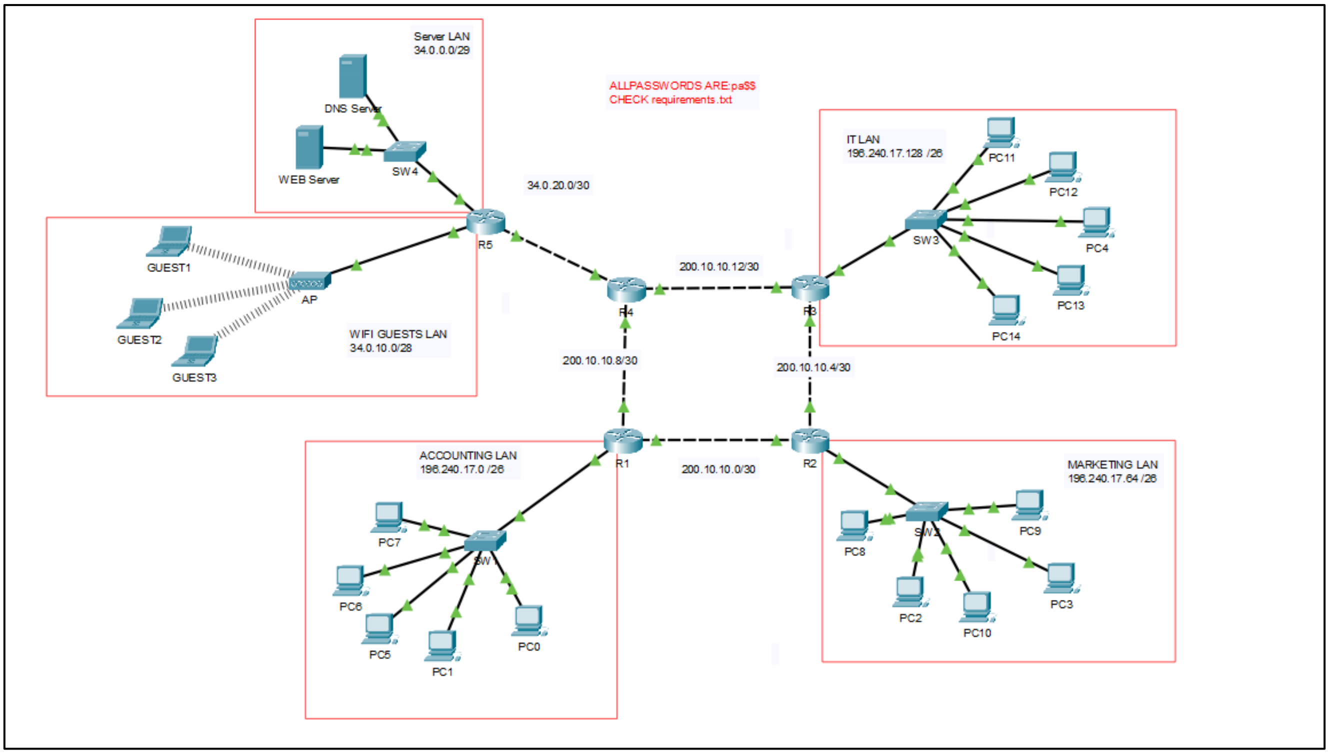
SOHO Network Implementation in Packet Tracer



Author: Emanoil-Raul SUCIU
raul.suciu293@gmail.com

Table of Contents

1. Introduction

In our modern, interconnected world, networking stands as the bedrock of communication systems, facilitating the seamless exchange of data and the sharing of resources across a multitude of devices. This project represents a deep dive into the fundamental concepts that support networking, providing participants with hands-on experience utilizing Packet Tracer, an advanced simulation tool renowned for its robust capabilities.

Network Subnetting emerges as a strategic technique, empowering network architects to partition sprawling networks into smaller, more manageable sub-networks. Through intelligent segmentation, subnetting enhances network efficiency, fortifies security postures, and amplifies scalability potentials.

Within the realm of Virtual Local Area Networks (VLANs), participants traverse the virtual landscapes of network segmentation, transcending physical boundaries to carve out logical domains based on functional, departmental, or application-centric criteria. VLANs indicate a new era of network flexibility and security, promoting agile architectures primed for dynamic organizational needs.

Open Shortest Path First (OSPF) Routing emerges as a dynamic force in our journey, orchestrating the intricate dance of data packet transmission across interconnected networks. Through OSPF, routers engage in a exchange of routing intelligence, charting optimal pathways that minimize latency, maximize bandwidth utilization, and ensure seamless connectivity.

Dynamic Host Configuration Protocol (DHCP) Addressing emerges as a beacon of automation, streamlining the labyrinthine process of IP address assignment and network configuration. By automating these tasks, DHCP liberates network administrators from the shackles of manual intervention, promoting agility and efficiency in network operations.

Access Control Lists (ACLs) emerge as the vigilant guardians of network integrity, meticulously inspects the flow of data traffic within network area. Armed with granular rule sets, ACLs enforce access policies, prevent unauthorized intrusions, and deploy formidable barriers against cyber threats.

Web Servers beckon participants into the digital domain of content delivery and accessibility, serving as the bastions of online presence and interaction. From configuration to optimization, participants navigate the nuances of web server management, ensuring swift and secure access to digital resources.

Domain Name System (DNS) Servers emerge as the unsung heroes of cyberspace, translating human-readable domain names into machine-readable IP addresses. As the backbone of internet navigation, DNS configuration emerges as a critical facet of network administration, ensuring seamless web browsing experiences for users worldwide.

Access Points (APs) announce the era of wireless connectivity, extending the reach of wired networks to embrace the mobility of modern workspaces. Through meticulous configuration and optimization, participants harness the power of access points to create robust wireless infrastructures, enabling seamless connectivity for a multitude of devices.

2. Subnetting the Network

Let's assume that our network will have a minimum of 3 departments (Accounting, Marketing, and IT), with a minimum of 40 hosts in each department, starting from the IP Address of 196.240.17.0 /24.
Table 1 below illustrates 3 subnetting possibilities:

- the /25 mask is not a good option because it has only 2 subnetworks, and we need a minimum of 3 subnetworks (departments),
- the /27 mask is not a good option because it has only 30 hosts/subnetwork, and we need a minimum of 40 hosts/department,
- the /26 mask is the right option for this scenario, having enough subnetworks and hosts.

Table 1. The three subnetting possibilities

Network	Mask	Nr. of subnetworks	Nr. of hosts/subnetwork
196.240.17.0	/25	$2^1 = 2$	$2^7 - 2 = 126$
	/26	$2^2 = 4$	$2^6 - 2 = 62$
	/27	$2^3 = 8$	$2^5 - 2 = 30$

Upon choosing the /26 mask, we have 4 subnetworks and 62 hosts/subnetwork, as explained above. Table 2 below illustrates the delimitation between the 4 subnetworks, showing the network addresses, the first and the last host, and the broadcast address of each of the departments.

Table 2. The delimitation between the four subnetworks

	Network Address	First Host		Last Host	Broadcast Address
Accounting	196.240.17.0 /26	196.240.17.1	...	196.240.17.62	196.240.17.63
Marketing	196.240.17.64 /26	196.240.17.65	...	196.240.17.126	196.240.17.127
IT	196.240.17.128 /26	196.240.17.129	...	196.240.17.190	196.240.17.191
Reserved	196.240.17.192 /26	196.240.17.193	...	196.240.17.254	196.240.17.255

3. The Network Topology

The topology starts with 4 routers, one for each department and one more for the reserved subnetwork, thus ensuring two fundamental network requirements: scalability and redundancy.

The routers chosen were the 2911 model, because we needed 3 ports/router for the topology, and they have exactly 3 GigabitEthernet ports. Each department LAN also has a model 2960 switch with 24 FastEthernet ports and 2 GigabitEthernet ports.

Table 3 below illustrates the 2 different types of copper cable connections used in the topology, and give some exemples of devices they interconnect:

Table 3. The copper cable connections interconnected devices

Copper cable connections	Interconnected devices
Straight-Through	ROUTER – SWITCH SWITCH – HOST SWITCH – SERVER ROUTER – ACCESS POINT
Cross-Over	ROUTER – ROUTER ROUTER – HOST SWITCH– SWITCH

Figure 1 below shows the Packet Tracer topology. The network can support a maximum of 24 hosts/subnetwork due to the limited interface numbers of the switches. The subnetworks could be extended using 1 or 2 more switches until the maximum number of 62 hosts. For simplicity, each department will have only 5 hosts, more than enough for connectivity verification or troubleshooting inside or outside the LANs.

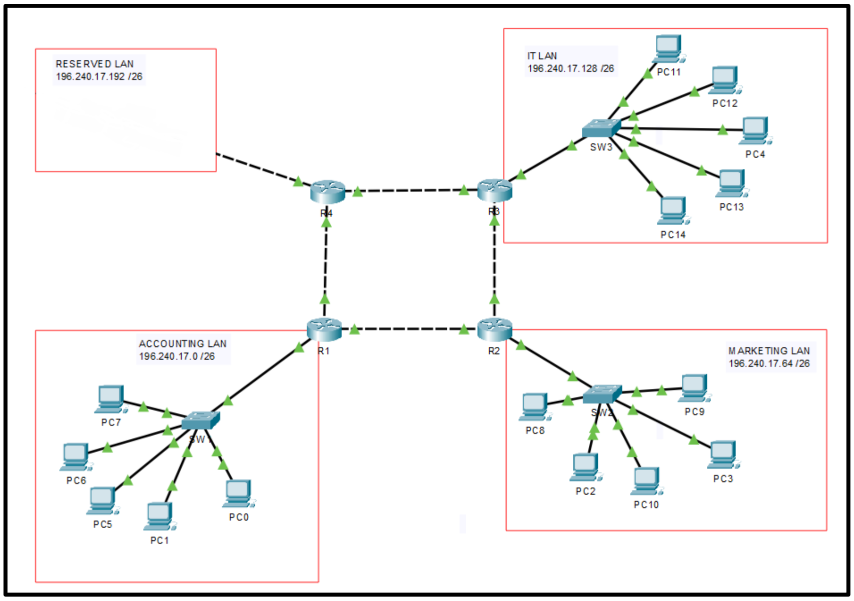


Figure 1. The Packet Tracer Topology

4. VLAN Configuration

The following configurations were applied to the switches:

- Accounting LAN Switch:

```
interface Vlan10
      description ACCOUNTING
      ip address 192.240.17.2 255.255.255.192
interface GigabitEthernet0/1
      switchport trunk native vlan 10
      switchport mode trunk
interface FastEthernet0/1 - 0/24
      switchport access vlan 10
      switchport mode access
```

- Marketing LAN Switch:

```
interface Vlan20
      description MARKETING
      ip address 192.240.17.66 255.255.255.192
interface GigabitEthernet0/1
      switchport trunk native vlan 20
      switchport mode trunk
interface FastEthernet0/1 - 0/24
      switchport access vlan 20
      switchport mode access
```

- IT LAN Switch:

```
interface Vlan30
      description IT
      ip address 192.240.17.130 255.255.255.192
interface GigabitEthernet0/1
      switchport trunk native vlan 30
      switchport mode trunk
interface FastEthernet0/1 - 0/24
      switchport access vlan 30
      switchport mode access
```

4.1 Experimental Results

Upon implementing the configuration from above, the first thing tried is a ping inside the accounting LAN, from PC 1 (196.240.17.3) to PC 0 (196.240.17.4), as shown in the figure 2 below.

The ping is successful, as we can see in the log below. Other pings were attempted inside the other two LANs, which were also successful, demonstrating that the inside LAN communication is working and the hosts are reachable.

```
C:\>ping 196.240.17.4

Pinging 196.240.17.4 with 32 bytes of data:

Reply from 196.240.17.4: bytes=32 time<1ms TTL=128
Reply from 196.240.17.4: bytes=32 time<1ms TTL=128
Reply from 196.240.17.4: bytes=32 time=16ms TTL=128
Reply from 196.240.17.4: bytes=32 time<1ms TTL=128

Ping statistics for 196.240.17.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

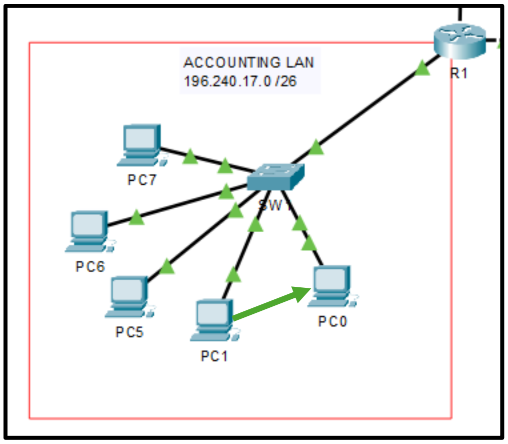


Figure 2. Ping inside Accounting LAN

Upon attempting to ping another host from PC 1, this time in the remote marketing LAN (PC 8 - 192.168.10.67),as illustrated in figure 3, the ping is unsuccessful, as shown in the log below the picture. This means that remote hosts are not yet reachable, which is to be expected, since the routers were not configured.

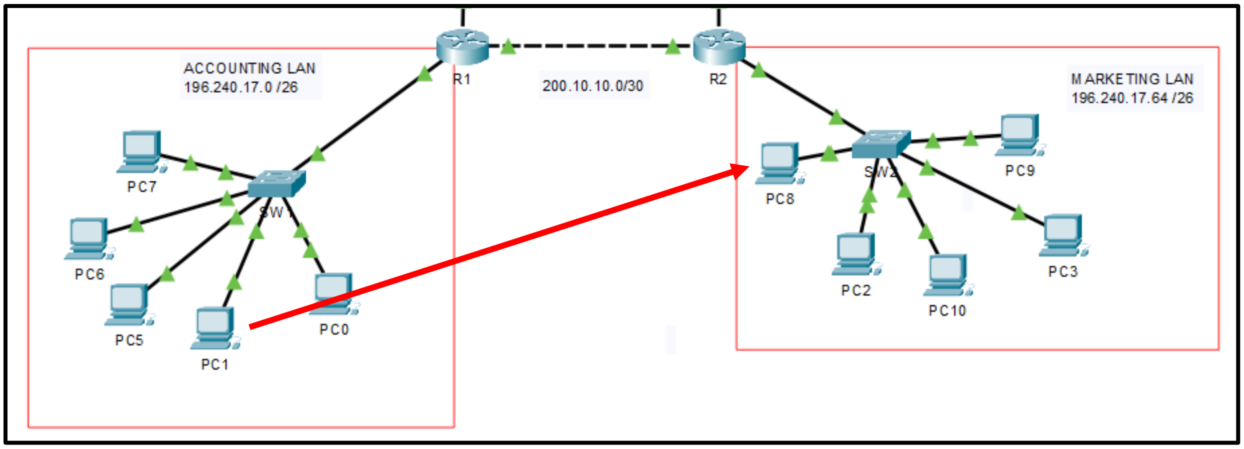


Figure 3. Ping outside the Accounting LAN

```
C:\>ping 196.240.17.67

Pinging 192.168.10.67 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.67:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

5. OSPF Routing

The following configurations were applied to the routers:

- Accounting Router:

```
interface GigabitEthernet0/0
      ip address 200.10.10.10 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/1
      ip address 200.10.10.1 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/2
      ip address 196.240.17.1 255.255.255.192
router ospf 10
      router-id 1.1.1.1
      network 200.10.10.0 0.0.0.3 area 0
      network 200.10.10.8 0.0.0.3 area 0
      network 196.240.17.0 0.0.0.63 area 0
```

- Marketing LAN Router:

```
interface GigabitEthernet0/0
      ip address 200.10.10.2 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/1
      ip address 200.10.10.5 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/2
      ip address 196.240.17.65 255.255.255.192
router ospf 10
      router-id 2.2.2.2
      network 200.10.10.0 0.0.0.3 area 0
      network 200.10.10.4 0.0.0.3 area 0
      network 196.240.17.64 0.0.0.63 area 0
```

- IT LAN Router:

```
interface GigabitEthernet0/0
      ip address 200.10.10.13 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/1
      ip address 200.10.10.6 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/2
      ip address 196.240.17.129 255.255.255.192
router ospf 10
      router-id 3.3.3.3
      network 200.10.10.4 0.0.0.3 area 0
      network 196.240.17.128 0.0.0.63 area 0
      network 200.10.10.12 0.0.0.3 area 0
```

- Reserved LAN Router:

```
interface GigabitEthernet0/0
      ip address 200.10.10.9 255.255.255.252
      ip ospf 10 area 0
interface GigabitEthernet0/1
      ip address 200.10.10.14 255.255.255.252
ip ospf 10 area 0
      router ospf 10
      router-id 4.4.4.4
      network 200.10.10.8 0.0.0.3 area 0
      network 200.10.10.12 0.0.0.3 area 0
```

5.1 Experimental Results

The experiment from the last chapter is repeated, and this time, PC 0 successfully pings PC 8 from the remote LAN, as we can see in the log below. Other pings between different LANs were attempted, all finishing successfully, demonstrating that now the network has outside LAN connectivity.

```
C:\>ping 196.240.17.67

Pinging 196.240.17.67 with 32 bytes of data:

Reply from 196.240.17.67: bytes=32 time=1ms TTL=126
Reply from 196.240.17.67: bytes=32 time<1ms TTL=126
Reply from 196.240.17.67: bytes=32 time<1ms TTL=126
Reply from 196.240.17.67: bytes=32 time<1ms TTL=126

Ping statistics for 196.240.17.67:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

6. Restricting access with ACLs

Let's assume that the following restrictions need to be implemented between the departments:

- The accounting department can access the marketing department but cannot access the IT department
- The marketing department cannot access the other 2 departments
- The IT department can access both other 2 departments

Those restrictions are visually explained in the figure 4 below.

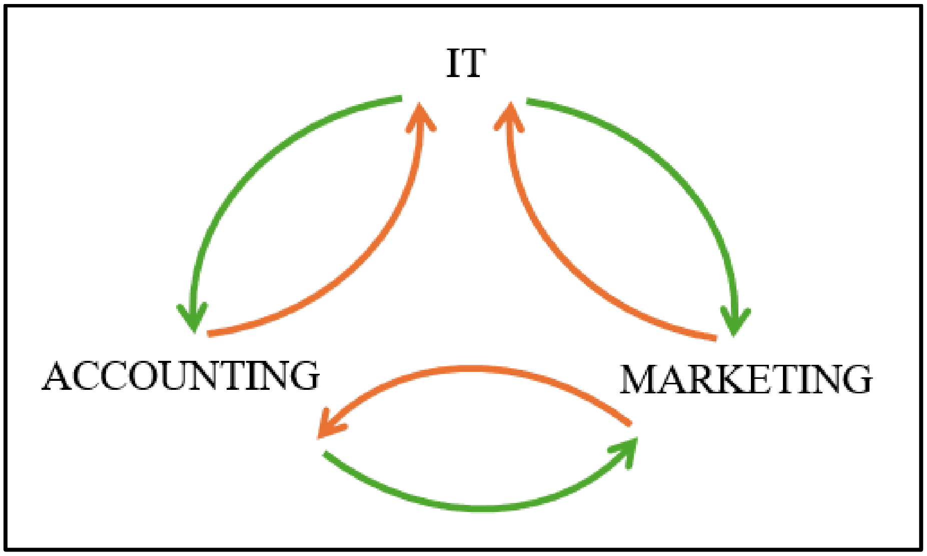


Figure 4. The restriction plan

The following configurations were applied:

- Accounting LAN Router:

```
access-list 110 permit icmp any 196.240.17.128 0.0.0.63 echo-reply
access-list 110 permit icmp any 196.240.17.64 0.0.0.63
access-list 110 permit tcp any 196.240.17.64 0.0.0.63
access-list 110 permit tcp any 196.240.17.128 0.0.0.63 established
```

- Marketing LAN Router:

```
access-list 110 permit icmp any 196.240.17.0 0.0.0.63 echo-reply
access-list 110 permit icmp any 196.240.17.128 0.0.0.63 echo-reply
access-list 110 permit tcp any 196.240.17.0 0.0.0.63 established
access-list 110 permit tcp any 196.240.17.128 0.0.0.63 established
```

- IT LAN Router:

```
access-list 110 permit icmp any 196.240.17.0 0.0.0.63
access-list 110 permit icmp any 196.240.17.64 0.0.0.63
access-list 110 permit tcp any 196.240.17.0 0.0.0.63
access-list 110 permit tcp any 196.240.17.64 0.0.0.63
```

6.1 Experimental Results

In the experimental part of this chapter, we test the connections between all the departments. For simplicity, we will not post all the logs, but resume them in the table 4 below. As we can see, the network restrictions were all applied successfully.

Table 4. Testing the ACLs

		Connection target		
		ACCOUNTING	MARKETING	IT
Connection initiator	ACCOUNTING	✓	✓	✗
	MARKETING	✗	✓	✗
	IT	✓	✓	✓

7. Automatic DHCP for hosts

The following configurations were applied:

- Accounting LAN Router:

```
ip dhcp excluded-address 196.240.17.1 196.240.17.2
ip dhcp excluded-address 196.240.17.63
ip dhcp pool ACCOUNTING
      network 196.240.17.0 255.255.255.192
      default-router 196.240.17.1
```

- Marketing LAN Router:

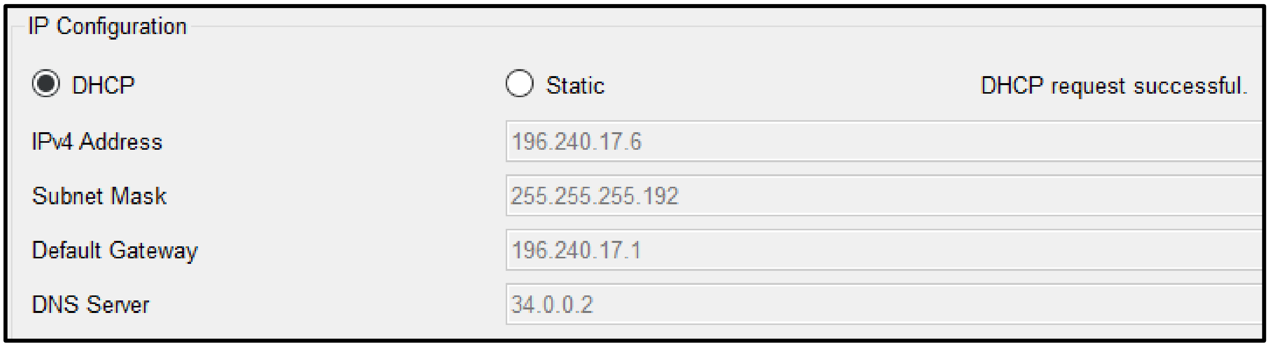
```
ip dhcp excluded-address 196.240.17.65 196.240.17.66
ip dhcp excluded-address 196.240.17.127
ip dhcp pool MARKETING
      network 196.240.17.64 255.255.255.192
      default-router 196.240.17.65
```

- IT LAN Router:

```
ip dhcp excluded-address 196.240.17.129 196.240.17.130
ip dhcp excluded-address 196.240.17.191
ip dhcp pool IT
      network 196.240.17.128 255.255.255.192
      default-router 196.240.17.129
```

7.1 Experimental Results

For the experimental part of this chapter, we attempted to go to one of the hosts and switch from the Static IP to DHCP. Immediately, the message "Requesting IP Address" pops out, and after a while, the host receives a correct configuration, as we can see in the figure 5 below. The experiment was repeated on multiple hosts, every time being successful, demonstrating that the network has automatic IP Assignment capacities through DHCP.



IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address	196.240.17.6
Subnet Mask	255.255.255.192
Default Gateway	196.240.17.1
DNS Server	34.0.0.2

Figure 5. DHCP Addressing on a host

8. Network Expansion

In the previous chapters of this paper, it has been mentioned the reserved LAN, for network scalability purposes. In this chapter, we are going to replace the reserved LAN with a remote subnetwork of 34.0.0.0 /16, simulating a connection to an outside network, thorugh a WAN link.

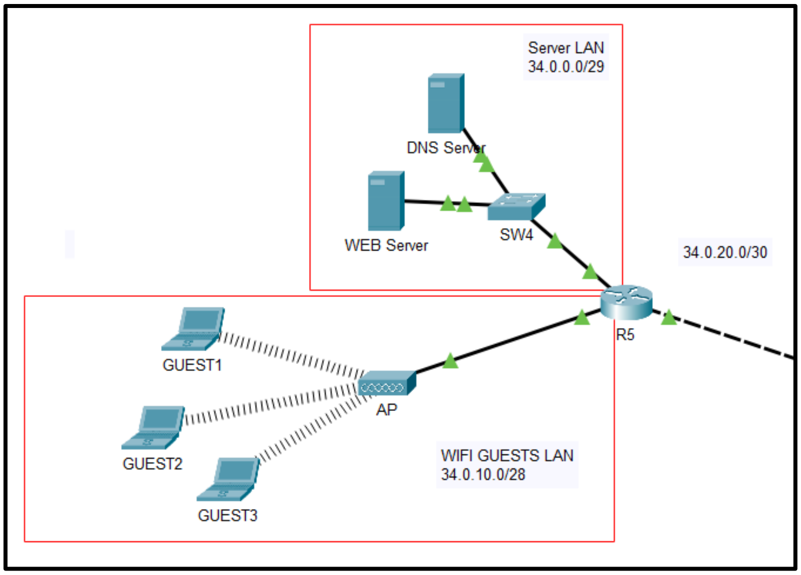
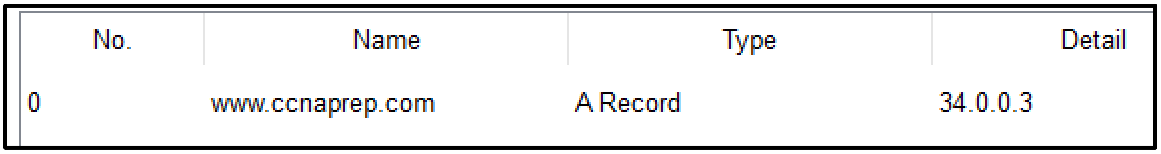


Figure 6. The new remote LAN

Figure 6 above shows the network expansion topology, where 2 servers were added, a Web Server and a DNS Server, and also an Access Point for connecting guests to the network, through wireless links.

An access list was configured to permit all the hosts to access the Web Server, and another one was configured to allow the guests connected to AP to have access to the Web Server, but not to the hosts.

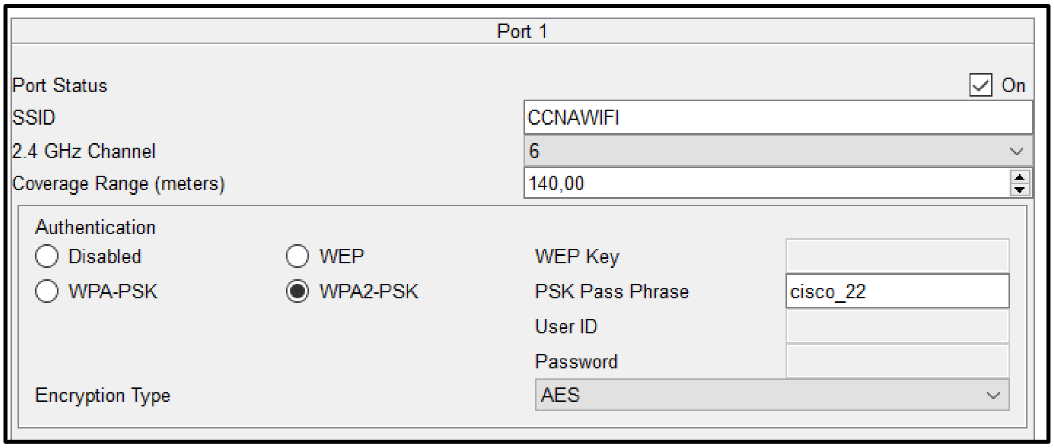
The DNS Server was also configured to be broadcast to all the hosts, and on this server, we configured a name for the Web Server, as shown in the picture 7 below.



No.	Name	Type	Detail
0	www.ccnaprep.com	A Record	34.0.0.3

Figure 7. The DNS Server configuration of the Web Server

The basic web page on the Web Server was also a little modified.The AP was configured with a basic password and a SSID, as presented in figure 8 below.



Port 1

Port Status ☑ On

SSID: CCNAWIFI

2.4 GHz Channel: 6

Coverage Range (meters): 140,00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: cisco_22

User ID:

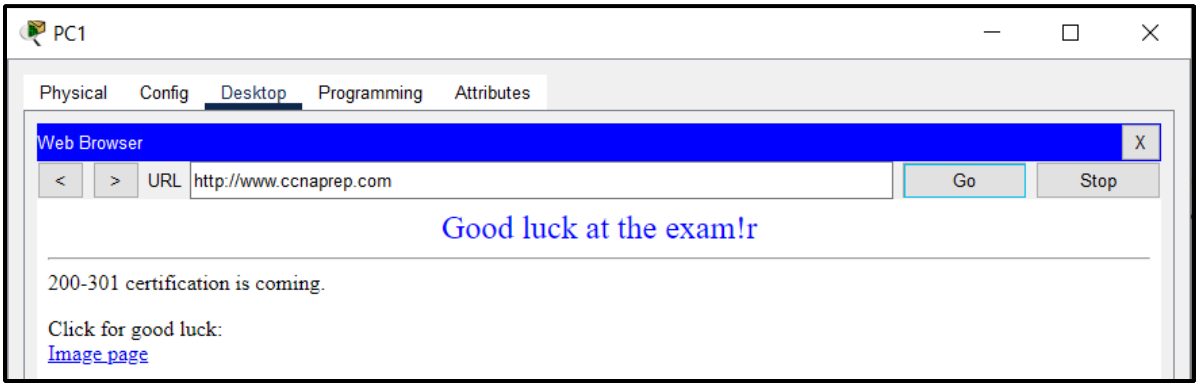
Password:

Encryption Type: AES

Figure 8. The AP Configuration

8.1 Experimental Results

When attempting to access the Web Server from one of the hosts, the connection establishes successfully, as we can see in figure 9 below, demonstrating that the DNS and Web Servers configurations were done successfully, and also, the access list is permitting hosts to access the Web Server.



URL: http://www.ccnaprep.com

Good luck at the exam!r

200-301 certification is coming.

Click for good luck:
Image page

Figure 9. The page from the Web Server

The guest Wi-Fi laptops successfully connect to the AP using the password, and when attempting to ping any of the PC hosts, they prompt the following log, demonstrating that the AP was correctly configured and the ACL was also applied.

```
C:\>ping 196.240.17.3

Pinging 196.240.17.3 with 32 bytes of data:

Reply from 34.0.10.1: Destination host unreachable.
Reply from 34.0.10.1: Destination host unreachable.
Reply from 34.0.10.1: Destination host unreachable.
Reply from 34.0.10.1: Destination host unreachable.

Ping statistics for 196.240.17.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

9. Conclusions and Future Work

This project starts with the fundamental process of subnetting the network, and continues with more complicated aspects, such as configuring the VLANs on the switches or the OSPF Routing between the routers, restricting access with ACLs, or providing automatic IP Addressing capabilities through DHCP. The last part of the network is the extended network, which adds two servers, a Web Server and a DNS Server, and also an AP. The two servers are configured with basic features, and the AP is configured to connect the wireless guests to the network. The network has a complete connectivity, unless the rules applied by the ACLs, the servers and the AP are working fine, and most important, the network offers two fundamental erquirements of any network, the scalability and the redundancy.

As a future work, the network can be expanded even more, providing RADIUS or TACACS+ servers, used for addressing the security part of the network. Talking about security, a VPN connection can also be implemented when conecting to a remote network. Redundancy aspects also can be improved, offering layer 2 redundancy with multiple switches and STP or layer 3 redundancy with FHRP.

References

[1] CCNAv7: Introduction to Networks courses
[2] CCNAv7: Switching, Routing, and Wireless Essentials courses
[3] CCNAv7: Enterprise Networking, Security, and Automation courses

Software Supplied

The implementation of this project was done in Packet Tracer. Attached to this documentation file can be found the Packet Tracer source: `SOHO_Network_Implementation_in_Packet_Tracer.pkt`