MSc Cyber Security Engineering

Network Security (WM9PD)

Assessment Report

Submitted By:
Madhuchandra Sethunath
Msc Cyber Security Engineering
Submission Date: 10 October 2025

I hereby declare that this assessment is my own work and that all sources have been acknowledged.

2025-26

TABLE OF CONTENTS

Executive Summary

Critical sectors wield an influence so indomitable that, are they to be disrupted, our daily lives would be in shambles. Over the past decades, thousands of interruptions, from data breaches to state-sponsored cyberattacks, have amplified the need for strong barriers, response strategies, and well-defined rules in the digital sphere. These safeguards are vital for the continuity and data security within industries like BFSI, healthcare, and aerospace. This report explores the design and implementation of a secure network for DesX Zolutions Ltd., emphasizing departmental isolation, reliable service delivery, and scalable defences using Cisco Packet Tracer. This report details a secure network design for DesX Zolutions Ltd., supporting five departments with distinct access requirements. Using logical segmentation and subnetting, the solution enables efficient operations and strong data protection. Key implementations include secure routing, shared servers, AAA authentication, and zone-based firewalls. The network is tested and validated, ensuring reliable connectivity and access control. Scalability and future adaptability are also critically evaluated.

1. Network Planning and Design

1.1 Organisational and Segmentation Analysis

The DeskX network is structured to reflect a mid-sized organisation comprising several departments with distinct operational functions and security requirements. Network segmentation was implemented to logically separate these departments, ensuring controlled communication, improved performance, and enhanced security across the infrastructure.

Design, Project Management, HR, Finance, and IT departments operates within their own subnets. This logical separation limits broadcast domains and prevents unnecessary inter-departmental traffic. Access between departments is restricted and only permitted where business operations require it, following the principle of least privilege.

To reinforce the organisation's security posture, the network adopts a **zoned security model** consisting of an **Internal (trusted)** zone, a **DMZ (semi-trusted)** zone, and an **External (untrusted)** zone. The internal zone hosts all departmental networks, while the DMZ accommodates shared resources such as the email, web, and DHCP servers that must communicate with both internal users and external systems. The external zone represents the wider Internet and is tightly controlled by edge security mechanisms such as ACLs and firewall policies.

This zoning approach aligns with standard enterprise network security practices, providing a layered defence that isolates sensitive internal systems from external threats while still supporting essential connectivity and scalability for future organisational needs.

1.2 IP Addressing and Subnetting Scheme

The IP addressing and subnetting scheme assigns each department its own logically separated subnet. This structure isolates departmental traffic, supports the application of tailored security controls, and simplifies management and troubleshooting. Each subnet reserves the **first usable IP address** as the **default gateway** and the **final address** as the **broadcast address**. The design uses the private address space **192.168.10.0/24**, which is subdivided to match departmental size and trust boundaries.

Design Department Subnet

The Design department requires connectivity for 55 hosts. To determine the appropriate subnet size, the number of host bits required can be calculated using the host addressing formula:

$$2^h - 2 >= required\ hosts$$

where *h* is the number of host bits, and 2 addresses are reserved (one for the network and one for broadcast).

Substituting the required number of hosts:

$$2^h - 2 >= 55$$

$$2^6 - 2 >= 62$$

$$2^5 - 2 >= 30$$

Since 30 hosts (with 5 bits) is insufficient, 6 host bits are required. The subnet mask, therefore, uses 32 − 6 = 26 network bits, giving a prefix of /26.

- Subnet Address: 192.168.10.0/26
- Subnet Mask: 255.255.255.192
- Total Addresses: 2^6 = 64
- Usable Hosts: 64 − 2 = 62
- Usable Host Range: 192.168.10.1 – 192.168.10.62
- Default Gateway: 192.168.10.1
- Broadcast Address: 192.168.10.63

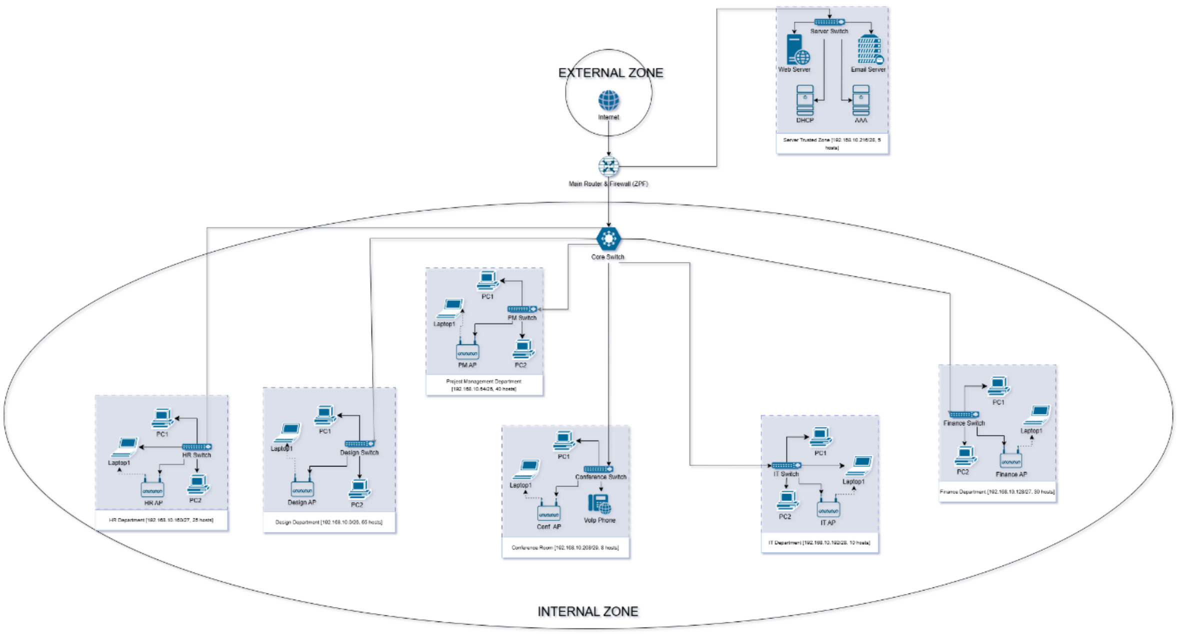
Thus Design department occupies the first block, leaving subsequent blocks available for other departments.

Subnet Name	Required Hosts	Usable Hosts	Network Address/CIDR	First Usable	Broadcast Address
Design	55	62	192.168.10.0 /26	192.168.10.1	192.168.10.63
Project Management	40	62	192.168.10.64 /26	192.168.10.65	192.168.10.127
Finance	30	30	192.168.10.128 /27	192.168.10.129	192.168.10.159
HR	25	30	192.168.10.160 /27	192.168.10.161	192.168.10.191
IT	10	14	192.168.10.192 /28	192.168.10.193	192.168.10.207
Conference	6	6	192.168.10.208 /29	192.168.10.209	192.168.10.215
Server Room	4	6	192.168.10.216 /29	192.168.10.217	192.168.10.223
Routers	2	2	192.168.10.224 /30	192.168.10.225	192.168.10.227

Table 1 - IP addressing and subnetting scheme

2.3 Proposed Physical Network Topology

The network employs a **hub-and-spoke topology** to balance scalability and security. All departmental switches connect to a central **distribution (core) router**, forming the **Internal (trusted) zone**. This router not only aggregates traffic but also **enforces access controls between departments**, ensuring that communication occurs only where explicitly permitted by organisational policy. The **server room** connects directly to the **edge router**, forming the **DMZ (semi-trusted) zone**, while the edge router manages all traffic between the internal networks, DMZ, and the **External zone** (Internet). This design provides **clear separation between zones**, controlled inter-departmental communication, and secure access to shared services while maintaining strict policy enforcement across all layers of the network.


EXTERNAL ZONE
Internet
Main Router & Firewall (ZPF)
Server Switch
Web Server
Email Server
DHCP
AAA
Server Trusted Zone [192.168.10.216/28, 5 hosts]
Core Switch
PC1
Laptop1
PM Switch
PM AP
PC2
Project Management Department [192.168.10.64/26, 40 hosts]
PC1
Laptop1
HR Switch
HR AP
PC2
HR Department [192.168.10.160/27, 25 hosts]
PC1
Laptop1
Design Switch
Design AP
PC2
Design Department [192.168.10.0/26, 65 hosts]
PC1
Laptop1
Conference Switch
Conf AP
Volp Phone
Conference Room [192.168.10.208/29, 8 hosts]
PC1
IT Switch
Laptop1
PC2
IT AP
IT Department [192.168.10.192/28, 10 hosts]
PC1
Finance Switch
Laptop1
PC2
Finance AP
Finance Department [192.168.10.128/27, 30 hosts]
INTERNAL ZONE

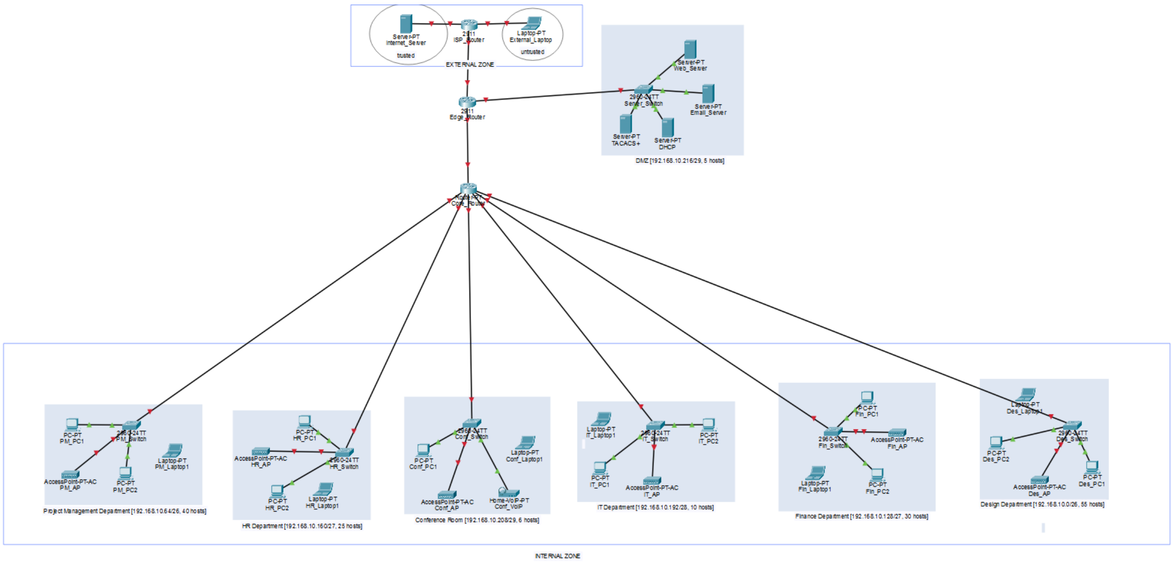
Physical Network Topology – DesX Zolutions Ltd.

2. Network Implementation and Configuration

2.1 Placement and Physical Setup

For deployment in Cisco Packet Tracer, devices were chosen to reflect enterprise standards while accommodating simulation limitations:

- **2911 Router:** Enterprise-grade router supporting OSPF, DHCP relay, ACLs, and ZPF; used as the main ISP/edge router.
- **Router-PT:** Distribution router to expand available interfaces for departmental connections; no routing or security configuration applied.
- **2960-24TT Switches:** Standard access switches for each department; provide sufficient ports, support security features, and emulate real-world enterprise access switches.
- **AccessPoint-PT-AC:** Wireless access points supporting WPA2, representing typical enterprise wireless deployments.



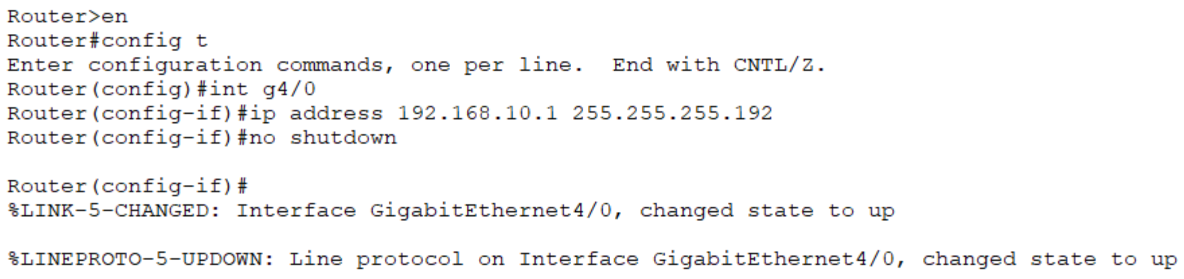
Screenshot showing physical layout in tracer

2.2 Interface Configuration

To ensure proper subnet segmentation and controlled inter-departmental communication, each core router interface was assigned a unique IP address, corresponding to the first usable host address of its respective subnet. These addresses serve as the **default gateways** for all hosts within the subnet, directing traffic through the router for communication outside the local department. By assigning interfaces in this way, the core router can effectively enforce access policies between departments, route traffic only where permitted, and maintain clear boundaries between internal zones, supporting both security and operational efficiency.

Core Router interface	First Usable Address/CIDR Mask	Dotted-Decimal Subnet Mask
G4/0	192.168.10.1/26	255.255.255.192
G6/0	192.168.10.65/26	255.255.255.192
G5/0	192.168.10.129/27	255.255.255.224
G3/0	192.168.10.161/27	255.255.255.224
G2/0	192.168.10.193/28	255.255.255.240
G8/0	192.168.10.209/29	255.255.255.248

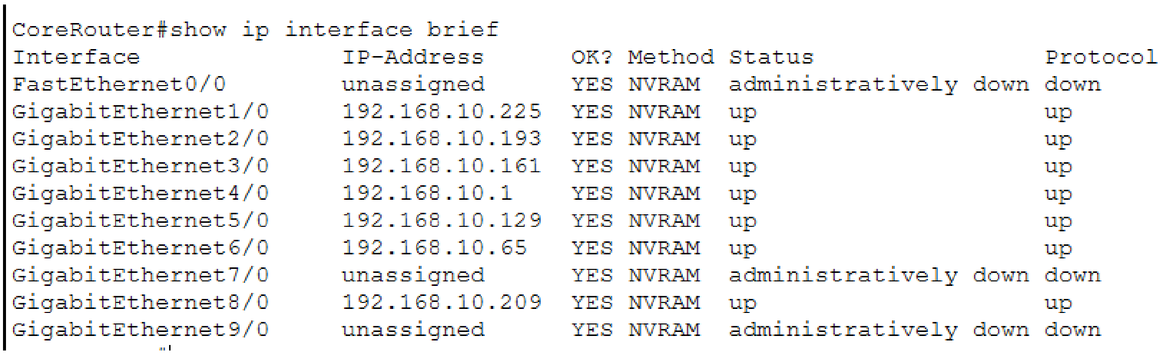
Table 2 - Interface assignments in the core router



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g4/0
Router(config-if)#ip address 192.168.10.1 255.255.255.192
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet4/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/0, changed state to up
```

Assigning the first usable address in Design Subnet to g4/0

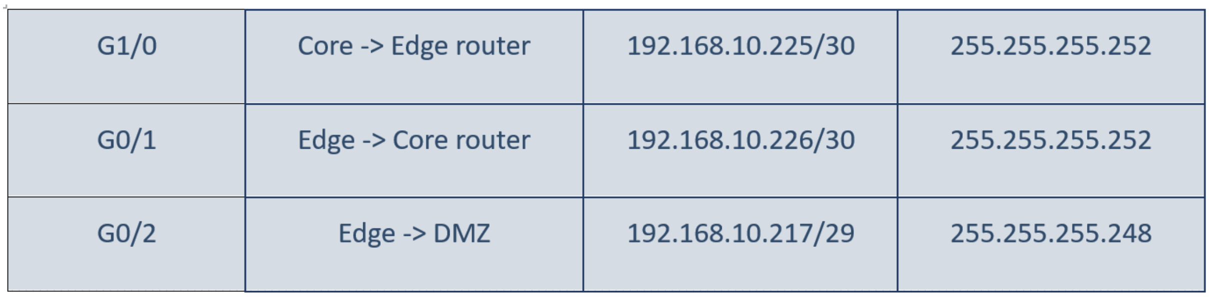
The remaining subnets were assigned to their respective core router interfaces per the addressing plan.



```
CoreRouter#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0     192.168.10.225  YES NVRAM  up                    up
GigabitEthernet2/0     192.168.10.193  YES NVRAM  up                    up
GigabitEthernet3/0     192.168.10.161  YES NVRAM  up                    up
GigabitEthernet4/0     192.168.10.1    YES NVRAM  up                    up
GigabitEthernet5/0     192.168.10.129  YES NVRAM  up                    up
GigabitEthernet6/0     192.168.10.65   YES NVRAM  up                    up
GigabitEthernet7/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet8/0     192.168.10.209  YES NVRAM  up                    up
GigabitEthernet9/0     unassigned      YES NVRAM  administratively down down
```

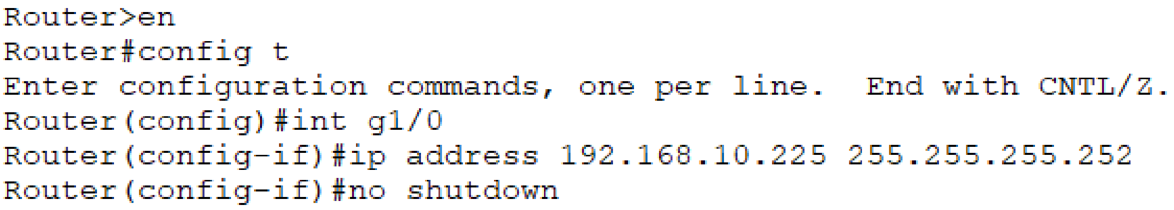
show ip brief

Since the broadcast address of the last subnet (Server Room) is 192.168.10.223/29, the point-to-point link between the core and edge routers was assigned IP addresses from the next available subnet segment.



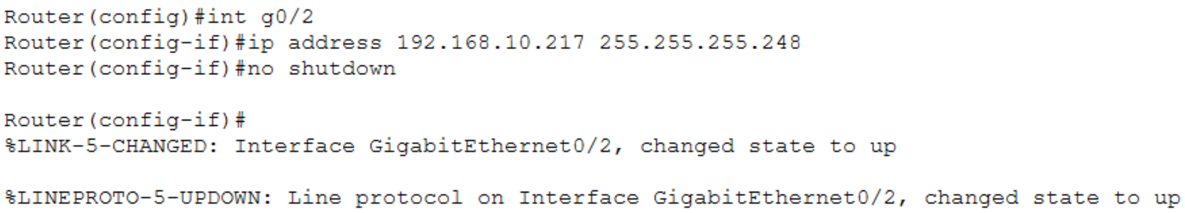
G1/0	Core -> Edge router	192.168.10.225/30	255.255.255.252
G0/1	Edge -> Core router	192.168.10.226/30	255.255.255.252
G0/2	Edge -> DMZ	192.168.10.217/29	255.255.255.248

Table 3 - Router Interface assignment



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g1/0
Router(config-if)#ip address 192.168.10.225 255.255.255.252
Router(config-if)#no shutdown
```

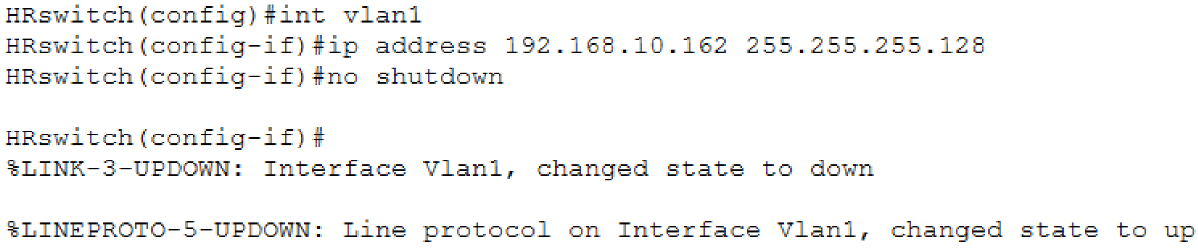
IP assignment of core to edge



```
Router(config)#int g0/2
Router(config-if)#ip address 192.168.10.217 255.255.255.248
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
```

Edge router to DMZ

VLAN 1 on each switch was assigned a subnet IP for management.



```
HRswitch(config)#int vlan1
HRswitch(config-if)#ip address 192.168.10.162 255.255.255.128
HRswitch(config-if)#no shutdown

HRswitch(config-if)#
%LINK-3-UPDOWN: Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

VLAN in switch

2.3 Dynamic Routing using OSPF

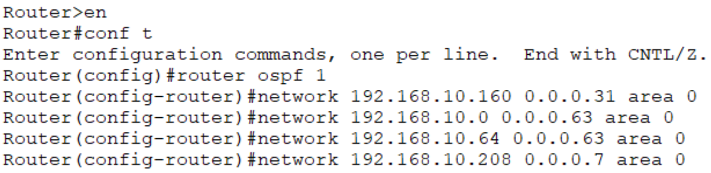
To enable efficient inter-department communication and support network scalability, Open Shortest Path First (OSPF) was implemented as the network's dynamic routing protocol. OSPF was selected over legacy protocols such as RIP due to its faster convergence, support for variable-length subnet masking, and improved stability in segmented environments.

Both routers operate within OSPF Area 0 (backbone area). The core router advertises all directly connected subnets, enabling dynamic route exchange and full internal connectivity, while the edge router uses a single network statement for the transit subnet linking it to the core and another for the DMZ.

OSPF Configuration Summary:

Process ID: 1 (both routers)

Core Router: Network statements for each directly connected subnet in Area 0

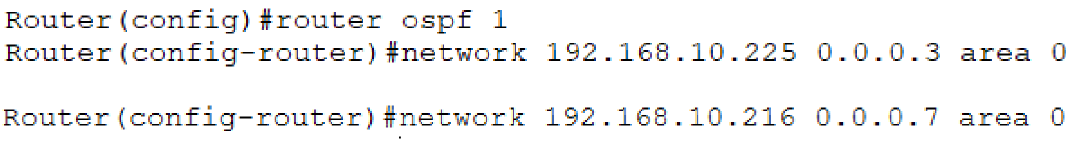


```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.10.160 0.0.0.31 area 0
Router(config-router)#network 192.168.10.0 0.0.0.63 area 0
Router(config-router)#network 192.168.10.64 0.0.0.63 area 0
Router(config-router)#network 192.168.10.208 0.0.0.7 area 0
```

OSPF configuration on core router

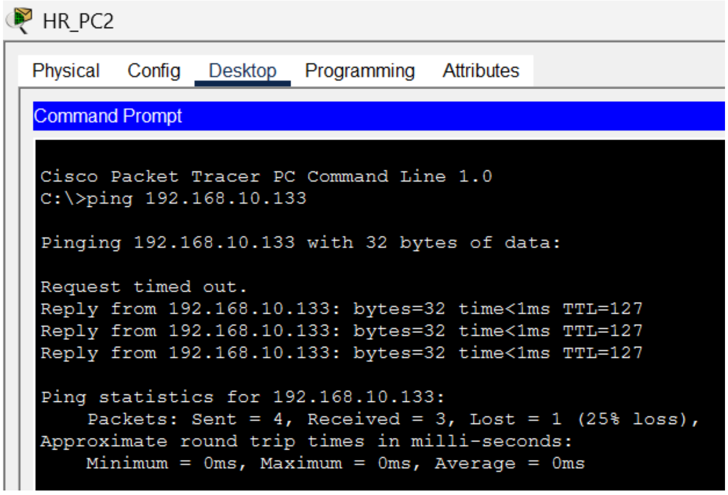
Edge Router: Network statements for the transit link and DMZ

This configuration ensures automatic route propagation, maintains efficient traffic paths between departments, and supports network expansion without manual route updates.



```
Router(config)#router ospf 1
Router(config-router)#network 192.168.10.225 0.0.0.3 area 0

Router(config-router)#network 192.168.10.216 0.0.0.7 area 0
```

OSPF on edge

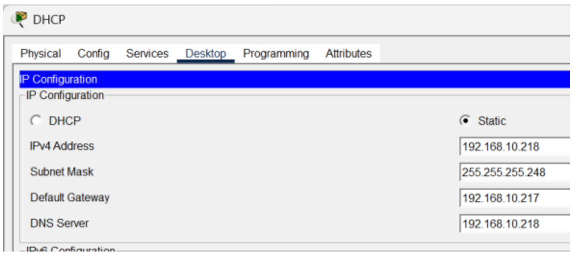


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.133

Pinging 192.168.10.133 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.133: bytes=32 time<1ms TTL=127
Reply from 192.168.10.133: bytes=32 time<1ms TTL=127
Reply from 192.168.10.133: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.133:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Successful ping between clients

2.4 DHCP Server

To automate IP assignment and reduce manual configuration errors, a **centralized DHCP server** was deployed in the server subnet, using the first usable IP after the gateway.



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.10.218

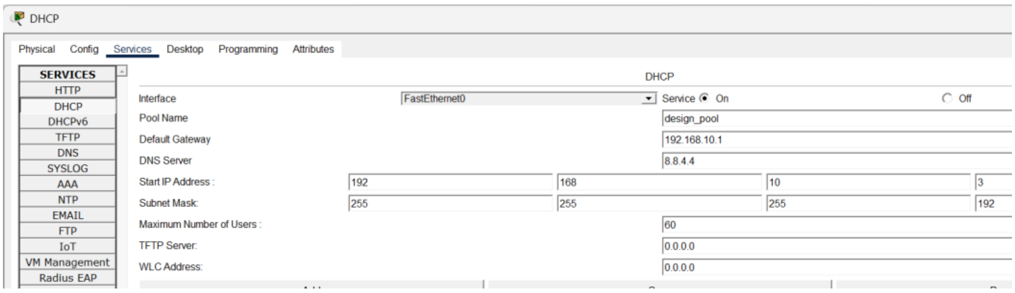
Subnet Mask: 255.255.255.248

Default Gateway: 192.168.10.217

DNS Server: 192.168.10.218

IP configuration of DHCP server

Separate **DHCP pools** were created for each departmental subnet to ensure correct address allocation, subnet masking, and gateway assignment within their respective zones.



DHCP

Interface: FastEthernet0 — Service ● On ○ Off

Pool Name: design_pool

Default Gateway: 192.168.10.1

DNS Server: 8.8.4.4

Start IP Address : 192 168 10 3

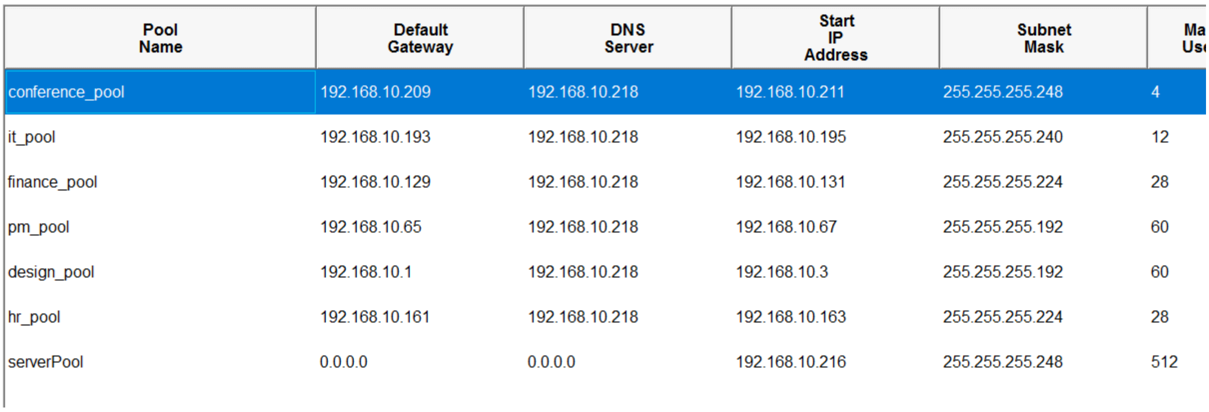
Subnet Mask: 255 255 255 192

Maximum Number of Users : 60

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

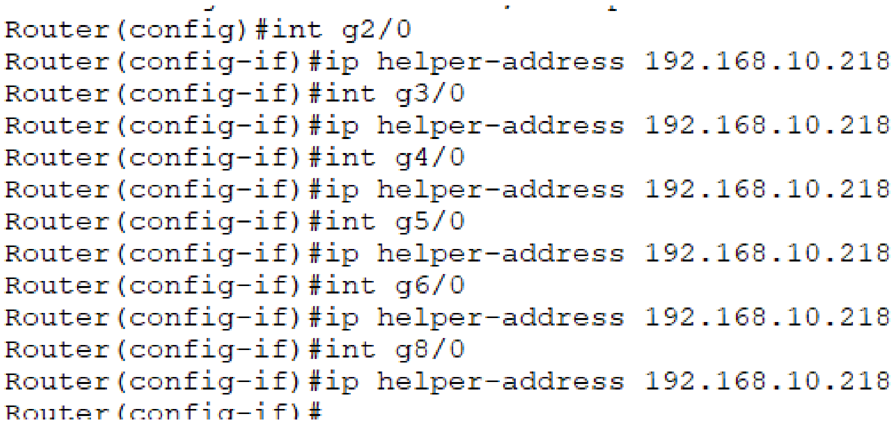
DHCP Pool for Design Subnet



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Ma Us
conference_pool	192.168.10.209	192.168.10.218	192.168.10.211	255.255.255.248	4
it_pool	192.168.10.193	192.168.10.218	192.168.10.195	255.255.255.240	12
finance_pool	192.168.10.129	192.168.10.218	192.168.10.131	255.255.255.224	28
pm_pool	192.168.10.65	192.168.10.218	192.168.10.67	255.255.255.192	60
design_pool	192.168.10.1	192.168.10.218	192.168.10.3	255.255.255.192	60
hr_pool	192.168.10.161	192.168.10.218	192.168.10.163	255.255.255.224	28
serverPool	0.0.0.0	0.0.0.0	192.168.10.216	255.255.255.248	512

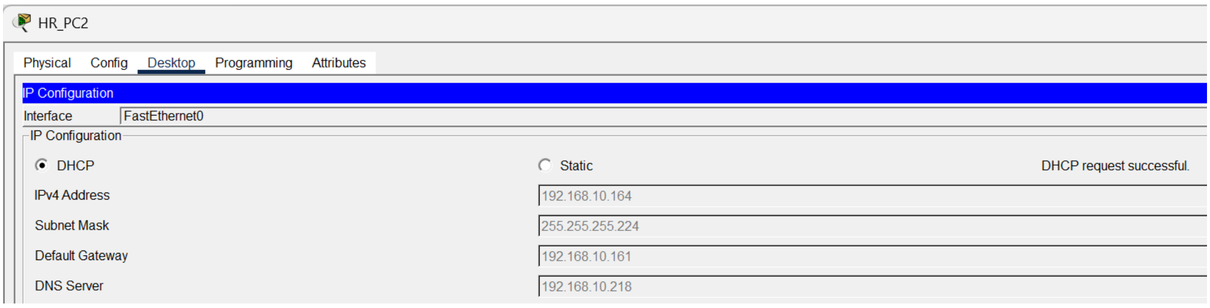
List of all pools

Router interfaces for each subnet were configured with the **ip helper-address** command to forward DHCP requests to the server, ensuring seamless address provisioning across all zones. This ensures all devices receive correct IP configuration automatically, supporting network scalability and ease of management.



```
Router(config)#int g2/0
Router(config-if)#ip helper-address 192.168.10.218
Router(config-if)#int g3/0
Router(config-if)#ip helper-address 192.168.10.218
Router(config-if)#int g4/0
Router(config-if)#ip helper-address 192.168.10.218
Router(config-if)#int g5/0
Router(config-if)#ip helper-address 192.168.10.218
Router(config-if)#int g6/0
Router(config-if)#ip helper-address 192.168.10.218
Router(config-if)#int g8/0
Router(config-if)#ip helper-address 192.168.10.218
Router(config-if)#
```

Helper address



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

DHCP request successful.

IPv4 Address: 192.168.10.164

Subnet Mask: 255.255.255.224

Default Gateway: 192.168.10.161

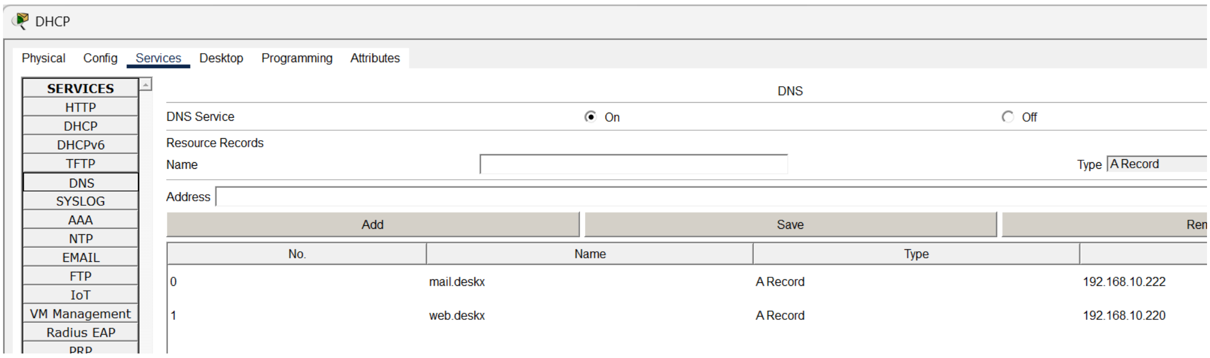
DNS Server: 192.168.10.218

Successful DHCP Request

2.5 Server Room Services: Web and Email Server Configuration

The Server Room hosts multiple shared resources including Web, Email, DHCP, and AAA servers.

The DNS service is configured in DHCP server itself, allowing it to provide local name resolution. The DNS configuration was included within the setup so that all clients automatically receive name resolution settings along with their IP addresses. To enable clients to access servers using domain names, **DNS records** were created with hostnames mapped to their respective IP addresses.



DNS

DNS Service ● On ○ Off

Resource Records

Name

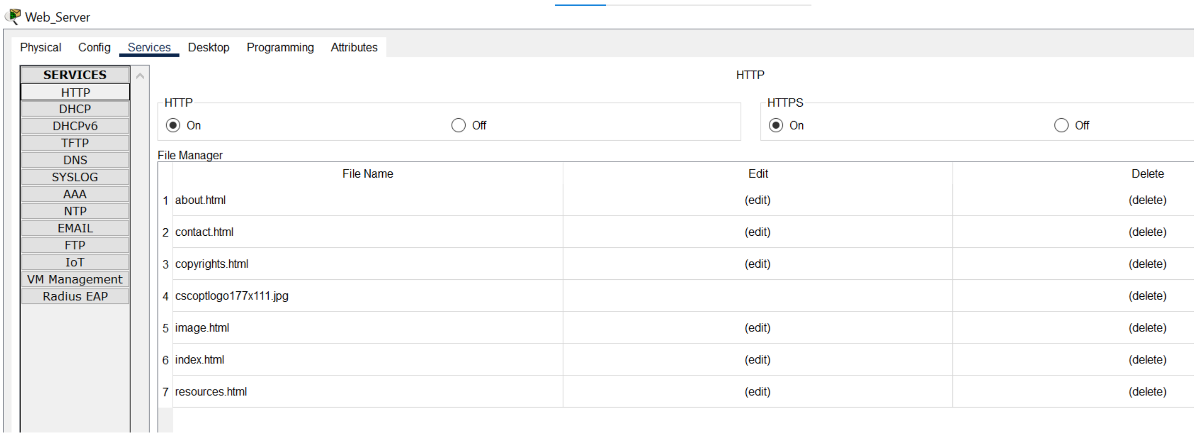
Type A Record

Address

No.	Name	Type	
0	mail.deskx	A Record	192.168.10.222
1	web.deskx	A Record	192.168.10.220

DNS Records

To provide internal web services, a **Web Server** was configured to host multiple HTML pages under the **DeskX portal**. This setup allows users across departments to easily access shared resources and internal tools via a unified web interface.



HTTP

HTTP ● On ○ Off

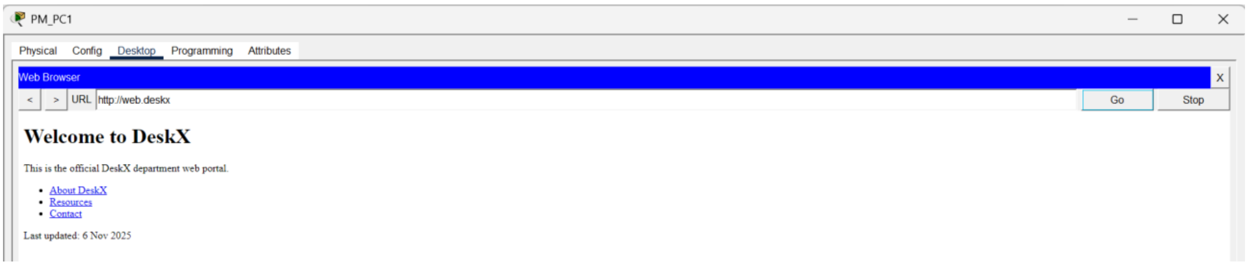
HTTPS ● On ○ Off

File Manager

	File Name	Edit	Delete
1	about.html	(edit)	(delete)
2	contact.html	(edit)	(delete)
3	copyrights.html	(edit)	(delete)
4	cscoptlogo177x111.jpg		(delete)
5	image.html	(edit)	(delete)
6	index.html	(edit)	(delete)
7	resources.html	(edit)	(delete)

Web page setup

Verification was performed by accessing the DeskX portal from a client system, confirming that the web service was fully operational.



URL http://web.deskx

Welcome to DeskX

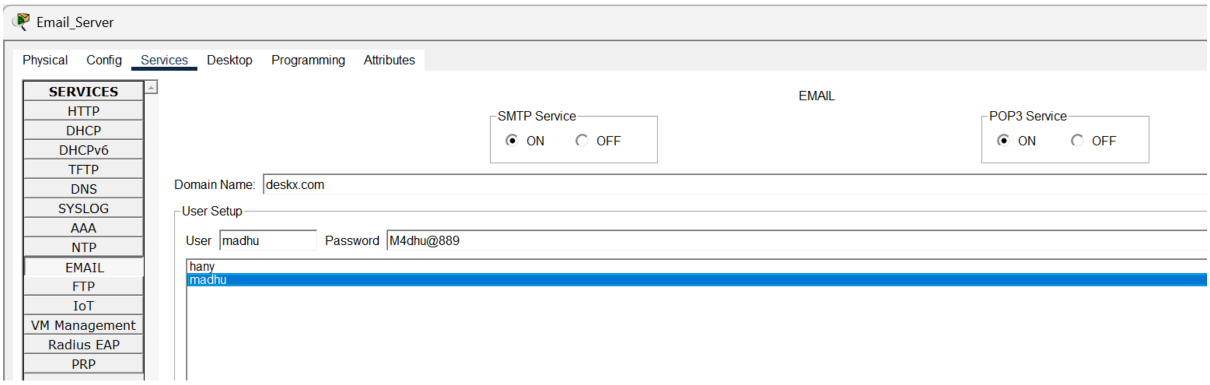
This is the official DeskX department web portal.

- About DeskX
- Resources
- Contact

Last updated: 6 Nov 2025

Successful web portal access

To provide internal email services, **SMTP and POP3** were enabled on the Email Server, allowing users to send and receive messages using addresses in the format **[username]@deskx.com**. Secure passwords were configured for each account to restrict access and maintain confidentiality.



EMAIL

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: deskx.com

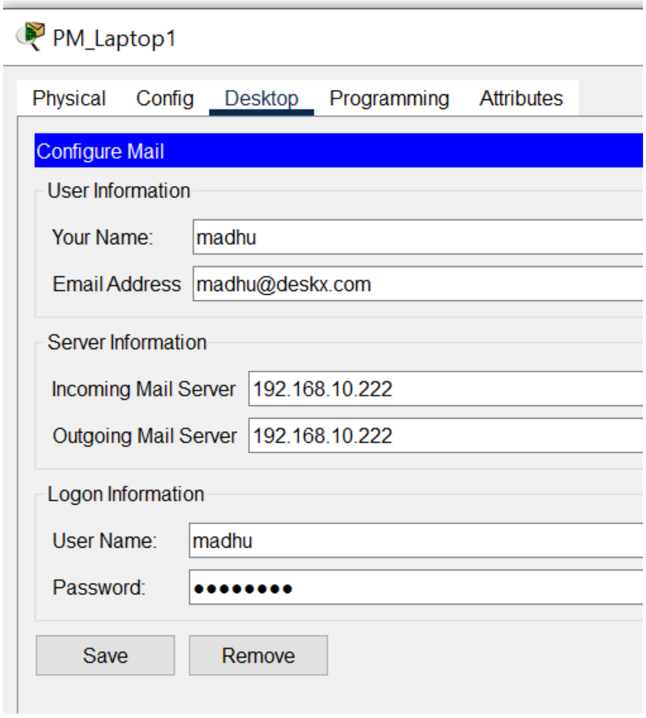
User Setup

User madhu Password M4dhu@889

hany
madhu

User setup and domain settings on the email server.

For example, when a Project Management user sends an email to a Finance user, **individual email accounts** must be created on each client device as illustrated below.



User Information

Your Name: madhu

Email Address madhu@deskx.com

Server Information

Incoming Mail Server 192.168.10.222

Outgoing Mail Server 192.168.10.222

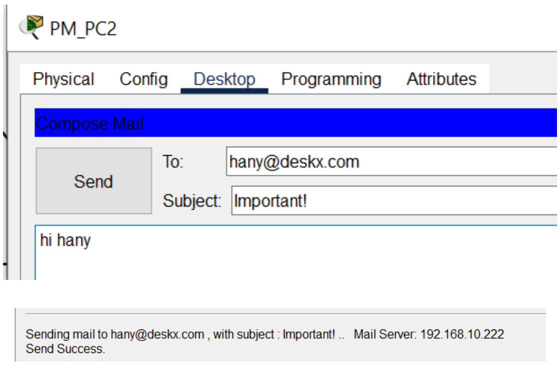
Logon Information

User Name: madhu

Password: ••••••••

Email account creation

An email was composed and sent from a **Project Management subnet** account to verify internal email functionality.



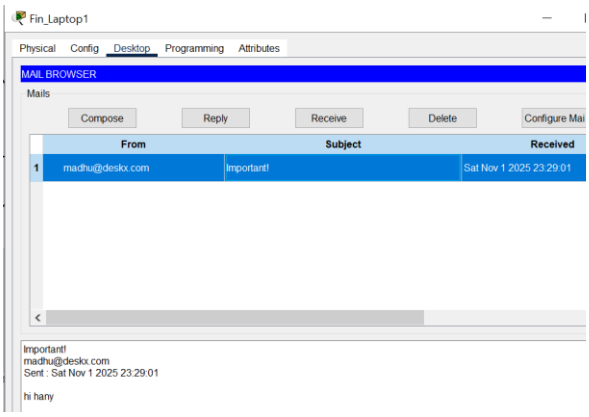
To: hany@deskx.com

Subject: Important!

hi hany

Sending mail to hany@deskx.com , with subject : Important! .. Mail Server: 192.168.10.222
Send Success.

Email sent successfully



	From	Subject	Received
1	madhu@deskx.com	Important!	Sat Nov 1 2025 23:29:01

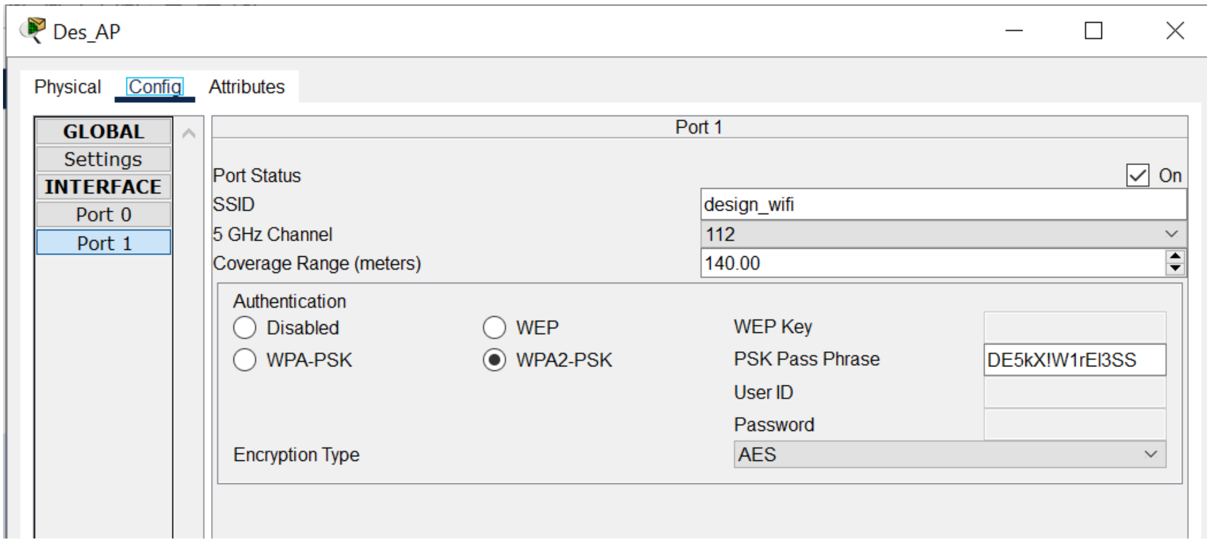
Important!
madhu@deskx.com
Sent : Sat Nov 1 2025 23:29:01

hi hany

Email received successfully

2.6 Wireless Access Point

Each department was provided with a dedicated wireless access point to support mobility and flexible client connectivity. For the highest level of security available in Packet Tracer, WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key) was selected as the authentication method, with a unique, strong passphrase configured on each AP.



Port 1

Port Status ☑ On

SSID: design_wifi

5 GHz Channel: 112

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP
○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: DE5kX!W1rEI3SS

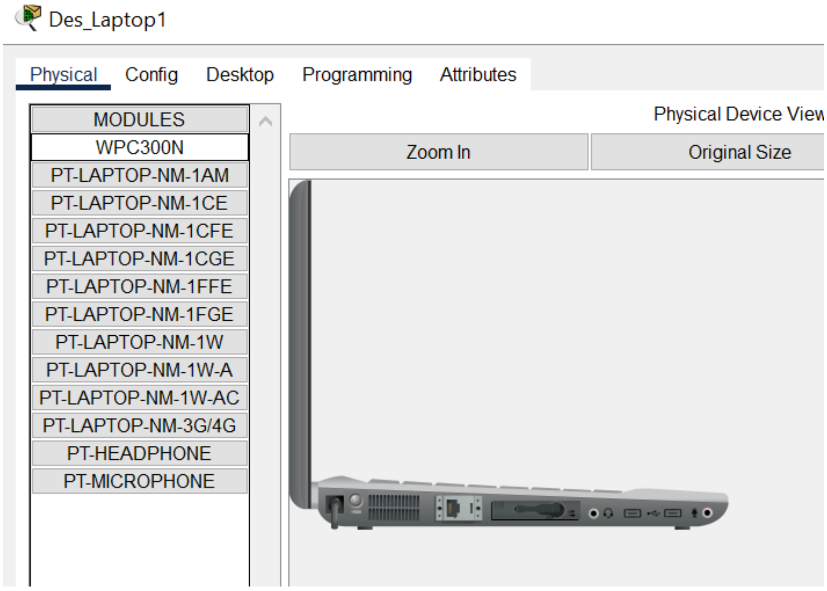
User ID:

Password:

Encryption Type: AES

WAP config

To enable wireless connectivity, a **WPC300N module** was installed in the laptop's expansion slot.

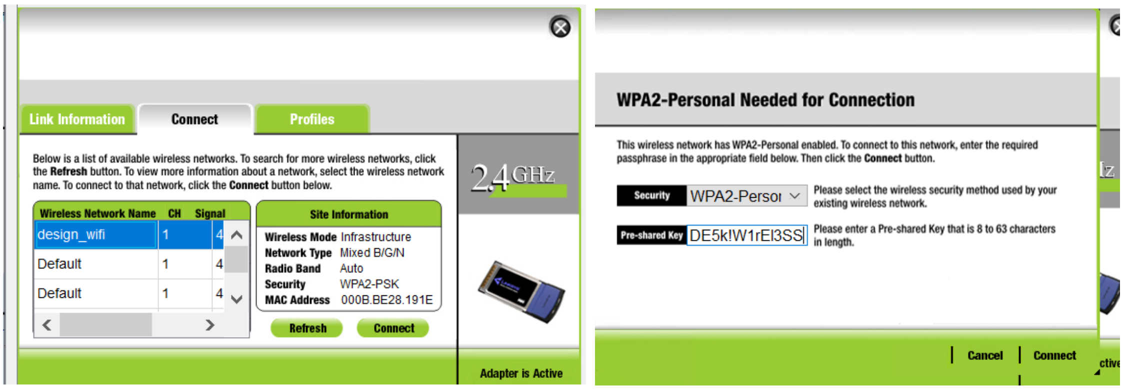


Des_Laptop1

Physical | Config | Desktop | Programming | Attributes

MODULES
- WPC300N
- PT-LAPTOP-NM-1AM
- PT-LAPTOP-NM-1CE
- PT-LAPTOP-NM-1CFE
- PT-LAPTOP-NM-1CGE
- PT-LAPTOP-NM-1FFE
- PT-LAPTOP-NM-1FGE
- PT-LAPTOP-NM-1W
- PT-LAPTOP-NM-1W-A
- PT-LAPTOP-NM-1W-AC
- PT-LAPTOP-NM-3G/4G
- PT-HEADPHONE
- PT-MICROPHONE

WPC300N added to laptop



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
design_wifi	1	4
Default	1	4
Default	1	4

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA2-PSK
MAC Address	000B.BE28.191E

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

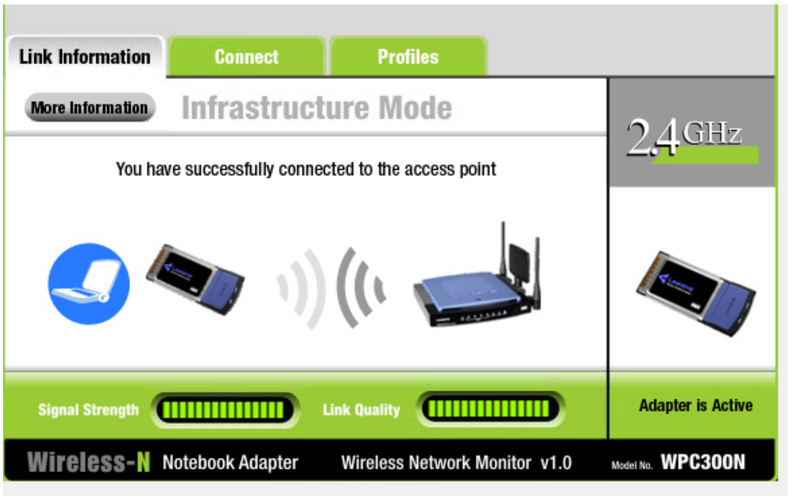
Security: WPA2-Persor

Please select the wireless security method used by your existing wireless network.

Pre-shared Key: DE5k!W1rEI3SS

Please enter a Pre-shared Key that is 8 to 63 characters in length.

Connecting to wifi using credentials



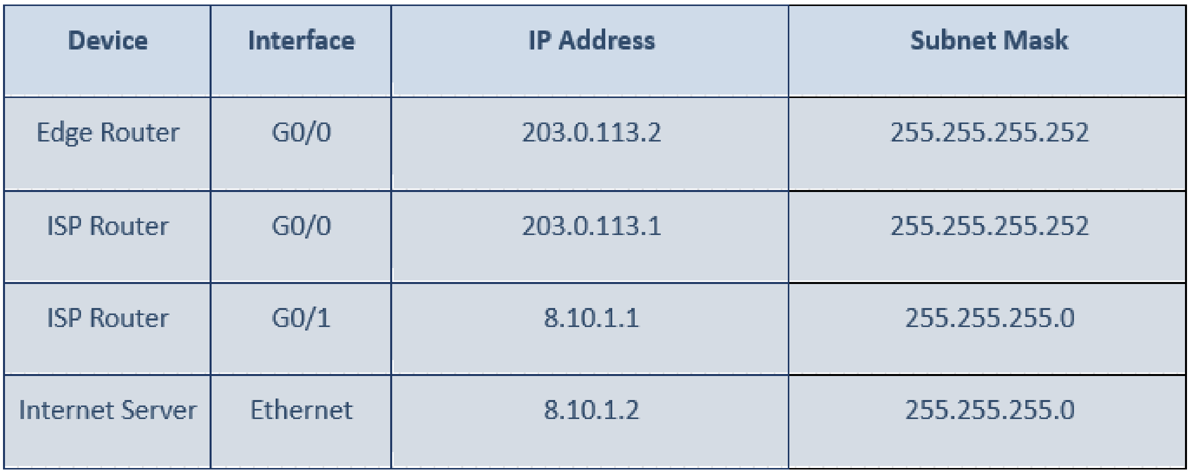
You have successfully connected to the access point

Wifi access successful

WPA2 was chosen over legacy protocols (such as WEP or open authentication) because it uses robust AES encryption, making unauthorized access or password cracking significantly more difficult. This ensures that only users who know the department-specific passphrase can join the wireless network, mitigating risks such as eavesdropping or rogue access. The network SSIDs were named according to their respective department zones (e.g., “design_wifi”), and all clients were successfully connected by entering the correct WPA2 credentials. This setup fulfills the security requirement by restricting wireless access to authorized users only.

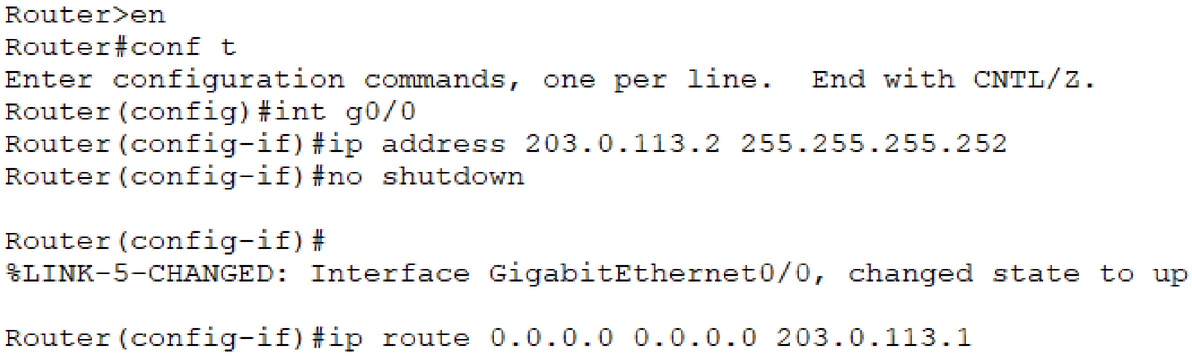
2.7 Internet Connectivity

To enable seamless connectivity within the network and with external resources, the edge router connects to an ISP router using a public IP subnet, simulating an Internet connection. An Internet server is attached to the ISP router to represent external web resources for NAT and outbound connectivity testing. Additionally, a PC is connected to the ISP router to simulate an untrusted external host. This layout ensures reliable intra-organization communication while supporting secure access to Internet-facing services and realistic testing of external threats.



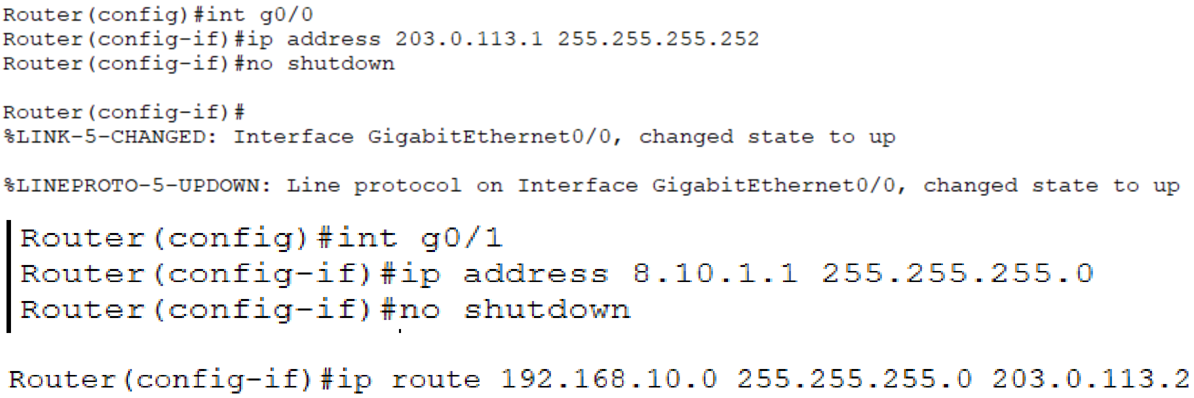
Device	Interface	IP Address	Subnet Mask
Edge Router	G0/0	203.0.113.2	255.255.255.252
ISP Router	G0/0	203.0.113.1	255.255.255.252
ISP Router	G0/1	8.10.1.1	255.255.255.0
Internet Server	Ethernet	8.10.1.2	255.255.255.0

Table 4 - Interface assignment for ISP and Internet Server



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 203.0.113.2 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#ip route 0.0.0.0 0.0.0.0 203.0.113.1
```

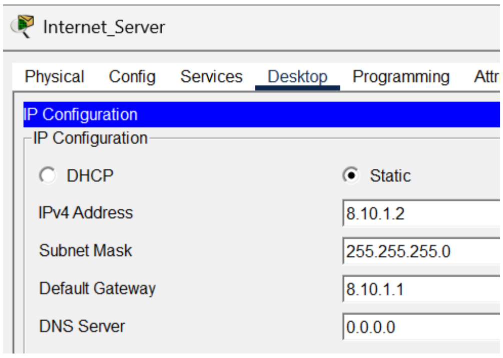
Interface config and default routing for ISP in edge router



```
Router(config)#int g0/0
Router(config-if)#ip address 203.0.113.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

```
Router(config)#int g0/1
Router(config-if)#ip address 8.10.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#ip route 192.168.10.0 255.255.255.0 203.0.113.2
```

Interface config and default routing inside ISP router



IP Configuration

IP Configuration

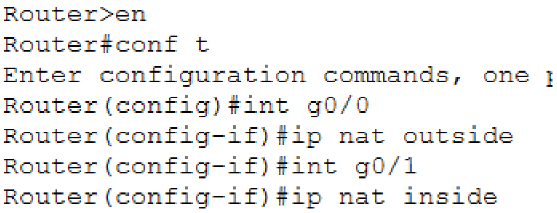
○ DHCP ● Static

IPv4 Address	8.10.1.2
Subnet Mask	255.255.255.0
Default Gateway	8.10.1.1
DNS Server	0.0.0.0

Setting up gateway and static ip in internet server

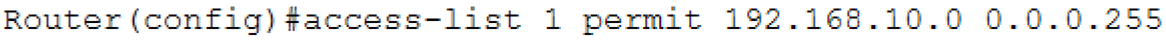
To enable secure and efficient Internet connectivity, **Network Address Translation (NAT)** was implemented on the edge router connecting internal departmental subnets to the ISP segment. NAT allows devices using private address spaces (such as 192.168.10.0/24) to communicate with the external public network by translating their IP addresses to the router's public-facing address.

PAT (Port Address Translation) with NAT Overload was chosen to allow multiple clients to share a single public IP, conserving global address space while maintaining full outbound access. The router's interfaces were designated as follows: the LAN port configured as 'inside' and the ISP port as 'outside'. An access list specified which internal addresses should be translated.



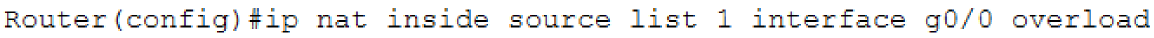
```
Router>en
Router#conf t
Enter configuration commands, one
Router(config)#int g0/0
Router(config-if)#ip nat outside
Router(config-if)#int g0/1
Router(config-if)#ip nat inside
```

Defined 'inside' and 'outside' in edge router



```
Router(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

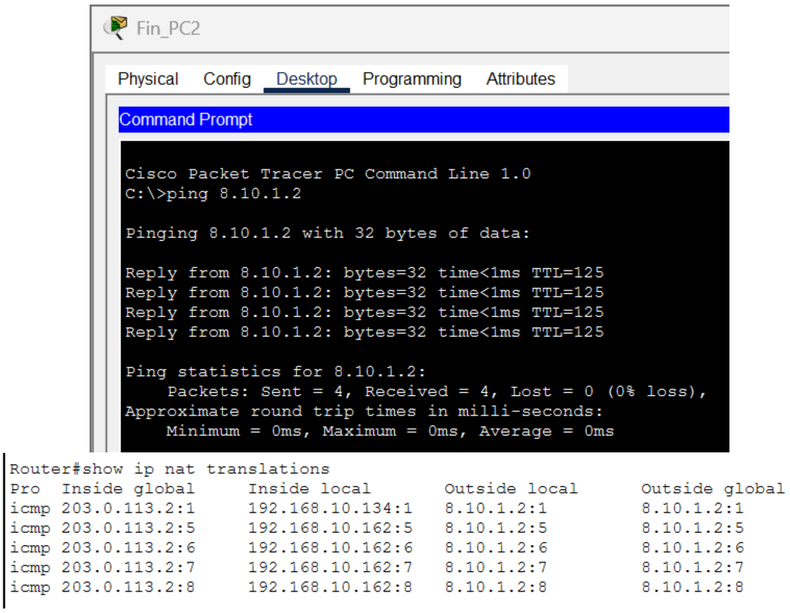
ACL that matches all internal devices in the network



```
Router(config)#ip nat inside source list 1 interface g0/0 overload
```

NAT overload to translate and forward traffic to the internet

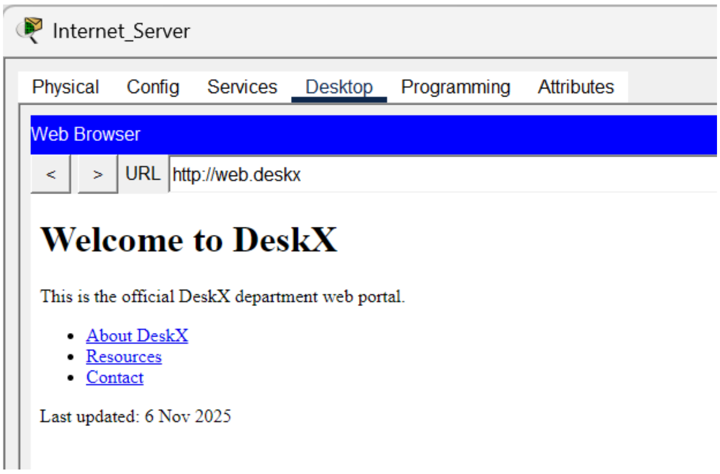
Connectivity was verified using ping and web tests from clients to simulated Internet hosts. This setup ensures privacy and security for internal devices while retaining Internet functionality.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.10.1.2

Pinging 8.10.1.2 with 32 bytes of data:

Reply from 8.10.1.2: bytes=32 time<1ms TTL=125
Reply from 8.10.1.2: bytes=32 time<1ms TTL=125
Reply from 8.10.1.2: bytes=32 time<1ms TTL=125
Reply from 8.10.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 8.10.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.0.113.2:1     192.168.10.134:1   8.10.1.2:1         8.10.1.2:1
icmp 203.0.113.2:5     192.168.10.162:5   8.10.1.2:5         8.10.1.2:5
icmp 203.0.113.2:6     192.168.10.162:6   8.10.1.2:6         8.10.1.2:6
icmp 203.0.113.2:7     192.168.10.162:7   8.10.1.2:7         8.10.1.2:7
icmp 203.0.113.2:8     192.168.10.162:8   8.10.1.2:8         8.10.1.2:8
```

Verification of Internet connectivity for internal clients using ICMP ping, with NAT translation table on Edge router confirming successful address translation for outbound traffic.



http://web.deskx

Welcome to DeskX

This is the official DeskX department web portal.

- About DeskX
- Resources
- Contact

Last updated: 6 Nov 2025

Accessing web from internet server

3. Security Controls and Access Policies

3.1 Basic Device Security Configuration

Configuring baseline security on every network devices, such as routers and managed switches, is essential to protect both the integrity and the manageability of the entire enterprise network. This process was performed on both the core (R2) and edge (R1) routers, as well as on each departmental switch in the network. I worked through the following standard template, ensuring consistent security parameters across the infrastructure.

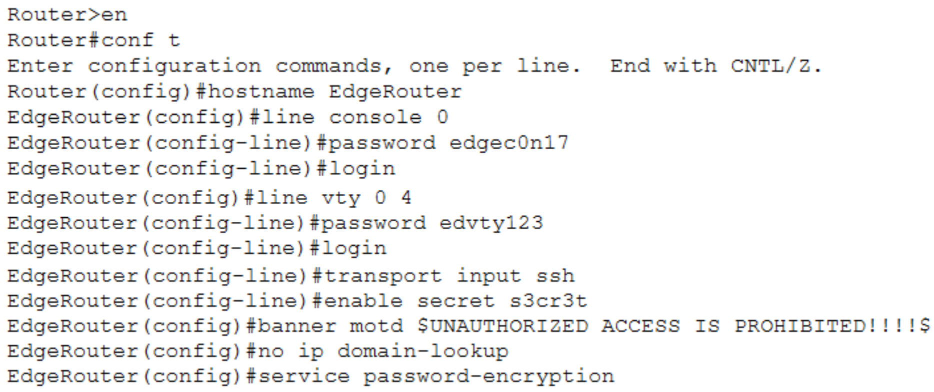
Unique, descriptive **hostname** for identification and network management.

Console, vty (remote access), and privileged EXEC (enable) passwords were established to control administrative access.

An **MOTD (Message of the Day) banner** was configured to provide a security warning, deterring unauthorized access.

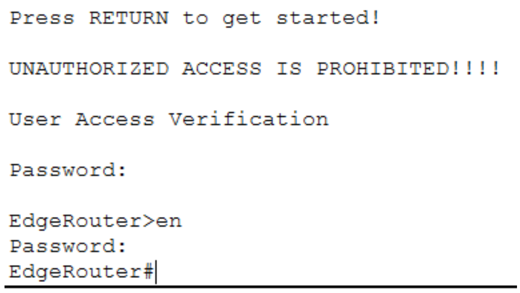
All plaintext passwords were **encrypted** using the built-in password encryption service for enhanced security.

The **no ip domain-lookup** command was used to prevent accidental delays caused by mistyped commands being interpreted as DNS queries.



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname EdgeRouter
EdgeRouter(config)#line console 0
EdgeRouter(config-line)#password edgec0n17
EdgeRouter(config-line)#login
EdgeRouter(config)#line vty 0 4
EdgeRouter(config-line)#password edvty123
EdgeRouter(config-line)#login
EdgeRouter(config-line)#transport input ssh
EdgeRouter(config-line)#enable secret s3cr3t
EdgeRouter(config)#banner motd $UNAUTHORIZED ACCESS IS PROHIBITED!!!!$
EdgeRouter(config)#no ip domain-lookup
EdgeRouter(config)#service password-encryption
```

Device security hardening in Edge Router



```
Press RETURN to get started!

UNAUTHORIZED ACCESS IS PROHIBITED!!!!

User Access Verification

Password:

EdgeRouter>en
Password:
EdgeRouter#
```

Password verification

Console line	c0n50le
VTY line	vty123
Enable Secret	s3cr3t

Table 5 - Passwords for Edge Router

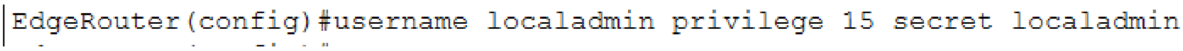
The same was implemented for Core and ISP Routers as well as every departmental switches.

Console line	edgec0n17
VTY line	edvty1
Enable Secret	s3cr3t

Table 6 - Passwords for Core, ISP Routers and all switches

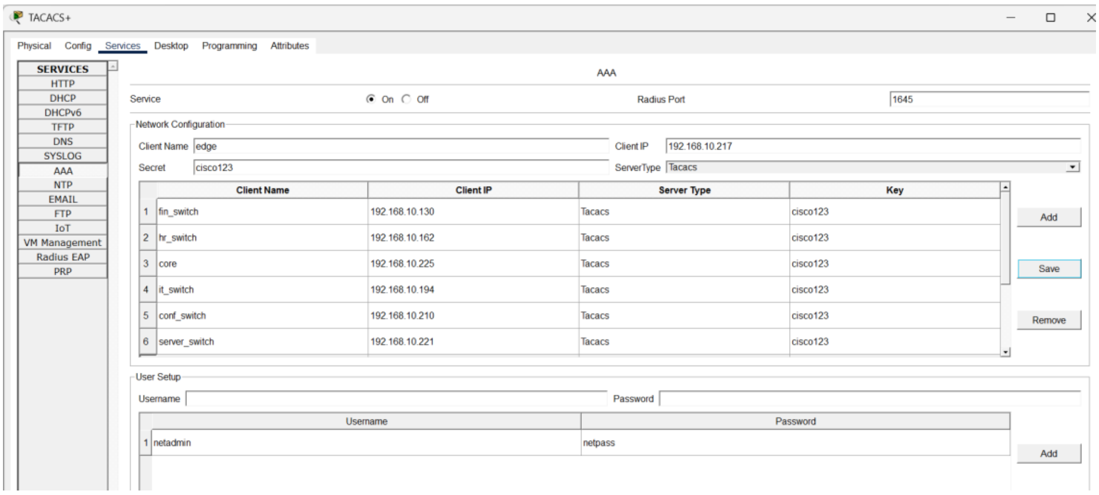
3.2 AAA

To ensure secure access control and administrative manageability, robust AAA practices were implemented throughout the network. As a foundational step, a local administrator account was configured on all network devices as a backup measure, enabling privileged access in the event of AAA server failure or connectivity issues.



```
EdgeRouter(config)#username localadmin privilege 15 secret localadmin
```

Creating local admin account on edge router



Service ● On ○ Off

Radius Port 1645

Network Configuration

Client Name edge

Client IP 192.168.10.217

Secret cisco123

ServerType Tacacs

	Client Name	Client IP	Server Type	Key
1	fin_switch	192.168.10.130	Tacacs	cisco123
2	hr_switch	192.168.10.162	Tacacs	cisco123
3	core	192.168.10.225	Tacacs	cisco123
4	it_switch	192.168.10.194	Tacacs	cisco123
5	conf_switch	192.168.10.210	Tacacs	cisco123
6	server_switch	192.168.10.221	Tacacs	cisco123

User Setup

Username

Password

	Username	Password
1	netadmin	netpass

TACACS+ AAA server with registered devices, IPs, and shared secret.

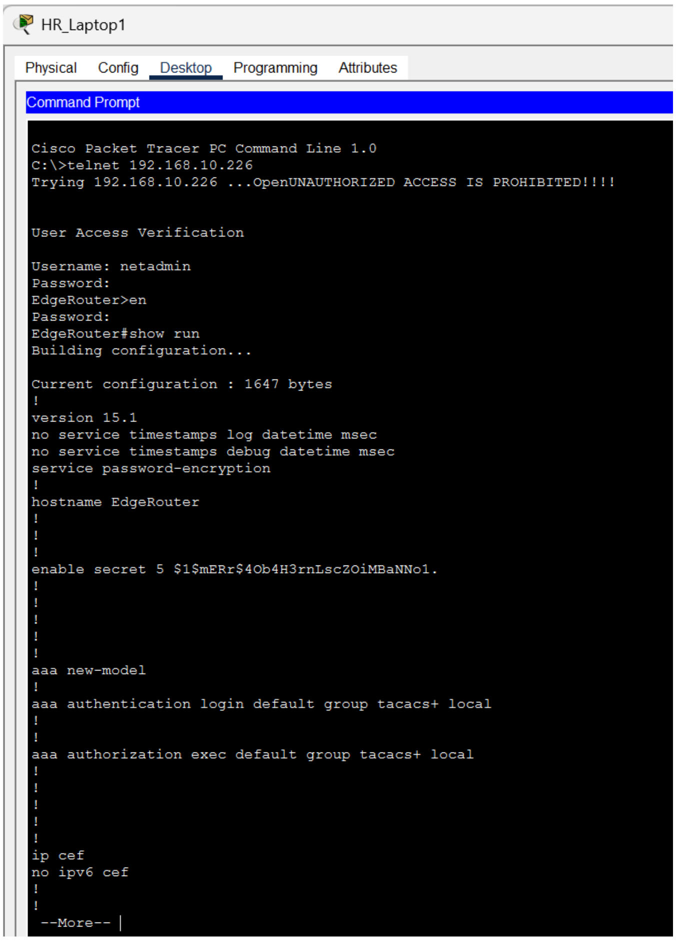
```
CoreRouter(config)#aaa new-model
CoreRouter(config)#username netadmin secret netpass
CoreRouter(config)#tacacs-server host 192.168.10.219 key cisco123
CoreRouter(config)#aaa authentication login default group tacacs+ local
CoreRouter(config)#aaa authorization exec default group tacacs+ local
CoreRouter(config)#line con 0
CoreRouter(config-line)# login authentication default
CoreRouter(config-line)#line vty 0 4
CoreRouter(config-line)# login authentication default
CoreRouter(config-line)# transport input telnet
```

Setting up AAA config in core router

Core switches and critical devices were registered on the AAA server with their respective client names and IP addresses, and a shared secret (**“cisco123”**) ensures secure communication between clients and the server. AAA authentication and authorization methods were applied globally, prioritizing TACACS+ with local fallback for both console and **vty (remote) access**. The vty lines were configured for default login authentication and enabled for **Telnet access**. This configuration ensures all administrative logins are securely authenticated and authorized through the central AAA server, following industry best practices for network security and device manageability.

username: netadmin

password: netpass

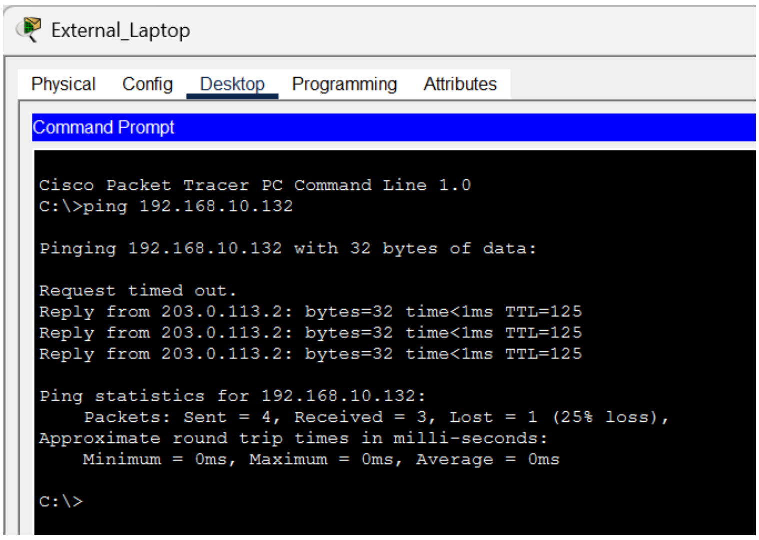


```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.10.226
Trying 192.168.10.226 ...OpenUNAUTHORIZED ACCESS IS PROHIBITED!!!!


User Access Verification

Username: netadmin
Password:
EdgeRouter>en
Password:
EdgeRouter#show run
Building configuration...

Current configuration : 1647 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname EdgeRouter
!
!
!
enable secret 5 $1$mERr$4Ob4H3rnLscZOiMBaNNo1.
!
!
!
!
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
!
aaa authorization exec default group tacacs+ local
!
!
!
!
!
ip cef
no ipv6 cef
!
!
 --More-- |
```

Successful telnet

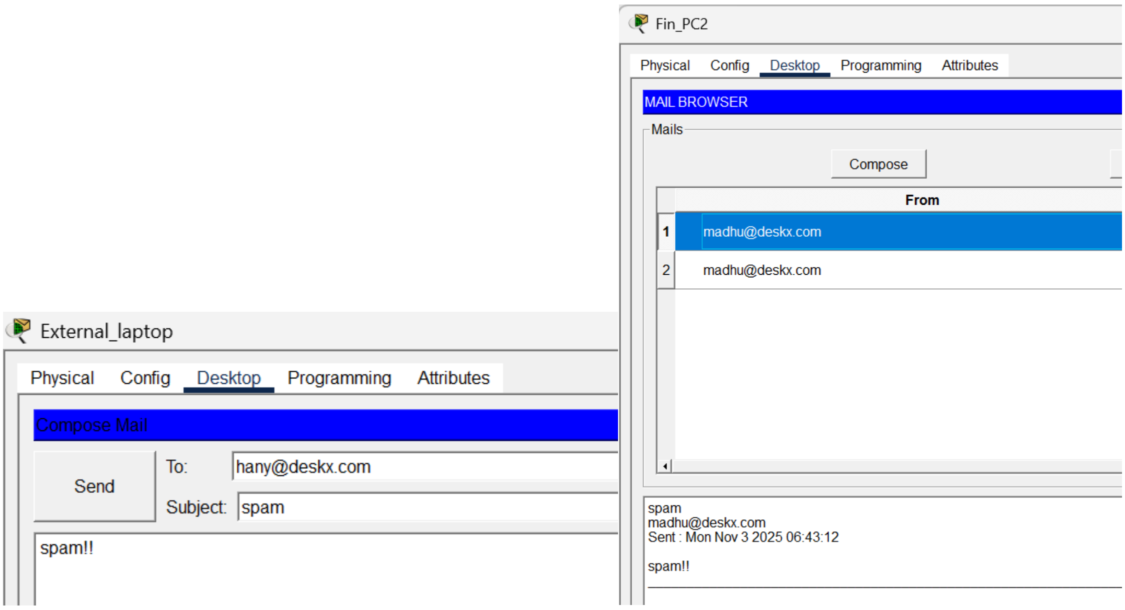
3.3 Zone Policy Firewall (ZPF) and Access Control Lists

Currently, a random laptop on the network can successfully **ping a host in the Finance subnet**, demonstrating that internal resources are exposed to unrestricted access. This includes sensitive servers and departmental hosts, creating potential security risks. To mitigate these threats, a **Cisco Zone-Based Policy Firewall (ZPF)** will be deployed on the edge router. ZPF provides **stateful, granular control of traffic between defined network zones**, enforcing security policies tailored to each segment. This ensures internal resources are protected while allowing legitimate communication, following best practices for segmentation and perimeter defense.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.132

Pinging 192.168.10.132 with 32 bytes of data:

Request timed out.
Reply from 203.0.113.2: bytes=32 time<1ms TTL=125
Reply from 203.0.113.2: bytes=32 time<1ms TTL=125
Reply from 203.0.113.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.10.132:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

An external host can reach out to finance department showing insecure design



To: hany@deskx.com
Subject: spam

spam!!

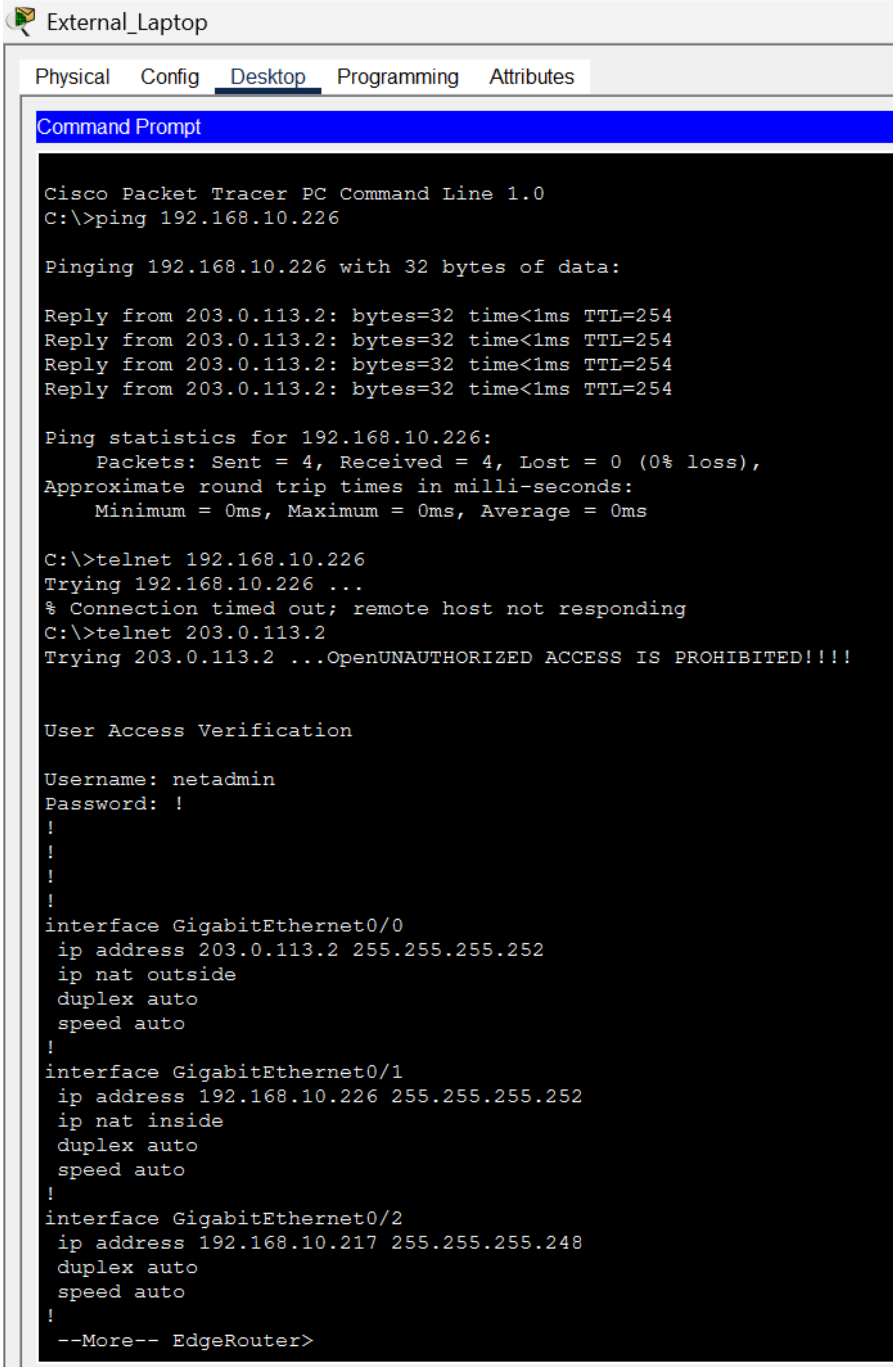
	From
1	madhu@deskx.com
2	madhu@deskx.com

spam
madhu@deskx.com
Sent : Mon Nov 3 2025 06:43:12

spam!!

External host sending emails to internal users via SMTP, demonstrating potential spam or unauthorized email activity.

The external host can access the edge router via its public IP (203.0.113.2), demonstrating a critical vulnerability. Without firewall rules in place, services such as Telnet are exposed to untrusted sources, allowing potential unauthorized administrative access and highlighting the need for strict zone-based policies.

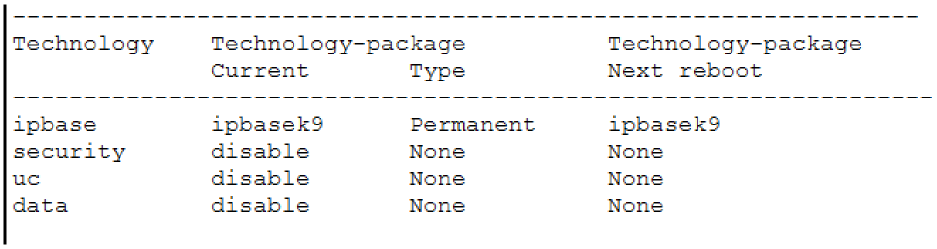


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.226

Pinging 192.168.10.226 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=254
Reply from 203.0.113.2: bytes=32 time<1ms TTL=254
Reply from 203.0.113.2: bytes=32 time<1ms TTL=254
Reply from 203.0.113.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.10.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>telnet 192.168.10.226
Trying 192.168.10.226 ...
% Connection timed out; remote host not responding
C:\>telnet 203.0.113.2
Trying 203.0.113.2 ...OpenUNAUTHORIZED ACCESS IS PROHIBITED!!!!


User Access Verification

Username: netadmin
Password: !
!
!
!
!
interface GigabitEthernet0/0
 ip address 203.0.113.2 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.10.226 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.10.217 255.255.255.248
 duplex auto
 speed auto
!
 --More-- EdgeRouter>
```

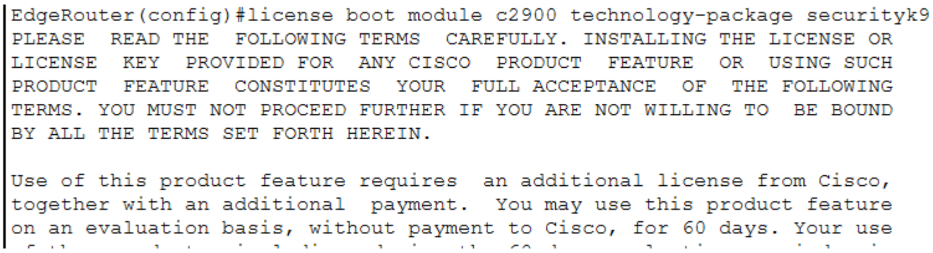
External laptop is able to telnet to the edge router

Step 1: Activate ZPF Package

On certain Cisco router models, such as the 2911, it is necessary to enable the Zone-Based Policy Firewall package (k9) before configuring security zones and policies. This ensures that all required features for zone-based filtering are available.



```
----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      disable       None           None
uc            disable       None           None
data          disable       None           None
```

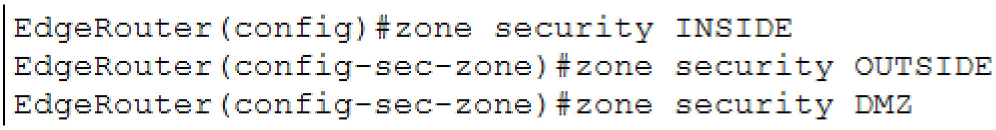


```
EdgeRouter(config)#license boot module c2900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
```

k9 package activation

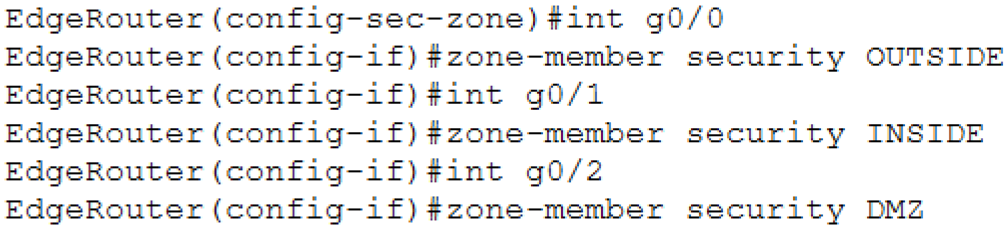
Step 2: Define Security Zones

After enabling ZPF, **security zones** are created to segment the network. Each interface is assigned to a zone based on its trust level: **Inside**, **DMZ**, **Outside**. These zones form the basis for applying firewall policies and controlling traffic between different parts of the network.



```
EdgeRouter(config)#zone security INSIDE
EdgeRouter(config-sec-zone)#zone security OUTSIDE
EdgeRouter(config-sec-zone)#zone security DMZ
```

Zone definition

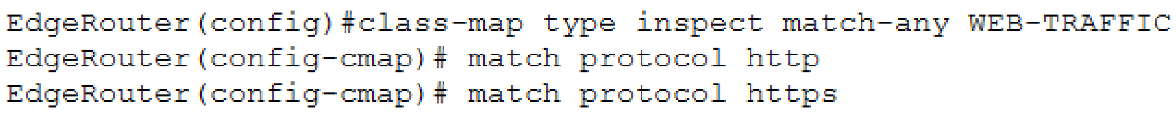


```
EdgeRouter(config-sec-zone)#int g0/0
EdgeRouter(config-if)#zone-member security OUTSIDE
EdgeRouter(config-if)#int g0/1
EdgeRouter(config-if)#zone-member security INSIDE
EdgeRouter(config-if)#int g0/2
EdgeRouter(config-if)#zone-member security DMZ
```

Assigning interfaces

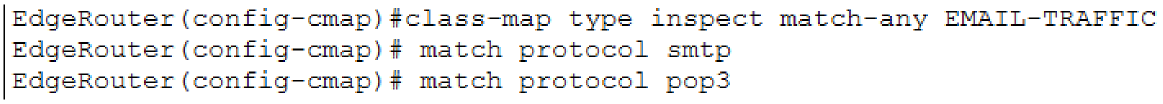
Step 3: Create Class Maps to Match Traffic

Once security zones are defined, class maps are configured to identify and classify the types of traffic that will be controlled by the firewall. Each class map specifies the protocols, ports, or other criteria for matching traffic, such as HTTP, SMTP, Telnet, or ICMP. These class maps serve as the foundation for applying policies, allowing the firewall to differentiate between allowed, restricted, or monitored traffic between zones.



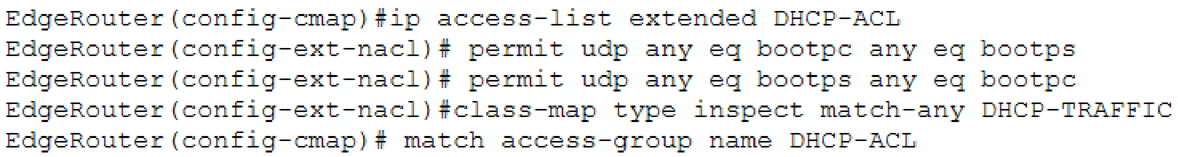
```
EdgeRouter(config)#class-map type inspect match-any WEB-TRAFFIC
EdgeRouter(config-cmap)# match protocol http
EdgeRouter(config-cmap)# match protocol https
```

Class map for web/http traffic



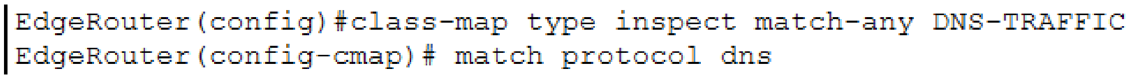
```
EdgeRouter(config-cmap)#class-map type inspect match-any EMAIL-TRAFFIC
EdgeRouter(config-cmap)# match protocol smtp
EdgeRouter(config-cmap)# match protocol pop3
```

Class map for email traffic



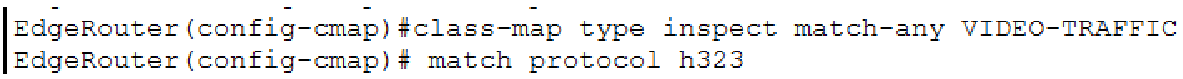
```
EdgeRouter(config-cmap)#ip access-list extended DHCP-ACL
EdgeRouter(config-ext-nacl)# permit udp any eq bootpc any eq bootps
EdgeRouter(config-ext-nacl)# permit udp any eq bootps any eq bootpc
EdgeRouter(config-ext-nacl)#class-map type inspect match-any DHCP-TRAFFIC
EdgeRouter(config-cmap)# match access-group name DHCP-ACL
```

DHCP traffic



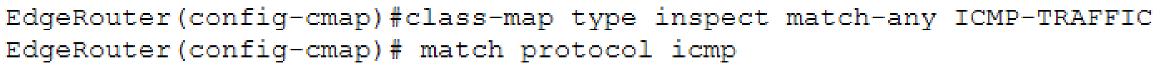
```
EdgeRouter(config)#class-map type inspect match-any DNS-TRAFFIC
EdgeRouter(config-cmap)# match protocol dns
```

Class map for DNS traffic



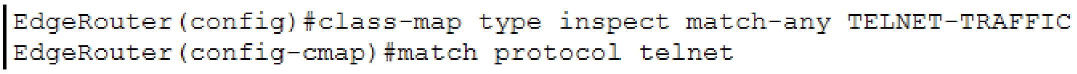
```
EdgeRouter(config-cmap)#class-map type inspect match-any VIDEO-TRAFFIC
EdgeRouter(config-cmap)# match protocol h323
```

Class map for video conferencing



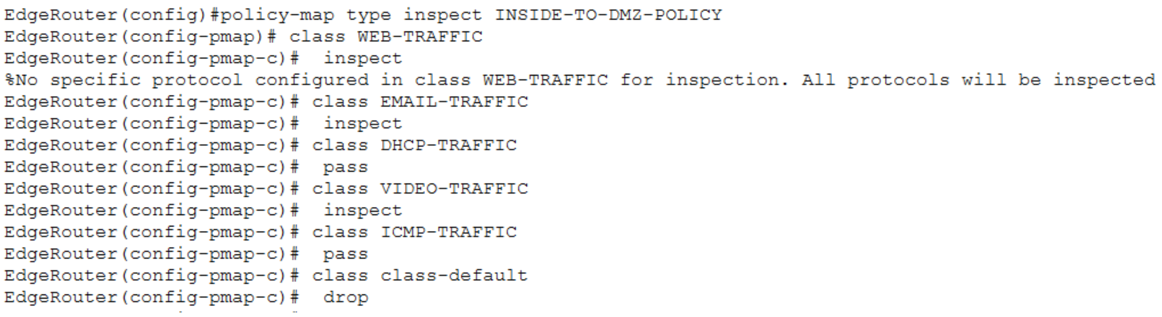
```
EdgeRouter(config-cmap)#class-map type inspect match-any ICMP-TRAFFIC
EdgeRouter(config-cmap)# match protocol icmp
```

ICMP class map



```
EdgeRouter(config)#class-map type inspect match-any TELNET-TRAFFIC
EdgeRouter(config-cmap)#match protocol telnet
```

Telnet traffic

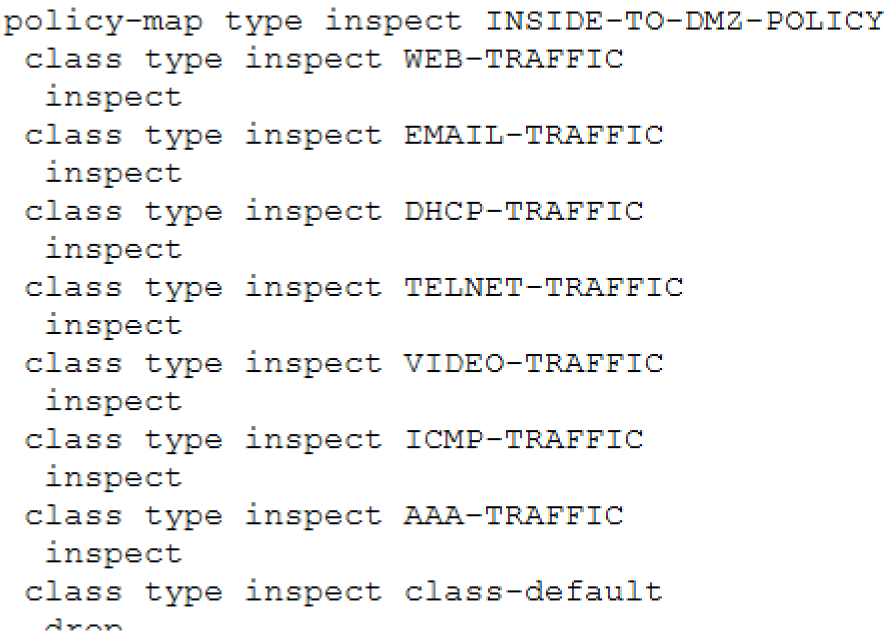


```
EdgeRouter(config)#policy-map type inspect INSIDE-TO-DMZ-POLICY
EdgeRouter(config-pmap)# class WEB-TRAFFIC
EdgeRouter(config-pmap-c)#  inspect
%No specific protocol configured in class WEB-TRAFFIC for inspection. All protocols will be inspected
EdgeRouter(config-pmap-c)# class EMAIL-TRAFFIC
EdgeRouter(config-pmap-c)#  inspect
EdgeRouter(config-pmap-c)# class DHCP-TRAFFIC
EdgeRouter(config-pmap-c)#  pass
EdgeRouter(config-pmap-c)# class VIDEO-TRAFFIC
EdgeRouter(config-pmap-c)#  inspect
EdgeRouter(config-pmap-c)# class ICMP-TRAFFIC
EdgeRouter(config-pmap-c)#  pass
EdgeRouter(config-pmap-c)# class class-default
EdgeRouter(config-pmap-c)#  drop
```

Policy Map for class inspection - allowing access to servers

Step 4: Create Policy Maps

After defining class maps, policy maps are created to specify the actions the firewall should take on the matched traffic. Each policy map links one or more class maps to a set of actions, such as inspect, drop, or pass, depending on the desired security policy. In this implementation, traffic is either inspected to allow and monitor legitimate flows or dropped to block unauthorized or risky connections.

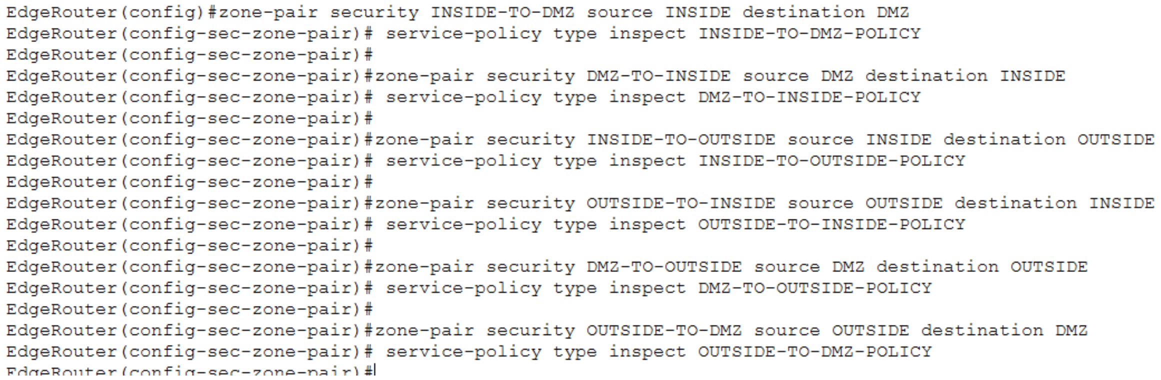


```
policy-map type inspect INSIDE-TO-DMZ-POLICY
 class type inspect WEB-TRAFFIC
  inspect
 class type inspect EMAIL-TRAFFIC
  inspect
 class type inspect DHCP-TRAFFIC
  inspect
 class type inspect TELNET-TRAFFIC
  inspect
 class type inspect VIDEO-TRAFFIC
  inspect
 class type inspect ICMP-TRAFFIC
  inspect
 class type inspect AAA-TRAFFIC
  inspect
 class type inspect class-default
  drop
```

Policy map configuration for "INSIDE-TO-DMZ-POLICY": Each traffic class (e.g., Web, Email, DHCP, Telnet, Video, ICMP, AAA) is set to inspect, enabling stateful firewall monitoring. All other unmatched traffic is dropped by default, ensuring strict security enforcement between the zones.

Step 5: Configure Zone Pairs

After policy maps are created, zone pairs are configured to define traffic flow between security zones. Each zone pair specifies a source zone and a destination zone, and the associated service-policy (policy map) is applied to control traffic between them. For example, an INSIDE-to-DMZ zone pair applies the INSIDE-TO-DMZ-POLICY, allowing inspected traffic to flow while dropping all other connections.

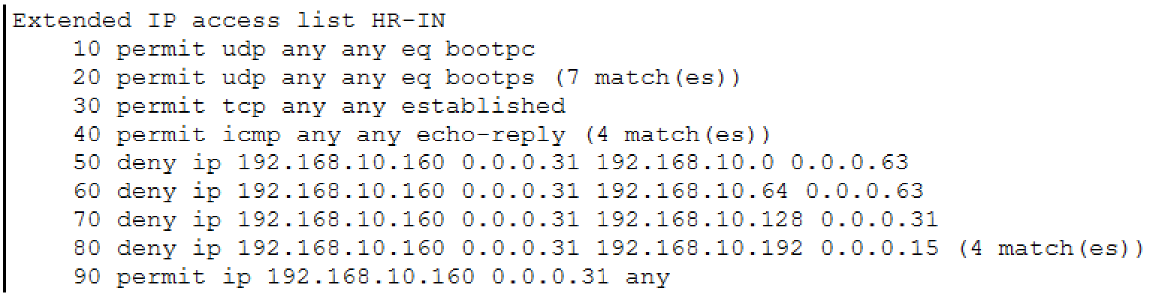


```
EdgeRouter(config)#zone-pair security INSIDE-TO-DMZ source INSIDE destination DMZ
EdgeRouter(config-sec-zone-pair)# service-policy type inspect INSIDE-TO-DMZ-POLICY
EdgeRouter(config-sec-zone-pair)#
EdgeRouter(config-sec-zone-pair)#zone-pair security DMZ-TO-INSIDE source DMZ destination INSIDE
EdgeRouter(config-sec-zone-pair)# service-policy type inspect DMZ-TO-INSIDE-POLICY
EdgeRouter(config-sec-zone-pair)#
EdgeRouter(config-sec-zone-pair)#zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
EdgeRouter(config-sec-zone-pair)# service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
EdgeRouter(config-sec-zone-pair)#
EdgeRouter(config-sec-zone-pair)#zone-pair security OUTSIDE-TO-INSIDE source OUTSIDE destination INSIDE
EdgeRouter(config-sec-zone-pair)# service-policy type inspect OUTSIDE-TO-INSIDE-POLICY
EdgeRouter(config-sec-zone-pair)#
EdgeRouter(config-sec-zone-pair)#zone-pair security DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
EdgeRouter(config-sec-zone-pair)# service-policy type inspect DMZ-TO-OUTSIDE-POLICY
EdgeRouter(config-sec-zone-pair)#
EdgeRouter(config-sec-zone-pair)#zone-pair security OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
EdgeRouter(config-sec-zone-pair)# service-policy type inspect OUTSIDE-TO-DMZ-POLICY
EdgeRouter(config-sec-zone-pair)#
```

Zone pairs

While the Zone-Based Policy Firewall (ZPF) effectively separates the network into monitored zones, it does not inherently control traffic within the Inside zone. To enforce inter-departmental access restrictions, **Access Control Lists (ACLs)** were implemented on the core router. These ACLs ensure that only authorized traffic reaches each department, preventing unnecessary or potentially harmful communications.

The ACLs were applied on inbound interfaces of the core router, which allows packets to be filtered as soon as they arrive from the source subnet. This approach minimizes the load on the router and prevents unauthorized traffic from entering the network, ensuring that only permitted packets are processed and forwarded. Using inbound ACLs also aligns with best practices for controlling internal traffic while maintaining network efficiency.

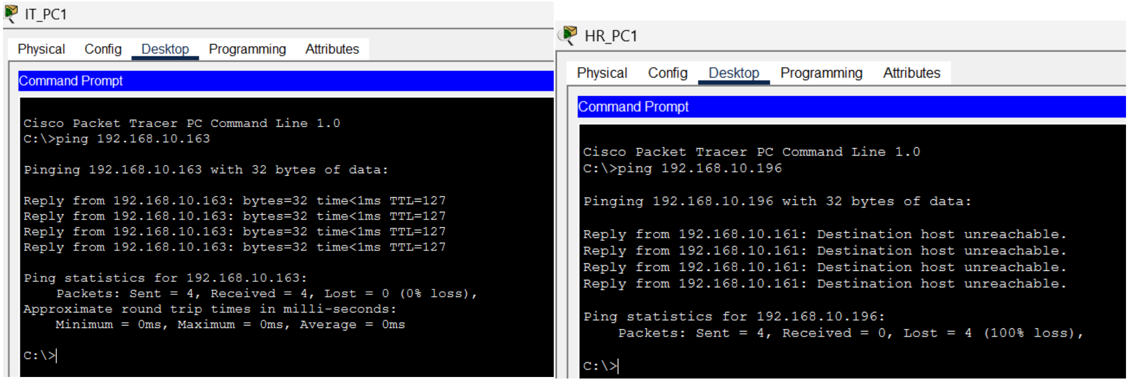


```
Extended IP access list HR-IN
    10 permit udp any any eq bootpc
    20 permit udp any any eq bootps (7 match(es))
    30 permit tcp any any established
    40 permit icmp any any echo-reply (4 match(es))
    50 deny ip 192.168.10.160 0.0.0.31 192.168.10.0 0.0.0.63
    60 deny ip 192.168.10.160 0.0.0.31 192.168.10.64 0.0.0.63
    70 deny ip 192.168.10.160 0.0.0.31 192.168.10.128 0.0.0.31
    80 deny ip 192.168.10.160 0.0.0.31 192.168.10.192 0.0.0.15 (4 match(es))
    90 permit ip 192.168.10.160 0.0.0.31 any
```

ACL for Design Department

The above ACL configuration permits ICMP echo-reply packets early in the rule set, allowing Design department hosts to receive ping responses for network diagnostics. Deny statements targeting restricted subnets prevent Design hosts from initiating communication to those areas. This ensures that Design can perform outbound connectivity tests while maintaining strict segmentation and protecting sensitive departmental resources.

In the following example, IT host can successfully ping a PC in HR, while HR host is unable to ping back, demonstrating enforced inter-departmental segmentation.

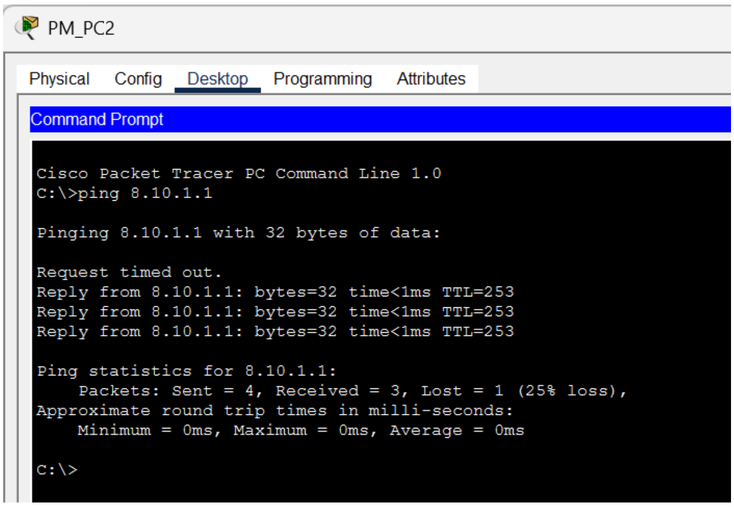


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.163

Pinging 192.168.10.163 with 32 bytes of data:

Reply from 192.168.10.163: bytes=32 time<1ms TTL=127
Reply from 192.168.10.163: bytes=32 time<1ms TTL=127
Reply from 192.168.10.163: bytes=32 time<1ms TTL=127
Reply from 192.168.10.163: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.196

Pinging 192.168.10.196 with 32 bytes of data:

Reply from 192.168.10.161: Destination host unreachable.
Reply from 192.168.10.161: Destination host unreachable.
Reply from 192.168.10.161: Destination host unreachable.
Reply from 192.168.10.161: Destination host unreachable.

Ping statistics for 192.168.10.196:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

One way ping

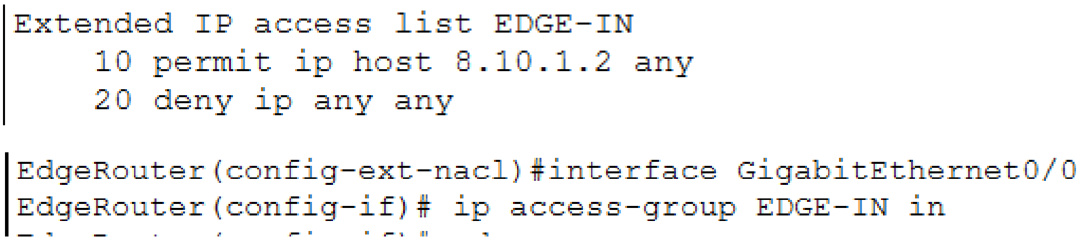
There is also accessibility to the internet server, tested through pinging from an internal server.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.10.1.1

Pinging 8.10.1.1 with 32 bytes of data:

Request timed out.
Reply from 8.10.1.1: bytes=32 time<1ms TTL=253
Reply from 8.10.1.1: bytes=32 time<1ms TTL=253
Reply from 8.10.1.1: bytes=32 time<1ms TTL=253

Ping statistics for 8.10.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Successful ping to the internet server after ZPF and ACL application

An extended ACL was applied on the edge router’s external interface to enforce a secure perimeter. Traffic is permitted only from the designated Internet server (8.10.1.2), while all other external sources are denied by the default rule. This ensures that only the authorized server can communicate with internal hosts, effectively blocking all other untrusted external access and maintaining the integrity of internal resources.

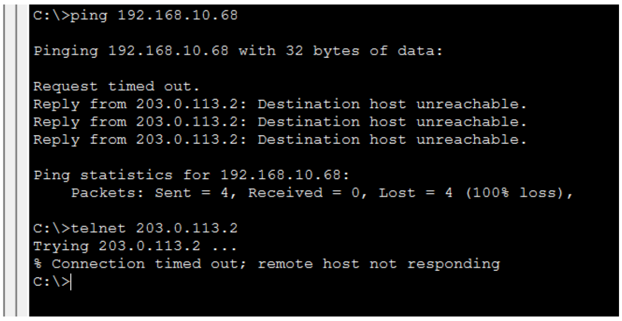


```
Extended IP access list EDGE-IN
    10 permit ip host 8.10.1.2 any
    20 deny ip any any
```

```
EdgeRouter(config-ext-nacl)#interface GigabitEthernet0/0
EdgeRouter(config-if)# ip access-group EDGE-IN in
```

Inbound ACL on edge router to block unwanted external traffic

In this manner, no other hosts other than the internet server, can access the DeskX environment as shown below.



```
C:\>ping 192.168.10.68

Pinging 192.168.10.68 with 32 bytes of data:

Request timed out.
Reply from 203.0.113.2: Destination host unreachable.
Reply from 203.0.113.2: Destination host unreachable.
Reply from 203.0.113.2: Destination host unreachable.

Ping statistics for 192.168.10.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>telnet 203.0.113.2
Trying 203.0.113.2 ...
% Connection timed out; remote host not responding
C:\>
```

Ping and Telnet failure in External Laptop (198.51.100.10)

4. Critical Reflection and Evaluation

4.1 Security Posture: Strengths, Weaknesses, and Improvements

The network enforces departmental isolation, dedicated subnetting, and strict access control. Core routing, Zone-Based Policy Firewall (ZPF), and layered ACLs ensure only authorized traffic between zones and from external sources. AAA authentication secures device management, and WPA2 protects wireless access.

Weaknesses include internal ACLs that could be more granular to limit inter-department connectivity and initial exposure of the edge router to external hosts. Enabling SSH for device management and implementing VPNs for secure remote access would improve security. Regular review of permissions and adoption of intrusion detection/prevention measures would further strengthen the posture.

4.2 Scalability and Future-Proofing

Hierarchical subnetting, OSPF routing, and zone separation support expansion, while wireless APs and centralized DHCP simplify adding devices. Some subnets only accommodate current host counts, so growth may require resizing. The design can extend to remote work and cloud integration through VPNs, updated firewall rules, and DMZ segmentation. Centralized identity management and multi-factor authentication would further future-proof the network.

4.3 Key Challenges and Mitigation

One of the initial challenges was the aim to implement a zero-trust approach by creating a separate zone of trust for each department using the core switch. As the switch operated at Layer 2, it could not enforce inter-zone policies effectively, requiring the replacement with a Layer 3 core router to achieve proper segmentation and control. Another significant issue arose with DHCP functionality after implementing the Zone-Based Policy Firewall (ZPF), which initially blocked dynamic address assignment. This was resolved by ensuring UDP traffic for bootpc/bootps was permitted through the firewall. Limited subnet space also affected the network design; for instance, the planned file server had to be removed to maintain proper subnet allocation for all departments. Additionally, configuring ACLs to enforce one-way ping and controlled inter-department connectivity required careful sequencing of permit and deny rules. These challenges highlight the importance of aligning device capabilities with security requirements, careful planning for IP addressing, and iterative testing to ensure functionality under strict segmentation policies.

5. APPENDICES

Network Device Configurations:

Edge Router:

- OSPF Routes

```
router ospf 1
log-adjacency-changes
network 192.168.10.224 0.0.0.3 area 0
network 192.168.10.216 0.0.0.7 area 0
default-information originate
```

- Full ZPF

```
class-map type inspect match-any WEB-TRAFFIC
match protocol http
match protocol https
class-map type inspect match-any EMAIL-TRAFFIC
match protocol smtp
match protocol pop3
class-map type inspect match-any DNS-TRAFFIC
match protocol dns
class-map type inspect match-any VIDEO-TRAFFIC
match protocol h323
class-map type inspect match-any ICMP-TRAFFIC
match protocol icmp
class-map type inspect match-any TELNET-TRAFFIC
match protocol telnet
class-map type inspect match-any DHCP-TRAFFIC
match access-group name DHCP-REL
class-map type inspect match-any AAA-TRAFFIC
match access-group name AAA-ACL
!
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
```

```
class type inspect WEB-TRAFFIC
inspect
class type inspect EMAIL-TRAFFIC
inspect
class type inspect DNS-TRAFFIC
inspect
class type inspect TELNET-TRAFFIC
inspect
class type inspect ICMP-TRAFFIC
inspect
class type inspect class-default
drop
!
policy-map type inspect DMZ-TO-OUTSIDE-POLICY
class type inspect WEB-TRAFFIC
inspect
class type inspect DNS-TRAFFIC
inspect
class type inspect EMAIL-TRAFFIC
inspect
class type inspect ICMP-TRAFFIC
inspect
class type inspect class-default
drop
!
policy-map type inspect OUTSIDE-TO-DMZ-POLICY
class type inspect WEB-TRAFFIC
inspect
class type inspect ICMP-TRAFFIC
inspect
class type inspect class-default
drop
```

```
!
policy-map type inspect OUTSIDE-TO-INSIDE-POLICY
class type inspect ICMP-TRAFFIC
inspect
class type inspect class-default
drop
!
policy-map type inspect INSIDE-TO-DMZ-POLICY
class type inspect WEB-TRAFFIC
inspect
class type inspect EMAIL-TRAFFIC
inspect
class type inspect DHCP-TRAFFIC
inspect
class type inspect TELNET-TRAFFIC
inspect
class type inspect VIDEO-TRAFFIC
inspect
class type inspect ICMP-TRAFFIC
inspect
class type inspect AAA-TRAFFIC
inspect
class type inspect class-default
drop
!
policy-map type inspect DMZ-TO-INSIDE-POLICY
class type inspect WEB-TRAFFIC
inspect
class type inspect EMAIL-TRAFFIC
inspect
class type inspect DHCP-TRAFFIC
inspect
```

```
class type inspect DNS-TRAFFIC
inspect
class type inspect ICMP-TRAFFIC
inspect
class type inspect AAA-TRAFFIC
inspect
class type inspect class-default
drop
!
!
!
zone security INSIDE
zone security OUTSIDE
zone security DMZ
zone-pair security INSIDE-TO-DMZ source INSIDE destination DMZ
service-policy type inspect INSIDE-TO-DMZ-POLICY
zone-pair security DMZ-TO-INSIDE source DMZ destination INSIDE
service-policy type inspect DMZ-TO-INSIDE-POLICY
zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
zone-pair security OUTSIDE-TO-INSIDE source OUTSIDE destination INSIDE
service-policy type inspect OUTSIDE-TO-INSIDE-POLICY
zone-pair security DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
service-policy type inspect DMZ-TO-OUTSIDE-POLICY
zone-pair security OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
service-policy type inspect OUTSIDE-TO-DMZ-POLICY
```

- Access Lists

```
access-list 1 permit 192.168.10.0 0.0.0.255
ip access-list extended DHCP-REL
permit udp any eq bootps 192.168.10.216 0.0.0.7 eq bootps
permit udp 192.168.10.216 0.0.0.7 eq bootps any eq bootps
permit udp any any eq bootps
permit udp any any eq bootpc
ip access-list extended AAA-ACL
permit tcp any host 192.168.10.219 eq 49
ip access-list extended EDGE-IN
permit ip host 8.10.1.2 any
deny ip any any
```

- Interfaces

```
interface GigabitEthernet0/0
ip address 203.0.113.2 255.255.255.252
zone-member security OUTSIDE
ip nat outside
ip access-group EDGE-IN in
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.10.226 255.255.255.252
zone-member security INSIDE
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.10.217 255.255.255.248
zone-member security DMZ
duplex auto
speed auto
!
```

Core Router:

- Full Access Lists

```
ip access-list extended HR-IN
permit udp any any eq bootpc
permit udp any any eq bootps
permit tcp any any established
permit icmp any any echo-reply
deny ip 192.168.10.160 0.0.0.31 192.168.10.0 0.0.0.63
deny ip 192.168.10.160 0.0.0.31 192.168.10.64 0.0.0.63
deny ip 192.168.10.160 0.0.0.31 192.168.10.128 0.0.0.31
deny ip 192.168.10.160 0.0.0.31 192.168.10.192 0.0.0.15
permit ip 192.168.10.160 0.0.0.31 any
ip access-list extended PM-IN
permit udp any any eq bootpc
permit udp any any eq bootps
permit tcp any any established
permit icmp any any echo-reply
deny ip 192.168.10.64 0.0.0.63 192.168.10.160 0.0.0.31
deny ip 192.168.10.64 0.0.0.63 192.168.10.192 0.0.0.15
permit ip 192.168.10.64 0.0.0.63 any
ip access-list extended DESIGN-IN
permit udp any any eq bootpc
permit udp any any eq bootps
permit tcp any any established
permit icmp any any echo-reply
deny ip 192.168.10.0 0.0.0.63 192.168.10.160 0.0.0.31
deny ip 192.168.10.0 0.0.0.63 192.168.10.128 0.0.0.31
deny ip 192.168.10.0 0.0.0.63 192.168.10.192 0.0.0.15
permit ip 192.168.10.0 0.0.0.63 any
ip access-list extended FIN-IN
permit udp any any eq bootpc
permit udp any any eq bootps
permit tcp any any established
permit icmp any any echo-reply
deny ip 192.168.10.128 0.0.0.31 192.168.10.0 0.0.0.63
deny ip 192.168.10.128 0.0.0.31 192.168.10.160 0.0.0.31
deny ip 192.168.10.128 0.0.0.31 192.168.10.192 0.0.0.15
permit ip 192.168.10.128 0.0.0.31 192.168.10.64 0.0.0.63
permit ip 192.168.10.128 0.0.0.31 any
ip access-list extended IT-IN
permit udp any any eq bootpc
permit udp any any eq bootps
permit tcp any any established
permit icmp any any echo
permit ip 192.168.10.192 0.0.0.15 any
```

- OSPF Routes

```
router ospf 1
log-adjacency-changes
network 192.168.10.160 0.0.0.31 area 0
network 192.168.10.0 0.0.0.63 area 0
network 192.168.10.64 0.0.0.63 area 0
network 192.168.10.208 0.0.0.7 area 0
network 192.168.10.128 0.0.0.31 area 0
network 192.168.10.192 0.0.0.15 area 0
network 192.168.10.224 0.0.0.3 area 0
```

- Interfaces

```
interface GigabitEthernet1/0
ip address 192.168.10.225 255.255.255.252
duplex auto
speed auto
!
```

```
interface GigabitEthernet2/0
ip address 192.168.10.193 255.255.255.240
ip helper-address 192.168.10.218
ip access-group IT-IN in
duplex auto
speed auto
!
interface GigabitEthernet3/0
ip address 192.168.10.161 255.255.255.224
ip helper-address 192.168.10.218
ip access-group HR-IN in
duplex auto
speed auto
!
interface GigabitEthernet4/0
ip address 192.168.10.1 255.255.255.192
ip helper-address 192.168.10.218
ip access-group DESIGN-IN in
duplex auto
speed auto
!
interface GigabitEthernet5/0
ip address 192.168.10.129 255.255.255.224
ip helper-address 192.168.10.218
ip access-group FINANCE-IN in
duplex auto
speed auto
!
interface GigabitEthernet6/0
```

```
ip address 192.168.10.65 255.255.255.192
ip helper-address 192.168.10.218
ip access-group PM-IN in
duplex auto
speed auto
!
interface GigabitEthernet7/0
no ip address
ip helper-address 192.168.10.218
duplex auto
speed auto
shutdown
!
interface GigabitEthernet8/0
ip address 192.168.10.209 255.255.255.248
ip helper-address 192.168.10.218
duplex auto
speed auto
!
interface GigabitEthernet9/0
no ip address
duplex auto
speed auto
shutdown
!
```

References

Anderson, R. (2020) *Security engineering: a guide to building dependable distributed systems.* 3rd edn. London: Wiley.

Donahue, G.A. (2024) *Network Warrior.* 2nd edn. Boston: O'Reilly Media.

Kozierok, C.M. (2024) *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.* 1st edn. San Francisco: No Starch Press.

Musa, S.M. (2018) *Network Security and Cryptography.* London: Springer.

Pfleeger, C., Pfleeger, S. and Coles-Kemp, L. (2023) *Security in Computing.* 6th edn. Harlow: Pearson.

ChatGPT (2025) AI-assisted planning and conceptual guidance for network design and documentation. OpenAI.

Perplexity (2025) AI-assisted planning and conceptual guidance for network design and documentation. [Online]