AKIN AREMU

This project demonstrates the implementation of a secure CoffeeCorp network using VLAN segmentation, inter-VLAN routing, ACL security, DNS configuration, and router hardening using Cisco Packet Tracer

Router running-config

```
Router>enable
Router#show running-config
Building configuration...

Current configuration : 970 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
```

```
!
!
!
!
license udi pid CISCO2911/K9 sn FTX15247S30-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
```

```
interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

!

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

!

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.0

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!
```

```
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
```

Switch running-config

```
Current configuration : 1256 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
```

```
hostname Switch

!

!

!

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport access vlan 10

switchport mode access

!

interface FastEthernet0/2

switchport access vlan 20

switchport mode access

!

interface FastEthernet0/3

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!
```

```
interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!
```

```
interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

switchport mode trunk

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

no ip address

shutdown

!

!

!

!

line con 0

!

line vty 0 4

login

line vty 5 15

login

!

!
```

```
!
!
end
```

VLAN TABLE

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/4, Fa0/5, Fa0/6, Fa0/7
Fa0/8, Fa0/9, Fa0/10, Fa0/11
Fa0/12, Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Gig0/1, Gig0/2
10 SALES active Fa0/1
20 FINANCE active Fa0/2
30 SERVERS active Fa0/3
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

Trunk Ports

```
Switch#show interfaces fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

PCs and Server IP Configuration

Sales PC

IP Address: 192.168.10.10 ; Subnet Mask: 255.255.255.0 ; Default Gateway: 192.168.10.1

Finance PC

IP Address: 192.168.20.10; Subnet Mask: 255.255.255.0 ; Default Gateway: 192.168.20.1

File Server

IP Address: 192.168.30.3 ; Subnet Mask: 255.255.255.0 ; Default Gateway: 192.168.30.1

Network Design Summary

I segmented CoffeeCorp's internal network using VLANs to improve security and traffic control. I assigned VLAN10 to the sales department, VLAN 20 to the Finance department, and VLAN 30 to the internal servers. I then used a single switch to connect end devices, with access ports assigned to their VLANs. The switch's FastEthernet0/24 port is configured as a trunk link to the router, in order to allow multiple VLANs to pass traffic using IEEE 802. 1Q tagging.

I further implemented Inter-VLAN routing using a router-on-a-stick design, and the router's GigabitEthernet0/0 interface contains subinterfaces for each VLAN:

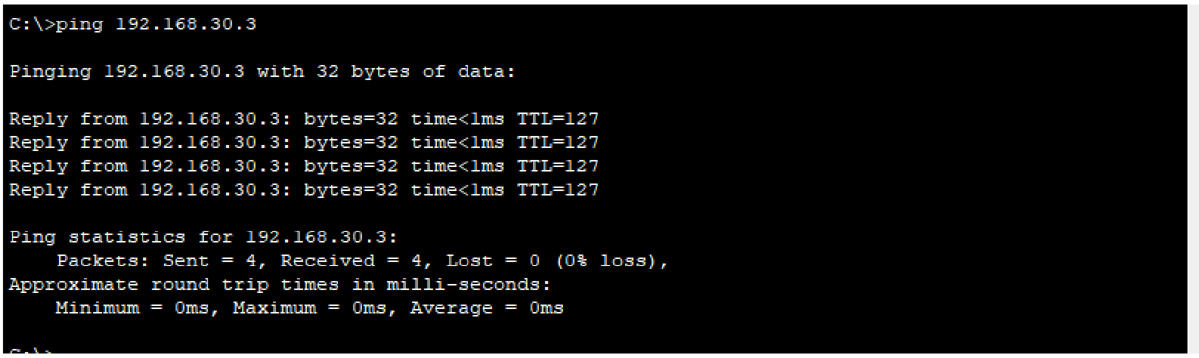
- G0/0.10 for VLAN 10 (192.168.10.1/24)

- G0/0.20 for VLAN 20 (192.168.20.1/24)

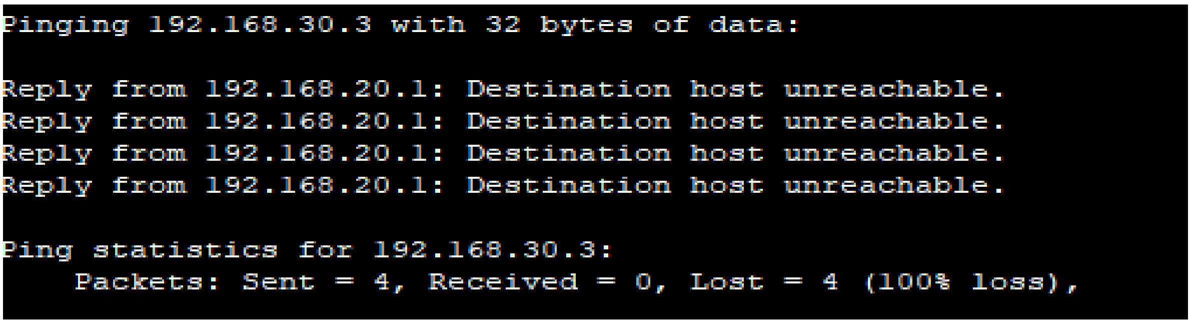
- G0/0.30 for VLAN 30 (192.168.30.1/24)

Each VLAN uses the router's subinterface IP address as its default gateway. End devices can communicate with their gateway and other authorised VLANs as configured.

❖ *Access Control Lists (ACL)*



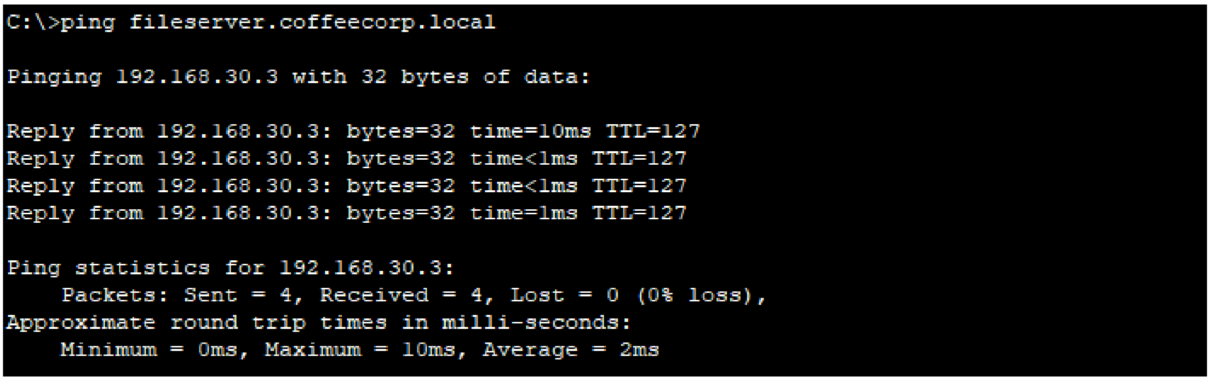
```
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



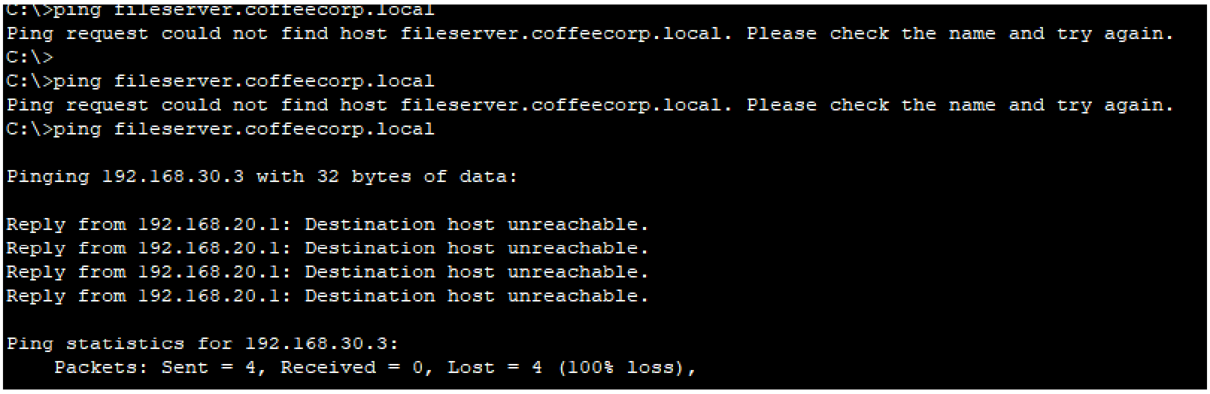
```
Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

I implemented a standard ACL on the router to restrict access to the File Server. Traffic originating from the Finance VLAN (192.168.20.0/24) is denied, while all other traffic is permitted. The ACL is applied outbound on the Server VLAN subinterface.

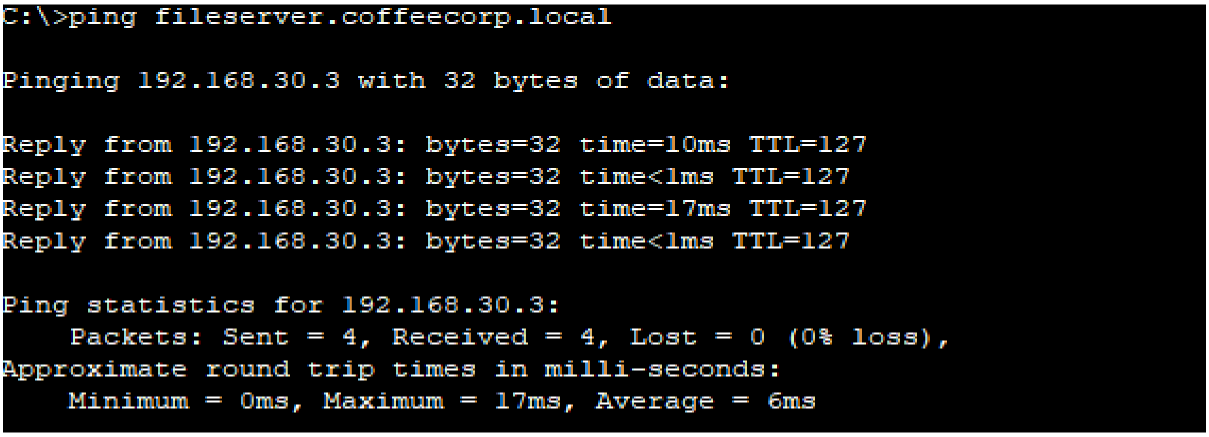
❖ *DNS Configuration (Internal Name Resolution)*



```
C:\>ping fileserver.coffeecorp.local

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=10ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```



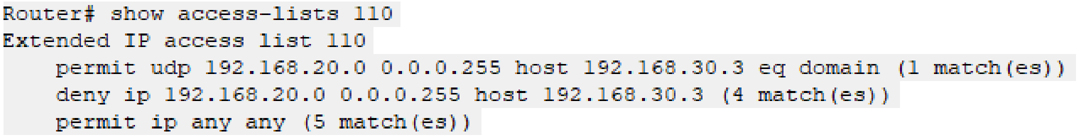
```
C:\>ping fileserver.coffeecorp.local
Ping request could not find host fileserver.coffeecorp.local. Please check the name and try again.
C:\>
C:\>ping fileserver.coffeecorp.local
Ping request could not find host fileserver.coffeecorp.local. Please check the name and try again.
C:\>ping fileserver.coffeecorp.local

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



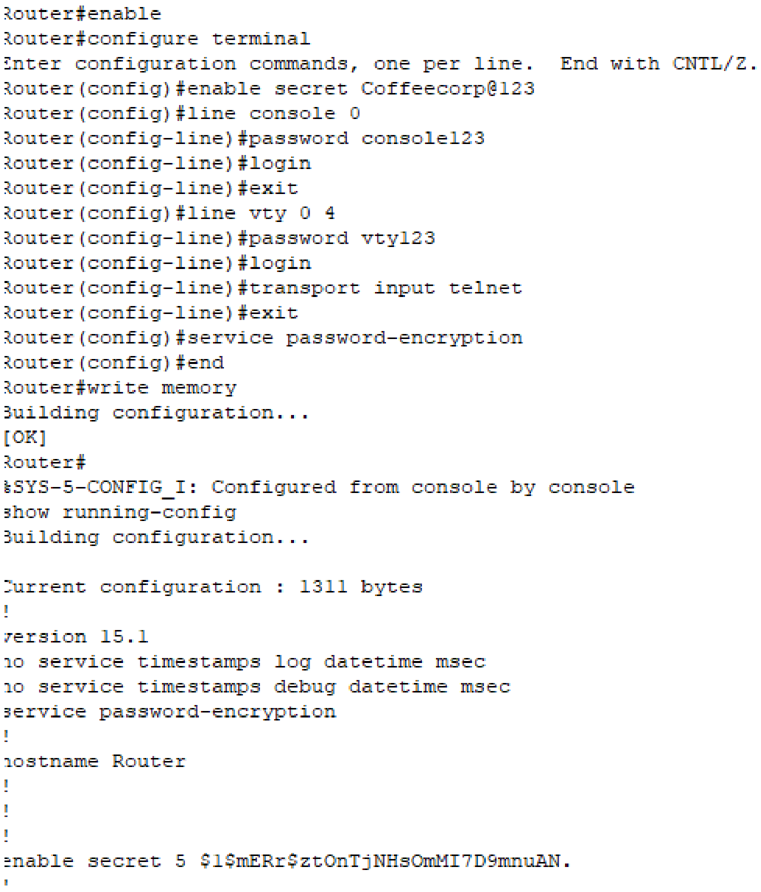
```
C:\>ping fileserver.coffeecorp.local

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=10ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time=17ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 6ms
```

I implemented an extended ACL to allow DNS queries from the Finance VLAN while still restricting access to the File Server. This ensures name resolution functions correctly without exposing sensitive server resources.

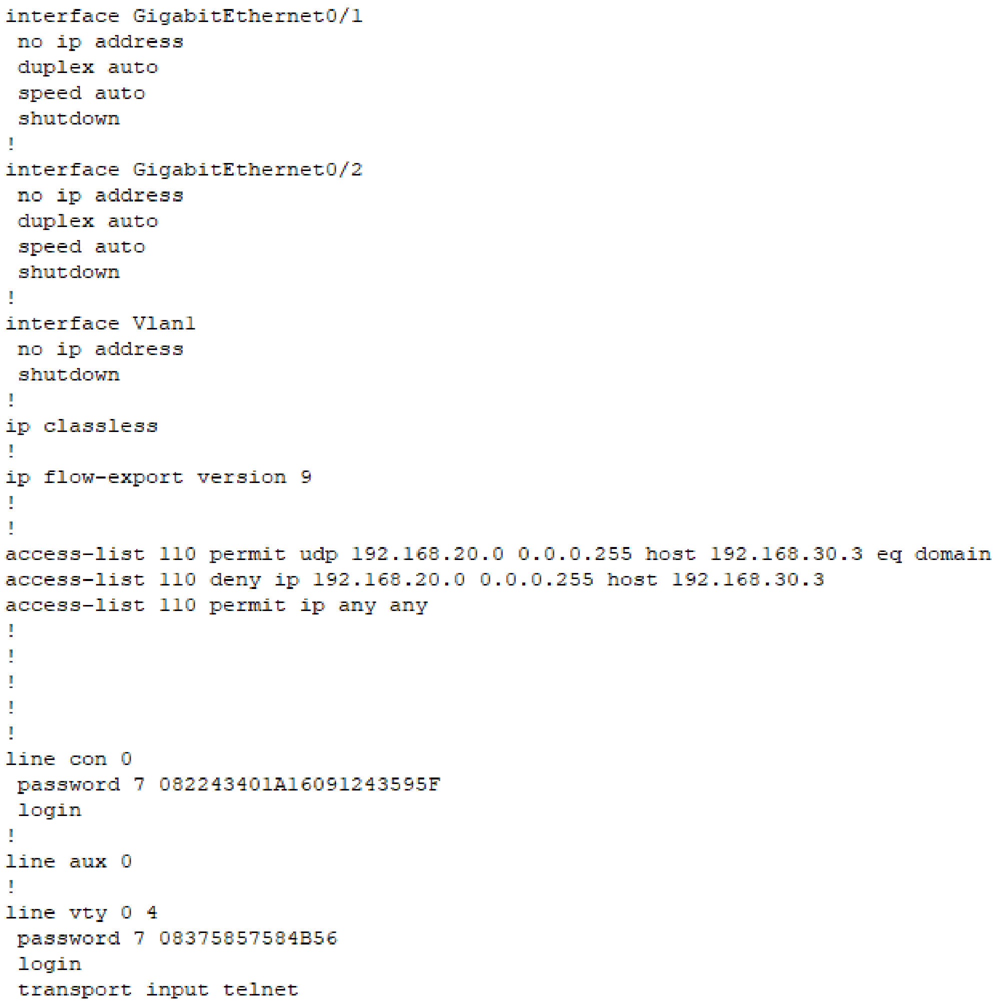
```
show ip interface g0/0.30
GigabitEthernet0/0.30 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 110
  Inbound  access list is not set
```



```
Router# show access-lists 110
Extended IP access list 110
    permit udp 192.168.20.0 0.0.0.255 host 192.168.30.3 eq domain (1 match(es))
    deny ip 192.168.20.0 0.0.0.255 host 192.168.30.3 (4 match(es))
    permit ip any any (5 match(es))
```



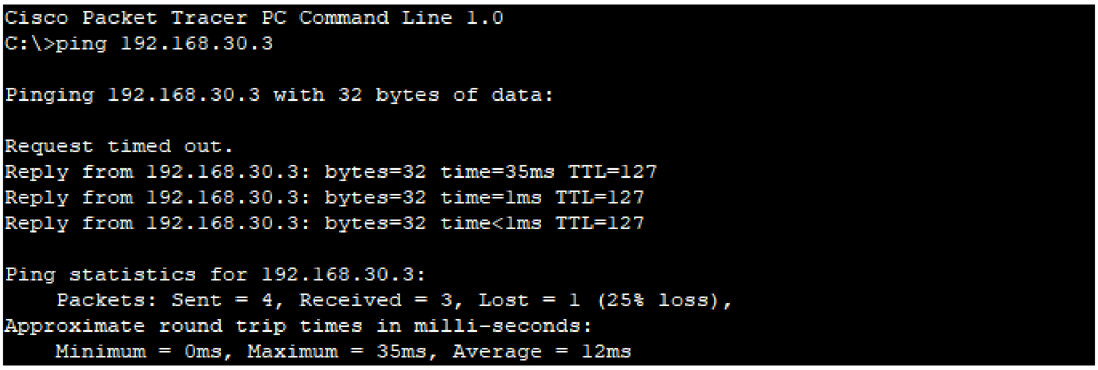
```
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret Coffeecorp@123
Router(config)#line console 0
Router(config-line)#password console123
Router(config-line)#login
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#password vty123
Router(config-line)#login
Router(config-line)#transport input telnet
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#end
Router#write memory
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
show running-config
Building configuration...

Current configuration : 1311 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$ztOnTjNHsOmMI7D9mnuAN.
!
```



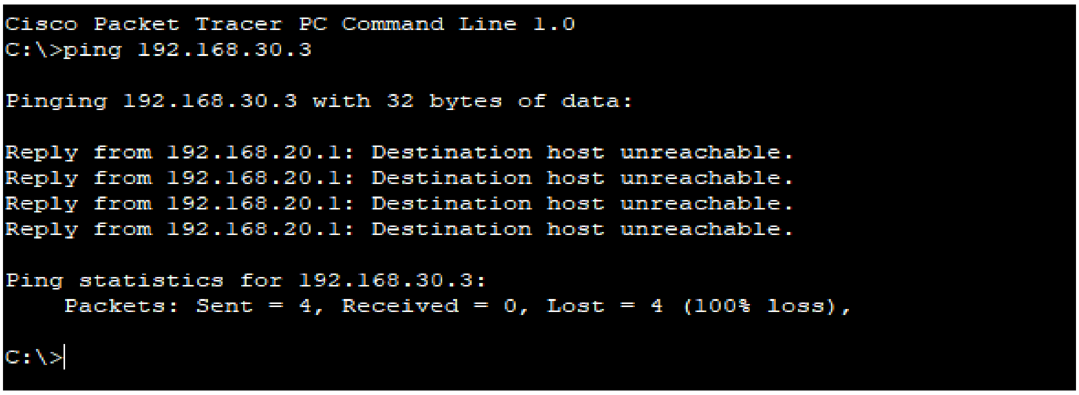
```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
access-list 110 permit udp 192.168.20.0 0.0.0.255 host 192.168.30.3 eq domain
access-list 110 deny ip 192.168.20.0 0.0.0.255 host 192.168.30.3
access-list 110 permit ip any any
!
!
!
!
!
line con 0
 password 7 082243401A16091243595F
 login
!
line aux 0
!
line vty 0 4
 password 7 08375857584B56
 login
 transport input telnet
```

I secured router management access by configuring an enable secret password and protecting console and VTY lines with authentication. I enabled password encryption was enabled to prevent plain-text password storage, ensuring only authorized personnel can manage the network infrastructure.

The network has been successfully secured using VLANs, ACLs, DNS, and router hardening. Testing confirmed that Sales can access sensitive resources while Finance is restricted appropriately.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.3: bytes=32 time=35ms TTL=127
Reply from 192.168.30.3: bytes=32 time=1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 35ms, Average = 12ms
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

The Sales PC successfully reaches the File Server, while the Finance PC experiences restricted access due to applied ACL rules.