ACADEMIC SESSION: 2024-2025

PRACTICAL NETWORKS 2

PRACTICAL ASSESSMENT REPORT

BORDON, JOSE

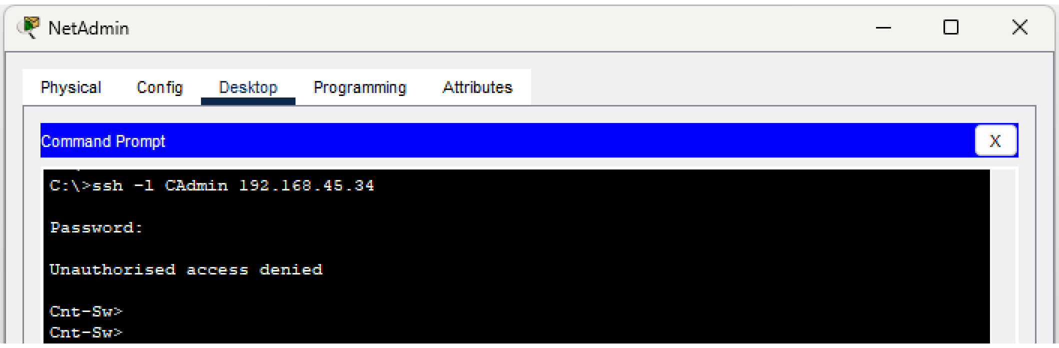
Introduction

This report documents the implementation and verification of a network design as part of the Practical Networks 2 (CSN08102) assessment. The objective has been to configure and secure a multi-VLAN network with inter-VLAN routing, DHCP, NAT, port security, SSH remote access, and RIP version 2.

Using Cisco Packet Tracer, I have completed the unconfigured devices (Central, Cnt-Sw, and NetAdmin), based on the provided topology and assessment requirements. Each of the network elements has been tested and verified, with screenshots and brief explanations provided to demonstrate full functionality and compliance with the brief.

Verify remote access to Cnt-Sw by using SSH from a PC

An SSH connection to Cnt-Sw was established from NetAdmin using the username CAdmin. The MOTD banner was displayed, and password prompt appeared, confirming that SSH access was securely configured on the switch.



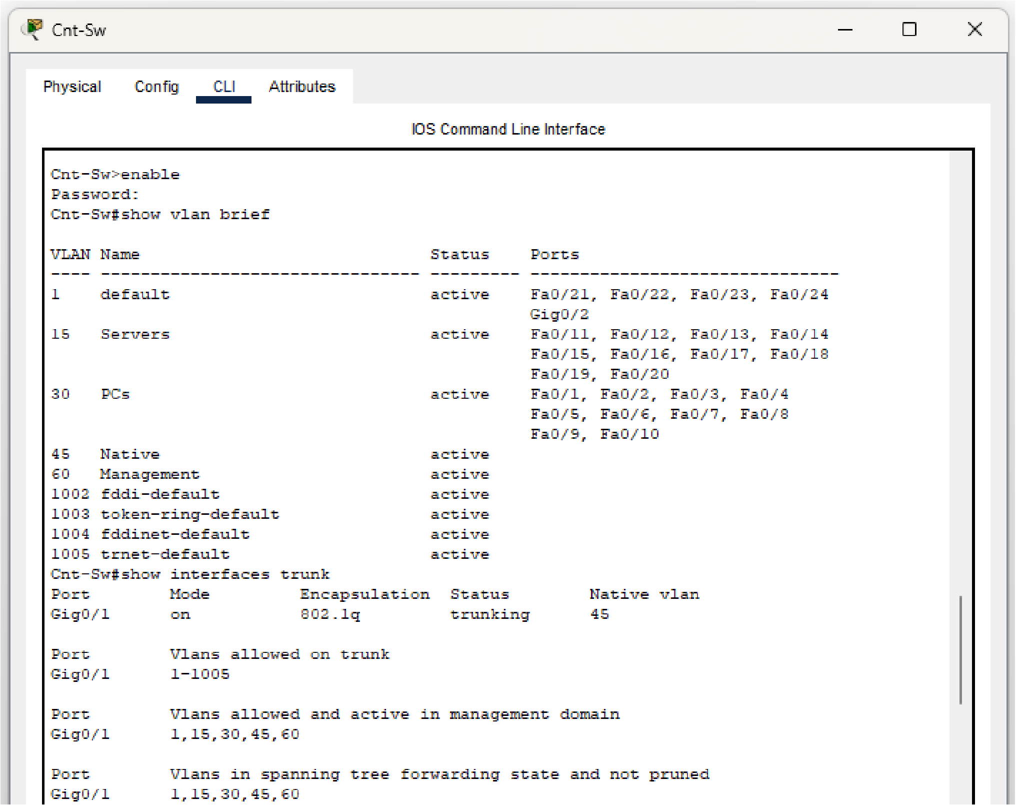
```
C:\>ssh -l CAdmin 192.168.45.34

Password:

Unauthorised access denied

Cnt-Sw>
Cnt-Sw>
```

Verify VLANs are assigned to appropriate ports and port security is in force

All VLANs (15, 30, 45, 60) were correctly created and assigned. Ports Fa0/1-Fa0/10 and Fa0/11-Fa0/20 were manually set as access ports to the correct VLANs.
Port security on Fa0/1 is active, with a sticky MAC address learned and violation mode set to restrict. All unused ports (Fa0/21-Fa0/24) are shut down.

Test: VLAN Assignments and Trunking

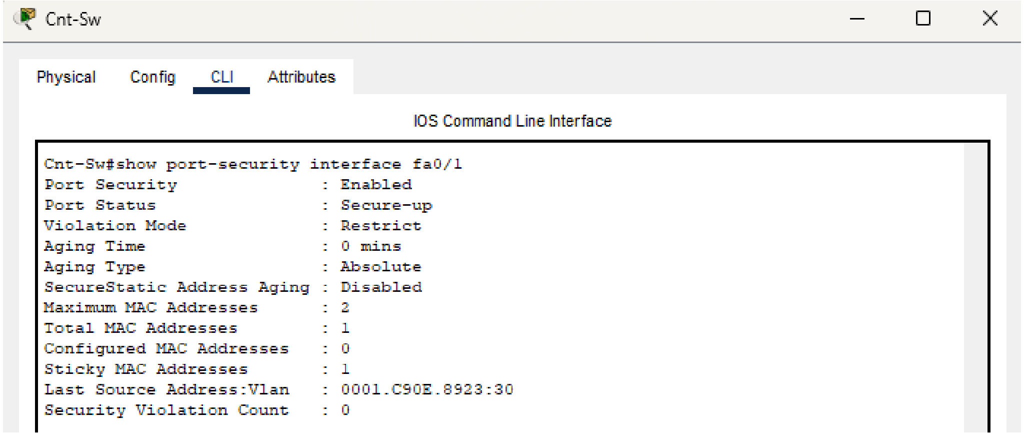
This screenshot below confirms that VLANs 15 (Servers), 30 (PCs), 45 (Native), and 60 (Management) are correctly configured and assigned to their respective access ports. It also verifies that interface Gig0/1 is operating as a trunk port, allowing VLANs 1, 15, 30, 45, and 60 with VLAN 45 set as the native VLAN.



```
Cnt-Sw>enable
Password:
Cnt-Sw#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
15   Servers                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
30   PCs                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
45   Native                           active
60   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Cnt-Sw#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      45

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,15,30,45,60

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,15,30,45,60
```

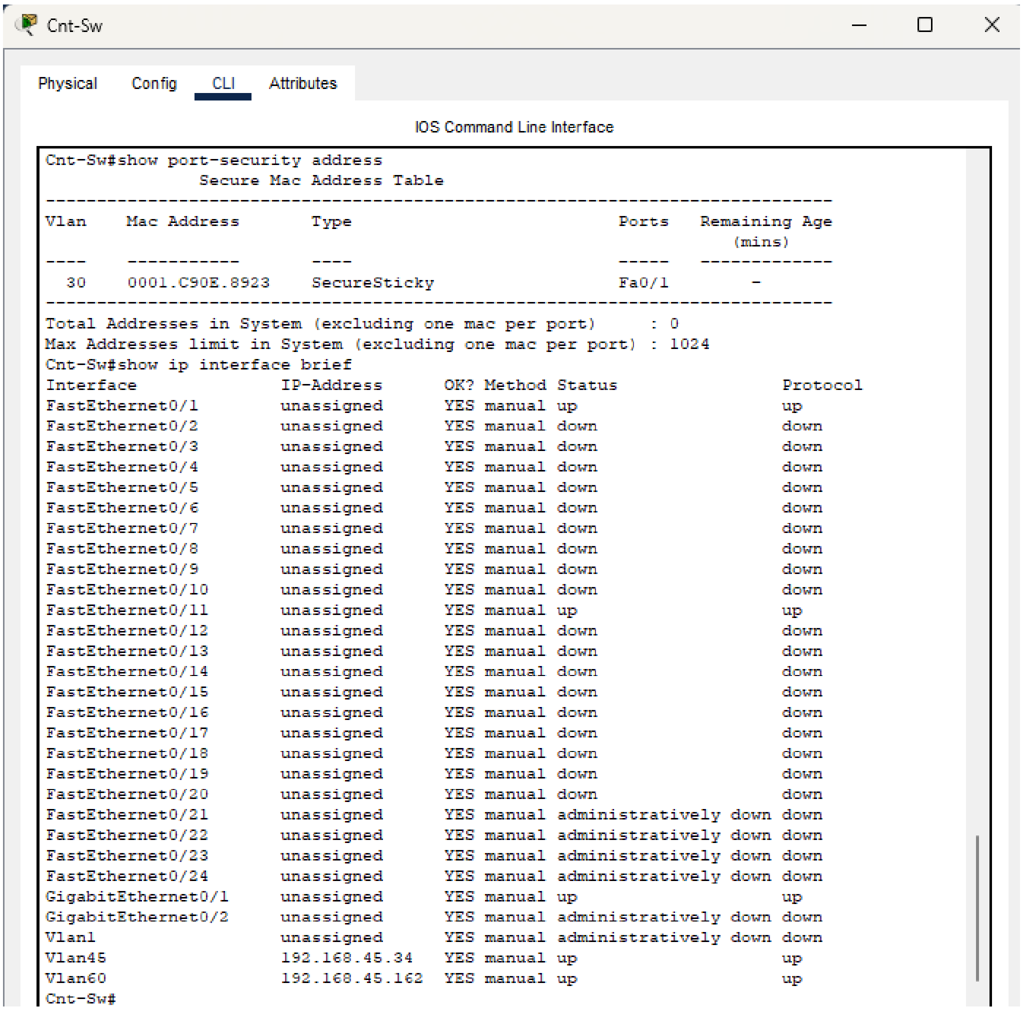
Test: Port Fa0/1 Port-Security Configuration

This screenshot confirms that Fa0/1 is secured with port security, configured to allow up to 2 MAC addresses using sticky MAC learning. The violation mode is set to restrict, and the interface is currently in a secure-up state with no violations recorded.



```
Cnt-Sw#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.C90E.8923:30
Security Violation Count   : 0
```

Test: Port Security and Interface Status
This output confirms that port Fa0/1 has port security enabled with a dynamically learned sticky MAC address (0001.C90E.8923). Additionally, all unused ports are administratively shut down or down, meeting the port security and unused port requirements from the specification.

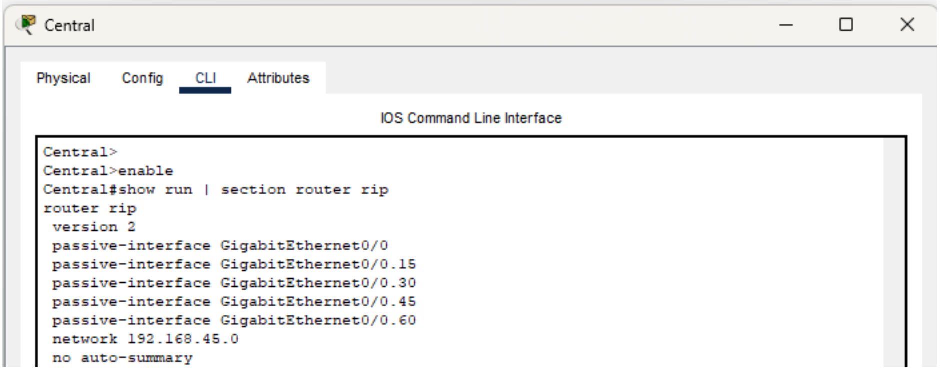


```
Cnt-Sw#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  30    0001.C90E.8923    SecureSticky                  Fa0/1        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Cnt-Sw#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan45                 192.168.45.34   YES manual up                    up
Vlan60                 192.168.45.162  YES manual up                    up
Cnt-Sw#
```

Verify RIPv2 is operational, and routing tables are complete

RIPv2 was configured with one network statement for 192.168.45.0. Passive interfaces were correctly set to prevent RIP advertisements on internal subinterfaces.
The show IP route output confirmed receipt of RIP-learned routes, and the debug IP rip showed updates being sent and received.

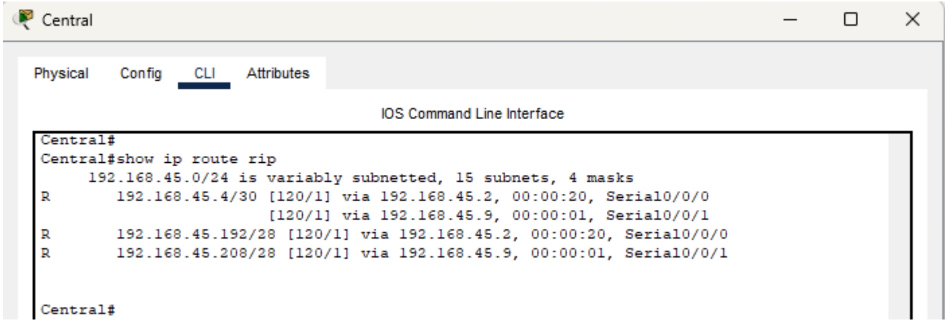
Test: Verify the RIP Configuration
This output confirms that RIP version 2 is enabled on Central, with all internal interfaces set to passive. A single network 192.168.45.0 statement is used, and auto-summary is disabled.



```
Central>
Central>enable
Central#show run | section router rip
router rip
 version 2
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/0.15
 passive-interface GigabitEthernet0/0.30
 passive-interface GigabitEthernet0/0.45
 passive-interface GigabitEthernet0/0.60
 network 192.168.45.0
 no auto-summary
```

Test: Check the RIP Learned Routes

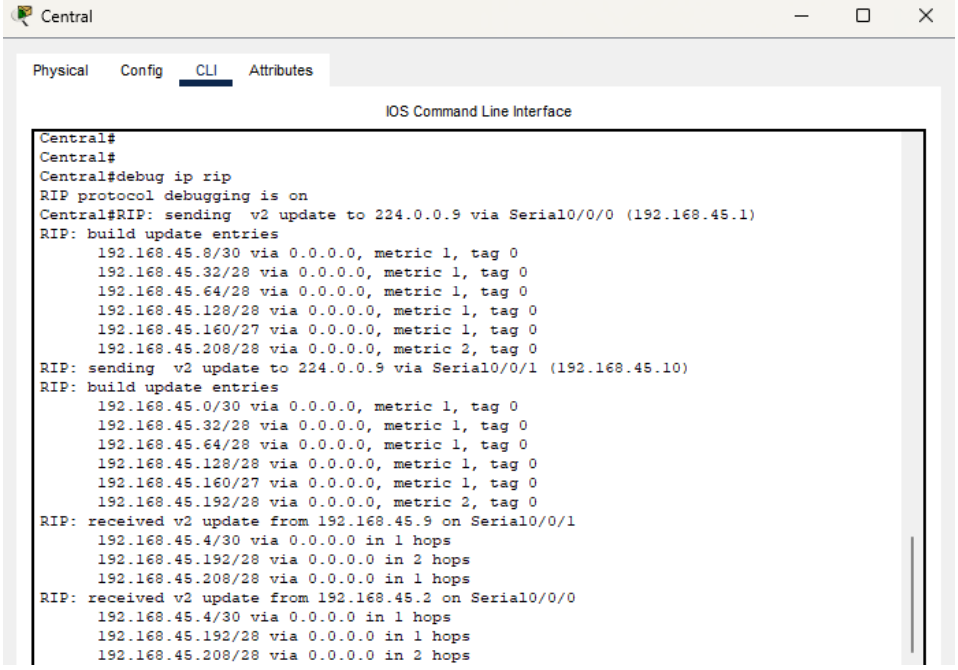
The output below confirms that Central received RIP routes from neighbouring routers. Subnets like 192.168.45.4/30, 192.168.45.192/28, and 192.168.45.208/28 were learned via RIPv2, indicating route propagation.



```
Central#
Central#show ip route rip
     192.168.45.0/24 is variably subnetted, 15 subnets, 4 masks
R       192.168.45.4/30 [120/1] via 192.168.45.2, 00:00:20, Serial0/0/0
                        [120/1] via 192.168.45.9, 00:00:01, Serial0/0/1
R       192.168.45.192/28 [120/1] via 192.168.45.2, 00:00:20, Serial0/0/0
R       192.168.45.208/28 [120/1] via 192.168.45.9, 00:00:01, Serial0/0/1


Central#
```

Test: RIP Debug Output

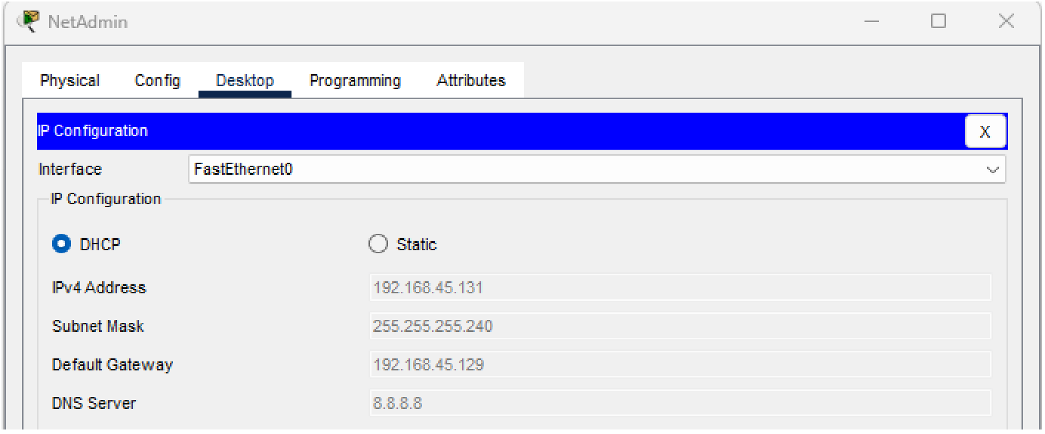
This output shows Central sending and receiving RIP v2 updates, confirming that routing information is actively exchanged over Serial links.



```
Central#
Central#
Central#debug ip rip
RIP protocol debugging is on
Central#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (192.168.45.1)
RIP: build update entries
      192.168.45.8/30 via 0.0.0.0, metric 1, tag 0
      192.168.45.32/28 via 0.0.0.0, metric 1, tag 0
      192.168.45.64/28 via 0.0.0.0, metric 1, tag 0
      192.168.45.128/28 via 0.0.0.0, metric 1, tag 0
      192.168.45.160/27 via 0.0.0.0, metric 1, tag 0
      192.168.45.208/28 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (192.168.45.10)
RIP: build update entries
      192.168.45.0/30 via 0.0.0.0, metric 1, tag 0
      192.168.45.32/28 via 0.0.0.0, metric 1, tag 0
      192.168.45.64/28 via 0.0.0.0, metric 1, tag 0
      192.168.45.128/28 via 0.0.0.0, metric 1, tag 0
      192.168.45.160/27 via 0.0.0.0, metric 1, tag 0
      192.168.45.192/28 via 0.0.0.0, metric 2, tag 0
RIP: received v2 update from 192.168.45.9 on Serial0/0/1
      192.168.45.4/30 via 0.0.0.0 in 1 hops
      192.168.45.192/28 via 0.0.0.0 in 2 hops
      192.168.45.208/28 via 0.0.0.0 in 1 hops
RIP: received v2 update from 192.168.45.2 on Serial0/0/0
      192.168.45.4/30 via 0.0.0.0 in 1 hops
      192.168.45.192/28 via 0.0.0.0 in 1 hops
      192.168.45.208/28 via 0.0.0.0 in 2 hops
```

Test: DHCP Configuration (NetAdmin)

The NetAdmin PC received its IP address automatically via DHCP from the Central router. This confirms that the DHCP pool for VLAN 30 (named "LAN") is correctly configured and functional.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.45.131

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.45.129

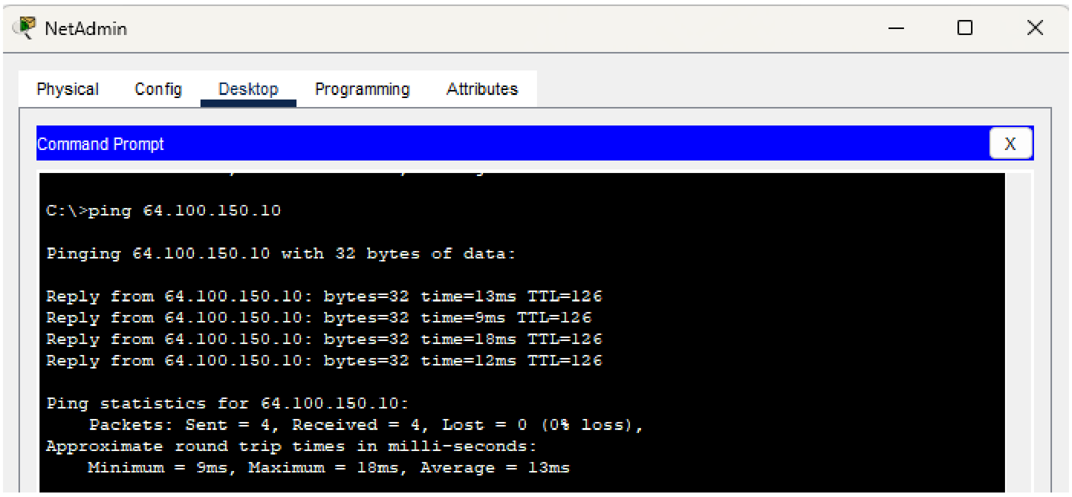
DNS Server: 8.8.8.8

Verify NAT translations both static and dynamic

NAT functionality was confirmed with dynamic PAT from NetAdmin to the Web Server and static NAT from the Outside Host to the File Server.

Test: Dynamic NAT from NetAdmin to Web Server

NetAdmin (192.168.45.131) successfully pinged 64.100.150.10, showing translation to 64.100.32.57 via PAT.

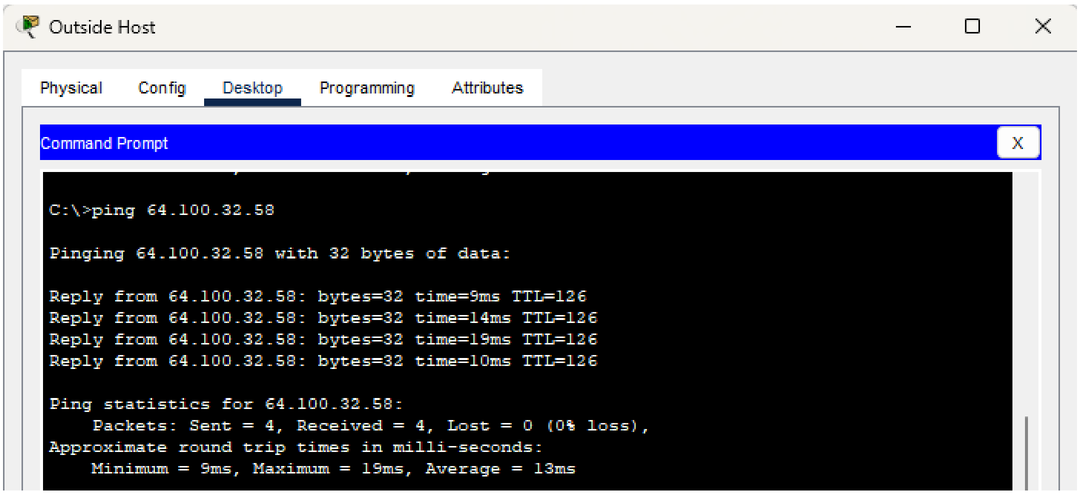


```
C:\>ping 64.100.150.10

Pinging 64.100.150.10 with 32 bytes of data:

Reply from 64.100.150.10: bytes=32 time=13ms TTL=126
Reply from 64.100.150.10: bytes=32 time=9ms TTL=126
Reply from 64.100.150.10: bytes=32 time=18ms TTL=126
Reply from 64.100.150.10: bytes=32 time=12ms TTL=126

Ping statistics for 64.100.150.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 18ms, Average = 13ms
```

Test: Static NAT from Outside Host to File Server

This screenshot shows a successful ping from the Outside Host to 64.100.32.58, the public IP statically mapped to the internal File Server 192.168.45.66.

The responses confirm that Static NAT is working, and the Outside Host can reach internal resources through the configured static translation.



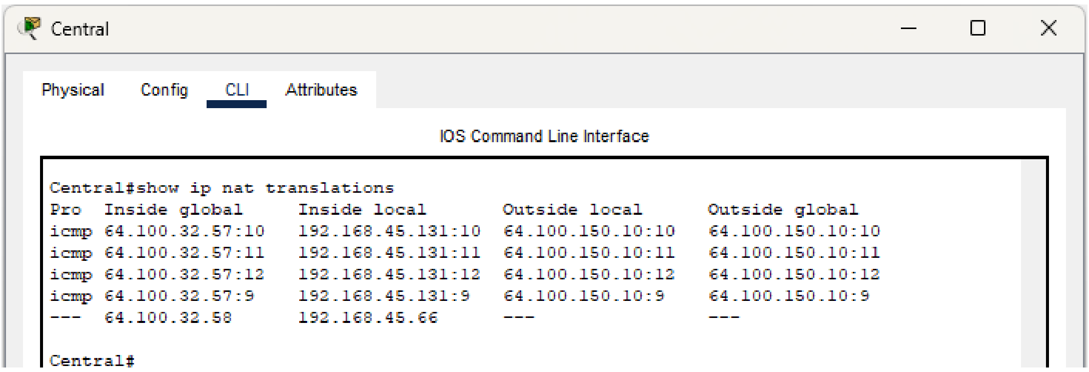
```
C:\>ping 64.100.32.58

Pinging 64.100.32.58 with 32 bytes of data:

Reply from 64.100.32.58: bytes=32 time=9ms TTL=126
Reply from 64.100.32.58: bytes=32 time=14ms TTL=126
Reply from 64.100.32.58: bytes=32 time=19ms TTL=126
Reply from 64.100.32.58: bytes=32 time=10ms TTL=126

Ping statistics for 64.100.32.58:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 19ms, Average = 13ms
```

Test: NAT Translation Table (Dynamic and Static) – Central Router

This output from show ip nat translations confirms:

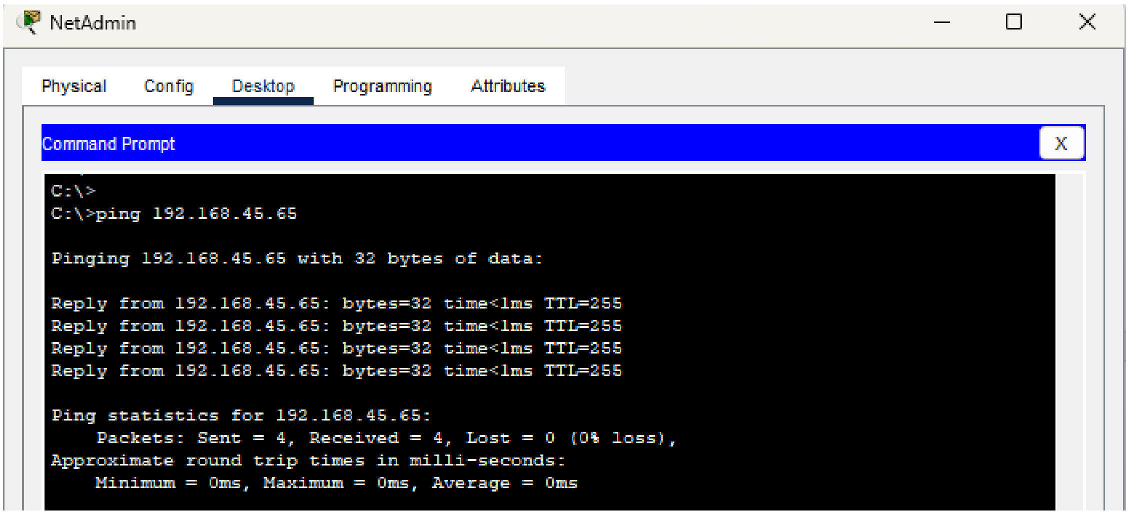
- **Dynamic NAT with PAT**: Internal host 192.168.45.131 (NetAdmin) is dynamically translated to 64.100.32.57 while accessing 64.100.150.10 (Web Server).
- **Static NAT**: Entry 64.100.32.58 - 192.168.45.66 verifies static mapping for the File Server.

This proves that static and dynamic NAT configurations work correctly on the Central router.



```
Central#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 64.100.32.57:10   192.168.45.131:10  64.100.150.10:10   64.100.150.10:10
icmp 64.100.32.57:11   192.168.45.131:11  64.100.150.10:11   64.100.150.10:11
icmp 64.100.32.57:12   192.168.45.131:12  64.100.150.10:12   64.100.150.10:12
icmp 64.100.32.57:9    192.168.45.131:9   64.100.150.10:9    64.100.150.10:9
---  64.100.32.58      192.168.45.66      ---                ---

Central#
```

Inter-VLAN Routing Test:
Although not listed as a required test, I verified inter-VLAN routing by pinging 192.168.45.65 (VLAN 15 gateway) from NetAdmin (VLAN 30). The response confirms that inter-VLAN communication is functioning correctly through the Central router.



```
C:\>
C:\>ping 192.168.45.65

Pinging 192.168.45.65 with 32 bytes of data:

Reply from 192.168.45.65: bytes=32 time<1ms TTL=255
Reply from 192.168.45.65: bytes=32 time<1ms TTL=255
Reply from 192.168.45.65: bytes=32 time<1ms TTL=255
Reply from 192.168.45.65: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.45.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```