Question 2: Networking Simulation (Cisco Packet Tracer)

You have recently been hired as a **Network Security Engineer Intern** at a mid-sized financial services company that is rapidly expanding across Africa and Europe. The company has requested that you **design and implement a secure small enterprise network** using **Cisco Packet Tracer** to simulate its branch office infrastructure.

The branch office has three core departments:

- **Administration (Admin VLAN)** – responsible for HR and Finance.
- **Sales (Sales VLAN)** – responsible for customer engagement and business growth.
- **IT Support (IT VLAN)** – responsible for managing technical operations.

Your Task

1. **Network Design & VLAN Segmentation**
    - Create at least **three VLANs** (Admin, Sales, and IT) with appropriate subnetting.
    - Assign each department to its VLAN and ensure end devices can only communicate within their assigned VLAN by default.
2. **Inter-VLAN Routing**
    - Configure a **Router-on-a-Stick (ROAS)** or **Layer 3 Switch** to allow secure communication between VLANs.
    - Ensure the routing is functional but controlled through security policies.
3. **Access Control Lists (ACLs)**
    - Apply **standard/extended ACLs** to **restrict traffic**:
        - Admin VLAN should only access Sales VLAN for reporting but not IT VLAN.
        - Sales VLAN should not access Admin VLAN but should be able to access IT VLAN for system support.
        - IT VLAN should have unrestricted access to all VLANs for administrative purposes.
    - Document the **security justification** behind each ACL rule.
4. **Secure Remote Access**
    - Configure **SSH (Secure Shell)** on the network devices (router/switch) for secure remote management.
    - Disable insecure protocols such as Telnet.
5. **Deliverables**
    - **Network Topology Diagram** showing devices, connections, and VLAN assignments.
    - **Configuration Commands** used for VLANs, routing, ACLs, and SSH setup.
    - A **Security Justification Report** explaining how your ACLs enforce the principle of least privilege and protect sensitive departmental resources.

REPORT

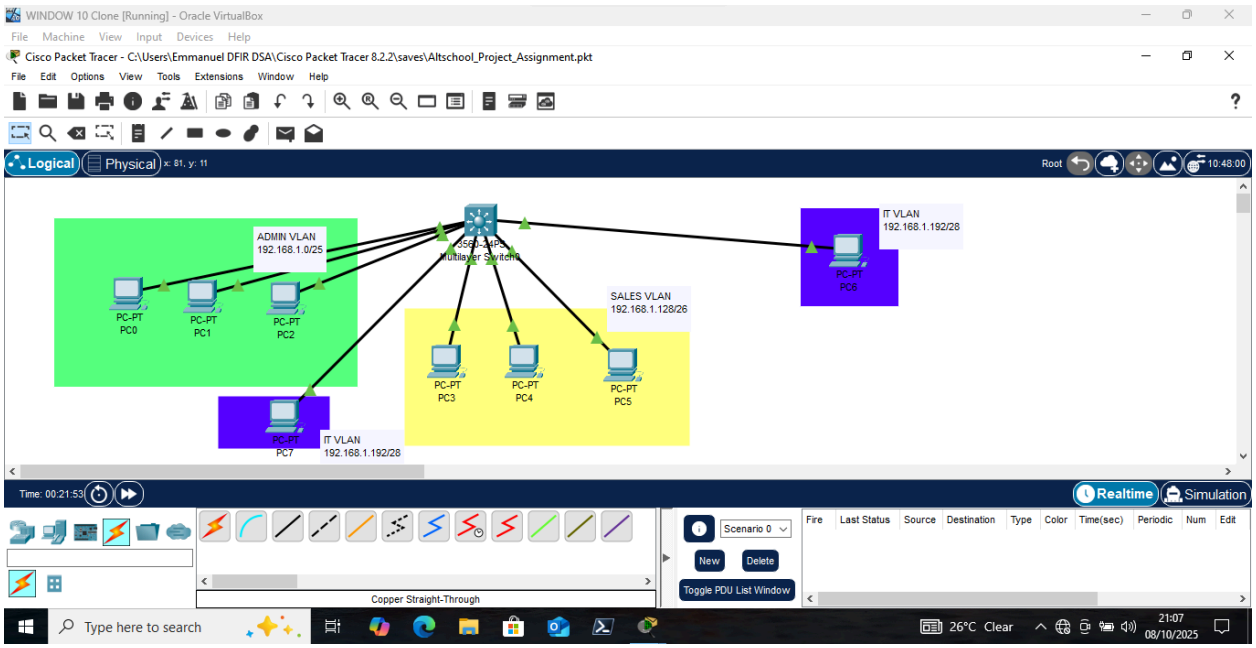
Description: This Project shows a simulation of a network architecture setup where a secure small enterprise network with three core department Administration, Sales and IT support form the following Vlans: ADMIN_VLAN, SALES_VLAN, IT_VLAN which were allowed to communicate through inter-vlan routing and secured through the use of Access Control List (ACLS) for least privilege of access and secure remote access through SSH for management of critical infrastructure.

TOOLS USED:

- Virtual Box
- Windows 10 Client
- Cisco Packet Tracer
- Layer3 switch
- PCs
- Snipping tool

Tools Used	**Description**
Virtual Box	This acts as the hypervisor used to simulate this lab
Windows 10 client	This is the base operating system upon which the applications used for this lab would run
Cisco Packet Tracer	This is the application used for this lab setup, including the network architecture design, configuration, and testing
Layer3 Switch	This was the choice device for my network architecture; it possesses the ability to perform inter-vlan routing
PCs	There are about 8 PCs used in the network architecture
Snipping Tool	This was used to take various vital screenshots that are shown in this report.

Network Architecture Setup



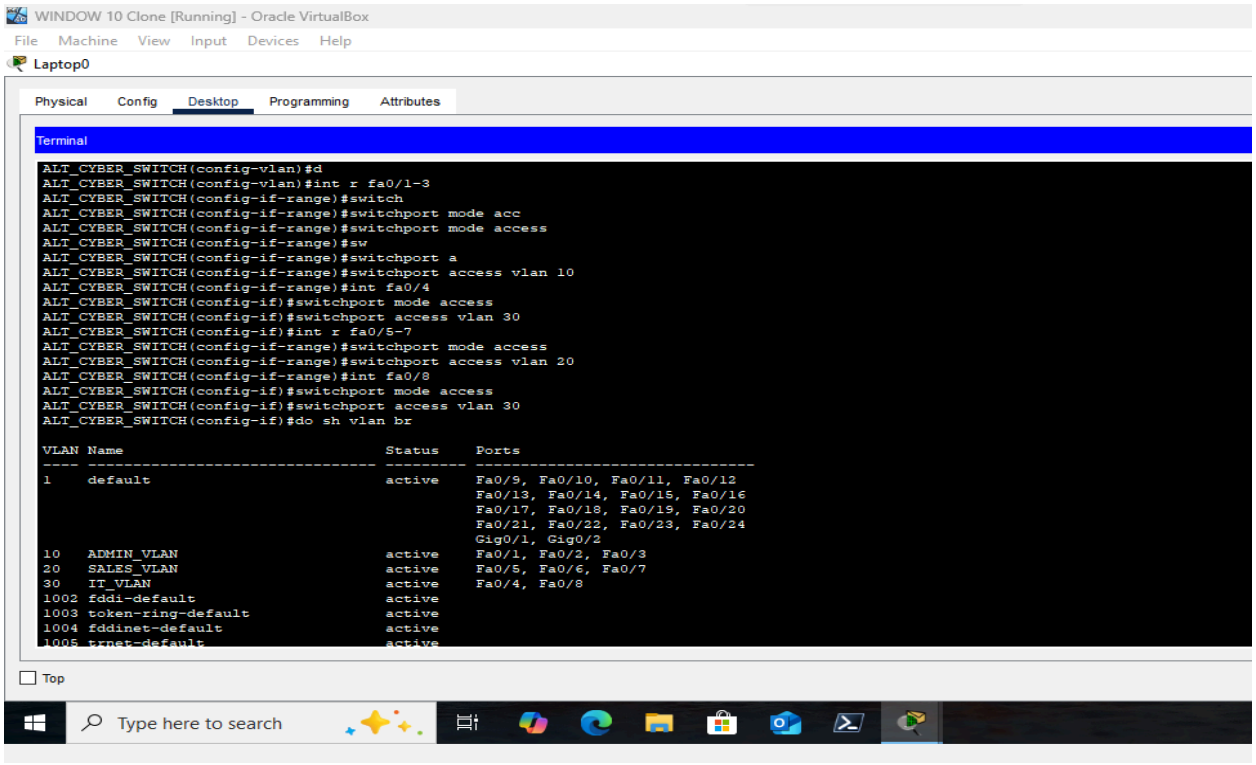
The snippet above shows the network architecture setup for this lab, and it consists of `one layer 3 switch` and `3 PCs highlighted in green as in the VLAN 10`, which is the `ADMIN_VLAN`, and they were configured with the IP address range `192.168.1.0/25 (subnet mask 255.255.255.128)`, with the `ADMIN_VLAN gateway` being `192.168.1.1/25` and `3 PCs highlighted in yellow as in VLAN 20` which is the `SALES_VLAN` and they were configured with the IP address range `192.168.1.128/26 (subnet mask 255.255.255.192)` with the `SALES_VLAN gateway being 192.168.1.129/26` and `2 PCs highlighted in blue as in VLAN 30` which is the `IT_VLAN` and they were configured with the IP address range of `192.168.1.192/28 (subnet mask 255.255.255.240)` with the `IT_VLAN gateway being 192.168.1.193/28`

VLAN CREATION AND CONFIRMATION

As seen in the snippet below, the hostname of the switch was changed with the command `"hostname ALT_CYBER_SWITCH"` at the global configuration mode and then Vlans were created using the command format `"vlan vlan_number"` and `"name vlan_name,"` and the ports were assigned to the Vlan by entering the interface or interfaces through the command `"interface interface_number" or "interface range interface_starting_point-interface_ending_point."` at the global config mode then the interface configuration mode and the command `"switchport mode access"` to

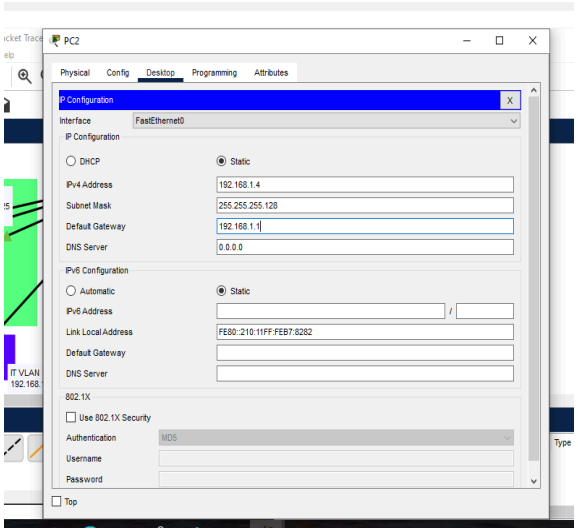
ensure the port acts as `an access port` and not trunk port or hybrid port and then `"switchpoint access vlan_number"` to access the specified Vlan.

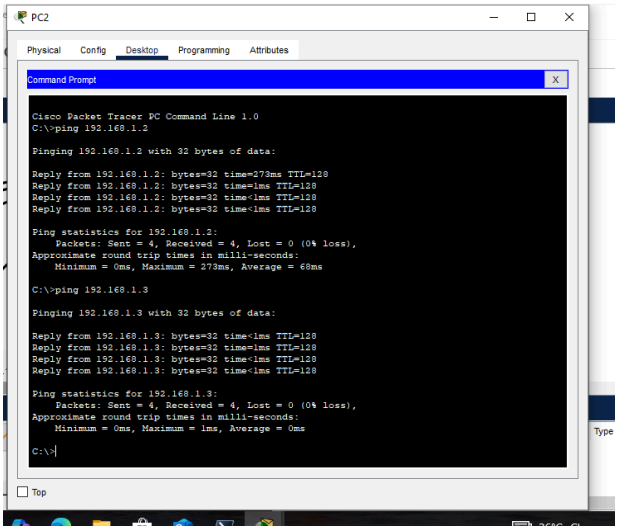
The commands are tested through the `"show vlan brief"` command

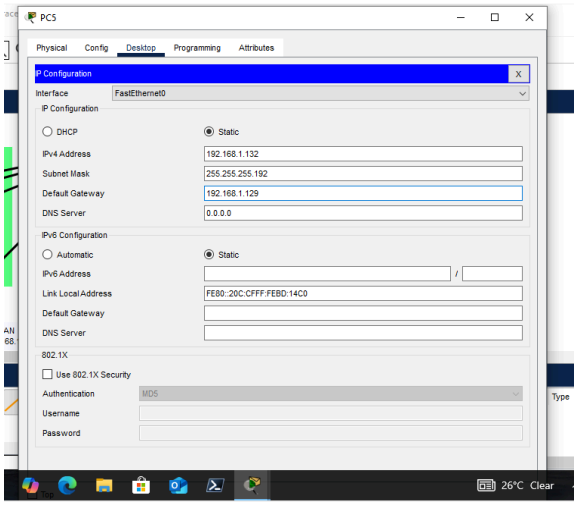


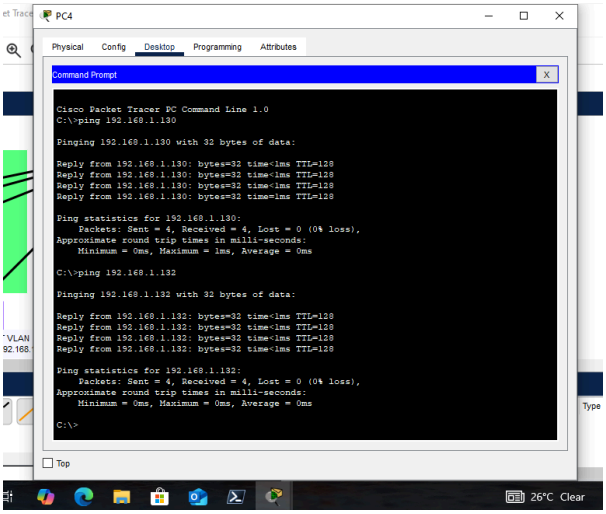
IP configuration at the PCs

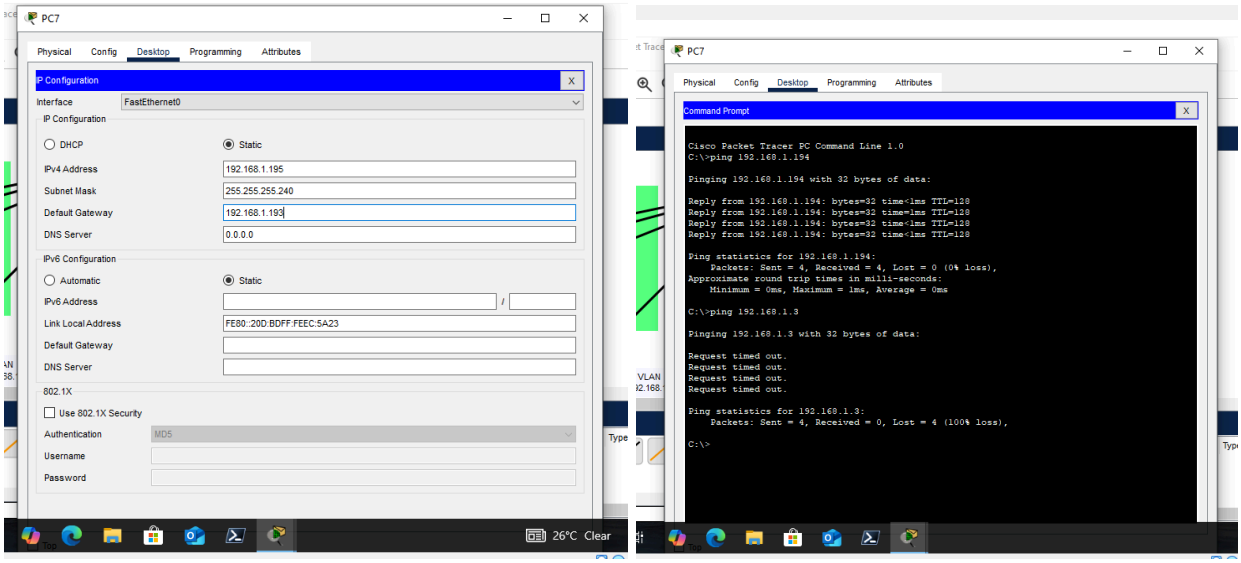
The IP addresses were individually set up for the PCs at the various VLANs and with their respective default gateway IP address, and tested to see if communication happened on the same VLANs. The following Snippets show this


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.128
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::210:11FF:FEB7:8282
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=273ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 273ms, Average = 68ms
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.132
Subnet Mask
255.255.255.192
Default Gateway
192.168.1.129
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20C:CFFF:FEBD:14C0
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
26°C Clear

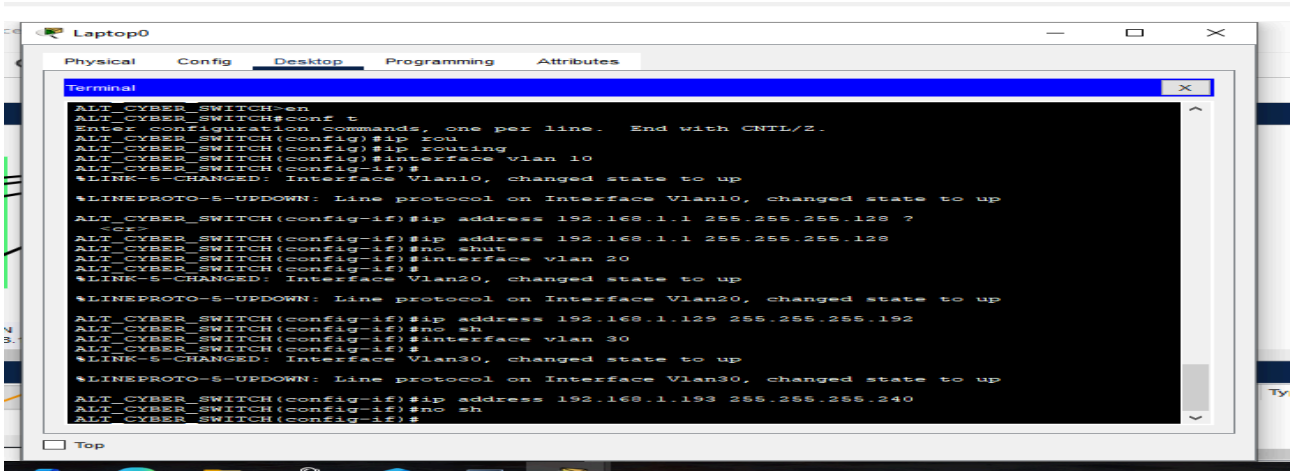

PC4
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.130
Pinging 192.168.1.130 with 32 bytes of data:
Reply from 192.168.1.130: bytes=32 time<1ms TTL=128
Reply from 192.168.1.130: bytes=32 time<1ms TTL=128
Reply from 192.168.1.130: bytes=32 time<1ms TTL=128
Reply from 192.168.1.130: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.132
Pinging 192.168.1.132 with 32 bytes of data:
Reply from 192.168.1.132: bytes=32 time<1ms TTL=128
Reply from 192.168.1.132: bytes=32 time<1ms TTL=128
Reply from 192.168.1.132: bytes=32 time<1ms TTL=128
Reply from 192.168.1.132: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.132:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top
26°C Clear



INTER-VLAN ROUTING

On the layer switch, Inter-vlan routing was configured using the commands "`ip routing`", which was configured on the switch in the global configuration mode, and the "`interface Vlan(vlan_number)`" command to enter the interface configuration of the Vlan and the "`ip address h.h.h.h x.x.x.x`" command to configure the ip address of the default gateway of the various Vlans, when `h` is the ip address and `x` is the subnet mask and the "`no shutdown`" command which is used to bring the status of the interface to `up`

The snippet below shows the use of the commands and the verification of the inter-vlan routing being active



```
!
hostname ALT_CYBER_SWITCH
!
!
!
!
!
!
ip routing
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
 --More-- |
```

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 0010.1146.b901
 ip address 192.168.1.1 255.255.255.128
!
interface Vlan20
 mac-address 0010.1146.b902
 ip address 192.168.1.129 255.255.255.192
!
interface Vlan30
 mac-address 0010.1146.b903
 ip address 192.168.1.193 255.255.255.240
!
ip classless
!
ip flow-export version 9
!
```

PC0

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.130

Pinging 192.168.1.130 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.130: bytes=32 time<1ms TTL=127
Reply from 192.168.1.130: bytes=32 time<1ms TTL=127
Reply from 192.168.1.130: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.130:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.194

Pinging 192.168.1.194 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.194: bytes=32 time<1ms TTL=127
Reply from 192.168.1.194: bytes=32 time<1ms TTL=127
Reply from 192.168.1.194: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.194:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

IMPLEMENTATION OF ACCESS CONTROL LISTS(ACLs)

Access Control Lists (ACLs) are tools used to determine the type of access that can be given to a network, network host, and so on. In this example, the extended ACLs were used, and they are in the form: "`access-list acl-list-number action protocol source_ip wildcard destination_ip wildcard`".

It was configured in the global configuration mode, and to implement it, we entered the interface through "`interface vlan(vlan_number)` and implemented it through "`ip access-group access-list-number direction`", the direction was inbound "`in`" in this lab

Based on the instructions in this lab, the following codes were used:

FOR ADMIN VLAN

"Admin VLAN should only access Sales VLAN for reporting, but not IT VLAN"

```
access-list 100 permit ip 192.168.1.0 0.0.0.127 192.168.1.128 0.0.0.63
```

```
access-list 100 deny   ip 192.168.1.0 0.0.0.127 192.168.1.192 0.0.0.15
```

FOR SALES VLAN

"Sales VLAN should not access Admin VLAN, but should be able to access IT VLAN for system support."

```
access-list 120 deny   ip 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.127
```

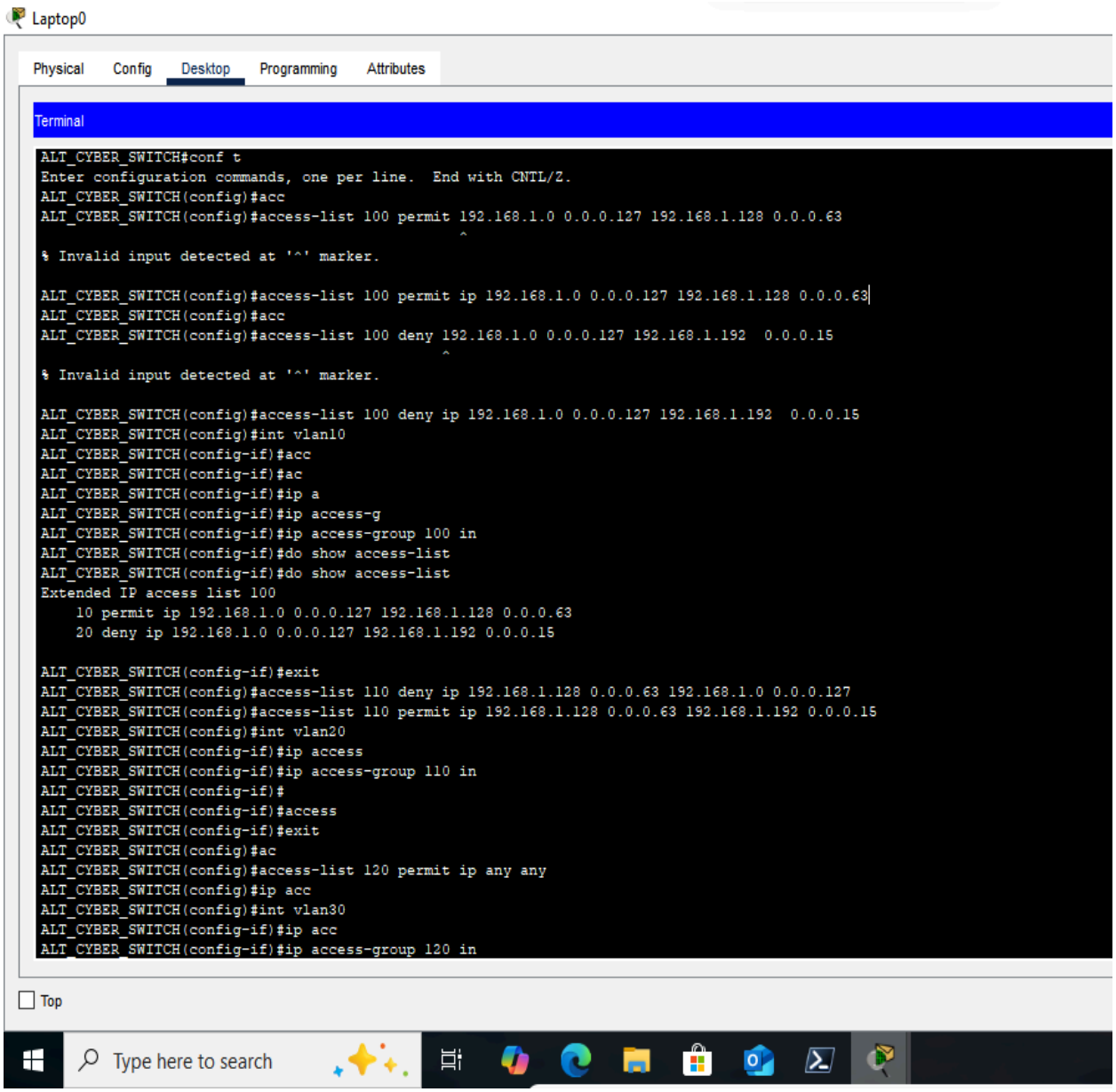
```
access-list 120 permit ip 192.168.1.128 0.0.0.63 192.168.1.192 0.0.0.15
```

FOR IT VLAN

“IT VLAN should have unrestricted access to all VLANs for administrative purposes.”

```
access-list 130 permit ip any any
```

The snippet below shows the configuration of the access control lists, and this configuration was confirmed through the “`show access-lists`” command, and after which the snippets show compliance with ACL lists



Terminal

```
ALT_CYBER_SWITCH>en
ALT_CYBER_SWITCH#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALT_CYBER_SWITCH(config)#ac
ALT_CYBER_SWITCH(config)#access-list 100 permit 192.168.10.0 0.0.0.127 192.168.1.128 0.0.0.63
                                               ^
% Invalid input detected at '^' marker.

ALT_CYBER_SWITCH(config)#access-list 100 permit ip 192.168.10.0 0.0.0.127 192.168.1.128 0.0.0.63
ALT_CYBER_SWITCH(config)#access-list 100 deny ip 192.168.10.0 0.0.0.127 192.168.1.192 0.0.0.15
ALT_CYBER_SWITCH(config)#int vlan 10
ALT_CYBER_SWITCH(config-if)#ip a
ALT_CYBER_SWITCH(config-if)#ip acc
ALT_CYBER_SWITCH(config-if)#ip access-group 100 in
ALT_CYBER_SWITCH(config-if)#exit
ALT_CYBER_SWITCH(config)#acc
ALT_CYBER_SWITCH(config)#access-list 110 deny ip 192.168.1.128 0.0.063 192.168.1.0 0.0.0.127
                                                              ^
% Invalid input detected at '^' marker.

ALT_CYBER_SWITCH(config)#access-list 110 deny ip 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.127
ALT_CYBER_SWITCH(config)#access-list 110 permit ip 192.168.1.128 0.0.0.63 192.168.1.192 0.0.0.15
ALT_CYBER_SWITCH(config)#int vlan20
ALT_CYBER_SWITCH(config-if)#ip acc
ALT_CYBER_SWITCH(config-if)#ip access-group 110 in
ALT_CYBER_SWITCH(config-if)#accc
ALT_CYBER_SWITCH(config-if)#acc
ALT_CYBER_SWITCH(config-if)#exit
```


```
ALT_CYBER_SWITCH(config)#access-list 100 permit ip 192.168.10.0 0.0.0.127 192.168.1.128 0.0.0.63
ALT_CYBER_SWITCH(config)#access-list 100 deny ip 192.168.10.0 0.0.0.127 192.168.1.192 0.0.0.15
ALT_CYBER_SWITCH(config)#int vlan 10
ALT_CYBER_SWITCH(config-if)#ip a
ALT_CYBER_SWITCH(config-if)#ip acc
ALT_CYBER_SWITCH(config-if)#ip access-group 100 in
ALT_CYBER_SWITCH(config-if)#exit
ALT_CYBER_SWITCH(config)#acc
ALT_CYBER_SWITCH(config)#access-list 110 deny ip 192.168.1.128 0.0.063 192.168.1.0 0.0.0.127
                                                              ^
% Invalid input detected at '^' marker.

ALT_CYBER_SWITCH(config)#access-list 110 deny ip 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.127
ALT_CYBER_SWITCH(config)#access-list 110 permit ip 192.168.1.128 0.0.0.63 192.168.1.192 0.0.0.15
ALT_CYBER_SWITCH(config)#int vlan20
ALT_CYBER_SWITCH(config-if)#ip acc
ALT_CYBER_SWITCH(config-if)#ip access-group 110 in
ALT_CYBER_SWITCH(config-if)#accc
ALT_CYBER_SWITCH(config-if)#acc
ALT_CYBER_SWITCH(config-if)#exit
ALT_CYBER_SWITCH(config)#acc
ALT_CYBER_SWITCH(config)#access-list 120 permit ip any any
ALT_CYBER_SWITCH(config)#interface vlan30
ALT_CYBER_SWITCH(config-if)#ip ac
ALT_CYBER_SWITCH(config-if)#ip access-group 120 in
ALT_CYBER_SWITCH(config-if)#
```


```
ALT_CYBER_SWITCH#show access
ALT_CYBER_SWITCH#show access-lists
Extended IP access list 100
    10 permit ip 192.168.10.0 0.0.0.127 192.168.1.128 0.0.0.63
    20 deny ip 192.168.10.0 0.0.0.127 192.168.1.192 0.0.0.15
Extended IP access list 110
    10 deny ip 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.127
    20 permit ip 192.168.1.128 0.0.0.63 192.168.1.192 0.0.0.15
Extended IP access list 120
    10 permit ip any any

ALT_CYBER_SWITCH#
```

ACL CONFIRMATION FOR ADMIN VLAN

```
C:\>ping 192.168.1.132

Pinging 192.168.1.132 with 32 bytes of data:

Reply from 192.168.1.132: bytes=32 time=2ms TTL=127
Reply from 192.168.1.132: bytes=32 time<1ms TTL=127
Reply from 192.168.1.132: bytes=32 time=23ms TTL=127
Reply from 192.168.1.132: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 23ms, Average = 6ms

C:\>ping 192.168.1.195

Pinging 192.168.1.195 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.195:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

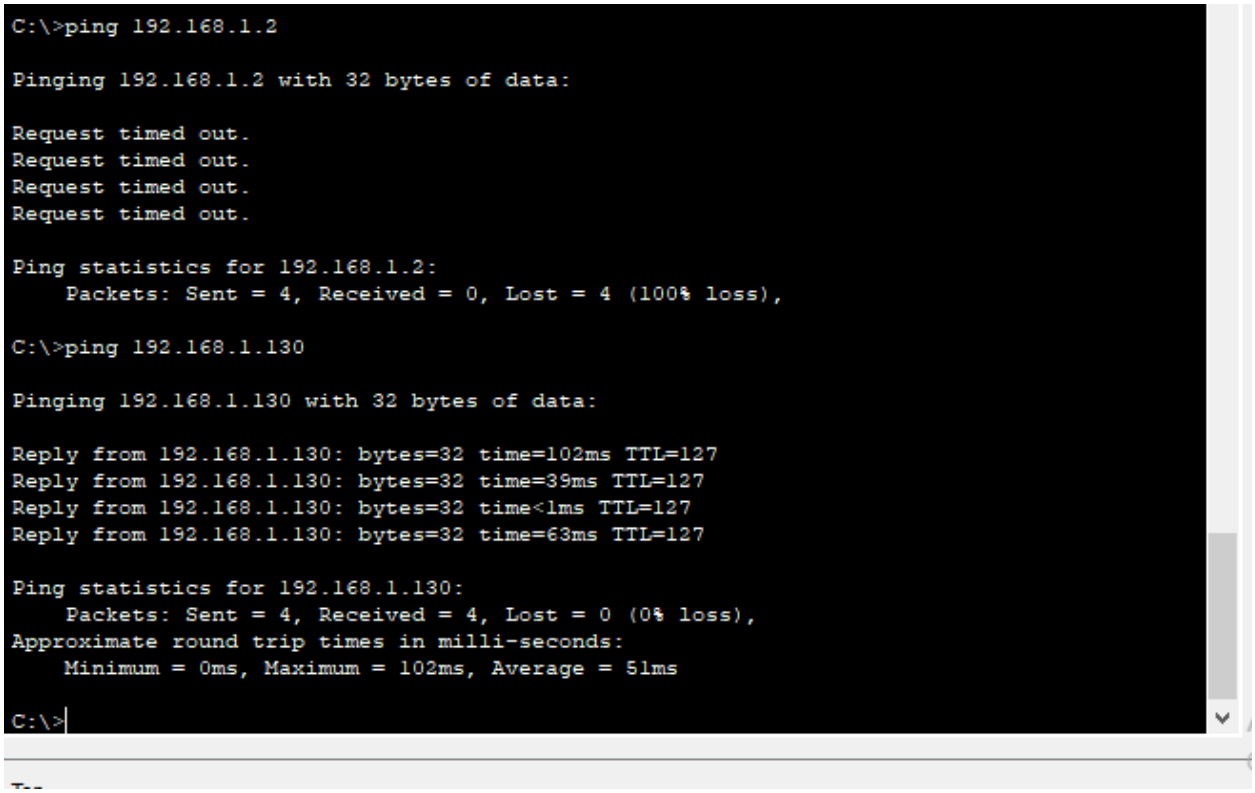
ACL CONFIRMATION FOR SALES VLAN

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.129: Destination host unreachable.
Reply from 192.168.1.129: Destination host unreachable.
Reply from 192.168.1.129: Destination host unreachable.
Reply from 192.168.1.129: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.195

Pinging 192.168.1.195 with 32 bytes of data:

Reply from 192.168.1.195: bytes=32 time=1ms TTL=127
Reply from 192.168.1.195: bytes=32 time<1ms TTL=127
Reply from 192.168.1.195: bytes=32 time<1ms TTL=127
Reply from 192.168.1.195: bytes=32 time=20ms TTL=127

Ping statistics for 192.168.1.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 5ms

C:\>
```

Top

ACL CONFIRMATION FOR IT_VLAN /MISCONFIGURED EXAMPLE

This section is highlighted as a misconfiguration as the `IT_VLAN` is supposed to be able to ping all Vlans, but based on the `ACLs` at `ADMIN_VLAN`, the `Ping` won't return to `IT_VLAN` as all `Admin_VLAN` IP addresses are blocked from accessing the I`T_VLAN`, and t`he ping would require an Echo reply`. This can be averted through proper IP and network planning

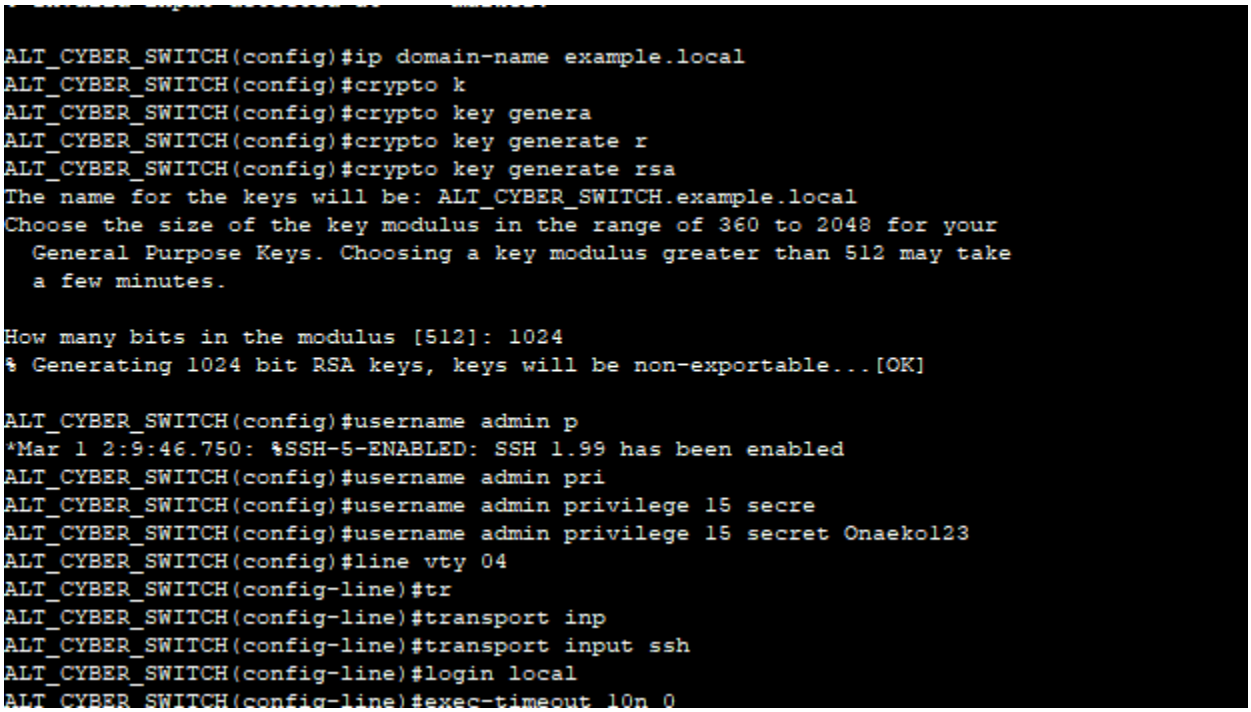


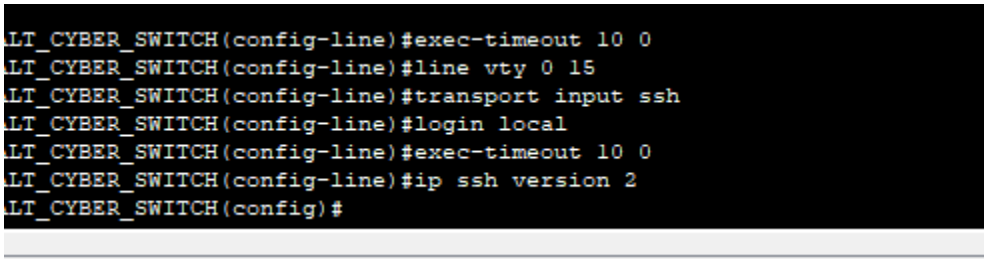
CONFIGURATION OF SSH

SSH is a tool that is used for secure remote access management to devices such as Routers and managed Switches. To configure SSH, We first configure the `domain name to example.local` by using the command `"ip domain-name example.local"` and generated the RSA key for the encryption of the SSH sessions through the command `"crypto key generate rsa"` and modified of the key size which I choose `"1024"` and the user login details using the command `"username admin privilege 15 secret Onaeko123"` and enter the vty line interface through the command `"line vty 0 4"` and choose virtual terminal lines and set the transport layer to only accept ssh through the `"transport input ssh"` and this automatically blocks `telnet` and enforce the login through the `"login-local"` command and determined the timeout for idle sessions as 10 minutes

through the command "`exec timeout 10 0`" and enforce that the sessions run on SSH 2 via the command "`ip ssh version 2`".

The screenshot shows the configuration of SSH and a login attempt from the device in the `ADMIN_VLAN`, and connection refusal through the use of `telnet`.





```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ssh -l admin 192.168.1.1

Password:



ALT_CYBER_SWITCH#
ALT_CYBER_SWITCH#
ALT_CYBER_SWITCH#
ALT_CYBER_SWITCH#
ALT_CYBER_SWITCH#
```

```
ALT_CYBER_SWITCH#exit

[Connection to 192.168.1.1 closed by foreign host]
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
C:\>
```