Network Infrastructure

BFE Students Graduation Project

Benha University
Benha Faculty of Engineering
Electrical Engineering Department

Computer Network Infrastructure with Security

Graduation Project

By
Team members

Abdelrahman Mohamed Mohamed

Abdelrahman Ayman Abualmaaty

Abdulrahim Mohamed Abdulrahim

Shaimaa El-Shafei AbdelGauad

Mohamed Reda Ahmed

Salah Ehab Mohamed

Abdullah Atef Eid

Supervised by

Dr/ Eman Salem

Electrical Engineering Department
Faculty of Engineering
Benha University

2021

Contents

Table of Figures

Acknowledgement

We gift this book for our faculty BFE and thank God for studying in it under its great staff, also we thank Dr\ Eman Salem and Dr/ Sara Hamdy for helping us in this book and the project described in it.

Also, we want to thank our families for helping us to bypass this step in our life and they are very patient for each of us.

Abstract

This project is designed to make a networking infrastructure system with some of security devices to make a private network and public network for a company that has three multiple departments and multiple branches as we made in the project.

We implemented connection between departments using routing and switching then connecting branches together using WAN technology like MPLS.

In this project, devices can reach or call each other according to the rules for each department in the company that added by firewalls.

Also, devices inside the network can access internet but that depends on the department which internet has a lot of websites so, through a firewall we could filters on the department to allow only needed websites to be accessible only and blocking other websites like Facebook, video websites, YouTube, and stream websites like TeamViewer.

List of Abbreviations

ADDC	Active Directory Domain Controller
MS	Microsoft
DC	Domain Controller
GPO	Group Policy Organization
IP	Internet Protocol
HTTP	Hyper Text Transfer Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
WAN	Wide Area Network
ICMP	Internet Control Message Protocol
NAT	Network Address Translation
DNS	Domain Name Server
DHCP	Dynamic Host Configuration Protocol
VTY	Virtual Terminal Line
VLAN	Virtual Local Area Network
MAC	Media Access Control Address
EIGRP	Enhanced Interior Gateway Routing Protocol
HSRP	Hot Standby Router Protocol
VRRP	Virtual Router Redundancy Protocol
GLBP	Gateway Load Balancing Protocol
MPLS	Multi-Protocol Label Switching
DSL	Digital Subscriber Line
ADSL	Asymmetric Digital Subscriber Line
SDSL	Symmetric Digital Subscriber Line

VoIP	Voice Over Internal Protocol
FEC	Forward Error Correction
TTL	Time To Live
LFIB	Label Forwarding Information Base
GRE	Generic Routing Encapsulation
QoS	Quality of Service
BC	Broadcast
STP	Spanning Tree Protocol

Introduction

In this Chapter we will discuss about the network in general and its importance in our life. Network is the most important thing was made in the previous century, without computer network people would not be able to communicate to each other remotely. Working or chatting remotely saves our time and effort for implementing some jobs like sending mails or reports for head PM in a project.

0.1 History [12]

Computer networking may be considered a branch of computer science, computer engineering, and telecommunications since it relies on the theoretical and practical application of the related disciplines. Computer networking was influenced by a wide array of technology developments and historical milestones.

- In the late 1950s, a network of computers was built for the U.S. military Semi-Automatic Ground Environment (SAGE) radar system using the Bell 101 modem. It was the first commercial modem for computers, released by AT&T Corporation in 1958. The modem allowed digital data to be transmitted over regular unconditioned telephone lines at a speed of 110 bits per second (bit/s).
- In 1959, Christopher Strachey filed a patent application for time-sharing and John McCarthy initiated the first project to implement time-sharing of user programs at MIT. Strachey passed the concept on to J. C. R. Licklider at the inaugural UNESCO Information Processing Conference in Paris that year. McCarthy was instrumental in the creation of three of the earliest time-sharing systems (Compatible Time-Sharing System in 1961, BBN Time-Sharing System in 1962, and Dartmouth Time Sharing System in 1963).
- In 1959, Anatolii Ivanovich Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organization of the control of the Soviet armed forces and of the Soviet economy based on a network of computing centers, the OGAS.
- In 1960, the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes.
- In 1963, J. C. R. Licklider sent a memorandum to office colleagues discussing the concept of the "Intergalactic Computer Network", a computer network intended to allow general communications among computer users.
- Throughout the 1960s, Paul Baran and Donald Davies independently developed the concept of packet switching to transfer information between computers over a network. Davies pioneered the implementation of the concept. The NPL network, a local area network at the National Physical Laboratory (United Kingdom) used a line speed of 768 kbit/s and later high-speed T1 links (1.544 Mbit/s line rate).
- In 1965, Western Electric introduced the first widely used telephone switch that implemented computer control in the switching fabric.
- In 1969, the first four nodes of the ARPANET were connected using 50 kbit/s circuits between the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah. In the early 1970s,

Leonard Kleinrock carried out mathematical work to model the performance of packet-switched networks, which underpinned the development of the ARPANET. His theoretical work on hierarchical routing in the late 1970s with student Farouk Kamoun remains critical to the operation of the Internet today.

- In 1972, commercial services were first deployed on public data networks in Europe, which began using X.25 in the late 1970s and spread across the globe. The underlying infrastructure was used for expanding TCP/IP networks in the 1980s.
- In 1973, the French CYCLADES network was the first to make the hosts responsible for the reliable delivery of data, rather than this being a centralized service of the network itself.
- In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii. In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks" and collaborated on several patents received in 1977 and 1978.
- In 1974, Vint Cerf, Yogen Dalal, and Carl Sunshine published the Transmission Control Protocol (TCP) specification, RFC 675, coining the term Internet as a shorthand for internetworking.
- In 1976, John Murphy of Datapoint Corporation created ARCNET, a token-passing network first used to share storage devices.
- In 1977, the first long-distance fiber network was deployed by GTE in Long Beach, California.
- In 1977, Xerox Network Systems (XNS) was developed by Robert Metcalfe and Yogen Dalal at Xerox.
- In 1979, Robert Metcalfe pursued making Ethernet an open standard.
- In 1980, Ethernet was upgraded from the original 2.94 Mbit/s protocol to the 10 Mbit/s protocol, which was developed by Ron Crane, Bob Garner, Roy Ogus, and Yogen Dalal.
- In 1995, the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of 1 Gbit/s. Subsequently, higher speeds of up to 400 Gbit/s were added (as of 2018). The scaling of Ethernet has been a contributing factor to its continued use.

0.2 Our project

After the previous history of the network, we will start in the project in this book. In our project we discussed about the infrastructure of the computer network that is the backbone of any web-based application that we can use in our daily life like WhatsApp and messenger, but we focus on or take an example for a company with 4 departments IT, SALES, PR, and HR also the company has headquarter and many branches over the network like branch in Cairo and Aswan, we talk about how these departments will communicate with each other and how each branch will reach another one, taking in the mind the security issues that we will face from inside and outside the network.

Chapter 1 Switching

1.1 Basic switch configuration

a Cisco switch is a much simpler network device compared with other devices (such as routers and firewalls for example). The Cisco switch needs some initial basic configuration to enable management, security, and some other important features.

Connect to the device via console: Use a terminal emulation software such as PuTTY and connect to the console of the switch. You will get the initial command prompt "Switch>"

Type "enable" and hit enter. You will get into privileged EXEC mode ("Switch#")
Now, get into Global Configuration Mode: [13]

```
Switch>ena
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Figure 1-1 . Accessing global configuration

Set up a hostname for the switch to distinguish it in the network:

```
Switch(config)#hostname SW1
SW1(config)#
```

Figure 1-2 Assign hostname for switch.

There are some useful commands that used to monitor your configuration or troubleshoot possible problems:

access-switch1#show run

(Displays the current running configuration)
access-switch1#show interfaces
(Displays the configuration of all interfaces and the status of each one)
access-switch1#show VLAN
(Displays all VLAN numbers, names, ports associated with each VLAN etc)
access-switch1#show interface status
(Displays status of interfaces, speed, duplex etc)
access-switch1#show mac address-table
(Displays current MAC address table and which MAC address is learned on each interface)
Save the configuration:[1]

```
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 1-3 Save configuration.

1.2 Cisco switch Password Settings

The types of passwords used in securing a CISCO switches.

- Passwords are the first line of defense for securing Cisco switches.
- There are five password types that can be configured on a Cisco switches:
  - **Privileged Level Passwords (Privilege EXEC):**

    Enable Password (not encrypted)
    Enable Secret Password (encrypted password)

```
SW1(config)#enable secret 1234
```

Figure 1-4 Encrypted privilege password.

We use 'enable secret' instead of 'enable password' to encrypt the password in the 'show running configuration' but we can encrypt also the enable password by activating the password encryption service.

- **Console Line Password**

```
Switch(config)#lin con 0
Switch(config-line)#password 1234
Switch(config-line)#login
Switch(config-line)#
```

Figure 1-5 Console password.

- **VTY Lines Password**

  First, we need to make the switch can be accessed by telnet then assign the password.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.0.0.4 255.0.0.0
Switch(config-if)#no shutdown
Switch(config-if)#lin vty 0 4
Switch(config-line)#password 12345
Switch(config-line)#ogin local
```

Figure 1-6 Telnet password

To access the switch by telnet: open command prompt and type telnet then the address of the VLAN 1 of the switch.[1]

1.3 VLAN configuration [8]

A VLAN is a group of end stations in a switched network that is logically segmented by function, team, or application, regardless to the physical locations of the users. VLANs have the same

attributes as physical LANs, but you can group end stations even if they are not physically connected to the same switch. VLANs are numbered from 1 to 4094 (extended range). All configured ports belong to the default VLAN when you first bring up the switch. The default VLAN (VLAN1) uses only default values, and you cannot create, delete, or suspend activity in the default VLAN. You can create a VLAN by assigning a number to it; you can delete VLANs as well as moving them from the active operational state to the suspended operational state. If you attempt to create a VLAN with an existing VLAN ID, the switch goes into the VLAN sub mode but does not create the same VLAN again.[2]

To create VLAN:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name first
```

Figure 1-7 Creation of VLAN.

Note: The name in above configuration is optional but helps administrator to keep config clean.

To assign an ethernet interface to a VLAN:

```
Switch(config)#interface f0/1
Switch(config-if)#switchport access vlan 10
```

Figure 1-8 Assign specified interface to VLAN.

Verifying the VLAN:

```
Switch#show vlan
```

Figure 1-9 Verify VLAN.

1.4 DHCP Attacks

DHCP Starvation Attack: a DHCP starvation attack is where a DHCP server is sent so many DHCP requests that eventually there are no more IP addresses available to allocate to legitimate devices, hence rendering the network unusable. A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. The result may involve the attacker installing their own DHCP server and responding to a client request for an IP address, which will result in data being sent to the wrong destination, thus compromising company data. Because DHCP responses typically include default gateway and DNS server information, the network attacker can supply their own system as the default gateway and DNS server, resulting in a man-in-the-middle-style attack [3].

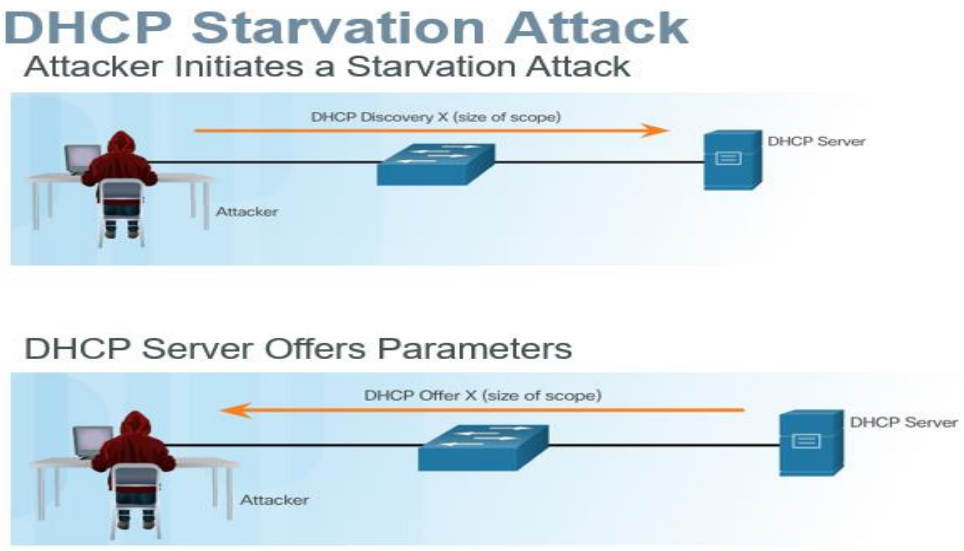


Figure 1-10 DHCP starvation attack (1)

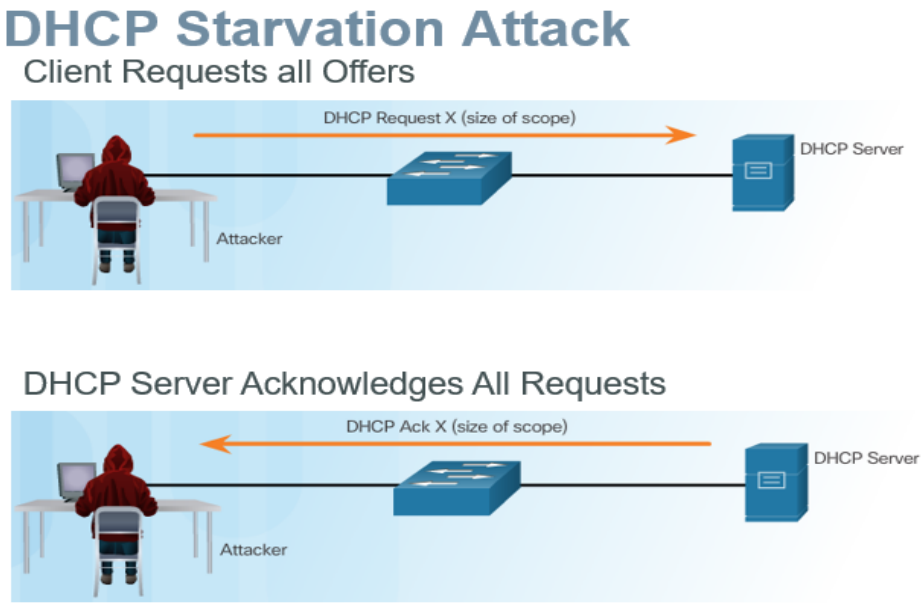


Figure 1-11 DHCP starvation attack (2)

Live Attack Phase:

- **Requirements**:
  Kali Linux Operating System
  Yersinia Tool

  Yersinia tool is an inbuilt tool in kali Linux, in fact it is a hidden tool, we need to install it with apt install yersinia command.

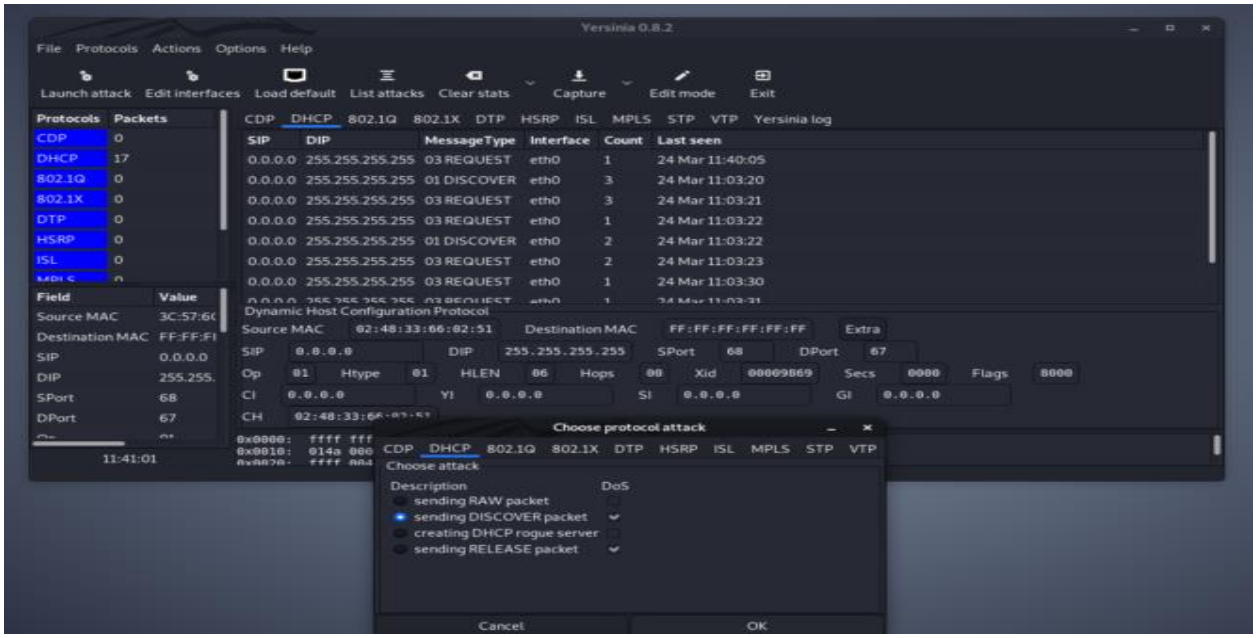


Figure 1-12 Yersinia tool.

1.5 DHCP Snooping

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers and protects from DHCP starvation attack (Denial of service attack). The DHCP snooping feature performs the following activities:

• Validates DHCP messages received from untrusted sources and filters out invalid messages.
• Rate-limits DHCP traffic from trusted and untrusted sources.
• Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
• Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

- **Configuration DHCP snooping example:**

Figure 1-13 Snooping reference topology.

```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)#
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)#
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)#
```

Figure 1-14 configure a Maximum number of MAC address.

1.6 Port Security

Port Security helps secure the network by preventing unknown devices from forwarding packets. You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted. [4]

There are three methods to determine the MAC addresses for each port.

1-Sticky Method.

Sticky secure MAC addresses are a hybrid. They are learned dynamically from the devices connected to the switchport, are put into the address table, AND are entered into the running configuration as a static secure MAC address (sometimes referred to as a static sticky MAC address). [5]

```
Switch(config)#interface f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

Figure 1-15 Sticky method configuration.

To remove the sticky MAC addresses.

```
Switch(config-if)#no switchport port-security sticky aaaa.aaaa.aaaa
```

Figure 1-16 Remove sticky MAC.

2-Maximum MAC Methods

This method that determines the maximum MAC addresses connected to the port if the maximum number exceeded port security violation action takes place. Dynamically learn MAC addresses. Add to MAC table and running configuration.[5]

```
Switch(config)#interface f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 10
```

Figure 1-17 Maximum MAC configuration.

3-Static MACs.

Static secure MAC addresses are statically configured on each switchport and stored in the address table. The configuration for a static secure MAC address is stored in the running configuration by default and can be made permanent by saving them to the startup configuration.[5]

```
Switch(config)#interface f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address abcb.d544.333
```

Figure 1-18 Static MAC configuration.

Port security violation actions.

there are two situations that can cause a violation, these two situations include:

- When the maximum number of secure MAC addresses has been added to a switchport's address table and traffic from another MAC address is received on the switchport.[5]
- When an address that has been seen on a secure switchport has already been seen on another secure switchport in the same VLAN.

There are three different main violation types: shutdown, protect, and restrict. These are described in more detail below:

- **Shutdown**.
  When a violation occurs in this mode, the switchport will be taken out of service and placed in the **err-disabled** state. The switchport will remain in this state until manually removed; this is the default switchport security violation mode.[5]

- **Protect**.
  When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. When using this mode, no notification message is sent when this violation occurs.[5]

- **Restrict**.

When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. However, unlike the protect violation type, a message is also sent indicating that a violation has occurred. We will use this mode in our project because we do not want the port to shutdown and if violation occurs, we need to know.[5]

Commands for each violation mode:

```
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#switchport port-security violation restrict
```

Figure 1-19 Violation mode commands.

Verify port security state and addresses.

```
Switch#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Figure 1-20 Verify port security.

```
Switch#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Figure 1-21 Verify port security for specified interface.

1.7 IP source guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that

assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports. The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.[6]

From the previous words we know now that IP source guard protects from the following attacks.

- Reserve All IP Range Attack.
- IP Spoofing Attack.
- IP Conflict Attack.

The violation action is dropping unknow IP.

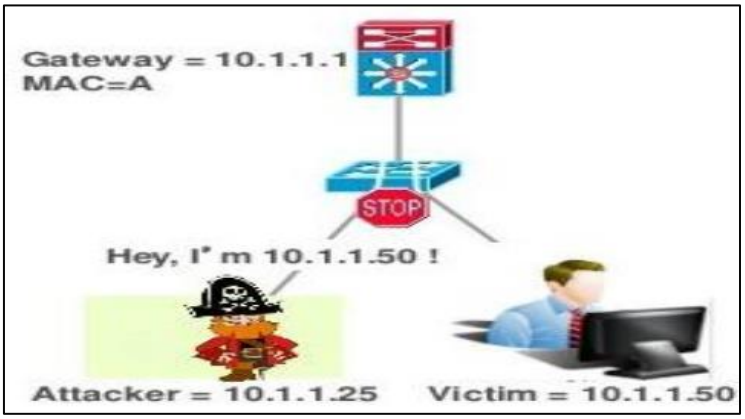


Figure 1-22 Spoofing IP address.

1.8 Configuration IP source guard.

For the untrusted ports:

```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

Figure 1-23 IP source guard configuration.

For the static IP devices.

- Disable IP Source Guard.
- or add Manual Entry in Binding Table.

```
Switch(config)#ip dhcp snooping binding {mac} vlan{#} {IP} interface f0/0
```

Figure 1-24 Adding device in binding table.

- or add Manual Entry in IP Source Table.

```
Switch(config)#ip dhcp source binding {mac} vlan{#} {IP} interface f0/0
```

Figure 1-25 Adding device to IP source table.

For the snooping Trusted ports and ports between switches.

- disable IP source guard.

1.9 Errdisable state

Errdisable is a feature that automatically disables a port on a Cisco Catalyst switch. When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port. The error disabled feature is supported on most Catalyst switches running the Cisco IOS software. [7]

Errdisable recovery.

The errdisable recovery command allows you to choose the type of errors that automatically reenable the ports after a specified amount of time. The show errdisable recovery command shows the default error-disable recovery state for all the possible conditions.

```
conf t
 errdisable recovery cause dhcp-rate-limit
                                default recovery time 300 sec
 errdisable recovery interval {time in sec}
```

Figure 1-26 Errdisable recovery.

1.10 Trunking [9]

A trunk is a **point-to-point** link between two network devices that carry more than one VLAN. With VLAN trunking, you can extend your configured VLAN across the entire network. Most Cisco switches support the IEEE 802.1Q used to coordinate trunks on Fast Ethernet and Gigabit Ethernet. Trunks are required to carry VLAN traffic from one switch to another. [8]

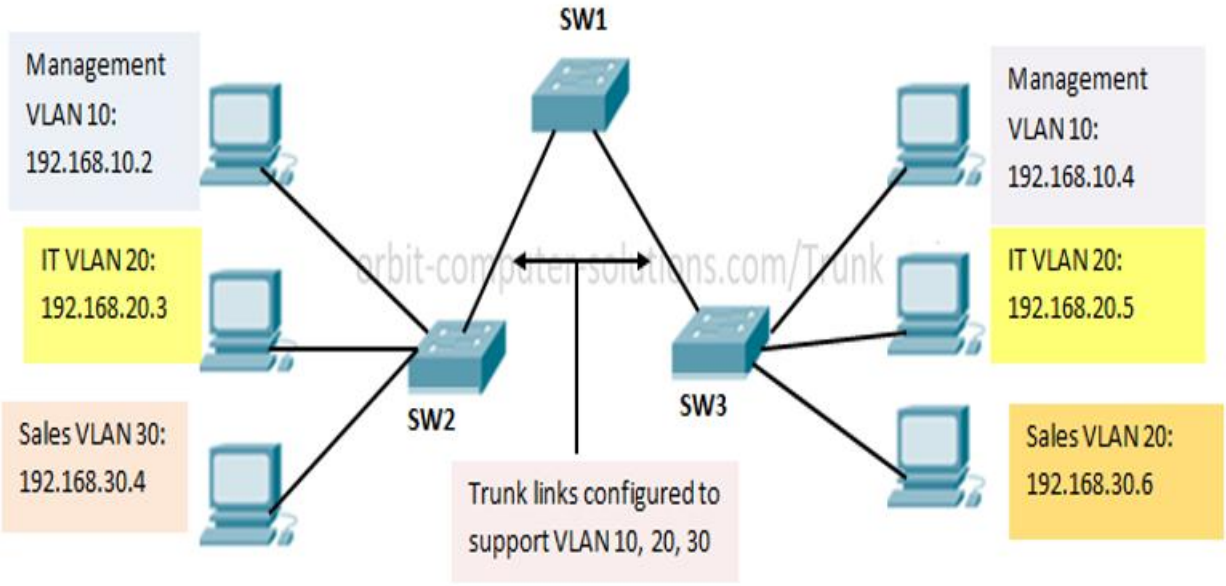


Figure 1-27 VLAN trunking.

1.11 How to Configure a Trunk Port [10]

To configure a switch port as a trunk link, use the switchport mode trunk command. This command puts the interface into permanent trunking mode and negotiates to convert the neighboring switch or links into trunk links.

Note: A trunk port is a port that is configured to carry traffic for all the VLANs on a switched network, Trunk ports mark frames traffic with unique identifying tags – either 802.1Q tags or Inter-Switch Link (ISL) tags as they move between switches.

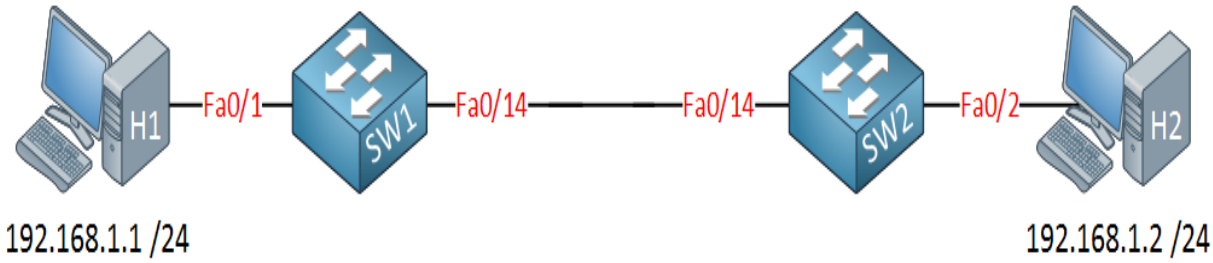


Figure 1-28 Basic trunking topology.

```
SW1(config)#interface fa0/14
```

Figure 1-29 accessing interface.

This is where you can choose between 802.1Q or ISL encapsulation. By default, our switch will negotiate about the trunk encapsulation type.

```
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
```

Figure 1-30 Trunking configuration (1)

The next step is to create a trunk between the two switches. Technically the interfaces between the two switches can also be in access mode right now because I only have a single VLAN.

```
SW2(config)#interface fa0/14
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
```

Figure 1-31 trunking configuration (2).

Chapter 2 Routing

2.1 Routing

Routing is the process your computer uses to send a packet between different subnets. If you want to connect to a computer that is on a different subnet than your own, your computer must forward data packets to a router. A router is the software and hardware responsible for delivering packets between two subnets. Each router uses an internal routing table to determine the best path to send a packet.

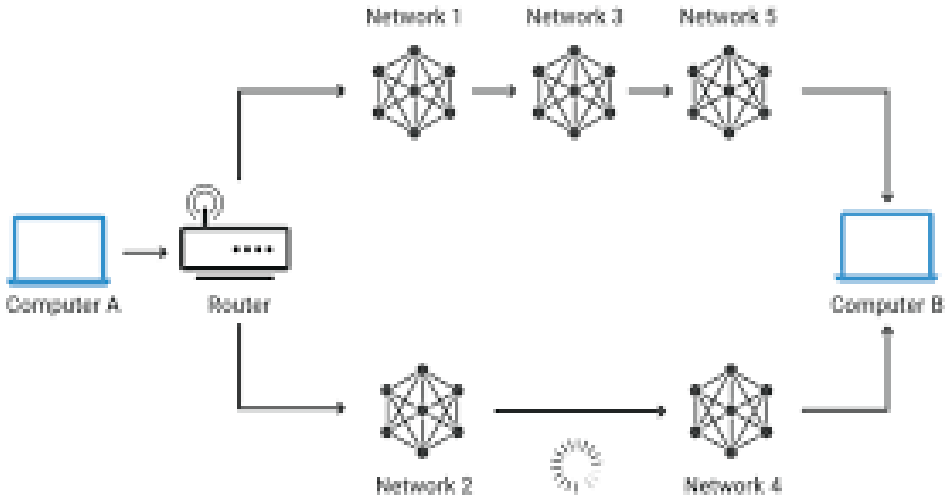


Figure 2-1 Network

2.2 How does routing work?

- Routers refer to internal routing tables to make decisions about how to route packets along network paths. The routing table records the paths that packets must take to reach each destination for which the router is responsible. Think of train schedules, which train passengers consult to decide which train to catch. Routing tables are like that, but for network paths rather than trains.
- A routing table is a set of rules, often presented in a table format, that are used to determine where data packets traveling over an Internet Protocol (IP) network will be routed. All IP-enabled devices, including routers and switches, use routing tables.
- The routing table contains the information needed to forward a packet along the best path to its destination. Each package contains information about its origin and destination. When a packet is received, the network device scans the packet and matches it with the routing table entry providing the best match for its destination. The table then provides the device with instructions to send the packet to the next hop on its path over the network.

2.3 Types of routing:

1- Static routing
2- Dynamic routing

2.4 Static Routing

The term static routing denotes the use of manually configured or injected static routes for traffic forwarding purposes. Using a static route might be appropriate in the following circumstances:

1- When it is undesirable to have dynamic routing updates forwarded across slow bandwidth links ,such as a dialup link

2-When the administrator needs total control over the routes used by the router
3-When a backup to a dynamically learned route is necessary
4-When it is necessary to reach a network that is accessible by only one path (a stub network)

Configuring and maintaining static routes is time-consuming. Properly implementing static routes requires complete knowledge of the entire network.

2.5 Dynamic Routing

Dynamic routing allows the network to adapt to changes in the topology automatically, without administrator intervention. A static route cannot respond dynamically to changes in the network.

If the link fails, the static path is no longer valid if it is configured to use this failed link, so a new static path must be configured. If a new router or link is added, this information should also be added.

It is configured on every router in the network. In a very large or unstable network, these changes can result in a significant effort for network administrators. It can also take a long time for each router in the network to receive the correct information.

In such cases, it may be better for routers to receive information about networks and links from each other using dynamic routing protocol.

2.6 Routing protocol

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way ,routers gain knowledge of the topology of the network. The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table. If the network is directly connected, then the router already knows how to get to the network. If the networks are not attached, the router must learn how to get to the remote network with either static routing) administrator manually enters the routes in the router's table) or dynamic routing (happens automatically using routing protocols like EIGRP, OSPF, etc.).

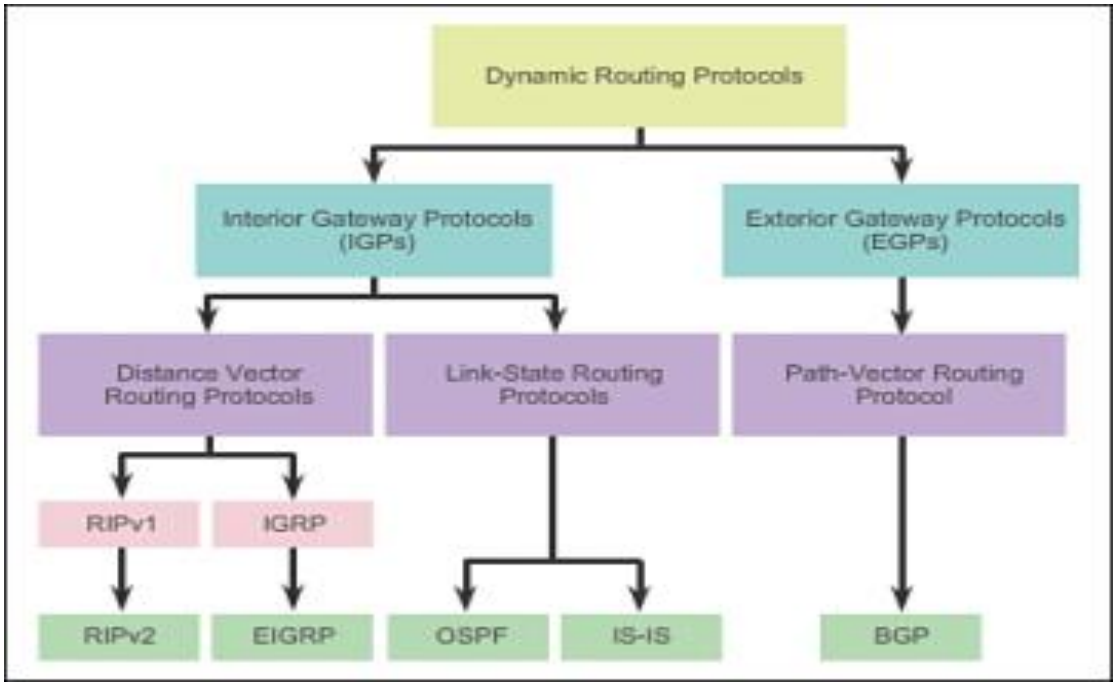


Figure 2-2 Dynamic router protocols.

2.7 Comparing Routing Protocols

	Distance Vector		Link-State			
	RIPv1	**RIPv2**	**IGRP**	**EIGRP**	**OSPF**	**IS-IS**
Speed of Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability – Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Figure 2-3 Comparison between protocols.

2.8 Routing Information Protocol (RIP)

Is a standards-based, distance-vector ,interior gateway protocol (IGP) used by routers to exchange routing information. RIP uses hop count to determine the best path between two locations. Hop count is the number of routers the packet must go through till it reaches the destination network. The maximum allowable number of hops a packet can traverse in an IP network implementing RIP is hops 15.

it has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed**.**

In a RIP network, each router broadcasts its entire RIP table to its. neighboring routers every 30 seconds. When a router receives a neighbor's RIP table, it uses the information provided to update its neighbors. routing table and then sends the updated table its

2.8.1 Differences between RIPv1 and RIPv2

RIPv1This is a simple distance vector protocol. It has been enhanced with various techniques, including Split Horizon and Poison Reverse in order to enable it to perform better in somewhat complicated networks. A class full protocol, broadcasts updates every 30 seconds ,hold-down period 180 seconds .Hop count is metric) Maximum15.

RIPv2 this version added several new features. RIPv2 uses multicasts, version 1 use broadcasts, RIPv2 supports triggered updates—when a change occurs, a RIPv2 router will immediately propagate its routing information to its connected neighbors. RIPv2 is a classless protocol. RIPv2 supports variable-length subnet masking (VLSM(RIPv2 supports authentication. You can restrict what routers you want to participate in RIPv2 .This is accomplished using a hashed password value.

2.8.2 RIP configuration

router (config)# host name R8

R8 (config)# enable secret 8888

```
hostname R8
!
!
!
enable secret 5 $1$mERr$O5OWki0IzrtCwK7.IvWqR/
```

Figure 2-4 Assigning hostname for a router.

R8 (config)# IP domain name project.com

R8 (config)# IP name server 192.168.2.7

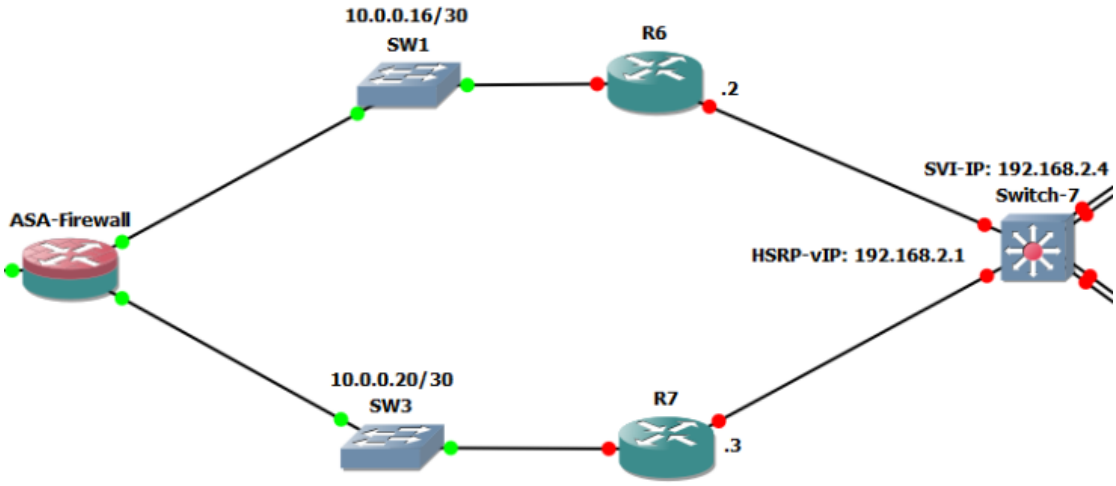


Figure 2-5 RIP Configuration.

R8 (config)# router rip

R8 (config-router) # network 192.168.2.3

R8 (config-router) # network 10.0.0.15

R8 (config-router) # version 2

```
Router#ping 10.0.0.18

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.18, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

Router#
```

Figure 2-6 Successful ping on 10.0.0.18.

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 17 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          10.0.0.0
          192.168.2.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
          10.0.0.21            120      00:00:13
Distance: (default is 120)
```

Figure 2-7 IP Protocols.

2.9 Open Shortest Path First (OSPF) [4]

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).

2.9.1 OSPF configuration [5]

Router (config) # hostname R4

R4 (config) # enable secret 4444

R4 (config) # IP domain name project.com

R4 (config) # IP name server 192.168.2.7

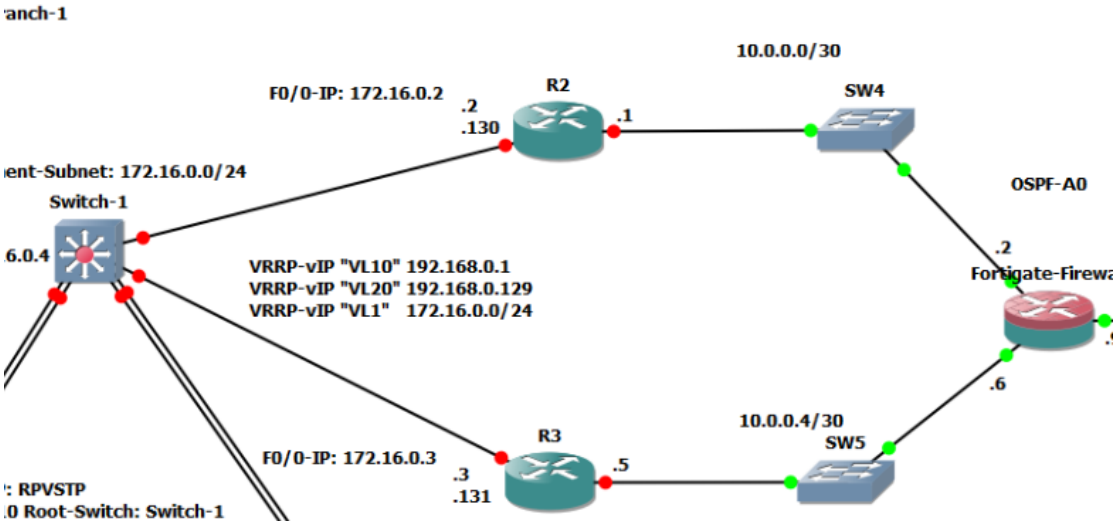


Figure 2-8 OSPF network connections.

router OSPF 100

network 10.0.0.6 0.0.0.0 area 0.0.0.0

network 10.0.0.2 0.0.0.0 area 0.0.0.0

```
Router#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figure 2-9 Successful ping

```
Router#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.0.0.9
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.9 0.0.0.0 area 0
    10.0.0.2 0.0.0.0 area 0
    10.0.0.6 0.0.0.0 area 0
```

Figure 2-10 OSPF run configuration.

2.10 Enhanced Internal Gateway Routing Protocol (EIGRP) [6]

Enhanced Inner Gateway Routing Protocol (EIGRP) is a hybrid routing protocol which provides significant improvements to IGRP. EIGRP replaced IGRP in 1993 since then The Internet Protocol is designed to support IPv4 addresses that IGRP cannot support. Hybrid The routing protocol includes the advantages of both link-state routing and vector-distance routing Protocols, it was based on the distance vector protocol but has more link-state features protocol. EIGRP saves all paths instead of the best path to ensure faster convergence. EIGRP maintains contiguous routing tables and only exchanges contiguous information will not contain. EIGRP is commonly used in large networks, and it only updates when there is a file.The architecture changes but does not differ periodically from older distance vector protocols such as RIP.

2.10.1 EIGRP configuration [7]

Router (config)# hostname R17

R17 (config)# enable secret 1717

R17 (config)# IP domain name project.com

R17 (config)# IP name server 192.168.2.7

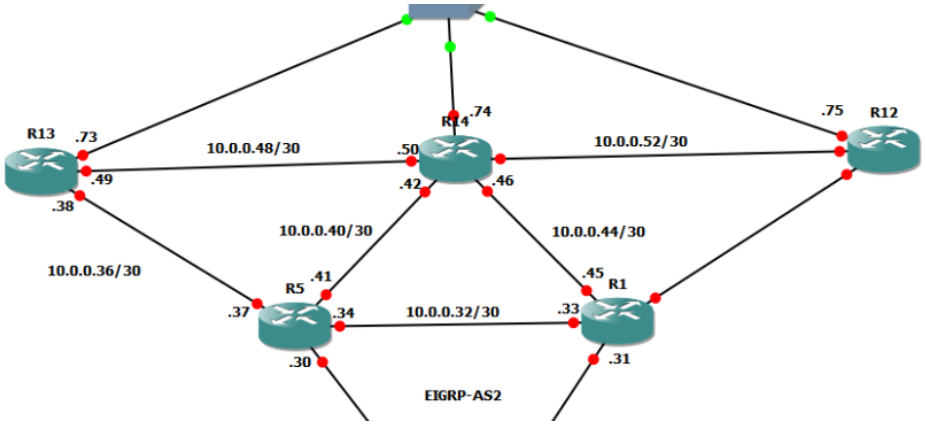


Figure 2-11 EIGRP network connection

R17 (config)#router EIGRP 1

R17 (config-router) #network 10.0.0.25

R17 (config-router) #network 10.0.0.34

R17 (config-router) #network 10.0.0.46

```
Router#ping 10.0.0.74

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.74, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figure 2-12 Successful ping

```
Router#show ip protocols

Routing Protocol is "eigrp  1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.34         90            5393648
    10.0.0.46         90            5394097
    10.0.0.25         90            5394420
  Distance: internal 90 external 170
```

Figure 2-13 IP Protocols

2.11 Route redistribution [3]

Figure 2-14 shows that the EIGRP in section 1 is redistributed into OSPF in section 2 and vice versa the OSPF is redistributed in the reverse direction to be able to communicate to each other.

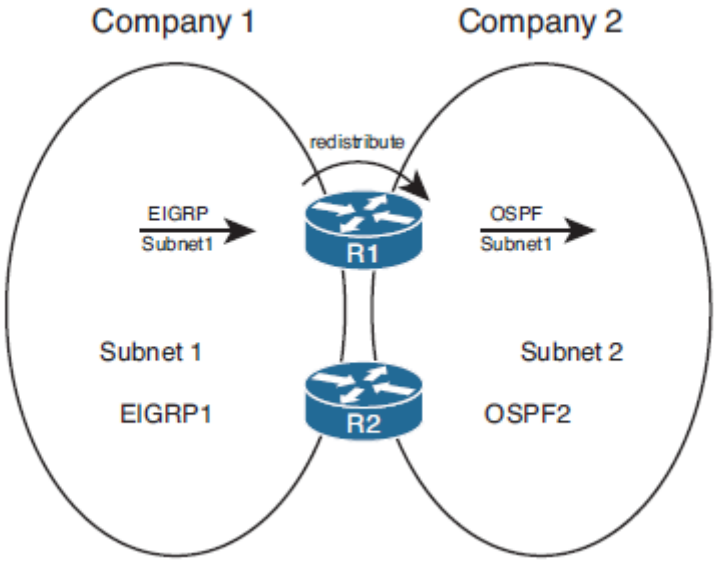


Figure 2-14 Typical Use of Redistribution.

Chapter 3 Redundancy

In the Internet Protocol (IP), computers split messages into packets and those packets hop from router to router on the way to their destination.

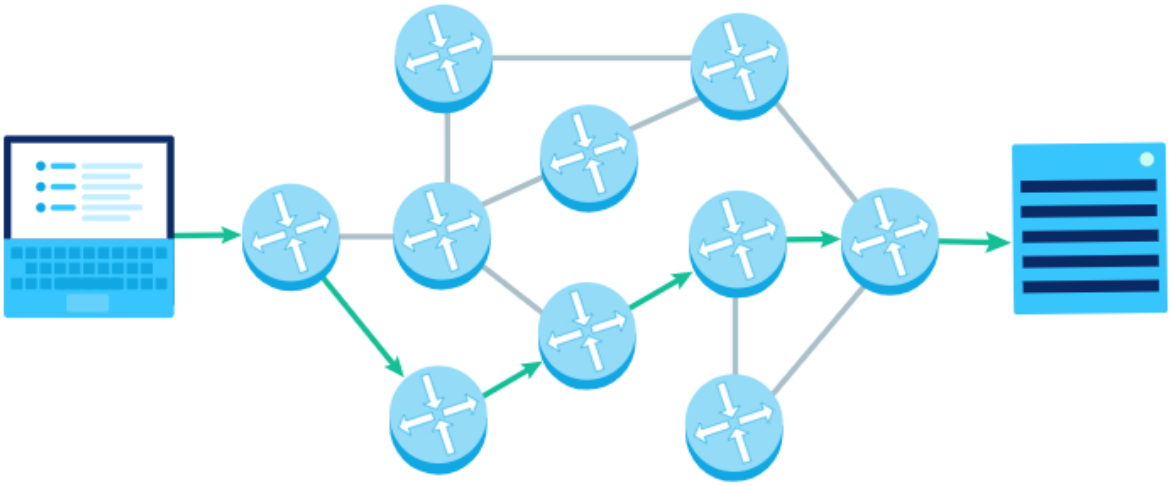


Figure 3-1 Redundancy routers connections.

What happens if a network path is no longer available, like due to a natural disaster physically destroying it or a cybercriminal hijacking it? Is the packet doomed to never reach its destination?

Redundancy in routing

Fortunately, there are often many possible paths a packet can go down to reach the same destination. The availability of multiple paths increases the **redundancy** of a network.

Consider this simplified network connecting routers in four major cities:

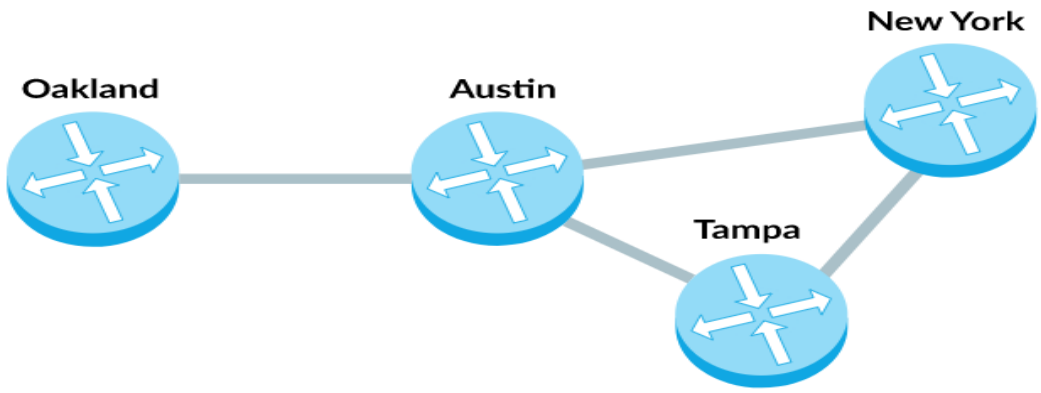


Figure 3-2 Network between different branches connected by redundancy technology.

If the connection between the Austin and New York router is no longer available, then there is still another way for the packet to reach its destination.

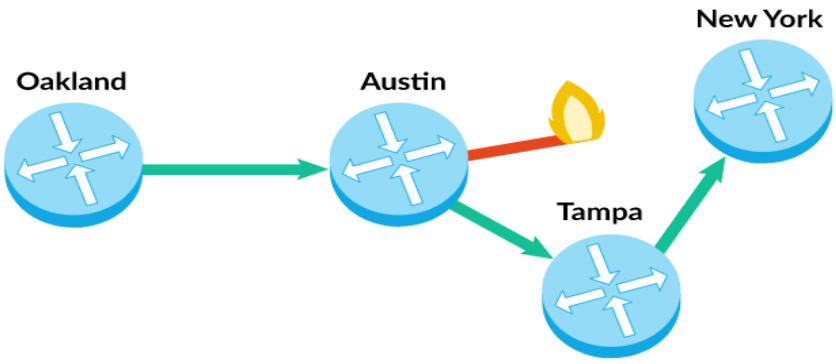


Figure 3-3 Showing if an interface of router down there is another one to do its work.

The redundancy of the paths in the network increases the number of possible ways that a packet can reach its destination.

3.1 Redundancy protocols:

1. Hot Standby Router Protocol (HSRP):

HSRP is a CISCO proprietary protocol used to provide redundancy in a network. Only one router is the active router while others will be in standby state.

Standby router will be responsible for forwarding the traffic when the active router fails.

Already we used this protocol in the project but there is a very important disadvantages in this protocol which is,

- No load balances.
- HSRP is a weak protocol from the security point of view.
- HSRP is a Cisco proprietary protocol.

2. Virtual Router Redundancy Protocol (VRRP):

VRRP is an open standard protocol, which is used to provide redundancy in a network. It is a network layer protocol (protocol number-112). The number of routers (group members) in a group acts as a virtual logical router which will be the default gateway of all the local hosts. If one router goes down, one of the other group members can take place for the responsibilities for forwarding the traffic.

3. Gateway Load Balancing Protocol (used in the project):

Gateway Load Balancing Protocol (GLBP) is one of First Hop Redundancy Protocol (FHRP) which provides redundancy like other First Hop Redundancy Protocol, also provides load Balancing. It is a Cisco proprietary protocol which can perform both functions. It provides load Balancing over multiple routers using single virtual IP address and multiple virtual MAC address.

3.2 GLBP terms:

1. **Virtual IP address**: An IP address is assigned as a virtual IP address from the local subnet which is configured as a default gateway for all the local hosts.
2. **Actual Virtual Gateway (AVG)**: It is one of the routers operating GLBP in a single group which is responsible for assigning virtual Mac address for each member in the group and for responding of the ARP request coming from the devices. The AVG has the highest priority value or IP address in the group.
3. **Actual Virtual forwarder (AVF)**: These are the routers including the AVG in a single GLBP group. These are responsible for forwarding the data after they are assigned by the AVG for the task. If in case AVG goes down, one of the AVFs can become the AVG.
4. **Preempt**: It is a state in which the one of the AVF will become the AVG router (when the AVG router goes down). Also, when the AVG router comes up again, it will become the AVG router as its priority is still higher (assumed).
5. **Object tracking**: GLBP uses a weighting scheme to determine the forwarding capacity of each router in the GLBP group. GLBP tracks interface and adjusts it's weighting i.e if the tracked interface goes down then it reduces by certain value (according to the configuration).

3.2.1 GLBP concepts:

The Actual Virtual Gateway (AVG) provides virtual Mac addresses to all the other routers operating GLBP of the same group. The remaining routers are Actual Virtual Forwarder (AVF). When an ARP request comes from subnet device to know the Mac address of the virtual IP address, one of the virtual Mac addresses is provided by the AVG. AVG will provide the virtual Mac address by using Round Robin algorithm or other algorithms that have been applied. In this way, all devices running GLBP are used to forward traffic.

GLBP virtual Mac address Assignment: When a subnet device (host) wants to send traffic, it requests a Mac address for the virtual IP (gateway) by sending an ARP request. In response to the ARP request, AVG will provide one of the virtual Mac addresses (provided to AVF by AVG).

Virtual Gateway Redundancy:

To detect a gateway failure, GLBP members communicate with each other through hello messages, sent in every 3-seconds to the multicast address 224.0.0.102. If AVG fails, then the AVF having highest priority will become the AVG i.e responsible for providing the MAC address of AVFs.

Virtual forwarder Redundancy:

Just like in **HSRP**, if one of the AVF fails then the other AVF in the same GLBP group will take the responsibility of forwarding the packets. There can be maximum 4 routers in a GLBP group.

3.2.2 Configurations:

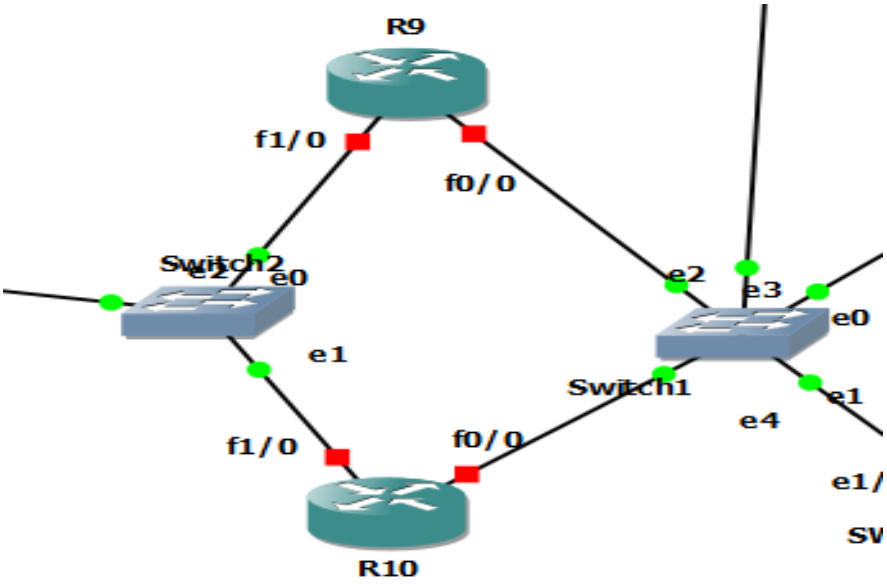


Figure 3-4 connections from GNS3

ROUTER 9 f0/0 config:

R9(config) # int fa0/0.2
R9(config-if) # GLBP 1 IP 192.168.2.4
R9(config-if) # GLBP 1 priority 120
R9(config-if) # GLBP 1 preempt
R9(config-if) # GLBP 1 load-balancing round-robin
R9(config) # int fa0/0.3
R9(config-if) # GLBP 1 IP 192.168.3.4
R9(config-if) # GLBP 1 priority 120
R9(config-if) # GLBP 1 preempt
R9(config-if) # GLBP 1 load-balancing round-robin
R9(config) # int fa0/0.4
R9(config-if) # GLBP 1 IP 192.168.4.4
R9(config-if) # GLBP 1 priority 120
R9(config-if) # GLBP 1 preempt
R9(config-if) # GLBP 1 load-balancing round-robin

ROUTER 10 f0/0 config:

R10(config)# int fa0/0.2
R10(config-if) # GLBP 1 IP 192.168.2.4
R10(config-if) # GLBP 1 priority 100
R10(config-if) # GLBP 1 preempt
R10(config-if) # GLBP 1 load-balancing round-robin
R10(config) # int fa0/0.3
R10(config-if) # GLBP 1 IP 192.168.3.4
R10(config-if) # GLBP 1 priority 100
R10(config-if) # GLBP 1 preempt

```
R10(config-if) # GLBP 1 load-balancing round-robin
R10(config) # int fa0/0.4
R10(config-if) # GLBP 1 IP 192.168.4.4
R10(config-if) # GLBP 1 priority 100
R10(config-if) # GLBP 1 preempt
R10(config-if) # GLBP 1 load-balancing round-robin
```

3.3 WAN Technologies [11]

WAN: is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

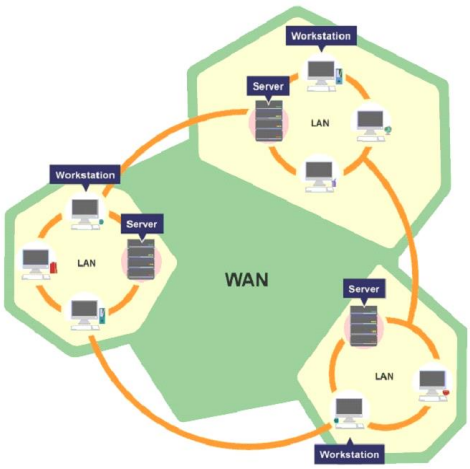


Figure 3-5 Linking networks using WAN technology.

There are two types of WAN:

1- Public WAN: Service providers provide Internet access to small offices and telecommuting employees such as DSL.

2- Private WAN: It's to make LANs to communicate with one another without access to the Internet.

Today, there are several types of Private WAN Technologies:

1- Dedicated Circuit Switching (Leased Line): The data always travel from source to destination using the same path so, Security is high.

2- On-Demond Circuit Switching: It is a leased line for a short period of time like Dial-Up and ISDN.

3- Packet Switching: Packet switching is a method of data transmission in which a message is broken into several parts, called packets, that are sent independently, in triplicate, over whatever route is optimum for each packet, and reassembled at the destination. Each packet contains a piece part, called the payload, and an identifying header that includes destination and reassembly information. The packets are sent in triplicate to check for packet corruption. Every packet is verified in a process that compares and confirms that at least two copies match. When verification fails, a request is made for the packet to be re-sent, Like (X.25, Frame Relay, ATM).

4- Label Switching: Like (MPLS) Multiprotocol Label Switching, it's a network routing-optimization technique. It directs data from one node to the next using short path labels rather than long network addresses, to avoid time-consuming table lookups.

5- Broadband Technology: refers to high-speed Internet access that is always on and faster than the traditional dial-up access, there are many types of Broadband Technology:

A. Digital Subscriber Line (DSL): is a wireline transmission technology that transmits data faster over traditional copper telephone lines already installed to homes and businesses, there are two types of DSL:

   1- Asymmetrical Digital Subscriber Line (ADSL): Used primarily by residential customers, such as Internet surfers, who receive a lot of data but do not send much So, ADSL provides faster speed in the downstream direction than the upstream direction.

   2- Symmetrical Digital Subscriber Line (SDSL): Used typically by businesses for services such as video conferencing, which need significant bandwidth both upstream and downstream.

B. Cable Modem: is a service enables cable operators to provide broadband using the same coaxial cables that deliver pictures and sound to your TV set?

C. Satellite: Just as satellites orbiting the earth provide necessary links for telephone and television service, they can also provide links for broadband. Satellite broadband is another form of wireless broadband and is also useful for serving remote or sparsely populated areas.

Now we will talk about **MPLS** in details:

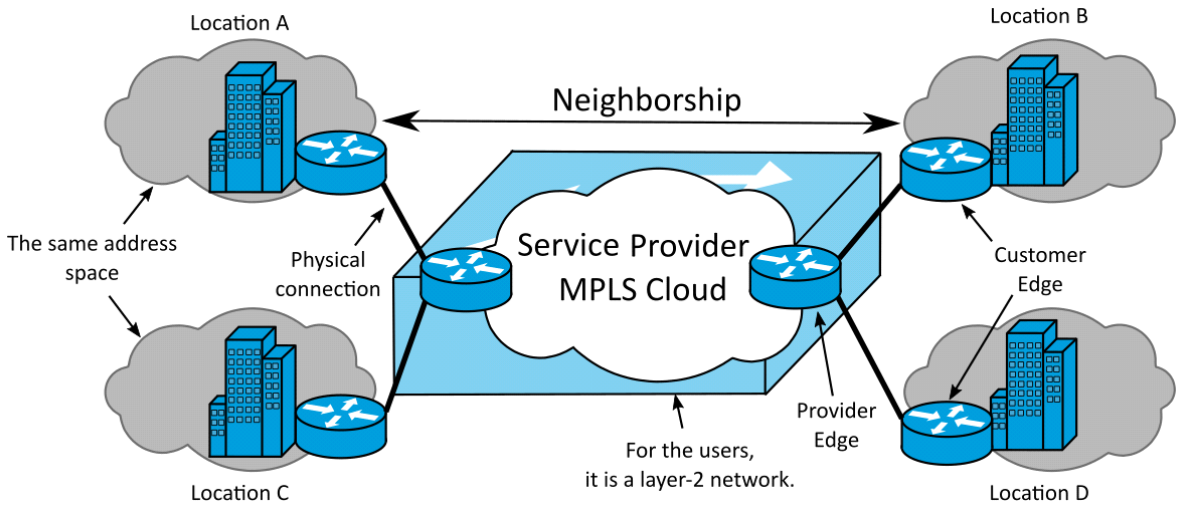


Figure 3-6 Connecting multiple Networks together using WAN technology.

When an internet router receives an IP packet, that packet carries no information beyond a destination IP address, there is no instruction on how that packet should get to its destination or how it should be treated along the way. Each router must make an independent forwarding decision for each packet based on the packet's network-layer header. Thus, every time a packet arrives at a router, the router must think through where to send the packet next, and the router does this by referring to complex routing tables, this process is repeated at each hop along the route until the packet reaches its destination, All those hops and all those individual routing decisions result in poor performance for time-sensitive applications like videoconferencing or voice over IP (VoIP).

So, we will use **MPLS** and with it, the first time a packet enters the network, it is assigned to a specific forwarding equivalence class (FEC), indicated by appending a short bit sequence (the label) to the packet.

Each router in the network has a table indicating how to handle packets of a specific FEC type, so once the packet has entered the network, routers do not need to perform header analysis. Instead, subsequent routers use the label as an index into a table that provides them with a new FEC for that packet, this gives the MPLS network the ability to handle packets with characteristics in a consistent fashion so packets carrying real-time traffic, such as voice or video, can easily be mapped to low-latency routes across the network.

3.3.1 MPLS Header:

There has been a lot of confusion about whether MPLS is a Layer 2 or Layer 3 service. But MPLS doesn't fit neatly into the OSI seven-layer hierarchy and is sometimes classified as Layer 2.5.

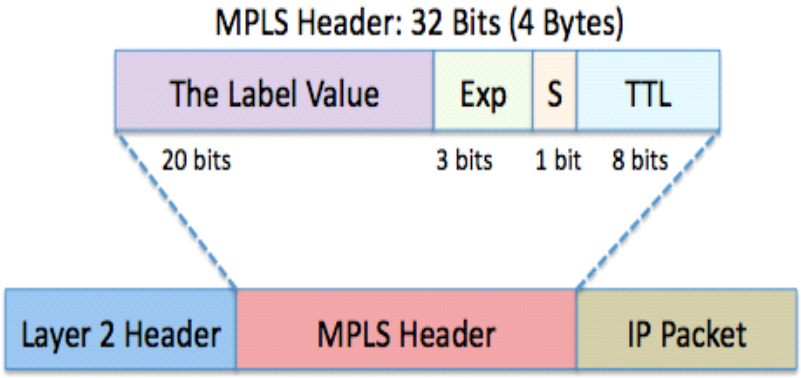


Figure 3-7 MPLS header.

The Label Value: The label holds all the information for the MPLS routers to determine where the packet should be forwarded.

Exp: Experimental bits are used for Quality of Service (**QoS**) to set the priority that the labeled packet should have.

S: The Bottom-of-Stack tells the MPLS Router if it is the last leg of the journey and there are no more labels to be concerned with. This usually means the router is an egress router.

TTL: This identifies how many hops the packet can make before it is discarded.

The importance of MPLS: scalability, high performance, better bandwidth utilization, reduced network congestion and a better end-user experience.

3.3.2 MPLS Configuration used in the project:

First, the routers in SP must connect with each other before configuring **MPLS**.

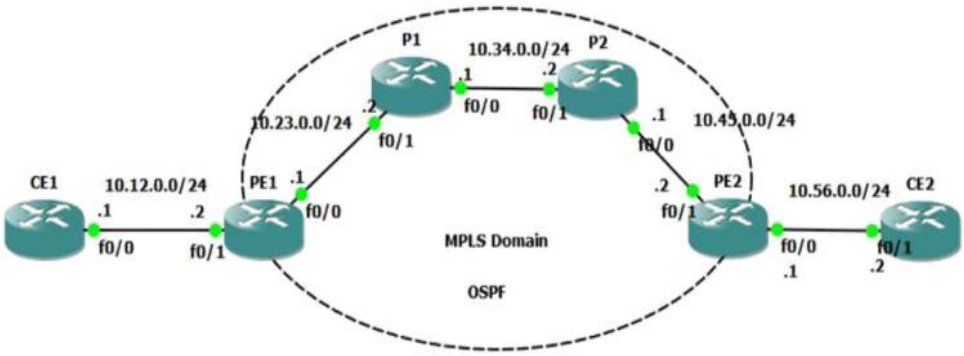


Figure 3-8 WAN routers.

```
R2(config)#int f0/1
R2(config-if)#ip address 10.12.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ip ospf 1 area
R2(config-if)#int f0/0
R2(config-if)#ip address 10.23.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#int loop 2
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ip ospf 1 area 0
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#passive-interface f0/1
```

Figure 3-9 R2 Configurations.

R3(config) # int f0/0

```
R3(config-if)#ip address 10.34.0.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#ip ospf 1 area 0
R3(config-if)#int f0/1
R3(config-if)#ip address 10.23.0.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#ip ospf 1 area 0
R3(config-if)#int loop 3
R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#ip ospf 1 area 0
```

Figure 3-10 R3 Configurations.

```
R4(config)#int f0/0
R4(config-if)#ip add 10.45.0.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#ip ospf 1 area 0
R4(config-if)#int f0/1
R4(config-if)#ip add 10.34.0.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#ip ospf 1 area 0
R4(config-if)#int loop 4
R4(config-if)#ip address 4.4.4.4 255.255.255.255
R4(config-if)#ip ospf 1 area 0
```

Figure 3-11 R4 configurations

```
R5(config)#int f0/0
R5(config-if)#ip address 10.56.0.5 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#ip ospf 1 area 0
R5(config-if)#int f0/1
R5(config-if)#ip address 10.45.0.5 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#ip ospf 1 area 0
R5(config-if)#int loop 5
R5(config-if)#ip address 5.5.5.5 255.255.255.255
R5(config-if)#ip ospf 1 area 0
R5(config-if)#router ospf 1
R5(config-router)#passive-interface f0/0
```

Figure 3-12 R5 Configurations

Now to configure **MPLS** on **SP** Routers:

```
R2(config)#mpls label range 200 299                    (optional)
R2(config)#mpls ip
R2(config)#int f0/0
R2(config-if)#mpls ip

R3(config)#mpls label range 300 399                    (optional)
R3(config)#mpls ip
R3(config)#int range f0/0 - 1
R3(config-if-range)#mpls ip
*Mar 1 00:30:19.335: %LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (1) is UP
```

Figure 3-13 R2 configurations.

```
R4(config)#mpls label range 400 499                    (optional)
R4(config)#mpls ip
R4(config)#int range f0/0 - 1
R4(config-if-range)#mpls ip
*Mar 1 00:30:49.323: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (1) is UP

R5(config)#mpls label range 500 599                    (optional)
```

Figure 3-14 R4 Configurations.

```
R5(config)#mpls ip
R5(config)#int f0/1
R5(config-if)#mpls ip
*Mar 1 00:30:54.923: %LDP-5-NBRCHG: LDP Neighbor 4.4.4.4:0 (1) is UP
```

Figure 3-15 R5 Configurations.

➢ **To test connectivity after configuring MPLS:**

```
R1#traceroute 10.56.0.6

Type escape sequence to abort.
Tracing the route to 10.56.0.6
 1 10.12.0.2 76 msec 72 msec 60 msec
 2 10.23.0.3 [MPLS: Label 305 Exp 0] 172 msec 140 msec 132 msec
 3 10.34.0.4 [MPLS: Label 405 Exp 0] 144 msec 140 msec 140
msec 4 10.45.0.5 140 msec 140 msec 168 msec
 5 10.56.0.6 136 msec 164 msec 136 msec
```

Figure 3-16 test connectivity.

Verification:

MPLS has 3 tables:

1- The Neighbors table:

```
R3#show mpls ldp neighbor
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 3.3.3.3:0
        TCP connection: 2.2.2.2.646 - 3.3.3.3.17834
        State: Oper; Msgs sent/rcvd: 51/52; Downstream
        Up time: 00:35:32
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 10.23.0.2
        Addresses bound to peer LDP Ident:
          10.23.0.2      10.12.0.2      2.2.2.2
```

Figure 3-17 show MPLS neighbors.

```
Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 3.3.3.3:0
    TCP connection: 4.4.4.4.18224 - 3.3.3.3.646
    State: Oper; Msgs sent/rcvd: 47/48; Downstream
    Up time: 00:31:12
    LDP discovery sources:
      FastEthernet0/0, Src IP addr: 10.34.0.4
    Addresses bound to peer LDP Ident:
      10.45.0.4      10.34.0.4      4.4.4.4
```

Figure 3-18 peer LDP Ident

2- The LIB (Label Information Base) table:

```
R3#show mpls ldp bindings 10.56.0.0 24
  tib entry: 10.56.0.0/24, rev 18
        local binding: tag: 305
        remote binding: tsr: 2.2.2.2:0, tag: 205
        remote binding: tsr: 4.4.4.4:0, tag: 405
```

Figure 3-19 show configurations.

3- The LFIB (Label Forwarding Information Base) (Forwarding) table:

```
R3#show mpls forwarding-table 10.56.0.0
Local  Outgoing    Prefix          Bytes tag   Outgoing    Next Hop
tag    tag or VC   or Tunnel Id    switched    interface
305    405         10.56.0.0/24    828         Fa0/0       10.34.0.4

R4#show mpls ldp bindings 10.56.0.0 24
  tib entry: 10.56.0.0/24, rev 18
        local binding: tag: 405
        remote binding: tsr: 3.3.3.3:0, tag: 305
        remote binding: tsr: 5.5.5.5:0, tag: imp-null

R4#show mpls forwarding-table 10.56.0.0
Local  Outgoing    Prefix          Bytes tag Outgoing Next Hop
tag    tag or VC   or Tunnel Id    switched interface
405    Pop tag     10.56.0.0/24    1596      Fa0/0    10.45.0.5
```

Figure 3-20 show MPLS forwarding table.

Chapter 4 Security and Servers.

Introduction

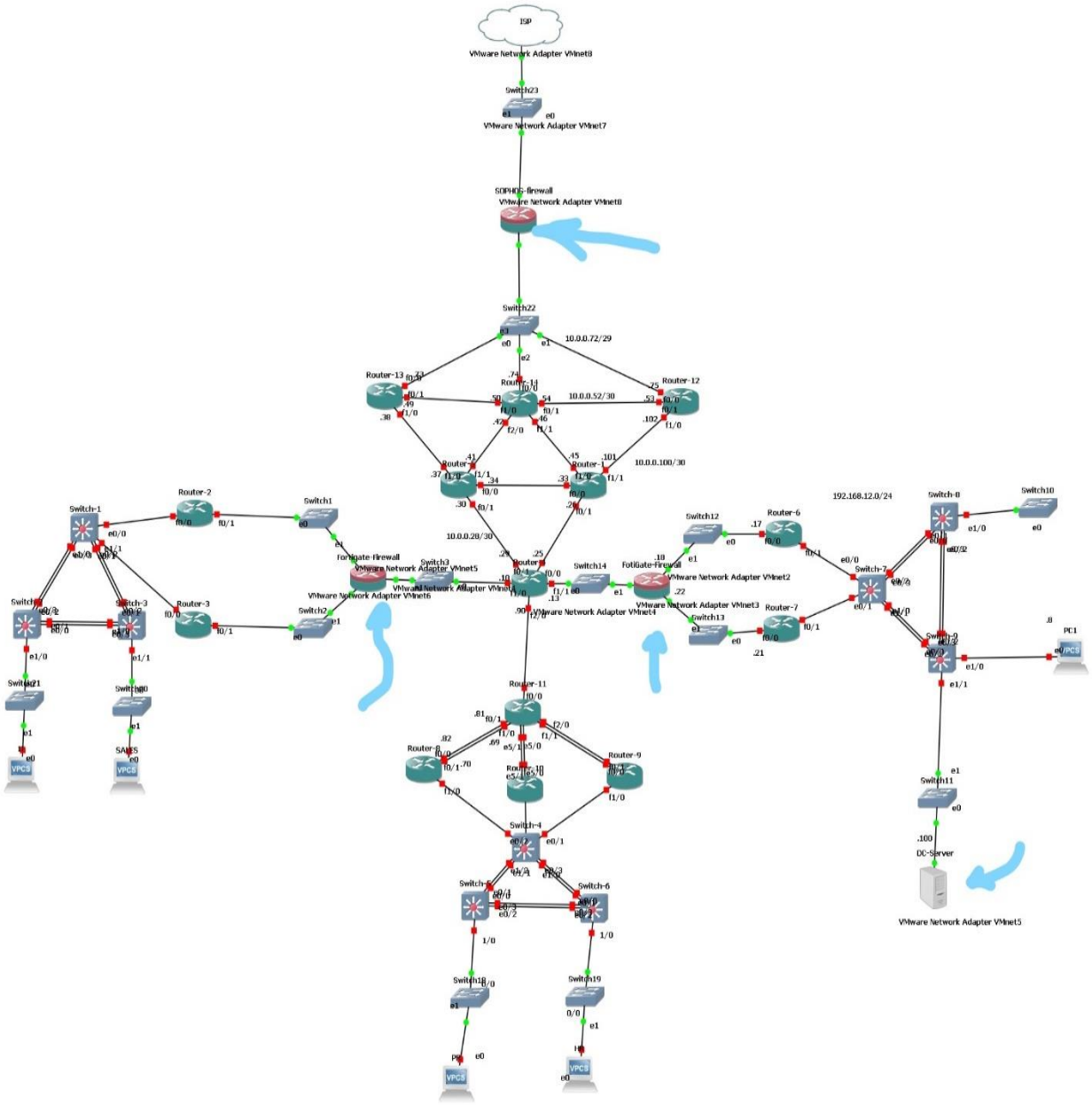


Figure 4-1 Small design of network infrastructure with security devices

The Figure 4-1 above contains a small design of network infrastructure with security devices. In our network we used Linux servers and MS server (firewalls are Linux based and ADDC is MS based). The devices with an arrow are firewall and ADDC (Active Directory Domain Controller). The devices that are responsible for security and connecting internet.

Devices are:

- FortiGate Firewall
- Sophos Firewall
- Active Directory Domain Controller

4.1 FortiGate Firewall [1]

We used two FortiGate Firewall one for each branch and here what we did in the configuration. Assigning IP address for the firewall to the hardware interface in my network 192.168.1.100 to be able to open it in the browser,

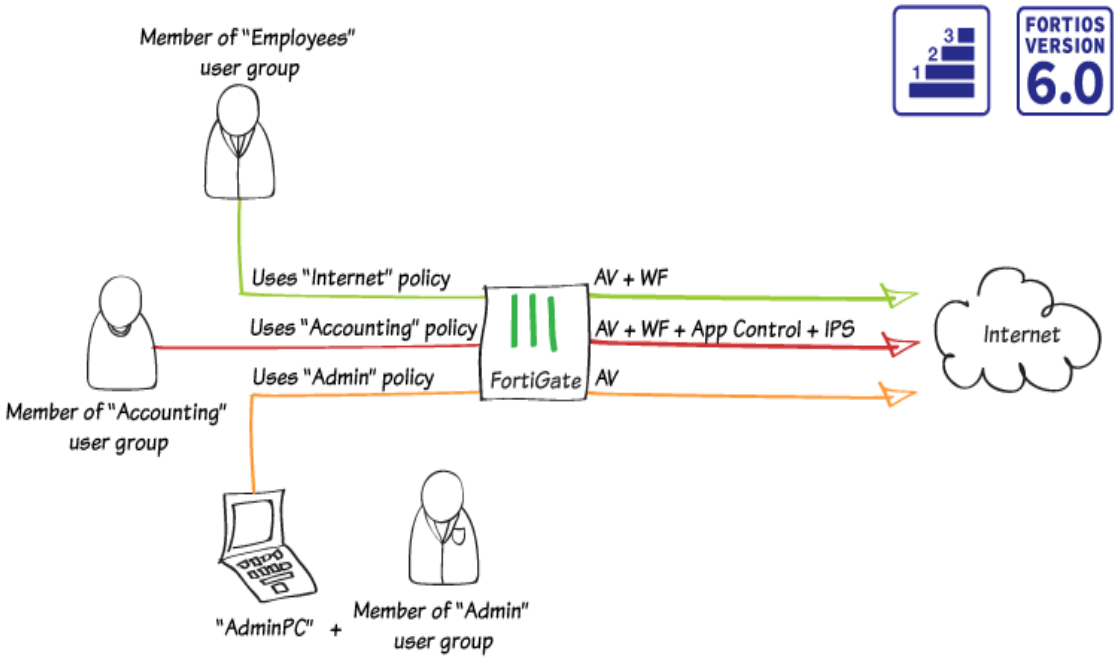


Figure 4-2 shows the place of firewall.

- config system interface➔to enter the access the network interfaces of the firewall.
- edit port1 ➔to edit port1 which is the physical interface we will access the firewall through it.
- set ip 192.168.1.101 255.255.255.0➔ in physical interface.
- set allow access ping http➔open ports like 80 to be able to access the firewall though browser and allowing ping for testing and troubleshooting.
- end ➔is entered to apply the editing in the interfaces.

```
FortiGate-VM64 login: admin
Password:
Welcome !

FortiGate-VM64 # config system interface

FortiGate-VM64 (interface) # set ip 192.168.1.101 255.255.255.0
Unknown action 0

FortiGate-VM64 (interface) # edit port 1

command parse error before '1'
Command fail. Return code -61

FortiGate-VM64 (interface) # edit port1

FortiGate-VM64 (port1) # set ip 192.168.1.101 255.255.255.0

FortiGate-VM64 (port1) # set allowaccess ping http

FortiGate-VM64 (port1) # end

FortiGate-VM64 #
```

Figure 4-3 Firewall physical interface

```
PS C:\Users\pc> ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=255
Reply from 192.168.1.101: bytes=32 time<1ms TTL=255
Reply from 192.168.1.101: bytes=32 time<1ms TTL=255
Reply from 192.168.1.101: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\pc>
```

Figure 4-4 Ping on firewall

This image shows that the firewall now is pingable and we able to connect it through browser.

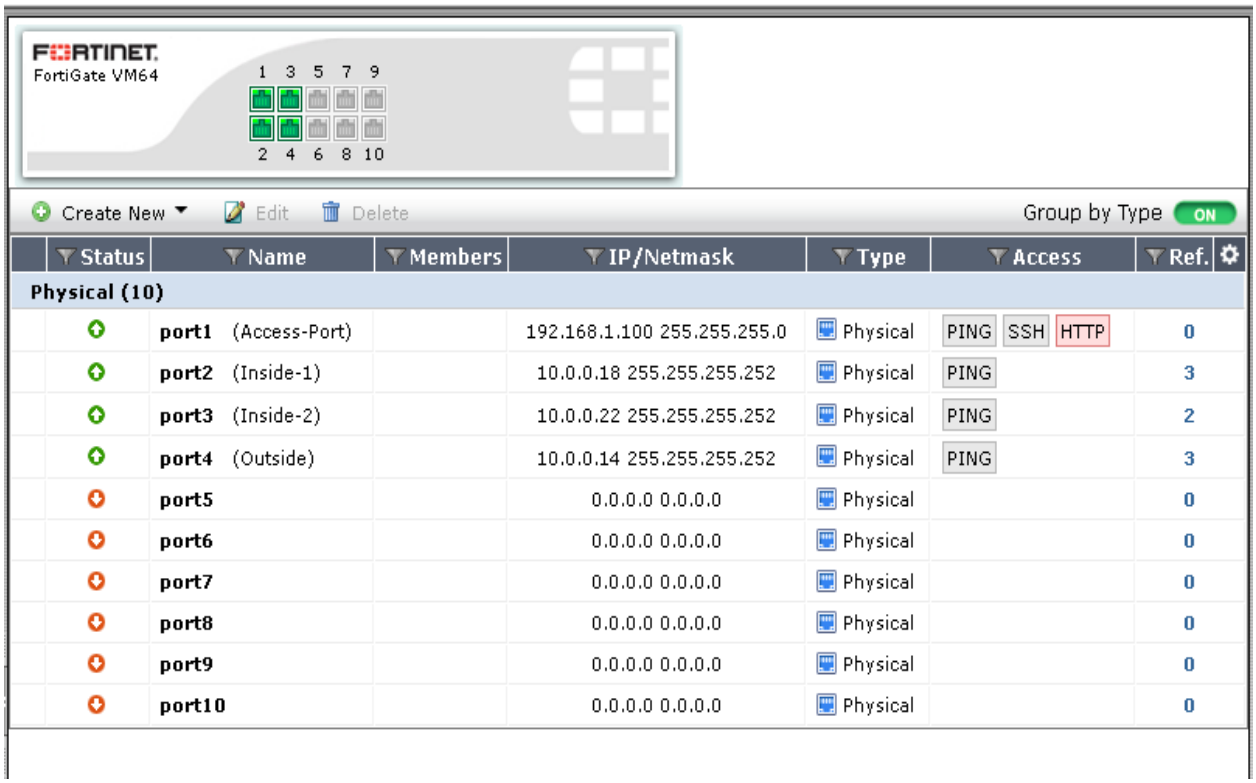


Figure 4-5 Firewall interfaces IPs.

Here the connected ports: 2, 3, and 4 are the interfaces connected to the networks, we opened the ping on firewall to allow troubleshooting.

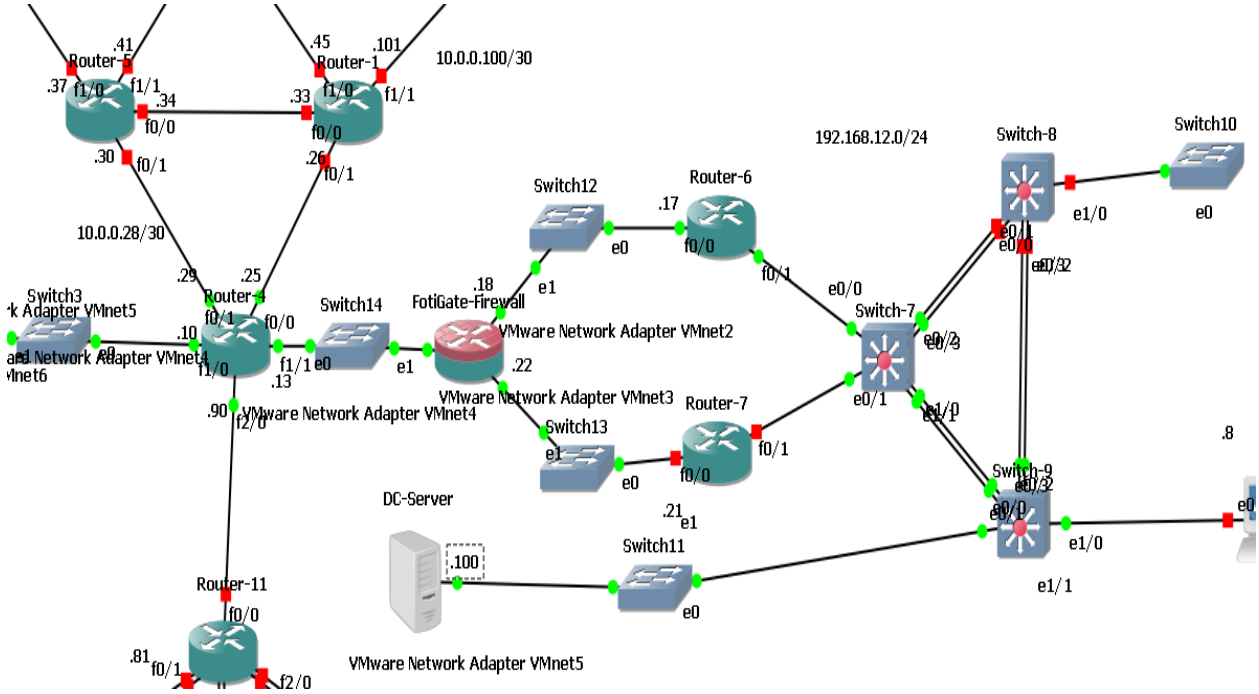


Figure 4-6 Connected devices in branch 2.

In the image above we see the branch 2 of the network with all connected devices they, running devices, all read each other, see.

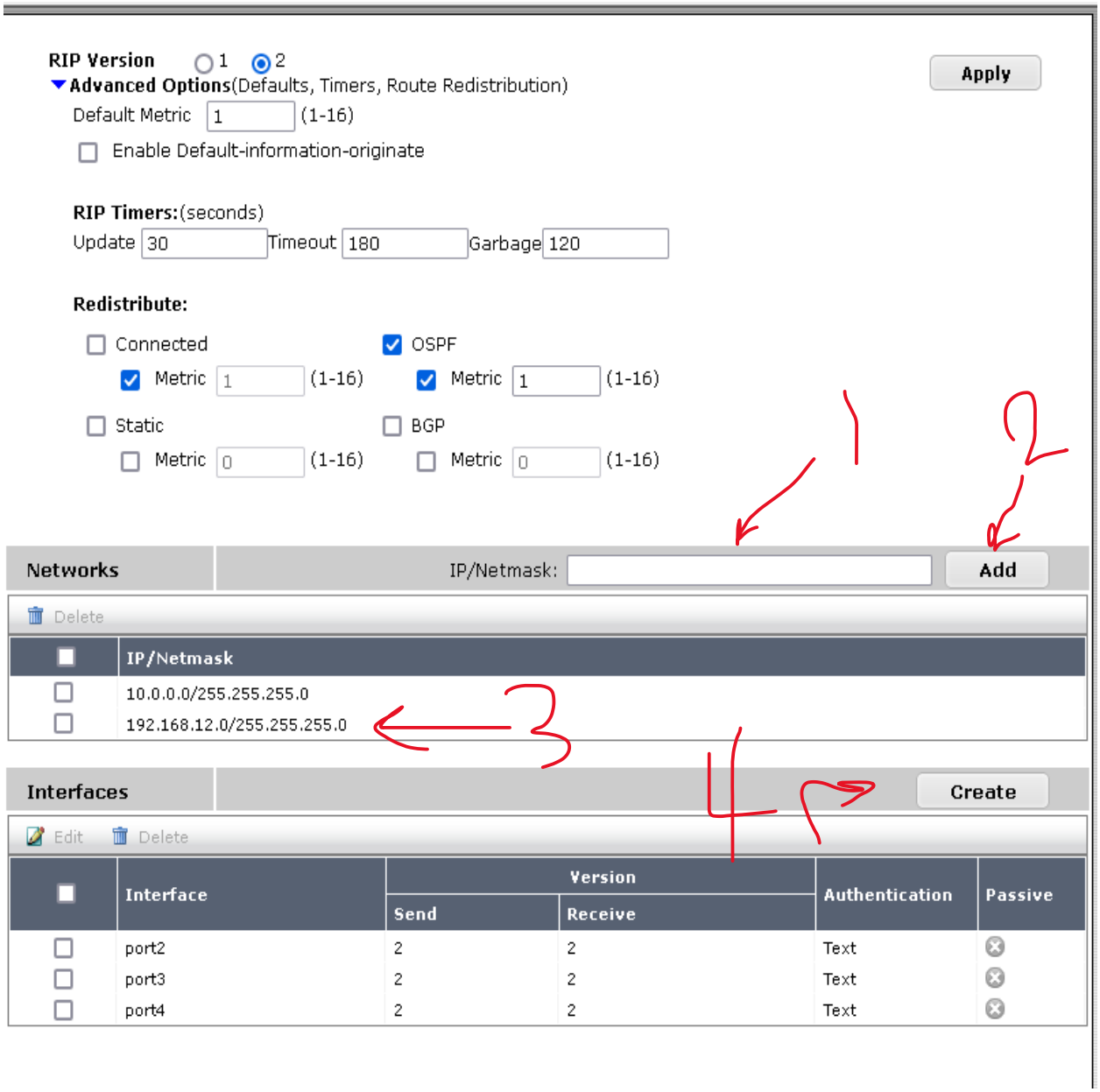


Figure 4-7 Firewall RIP configuration

Allowing RIP in the whole firewall and redistribute the OSPF to allow reading the networks it will get them.

1. The text box to write a network id.
2. The button to press to add network.
3. The added network.
4. Create button to create interfaces that will allow RIP packets.

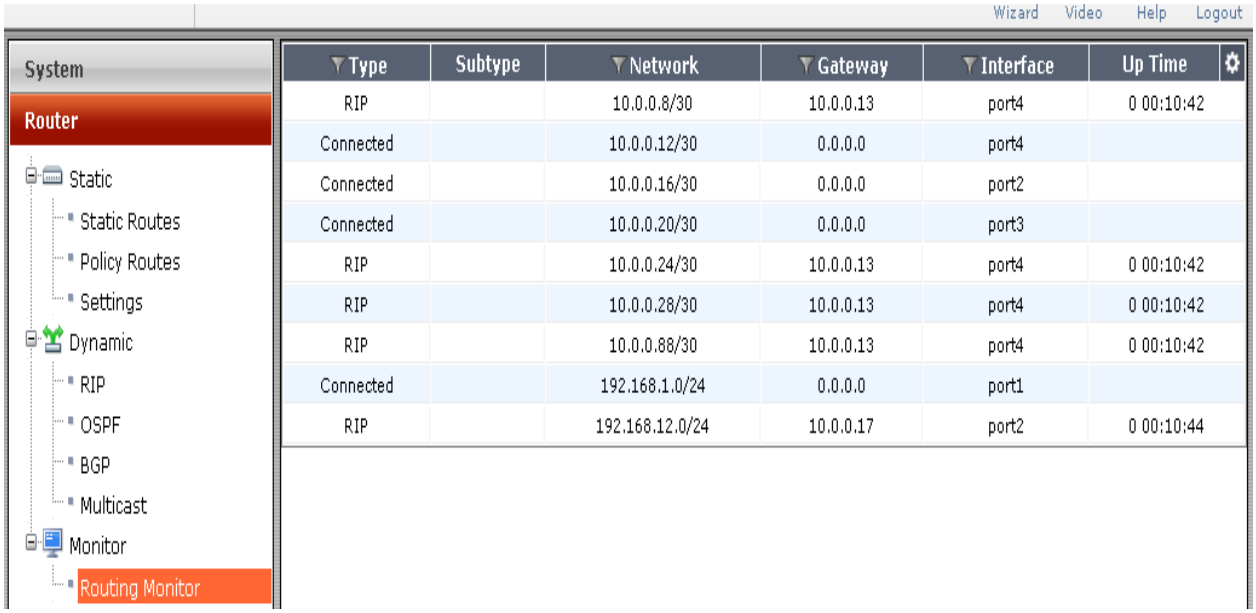


Figure 4-8 Routing Monitor in firewall

Monitoring the routing from firewall, this screen shows the network that the firewall sees from routing protocol, RIP, or the directly connected ones.

4.1.1 Object creation

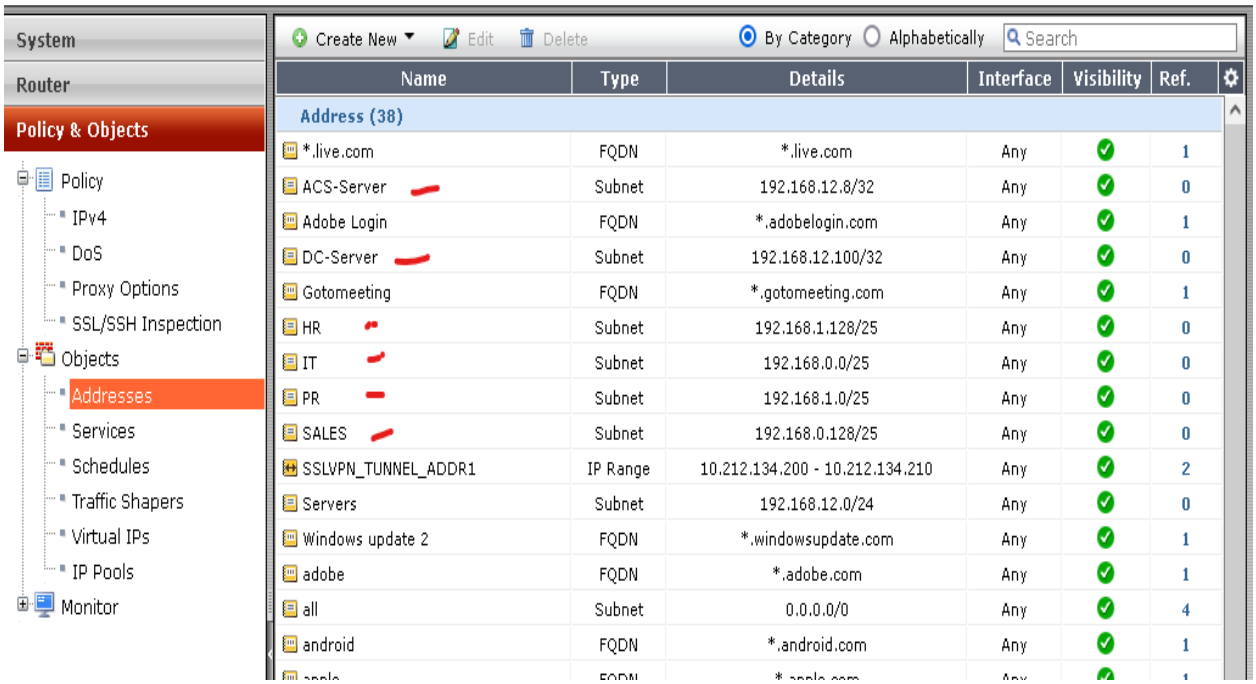


Figure 4-9 objects in firewall

Here are the objects of each department. Objects in firewall for organizing the control of users and department of a company that these objects. We will use later to prevent and allow some features for each user and each branch.

4.1.2 Authentication [2]

The authentication section in firewall is to create users on firewall.

1- We created users in ADDC Server not locally on firewall.
2- The Figure 4-10 shows the IP of ADDC Server that is used.

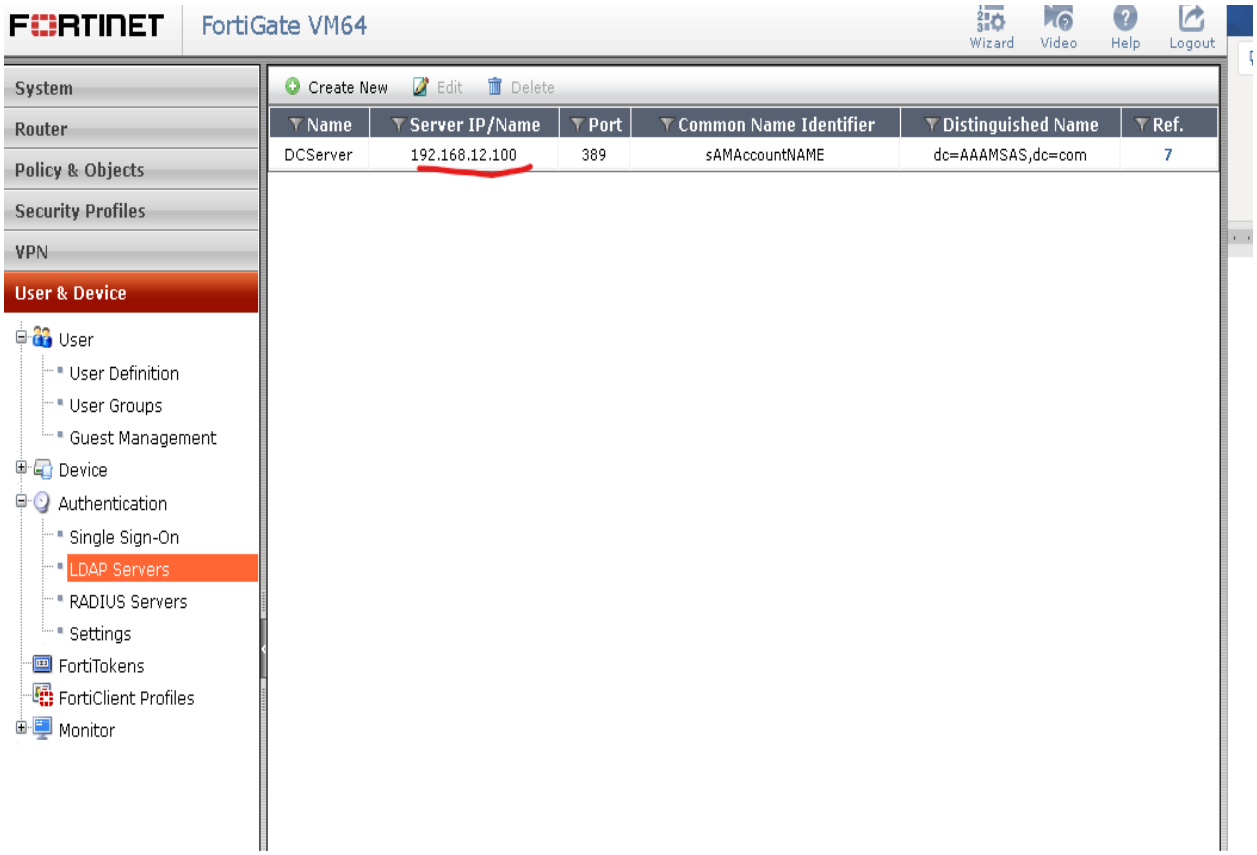


Figure 4-10 Firewall reads ADDC Server.

defining ADDC Server on firewall

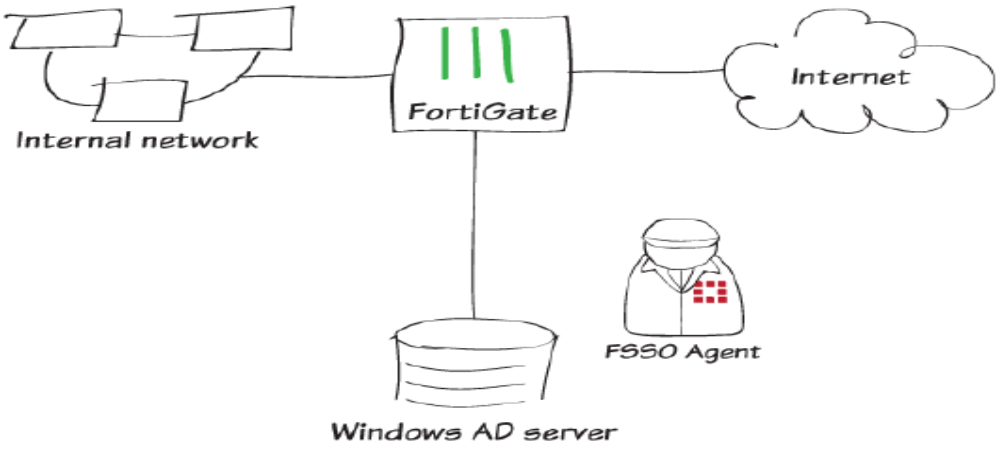


Figure 4-11 FSSO authentication.

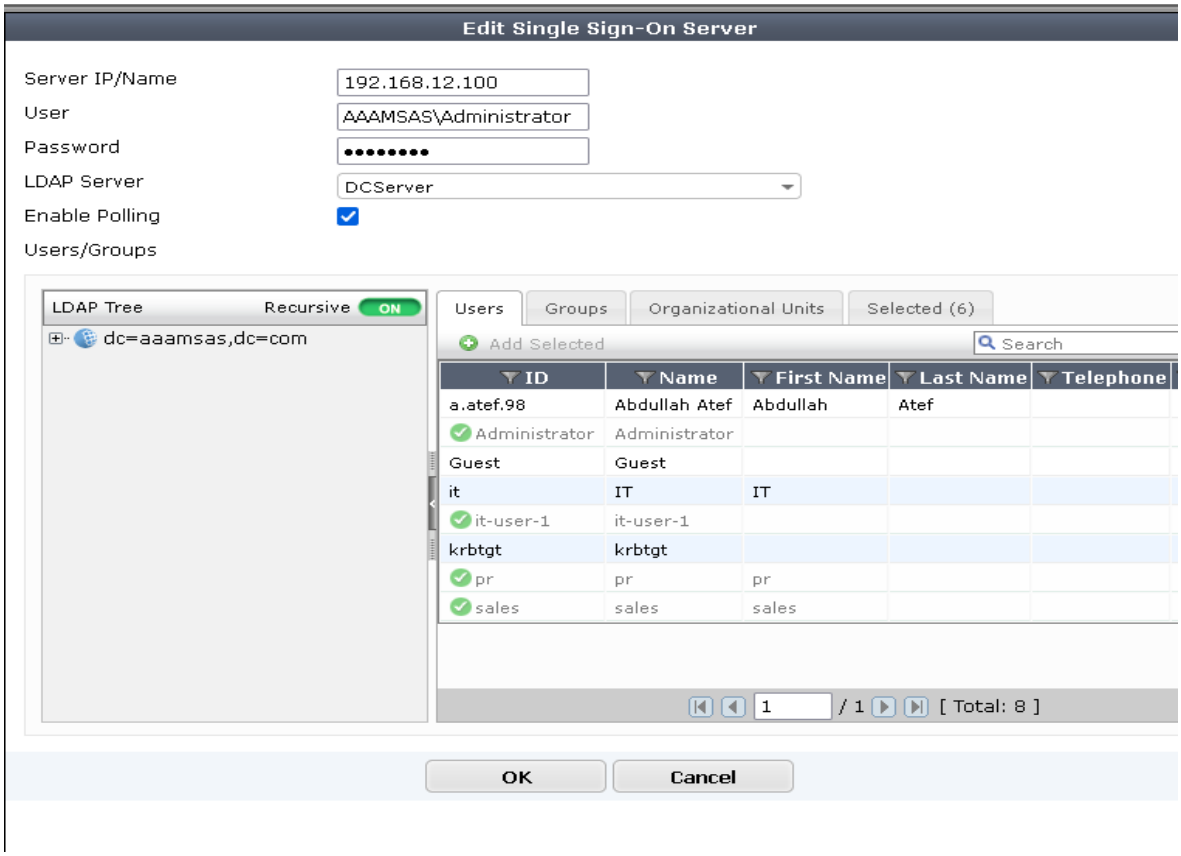


Figure 4-12 FSSO Configurations.

Adding FSSO from AD to allow users from AD to single sign-on FortiGate or other web services.

4.1.3 User addition

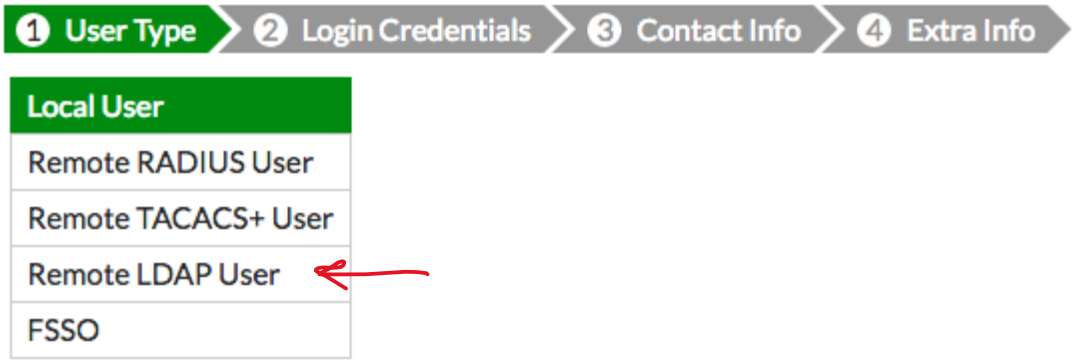


Figure 4-13 Selecting LDAP Server.

The first step to choose ADDC Server is selecting LDAP section as in the Figure *4-13*.

Adding users from ADDC Server.

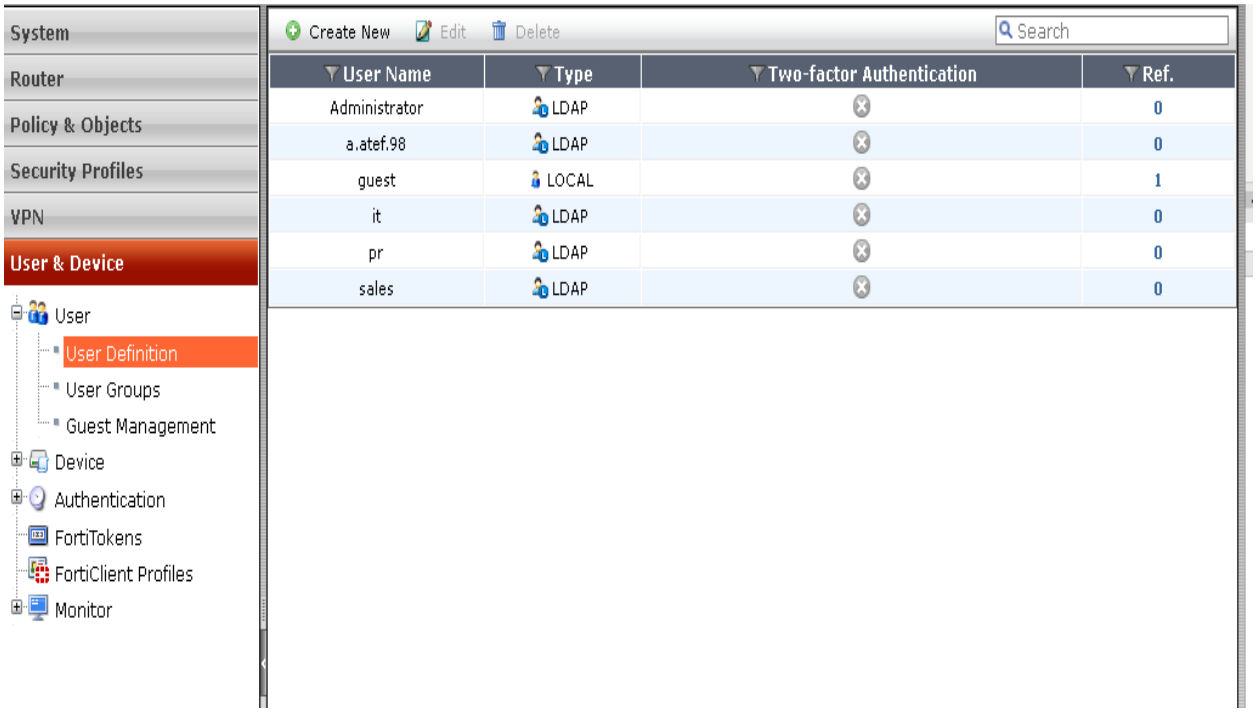


Figure 4-14 User definition in FortiGate Firewall

Adding users from ADDC Server on firewall, these users coming from **A**ctive **D**irectory **D**omain **C**ontroller, that also means the network is working successfully with no errors till now and firewall allowed ADDC to transfer packets through it.

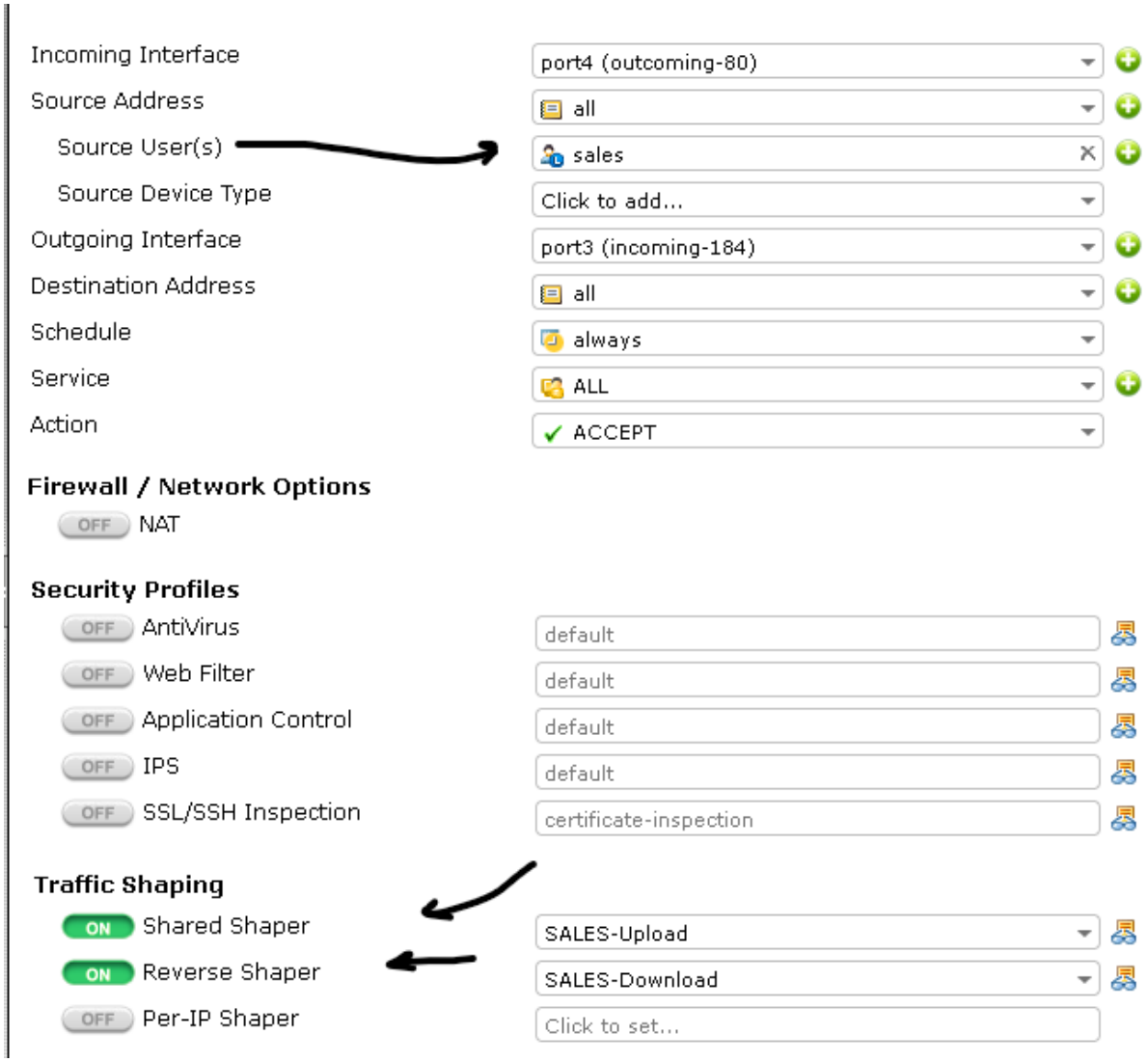


Figure 4-15 control traffic by users.

Here in the Figure *4-15* we control the upload and download speed for sales users.

4.1.4 Testing

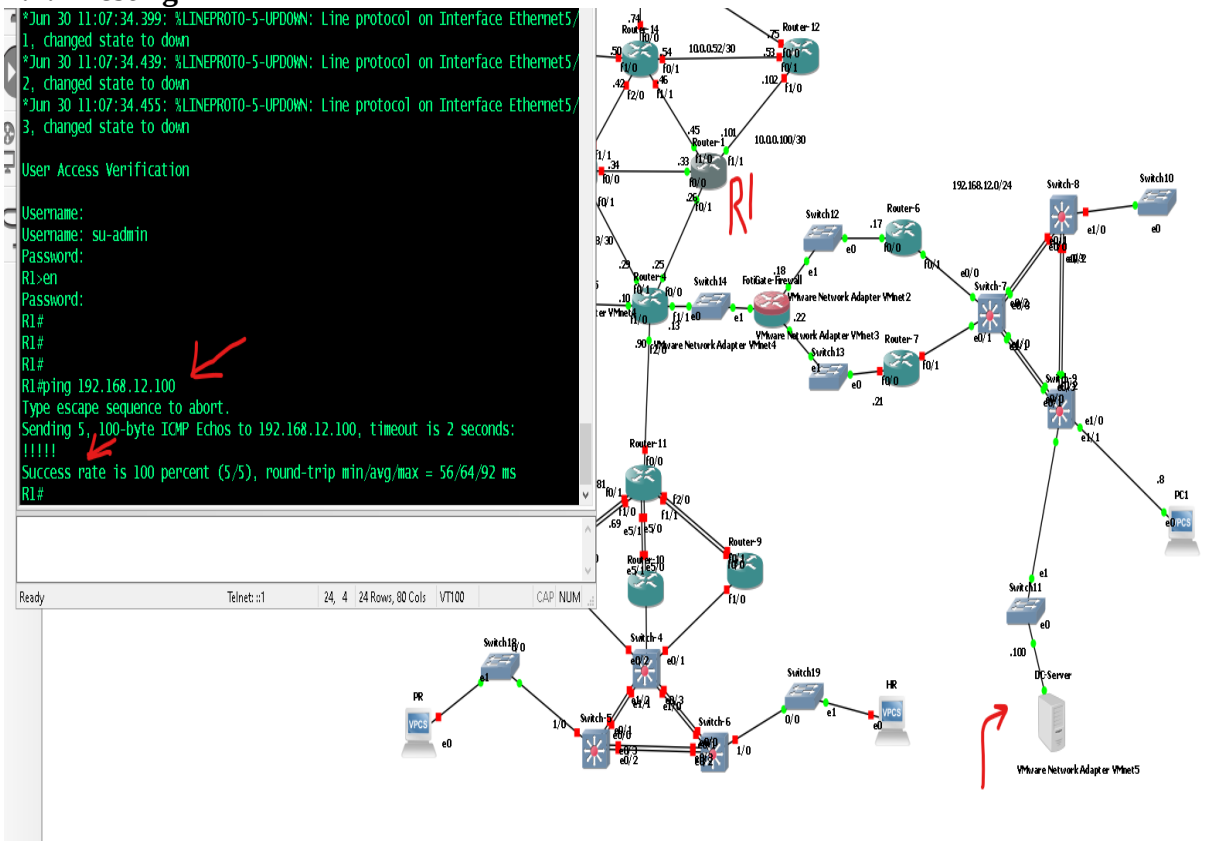


Figure 4-16 Ping on ADDC from R1

Shows that the ADDC Server is pingable from outside interface of the firewall, also **R1** is in WAN infrastructure that means that ADDC Server can reach to SOPHOS firewall easily.

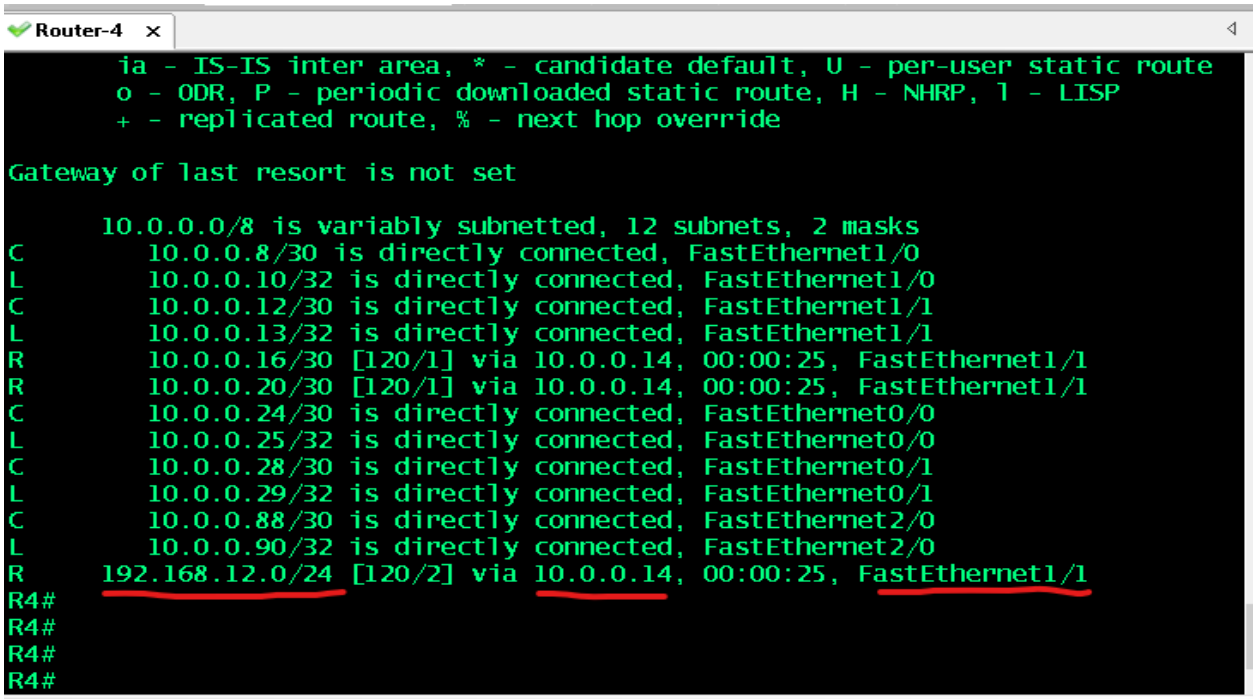


Figure 4-17 R4 reads Firewall.

The IPs in the right side of firewall appears in the router (**R4**) before firewall, that means firewall is allowing connection through it.

4.2 SOPHOS Firewall

As we did in FortiGate firewall in previous section, we start first by defining IPs for firewall interfaces. First the physical interface that we will access the firewall through got an IP 192.168.146.100 on port 4444. Second the interface that is connected to the network itself as shown in figure 4-19.

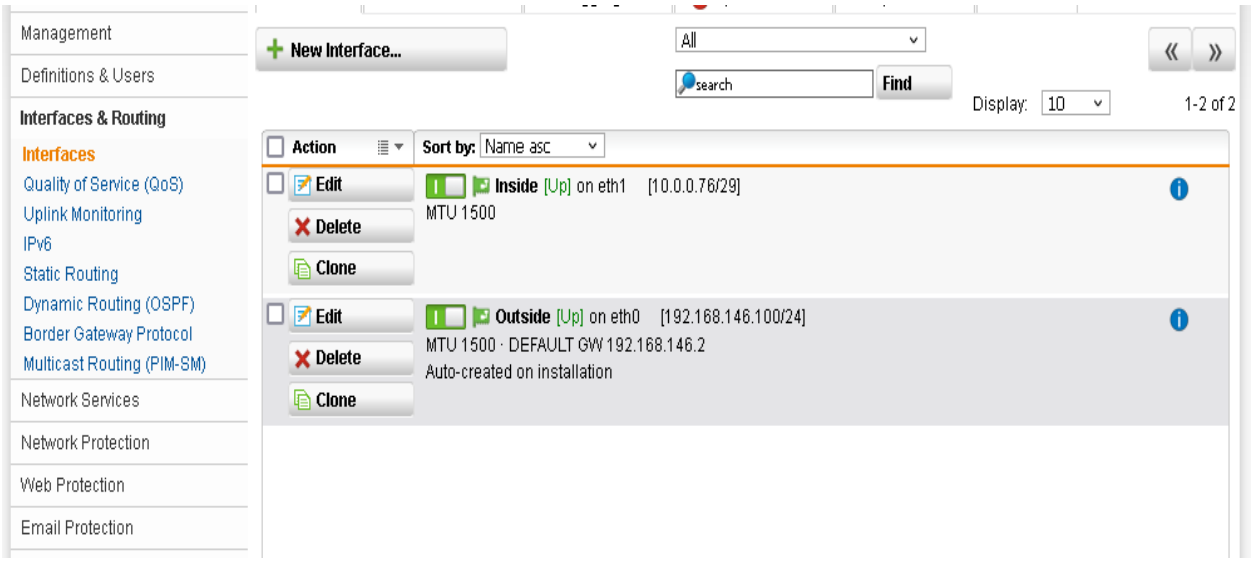


Figure 4-18 Interfaces IP assignment for SOPHOS Firewall.

Figure 4-19 Sophos firewall network interfaces.

Assigning router ID in firewall

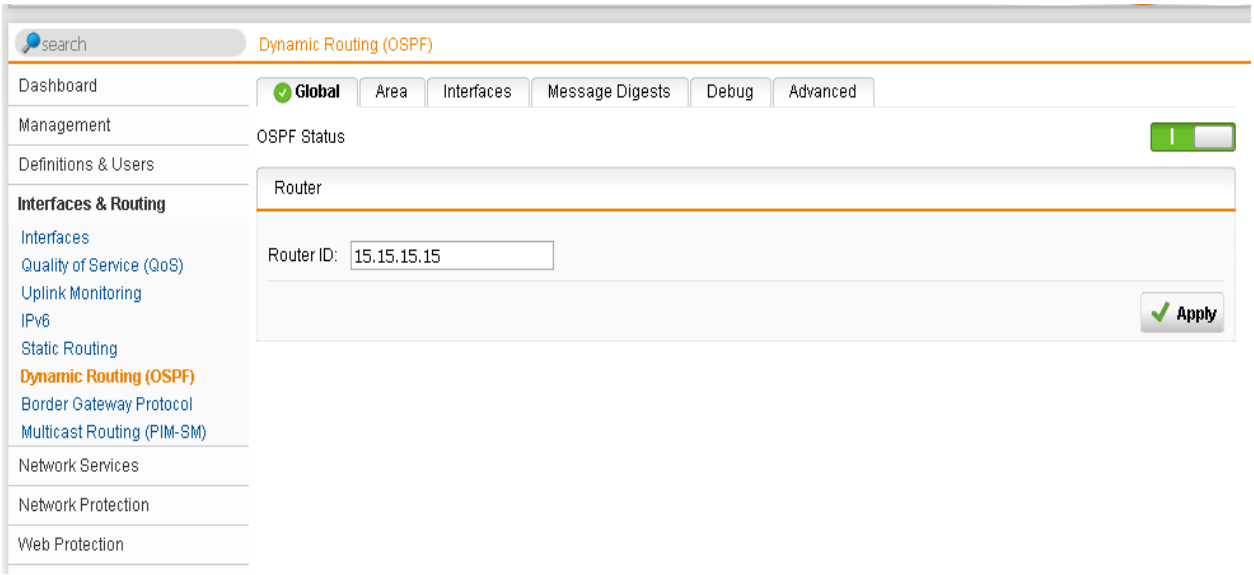


Figure 4-20 Define OSPF protocol on SOPHOS Firewall.

OSPF area definition in firewall.

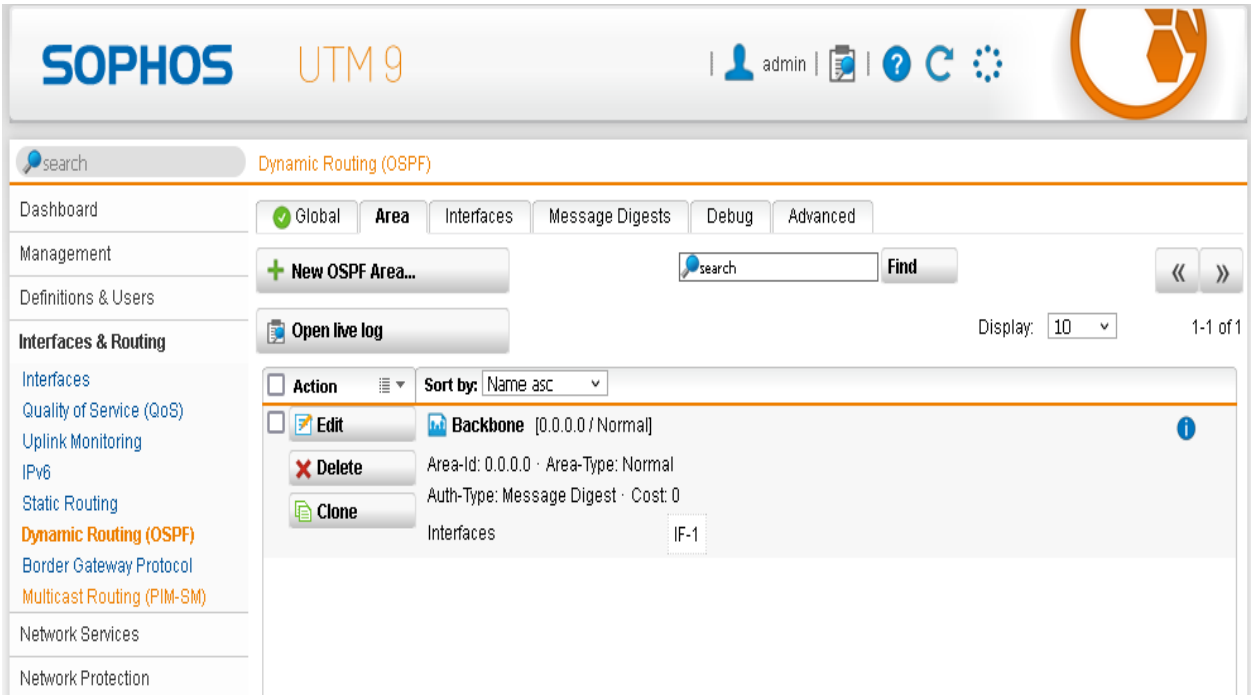


Figure 4-21 Configure area for OSPF routing protocol.

Selecting interfaces that configured or connected to OSPF network.

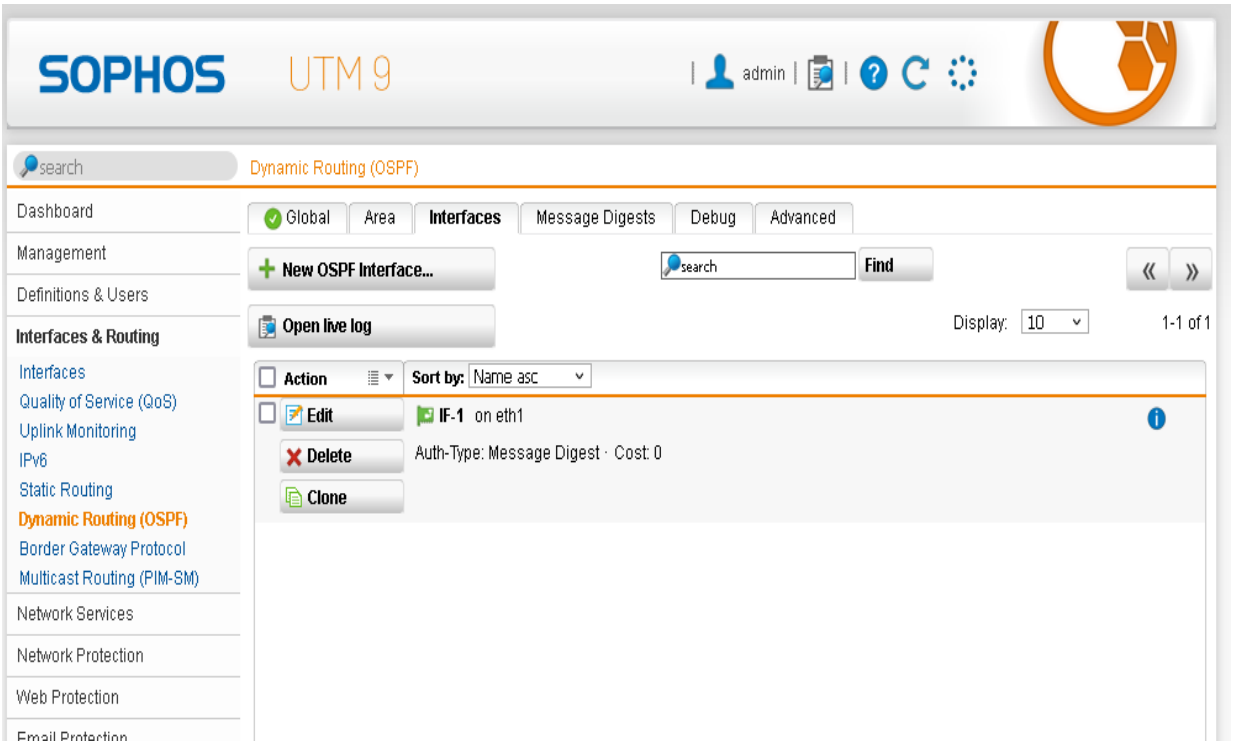


Figure 4-22 Define interfaces that will have OSPF protocol.

Define message digest for OSPF authentication.

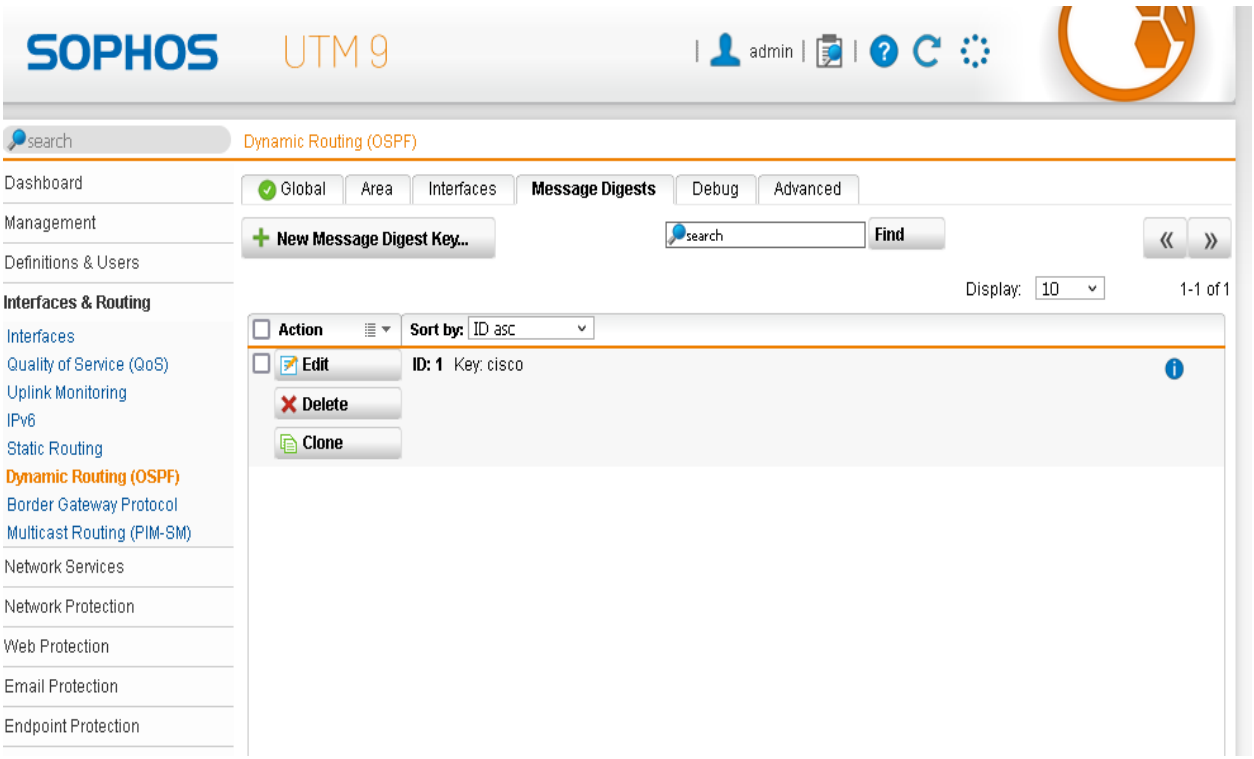


Figure 4-23 Define message digests for OSPF authentication.

Country filtering.

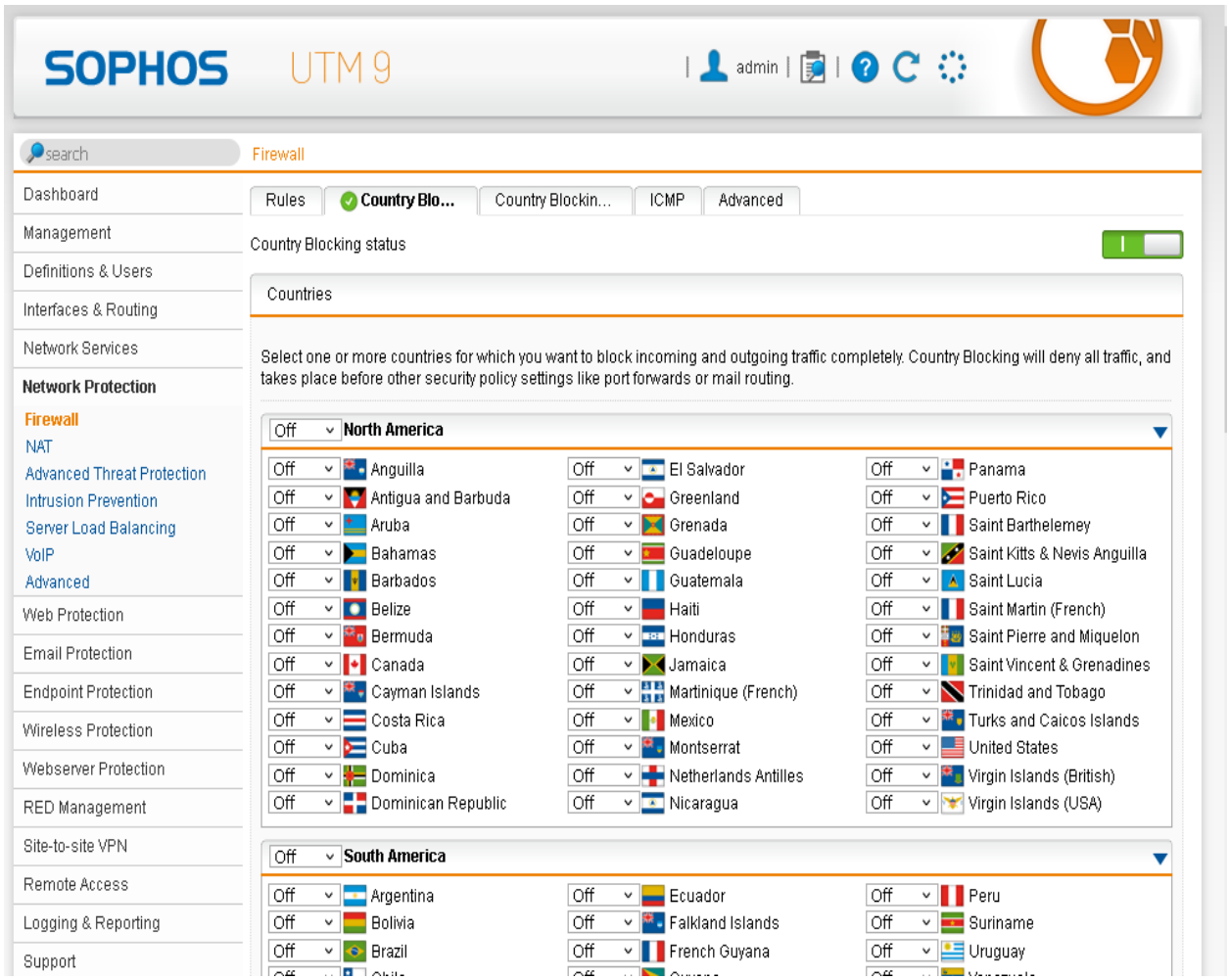


Figure 4-24 Country filtering in SOPHOS Firewall.

In firewall preventing and allowing connections from specific countries and continents.

ICMP packets control.

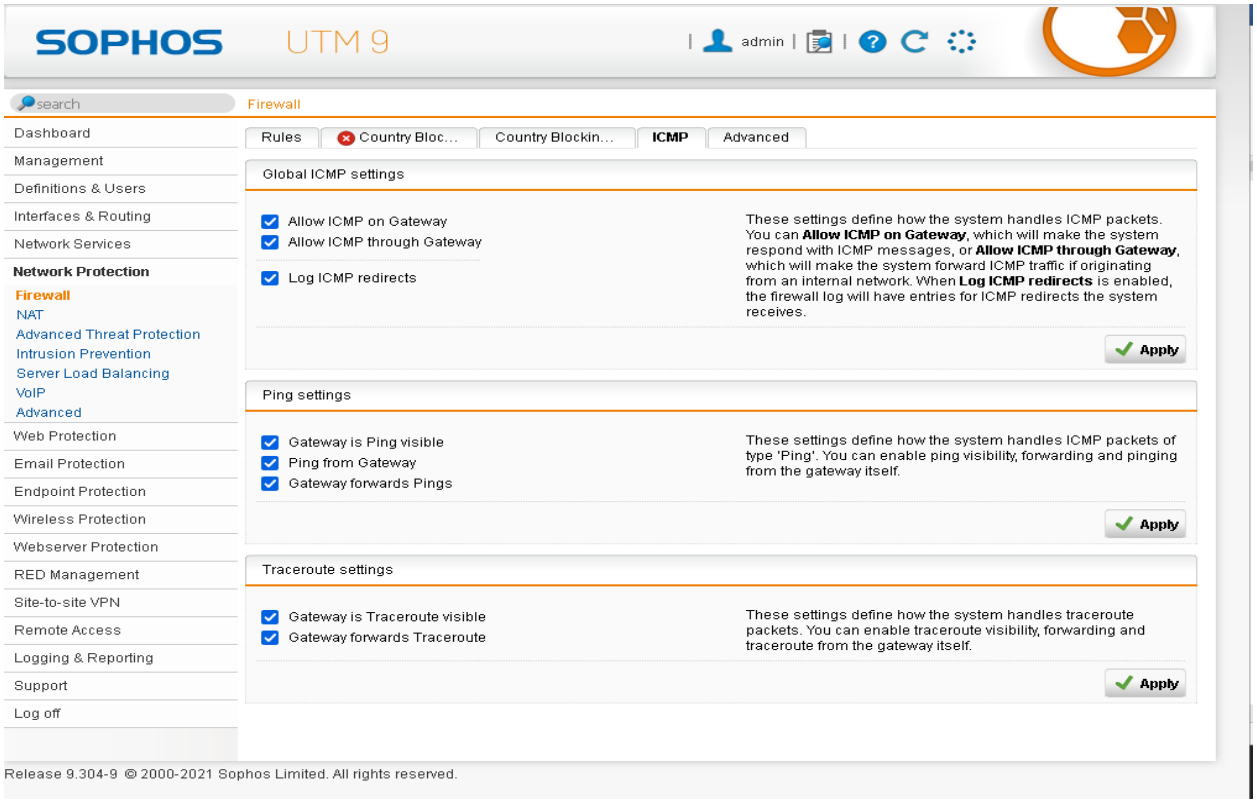


Figure 4-25 Define message digests for OSPF authentication.

Allowing internet connection.

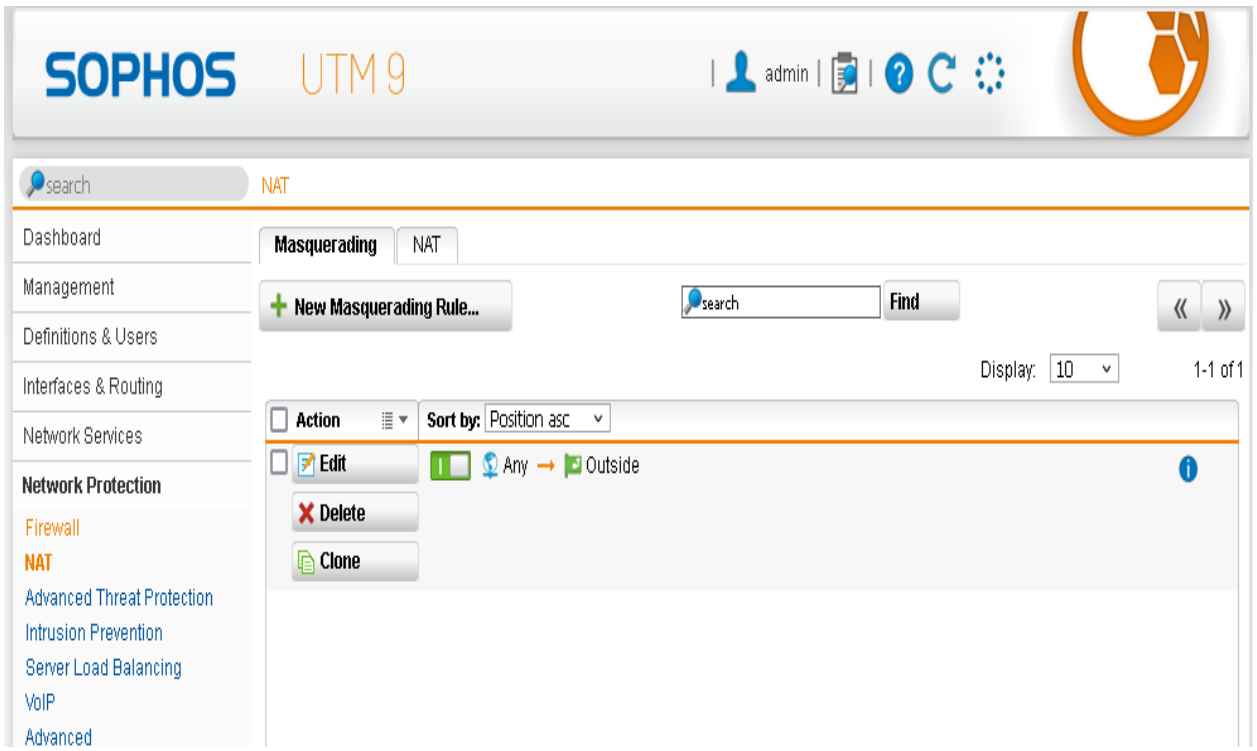


Figure 4-26 Allowing any connection from inside network to Sophos Firewall.

Allowing NAT to be able to connect to internet but still unable to connect to internet because that is not allowed on the firewall so, in the following images, we will allow internet connections in the firewall.

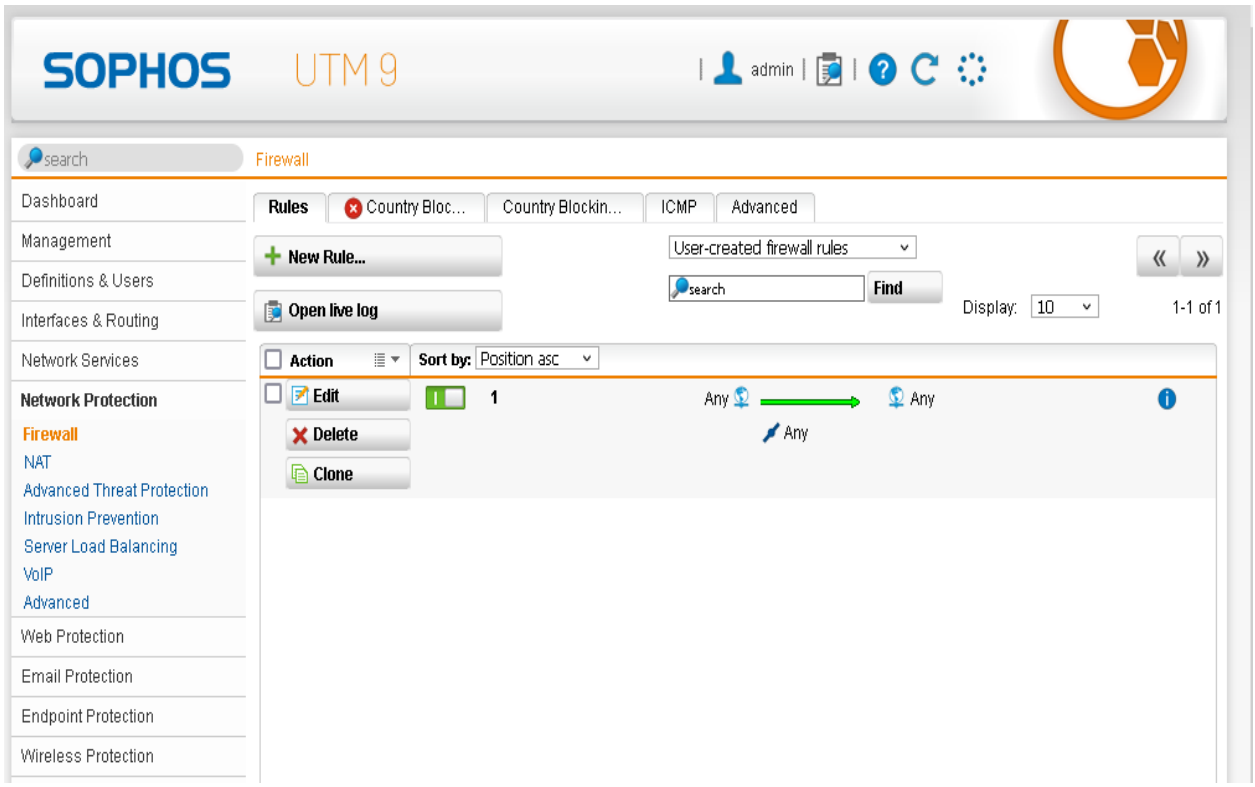


Figure 4-27 Allowing Internet Connections through Sophos Firewall.

This is what allow any connection to the internet.

Network definitions.

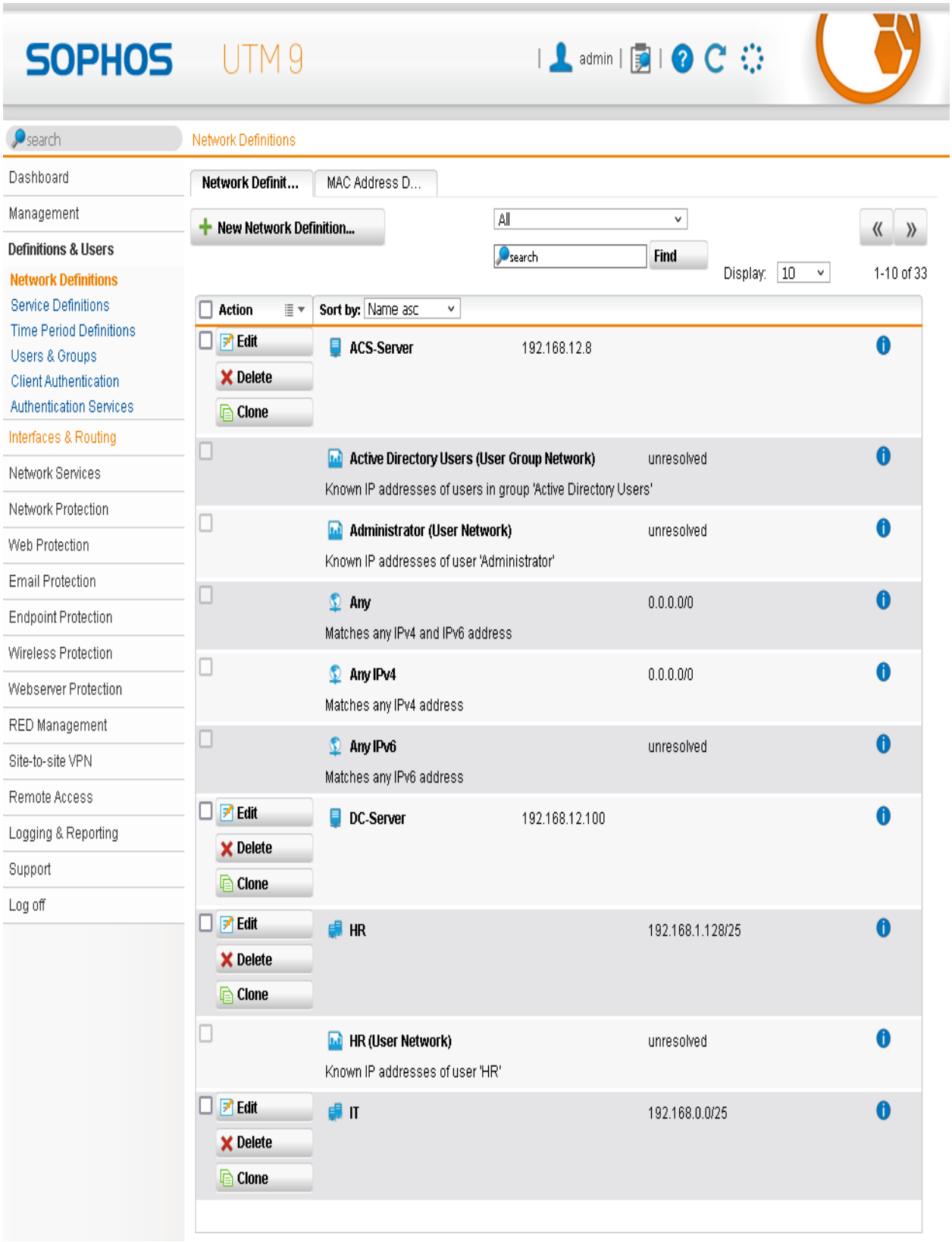


Figure 4-28 User-definition and servers in the firewall.

Web filter profiles

This section in figure 4-29 is used to filter packets to prevent or allow them from stablish connections to specific websites according to the department need.

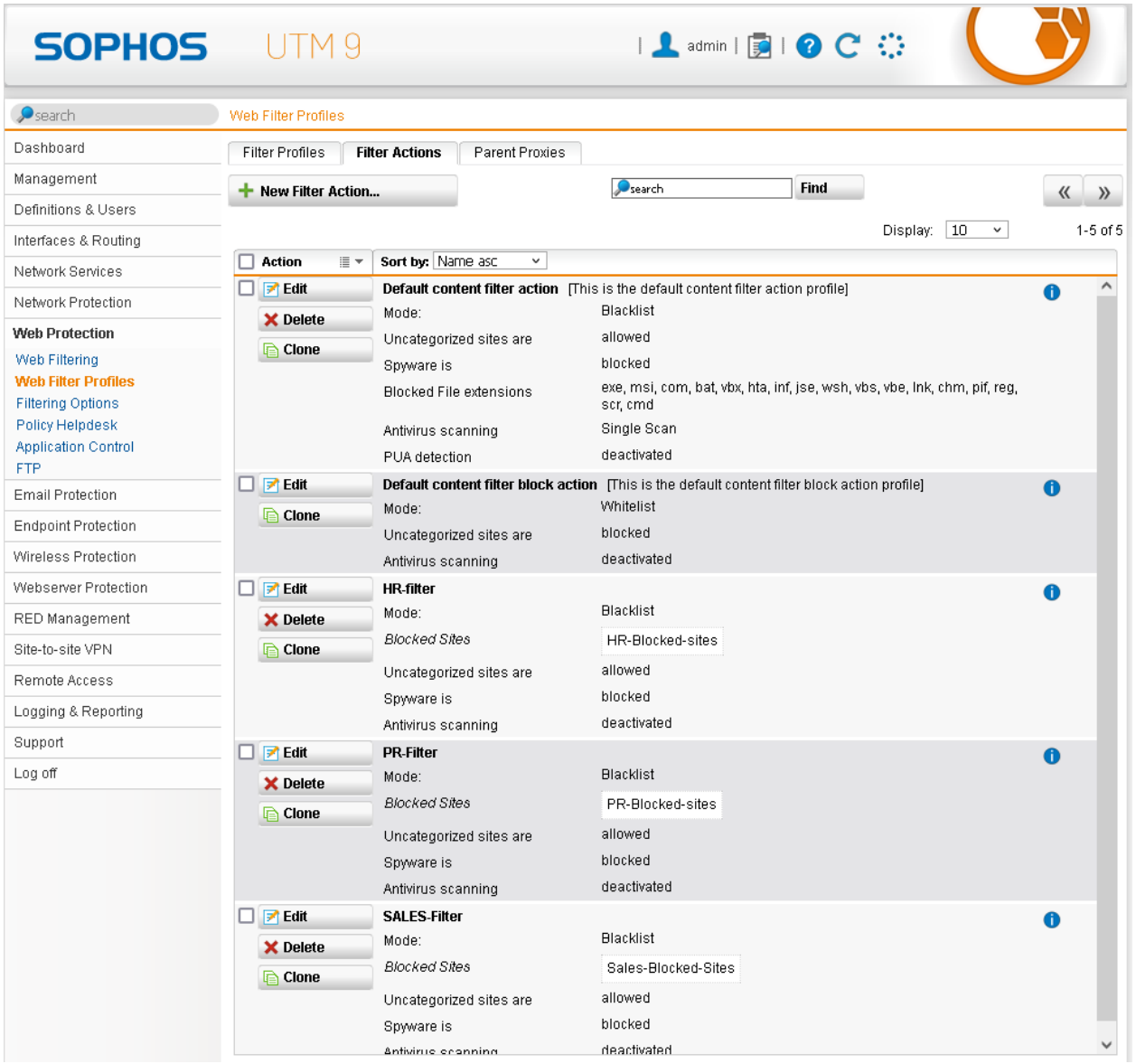


Figure 4-29 filters for websites and applications for each department.

Defining filter actions by department in SOPHOS Firewall to allow or deny the website only will be useful for department.

Application control

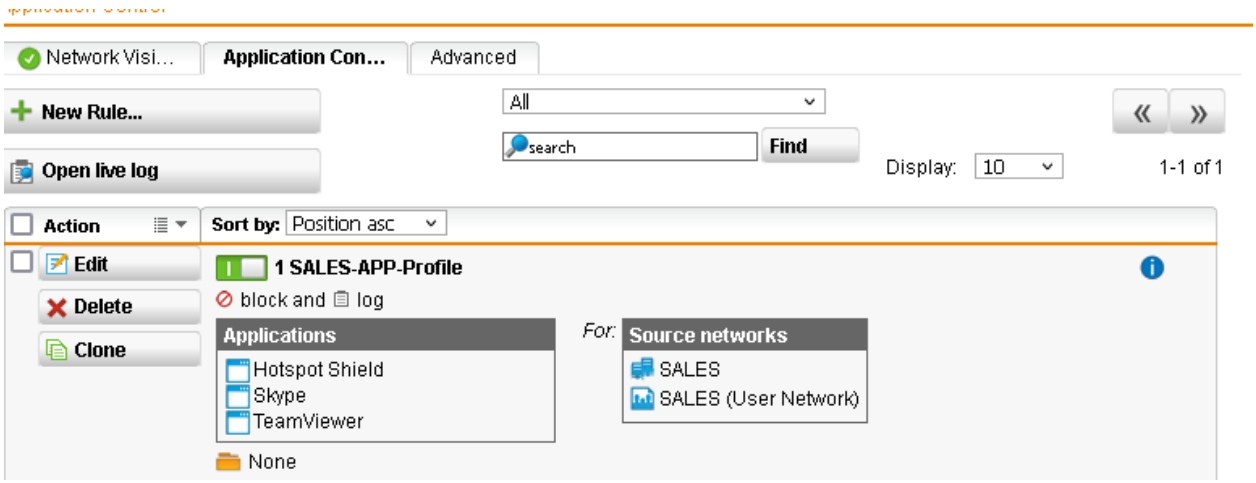


Figure 4-30 application filtering for user needs.

Allow and disallow specific applications for specific department, here, we closed skype, TeamViewer, and hotspot shared for sales.

4.2.1 Testing

```
R14#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.0.76 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/25] via 10.0.0.76, 00:00:19, FastEthernet0/0
R14#ping 10.0.0.76
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.76, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/19/60 ms
R14#ping 10.0.0.73
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.73, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 16/22/24 ms
R14#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R14#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/72/96 ms
R14#
```

Figure 4-31 R14 reads Firewall and ping correctly to internet.

Shows that the firewall permits connecting to internet, here shows before allowing it in firewall no ping to internet then pinging to it again (8.8.8.8 ➔google Servers)

but because of not running all devices of the project at once, I cannot ping to "**google.com**" which will be changed from DNS that running on Active Directory.

```
R14#ping google.com
Translating "google.com"...domain server (192.168.12.100)
% Unrecognized host or address, or protocol not running.

R14#
R14#ping google.com
Translating "google.com"...domain server (192.168.12.100) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.58.198.78, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/77/108 ms
R14#
```

Figure 4-32 Ping correctly to google.

Here, ping to google.com is unrecognized then after ADDC opened the ping command to "google.com" or any other website will work correctly as shown in the previous image, that means that the DNS working correctly, and this device reads DC.

Sophos firewall interfaces➔the physical interface we will access the firewall through it, IP address **https://192.168.146.100:4444**

Interface inside and outside with IP addresses 10.0.0.76 and outside interface.

```
R#ping 10.0.0.76
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.76, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/22/56 ms
R#
```

Figure 4-33 Successful Ping on Sophos Firewall from R13.

The firewall is pingable from the router (**R13**) connected to it, that means SOPHOS Firewall is working successfully.

```
Gateway of last resort is 10.0.0.76 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/25] via 10.0.0.76, 00:06:03, FastEthernet0/0
      10.0.0.0/8 is variably subnetted, 18 subnets, 3 masks
D EX      10.0.0.8/30 [170/2556160] via 10.0.0.45, 00:05:45, FastEthernet1/1
                      [170/2556160] via 10.0.0.41, 00:05:45, FastEthernet2/0
D EX      10.0.0.12/30 [170/2556160] via 10.0.0.45, 00:05:45, FastEthernet1/1
                       [170/2556160] via 10.0.0.41, 00:05:45, FastEthernet2/0
D         10.0.0.24/30 [90/30720] via 10.0.0.45, 00:52:48, FastEthernet1/1
D         10.0.0.28/30 [90/30720] via 10.0.0.41, 00:34:51, FastEthernet2/0
D         10.0.0.32/30 [90/30720] via 10.0.0.45, 00:34:51, FastEthernet1/1
                       [90/30720] via 10.0.0.41, 00:34:51, FastEthernet2/0
D         10.0.0.36/30 [90/30720] via 10.0.0.49, 00:34:56, FastEthernet1/0
  --More--
```

Figure 4-34 R13 reads Sophos Firewall.

R13 reads firewall, and SOPHOS is configured successfully for routing protocols.

4.3 Servers

4.3.1 DHCP Server

This section shows you the DHCP Server Pools and how to configure a POOL then the results will be in the testing section.

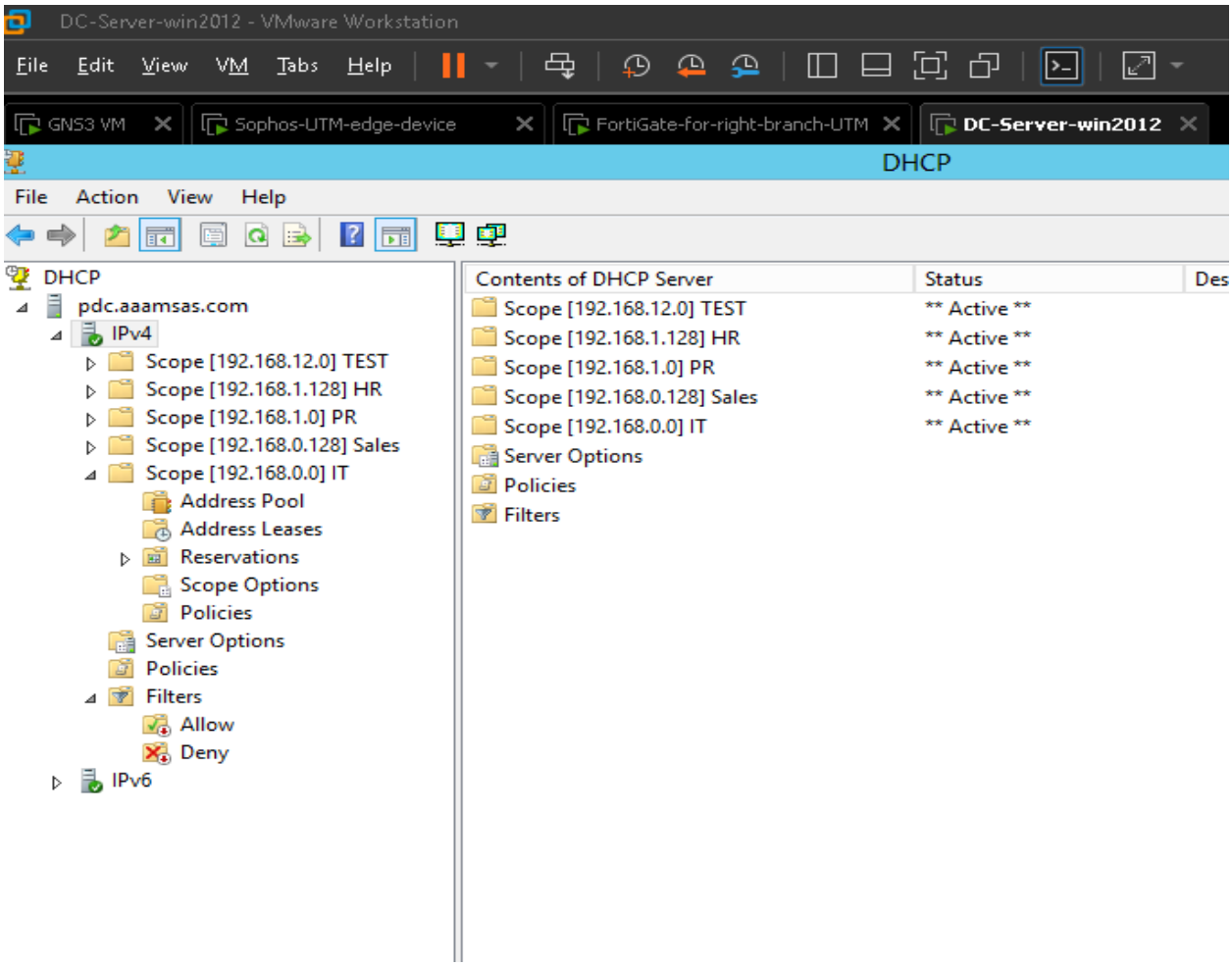


Figure 4-35 DHCP POOLs for each branch.

DHCP POOLs for each department of the company

4.3.1.1 Creation of POOL

Steps for creating new scope or new pool in DHCP Server.

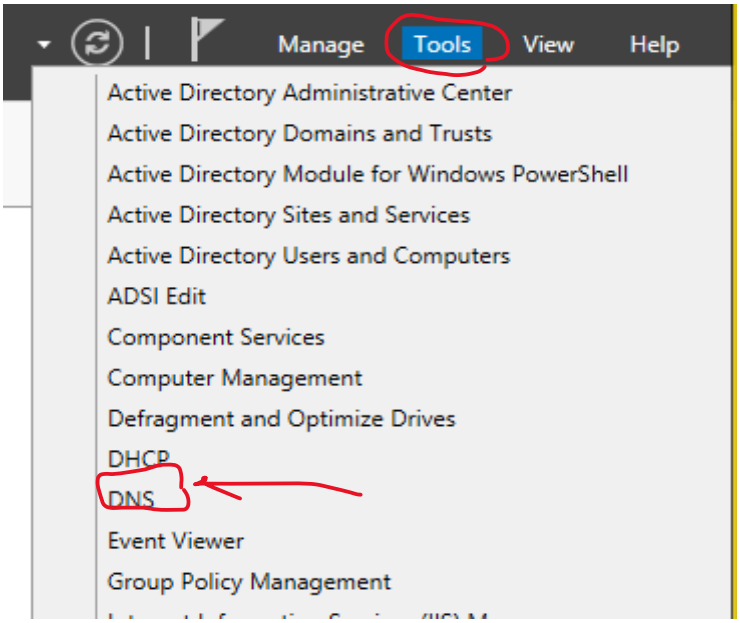


Figure 4-36 Tools of windows server.

Choose DHCP from tools list.

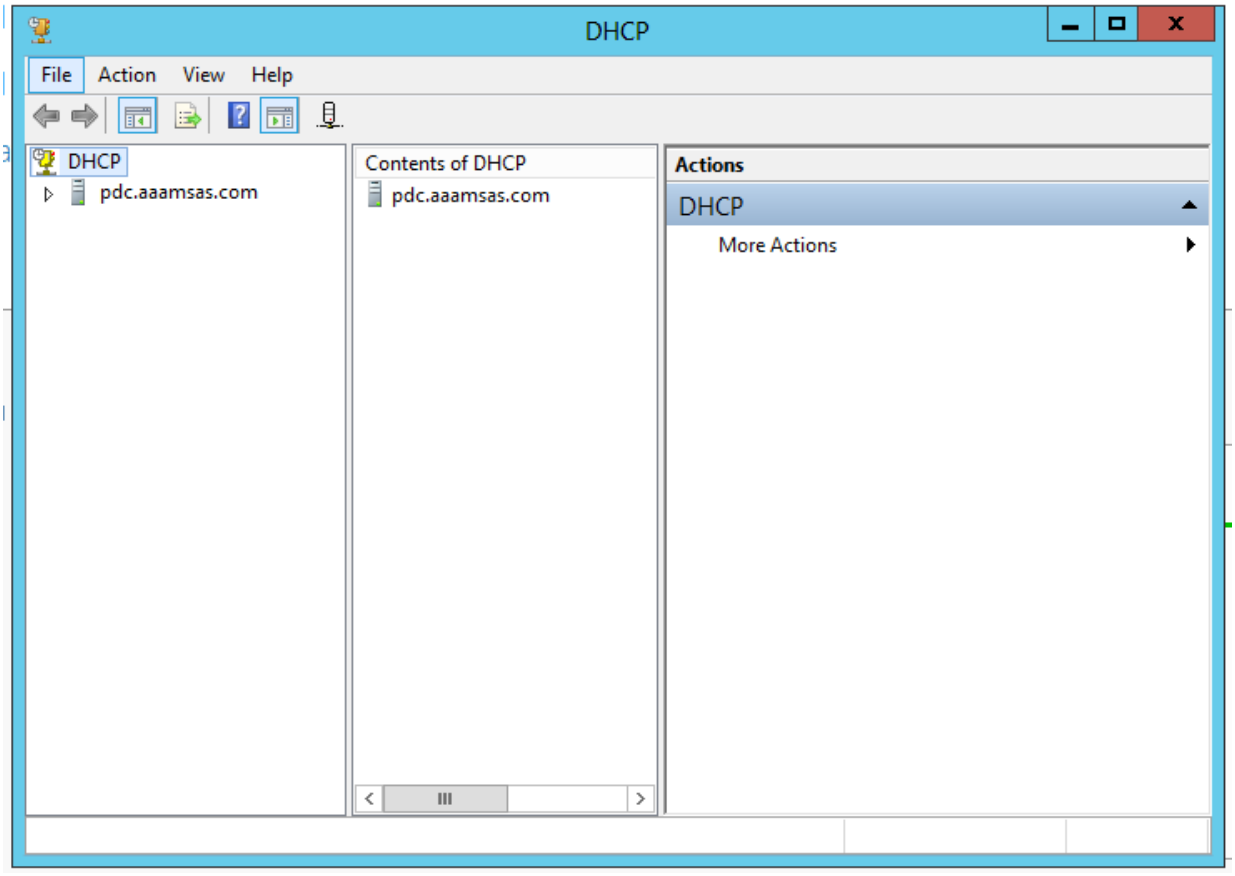


Figure 4-37 Adding DHCP POOL step 2.

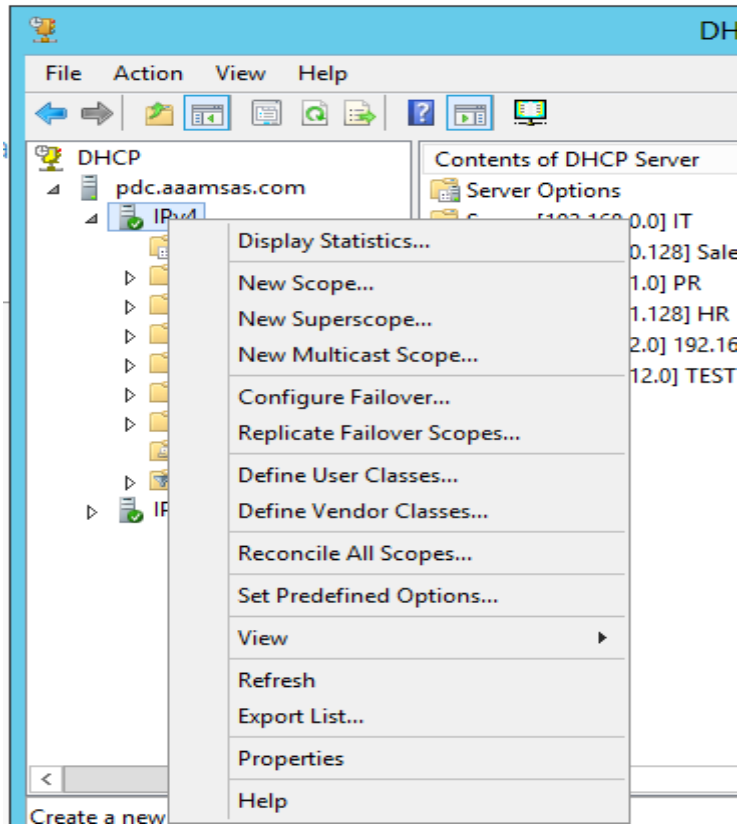


Figure 4-38 Adding DHCP POOL step 3

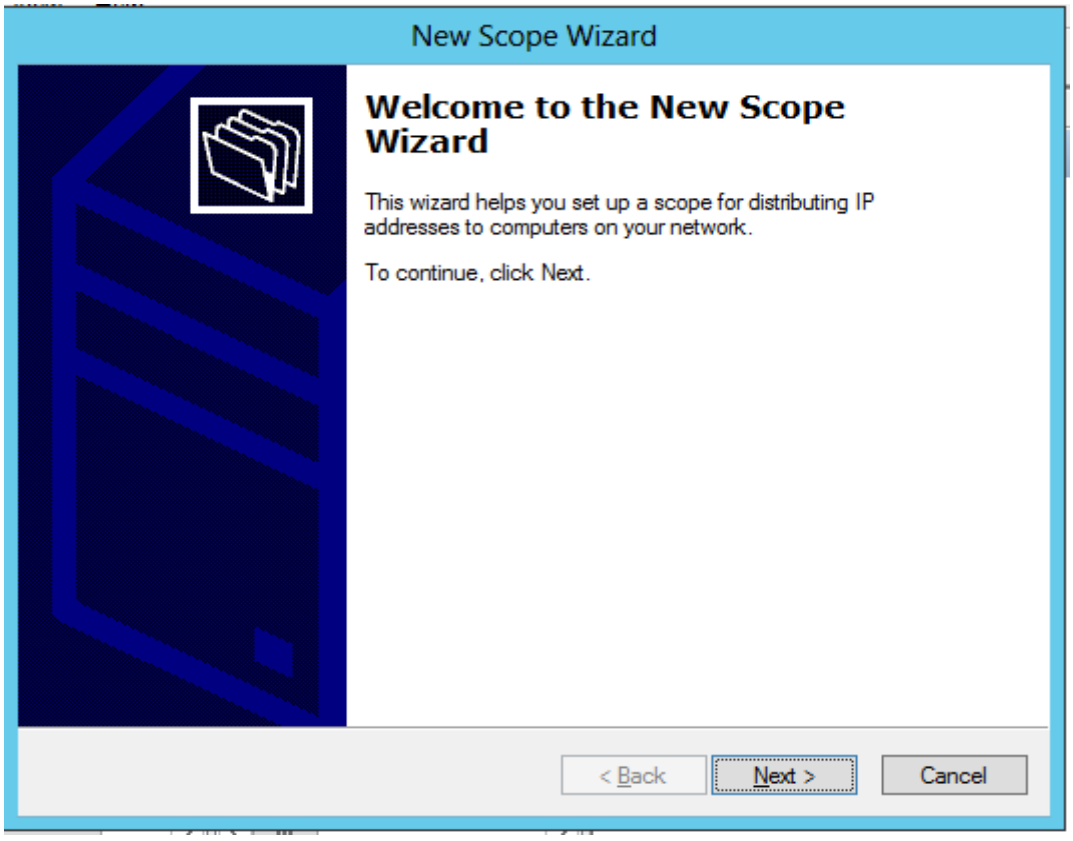


Figure 4-39 Adding DHCP POOL step 4.

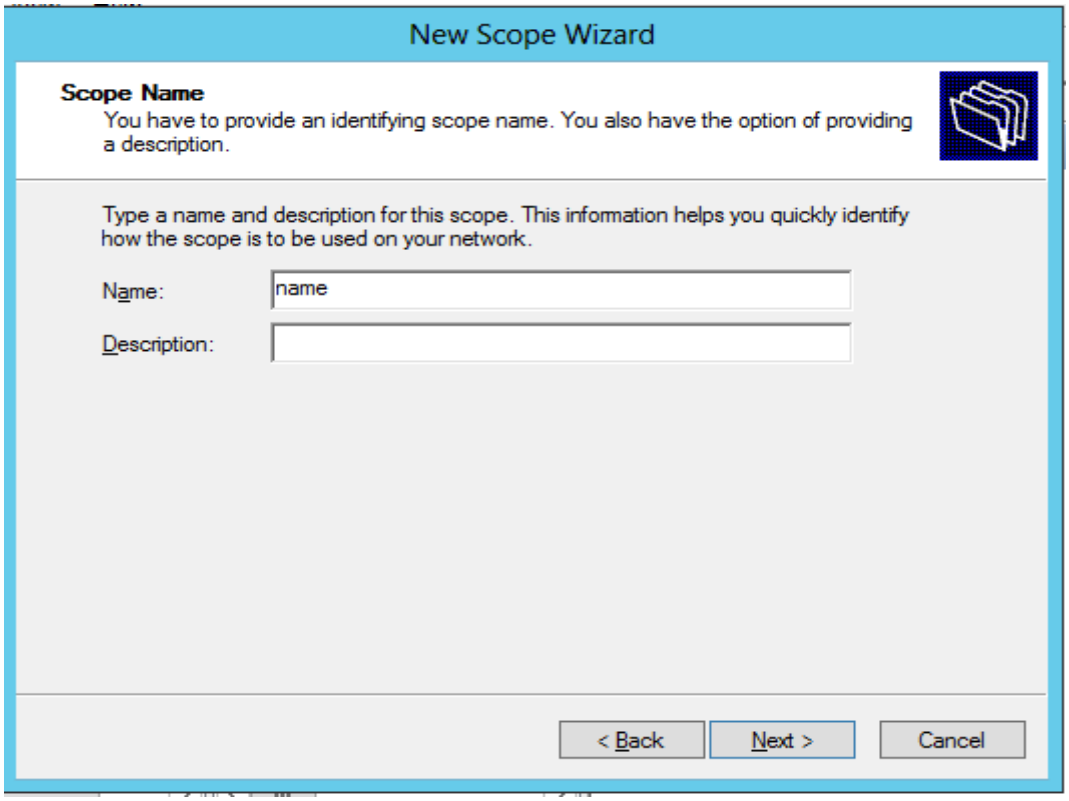


Figure 4-40 Adding DHCP POOL step 5.

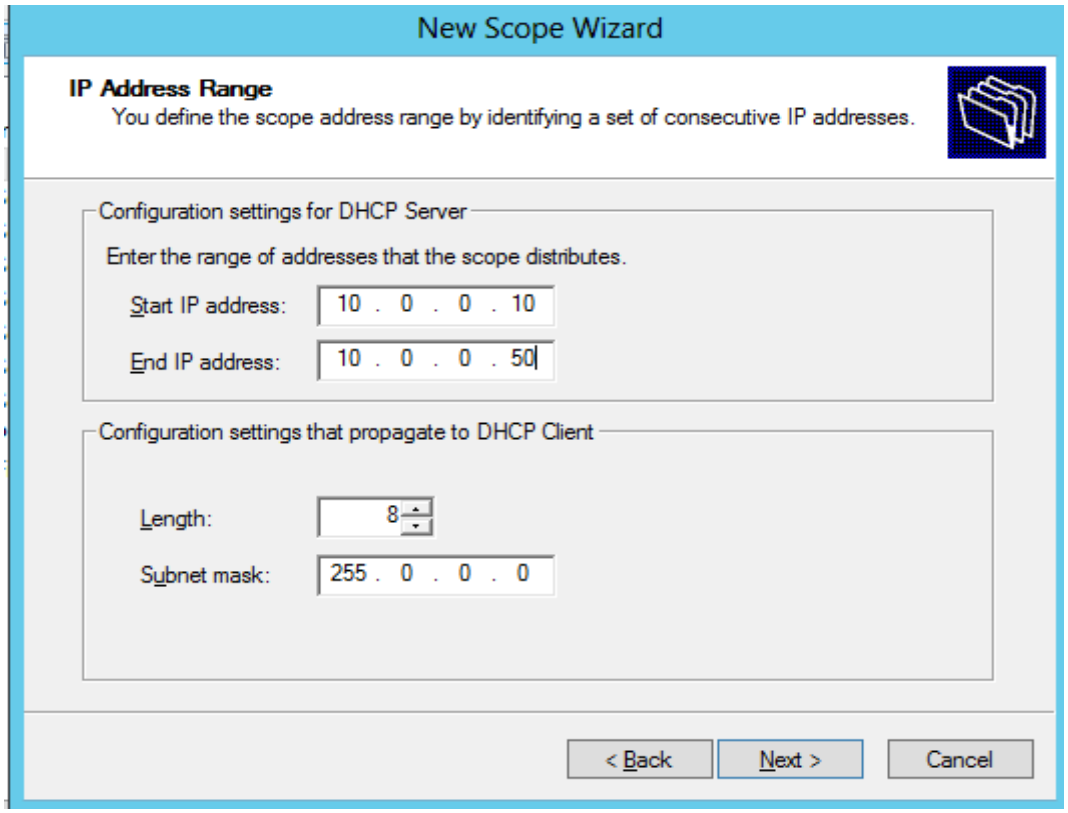


Figure 4-41 Adding DHCP POOL step 6.

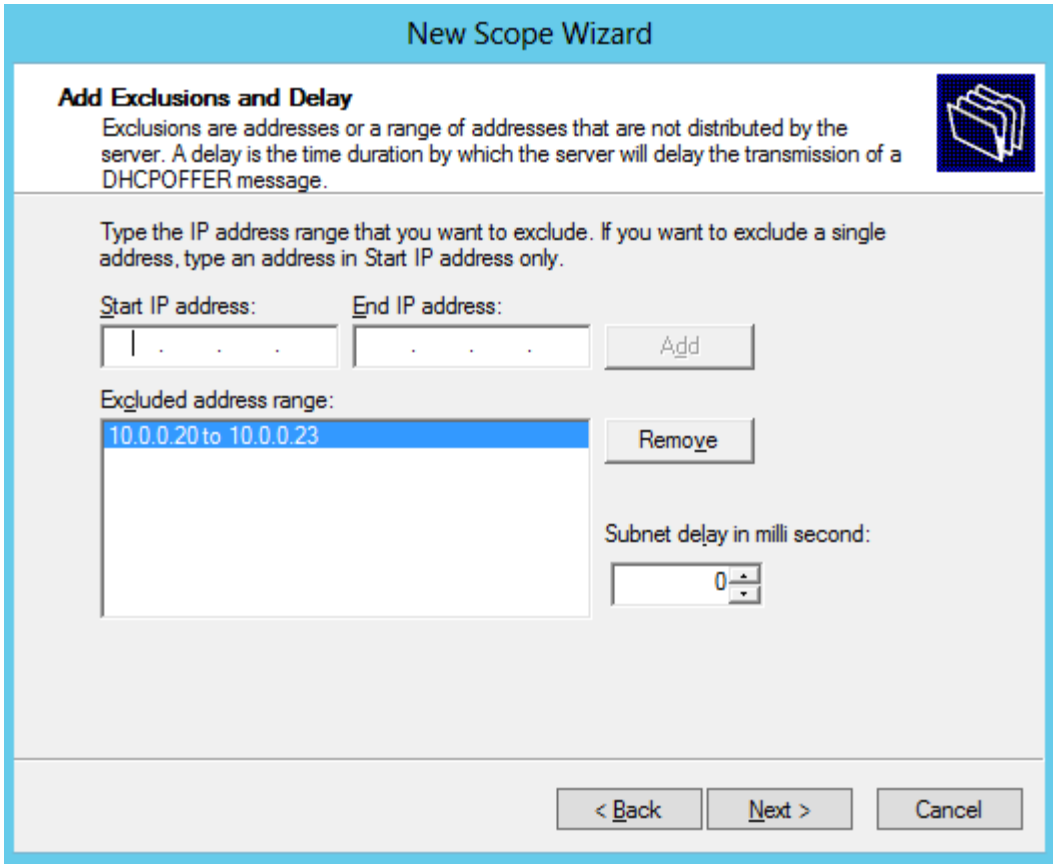


Figure 4-42 Adding DHCP POOL step 7.

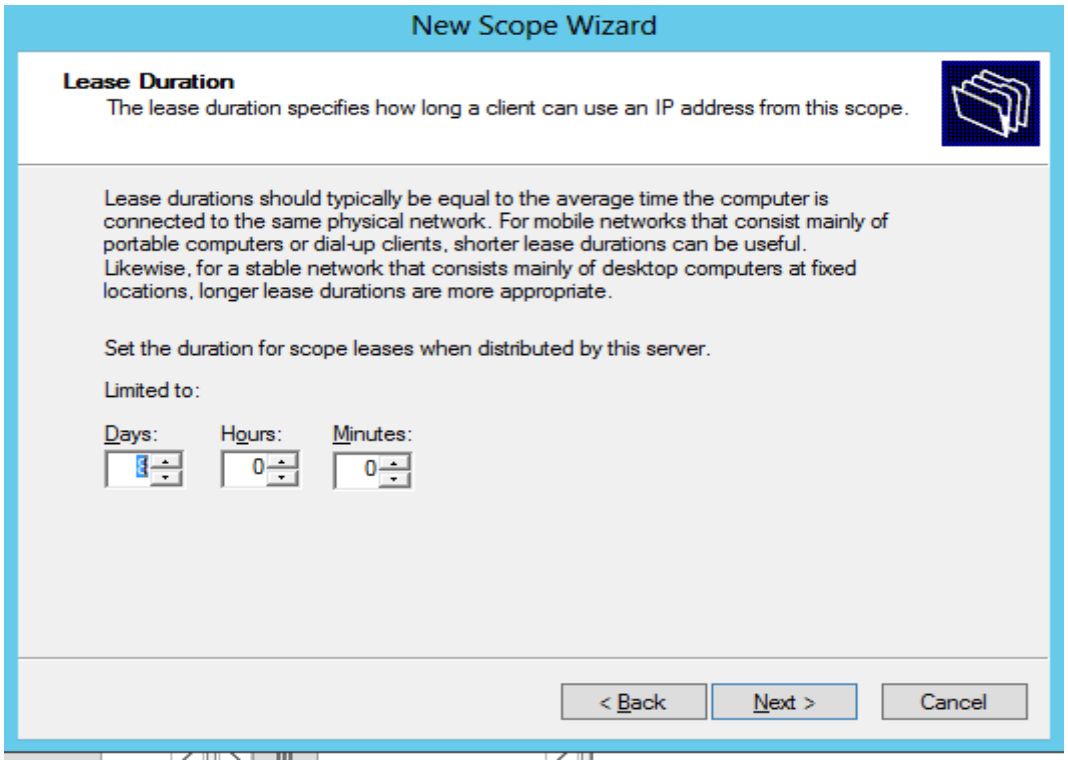


Figure 4-43 Adding DHCP POOL step 8.

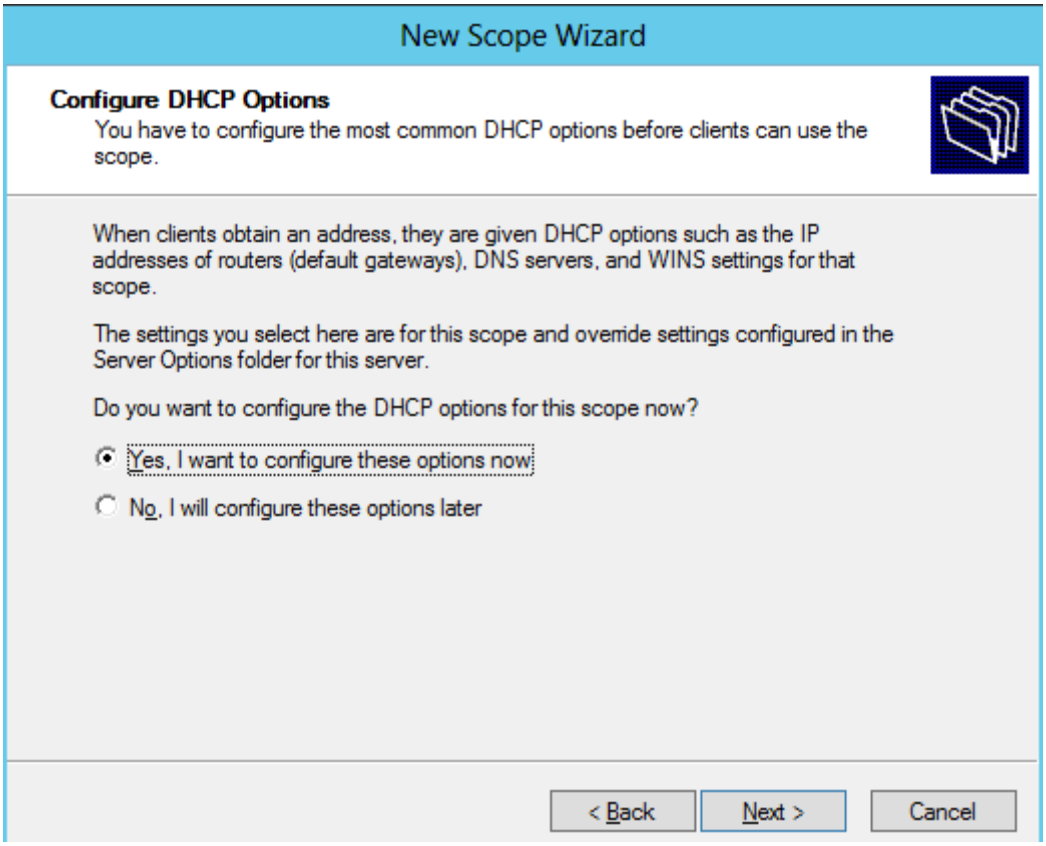


Figure 4-44 Adding DHCP POOL step 9.

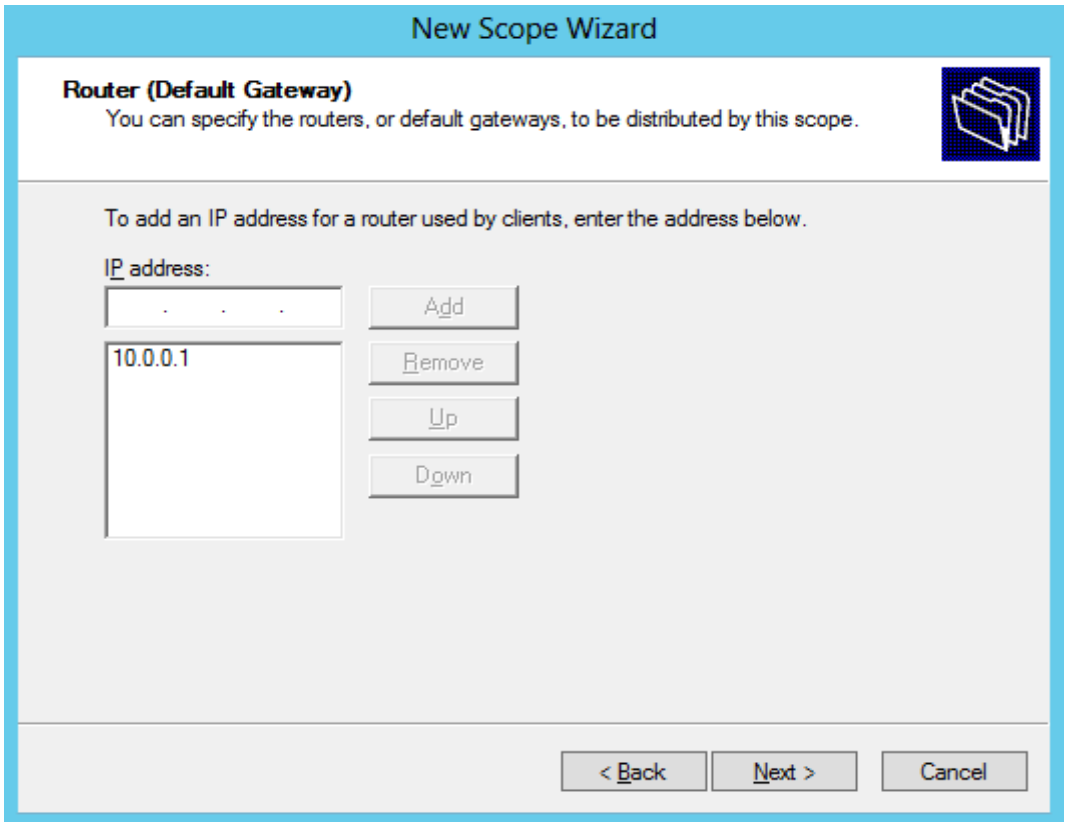


Figure 4-45 adding DHCP POOL step 10.

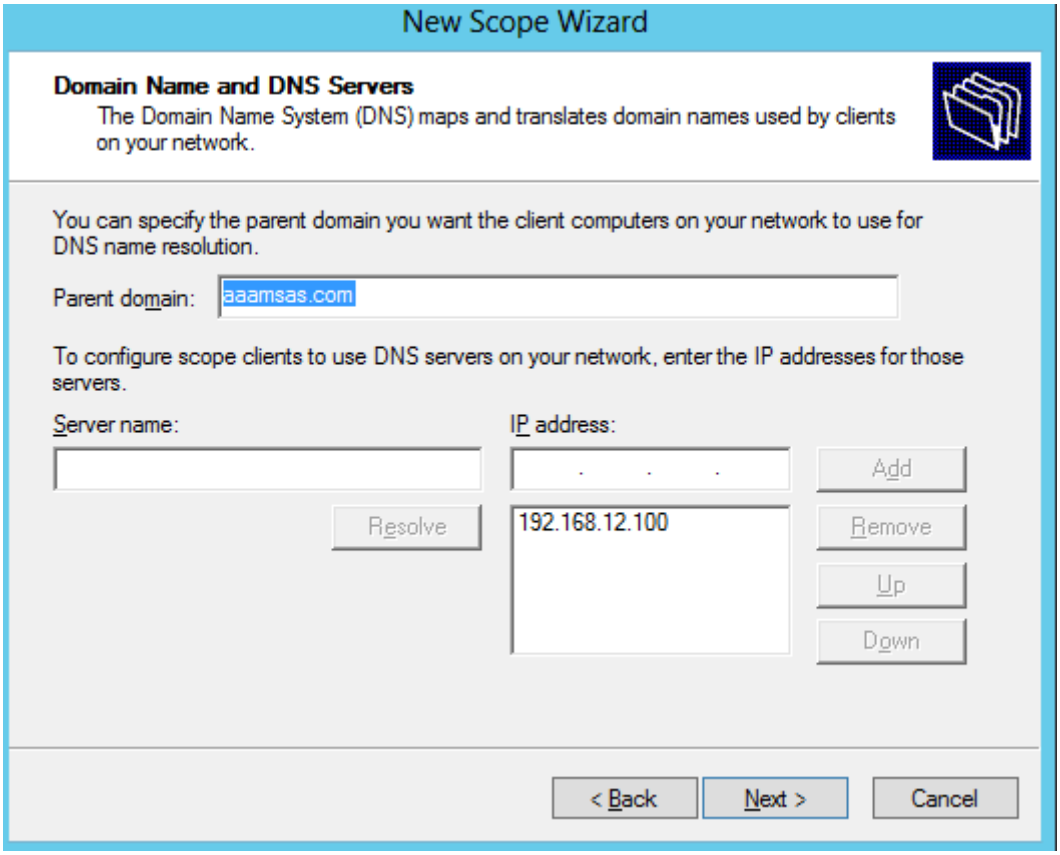


Figure 4-46 Adding DHCP POOL step 11.

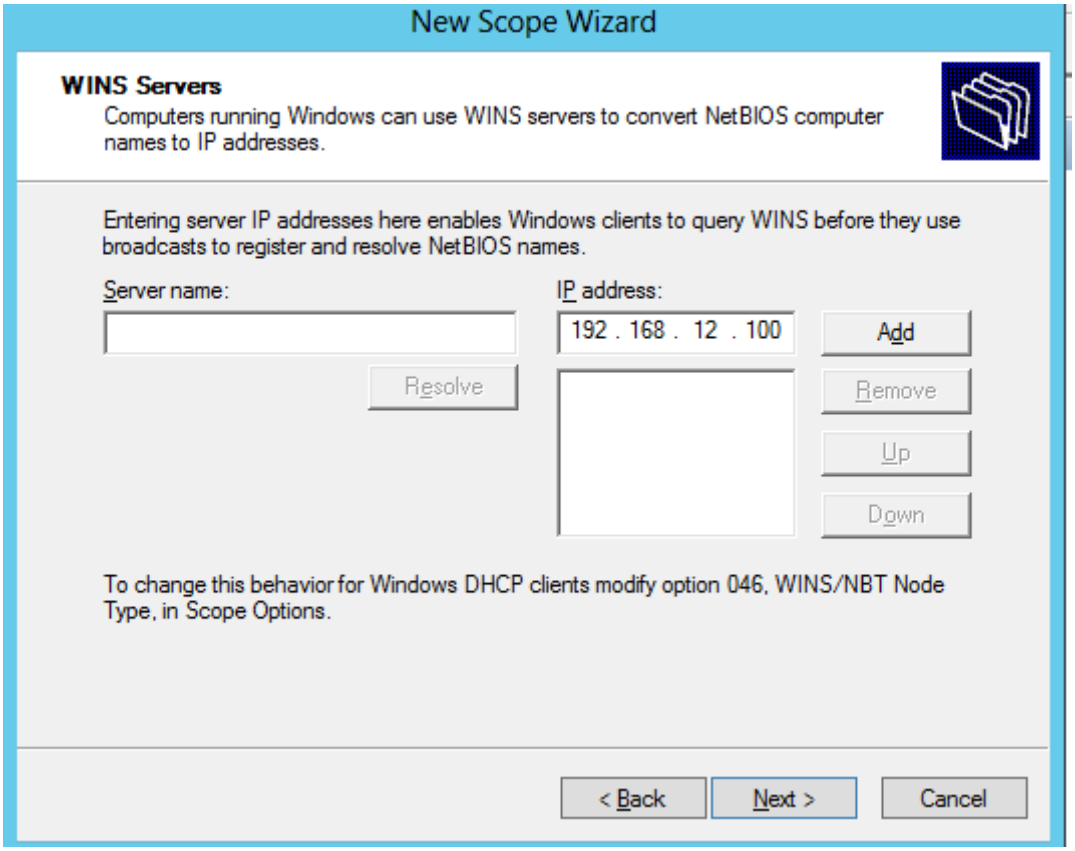


Figure 4-47 Adding DHCP POOL step 12.

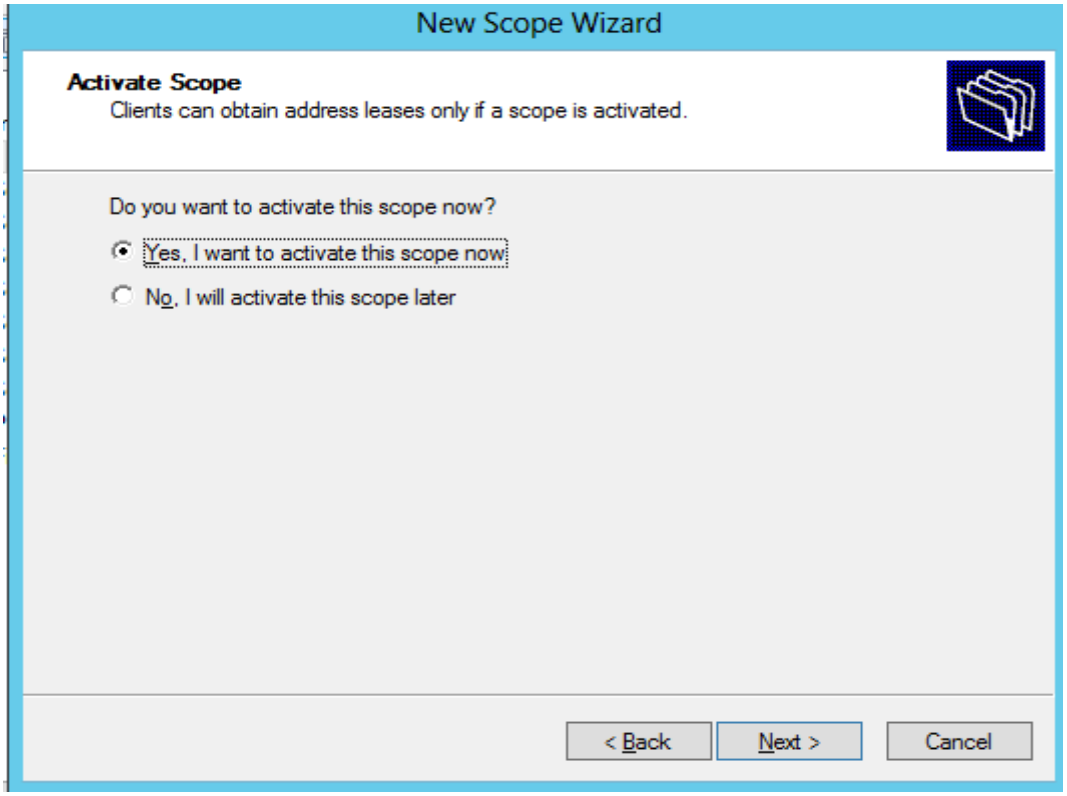


Figure 4-48 adding DHCP POOL step 13.

Obtaining DHCP from SALES Pool of DHCP Server for a sales PC.

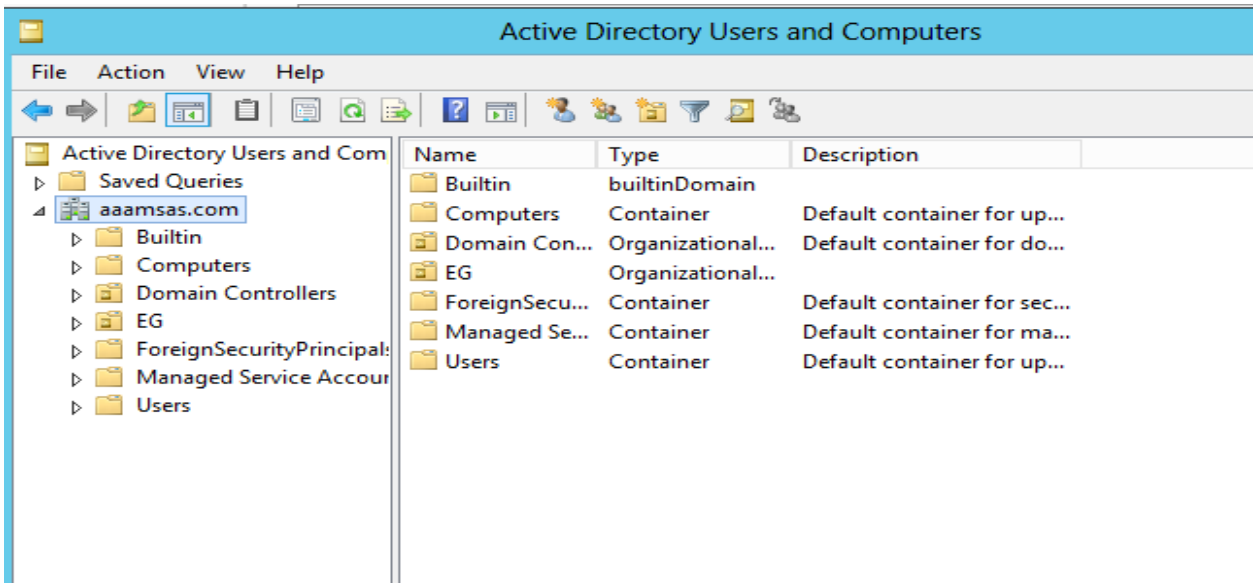


Figure 4-49 User definition in DC Server.

Creating users and groups on the ADDC Server all in EG folder.

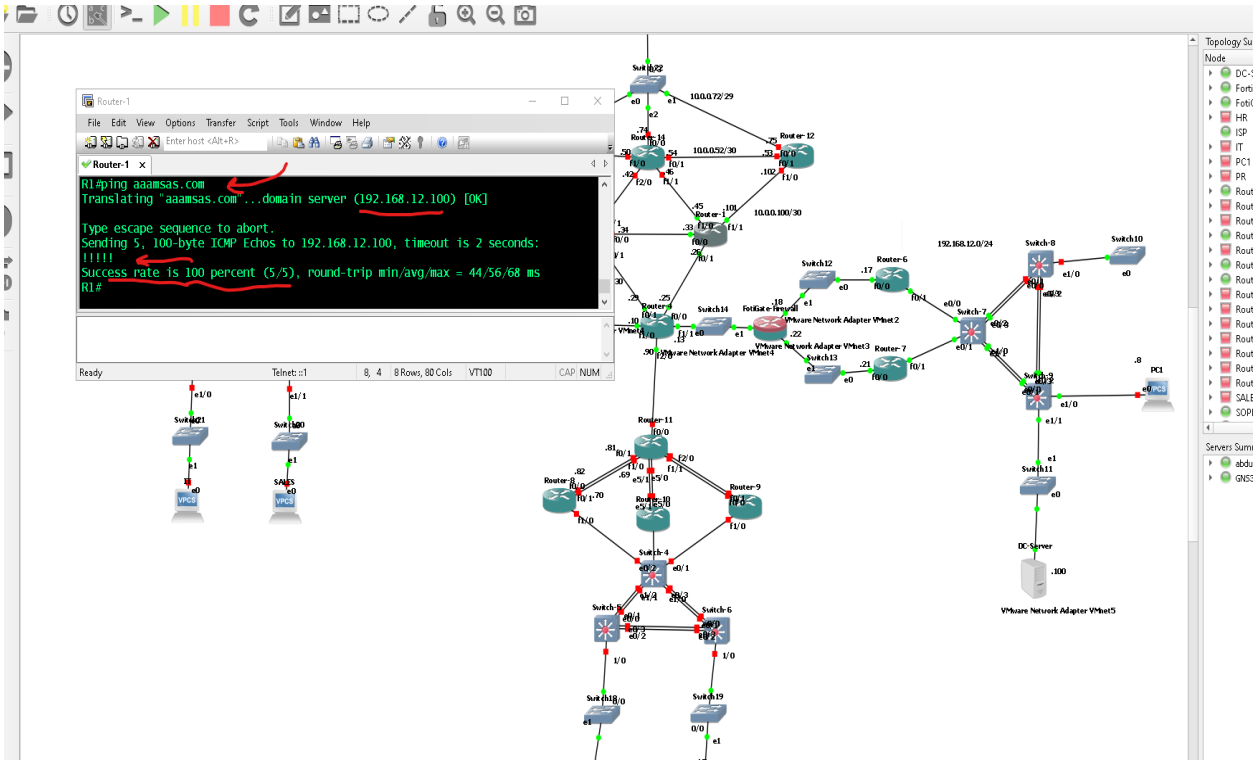


Figure 4-50 Successful ping on DC Server from R1

Here, successfully ping to the domain. We created “aaamsas.com” is the same as ping on 192.168.12.100

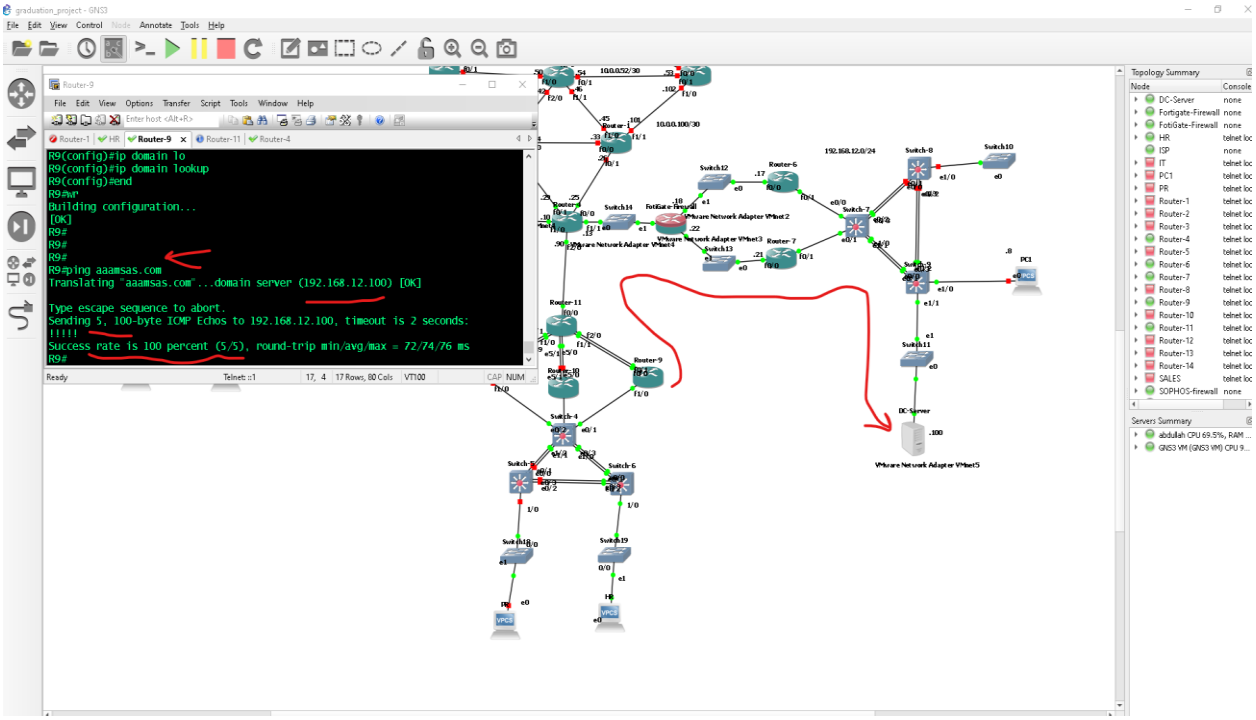


Figure 4-51 Successful ping on DC Server from R9

As shown in the image R9 ping to ADDC successfully.

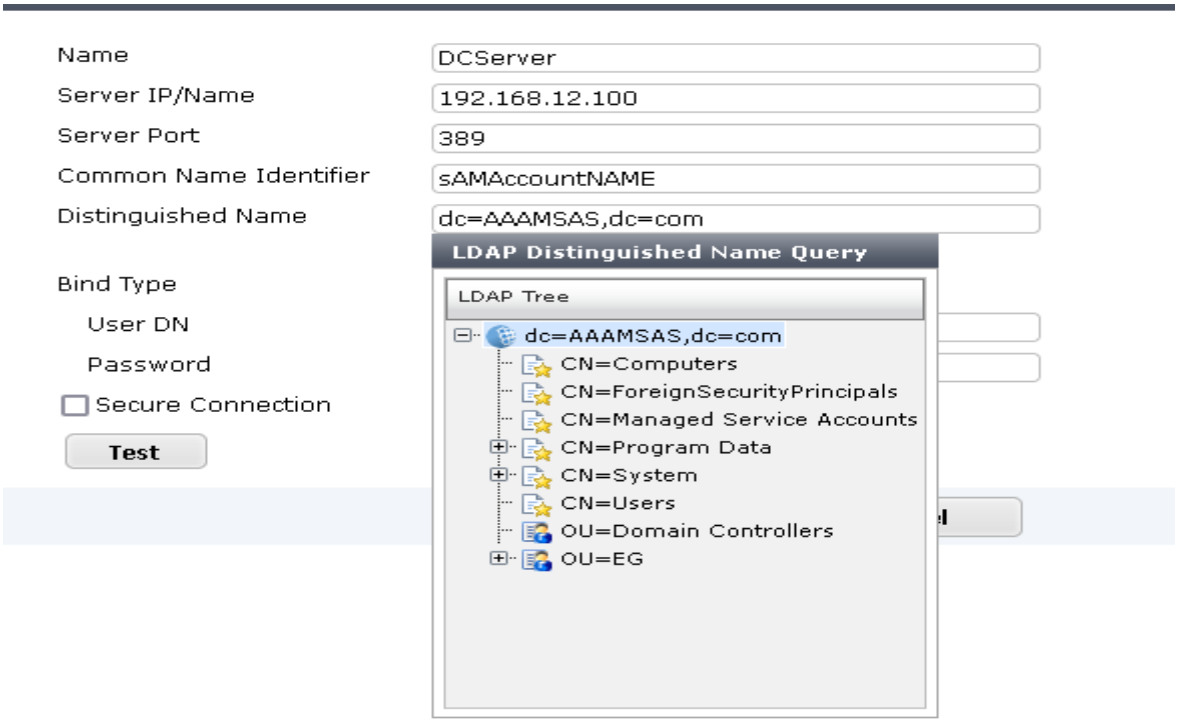


Figure 4-52 ADDC definition in FortiGate Firewall.

Defining ADDC in FortiGate firewall.

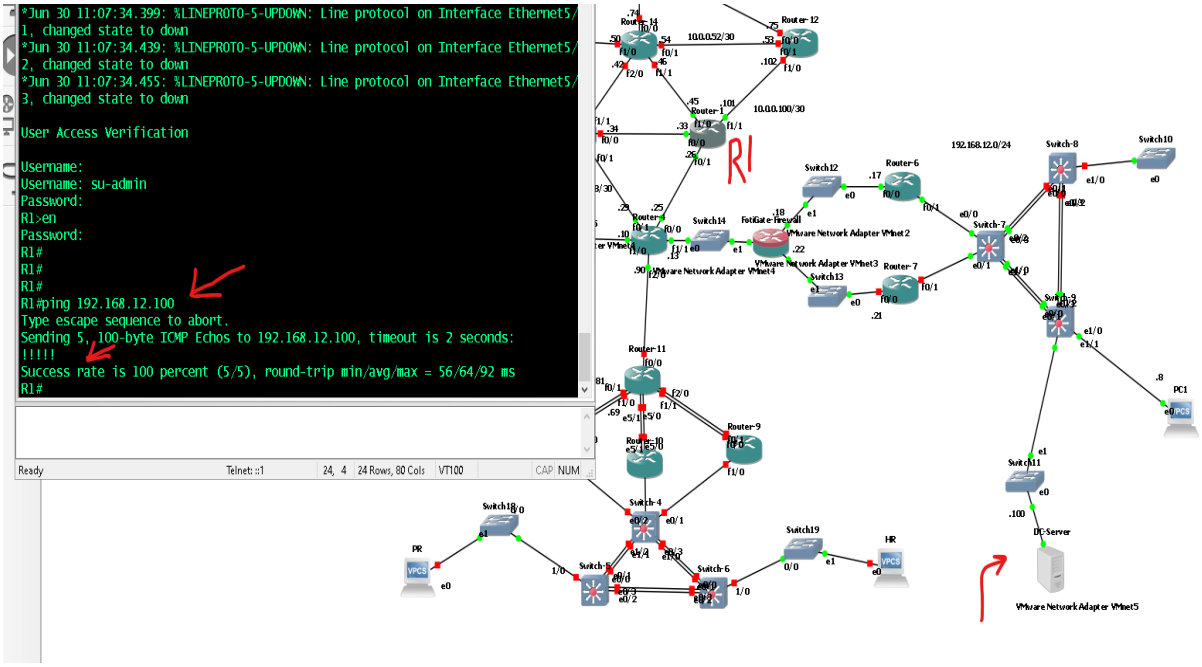


Figure 4-53 Successful ping on DC Server IP Address.

Successfully ping on ADDC from R1.

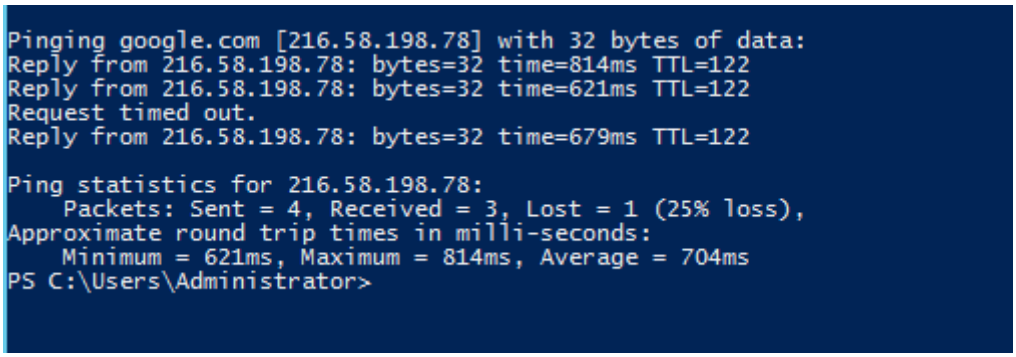


Figure 4-54 Successful internet connection from DC Server.

This ping command is successfully and request time out because of high traffic in the network, that means that DNS and DC working correctly which it correctly resolved google.com to its IP address.

Note:

I tell you high traffic because of Wireshark captured +6M packets in 1 minute.

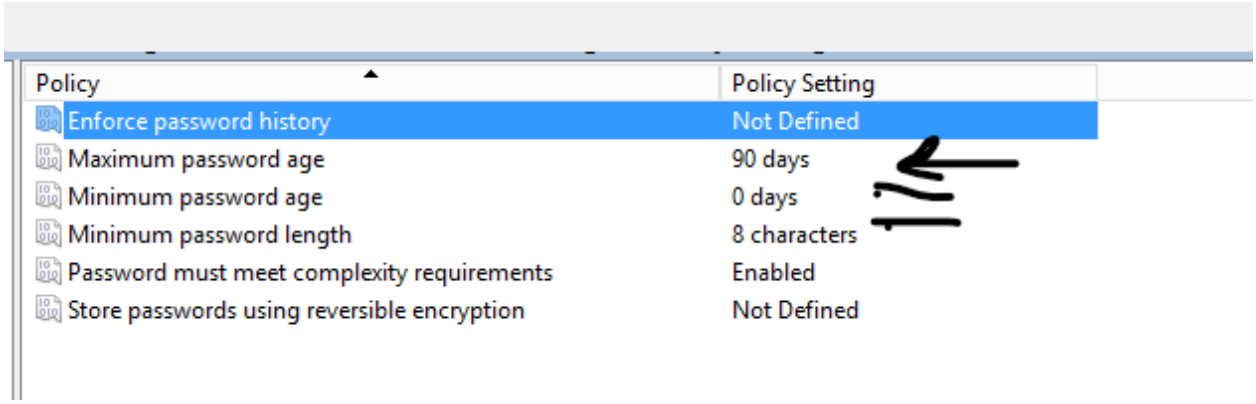


Figure 4-55 Password specs on DC Server.

Here, allowing password to be changed after 90 days as a maximum period or account will be deleted or halted, also we make the password to be strong password and at least 8 characters as shown in the image.

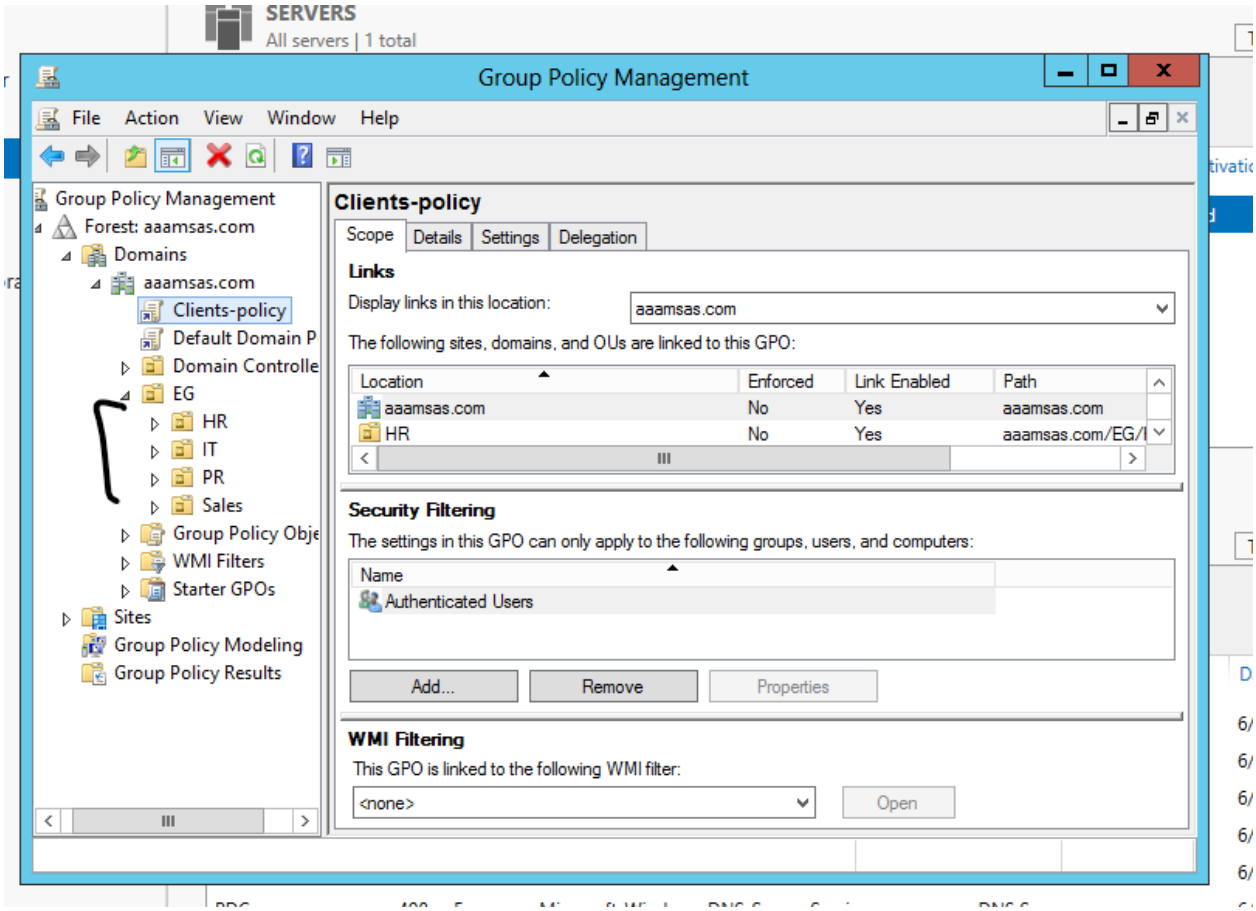


Figure 4-56 Users GPO.

Creating group policy in ADDC for clients to enable or disable specific features.

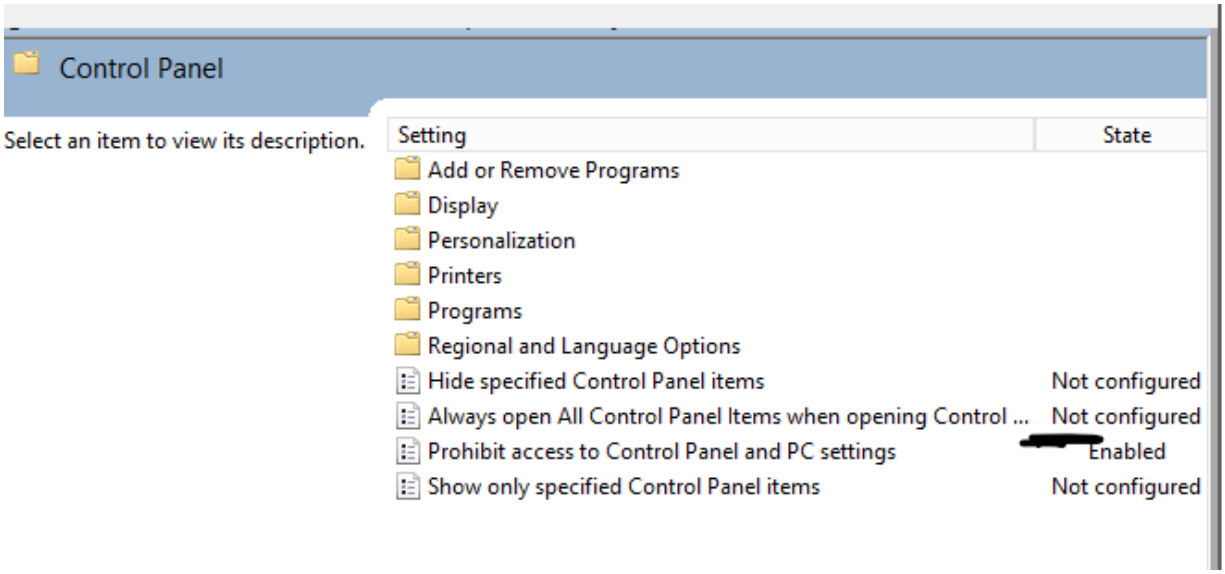


Figure 4-57 Control Panel blocking for ordinary user.

Prevent ordinary users from accessing control panel.

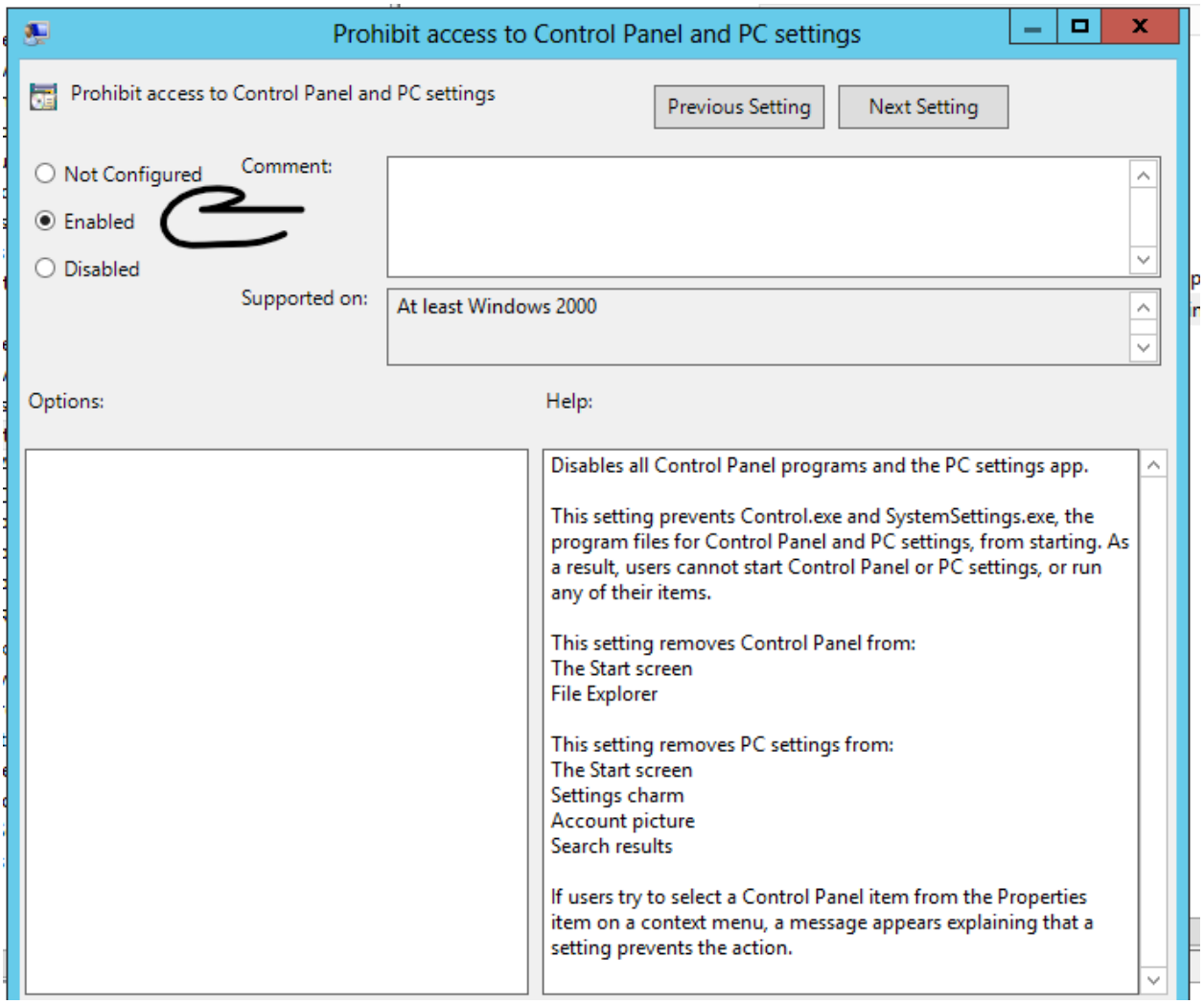


Figure 1.41 Control Panel prohibit access

Enable the feature of preventing control panel.

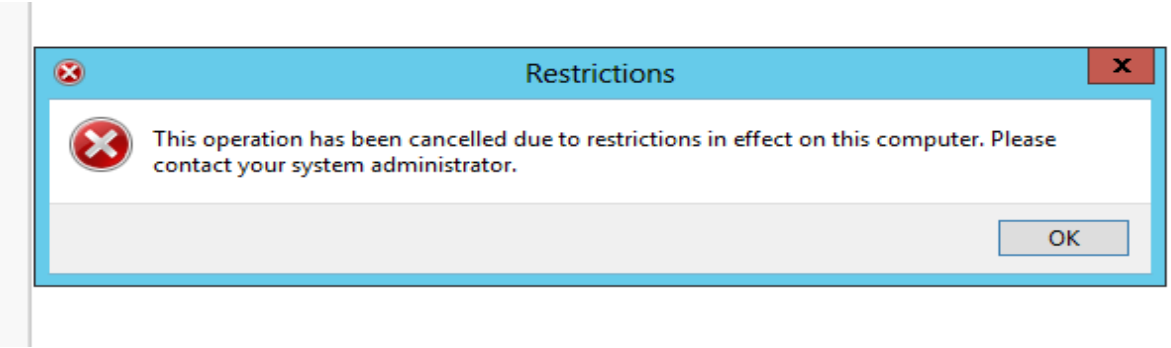


Figure 4-58 Pop Up window by clicking on control panel by non admin users.

This image shows the privilege of users not admin users that are prevented from accessing control panel.

4.3.2 Testing

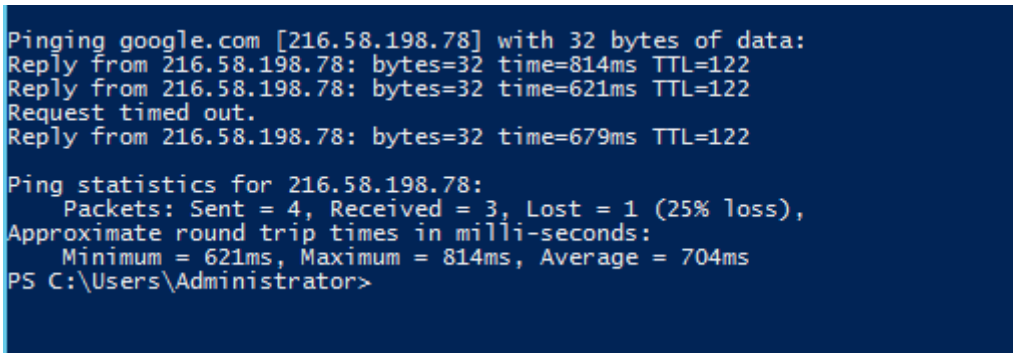


Figure 4-59 DC pings to internet correctly.

Ping on google.com from active directory domain controller successfully.

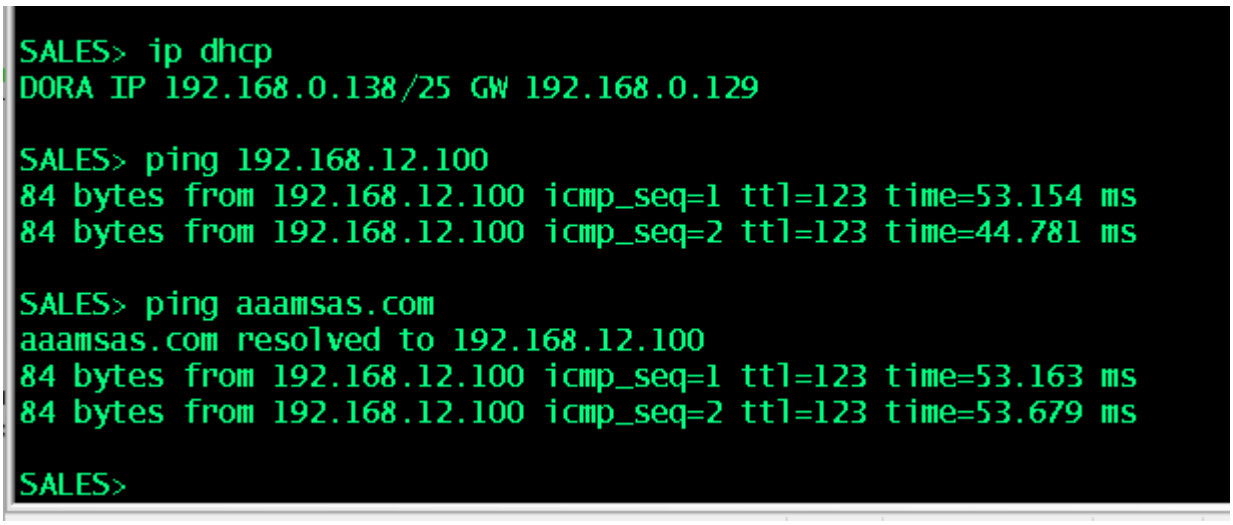


Figure 4-60 Successfully SALES PC takes DHCP IP.

```
SALES> sh ip

NAME         : SALES[1]
IP/MASK      : 192.168.0.138/25
GATEWAY      : 192.168.0.129
DNS          : 192.168.12.100
DHCP SERVER  : 192.168.12.100
DHCP LEASE   : 691022, 691200/345600/604800
DOMAIN NAME  : aaamsas.com
MAC          : 00:50:79:66:68:02
LPORT        : 10186
RHOST:PORT   : 127.0.0.1:10187
MTU:         : 1500
```

Figure 4-61 DHCP content of SALES PC.

```
IT> ip dhcp
DORA IP 192.168.0.10/25 GW 192.168.0.1

IT> ping 192.168.12.100
84 bytes from 192.168.12.100 icmp_seq=1 ttl=123 time=61.990 ms
84 bytes from 192.168.12.100 icmp_seq=2 ttl=123 time=45.099 ms
84 bytes from 192.168.12.100 icmp_seq=3 ttl=123 time=58.395 ms
84 bytes from 192.168.12.100 icmp_seq=4 ttl=123 time=51.708 ms
84 bytes from 192.168.12.100 icmp_seq=5 ttl=123 time=39.347 ms

IT> ping aaamsas.com
aaamsas.com resolved to 192.168.12.100
84 bytes from 192.168.12.100 icmp_seq=1 ttl=123 time=59.280 ms
84 bytes from 192.168.12.100 icmp_seq=2 ttl=123 time=71.489 ms
84 bytes from 192.168.12.100 icmp_seq=3 ttl=123 time=62.291 ms
84 bytes from 192.168.12.100 icmp_seq=4 ttl=123 time=64.433 ms
84 bytes from 192.168.12.100 icmp_seq=5 ttl=123 time=63.402 ms

IT>
```

Figure 4-62 Successfully IT PC takes DHCP IP.

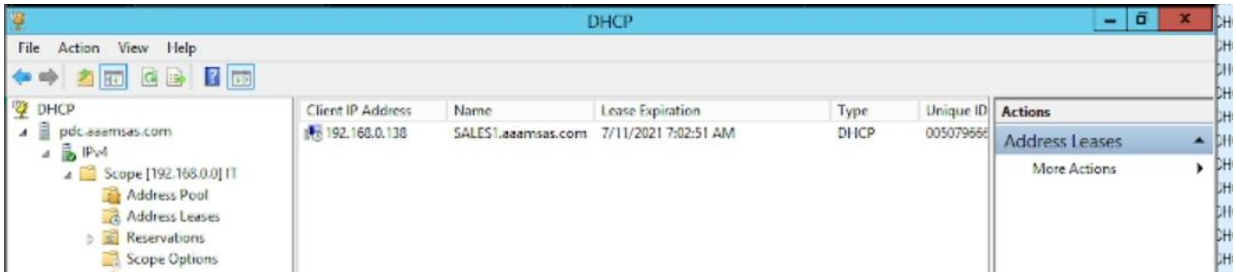


Figure 4-63 SALES PC IPC Stored in the DHCP Server in released IP section.

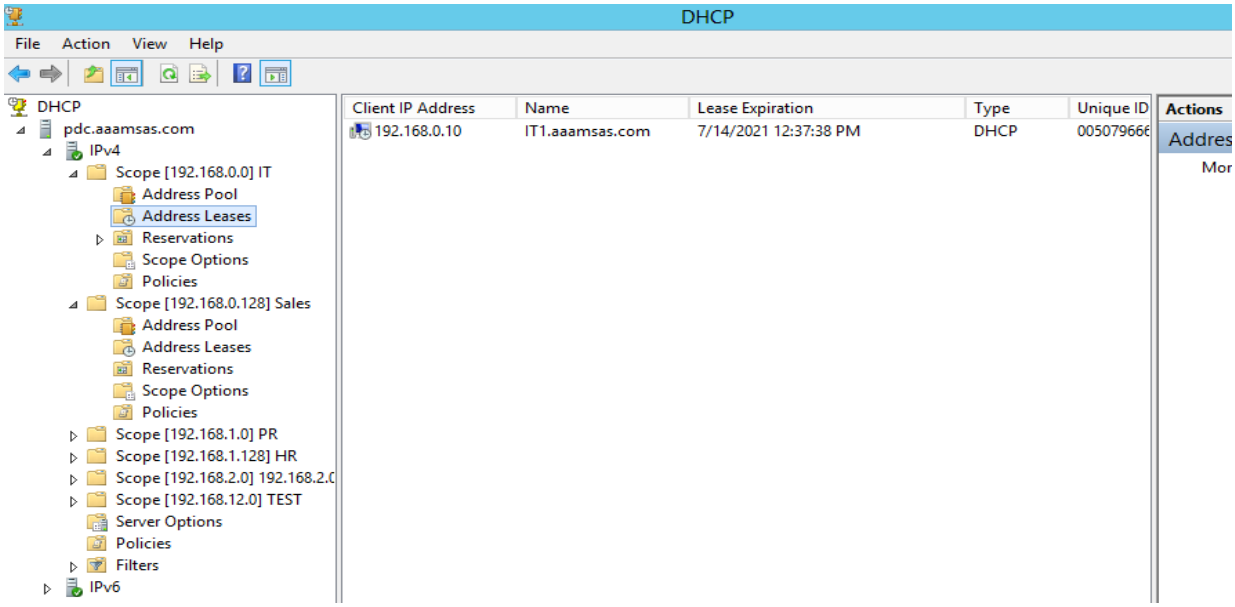


Figure 4-64 IT IP is released from DHCP Server.

Chapter 5 IPv6 Migration

Service providers are feeling increasing pressure to transition from the well-known and universal Internet Protocol version 4 (IPv4) standard to the newer IPv6 standard, while still supporting both network topologies. There are many reasons for this, not the least of which are the continually shrinking number of available IPv4 addresses and the exploding number of devices that require access to Internet applications and services.

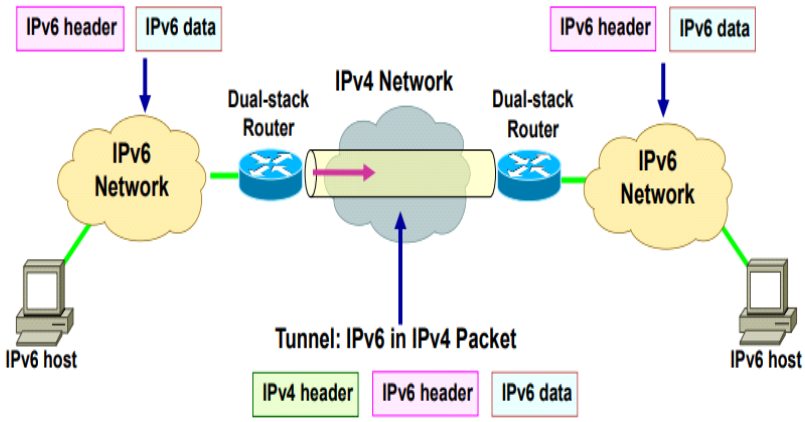


Figure 5-1 IPv6 used in the network.

GRE tunnels can be configured to run over an IPv6 network layer and to transport IPv6 packets in IPv6 tunnels and IPv4 packets in IPv6 tunnels so, When GRE IPv6 tunnels are configured, IPv6 addresses are assigned to the tunnel source and the tunnel destination. The tunnel interface can have either IPv4 or IPv6 addresses assigned. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks.

IPv6 traffic can be carried over IPv4 GRE tunnels using the standard GRE tunneling technique that is designed to provide the services to implement any standard point-to-point encapsulation scheme. As in IPv6 manually configured tunnels, GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol but, in this case, carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol.

The primary use of GRE tunnels is for stable connections that require regular secure communication between two edge devices or between an edge device and an end system. The edge devices and the end systems must be dual-stack implementations.

5.1 IPV6 Migration Configuration used in the project:

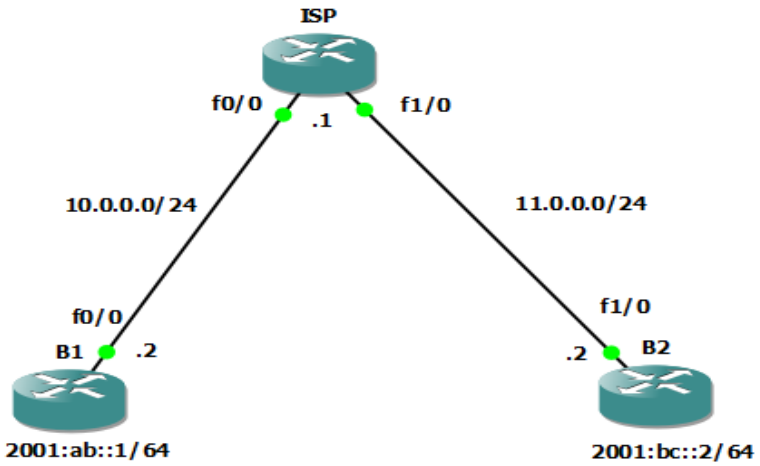


Figure 5-2 IPv6 in the project

```
B1(config) # IPV6 unicast-routing
B1(config) # IP route 0.0.0.0 0.0.0.0 10.0.0.1
B1(config) # int loopback 1
B1(config-if) # IPV6 add 2001:ab::1/64
B1(config-if) # IPV6 OSPF 1 area 0
B1(config) # int tunnel 1
B1(config-if) # IPV6 add 2001:cd::1/64
B1(config-if) # tunnel mode ipv6ip
B1(config-if) # tunnel source f0/0
B1(config-if) # tunnel destination 11.0.0.2
B1(config-if) # IPV6 OSPF 1 area 0
B2(config) # IPV6 unicast-routing
B2(config) # IP route 0.0.0.0 0.0.0.0 11.0.0.1
B2(config) # int loopback 2
B2(config-if) # IPV6 add 2001:bc::2/64
B2(config-if) # IPV6 OSPF 1 area 0
B2(config) # int tunnel 1
B2(config-if) # IPV6 add 2001:cd::2/64
B2(config-if) # tunnel mode ipv6ip
B2(config-if) # tunnel source f1/0
B2(config-if) # tunnel destination 10.0.0.2
B2(config-if) # IPV6 OSPF 1 area 0
```

To test connectivity:

```
B1(config)#do ping 2001:bc::2 source loo 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:BC::2, timeout is 2 seconds:
Packet sent with a source address of 2001:AB::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/36 ms
B1(config)#
```

Figure 5-3 Successful ping using IPv6.

Chapter 6 Results

6.1 Routing, Switching, and Servers.

After describing the project and understanding it correctly we now will show you the results of the project first thing we will see the network connectivity and that each device reaches to servers.

```
R14#ping google.com
Translating "google.com"...domain server (192.168.12.100)
% Unrecognized host or address, or protocol not running.

R14#
R14#ping google.com
Translating "google.com"...domain server (192.168.12.100) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.58.198.78, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/77/108 ms
R14#
```

Figure 6-1 Internet ping.

```
R14#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.0.76 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/25] via 10.0.0.76, 00:00:19, FastEthernet0/0
R14#ping 10.0.0.76
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.76, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/19/60 ms
R14#ping 10.0.0.73
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.73, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 16/22/24 ms
R14#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R14#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/72/96 ms
R14#
```

Figure 6-2 OSPF Successfully configured on firewall.

In figure 6-2, we see the successful ping to internet that means the OSPF is correctly defined in firewall and routers.

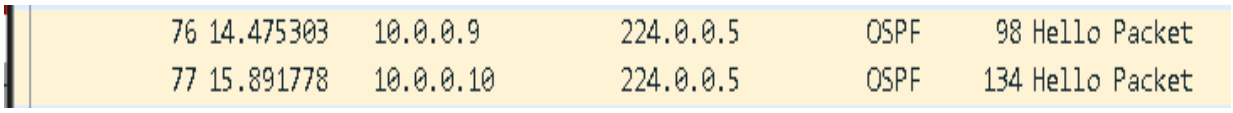


Figure 6-3 Wireshark captures.

OSPF sends hello packet in the network on multicast IP 224.0.0.5 as shown in figure 6-3 to discover OSPF other devices.

Figure 6-4 RIP captured from Wireshark.

RIPv2 that is used in the right branch of the network.

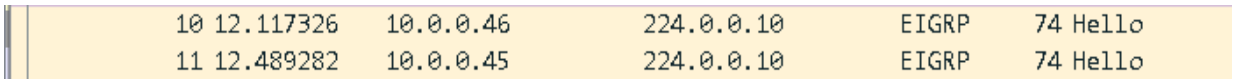


Figure 6-5 EIGRP captures.

EIGRP discover the other EIGRP protocols.

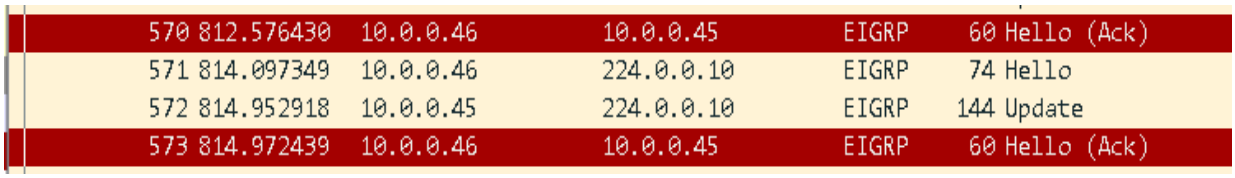


Figure 6-6 EIGRP communication.

In figure 6-6, shows you the EIGRP hello, update and ACK message.

From figure 6-1 we ensure that the network working correctly which DNS can resolve the name google.com to its IP address, and R14 device is able to reach the DC Server, which is itself the DNS and DHCP, so we start now displaying the results.

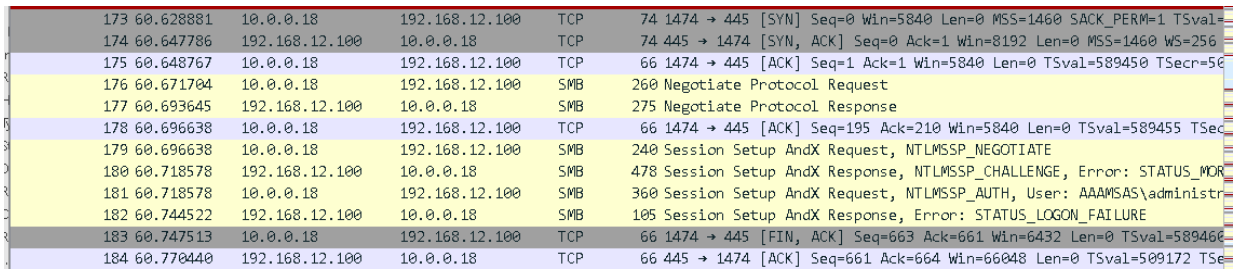


Figure 6-7 Captures show the connections between DC Server and a device in the network.

As we see in the figure 6-2 the Wireshark results shows the DC Server 192.168.12.100 can accept connection from a device in a network 10.0.0.8 correctly that mean the routing protocols working correctly and firewall is correctly configured.

Here we will display a figure 6-3 that shows the place of previous IPs.

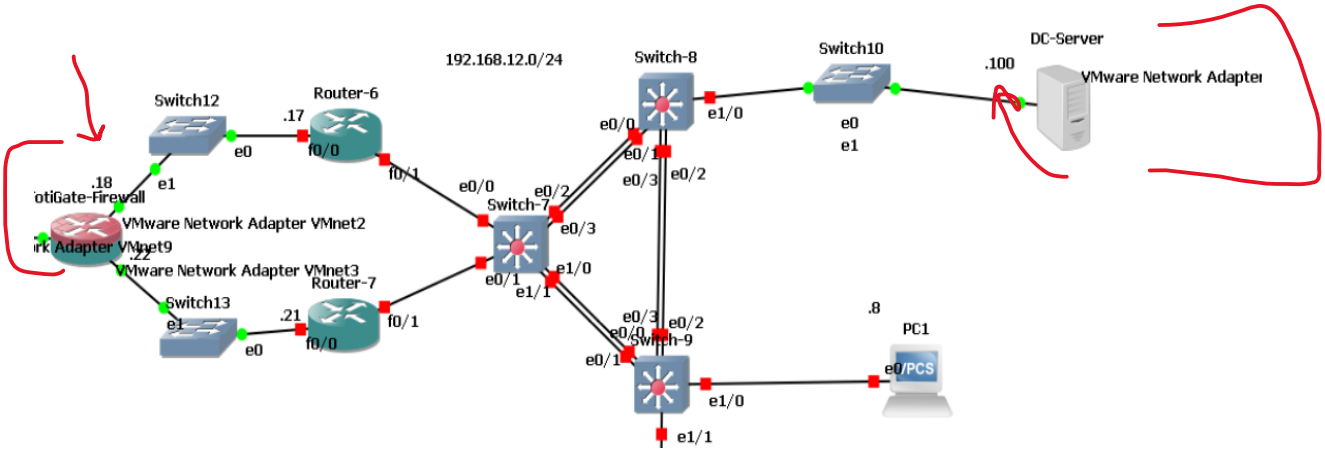


Figure 6-8 place of devices in previous figure.

189	67.593809	10.0.0.9	192.168.12.100	TCP	74 1457 → 445 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=590266 TSecr=0 WS=1
190	67.625722	192.168.12.100	10.0.0.9	TCP	74 445 → 1457 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=509857 TSecr=5
191	67.643691	10.0.0.9	192.168.12.100	TCP	66 1457 → 445 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=590270 TSecr=509857
192	67.650656	10.0.0.9	192.168.12.100	SMB	260 Negotiate Protocol Request
193	67.669608	192.168.12.100	10.0.0.9	SMB	275 Negotiate Protocol Response
194	67.685565	10.0.0.9	192.168.12.100	TCP	66 1457 → 445 [ACK] Seq=195 Ack=210 Win=5840 Len=0 TSval=590275 TSecr=509862
195	67.685565	10.0.0.9	192.168.12.100	SMB	240 Session Setup AndX Request, NTLMSSP_NEGOTIATE
196	67.702518	192.168.12.100	10.0.0.9	SMB	478 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
197	67.718475	10.0.0.9	192.168.12.100	SMB	360 Session Setup AndX Request, NTLMSSP_AUTH, User: AAAMSAS\administrator
198	67.735430	192.168.12.100	10.0.0.9	SMB	105 Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
199	67.757380	10.0.0.9	192.168.12.100	TCP	66 1457 → 445 [FIN, ACK] Seq=663 Ack=661 Win=6432 Len=0 TSval=590282 TSecr=509868
200	67.781325	192.168.12.100	10.0.0.9	TCP	66 445 → 1457 [ACK] Seq=661 Ack=664 Win=66048 Len=0 TSval=509873 TSecr=590282

Figure 6-9 successful connection between server and device.

As previous figure 6-2 here we see another device 10.0.0.9 is correctly see DC Server and its place is in the following figure 6-5.

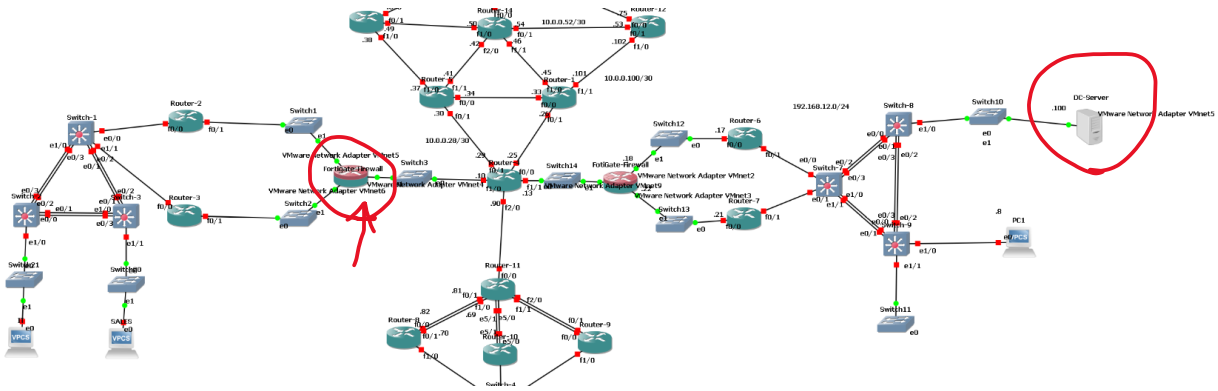


Figure 6-10 place of device used in figure 6-4.

As we are sure now that the firewalls can connect to DC server, now we will show the results of DHCP Server and taking IPs for the branches.

```
SALES> ip dhcp
DORA IP 192.168.0.138/25 GW 192.168.0.129

SALES> ping 192.168.12.100
84 bytes from 192.168.12.100 icmp_seq=1 ttl=123 time=53.154 ms
84 bytes from 192.168.12.100 icmp_seq=2 ttl=123 time=44.781 ms

SALES> ping aaamsas.com
aaamsas.com resolved to 192.168.12.100
84 bytes from 192.168.12.100 icmp_seq=1 ttl=123 time=53.163 ms
84 bytes from 192.168.12.100 icmp_seq=2 ttl=123 time=53.679 ms

SALES>
```

Figure 6-11 SLAES client takes IP from DHCP Server.

By showing that now we will display the captures that ensure our work,

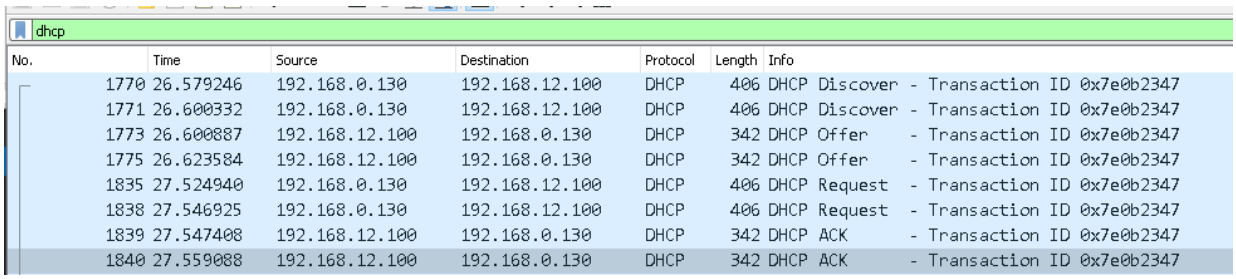


Figure 6-12 Captures of IP DHCP DORA message.

In figure 6-7, we see the process of taking IP 192.168.0.138 for SALES PC from DHCP Server 192.168.12.100, the IP of 1962.168.0.130 is the IP of virtual interface the router that is made to make each device to take an IP from its POOL in DHCP Server.

The following figures are show the same process for the IT client,

```
IT> ip dhcp
DORA IP 192.168.0.10/25 GW 192.168.0.1

IT> ping 192.168.12.100
84 bytes from 192.168.12.100 icmp_seq=1 ttl=123 time=61.990 ms
84 bytes from 192.168.12.100 icmp_seq=2 ttl=123 time=45.099 ms
84 bytes from 192.168.12.100 icmp_seq=3 ttl=123 time=58.395 ms
84 bytes from 192.168.12.100 icmp_seq=4 ttl=123 time=51.708 ms
84 bytes from 192.168.12.100 icmp_seq=5 ttl=123 time=39.347 ms

IT> ping aaamsas.com
aaamsas.com resolved to 192.168.12.100
84 bytes from 192.168.12.100 icmp_seq=1 ttl=123 time=59.280 ms
84 bytes from 192.168.12.100 icmp_seq=2 ttl=123 time=71.489 ms
84 bytes from 192.168.12.100 icmp_seq=3 ttl=123 time=62.291 ms
84 bytes from 192.168.12.100 icmp_seq=4 ttl=123 time=64.433 ms
84 bytes from 192.168.12.100 icmp_seq=5 ttl=123 time=63.402 ms

IT>
```

Figure 6-13 IT client took IP DHCP.

The figure 6-8, shows that IT took an IP DHCP from DHCP Server and successfully ping to the domain by name.

6363	96.232976	192.168.0.32	192.168.12.100	DHCP	406 DHCP Discover - Transaction ID 0xe1cf8b6d
6366	96.255143	192.168.0.32	192.168.12.100	DHCP	406 DHCP Discover - Transaction ID 0xe1cf8b6d
6367	96.255650	192.168.12.100	192.168.0.32	DHCP	342 DHCP Offer - Transaction ID 0xe1cf8b6d
6369	96.276049	192.168.12.100	192.168.0.32	DHCP	342 DHCP Offer - Transaction ID 0xe1cf8b6d
6442	97.218240	192.168.0.32	192.168.12.100	DHCP	406 DHCP Request - Transaction ID 0xe1cf8b6d
6444	97.231527	192.168.0.32	192.168.12.100	DHCP	406 DHCP Request - Transaction ID 0xe1cf8b6d
6445	97.232016	192.168.12.100	192.168.0.32	DHCP	342 DHCP ACK - Transaction ID 0xe1cf8b6d
6446	97.243201	192.168.12.100	192.168.0.32	DHCP	342 DHCP ACK - Transaction ID 0xe1cf8b6d

Figure 6-14 Wireshark captures that ensure our work.

The Wireshark captures shows that the DORA process is working correctly. Then we will see the redundancy configurations in the project for routers,

We configured VRRP and GLBP for branch 1 and 2 respectively.

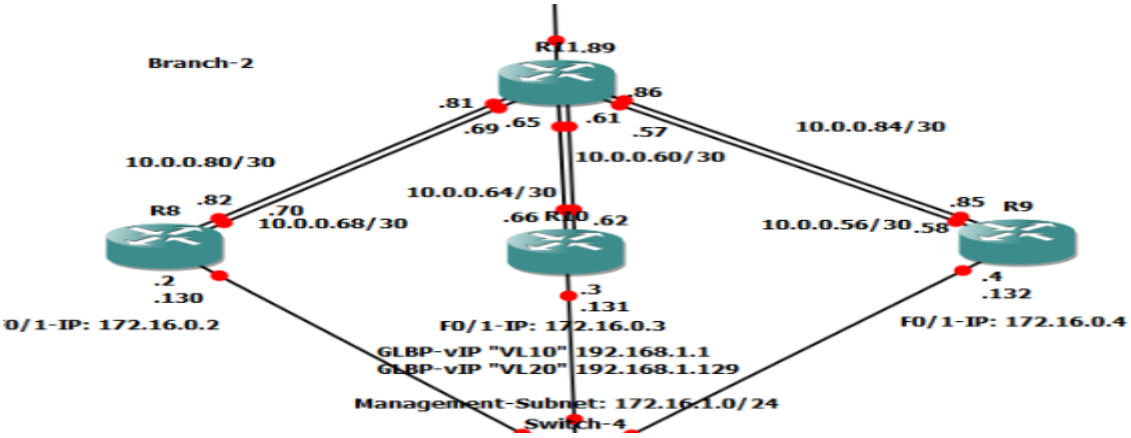


Figure 6-15 Place of devices that configured in GLBP.

```
R8(config-if)#glbp 1 weighting 50 lower 30 upper 34
R8(config-if)#
R8(config-if)#
```

Figure 6-16 GLBP 1 configurations.

```
[OK]
R9(config)#do sh glbp
FastEthernet1/0 - Group 1
  State is Listen
    127 state changes, last state change 00:00:06
  Virtual IP address is 172.16.1.1
  Hello time 50 msec, hold time 70 msec
    Next hello sent in 0.064 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is 172.16.1.2, priority 130 (expires in 0.064 sec)
  Standby is 172.16.1.3, priority 120 (expires in 0.032 sec)
  Priority 110 (configured)
  Weighting 50 (configured 50), thresholds: lower 30, upper 34
    Track object 1 undefined
    Track object 2 undefined
  Load balancing: weighted
  Group members:
    ca08.3538.001c (172.16.1.2)
    ca09.3fb0.001c (172.16.1.4) local
    ca0a.0e2c.0008 (172.16.1.3)
  There are 3 forwarders (2 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:02:50
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is ca08.3538.001c
    Time to live: 14400.000 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
 --More--
```

Figure 6-17 GLBP running configuration.

6.2 WAN technology

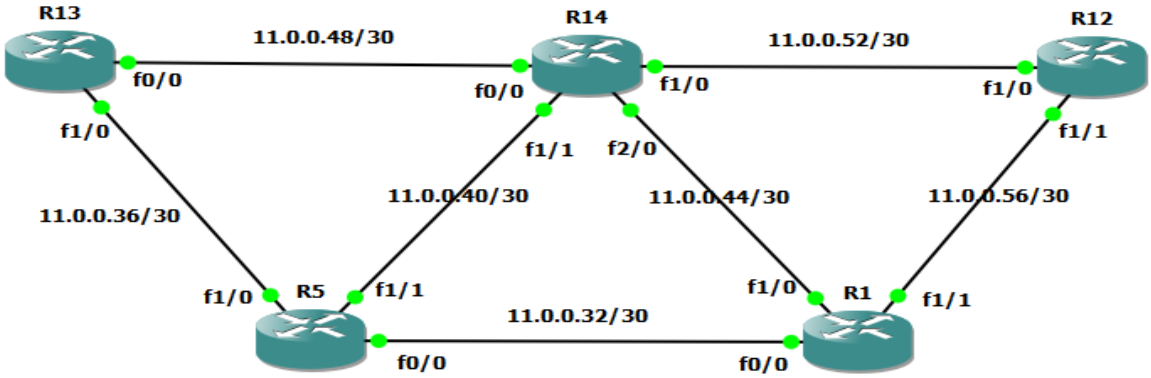


Figure 6-18 WAN routers connection.

First, the routers in SP must connect with each other before configuring MPLS so, we will use EIGRP routing protocol.

```
R1(config)#router eigrp 2
R1(config-router)#net
R1(config-router)#router eigrp 2
R1(config-router)#network 11.0.0.32
R1(config-router)#network 11.0.0.44
R1(config-router)#network 11.0.0.56
R1(config-router)#
```

```
R5(config)#router eigrp 2
R5(config-router)#network 11.0.0.32
R5(config-router)#network 11.0.0.
*Jul  8 23:31:20.847: %DUAL-5-NBRCHA
R5(config-router)#network 11.0.0.36
R5(config-router)#network 11.0.0.40
R5(config-router)#
```

```
R13(config)#router eigrp 2
R13(config-router)#network 11.0.0.36
R13(config-router)#
*Jul  8 23:32:59.727: %DUAL-5-NBRCHAN
R13(config-router)#network 11.0.0.48
R13(config-router)#
```

```
R14(config)#router eigrp 2
R14(config-router)#network 11.0.0.48
R14(config-router)#
*Jul  8 23:34:50.323: %DUAL-5-NBRCHAN
*Jul  8 23:34:50.331: %DUAL-5-NBRCHAN
*Jul  8 23:34:50.343: %DUAL-5-NBRCHAN
R14(config-router)#network 11.0.0.52
R14(config-router)#network 11.0.0.40
R14(config-router)#network 11.0.0.44
R14(config-router)#
```

To test connectivity before configuring MPLS

```
R1(config)#do ping 11.0.0.53
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.53, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/20/28 ms
R1(config)#
```

Now we will configure MPLS on SP Routers

```
R1(config)#mpls label range 100 199
R1(config)#mpls ip
R1(config)#int range f0/0 , f1/0 , f1/1
R1(config-if-range)#mpls ip
R1(config-if-range)#
```

```
R5(config)#mpls label range 500 599
R5(config)#mpls ip
R5(config)#int range f0/0 , f1/0 , f1/1
R5(config-if-range)#mpls ip
R5(config-if-range)#
```

```
R13(config)#mpls label range 300 399
R13(config)#mpls ip
R13(config)#int range f0/0 , f1/0
R13(config-if-range)#mpls ip
R13(config-if-range)#
```

```
R14(config)#mpls label range 400 499
R14(config)#mpls ip
R14(config)#int range f0/0 , f1/0 , f1/1 , f2/0
R14(config-if-range)#mpls ip
R14(config-if-range)#
```

```
R12(config)#mpls label range 200 299
R12(config)#mpls ip
R12(config)#int range f1/0 , f1/1
R12(config-if-range)#mpls ip
R12(config-if-range)#
```

```
R1(config)#
*Jul  8 23:56:30.783: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.41:0 (1) is UP
R1(config)#
*Jul  8 23:56:44.031: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.54:0 (2) is UP
R1(config)#
*Jul  8 23:56:47.987: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.58:0 (3) is UP
R1(config)#
```

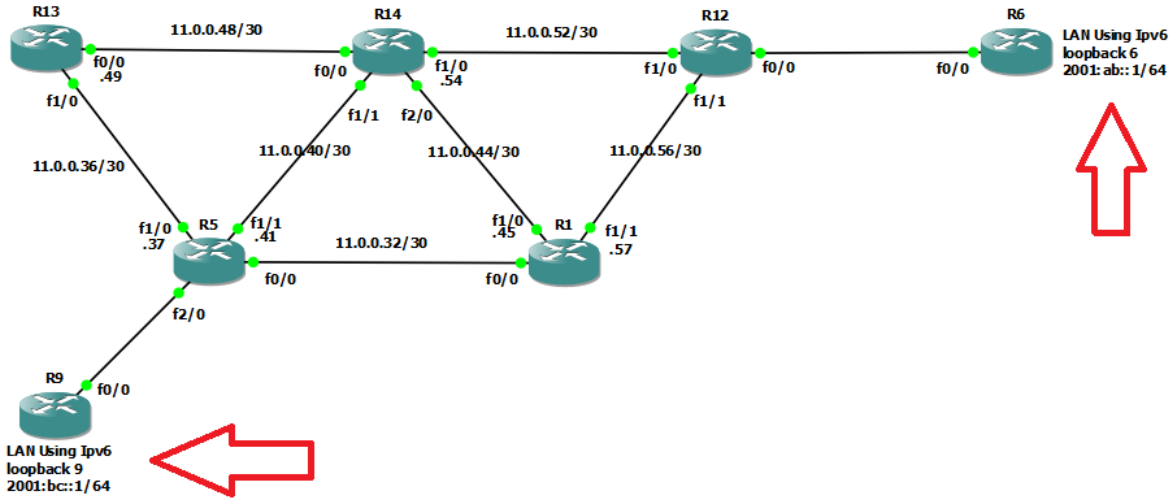
```
R5(config)#
*Jul  8 23:56:30.447: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.57:0 (1) is UP
R5(config)#
*Jul  8 23:56:36.583: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.49:0 (2) is UP
R5(config)#
*Jul  8 23:56:40.815: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.54:0 (3) is UP
R5(config)#
```

```
R13(config)#
*Jul  8 23:56:06.975: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.41:0 (1) is UP
R13(config)#
*Jul  8 23:56:15.995: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.54:0 (2) is UP
R13(config)#
```

```
R14(config)#
*Jul  8 23:56:21.039: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.41:0 (1) is UP
R14(config)#
*Jul  8 23:56:23.931: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.57:0 (2) is UP
R14(config)#
*Jul  8 23:56:25.599: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.58:0 (3) is UP
*Jul  8 23:56:25.795: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.49:0 (4) is UP
R14(config)#
```

```
R12(config)#
*Jul  8 23:49:45.655: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.54:0 (1) is UP
R12(config)#
*Jul  8 23:49:47.871: %LDP-5-NBRCHG: LDP Neighbor 11.0.0.57:0 (2) is UP
R12(config)#
```

6.3 IPv6 Migration configuration



Ipv6 Configuration for our LANs

```
R6(config)#int loo 6
R6(config-if)#
*Jul  9 00:36:38.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R6(config-if)#ipv6 add 2001:ab::1/64
R6(config-if)#
```

```
R9(config)#int loo 9
R9(config-if)#
*Jul  9 00:38:29.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback9, changed state to up
R9(config-if)#ipv6 add 2001:bc::1/64
R9(config-if)#
```

Configuration for Migration

```
R6(config)#ipv6 unicast-routing
R6(config)#ip route 0.0.0.0 0.0.0.0 12.0.0.2
R6(config)#int tunnel 1
R6(config-if)#ipv6 add 2001:cd::1/64
R6(config-if)#tunnel source f0/0
R6(config-if)#tunnel destination 12.0.0.6
R6(config-if)#ipv6 ospf 2 area 0
R6(config-if)#int loo 6
R6(config-if)#ipv6 ospf 2 area 0
R6(config-if)#
```

```
R9(config)#ipv6 unicast-routing
R9(config)#ip route 0.0.0.0 0.0.0.0 12.0.0.5
R9(config)#int tunnel 1
R9(config-if)#
*Jul  9 00:53:28.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
R9(config-if)#ipv6 add 2001:cd::2/64
R9(config-if)#tunnel source f0/0
R9(config-if)#tunnel destination 12.0.0.1
R9(config-if)#
*Jul  9 00:56:40.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
R9(config-if)#ipv6 ospf 2 area 0
R9(config-if)#int loo 9
R9(config-if)#ipv6 ospf 2 area 0
R9(config-if)#
```

Testing connectivity using ping command ➔ ping 2001:ab::1 source loo 6

```
R6(config)#do ping 2001:ab::1 source loo 6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB::1, timeout is 2 seconds:
Packet sent with a source address of 2001:AB::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
R6(config)#
```

6.4 Problems

As any work in the world, we faced some problems and project did not work correctly form the first run, and we solved these problems as we saw the results above.

```
704 987.765396  10.0.0.54   10.0.0.101  ICMP  114 Echo (ping) request  id=0x0008, seq=0/0, ttl=255 (no response found!)
705 987.790518  10.0.0.54   10.0.0.101  ICMP  114 Echo (ping) request  id=0x0008, seq=1/256, ttl=255 (no response found!)
706 987.815895  10.0.0.54   10.0.0.101  ICMP  114 Echo (ping) request  id=0x0008, seq=2/512, ttl=255 (no response found!)
707 987.841891  10.0.0.54   10.0.0.101  ICMP  114 Echo (ping) request  id=0x0008, seq=3/768, ttl=255 (no response found!)
708 987.879901  10.0.0.54   10.0.0.101  ICMP  114 Echo (ping) request  id=0x0008, seq=4/1024, ttl=255 (no response found!)
```

Figure 6-19 unsuccessful ping.

In the figure 6-10, we see an unsuccessful ping from 2 routers, the place of them is shown in the following figure,

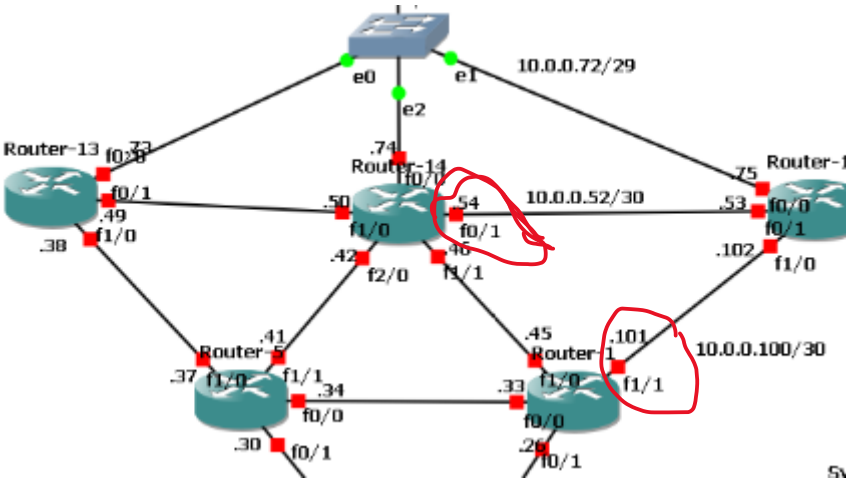


Figure 6-20 place of devices.

The problem was the misconfiguration in subnet mask of one of routers, we knew this problem by reviewing the running configurations using command, R# show running, and these files for each device is available for review for anyone want to see them.

Conclusion

Networking is the most important thing that is making computers useful for each human, without networking there is no way to make PCs to call each other, in the previous centuries, human used homers to send message to each other, now in internet era we use E-mail applications for official messages and e.g., WhatsApp for non-official messages, to chat with each other. The backend of the previous messenger apps is the networking so, without networking we could not be able to use messenger apps,

In our project we made the basic infrastructure, or we can say the most important devices, concepts, and devices in the network like Switches, Routers, Firewalls, and Servers.

Switches are used to create LANs and Router are used to link Switches together creating WAN, from here we implemented the WAN Technology because communication in LANs in not the as in WAN each has its technology, then in WAN we have some security issues, so we implemented and use security devices like Firewalls and some types of servers, e.g., ADDC. In Switches we created VLANs to reduces BC messages which makes a high load on switches and will take the BW for its and connection will be very slow in case of it are not down, also we implemented STP and VTP.

In Routers, we implemented the VRRP and GLBP for redundancy and routing protocols to make it easy to discover best routes and discover new and far networks.

In WAN, we implemented the MPLS protocol that is standard not a vendor proprietary.

Lastly, we talk about the IPv6 that will replace IPv4 because of lack in IPs in IPv4 in general its configuration is somehow close to IPv4.

References

[1] B.Dickie, “FortiOS-6.0.0-Cook Book” , Fortinet Technology Inc, Authentication, P.65, 2020

[2] B.Dickie, “FortiOS-6.0.0-Cook Book” , Fortinet Technology Inc, Authentication, P.121, 2020

[3] K.Wallace, “CCNP Routing and Switching ROUTE 300-101

Official Cert Guide”, Cisco Press, Chapter 10, P.405, 2021

[4] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 7 Understanding OSPF Concepts, P.172, 2016

[5] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 8 Implementing OSPF for IPv4, P.196, 2016

[6] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 9 Understanding EIGRP Concepts, P.226, 2016

[7] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 10 Implementing EIGRP for IPv4, P.246, 2016

[8] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 1 implementing virtual Ethernet LANs, P.17, 2016

[9] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 5 VLAN Trunking Protocol, P.122, 2016

[10] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 19 VLAN Routing with router 802.1Q Trunk, P.522, 2016

[11] W.Odom, “CCNA Routing and Switching ICND2 200-105 Official cert Guide”, Cisco Press, Chapter 14 Private WANs with Ethernet and MPLS, P.364, 2016

[12] Wikipedia article

[13] T.Lammle, “Understanding Cisco networking technologies: exam 200-301”, volume 1, Part II. John Wiley & Sons, Inc. 2020.

الملخص العربي

الشبكات هي أهم شيء يجعل أجهزة الحاسوب مفيدة لكل إنسان، فبدون الشبكات لا توجد طريقة لجعل أجهزة الحاسوب تتصل ببعضها البعض، في القرون السابقة، استخدم الإنسان homers لإرسال رسائل لبعضهم البعض، والآن في عصر الإنترنت نستخدمه تطبيقات البريد الإلكتروني للرسائل الرسمية مثل WhatsApp للرسائل غير الرسمية للدردشة مع بعضها البعض .الواجهة الخلفية لتطبيقات المراسلة السابقة هي الشبكات، لذا بدون الشبكات لا يمكننا استخدام تطبيقات المراسلة،

تم تصميم هذا المشروع لإنشاء نظام البنية التحتية للشبكات مع بعض الأجهزة الأمنية لإنشاء شبكة خاصة وشبكة عامة لشركة لديها ثلاثة أقسام متعددة وفروع متعددة كما فعلنا في المشروع، قمنا بتنفيذ الاتصال بين الإدارات باستخدام التوجيه والتبديل ثم ربط الفروع معًا باستخدام تقنية WAN .مثلMPLS

في هذا المشروع، يمكن للأجهزة الوصول أو الاتصال ببعضها البعض وفقًا لقواعد كل قسم في الشركة تمت إضافته بواسطة جدران الحماية. أيضًا، يمكن للأجهزة الموجودة داخل الشبكة الوصول إلى الإنترنت، ولكن هذا يعتمد على القسم الذي يحتوي الإنترنت على الكثير من مواقع الويب، لذلك من خلال جدار الحماية يمكننا تصفية القسم للسماح بالوصول إلى مواقع الويب المطلوبة فقط وحظر مواقع الويب الأخرى مثل Facebook ومواقع الفيديو مثل YouTube ودفق مواقع الويب مثل TeamViewer.

أنشأنا في مشروعنا البنية التحتية الأساسية، أو يمكننا أن نقول أهم الأجهزة والمفاهيم والأجهزة في الشبكة مثل المحولات، وأجهزة التوجيه، وجدران الحماية، والخوادم .تُستخدم المحولات لإنشاء شبكات LAN وجهاز التوجيه لربط المحولات معًا لإنشاءWAN ، ومن هنا قمنا بتطبيق تقنية WAN لأن الاتصال في الشبكات المحلية ليس كما هو الحال في WAN لكل منها تقنيتها، ثم في WAN لدينا بعض المشكلات الأمنية، لذلك نحن نفذت واستخدمت أجهزة أمنية مثل جدران الحماية وبعض أنواع الخوادم، مثل.ADDC

في المحولات، أنشأنا شبكات محلية ظاهرية (VLAN) لتقليل رسائل BC مما يؤدي إلى حمل كبير على المحولات وسيأخذ BWمن أجله وسيكون الاتصال بطيئًا جدًا في حالة عدم تعطله، كما قمنا بتطبيق STP و.VTP

في أجهزة التوجيه، قمنا بتطبيق VRRP و GLBPلبروتوكولات التكرار والتوجيه لتسهيل اكتشاف أفضل المسارات واكتشاف الشبكات الجديدة والبعيدة .فيWAN ، قمنا بتطبيق بروتوكول MPLS الذي يعتبر قياسيًا وليس مملوكًا للبائع. أخيرًا، نتحدث عن IPv6 الذي سيحل محل IPv4 بسبب نقص عناوين IP في IPv4 بشكل عام، فإن تكوينه قريب إلى حد ما من.IPv4

جامعة بنها
كلية الهندسة ببنها
قسم الهندسة الكهربية

البنية التحتية لشبكات الحاسب مع تأمين البيانات.

مشروع مقدم من الطلاب

عبد الرحمن أيمن أبو المعاطي

عبد الرحيم محمد عبد الرحيم

شيماء الشافعي عبد الجواد

عبد الرحمن محمد محمد

صلاح إيهاب محمد

عبد الله عاطف عيد

محمد رضا أحمد

تحت إشراف

د/إيمان سالم

قسم الهندسة الكهربية
كلية الهندسة ببنها
جامعة بنها

2021