CISCO PACKET TRACER

Network Simulation

Jeffrey Obi
September 2025

Contents

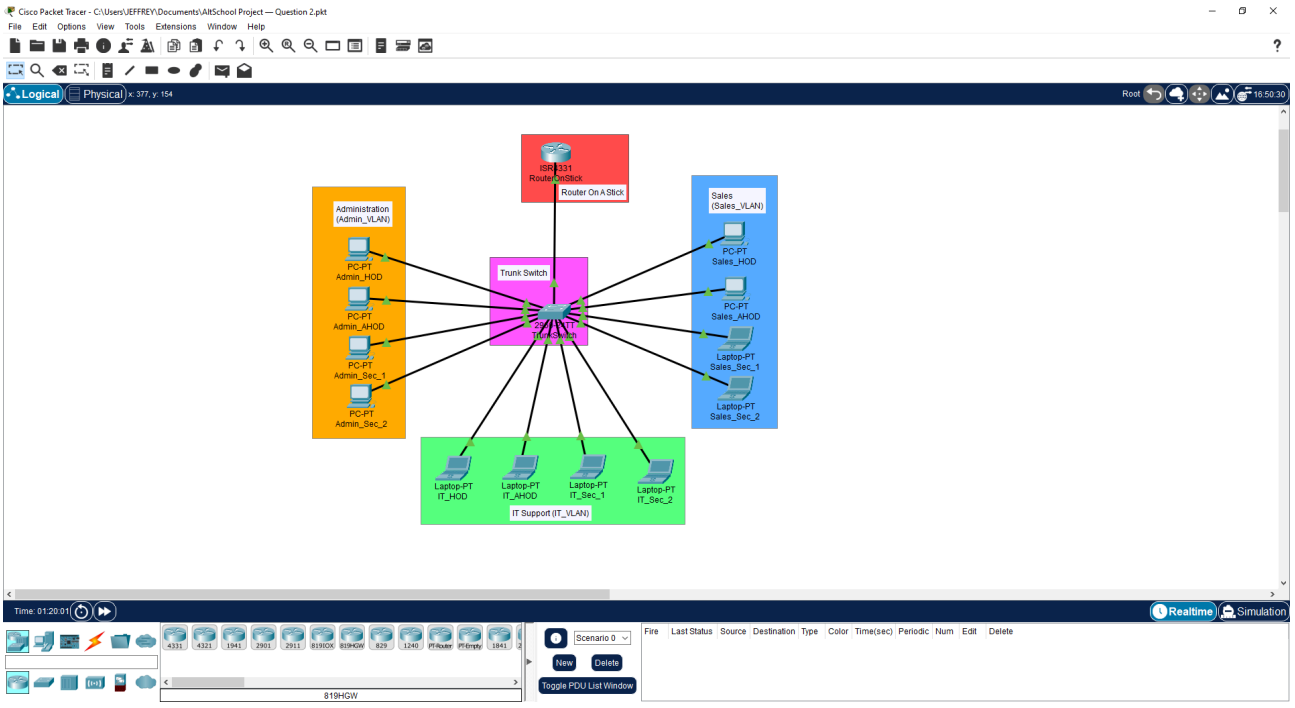
Procedure

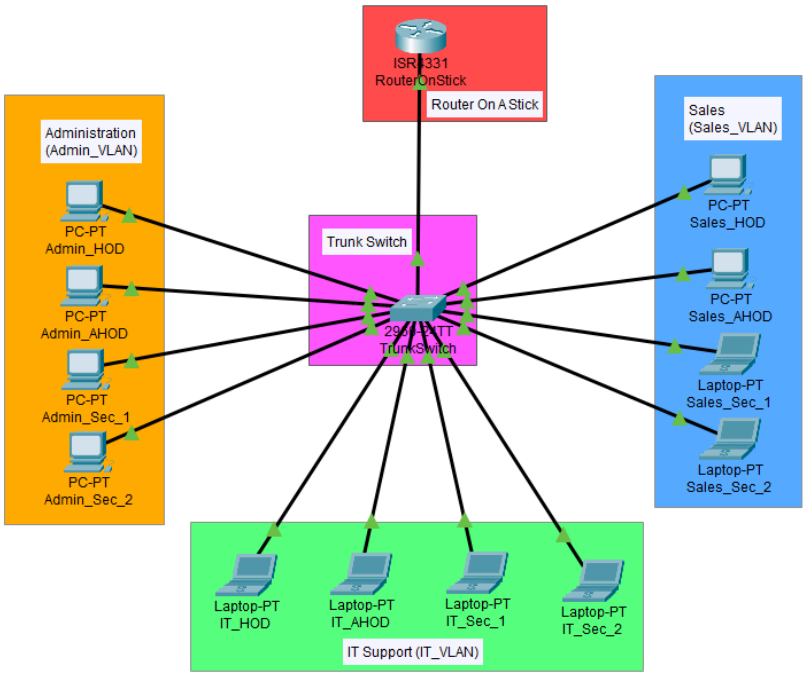
Step 1: Download and Login to CISCO Packet Tracer

a. Download and Install Packet Tracer Software (Windows) from Cisco's **Networking Academy** Domain.
b. Install on Windows (Windows 10 operating system) machine.
c. Launch software and sign up to 'Skills for All' to access the software.

Step 2: Design Network Topology

a. Placement of Devices
    i. Selecting & placing the **Router** (Cisco ISR4331).
    ii. Selecting & placing the **Switch** (Cisco 2960 IOS 15).
    iii. Positioning of **Endpoint Devices** (PCs & Laptops) in accordance with their Departments & VLANs.
    iv. Renaming the Router, Switch and Endpoint Devices.
b. Connecting Devices
    i. Connecting **Endpoint Devices** to the **Switch** via **FastEthernet** cables.
    ii. Connecting the **Switch** to the **Router** via a **GigabitEthernet** cable.
c. Graphically Grouping Devices
    i. Graphically grouping the **Endpoint Devices** in accordance with their VLANs, using different coloured rectangles.
    ii. Labelling the VLAN groups





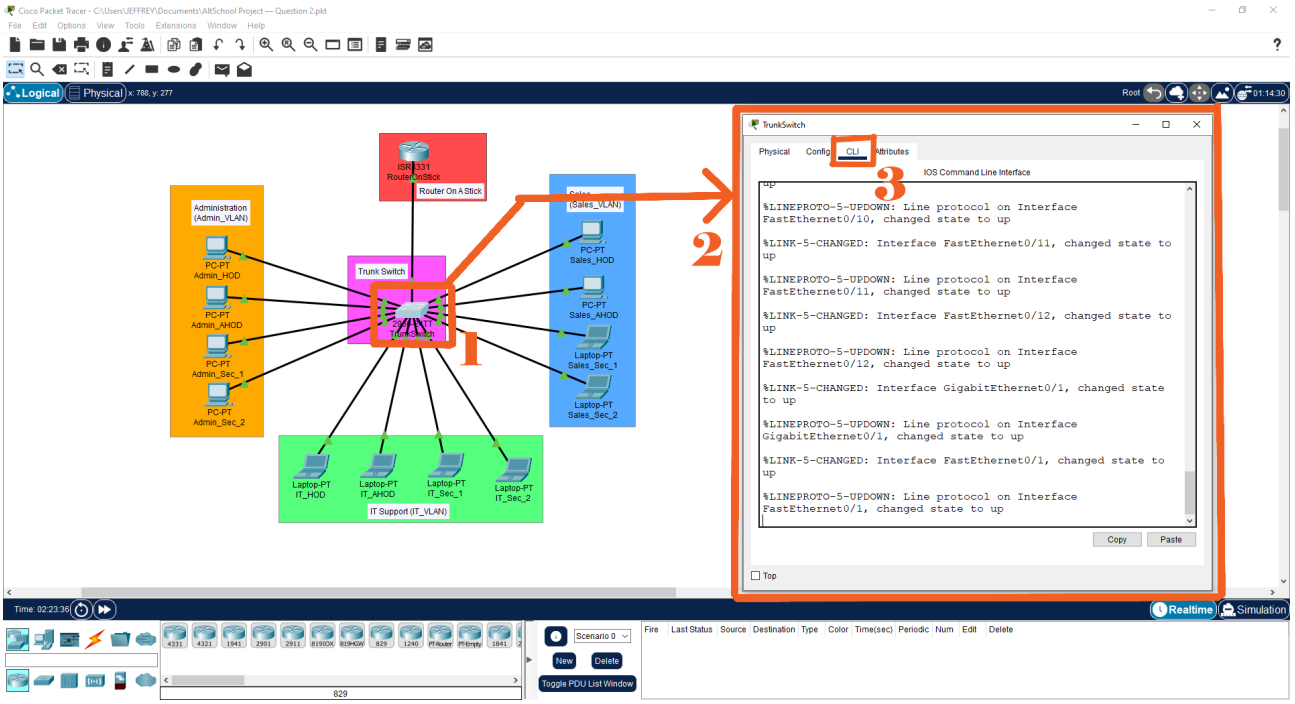
Step 3: Create & Name VLANs

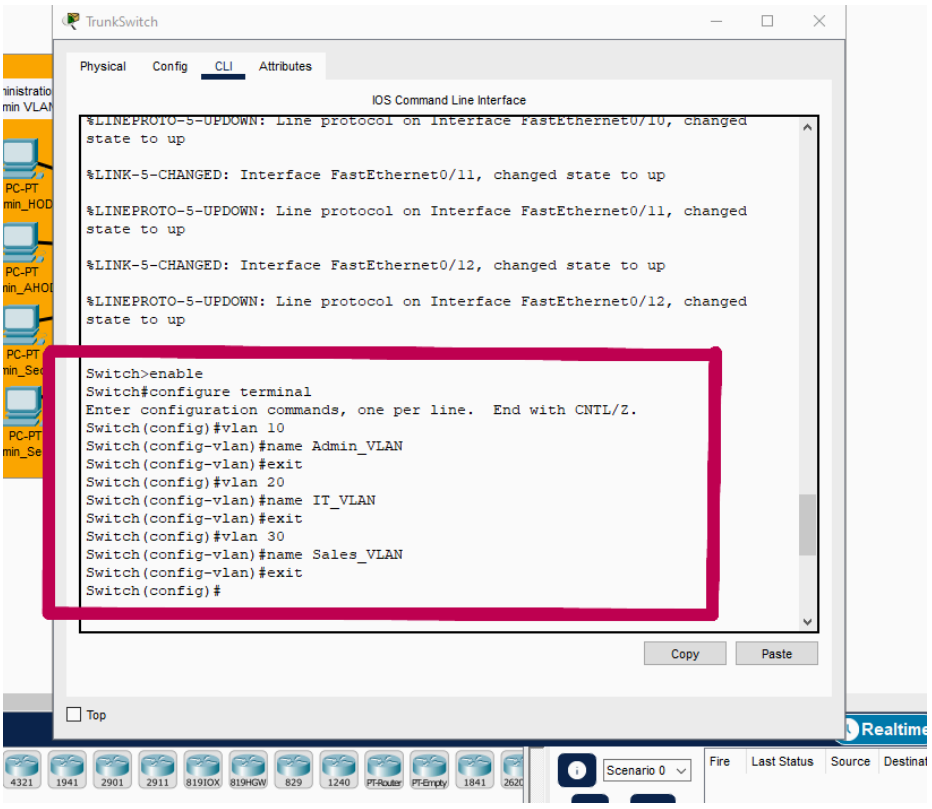
a. Launch the Switch CLI (Command Line Interface)
   i. Click on the switch to open the "TrunkSwitch" Configuration Window
   ii. Navigate to the CLI tab.

b. Create and name VLAN segments with the following details:
   i. VLAN 10: Admin_VLAN
   ii. VLAN 20: IT_VLAN
   iii. VLAN 30: Sales_VLAN

c. Configuration Commands:

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name Admin_VLAN
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name IT_VLAN
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Sales_VLAN
Switch(config-vlan)#exit
Switch(config)#
```





Step 4: Assign Switch Port Interfaces to VLANs

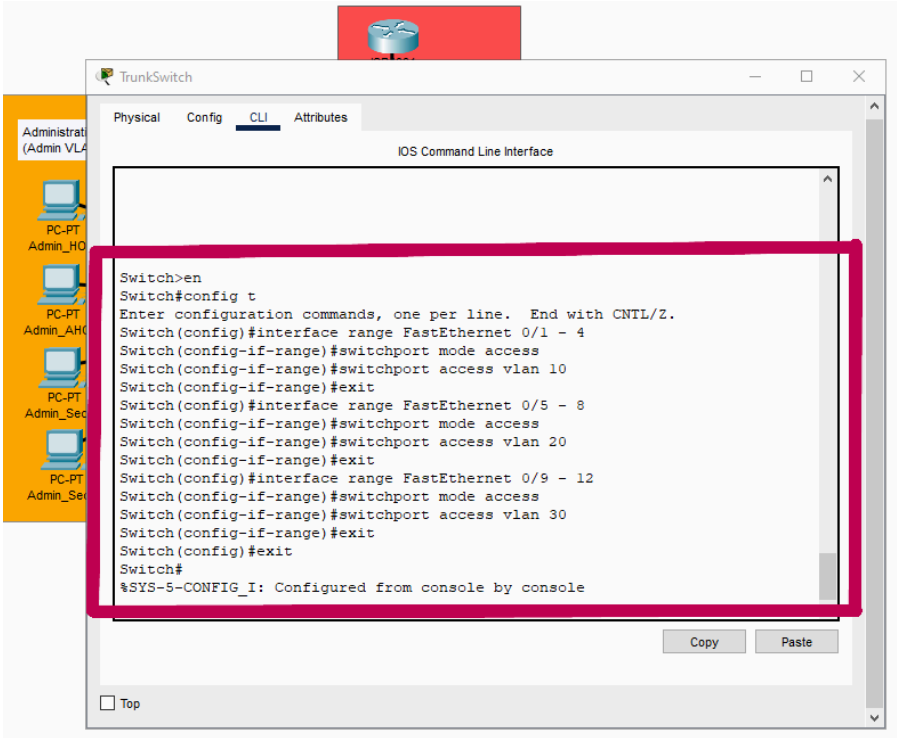
a. Launch the Switch CLI (Command Line Interface)
   i. Click on the Switch to open the "TrunkSwitch" Configuration Window
   ii. Navigate to the CLI tab.

b. Assign FastEthernet interfaces to their respective VLANs
   i. Assign FastEthernet 0/1, 0/2, 0/3, & 0/4 to **VLAN 10**
   ii. Assign FastEthernet 0/5, 0/6, 0/7, & 0/8 to **VLAN 20**

iii. Assign FastEthernet 0/9, 0/10, 0/11, & 0/12 to **VLAN 30**

c. Configuration Commands:

```
Switch>en
Switch#config t
Switch(config)#interface range FastEthernet 0/1 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range FastEthernet 0/5 - 8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range FastEthernet 0/9 - 12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#exit
```



Step 5: Configure IP Addresses on Endpoint Devices

a. Begin IP Configuration

i. Click on each **Endpoint Device** (PCs & Laptops) to open their Configuration Window.

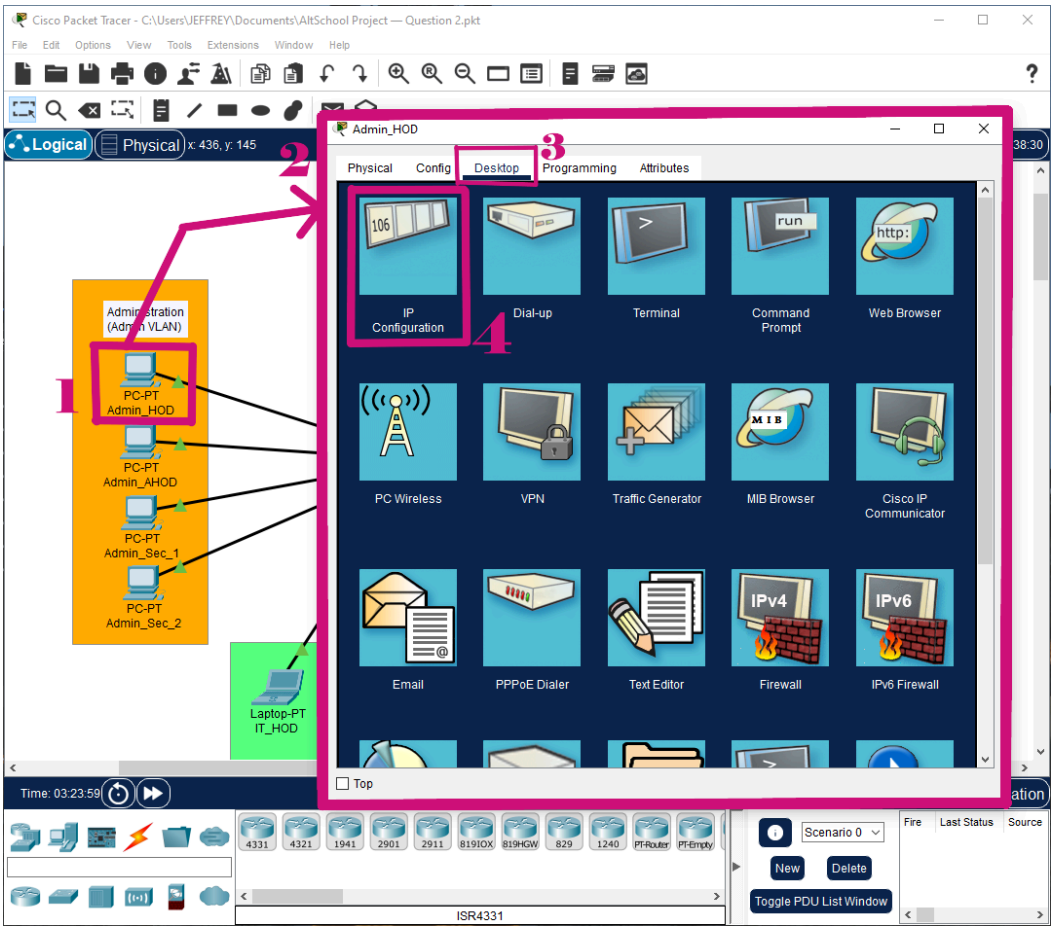
ii. Navigate to the **Desktop** tab.

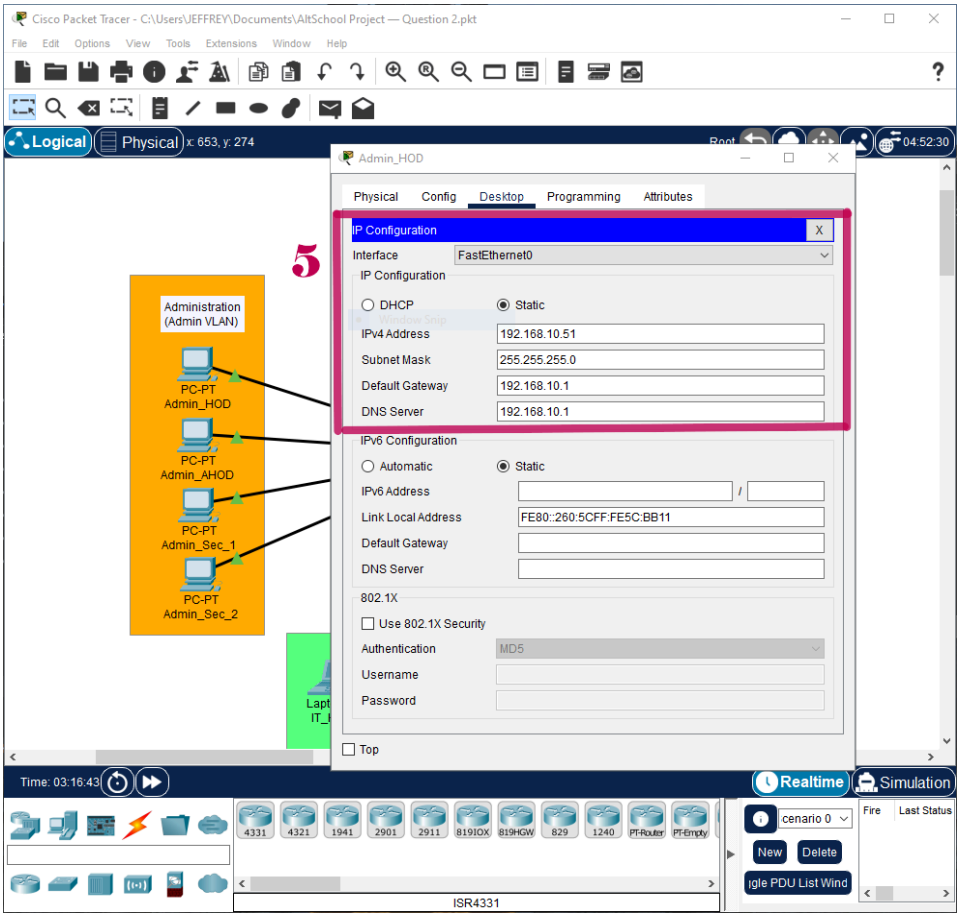
iii. Open "**IP Configuration**."

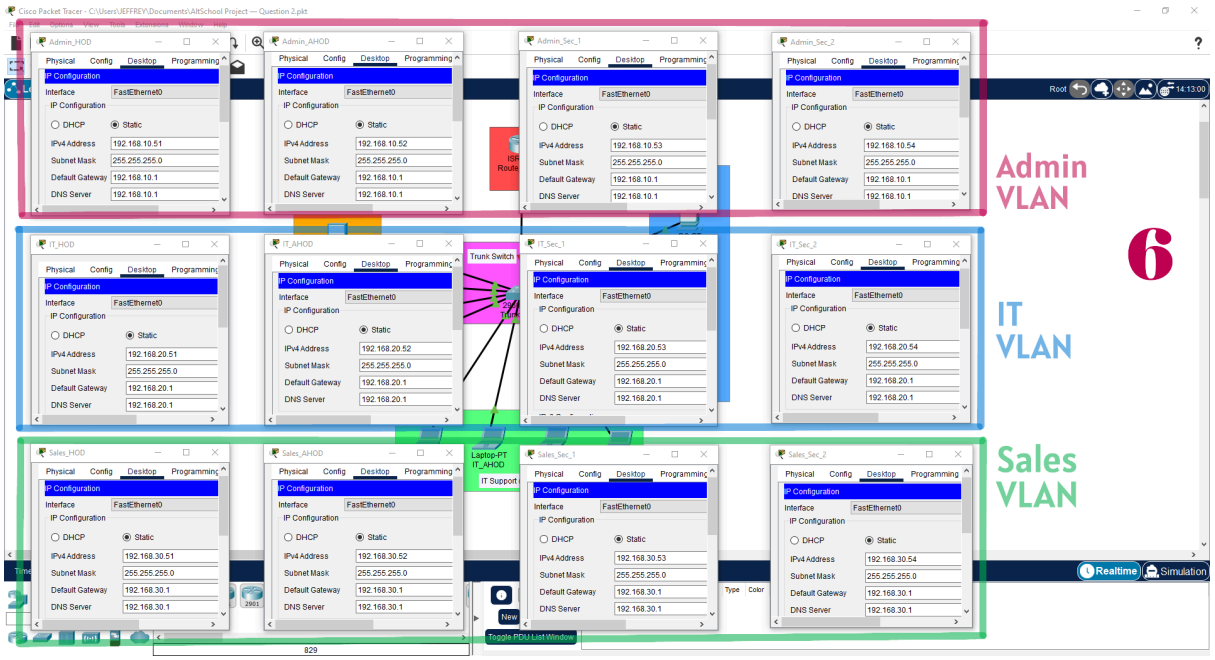
b. Configure the IP Addresses

i. Select "**Static**" for static IP addresses.

ii. Input the unique **IPv4 address** with the correct VLAN (e.g., 10 for VLAN 10)
iii. Input the **Subnet Mask** (255.255.255.0 for the Class C Subnet)
iv. Input the **Default Gateway** with the correct VLAN (e.g., 10 for VLAN 10)
v. Input the **DNS Server** IP (assumed same as Default Gateway IP)
vi. Apply configuration to other **Endpoint Devices**.







Step 6: Configure Trunk-Port on Switch

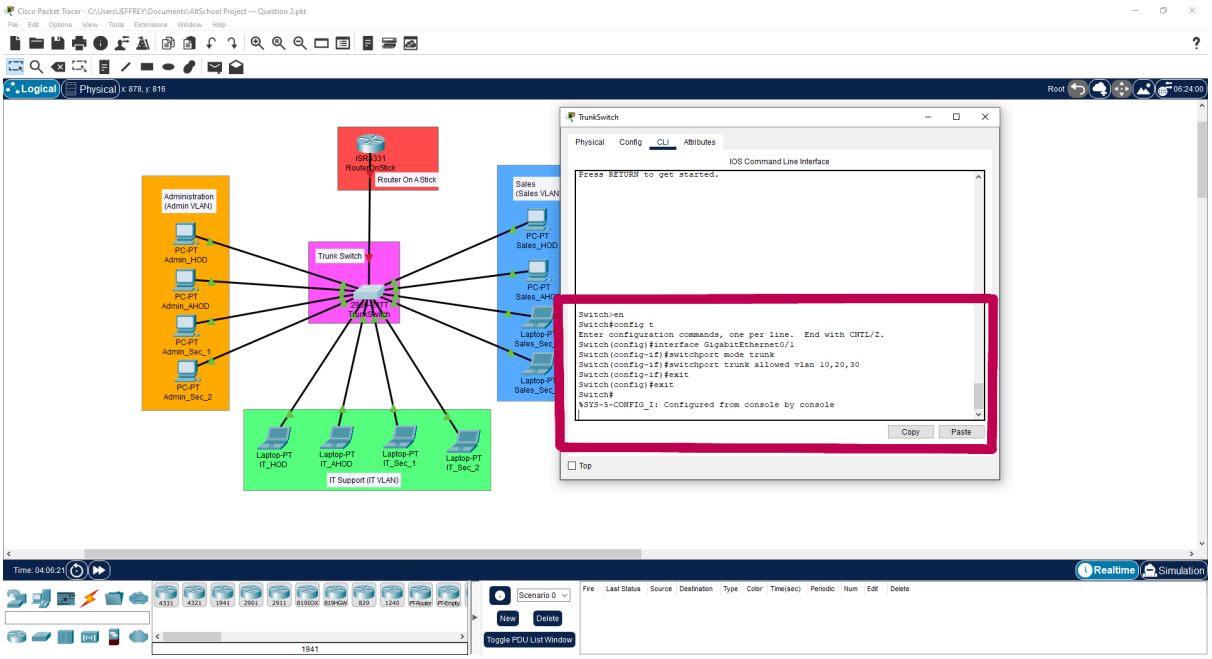
a. Launch the Switch CLI (Command Line Interface)
   i. Click on the Switch to open the “TrunkSwitch” Configuration Window
   ii. Navigate to the CLI tab.

b. Configure Interface

i. Turn on Trunk Mode
ii. Allow VLANs (10, 20 & 30)

c. Configuration Commands

```
Switch>en
Switch#config t
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan
10,20,30
Switch(config-if)#exit
Switch(config)#exit
```



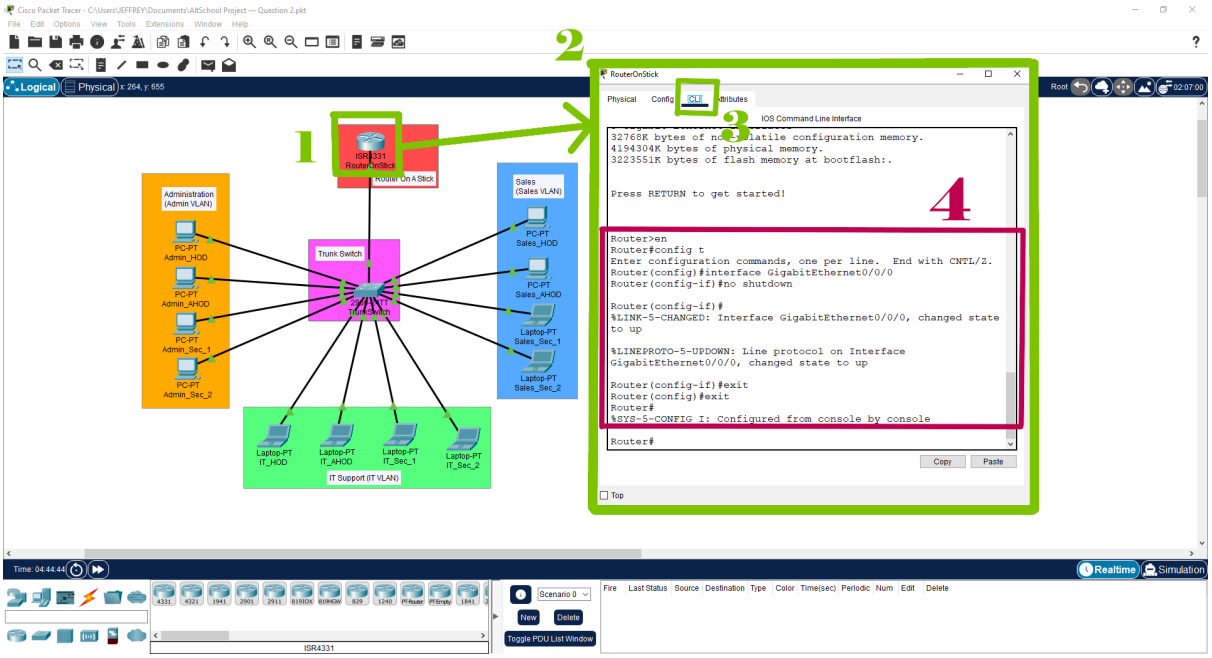
Step 7: Turn on Physical Interface on ROAS (Router-On-A-Stick)

a. Launch the Router CLI (Command Line Interface).
   i. Click on the Router to open the “RouterOnStick” Configuration Window.
   ii. Navigate to the CLI tab.

b. Turn on GigabitEthernet interface.
   i. Apply “no shutdown” command to GigabitEthernet interface.

c. Configuration Commands:

```
Router>en
Router#config t
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```



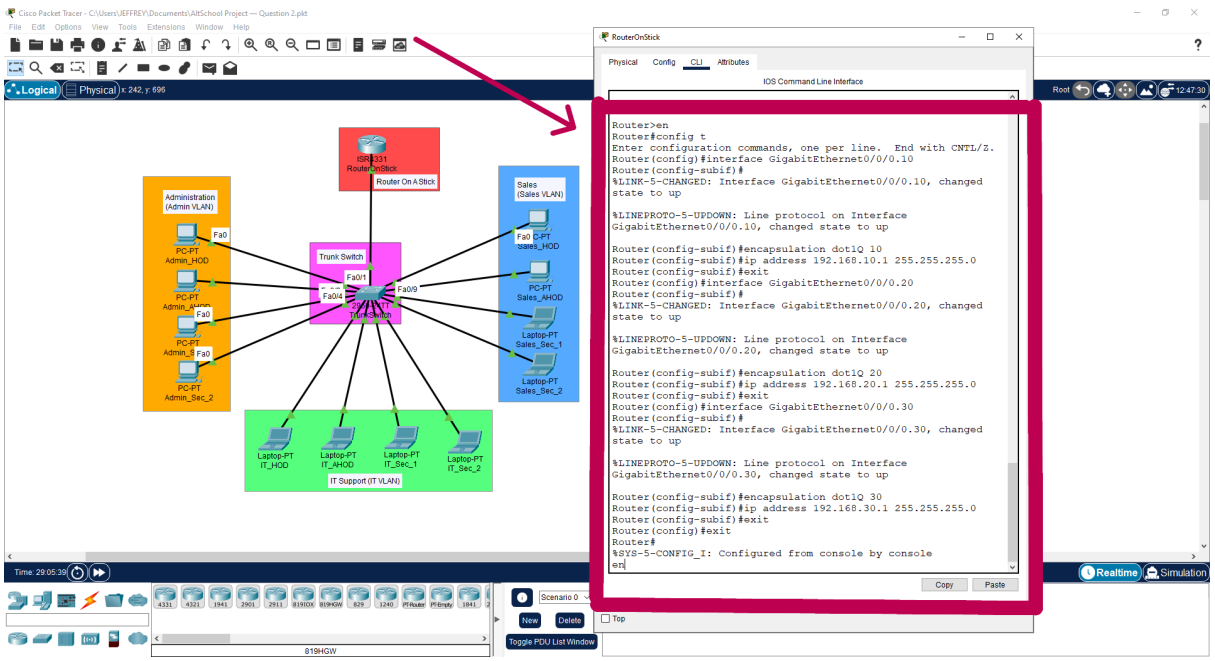
Step 8: Enable Routing Between VLANs (Inter-VLAN Routing)

a. Launch the Router CLI (Command Line Interface).
   i. Click on the Router to open the “RouterOnStick” Configuration Window.
   ii. Navigate to the CLI tab.

b. Configure Sub-Interfaces

c. Configuration Commands:

```
Router>en
Router#config t
Router(config)#interface GigabitEthernet0/0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1
255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1
255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1
255.255.255.0
Router(config-subif)#exit
Router(config)#exit
Router#
```



Step 9: Verify Routing Between VLANs (Inter-VLAN Routing)

a. Launch **Command Prompt** on **Endpoint Device** (PC/Laptop).
   i. Click on each **Endpoint Device** (PCs & Laptops) to open their Configuration Window.
   ii. Navigate to the **Desktop** tab
   iii. Open "**Command Prompt**."

b. From the **Command Prompt** of an Endpoint Device on **Admin_VLAN**
   i. Ping a device on **IT_VLAN**
   ii. Ping a device on **Sales_VLAN**

c. From the **Command Prompt** of an Endpoint Device on **IT_VLAN**
   i. Ping a device on **Admin_VLAN**
   ii. Ping a device on **Sales_VLAN**

d. From the **Command Prompt** of an Endpoint Device on **Sales_VLAN**
   i. Ping a device on **Admin_VLAN**
   ii. Ping a device on **IT_VLAN**

e. Results: All pings were returned **(Success!)**.

f. Configuration Commands:

From Admin_HOD (Admin_VLAN)

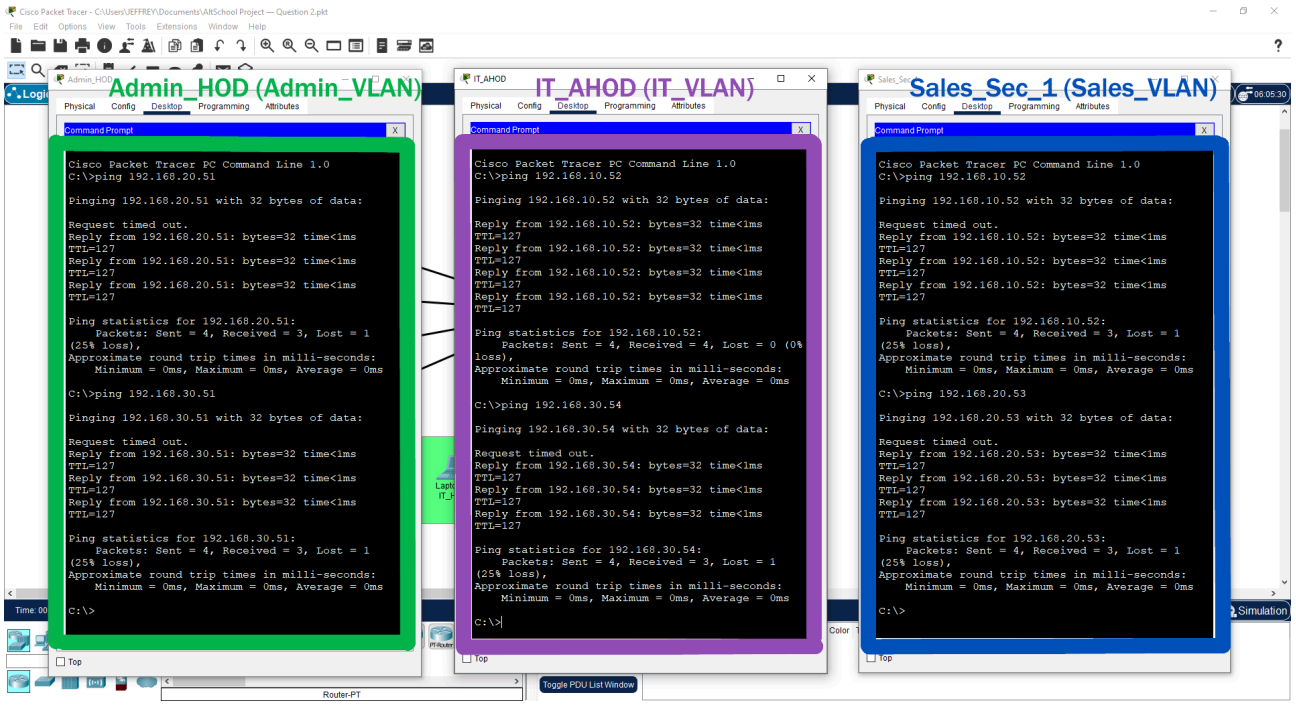
```
# to IT_VLAN
C:\>ping 192.168.20.51
# to Sales_VLAN
C:\>ping 192.168.30.54
```

From IT_Sec_1 (IT_VLAN)

```
# to Admin_VLAN
C:\>ping 192.168.10.53
# to Sales_VLAN
C:\>ping 192.168.30.52
```

From Sales_Sec_2 (Sales_VLAN)

```
# to Admin_VLAN
C:\>ping 192.168.10.51
# to IT_VLAN
C:\>ping 192.168.20.54
```



Step 10: Configure Access Control Lists

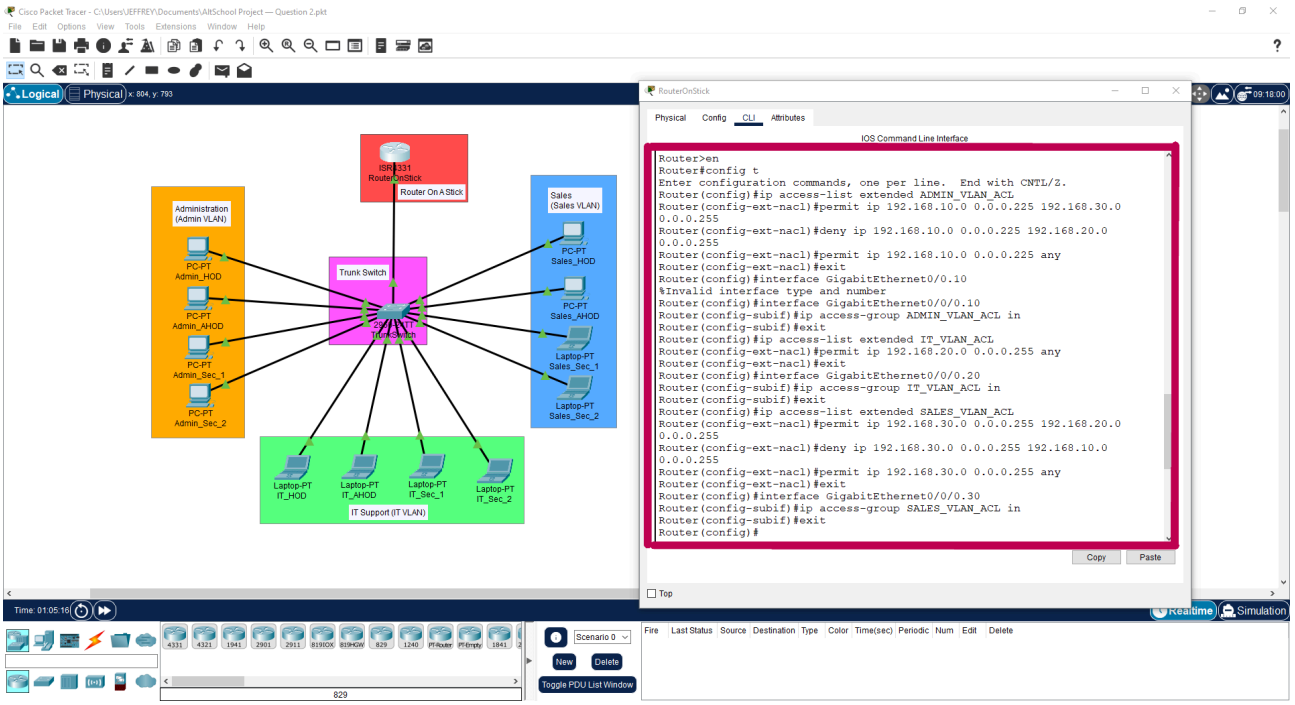
a. Launch the Router CLI (Command Line Interface).
   i. Click on the Router to open the “RouterOnStick” Configuration Window.
   ii. Navigate to the CLI tab.

b. Configure **Extended ACL** on the **Router**.
   i. Define the Extended ACLs for each VLAN.
      - **ADMIN_VLAN_ACL** for *Admin_VLAN*.
      - **IT_VLAN_ACL** for *IT_VLAN*.
      - **SALES_VLAN_ACL** for *Sales_VLAN*.
   ii. Set permit and deny rules for the VLANs
      - Admin_VLAN **should** access Sales_VLAN.
      - Admin_VLAN **should not** access IT_VLAN.
      - IT_VLAN **should** access **all** VLANs.
      - Sales_VLAN **should** access IT_VLAN.
      - Sales_VLAN **should not** access Admin_VLAN.
   iii. Apply the ACLs to the inbound traffic on the relevant interfaces for the VLANs (e.g., apply **ADMIN_VLAN_ACL** to inbound traffic on **GigabitEthernet0/0/0.10**)

c. Configuration Commands:

```
Router>en
Router#config t
Router(config)#ip access-list extended ADMIN_VLAN_ACL
Router(config-ext-nacl)#permit ip 192.168.10.0
0.0.0.225 192.168.30.0 0.0.0.255
```

```
Router(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.225
192.168.20.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.10.0
0.0.0.225 any
Router(config-ext-nacl)#exit
Router(config)#interface GigabitEthernet0/0/0.10
Router(config-subif)#ip access-group ADMIN_VLAN_ACL in
Router(config-subif)#exit
Router(config)#ip access-list extended IT_VLAN_ACL
Router(config-ext-nacl)#permit ip 192.168.20.0
0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface GigabitEthernet0/0/0.20
Router(config-subif)#ip access-group IT_VLAN_ACL in
Router(config-subif)#exit
Router(config)#ip access-list extended SALES_VLAN_ACL
Router(config-ext-nacl)#permit ip 192.168.30.0
0.0.0.255 192.168.20.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255
192.168.10.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.30.0
0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#interface GigabitEthernet0/0/0.30
Router(config-subif)#ip access-group SALES_VLAN_ACL in
Router(config-subif)#exit
Router(config)#
```



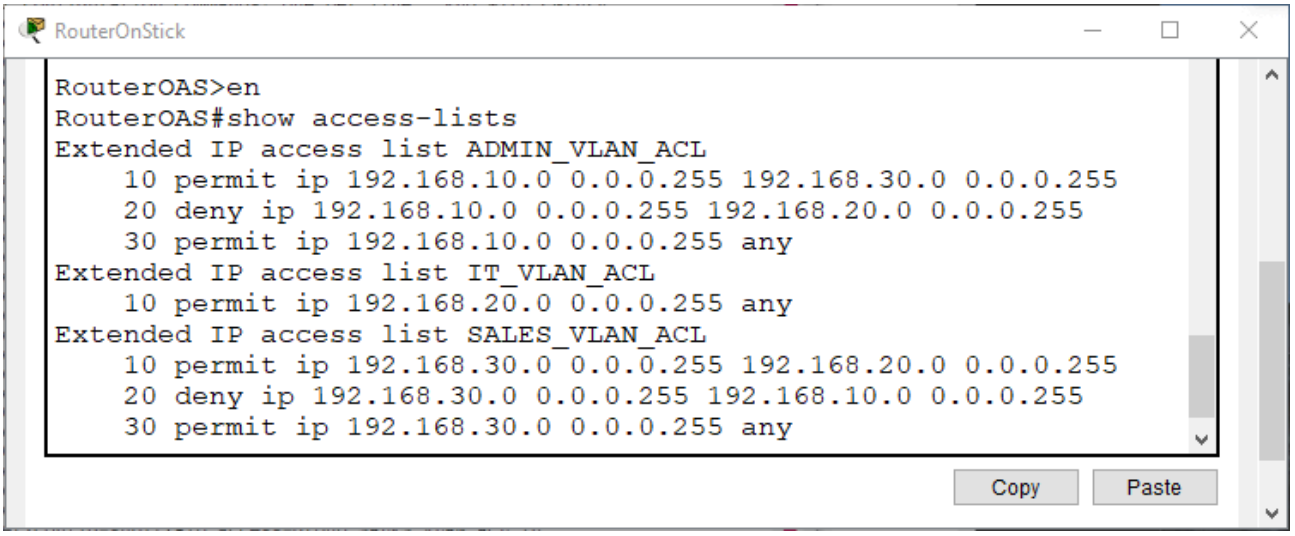
Step 11: Verify Access Control Lists

a. Launch the Router CLI (Command Line Interface).

i. Click on the Router to open the “RouterOnStick” Configuration Window.
ii. Navigate to the CLI tab.

b. Display Access Control Lists.
c. Configuration Commands:

```
RouterOAS>en
RouterOAS#show access-lists
      Extended IP access list ADMIN_VLAN_ACL
      10 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
      0.0.0.255
      20 deny ip 192.168.10.0 0.0.0.255 192.168.20.0
      0.0.0.255
      30 permit ip 192.168.10.0 0.0.0.255 any
      Extended IP access list IT_VLAN_ACL
      10 permit ip 192.168.20.0 0.0.0.255 any
      Extended IP access list SALES_VLAN_ACL
      10 permit ip 192.168.30.0 0.0.0.255 192.168.20.0
      0.0.0.255
      20 deny ip 192.168.30.0 0.0.0.255 192.168.10.0
      0.0.0.255
      30 permit ip 192.168.30.0 0.0.0.255 any
```



Step 12: Verify ACL From Endpoint Devices Using Command Prompt

a. Launch **Command Prompt** on **Endpoint Device** (PC/Laptop).
   i. Click on each **Endpoint Device** (PCs & Laptops) to open their Configuration Window.
   ii. Navigate to the **Desktop** tab
   iii. Open “**Command Prompt**.”
b. From the **Command Prompt** of an Endpoint Device on **Admin_VLAN**
   i. Ping a device on the same VLAN **(Admin_VLAN)**
      - Result: **Success** • all 4 pings replied • 0% packet loss.
      - Reason: Intra-VLAN routing is enabled on the router & can’t be restricted by ACL.

ii. Ping a device on **IT_VLAN**
- Result: **Failed** • "*Destination host unreachable*" • 100% packet loss.
- Reason: Inter-VLAN routing is enabled but **Admin_VLAN_ACL** denies movement of packets (request) from **Admin_VLAN** destined for **IT_VLAN.** Request packets never reached their destination.

iii. Ping a device on **Sales_VLAN**
- Result: **Failed** • "*Request timed out*" • 100% packet loss.
- Reason: Inter-VLAN routing is enabled but while **Admin_VLAN_ACL** permits movement of packets (request) from **Admin_VLAN** destined for **Sales_VLAN, Sales_VLAN_ACL** denies movement of packets (reply) from **Sales_VLAN** destined for **Admin_VLAN.**

c. From the **Command Prompt** of an Endpoint Device on **IT_VLAN**

i. Ping a device on the same VLAN **(IT_VLAN)**
- Result: **Success** • all 4 pings replied • 0% packet loss.
- Reason: Intra-VLAN routing is enabled on the router & can't be restricted by ACL

ii. Ping a device on **Admin_VLAN**
- Result: **Failed** • "*Request timed out*" • 100% packet loss.
- Reason: Inter-VLAN routing is enabled but while **IT_VLAN_ACL** permits movement of packets (request) from **IT_VLAN** destined for **Admin_VLAN, Admin_VLAN_ACL** denies movement of packets (reply) from **Admin_VLAN** destined for **IT_VLAN.**

iii. Ping a device on **Sales_VLAN**
- Result: **Success** • 3/4 pings replied • 25% packet loss.
- Reason: Inter-VLAN routing is enabled. **IT_VLAN_ACL** permits movement of packets (request) from **IT_VLAN** destined for **Sales_VLAN.** Also, **Sales_VLAN_ACL** permits movement of packets (reply) from **Sales_VLAN** destined for **IT_VLAN.**

d. From the Command Prompt of an Endpoint Device on **Sales_VLAN**

i. Ping a device on the same VLAN **(Sales_VLAN)**
- Result: **Success** • all 4 pings replied • 0% packet loss
- Reason: Intra-VLAN routing is enabled on the router & can't be restricted by ACL.

ii. Ping a device on **Admin_VLAN**
- Result: **Failed** • "*Destination host unreachable*" • 100% packet loss.
- Reason: Inter-VLAN routing is enabled but **Sales_VLAN_ACL** denies movement of packets (request) from **Sales_VLAN** destined

for **Admin_VLAN.** Request packets never reached their destination.

iii. Ping a device on **IT_VLAN**

- Result: **Success** • 3/4 pings replied • 25% packet loss.
- Reason: Inter-VLAN routing is enabled. **Sales_VLAN_ACL** permits movement of packets (request) from **Sales_VLAN** destined for **IT_VLAN.** Also, **IT_VLAN_ACL** permits movement of packets (reply) from **IT_VLAN** destined for **Sales_VLAN.**

e. Configuration Commands:

From Admin_HOD (Admin_VLAN)

```
# to Admin_VLAN
C:\>ping 192.168.10.53
Pinging 192.168.10.53 with 32 bytes of data:
Reply from 192.168.10.53: bytes=32 time<1ms TTL=128
Reply from 192.168.10.53: bytes=32 time<1ms TTL=128
Reply from 192.168.10.53: bytes=32 time<1ms TTL=128
Reply from 192.168.10.53: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.53:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
# to IT_VLAN
C:\>ping 192.168.20.51
Pinging 192.168.20.51 with 32 bytes of data:
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Ping statistics for 192.168.20.51:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
# to Sales_VLAN
C:\>ping 192.168.30.54
Pinging 192.168.30.54 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.30.54:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

From IT_Sec_1 (IT_VLAN)

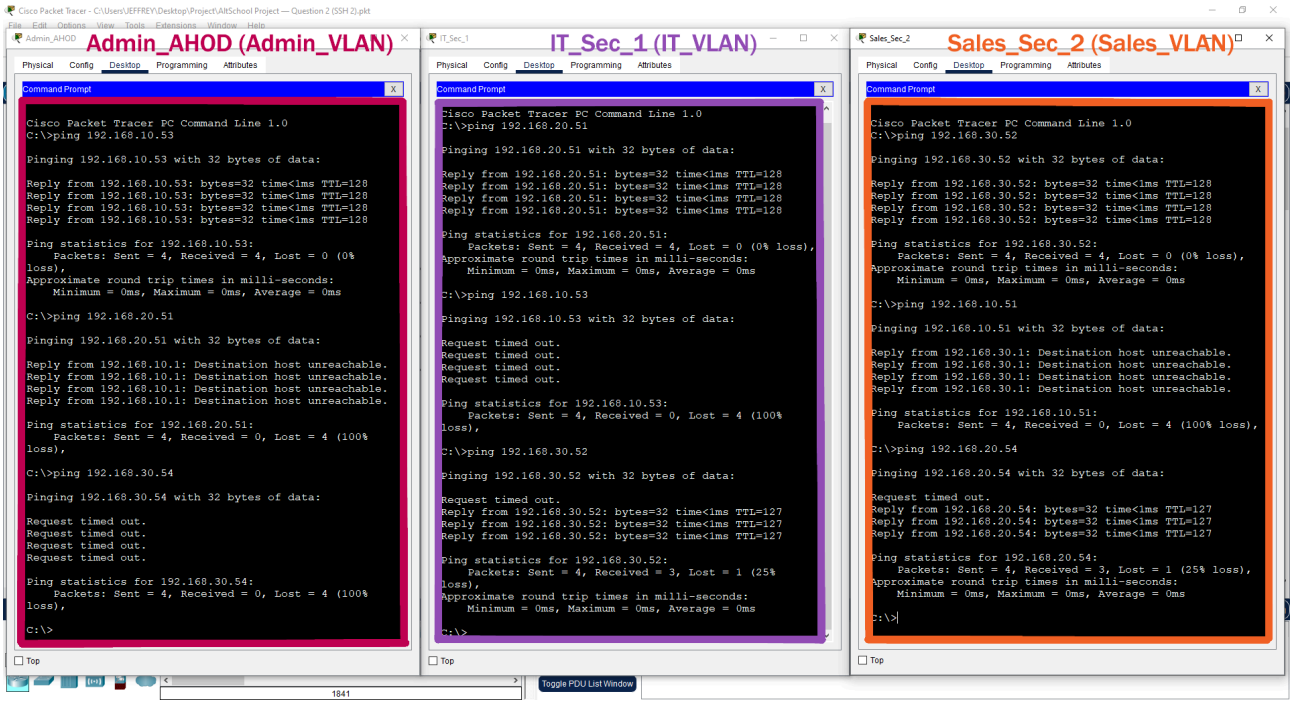
```
# to IT_VLAN
C:\>ping 192.168.20.51
Pinging 192.168.20.51 with 32 bytes of data:
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128
Reply from 192.168.20.51: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.20.51:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
# to Admin_VLAN
C:\>ping 192.168.10.53
Pinging 192.168.10.53 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.53:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
# to Sales_VLAN
C:\>ping 192.168.30.52
Pinging 192.168.30.52 with 32 bytes of data:
Request timed out.
Reply from 192.168.30.52: bytes=32 time<1ms TTL=127
Reply from 192.168.30.52: bytes=32 time<1ms TTL=127
Reply from 192.168.30.52: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.30.52:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

From Sales_Sec_2 (Sales_VLAN)

```
# to Sales_VLAN
C:\>ping 192.168.30.52
Pinging 192.168.30.52 with 32 bytes of data:
Reply from 192.168.30.52: bytes=32 time<1ms TTL=128
Reply from 192.168.30.52: bytes=32 time<1ms TTL=128
Reply from 192.168.30.52: bytes=32 time<1ms TTL=128
Reply from 192.168.30.52: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.30.52:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
# to Admin_VLAN
C:\>ping 192.168.10.51
Pinging 192.168.10.51 with 32 bytes of data:
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Ping statistics for 192.168.10.51:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
# to IT_VLAN
C:\>ping 192.168.20.54
Pinging 192.168.20.54 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.54: bytes=32 time<1ms TTL=127
Reply from 192.168.20.54: bytes=32 time<1ms TTL=127
Reply from 192.168.20.54: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.54:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



Step 13: Configure Secure Shell (SSH) on Router

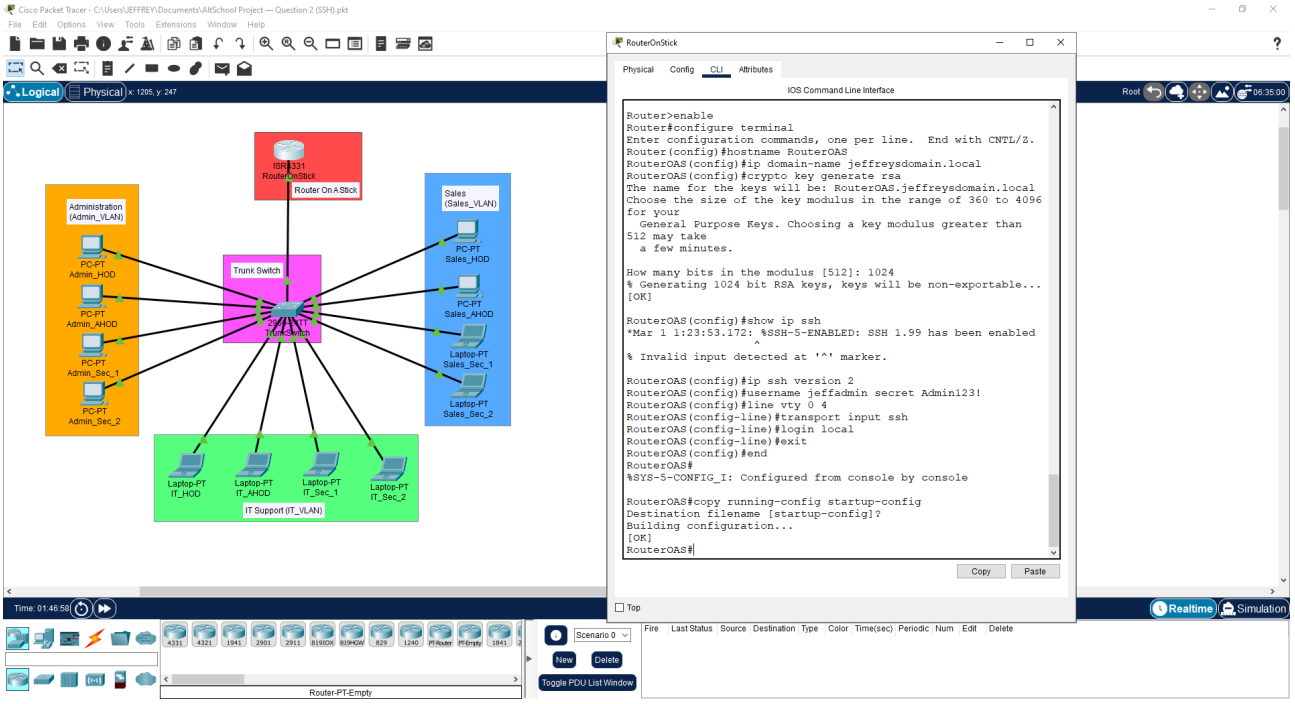
a. Launch the Router CLI (Command Line Interface).
   i. Click on the Router to open the “RouterOnStick” Configuration Window.
   ii. Navigate to the CLI tab.

b. Configure Secure Shell
   i. Configure **hostname** (RouterOAS) and **domain** (jeffreysdomain.local)
   ii. Generate **RSA Cryptographic Keys** (Size: 1024 bit)
   iii. Create Local Account **Username** (jeffreyadmin) and encrypted **Password (SECURITY BEST PRACTICES)**
   iv. Restrict Traffic type to **SSH Version** (Version 2).
   NOTE: This makes the device only accept encrypted SSH traffic and disqualifies/disables all unsecure connection types including **TELNET.**
   v. Configure **VTY (Virtual Terminal) Lines**.

c. Configuration Commands:

```
Router>enable
```

```
Router#configure terminal
Router(config)#hostname RouterOAS
RouterOAS(config)#ip domain-name jeffreysdomain.local
RouterOAS(config)#crypto key generate rsa
The name for the keys will be:
RouterOAS.jeffreysdomain.local
Choose the size of the key modulus in the range of 360
to 4096 for your General Purpose Keys. Choosing a key
modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable...[OK]
RouterOAS(config)#show ip ssh
*Mar 1 1:23:53.172: %SSH-5-ENABLED: SSH 1.99 has been
enabled
RouterOAS(config)#ip ssh version 2
RouterOAS(config)#username jeffadmin secret Admin123!
RouterOAS(config)#line vty 0 4
RouterOAS(config-line)#transport input ssh
RouterOAS(config-line)#login local
RouterOAS(config-line)#exit
RouterOAS(config)#end
RouterOAS#
```



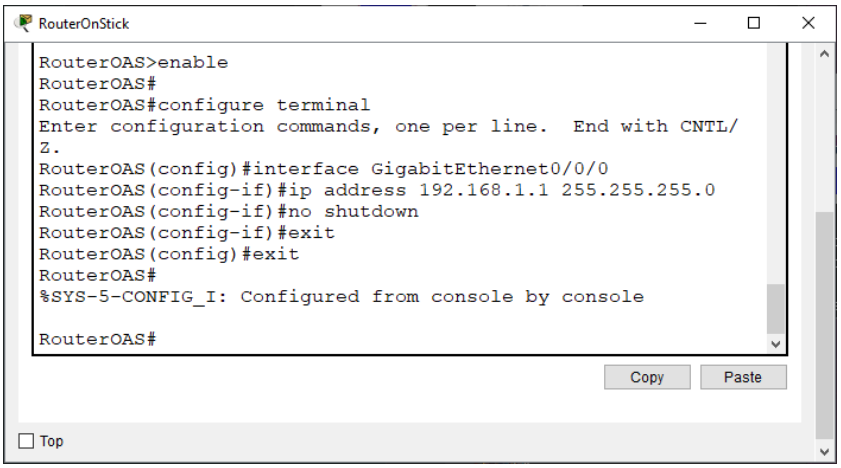
Step 14: Assign IP Address to Router Interface

a. Launch the Router CLI (Command Line Interface).
   i. Click on the Router to open the “RouterOnStick” Configuration Window.
   ii. Navigate to the CLI tab.

b. Assign IP address to Router interface

c. Configuration Commands:

```
RouterOAS>enable
RouterOAS#configure terminal
RouterOAS(config)#interface GigabitEthernet0/0/0
RouterOAS(config-if)#ip address 192.168.1.1
255.255.255.0
RouterOAS(config-if)#no shutdown
RouterOAS(config-if)#exit
RouterOAS(config)#exit
RouterOAS#
```



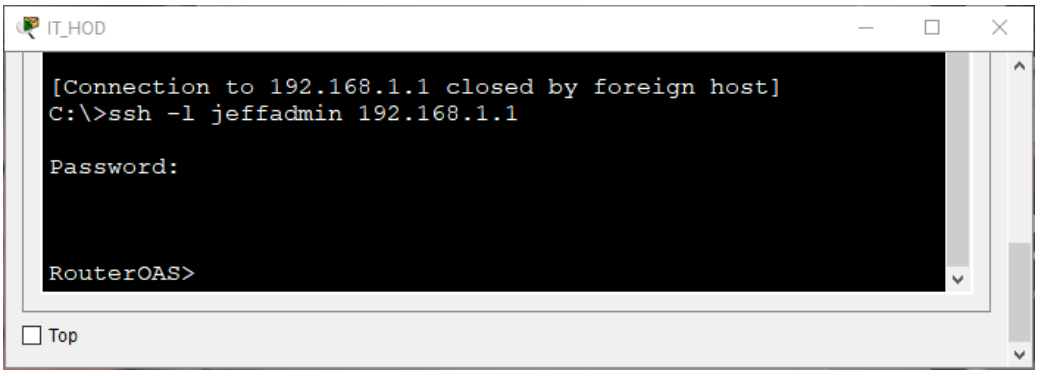
Step 15: Verify SSH Configuration on Router Using Endpoint Device

a. Launch Endpoint Device CLI (Command Line Interface).
   i. Click on an **Endpoint Device** (IT_HOD PC) to open its Configuration Window.
   ii. Navigate to the **Desktop** tab.
   iii. Open "**Command Prompt**"

b. Test connection from **Endpoint Device**.
   i. Login to **Router** domain using pre-established credentials **(Success!)**

c. Configuration Commands:

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



Step 16: Verify SSH Configuration on Router Using Router CLI

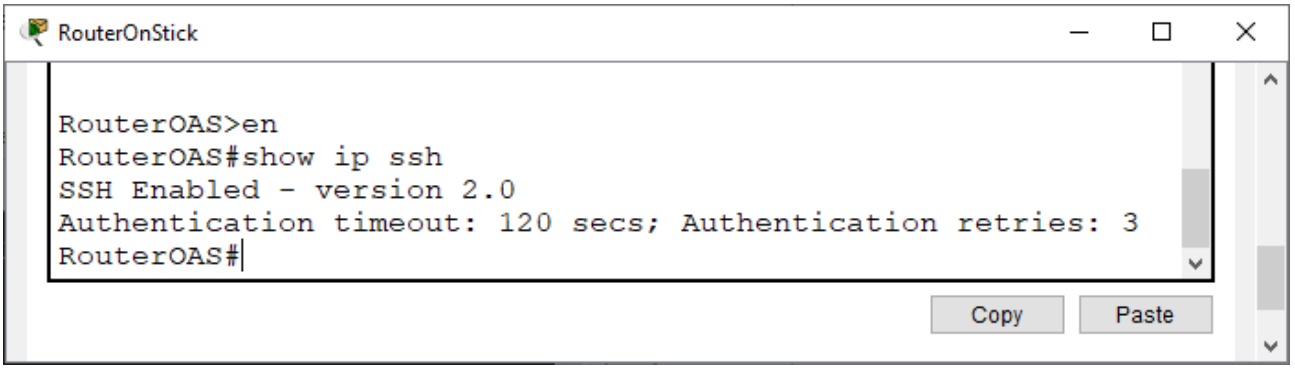
a. Launch the Router CLI (Command Line Interface).

i. Click on the Router to open the "**RouterOnStick**" Configuration Window.
ii. Navigate to the **CLI** tab.

b. Check **SSH (Version 2)** Server status **(Success!)**

c. Configuration Commands:

```
RouterOAS>en
RouterOAS#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication
retries: 3
RouterOAS#
```



Step 17: Configure Secure Shell (SSH) on Switch

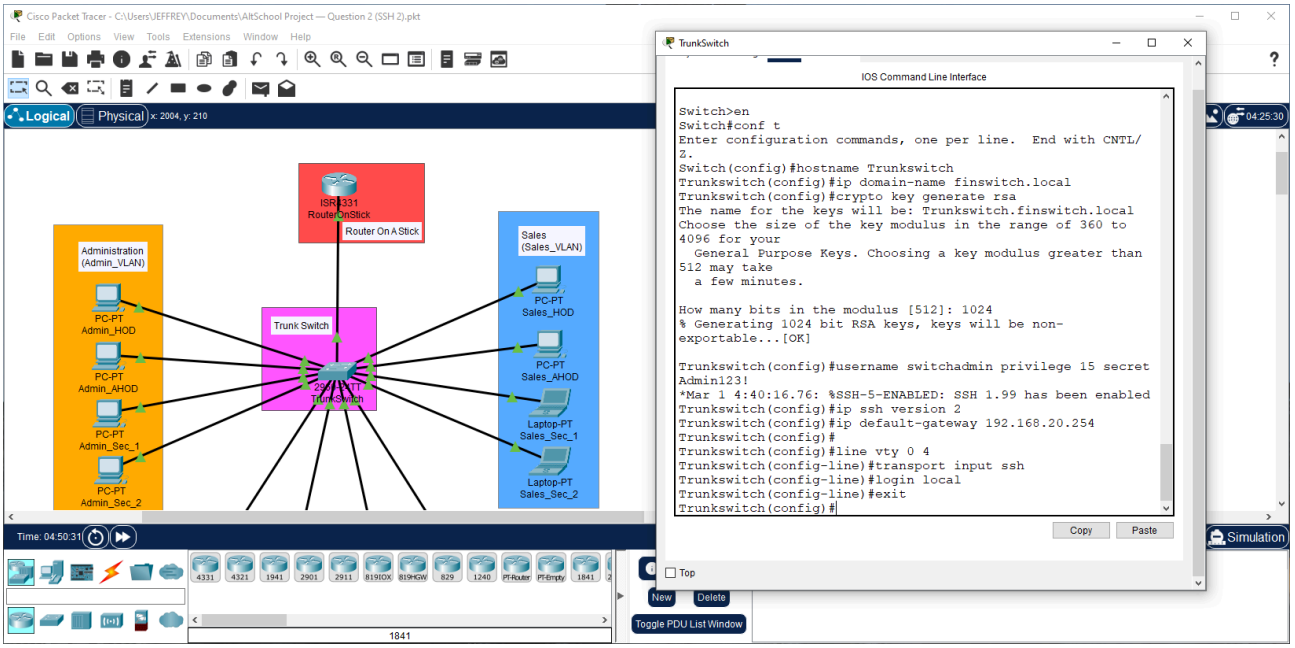
a. Launch the **Switch** CLI (Command Line Interface).
i. Click on the Switch to open the "TrunkSwitch" Configuration Window.
ii. Navigate to the **CLI** tab.

b. Configure Secure Shell
i. Configure **hostname** (switchadmin) and **domain** (finswitch.local)
ii. Generate **RSA Cryptographic Keys** (Size: 1024 bit)
iii. Create a local account **Username** (jeffreyadmin) and encrypted **Password** and grant full administrative/privileged access.
iv. Assign **Default Gateway** to IP address inside IT_VLAN.
v. Restrict Traffic type to **SSH Version** (Version 2).
NOTE: This makes the device only accept encrypted SSH traffic and disqualifies/disables all unsecure connection types including **TELNET.**
vi. Configure **VTY (Virtual Terminal) Lines**.

c. Configuration Commands:

```
Switch>en
Switch#conf t
Switch(config)#hostname Trunkswitch
Trunkswitch(config)#ip domain-name finswitch.local
Trunkswitch(config)#crypto key generate rsa
The name for the keys will be:
Trunkswitch.finswitch.local
Choose the size of the key modulus in the range of 360
to 4096 for your
```

```
General Purpose Keys. Choosing a key modulus greater
than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable...[OK]
Trunkswitch(config)#username switchadmin privilege 15
secret Admin123!
*Mar 1 4:40:16.76: %SSH-5-ENABLED: SSH 1.99 has been
enabled
Trunkswitch(config)#ip ssh version 2
Trunkswitch(config)#ip default-gateway 192.168.20.254
Trunkswitch(config)#line vty 0 4
Trunkswitch(config-line)#transport input ssh
Trunkswitch(config-line)#login local
Trunkswitch(config-line)#exit
Trunkswitch(config)#
```



Step 18: Verify SSH Status

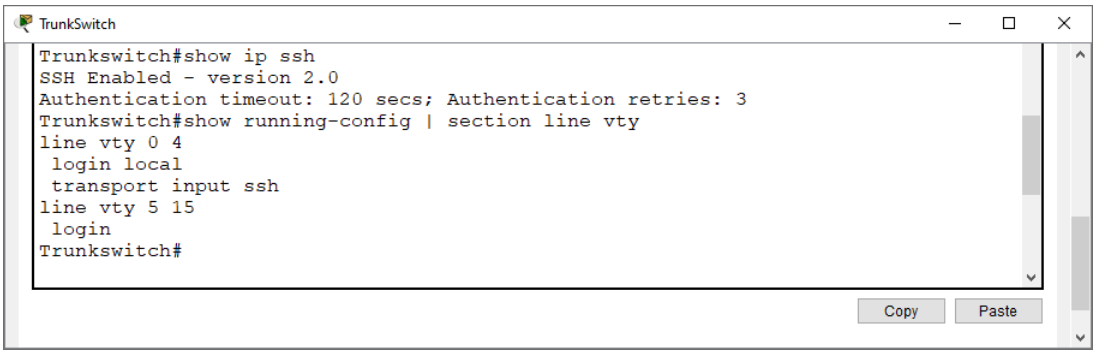
a. Launch the **Switch** CLI (Command Line Interface).
   i. Click on the Switch to open the "TrunkSwitch" Configuration Window.
   ii. Navigate to the **CLI** tab.

b. Check **SSH (Version 2)** Server status **(Success!)** and display active configurations.

c. Configuration Commands:

```
Trunkswitch#show ip ssh
      SSH Enabled - version 2.0
      Authentication timeout: 120 secs; Authentication
      retries: 3
Trunkswitch#show running-config | section line vty
```

```
line vty 0 4
login local
transport input ssh
line vty 5 15
login
Trunkswitch#
```



Challenges & Lessons Learned

- Interpreting the difference between results of pings between computers on different VLANs before and after configuring ACLs was at first challenging to interpret, but it became clearer with an applied understanding of the travel route of pings (ICMP echo request and reply packets) and how they would be affected by the configuration and location of ACL rules.
- Configuring Secure Shell (SSH) on the Router and on the Switch provided an opportunity to securely and remotely access and configure the network devices. Limiting all traffic input on the Router and the Switch to (the encrypted) SSH restricts any unsecure traffic, including that of the TELNET variety.
- CLIs provide an opportunity for extensive device configuration.

Security Justification

Access Control Lists (ACL)

An Access Control List (ACL) is a security mechanism which controls access to resources. It is a list which includes instructions/rules about who is allowed or denied access to computer environments. It functions as a security control by specifying what directions of data traffic in a network are permitted and which are not, utilizing source and destination details.

ACL & Security

ACLs ensure security in situations where multiple users, via their endpoint devices, share network infrastructure and resources. A most common situation of this sort is in organizations, where different departments are both interconnected and connected to the wider internet, via local network devices. ACLs help maintain security by controlling access between network devices and network segments. This, in addition to controls like network segmentation, helps keep communication parameters well within established security policies. ACLs are used to support security in the following ways:

- **Principle of Least Privilege**
  ACLs are an effective tool for administrators to achieve the Principle of Least Privilege. It helps them define access permissions for users and groups, granting them the minimum access that's needed for them to effectively fulfil their roles.
  In the example of the preceding network configuration project, ACLs were used to enact the security design which was developed with the Least Privilege Principle, as is relevant to the organization.
- **Zero Trust**
  ACLs can be implemented in the enactment of zero-trust policies, by enforcing granular and detailed permissions in a network.
- **Separation of Duties**
  ACLs help achieve Separation of Duties by restricting users' access to only the data, devices and resources they need for their specific roles, preventing the likelihood of a single user (or an attacker, if the user's system is compromised) having access to a broader range of sensitive data and misusing it. ACLs ensure users aren't granted conflicting permissions, as well as reduce the complexity of security investigations and audits.

Conclusion

ACLs are an effective tool in a security administrator's kit to help ensure a secure network environment and to actualize organizations' security policies.