

Hierarchical Enterprise Network Infrastructure Design and Deployment

A Layered VLAN-Based Architecture Utilizing VLSM, Inter-VLAN Routing, and Site-to-Site VPN to Connect Multi-Department Offices with Scalable and Secure Communication

WE INNOVATE BOOTCAMP – 2025

Omar Khaled

Yehia Mostafa

Youssef Emad

Ziad Mahmoud

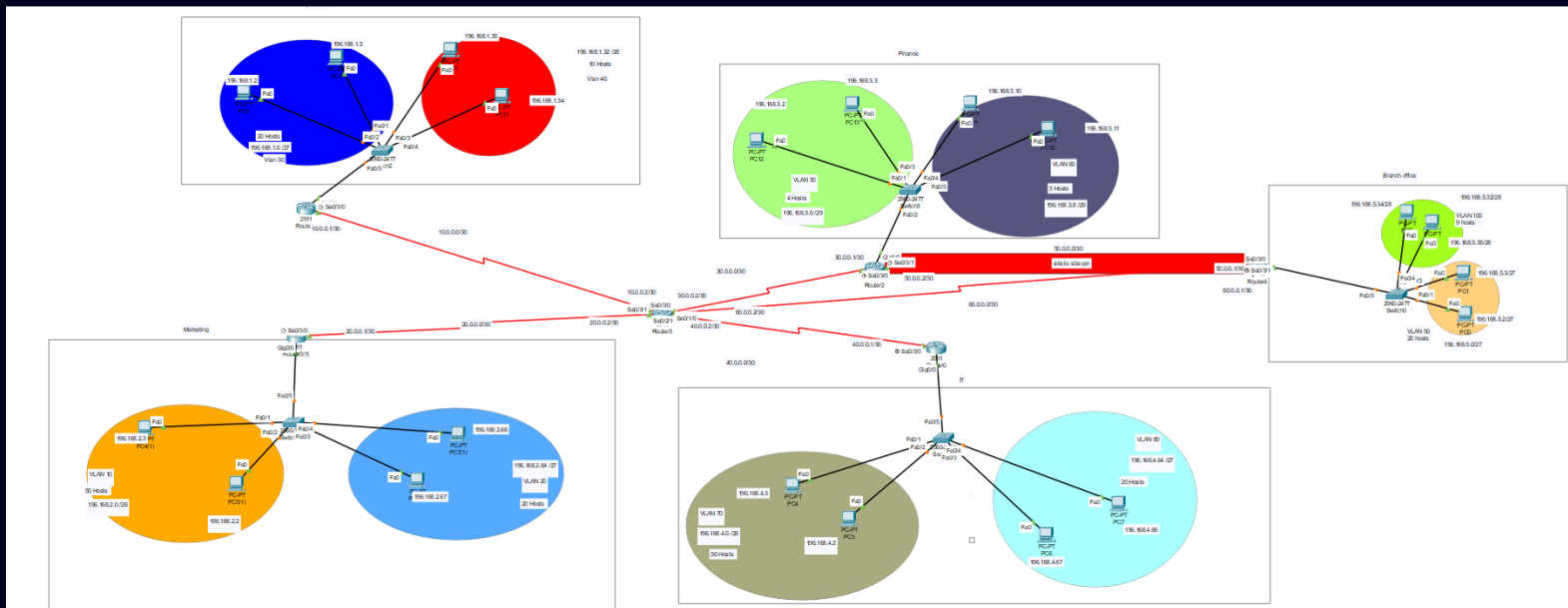
Ziad Tarek

TABLE OF CONTENTS

- Project Overview
- Network Topology Diagram
- IP Addressing Scheme
- VLAN Configuration and Design
- Switching Infrastructure and Inter-VLAN Routing
- Routing Design and Protocols
- Security & Branch Connectivity
- SSH Configuration & testing

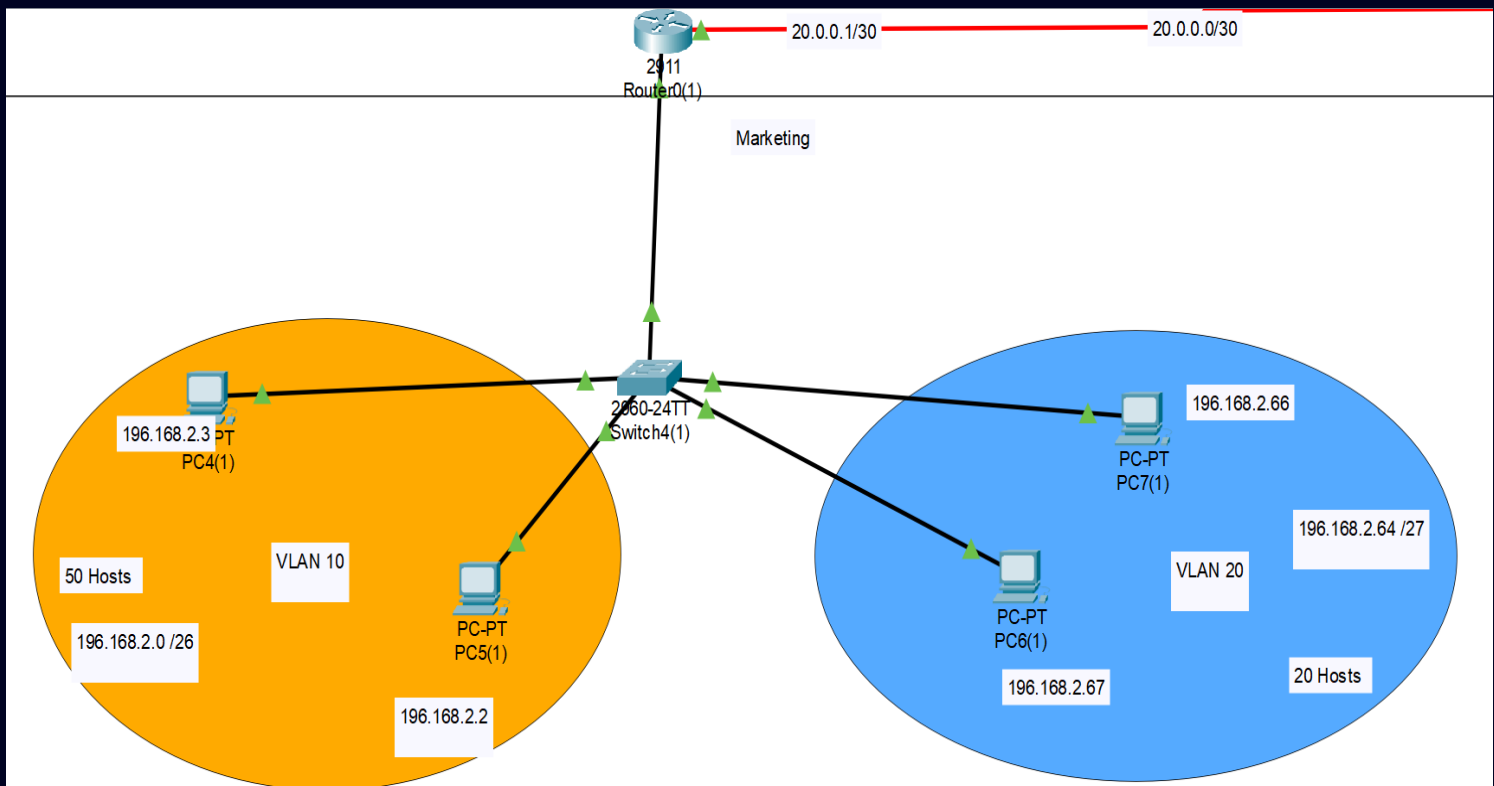
PROJECT OVERVIEW

This project aims to design and simulate a complete enterprise network using Cisco Packet Tracer. The network connects a main site with four departments and one remote branch office. Each department is assigned two VLANs for logical segmentation. Advanced networking features such as VLSM, Inter-VLAN Routing, and a site-to-site VPN are implemented to ensure efficient and secure communication.



NETWORK TOPOLOGY

For each department, a star topology was implemented. It consists of 2 VLANs with a VLSM adoption to maximize the efficiency of the number of hosts chosen. Here is an example department which you can scale the 3 other departments upon with statically assigned pcs and interfaces Ips.



IP ADDRESSING SCHEME

For the IP Addressing, we implemented **static** IP assignment and **VLSM (Variable Length Subnet Masking)** to subnet each VLAN with the expected number of hosts e.g. for 50 hosts the closest number of possible IP addresses is 62 usable IP addresses ($2^6 - 2$). Here is an example of the implementation in the Marketing department. As shown in the previous photo, the subnet mask is 255.255.255.192 in VLAN 10 because the number of host bits needed is 6 (2^6) therefore it needs 2 network bits. Here is a table showing the IP addresses of the 4 departments and the branch office.

Department	VLAN	Subnet	CIDR	Gateway IP	Usable Range	Broadcast
Operations	30	196.168.1.0	/27	196.168.1.1	.2 – .30	.31
	40	196.168.1.32	/28	196.168.1.33	.34 – .46	.47
Marketing	10	196.168.2.0	/26	196.168.2.1	.2 – .62	.63
	20	196.168.2.64	/27	196.168.2.65	.66 – .94	.95
Finance	50	196.168.3.0	/29	196.168.3.1	.2 – .6	.7
	60	196.168.3.8	/29	196.168.3.9	.10 – .14	.15
IT	70	196.168.4.0	/26	196.168.4.1	.2 – .62	.63
	80	196.168.4.64	/27	196.168.4.65	.66 – .94	.95
Branch Teller	100	196.168.5.32	/28	196.168.5.33	.34 – .46	.47
Branch Mgmt	90	196.168.5.0	/27	196.168.5.1	.2 – .30	.31

VLAN CONFIGURATION

For the VLAN Configuration, the table below summarizes the VLAN configuration, including VLAN IDs, names, and the departments and ports assigned to each.

VLAN ID	Name	Department	Number of Hosts	Subnet	Switch Port Assignments
10	VLAN10	Marketing	50	196.168.2.0/26	Fa0/1, Fa0/2
20	VLAN20	Marketing	20	196.168.2.64/27	Fa0/3, Fa0/4
30	VLAN30	Operations	20	196.168.1.0/27	Fa0/1, Fa0/2
40	VLAN40	Operations	10	196.168.1.32/28	Fa0/3, Fa0/4
50	VLAN50	Finance	4	196.168.3.0/29	Fa0/1, Fa0/2
60	VLAN60	Finance	3	196.168.3.8/29	Fa0/3, Fa0/4
70	VLAN70	IT	50	196.168.4.0/26	Fa0/1, Fa0/2
80	VLAN80	IT	20	196.168.4.64/27	Fa0/3, Fa0/4
90	VLAN90	Branch Mgmt	20	196.168.5.0/27	Fa0/1, Fa0/2
100	VLAN100	Branch Teller	9	196.168.5.32/28	Fa0/3, Fa0/4

SWITCH INFRASTRUCTURE AND INTER-VLAN ROUTING

Each department is connected to an access switch, which connects to a router via trunk links. The switches are responsible for VLAN segmentation, local switching, and forwarding traffic to the router. For inter-VLAN communication, let's explain on the Marketing department. Default gateways (subinterfaces' IP addresses) were set for each VLAN and switch ports were manually assigned to access or trunk mode. Router-on-a-stick has been implemented, having a single router with multiple subinterfaces (e.g. g0/0.10, g0/0.20) handles routing between VLANs. DOT1Q protocol was used for router trunk. Let's show a sample of the configuration of the switch and router.

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#end
Switch#write memory

# Router
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 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 gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#end
Router#write memory
```



ROUTING DESIGNS AND PROTOCOLS

The enterprise network employs a hierarchical routing structure using OSPF (Open Shortest Path First) as the primary dynamic routing protocol. Main Router Configuration

The main router connects to all departmental routers and the branch office through WAN serial interfaces:

Serial0/3/0: 10.0.0.0/30 (Operations)

Serial0/3/1: 20.0.0.0/30 (Marketing)

Serial0/2/0: 30.0.0.0/30 (Finance)

Serial0/2/1: 40.0.0.0/30 (IT)

Serial0/1/0: 60.0.0.0/30 (Branch)

THE MAIN ROUTING TABLE

```
Main# show ip route
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      20.0.0.0/30 is directly connected, Serial0/3/1
L      20.0.0.2/32 is directly connected, Serial0/3/1
      30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      30.0.0.0/30 is directly connected, Serial0/2/0
L      30.0.0.2/32 is directly connected, Serial0/2/0
      40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      40.0.0.0/30 is directly connected, Serial0/2/1
L      40.0.0.2/32 is directly connected, Serial0/2/1
      60.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      60.0.0.0/30 is directly connected, Serial0/1/0
L      60.0.0.2/32 is directly connected, Serial0/1/0
      196.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
O      196.168.1.0/27 [110/65] via 10.0.0.1, 00:25:45, Serial0/3/0
O      196.168.1.32/28 [110/65] via 10.0.0.1, 00:25:45, Serial0/3/0
      196.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
O      196.168.2.0/26 [110/65] via 20.0.0.1, 00:25:45, Serial0/3/1
O      196.168.2.64/27 [110/65] via 20.0.0.1, 00:25:45, Serial0/3/1
      196.168.3.0/29 is subnetted, 2 subnets
O      196.168.3.0/29 [110/65] via 30.0.0.1, 00:25:45, Serial0/2/0
O      196.168.3.8/29 [110/65] via 30.0.0.1, 00:25:45, Serial0/2/0
      196.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
O      196.168.4.0/26 [110/65] via 40.0.0.1, 00:25:45, Serial0/2/1
O      196.168.4.64/27 [110/65] via 40.0.0.1, 00:25:45, Serial0/2/1
```

BRANCH ROUTER CONFIGURATION

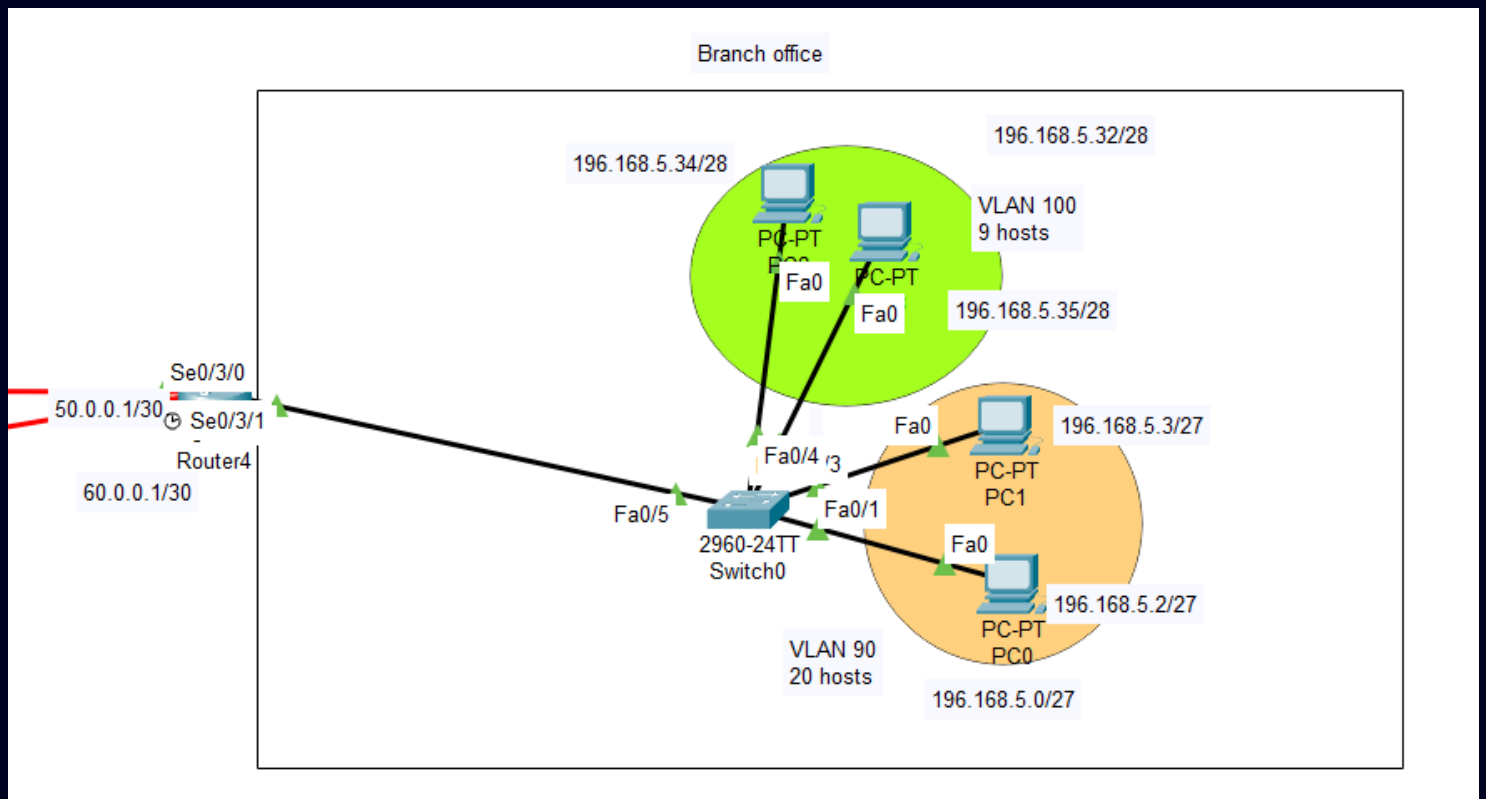
The branch router connects back to the Finance and Main routers using two serial links:

Serial 0/3/0: 50.0.0.0/30 (to Finance)

Serial 0/3/1: 60.0.0.0/30 (to Main)

KEY ROUTES

This router uses static routing to reach remote subnets in the Finance department (196.168.3.0/29 & 196.168.3.8/29). It is Directly connected to VLANs (196.168.5.0/27, 196.168.5.32/28).



ROUTING TABLE

```
50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    50.0.0.0/30 is directly connected, Serial0/3/0
L    50.0.0.1/32 is directly connected, Serial0/3/0
60.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    60.0.0.0/30 is directly connected, Serial0/3/1
L    60.0.0.1/32 is directly connected, Serial0/3/1
196.168.3.0/29 is subnetted, 2 subnets
S    196.168.3.0/29 [1/0] via 50.0.0.2
S    196.168.3.8/29 [1/0] via 50.0.0.2
196.168.5.0/24 is variably subnetted, 4 subnets, 3 masks
C    196.168.5.0/27 is directly connected, GigabitEthernet0/0.90
L    196.168.5.1/32 is directly connected, GigabitEthernet0/0.90
C    196.168.5.32/28 is directly connected,
GigabitEthernet0/0.100
L    196.168.5.33/32 is directly connected,
GigabitEthernet0/0.100
Branch#
```

DEPARTMENTS' ROUTERS

The network uses OSPF for dynamic routing, with the Main router configured as the central OSPF router. All VLAN subnets from the departments are advertised into the OSPF process, allowing for efficient route distribution across the enterprise. Inter-VLAN routing is implemented using a router-on-a-stick setup, where each VLAN has a dedicated subinterface on the router, enabling communication between different VLANs and across departments.

SECURITY & BRANCH CONNECTIVITY

For secure communication, VPN connects the Finance VLANs (196.168.3.0/29 and 196.168.3.8/29) with the Branch VLANs (196.168.5.0/27 and 196.168.5.32/28). The connection type is a Site-to-Site IPsec VPN tunnel utilizing ESP (Encapsulating Security Payload) as the transport protocol. AES is used for encryption, and SHA-HMAC is applied for authentication. The VPN operates with IKE Phase 1 in the active QM_IDLE state. The VPN endpoints are defined as 50.0.0.2 on the Finance router and 50.0.0.1 on the Branch router.

VPN TRAFFIC FLOW

The VPN traffic flow defines the protected communication between the Finance and Branch networks, where specific subnets are secured through the IPsec tunnel. The protected traffic includes communication from 196.168.3.0/29 (Finance) to both 196.168.5.0/27 and 196.168.5.32/28 (Branch), and from 196.168.3.8/29 (Finance) to the same two Branch subnets. The corresponding subnet masks are 255.255.255.224 and 255.255.255.240, respectively. To facilitate this communication, the Finance router has static routes pointing to the Branch LAN subnets through the Branch router IP 50.0.0.1, while the Branch router has static routes pointing to the Finance LAN subnets via the Finance router IP 50.0.0.2. The IPsec VPN guarantees encrypted and secure data transfer between these defined networks.

CONFIGURATION VERIFICATION

```

Finance#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
50.0.0.1     50.0.0.2     QM_IDLE        1042      0  ACTIVE

IPv6 Crypto ISAKMP SA

Finance#
Finance#show crypto ipsec sa

interface: Serial0/3/1
  Crypto map tag: VPN-MAP, local addr 50.0.0.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (196.168.3.0/255.255.255.248/0/0)
  remote ident (addr/mask/prot/port): (196.168.5.0/255.255.255.192/0/0)
  current_peer 50.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 0
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

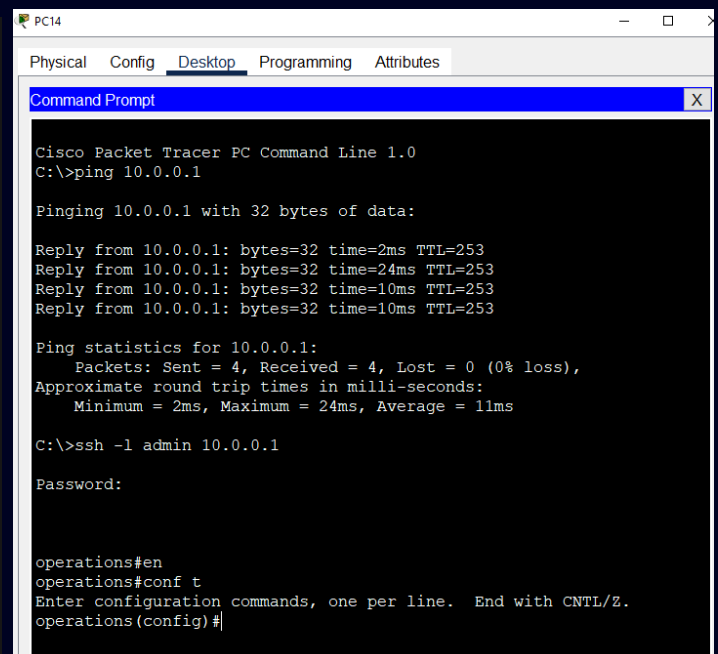
    local crypto endpt.: 50.0.0.2, remote crypto endpt.:50.0.0.1
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/1
    current outbound spi: 0xF1CBB168(4056658280)

  inbound esp sas:
    spi: 0x5F59EBB7(1599728567)
      transform: esp-aes esp-sha-hmac ,
  
```

SSH CONFIGURATION & TESTING

The SSH configuration was implemented on the Operations router. First, the domain name was defined to allow for cryptographic operations, followed by the generation of an RSA key pair used for SSH encryption. The router was then configured to enforce the more secure SSH Version 2 protocol. A local administrative user account was created with an encrypted password to control access. To finalize SSH access, virtual terminal lines were restricted to allow only SSH connections and were set to authenticate using the locally defined credentials. Connectivity to the router was verified using ICMP ping from a remote PC, showing 100% successful packet transmission with stable latency. After confirming network availability, an SSH session was established using the username and password, successfully accessing the router at 10.0.0.1. Here is an example connection and commands used.

```
ip domain-name mynetwork.local
crypto key generate rsa
ip ssh version 2
username admin secret admin123
line vty 0 4
transport input ssh
login local
```



```
PC14
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=2ms TTL=253
Reply from 10.0.0.1: bytes=32 time=24ms TTL=253
Reply from 10.0.0.1: bytes=32 time=10ms TTL=253
Reply from 10.0.0.1: bytes=32 time=10ms TTL=253

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 24ms, Average = 11ms

C:\>ssh -l admin 10.0.0.1

Password:

operations#en
operations#conf t
Enter configuration commands, one per line. End with CNTL/Z.
operations(config)#
```