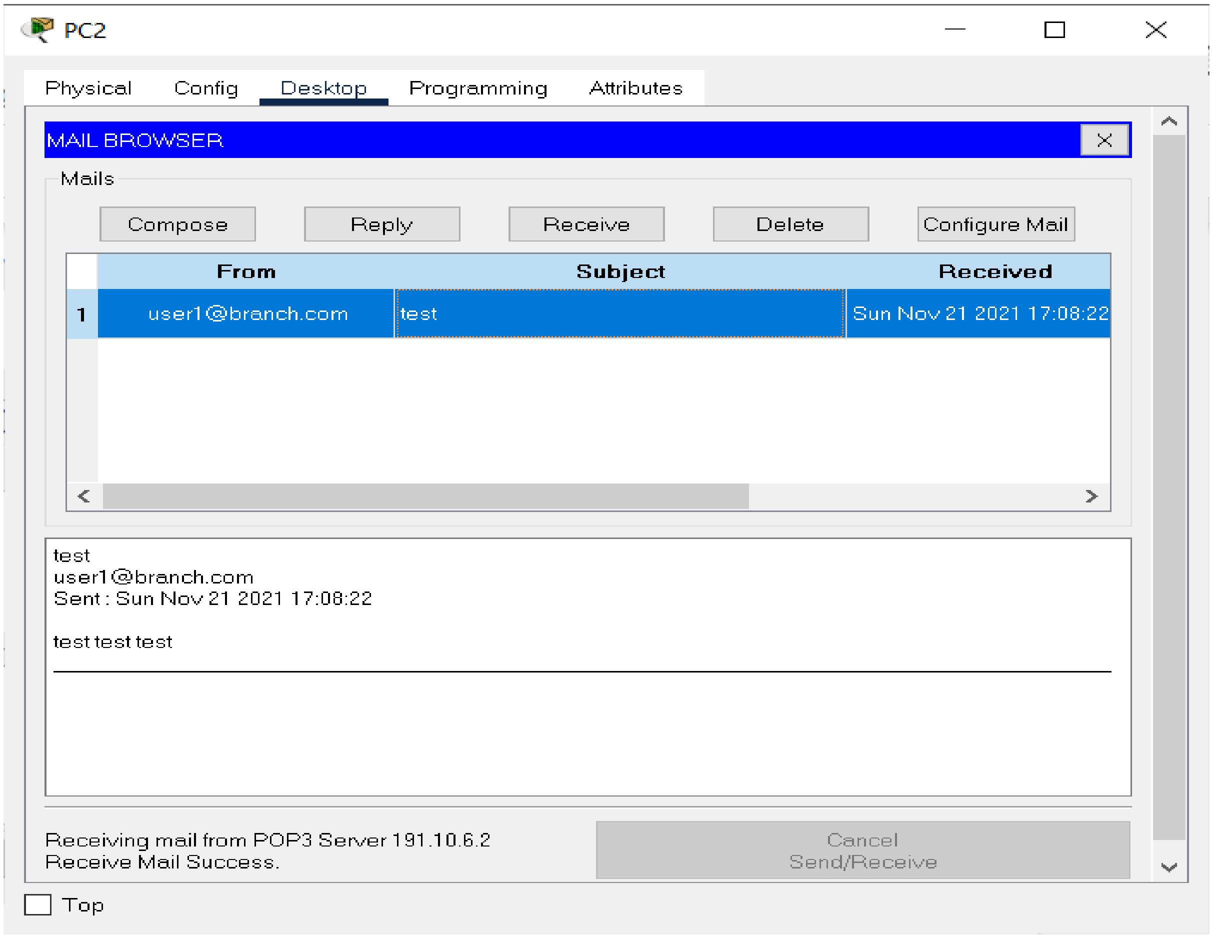
Sending mail to user2@branch.com , with subject : test .. Mail Server: 191.10.6.2
Send Success.

PC2:

	From	Subject	Received
1	user1@branch.com	test	Sun Nov 21 2021 17:08:22

Receiving mail from POP3 Server 191.10.6.2
Receive Mail Success.

Showing the content of the message itself:



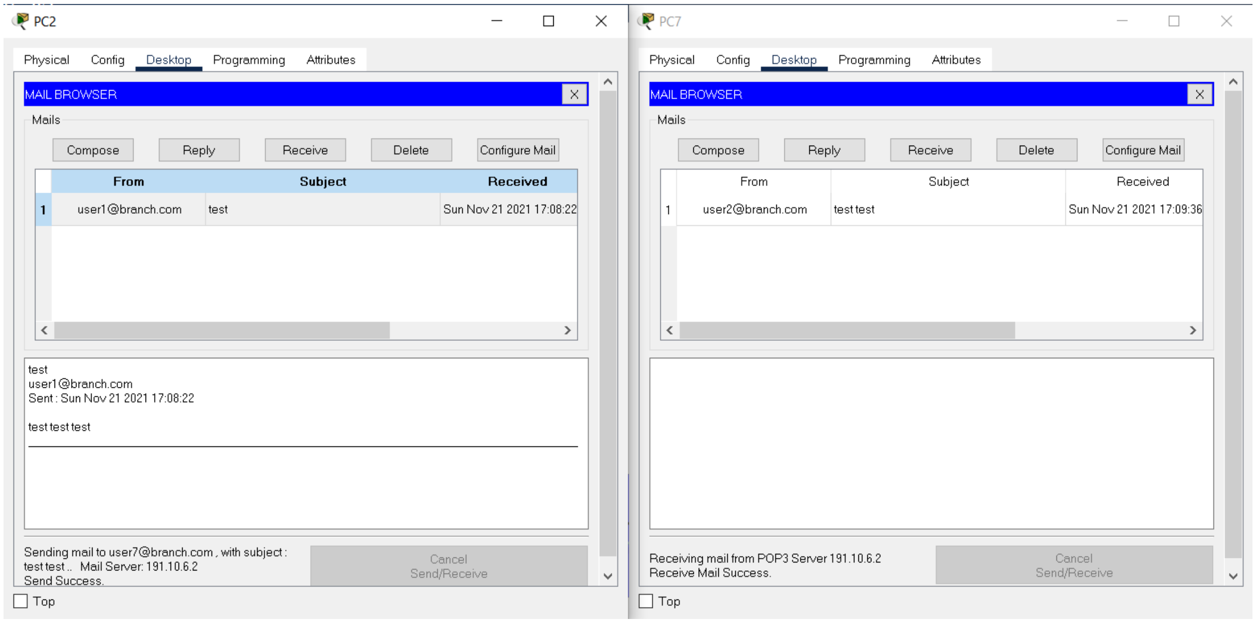
	From	Subject	Received
1	user1@branch.com	test	Sun Nov 21 2021 17:08:22

test
user1@branch.com
Sent : Sun Nov 21 2021 17:08:22

test test test

Receiving mail from POP3 Server 191.10.6.2
Receive Mail Success.

Sending a message from and to two PCs in the different vlans:



PC2

	From	Subject	Received
1	user1@branch.com	test	Sun Nov 21 2021 17:08:22

test
user1@branch.com
Sent : Sun Nov 21 2021 17:08:22

test test test

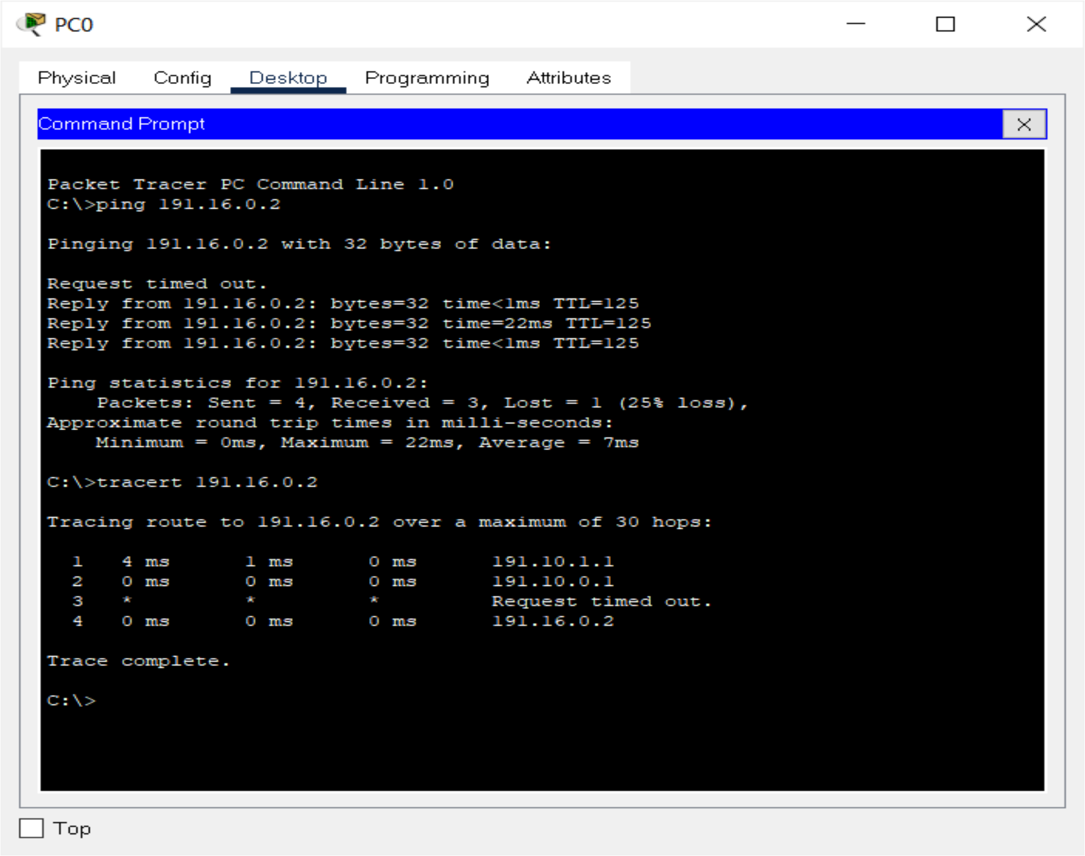
Sending mail to user7@branch.com , with subject : test test .. Mail Server: 191.10.6.2
Send Success.

PC7

	From	Subject	Received
1	user2@branch.com	test test	Sun Nov 21 2021 17:09:36

Receiving mail from POP3 Server 191.10.6.2
Receive Mail Success.

Showing the VPN in action through pining PC20 from PC1 while shedding light on the route it took by using tracert command:



```
Packet Tracer PC Command Line 1.0
C:\>ping 191.16.0.2

Pinging 191.16.0.2 with 32 bytes of data:

Request timed out.
Reply from 191.16.0.2: bytes=32 time<1ms TTL=125
Reply from 191.16.0.2: bytes=32 time=22ms TTL=125
Reply from 191.16.0.2: bytes=32 time<1ms TTL=125

Ping statistics for 191.16.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 7ms

C:\>tracert 191.16.0.2

Tracing route to 191.16.0.2 over a maximum of 30 hops:

  1   4 ms      1 ms      0 ms      191.10.1.1
  2   0 ms      0 ms      0 ms      191.10.0.1
  3   *         *         *         Request timed out.
  4   0 ms      0 ms      0 ms      191.16.0.2

Trace complete.

C:\>
```

The commands used for setting the ipsec VPN configuration up:

On Router 1, write the following commands:

Initializing the interfaces

```
hostname R1
interface g0/0
ip address 191.10.0.1 255.255.0.0
no shut
interface g0/1
ip address 191.0.0.2 255.248.0.0
no shut
exit
```

Defining the gateway (static routing)

```
ip route 0.0.0.0 0.0.0.0 191.0.0.1
```

Installing the license and saving the configuration

```
license boot module c1900 technology-package securityk9
end
copy running-config startup-config
reload
```

Configuring VPN on router 1

```
access-list 100 permit ip 191.10.0.0 0.0.255.255 191.16.0.0 0.0.255.255
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key secretkey address 191.8.0.2
crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 191.8.0.2
set pfs group5
set security-association lifetime seconds 86400
set transform-set R1-R3
match address 100
interface GigabitEthernet0/1
crypto map IPSEC-MAP
```

On Router 3, write the following commands:

Initializing the interfaces

```
hostname R2
interface g0/1
ip address 191.16.0.1 255.255.0.0
no shut
interface g0/0
ip address 191.8.0.2 255.248.0.0
no shut
exit
```

Defining the gateway (static routing)

```
ip route 0.0.0.0 0.0.0.0 191.8.0.1
```

Installing the license and saving the configuration

```
license boot module c1900 technology-package securityk9
end
copy running-config startup-config
reload
```

Configuring VPN on router 3

```
access-list 100 permit ip 191.16.0.0 0.0.255.255 191.10.0.0 0.0.255.255
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key secretkey address 191.0.0.2
crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 191.0.0.2
set pfs group5
set security-association lifetime seconds 86400
set transform-set R3-R1
match address 100
interface GigabitEthernet0/0
crypto map IPSEC-MAP
```

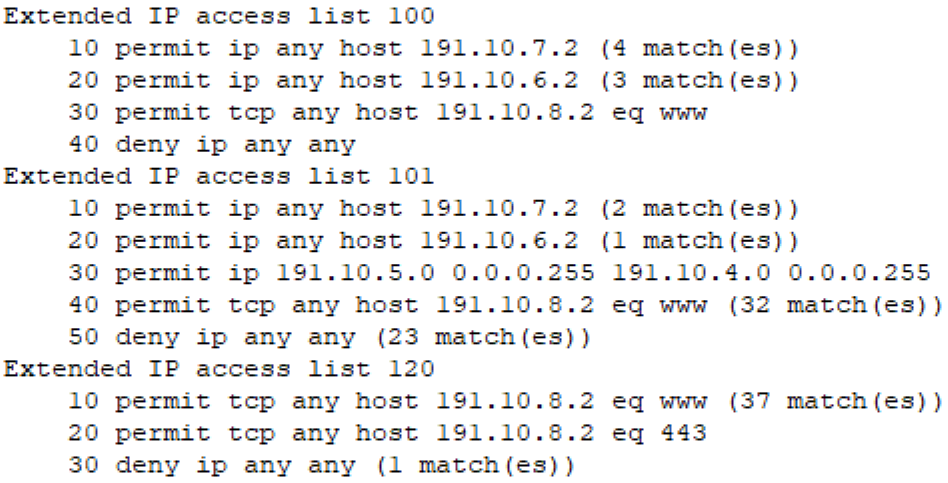
On Router 2, write the following commands:

```
en
config t
hostname ISP
int g0/0
ip add 191.0.0.1 255.248.0.0
no shut
exit
int g0/1
ip add 191.8.0.1 255.248.0.0
no shut
```

In order to verify that the VPN works, we write the following command router 1

```
show crypto ipsec sa
```

Access Lists



```
Extended IP access list 100
    10 permit ip any host 191.10.7.2 (4 match(es))
    20 permit ip any host 191.10.6.2 (3 match(es))
    30 permit tcp any host 191.10.8.2 eq www
    40 deny ip any any
Extended IP access list 101
    10 permit ip any host 191.10.7.2 (2 match(es))
    20 permit ip any host 191.10.6.2 (1 match(es))
    30 permit ip 191.10.5.0 0.0.0.255 191.10.4.0 0.0.0.255
    40 permit tcp any host 191.10.8.2 eq www (32 match(es))
    50 deny ip any any (23 match(es))
Extended IP access list 120
    10 permit tcp any host 191.10.8.2 eq www (37 match(es))
    20 permit tcp any host 191.10.8.2 eq 443
    30 deny ip any any (1 match(es))
```

For the Vlans of the Investments, insurance, and loans Departments as they have only access for the three servers. The web server can be accessed only through the ports 80 for the HTTP and 443 for the ports HTTPS:

```
Switch(config)#access-list 100 per ip any host 191.10.7.2
Switch(config)#access-list 100 per ip any host 191.10.6.2
Switch(config)#access-list 100 per tcp any host 191.10.8.2 eq 80
Switch(config)#access-list 100 per tcp any host 191.10.8.2 eq 443
Switch(config)#access-list 100 deny ip any any
Switch(config)#
```

For the Vlan of the help desk department, in addition to the above configuration, it needed an additional access permit to the loans Vlan

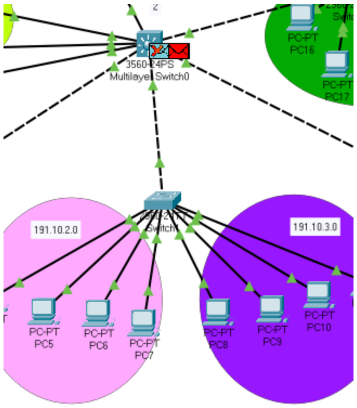
```
Switch(config)#access-list 101 permit ip any host 191.10.7.2
Switch(config)#access-list 101 permit ip any host 191.10.6.2
Switch(config)#access-list 101 permit ip 191.10.5.0 0.0.0.255 191.10.4.0 0.0.0.255
Switch(config)#access-list 101 permit tcp any host 191.10.8.2 eq 80
Switch(config)#access-list 101 permit tcp any host 191.10.8.2 eq 443
Switch(config)#access-list 101 deny ip any any
Switch(config)#int vlan 6
Switch(config-if)#ip access-group 101 in
```

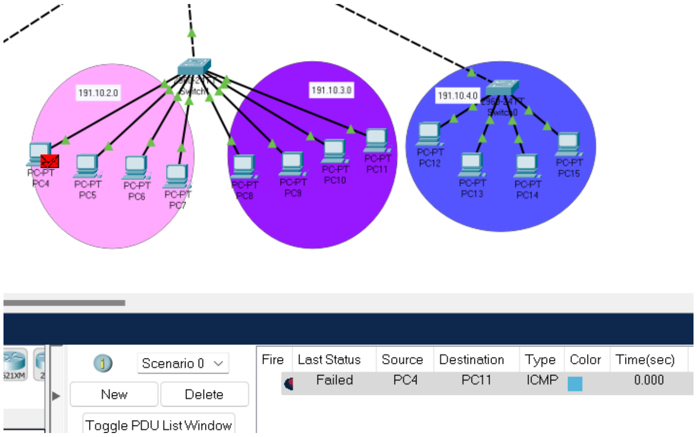
The last Access list was added to restrict the access of the IT department to the web server to be excluded only on the HTTP and the HTTPs Ports.

Since each vlan was considered as a group with an in and out places for filters to restrict the flow of the network traffic through it based on the logic of the access lists.

Below are screenshots of how the access lists worked correctly.

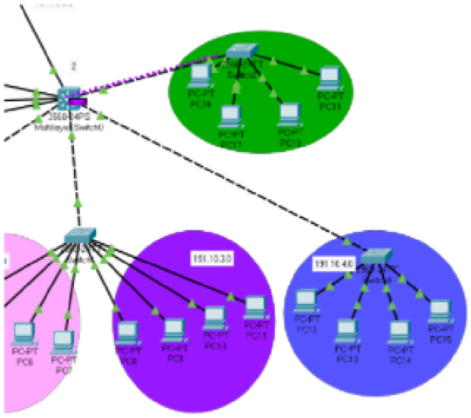
1- Investment - Insurance: No communication between them.

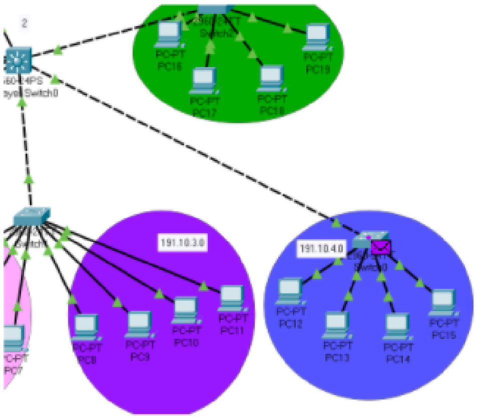


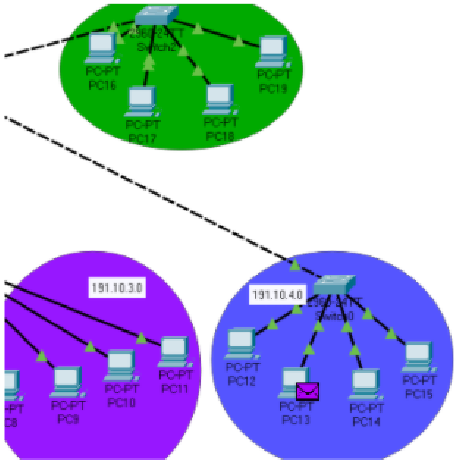


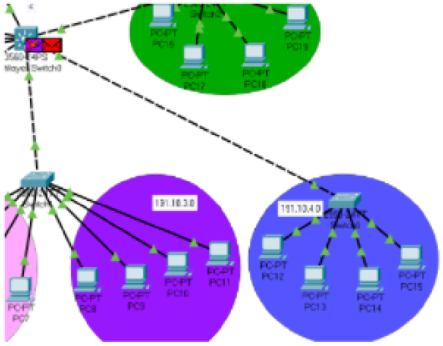
Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Failed	PC4	PC11	ICMP	🟦	0.000

2- Help Desk- Loans: Help Desk can access the loans department but not the opposite.

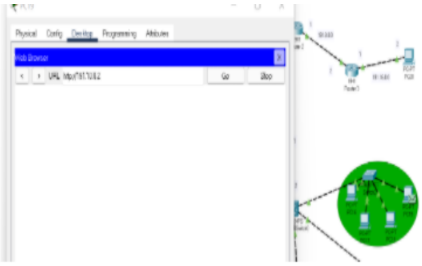




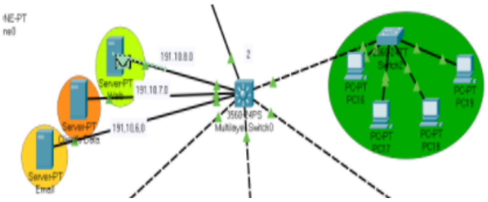


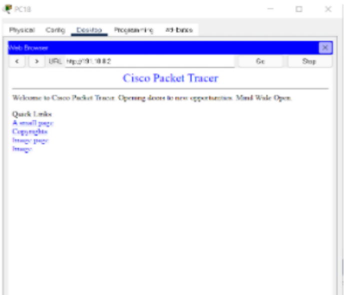


3- Help Desk- Web Server: No ping allowed but browsing is by using only the port 80 for HTTP and 443 for HTTPs.



URL http://191.10.8.2





URL http://191.10.8.2

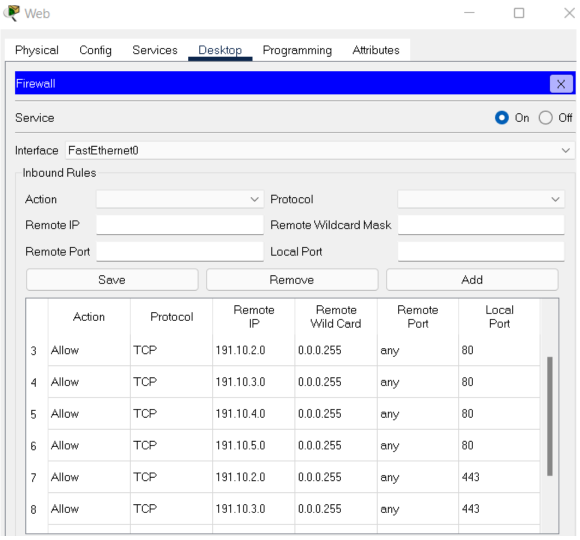
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links
A small page
Copyrights
Image page
Image

Firewalls:

1- Web Server



Service ● On ○ Off

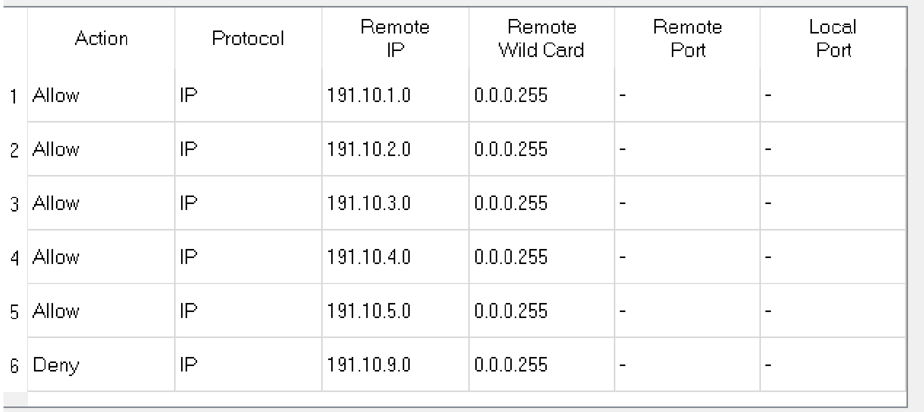
Interface FastEthernet0

Inbound Rules

Action
Protocol
Remote IP
Remote Wildcard Mask
Remote Port
Local Port

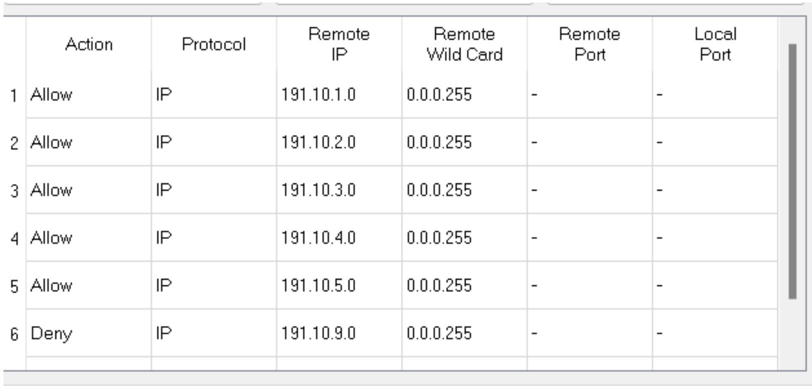
	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
3	Allow	TCP	191.10.2.0	0.0.0.255	any	80
4	Allow	TCP	191.10.3.0	0.0.0.255	any	80
5	Allow	TCP	191.10.4.0	0.0.0.255	any	80
6	Allow	TCP	191.10.5.0	0.0.0.255	any	80
7	Allow	TCP	191.10.2.0	0.0.0.255	any	443
8	Allow	TCP	191.10.3.0	0.0.0.255	any	443

2- Data Server



	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	IP	191.10.1.0	0.0.0.255	-	-
2	Allow	IP	191.10.2.0	0.0.0.255	-	-
3	Allow	IP	191.10.3.0	0.0.0.255	-	-
4	Allow	IP	191.10.4.0	0.0.0.255	-	-
5	Allow	IP	191.10.5.0	0.0.0.255	-	-
6	Deny	IP	191.10.9.0	0.0.0.255	-	-

3- Email Server



	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	IP	191.10.1.0	0.0.0.255	-	-
2	Allow	IP	191.10.2.0	0.0.0.255	-	-
3	Allow	IP	191.10.3.0	0.0.0.255	-	-
4	Allow	IP	191.10.4.0	0.0.0.255	-	-
5	Allow	IP	191.10.5.0	0.0.0.255	-	-
6	Deny	IP	191.10.9.0	0.0.0.255	-	-

Questions

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

Yes, if we forgot to save our configuration, we will lose the configuration we did. In other words, the configuration register (a special 16 bits value that can be configured in Cisco routers to determine how the router boots and specify the boot options) that should contain the new configuration will not be updated and will still be holding the original startup configuration we started with.

We can solve this issue by saving the configuration by using the following command:

- copy running-config startup-config (this command copies the current active configuration to NVRAM)
- wr (this command which writes memory is responsible for copying the configuration into flash and saving it even after the router is powered off and restarted).

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

In order to secure the server hosting the clients' DB we need to follow one of the following options:

1) We can encrypt the stored files and backups

If we stored such information in plain text, any attacher or even an employer can easily access, steal, or even destroy the sensitive data contained in the server. Thus, the data must be encrypted, especially if the storage server is out of the administrator's security authority.

2) We can install SSL certificates

In order to guard the communication between our server and any other system over the internet, we can install the secure socket layer certificates security protocols. Such certificates constitute a crucial server security element that ensures that data transfer or communication in general between our server and any other server or client is encrypted. Even if an attacker managed to get the data, he/she will not be able to decipher it and understand its meaning, rather the only One who will understand its meaning will be the intended recipient that has the right decryption keys.

3) We can use severe password security policies

To elaborate, the bank should use password best practices. For example, clear password policies and rules should be developed and used by all the members who are using the server. Moreover, password complexity guidelines should be set and minimum character length for passwords should be specified, not to mention enabling session timeout for inactivity, using a multiple-factor authentication strategy, and having a clear password expiration policy.

4) We can use private networking (VPNs) which will allow us to carry out operations on our server in a secure manner.

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

The main type of access restriction used in the wireless router in our network is the extended access list that restricts the guests' access to be only to the web server with enabling only port 80 for HTTP browsing and port 443 for HTTPs browsing.
If we used DHCP pool to dynamically assign the IPs to the guests instead of using static assignments, that would result in another type of access restriction "DHCP enforcement", which enforces limited access by issuing restricted network IP addresses to the hosts and mainly restricts the connection of the hosts with static IP addresses.

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

Since our network mainly consists of 2 branch routers and a multilayer switch from which the rest of the network stems, removing the multilayer switch will affect the whole internal network structure of each branch. Moreover, removing the multilayer switch will deprive us from the benefits that we get from using it. These benefits include:

1) Providing high-speed scalability with low latency.
2) Moving the traffic at wire speed while providing layer 3 routing.
3) Allowing administrators at the bank to collapse the network, creating fewer layers, while still maintaining the same level of redundancy.
4) Meeting the higher-performance need for the connectivity of intranets and multimedia applications.

Thus, the benefits gained of both switching and routing on the same platform will be totally gone when we remove it.