

Complex Engineering Problem

**Group members:**

FAZEEL ABBAS FA20-BCE-041

MOIZ USMAN FA20-BCE-025

**Submitted to:**

MODASSIR ISHAFQ

Table of Contents

[Implementation Details: 4](#_Toc137414163)

[1: 4](#_Toc137414164)

[2: 5](#_Toc137414165)

[3: 5](#_Toc137414166)

[4: 5](#_Toc137414167)

[5: 5](#_Toc137414168)

[6: 5](#_Toc137414169)

[7: 5](#_Toc137414170)

[8: 5](#_Toc137414171)

[9: 5](#_Toc137414172)

[10: 5](#_Toc137414173)

[11: 6](#_Toc137414174)

[12: 6](#_Toc137414175)

[Connectivity verification report: 6](#_Toc137414176)

[VLAN 10: 6](#_Toc137414177)

[VLAN 20: 7](#_Toc137414178)

[VLAN 30: 7](#_Toc137414179)

[AREA 1 to AREA 2: 8](#_Toc137414180)

[AREA 1 to AREA 3: 9](#_Toc137414181)

[AREA 1to AREA 4: 10](#_Toc137414182)

[AREA 1 to AREA 5: 11](#_Toc137414183)

[AREA 2 to AREA 3: 11](#_Toc137414184)

[AREA 2 to AREA 4: 11](#_Toc137414185)

[AREA 2 to AREA 5: 13](#_Toc137414186)

[AREA 3 to AREA 4: 13](#_Toc137414187)

[AREA 3 to AREA 5: 14](#_Toc137414188)

[AREA 4 to AREA 5: 15](#_Toc137414189)

[Servers’ operability report: 16](#_Toc137414190)

[HTTP 16](#_Toc137414191)

[AREA 1 to 4: 16](#_Toc137414192)

[AREA 5: 16](#_Toc137414193)

[DNS 17](#_Toc137414194)

[DHCP 17](#_Toc137414195)

[PC13 From AREA 1: 18](#_Toc137414196)

[PC8 From AREA 2: 19](#_Toc137414197)

[PC6 From AREA 3: 19](#_Toc137414198)

[PC1 From AREA 4: 19](#_Toc137414199)

[PC4 From AREA 5: 19](#_Toc137414200)

[ALTERNTIVE IMPLEMENTATION METHODS: 20](#_Toc137414201)

[APPENDIX: 20](#_Toc137414202)

[ROUTER: 20](#_Toc137414203)

[Basic Configurations: 20](#_Toc137414204)

[For Securing console and virtual line: 20](#_Toc137414205)

[OSPF: 20](#_Toc137414206)

[For VLANs: 20](#_Toc137414207)

[SWITCHES FOR VLANS: 21](#_Toc137414208)

[SERVERS: 21](#_Toc137414209)

[HTTP: 21](#_Toc137414210)

[DNS: 21](#_Toc137414211)

[DHCP: 22](#_Toc137414212)

[NAT: 22](#_Toc137414213)

[For DHCP: 22](#_Toc137414214)

[For HTTP: 22](#_Toc137414215)

[For DNS: 22](#_Toc137414216)

[ACL: 22](#_Toc137414217)

[On router 12 to make area 3 secure: 22](#_Toc137414218)

[On R8 so AREA 2 won’t Access PC1: 23](#_Toc137414219)

[EXTENDED ACL: 23](#_Toc137414220)

**LIST OF FIGURES:**

[Figure 1.VLAN10 6](#_Toc137413446)

[Figure 2.VLAN20 7](#_Toc137413447)

[Figure 3.VLAN30 7](#_Toc137413448)

[Figure 4.Ping A1 to A2 8](#_Toc137413449)

[Figure 5.Ping A2 to A3 9](#_Toc137413450)

[Figure 6.Ping A1 to A4 10](#_Toc137413451)

[Figure 7.Trace A1 to A5 10](#_Toc137413452)

[Figure 8. Ping A1 to A5 11](#_Toc137413453)

[Figure 9. Ping A2 to A3 11](#_Toc137413454)

[Figure 10. Ping A2 to A4 12](#_Toc137413455)

[Figure 11.Tracert A2 to A4 12](#_Toc137413456)

[Figure 12 Ping A2 to A5 13](#_Toc137413457)

[Figure 13.Tracert A2 to A5 13](#_Toc137413458)

[Figure 14.Tracert A2 to A5 14](#_Toc137413459)

[Figure 15.Ping A4 to A5 15](#_Toc137413460)

[Figure 16.Tracert A4 to A5 15](#_Toc137413461)

# Implementation Details:

**PASSWORD: class**

**SECRET: cisco**

## 1:

Multi ospf was configured.

For Area 1 router 16 is summarizing WAN links used in that Area. Summarization range is 172.168.0.0/28. Network 172.168.0.12/30 is not used because there are only 3 WAN links in area. And if used anywhere in the network it won’t be summarized properly.

For Area 2, router 17 is summarizing WAN links used in that Area. Summarization range is 172.168.0.16/28. Network 172.168.0.28/30 is not used.

For Area 3 router 11 is summarizing WAN links used in that Area. The summarization range is 172.168.0.32/28. Network 172.168.0.44/30 is not used.

For Area 4 router 9 is summarizing WAN links used in that Area. The summarization range is 172.168.0.48/28. Network 172.168.0.60/30 is not used.

For Area 5 router 2 is summarizing WAN links used in that Area. The Summarization range is 172.168.0.64/28. Network 172.168.0.76/30 is not used.

## 2:

According to the requirement all WAN links in the network have different bandwidths. Each bandwidth is increasing by 50kb.

## 3:

For all WAN links, the public address **172.168.0.0/30** is used. Its subnet mask is 30 because each WAN link only requires 2 IP addresses.

## 4:

For All the LAN links 172.25.0.0/28 private address is used. The first range of IP addresses from 172.25.0.0/28 to 172.25.0.15 is not used anywhere in the network.

## 5:

IP addresses of range 172.16.0.0/16 are used for all the servers. These IP addresses are private.

## 6:

NAT is configured on Router 17. So, all the networks’ devices can only use public address of servers.

NAT inside Network is connected to fa0/0. NAT outside networks is connected to Se6/0, Se3/0, Se2/0 of R17.

Servers Public address is 172.168.0.110/30 which is IP address of Se6/0 on router 17.

The same Public IP address is used for all the servers but with different port numbers. For http Port number is 80. For DNS port number is 53.

## 7:

All end networks are successfully leasing their IP address for DHCP server. For this All the LANs and VLANs with their network address are added in DCHP services.

## 8:

DNS and HTTP servers are configured properly. All the hosts in the network can access html page by public address and name.

## 9:

For VLANs in Area 1. 172.17.0.0/16. IP address is used. VLAN 10 IP address is 172.17.10.0/24. VLAN 20 IP address is 172.17.20.0/24. VLAN 30 IP address is 172.17.30.0/24. All VLANs hosts can lease their IP addresses from DHCP server. And can connect to other hosts.

## 10:

For this ACL is used at R12. Which filters the outbound traffic, and no outside device can connect the LAN in Area 3.

## 11:

For this Extended ACL is used at R17 which filters all the outbound traffic with port 80 from Area 5.

## 12:

ACL is used at R8 to filter out IP address from network 172.25.0.64/28 of area 2.

# Connectivity verification report:

## VLAN 10:

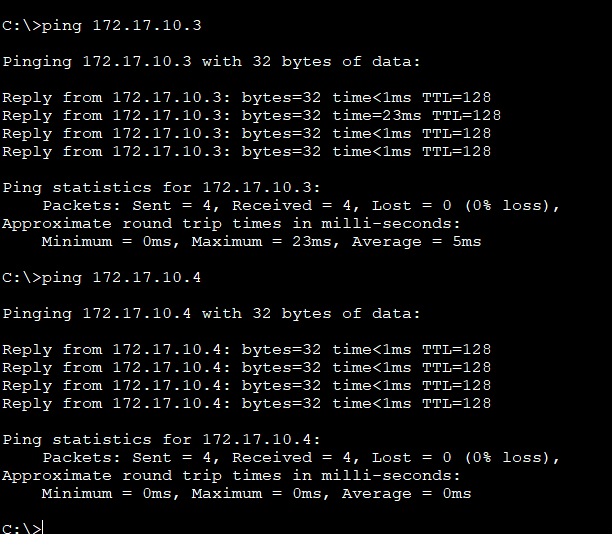


Figure 1.VLAN10

## VLAN 20:

A picture containing text, screenshot, font

Description automatically generated

Figure 2.VLAN20

## VLAN 30:

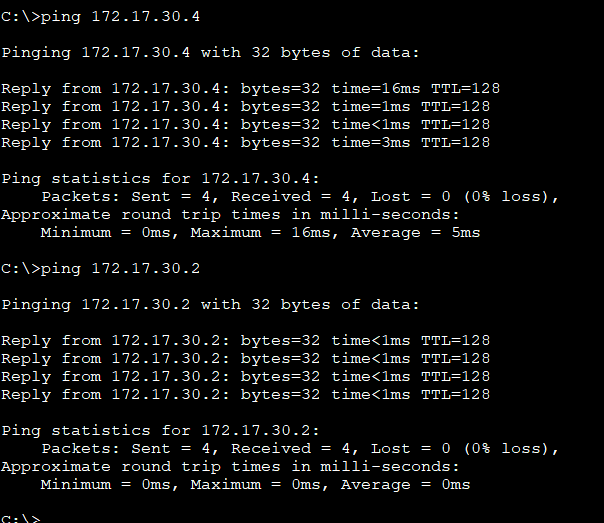


Figure 3.VLAN30

## AREA 1 to AREA 2:

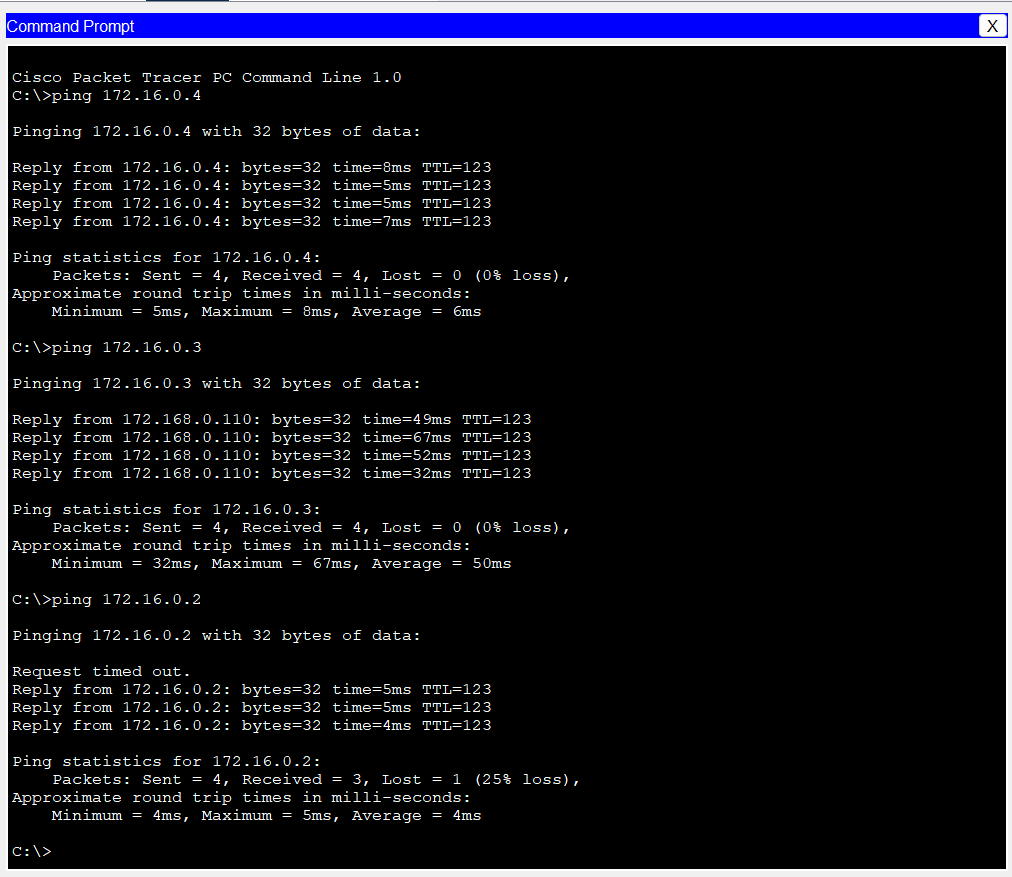


Figure 4.Ping A1 to A2

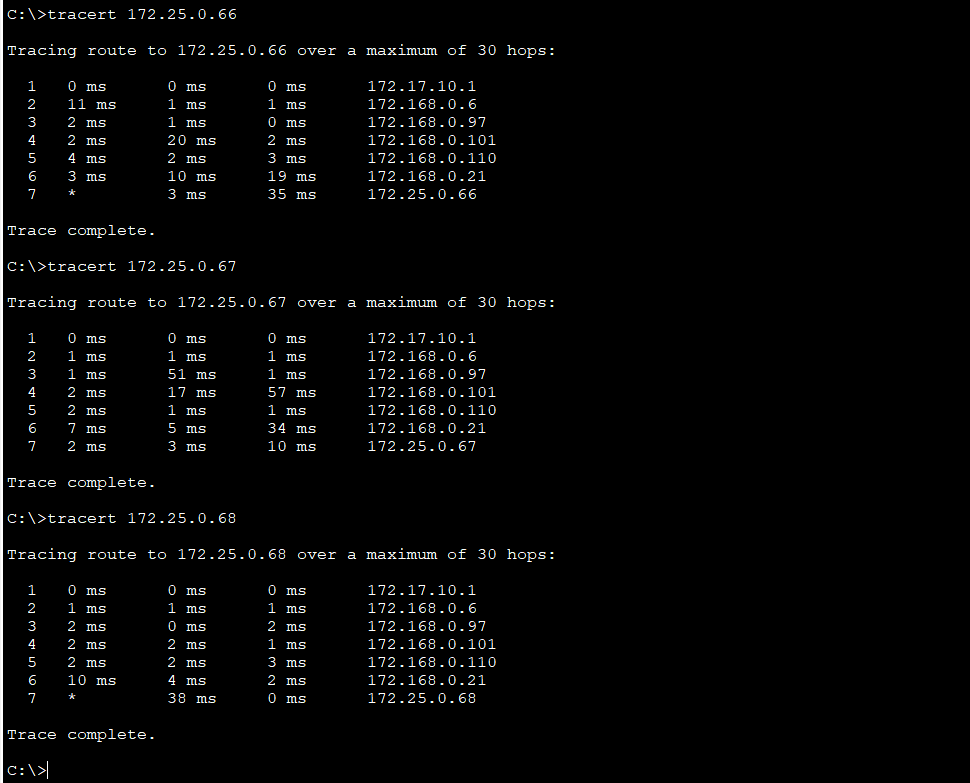


Figure 5.Ping A2 to A3

## AREA 1 to AREA 3:

ACL is implemented on Area 3.

## AREA 1to AREA 4:

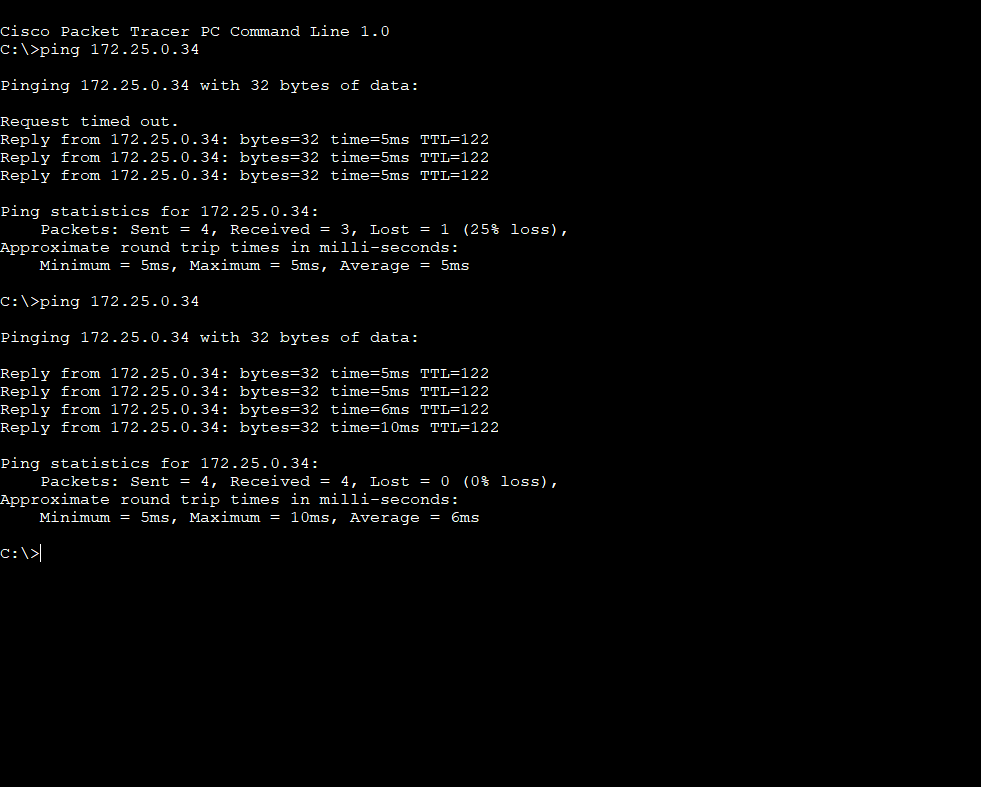


Figure 6. Ping A1 to A4

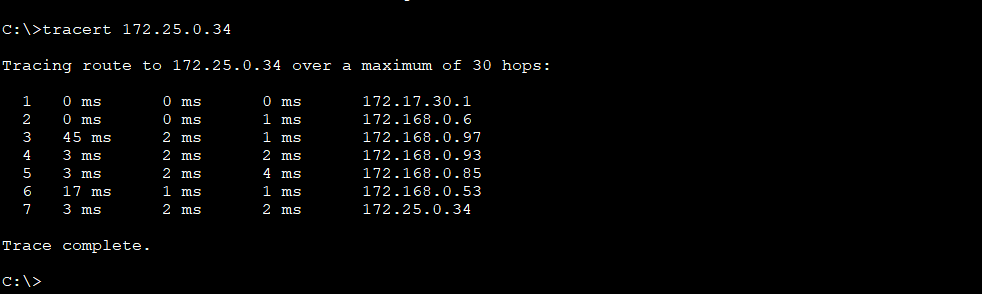


Figure 7.Trace A1 to A5

## AREA 1 to AREA 5:

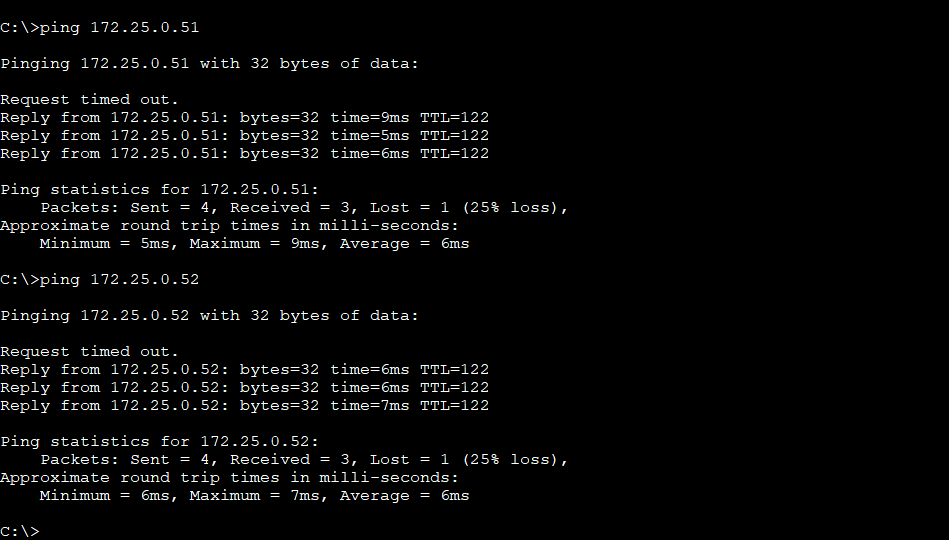


Figure 8. Ping A1 to A5

## AREA 2 to AREA 3:

ACL is implemented on Area 3.

A screen shot of a computer

Description automatically generated with low confidence

Figure 9. Ping A2 to A3

## AREA 2 to AREA 4:

ACL is implemented

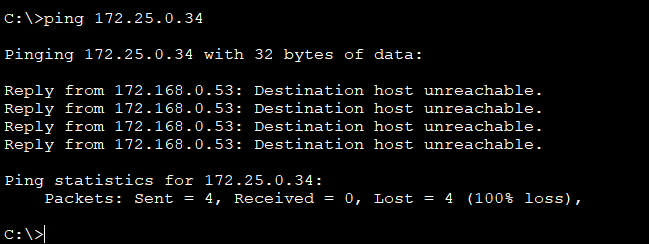


Figure 10.Ping A2 to A4

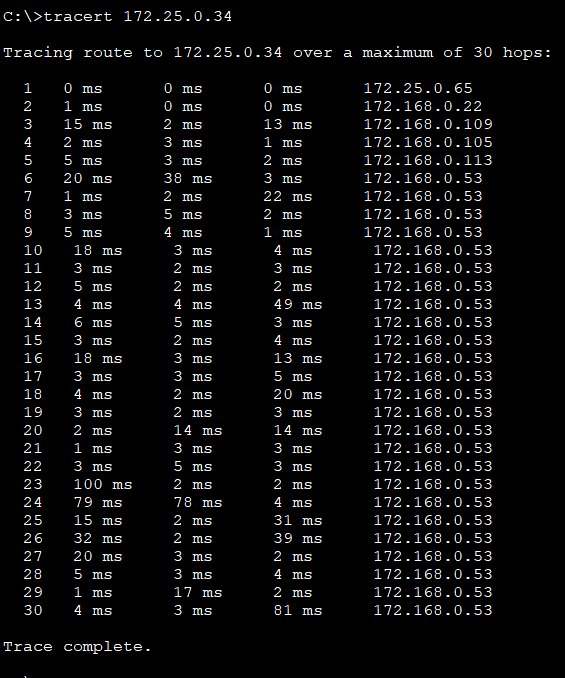


Figure 11. Tracert A2 to A3

## AREA 2 to AREA 5:

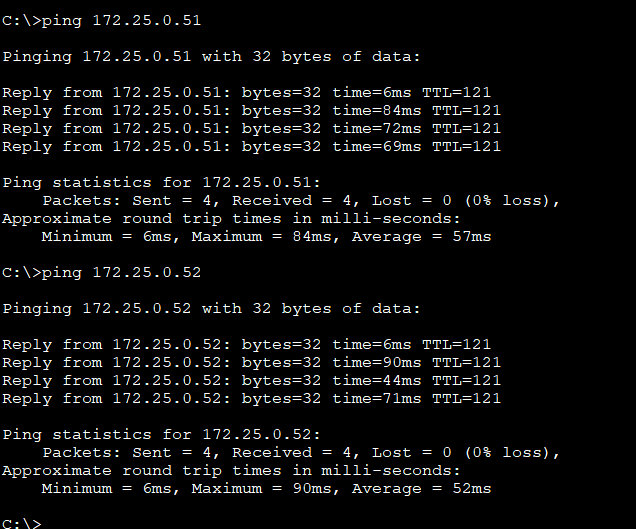


Figure 12Ping A2 to A5

A screenshot of a computer

Description automatically generated with medium confidence

Figure 13.Tracert A2 to A5

## AREA 3 to AREA 4:

ACL implemented (Connectivity not possible).

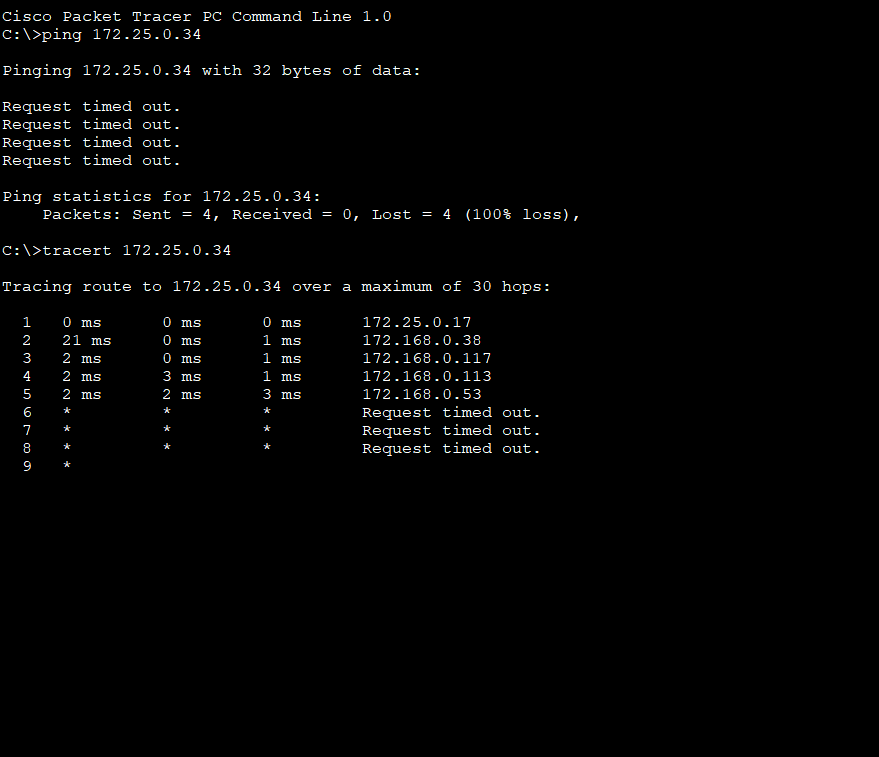


Figure 14. tracert Ping A3 to A4

## AREA 3 to AREA 5:

ACL implemented on AREA 3.

## AREA 4 to AREA 5:

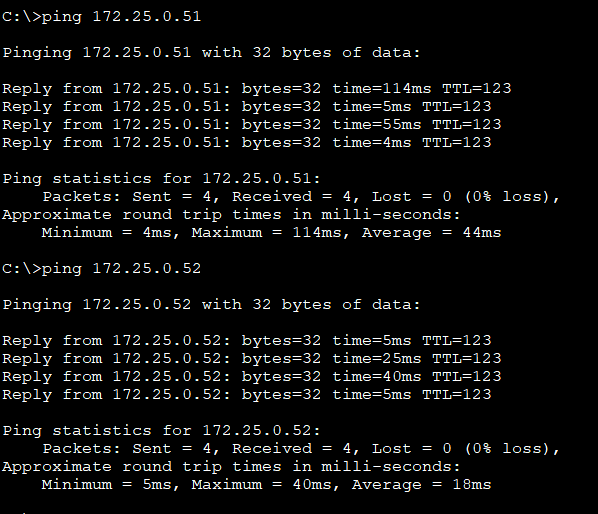


Figure 15. Ping A4 to A5

A screenshot of a computer

Description automatically generated with medium confidence

Figure 16.Tracert A4 to A5

# Servers’ operability report:

## HTTP

HTTP address 172.168.0.110

### AREA 1 to 4:

A screenshot of a computer

Description automatically generated with medium confidence

### AREA 5:

Can’t access http because of Extended ACL

A picture containing text, software, line, screenshot

Description automatically generated

## DNS

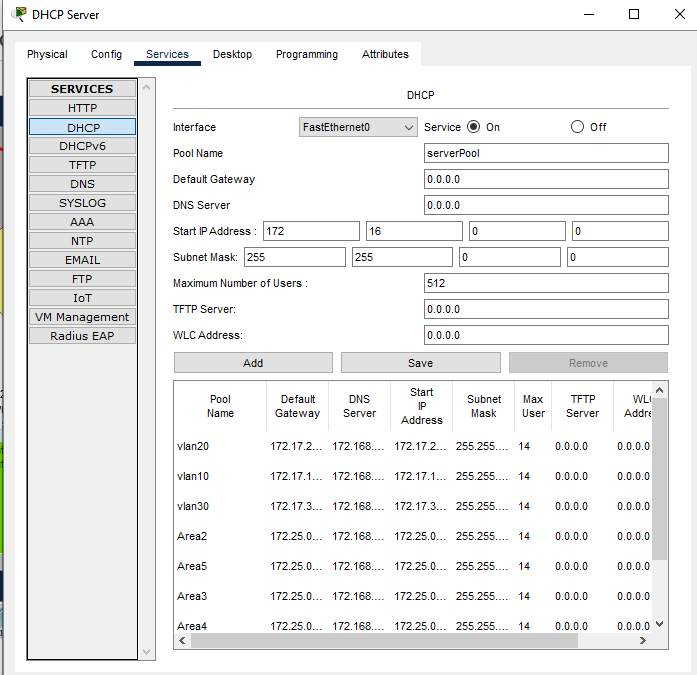
Website name is **hi**. Whose address is 172.168.0.110

A screenshot of a computer

Description automatically generated with medium confidence

## DHCP

Pools of All areas are configured.



### PC13 From AREA 1:

A screenshot of a computer

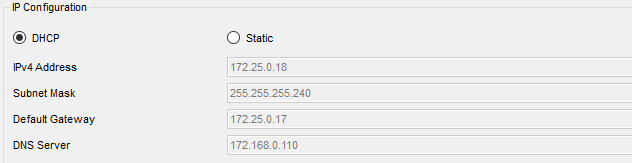
Description automatically generated with medium confidence

### PC8 From AREA 2:

A screenshot of a computer

Description automatically generated with medium confidence

### PC6 From AREA 3:



### PC1 From AREA 4:

A screenshot of a computer

Description automatically generated with medium confidence

### PC4 From AREA 5:

A screenshot of a computer

Description automatically generated with medium confidence

# ALTERNTIVE IMPLEMENTATION METHODS:

1: other routing protocols such as RIP can be used instead of OSPF

2: PAT can be used not translation of servers’ private address to public instead of NAT.

# APPENDIX:

## ROUTER:

### Basic Configurations:

Config t

hostname R ….

enable secret …..

enable password ……

### For Securing console and virtual line:

Config t

line con 0

password cisco

login

line aux 0

line vty 0 15

password cisco

login

### OSPF:

Config t

router ospf process id

**network** IP address wildcard mask **area** number

### For VLANs:

interface FastEthernet0/0.10

encapsulation dot1Q 10

ip address 172.17.10.1 255.255.255.0

## SWITCHES FOR VLANS:

Perform basic configurations like routers before

Config t

vlan id

vlan name

interface ………… // to change ports to vlans

switchport mode access

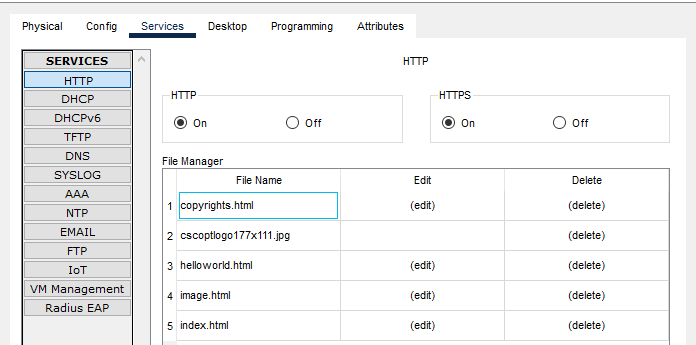
switchport access vlan id

## SERVERS:

### HTTP:

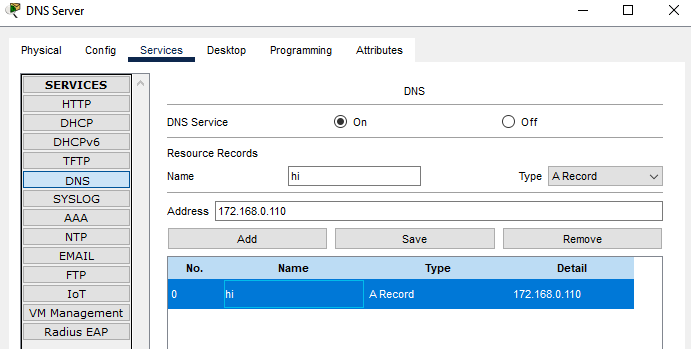
Go to services -> HTTP. Create a new file. Or you can edit the previous one.

I created helloworld.html



### DNS:

On DNS server go to services. Write name and it’s address



### DHCP:

Interface ………………

ip helper-address 172.168.0.110

on routers links connected to LANs

## NAT:

### For DHCP:

ip nat inside source static 172.16.0.3 172.168.0.110

### For HTTP:

ip nat inside source static tcp 172.16.0.4 80 172.168.0.110 80

### For DNS:

ip nat inside source static udp 172.16.0.2 53 172.168.0.110 53

## ACL:

### On router 12 to make area 3 secure:

config t

access-list 10 deny 172.25.0.48 0.0.0.15

access-list 10 deny 172.25.0.32 0.0.0.15

access-list 10 deny 172.25.0.64 0.0.0.15

access-list 10 deny 172.16.0.0 0.0.255.255

access-list 10 deny 172.17.0.0 0.0.255.255

access-list 10 permit any

interface FastEthernet0/0

ip access-group 10 out

### On R8 so AREA 2 won’t Access PC1:

config t

access-list 1 deny 172.25.0.64 0.0.0.15

access-list 1 permit any

interface FastEthernet0/0

ip access-group 1 out

## EXTENDED ACL:

Config t

access-list 101 deny tcp 172.25.0.48 0.0.0.15 any eq 80

access-list 101 permit ip any any

interface FastEthernet0/0

ip access-group 101 out