|  |
| --- |
| **Luminus Technical University College**  **Computer Networking**  **C:\Users\STUDENT\AppData\Local\Microsoft\Windows\INetCache\Content.Word\307059568_461032855779622_1906187270458418347_n.png**  **Final Project Report**  **(IIS Company)**  **Laith Obeidat**  **Khaldoon Al-Azzam**  **Rahmah Gharaibeh**    **Supervisor: Eng. Israa Saadeh**  **Date: 22th September 2022** |
|  |

|  |  |  |
| --- | --- | --- |
|  |  |  |

Table of Contents

[Abstract i](#_Toc114690096)

[Chapter 1: Introduction ii](#_Toc114690097)

[Chapter 2: Background 2](#_Toc114690098)

[Chapter 3: Design 3](#_Toc114690099)

[Chapter 4: Implementation 9](#_Toc114690100)

[Chapter 5: Results and Discussion 18](#_Toc114690101)

[Chapter 6: Economical, Cost and Environment 19](#_Toc114690102)

[Chapter 7: Project Management 20](#_Toc114690103)

[Chapter 8: Conclusion and Future Work 21](#_Toc114690104)

# Abstract

The general aim of this project is to You are senior Network Engineer at IIS Company, the company is applying new infrastructure deployments, new devices are needed to be brought for Head Quarter (HQ) site and remote branches, and they have three branches (Amman, Irbid, and Salt).

You are requested to build a topology where you can achieve full connectivity between the clients in HQ and all branches’ sites. You also asked to achieve a secure connection between the main site and branch Amman site using VPN site-to-site connection, it is important that you don’t exceed the budget for the company project.

Security measures need to be taken to consideration on your solution (ACL, Telnet, SSH and basic network device security).

Your budget should not exceed 85,000 USD for routers, switches cabling and any required expansion cards such as HWIC.

# Chapter 1: Introduction

* 1. **Overview**

The aim of this project is to build a complete network containing three branches connected with the HQ branch to prepare us for the job technical after completing the CCNA course.

This project has the HQ and remote branches and they have three branches of Irbid, Amman and Salt.

* 1. **Aims and objectives**

The general aim of this project is to simulate a Network system which is secure and fast and reliable that can handle the requirements of company and adopt to technology growth.

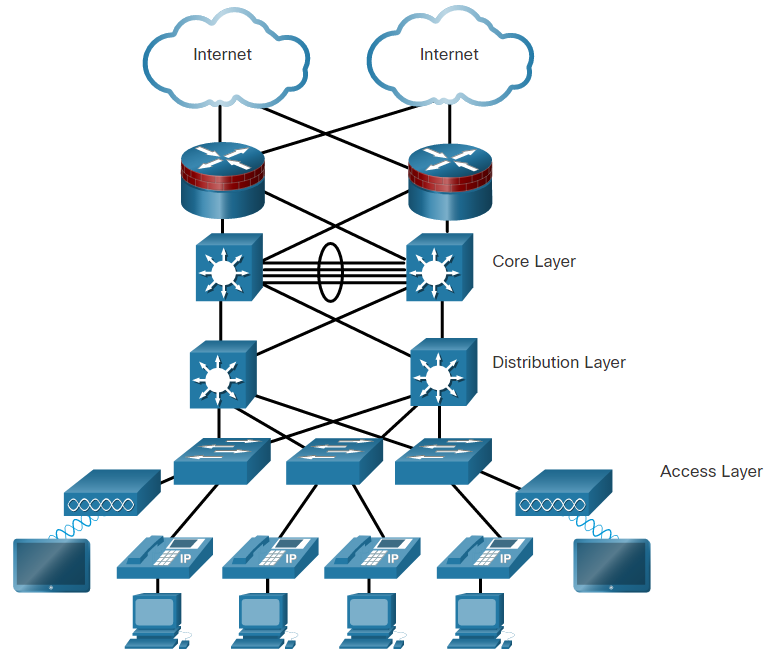
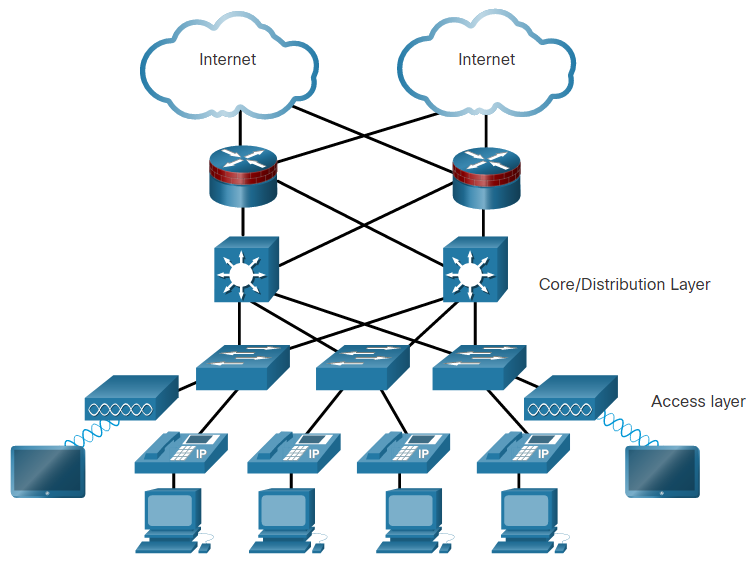
* 1. **The main solution idea**

simulate a Company Network system which is secure, fast, full redundancy, scalability and reliable that will help the company to make the right adjustments on the network infrastructure, with all the configurations and step by step on how to adjust the network infrastructure to meet the right requirements of company.

* 1. **The key technical details of the solution**

In our network structure we used The Three Tier Architecture in Head Quarter build an extended-star physical network topology from a centralized building location to all other buildings on the same company.

In other branches we used The Tow Tier Architecture useful for smaller company locations, or in company sites consisting of a single building.

 ****

**Figure 1: The Three Tier Architecture Figure 2: The Tow Tier Architecture**

* 1. **Summary of report structure**

In this report we try to discuss all aspects of the project background, design, implementation etc. In abstract we provided a brief about the idea of the problem and the solution it needs ,in the introduction we provided more details about the design, in the background we talk about the problem and the importance of solving it, in the design we talk about the details of the network infrastructure design and what is the functionality of each element also we talk about design alternatives and specifications, in the implementation we talk about how to simulate network infrastructure and the right configurations needed with a lot of protocols used , in the result and discussion we talk about the success of the simulation and how each adjustment is met and the strengths and weakness of network infrastructure , in project management we provide a chart using Gantt project to describe the sequences that followed to achieve this project, in the conclusion and future work we talk about a brief conclusion about the whole project and about possible future updates to the network infrastructure and trying to implement cloud computing solutions in the future.

# Chapter 2: Background

* 1. **Background of the problem**

Technology continues to create new learning and job opportunities for todays, but the rapid rate at which it advances can make it difficult for many company establishments to keep up.

From familiar challenges like work experience, a number of common IT company need need employees have work experience.

* 1. **Target market and their needs**

Companies that need experienced practical staff to keep pace with technological development in IT companies and rapid harmony in the working environment.

* 1. **The different approaches currently/previously used to solve the problem**

Most of the old approaches was by updating the software and applying certain fixes which is just for small period of time solutions, but for the new approaches now is moving the infrastructure to the cloud, and we could move some applications to the cloud to lower the demands of the current, on-premise infrastructure and this will lower the cost and give a lot of advantages.

# Chapter 3: Design

* 1. **Design Overview:**
     1. **Network design**

In our network structure we will use The Three Tier Architecture in Head Quarter:

Also known as Three-layered Hierarchical Model, this is the Cisco flagship design for networks.

Its concepts can be applied to any network.

This three-tier architecture is the most scalable and resilient solution. It’s clear and simple design makes it also really easy to manage.

The combination of these characteristics makes this design the best for large enterprises, where you need to connect thousands of devices on a large company, even spanning onto several buildings.

Devices into the same tier have all the same roles. Even for this, Cisco provides us the best practices and specifications.

This approach defines three layers: Core, Distribution, and Access. Each layer has its specific purpose, so what we implement into the access layer won’t be implemented on the distribution and so on.

In our network structure we will use The Tow Tier Architecture in other branches:

We didn't need to use Three Tier Architecture as we fulfilled all the requirements of full-connectivity and redundancy with more performance, speed and less cost.

* The Access Layer

The Access Layer is the one closer to the users***.*** In fact, at this layer, we find the users themselves and the access-layer switches. The main purpose of this layer is to physically connect users to the network. In other words, there is just a cable between end-user PCs and access-layer switches.

At this layer, we apply **network-access policies**. These are the security policies we want to enforce in order to allow access to the network. For example, we can configure port-security or Network Access Control to ensure that only our company’s PC can have access to the network. Access switches propagate layer 2 broadcast domains to users, so we need to implement **VLANs**there.

* The Distribution Layer

The Distribution layer bridges users to the core layer*.* It serves as a major spine for all users in an area, so it connects several access switches. In most deployment, Default Gateways for all the VLANs reside at the Distribution layer.

Cisco encourages you to reduce Layer 2 links in your network, having all Layer 3 links but the ones going directly to users. However, this is not yet possible as it requires some advanced access switches. As a result, the compromise implemented often-times is to have Layer 2 links between the Access and Distribution layer. This way, you can have**default gateways** residing at the distribution layer. Furthermore, here you can apply **distribution policies**. These policies include filtering traffic to allow some devices to reach only some of the other devices, or policy-routing

While possible to connect server devices directly to the distribution switches, Cisco recommends connecting all end devices to access switches. This way, you reduce the overall cost-per-port of the infrastructure.

At this layer, you have to use multilayer switches. Furthermore, their form factor should be at least stackable, so that you can expand the distribution layer in case you need more ports. In large deployments, you can find modular switches at this layer.

* The Core Layer

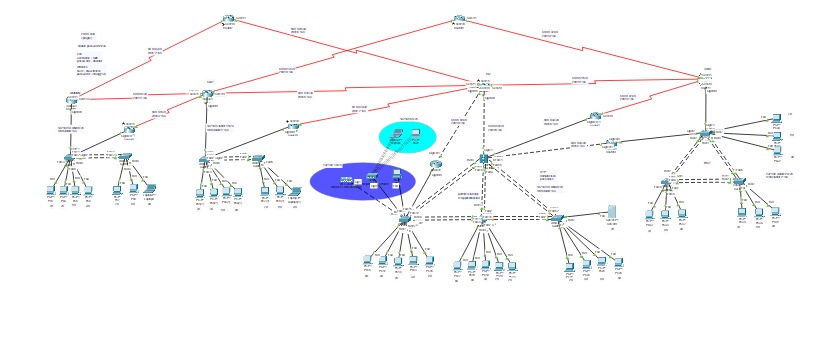
In the Three-Tier Architecture, the Core Layer is the one coordinating everything***.*** It has only one, simple purpose: connecting all the distribution layers together. In large enterprises, where you have several distribution switches, the core layer is also known as **Backbone.**

Cisco is very clear about the purpose of this layer. Its only role is to **forward traffic, the fastest it can.** Here you don’t apply any policy, as you must try to reduce the load of the core so it can focus on routing. It is likely that your core switches talk with distribution switches using dynamic routing protocols***,*** such as OSPF or EIGRP.

At this layer, we find the most advanced and expensive switches, the ones with the modular form factor. These are fully redundant devices supporting advanced Layer 3 switching features and dynamic routing protocols. However, remember that you need to keep your configuration as simple as possible on devices in this role.

* + 1. **Network Infrastructure**

This is the network infrastructure which consist of 4 branches: Head Quarter, Amman, Irbid and Salt.



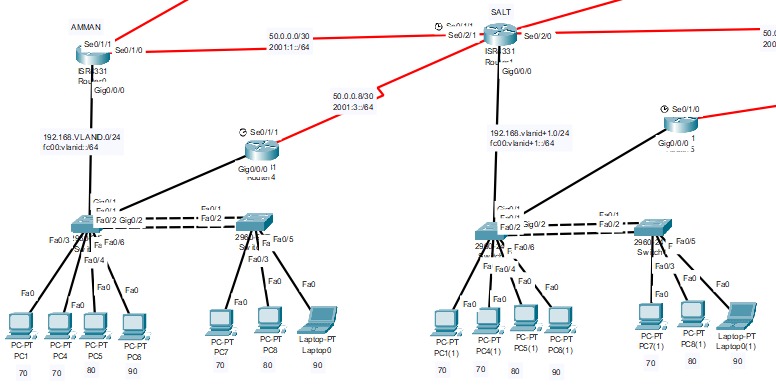
**Figure3: Network Design**

The network infrastructure has the three phases: availability, Security, Speed which will give the company the full ability to interact with each other fast and securely.

All L3 and L2 devices have full redundancy each other’s, so if one device has any problem, we have other for this:

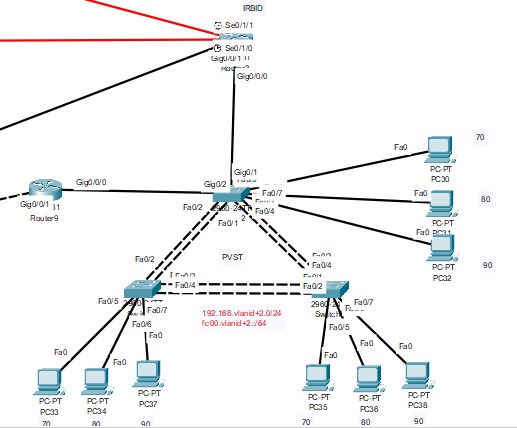
* Amman has two paths connected to the HQ and the second in the Salt and if the Amman router is down, it has a backup router (HSRP).
* Salt has three paths connected to the HQ, to the Irbid, and Amman, and if the Salt router is down, it has a backup router (HSRP).

We have scalability if any branches need this and full connectivity in IPversion6



**Figure6: Salt and Amman**

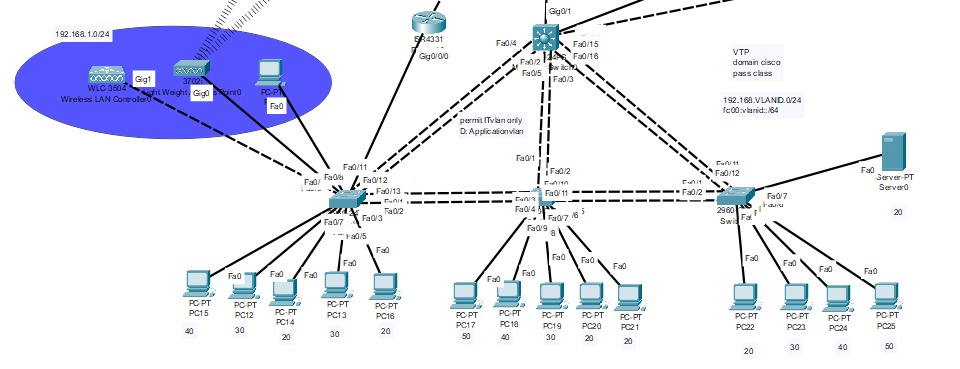
It consists of the two layers Distribution layer, Access layer. Router for routing between VLANs using Router-on-Stick. Redundancy for L3 by using HSRP and backup paths. We applied full redundancy in all L2 devices (switches) and used by EtherChannel protocol. Router Salt is DHCP server. We used dynamic protocol for IPV4 and IPV6 by OSPF routing protocol in Amman area 4 , Salt area 0.



**Figure5: Irbid**

It consists of the two layers Distribution layer, Access layer. Router for routing between VLANs using Router-on-Stick. Redundancy for L3 by using HSRP and back up path. We blocked all network to management VLAN (remote configuration) except VLAN IT in all branches and Head Quarter. We applied full redundancy and load balancing in all L2 devices (switches) and used by EtherChannel protocol. We used dynamic protocol for IPV4 and IPV6 by OSPF routing protocol in area 99. We applied PVST on VLANs to redundancy and load balancing (Each switch root bridge to VLAN and backup to other VLAN, each path blocked to VLAN).

* Switch 1 root bridge VLAN 70, Backup root VLAN 90
* Switch 2 root bridge VLAN 80, Backup root VLAN 70
* Switch 3 root bridge VLAN 90, Backup root VLAN 80



**Figure4: Head Quarter**

It consists of the three layers Core layer, Distribution layer, Access layer. Multilayer switch in HQ for routing between VLANs using SVI. The router is a backup for multilayer by using HSRP. We applied backup for HQ router by connect Multilayer with IRBID branches. We blocked all network to access in VLAN Application except VLAN IT in all branches and Head Quarter. We applied full redundancy and load balancing in all L2 devices (switches) and used by EtherChannel protocol. we used dynamic protocol for IPV4 and IPV6 by OSPF routing protocol in area 0. Router HQ is DHCP server for all network in all branches.

We applied WLC with one LAP for wireless clients in HQ.

* Configure the WLC username “ADMIN” and password “Admin123”.
* Configure one SSID and name HQ-wireless and password (Israa@123) and map it to VLAN 5.
* We add pool to VLAN 5 on Multilayer.

VTP: VLAN Trucking Protocol

* Multilayer switch is server mode and other switch in HQ mode client.
* Domain (cisco) pass (class).
  1. **Design Details:**
     1. **Design Specifications**

The network structure has many phases:

1. Availability.

2. Security.

3. Speed.

4.Full-Reduncy.

5.Scalability

6.Easy of management.

7.Full-Connectivity.

8.Performance.

It will consist of: Routers, switches, servers, physical links.

Also consist of all the necessary technologies to deploy the many phases such as :ACL,VLAN,IP ADDRESS,DHCP,SPANNING-TREE, BPDU Guard, OSPF, VLSM, HSRP, SSH, Port Security, NAT BY PAT, VPN by GRE ,SYSLOG,NTP,DTP,ETHERCHANNEL.

* + 1. **Design Standards**

1. The IEEE -Standards Association (IEEE-SA): the leading developer of global industry standards in a broad-range of industries, including Power and Energy, Biomedical and Healthcare, Information Technology, Telecommunications, Transportation, Nanotechnology, and Information Assurance
2. The National Standards Network (NSSN)
3. Internet Assigned Numbers Authority (IANA)

# Chapter 4: Implementation

* 1. **Methods and tools (hardware, software … etc.) used to implement the solution**

We used Packet tracer to simulate the network infrastructure with all the configurations needed

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

* 1. **Infrastructure used in the solution**

The Three Tier Architecture Also known as Three-layered Hierarchical Model, this is the Cisco flagship design for Company networks in HQ. The Tow Tier Architecture Also known as Tow layered Hierarchical Model, used when separate distribution and core layers is not required, Useful for smaller company locations, or in company sites consisting of a single building.

* 1. **The trade-offs that we had to make in the design/implementation?**

We used Copper cross-over instead of fiber optic because the simulation does not offer it but in real world implementations it’s preferred to use fiber optics for high speed and low latency.

* 1. **The dependencies/assumptions of the implementation?**

|  |  |  |  |
| --- | --- | --- | --- |
| Device | port | IPv4 | IPv6 |
| Amman | GIG 0/0/0.10 | 192.168.10.1/24 | Fc00:10: :1/64 |
| Amman | GIG 0/0/0.70 | 192.168.70.1/24 | Fc00:70: :1/64 |
| Amman | GIG 0/0/0.80 | 192.168.80.1/24 | Fc00:80: :1/64 |
| Amman | GIG 0/0/0.90 | 192.168.90.1/24 | Fc00:90: :1/64 |
| Amman | SER0/1/0 | 50.0.0.5/30 | 2001:2::1/64 |
| Amman | SER0/1/1 | 50.0.0.1/30 | 2001:1::1/64 |
| AmmanHsrp | GIG 0/0/0.10 | 192.168.10.2/24 | Fc00:10: :2/64 |
| AmmanHsrp | GIG 0/0/0.70 | 192.168.70.2/24 | Fc00:70: :2/64 |
| AmmanHsrp | GIG 0/0/0.80 | 192.168.80.2/24 | Fc00:80: :2/64 |
| AmmanHsrp | GIG 0/0/0.90 | 192.168.90.2/24 | Fc00:90: :2/64 |
| AmmanHsrp | SER0/1/1 | 50.0.0.9/30 | 2001:3::1/64 |
| Salt | GIG 0/0/0.10 | 192.168.11.1/24 | Fc00:11: :1/64 |
| Salt | GIG 0/0/0.70 | 192.168.71.1/24 | Fc00:71: :1/64 |
| Salt | GIG 0/0/0.80 | 192.168.81.1/24 | Fc00:81: :1/64 |
| Salt | GIG 0/0/0.90 | 192.168.91.1/24 | Fc00:91: :1/64 |
| Salt | SER0/1/0 | 50.0.0.17/30 | 2001:5::1/64 |
| Salt | SER0/1/1 | 50.0.0.2/30 | 2001:1::2/64 |
| Salt | SER0/2/0 | 50.0.0.13/30 | 2001:4::1/64 |
| Salt | SER0/2/1 | 50.0.0.10/30 | 2001:3::2/64 |
| SaltHsrp | GIG 0/0/0.10 | 192.168.11.2/24 | Fc00:11: :2/64 |
| SaltHsrp | GIG 0/0/0.70 | 192.168.71.2/24 | Fc00:71: :2/64 |
| SaltHsrp | GIG 0/0/0.80 | 192.168.81.2/24 | Fc00:81: :2/64 |
| SaltHsrp | GIG 0/0/0.90 | 192.168.91.2/24 | Fc00:91: :2/64 |
| SaltHsrp | SER0/1/0 | 50.0.0.25/30 | 2001:7::1/64 |
| HQ | SER0/1/0 | 50.0.0.18/30 | 2001:5::2/64 |
| HQ | SER0/1/1 | 50.0.0.22/30 | 2001:6::2/64 |
| HQ | SER0/2/0 | 50.0.0.29/30 | 2001:8::1/64 |
| HQ | SER0/2/1 | 50.0.0.26/30 | 2001:7::2/64 |
| HQ | GIG 0/0/0 | 50.0.0.41/30 | 2001: b: :1/64 |
| HQ | GIG 0/0/1 | 50.0.0.49/30 | 2001: d: :1/64 |
| MLSHQ | GIG 0/1 | 50.0.0.42/30 | 2001:b::2/64 |
| MLSHQ | GIG 0/2 | 50.0.0.37/30 | 2001:a::1/64 |
| MLSHQ | VLAN1 | 192.168.1.1/24 | Fc00:1::1/64 |
| MLSHQ | VLAN5 | 192.168.5.1/24 | Fc00:5::1/64 |
| MLSHQ | VLAN10 | 192.168.13.1/24 | Fc00:13::1/64 |
| MLSHQ | VLAN20 | 192.168.20.1/24 | Fc00:20::1/64 |
| MLSHQ | VLAN30 | 192.168.30.1/24 | Fc00:30::1/64 |
| MLSHQ | VLAN40 | 192.168.40.1/24 | Fc00:40::1/64 |
| MLSHQ | VLAN50 | 192.168.50.1/24 | Fc00:50::1/64 |
| HsrpMLS | GIG 0/0/1 | 50.0.0.50/30 | 2001: d: :2/64 |
| HsrpMLS | GIG 0/0/0.1 | 192.168.1.2/24 | Fc00:1::2/64 |
| HsrpMLS | GIG 0/0/0.5 | 192.168.5.2/24 | Fc00:5::2/64 |
| HsrpMLS | GIG 0/0/0.10 | 192.168.13.2/24 | Fc00:13::2/64 |
| HsrpMLS | GIG 0/0/0.20 | 192.168.20.2/24 | Fc00:20::2/64 |
| HsrpMLS | GIG 0/0/0.30 | 192.168.30.2/24 | Fc00:30::2/64 |
| HsrpMLS | GIG 0/0/0.40 | 192.168.40.2/24 | Fc00:40::2/64 |
| HsrpMLS | GIG 0/0/0.50 | 192.168.50.2/24 | Fc00:50::2/64 |
| SYSLOG and NTP | N/R | 192.168.20.20 | Fc00:20::20/64 |
| Irbid | GIG 0/0/0.10 | 192.168.12.1/24 | Fc00:12: :1/64 |
| Irbid | GIG 0/0/0.70 | 192.168.72.1/24 | Fc00:72: :1/64 |
| Irbid | GIG 0/0/0.80 | 192.168.82.1/24 | Fc00:82: :1/64 |
| Irbid | GIG 0/0/0.90 | 192.168.92.1/24 | Fc00:92: :1/64 |
| Irbid | SER0/1/0 | 50.0.0.30/30 | 2001:9::2/64 |
| Irbid | SER0/1/1 | 50.0.0.34/30 | 2001:8::2/64 |
| Irbid | SER0/2/0 | 50.0.0.54/30 | 2001: e: :2/64 |
| IrbidHsrp | GIG 0/0/0.10 | 192.168.12.2/24 | Fc00:12: :2/64 |
| IrbidHsrp | GIG 0/0/0.70 | 192.168.72.2/24 | Fc00:72: :2/64 |
| IrbidHsrp | GIG 0/0/0.80 | 192.168.82.2/24 | Fc00:82: :2/64 |
| IrbidHsrp | GIG 0/0/0.90 | 192.168.92.2/24 | Fc00:92: :2/64 |
| IrbidHsrp | GIG 0/0/1 | 50.0.0.46/30 | 2001:c: :2/64 |
| Backup1 | SER0/1/0 | 50.0.0.6/30 | 2001:2::2/64 |
| Backup1 | SER0/1/1 | 50.0.0.21/30 | 2001:6::1/64 |
| Backup2 | SER0/1/0 | 50.0.0.14/30 | 2001:4::2/64 |
| Backup2 | SER0/1/1 | 50.0.0.33/30 | 2001:9::1/64 |
| BackupHQ | SER0/1/0 | 50.0.0.53/30 | 2001: e: :1/64 |
| BackupHQ | GIG 0/0/0 | 50.0.0.38/30 | 2001:a: :2/64 |

**Table2 : IP Schema**

* 1. **virtual LAN (VLAN)**

VLANs are logical connections with other similar devices.

Placing devices into various VLANs have the following characteristics:

* Provides segmentation of the various groups of devices on the same switches
* Provide organization that is more manageable
* Broadcasts, multicasts and unicasts are isolated in the individual VLAN
* Each VLAN will have its own unique range of IP addressing
* Smaller broadcast domains

**Table of VLAN’s in HQ**

|  |  |  |
| --- | --- | --- |
| **VLAN ID** | **VLANs Name** | **Number of Clients** |
| 10 | Management | None |
| 99 | Native | None |
| 20 | Sales | 5 |
| 30 | Engineers | 4 |
| 40 | IT | 3 |
| 50 | Application | 2 |
| 5 | Wireless | 1 |

**Table3: VLAN’s in HQ**

**Table of VLAN in Branch Office (Branch Amman, Irbid, and Salt)**

|  |  |  |
| --- | --- | --- |
| **VLAN ID** | **VLAN Name** | **Number of Client** |
| 10 | Mgmt. | None |
| 99 | Native | None |
| 70 | Auditing | 3 |
| 80 | IT | 2 |
| 90 | Admin | 2 |

**Table4: VLAN’s in Other branches.**

* 1. **Dynamic Host Configuration Protocol (DHCP)**

Dynamic Host Configuration Protocol v4 (DHCPv4) assigns IPv4 addresses and other network configuration information dynamically. DHCPv4 is an extremely useful and timesaving tool for network administrators.

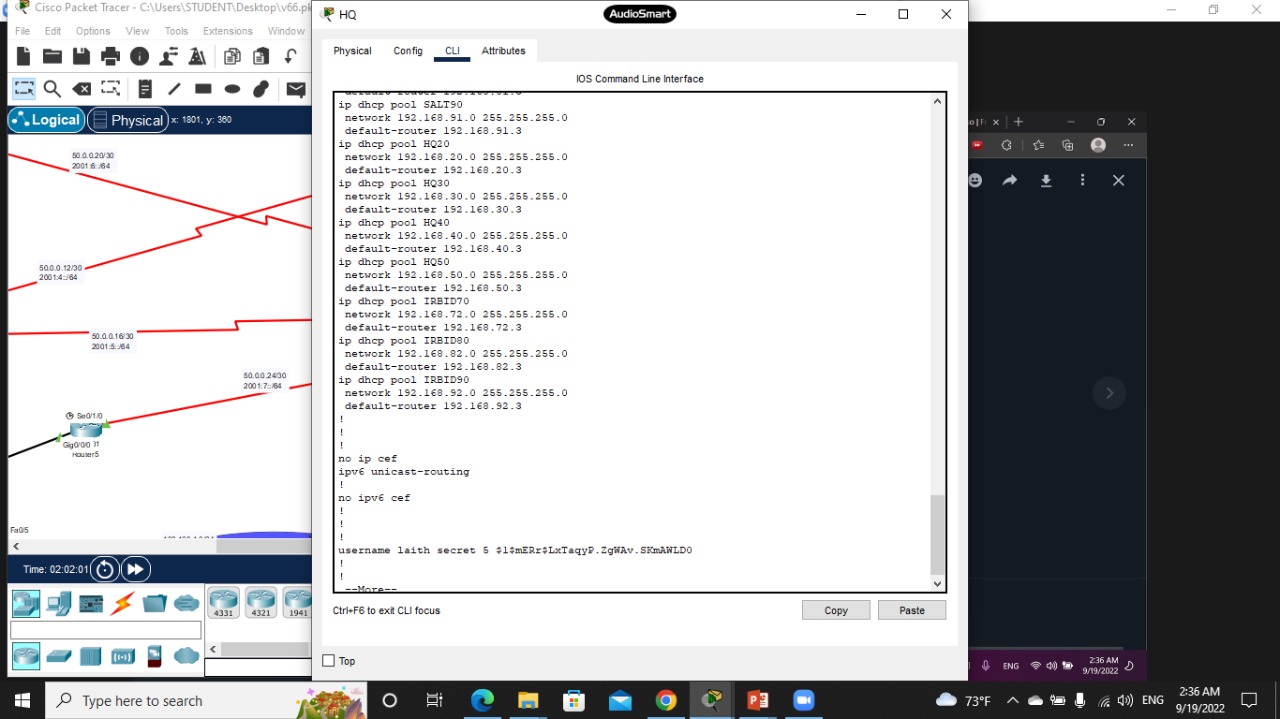
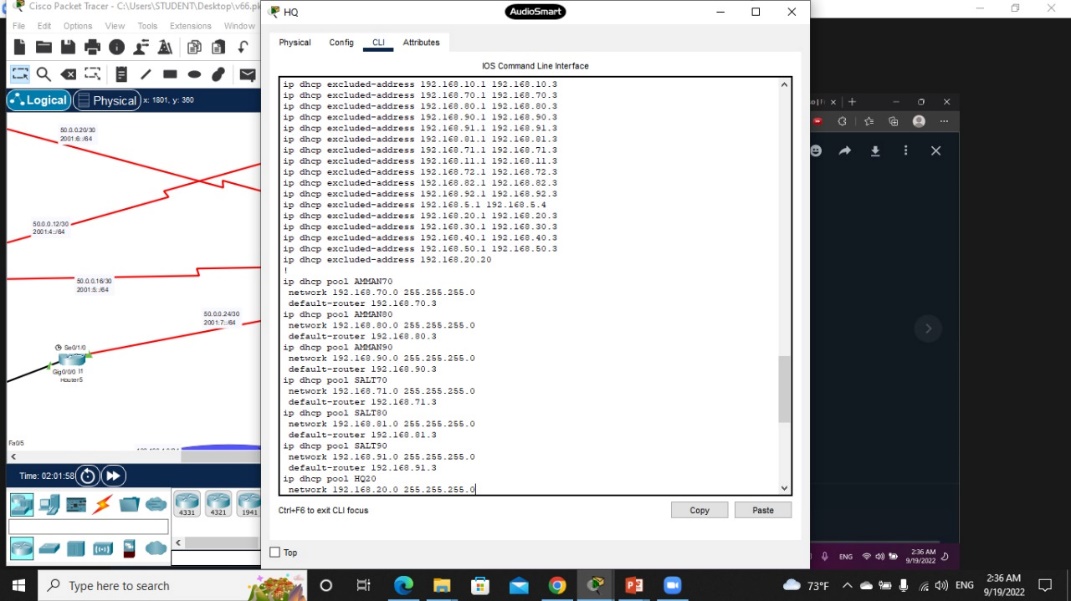
A dedicated DHCPv4 server is scalable and relatively easy to manage. However, in a small branch or SOHO location, a Cisco router can be configured to provide DHCPv4 services without the need for a dedicated server. Cisco IOS software supports an optional, full-featured DHCPv4 server.

The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address.

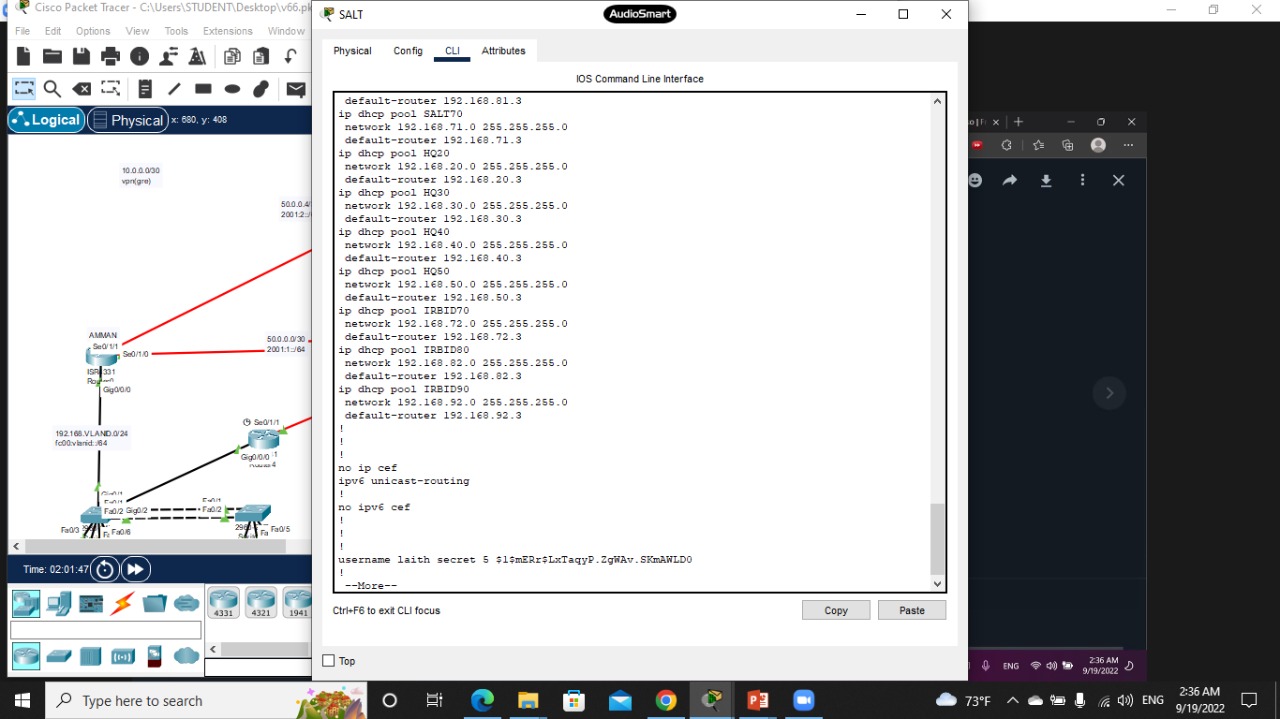
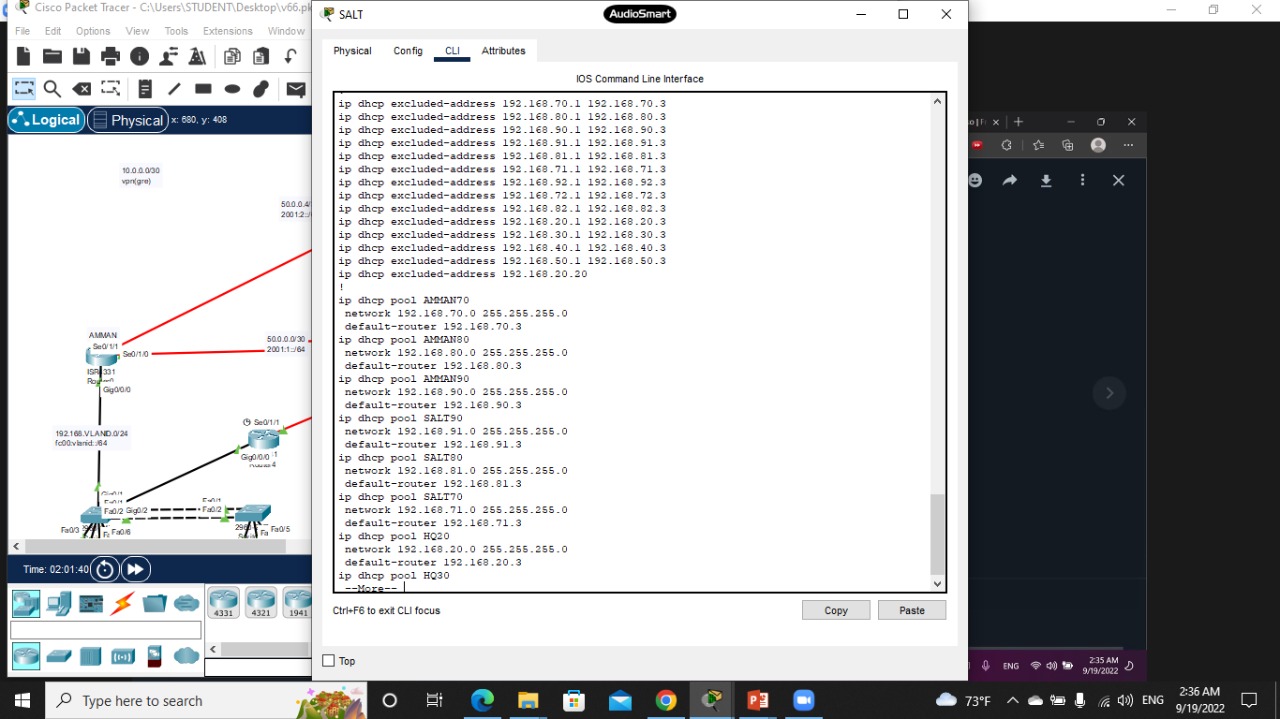
The lease is typically anywhere from 24 hours to a week or more. When the lease expires, the client must ask for another address, although the client is typically reassigned the same address.

We configure DHCP for each VLAN through 2 DHCP Router redundant to each other.

ALL client in each Branches take IP address from DHCP.The HQ and Salt Router is the DHCP server.

**Figure5: DHCP in Head Quarter**

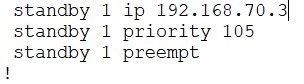


**Figure6: DHCP in Salt**

* 1. **Hot Standby Router Protocol** (**HSRP**):

Cisco provides HSRP and HSRP for IPv6 as a way to avoid losing outside network access if your default router fails. HSRP is a Cisco-proprietary FHRP that is designed to allow for transparent failover of a first-hop IP device.

HSRP ensures high network availability by providing first-hop routing redundancy for IP hosts on networks configured with an IP default gateway address. In a group of device interfaces, the active device is the device that is used for routing packets; the standby device is the device that takes over when the active device fails, or when pre-set conditions are met. The function of the HSRP standby router is to monitor the operational status of the HSRP group and to quickly assume packet-forwarding responsibility if the active router fails.

**Figure6: DHCP in Amman**

* 1. **The Spanning Tree Protocol (STP):**

Spanning Tree Protocol (STP) is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology.

STP logically blocks physical loops in a Layer 2 network, preventing frames from circling the network forever.

STP compensates for a failure in the network by recalculating and opening up previously blocked ports.

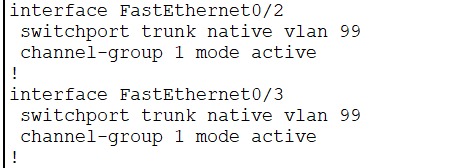
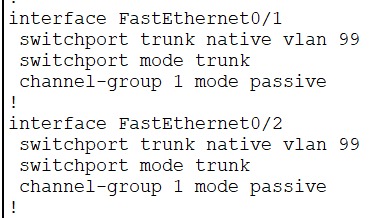
By default, in all switches.

It Work in HQ switches when we connect all switches to other as a triangle this is make loop so STP it works by default.

* 1. **EtherChannel:**

EtherChannel technology was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel.

EtherChannel provides redundancy because the overall link is seen as one logical connection. Additionally, the loss of one physical link within the channel does not create a change in the topology.

**Figure7: EtherChannel**

* 1. **NAT by using PAT:**

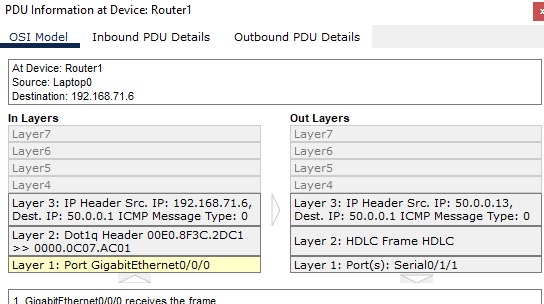
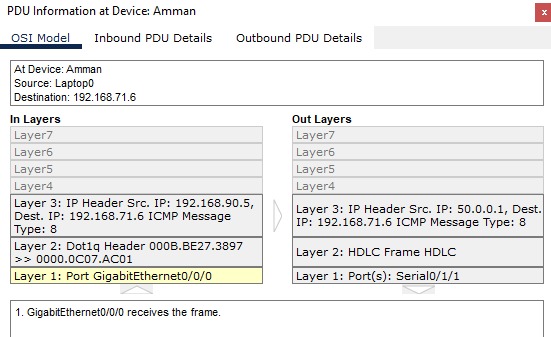
The primary use of NAT is to conserve public IPv4 addresses.

NAT allows networks to use private IPv4 addresses internally and translates them to a public address when needed.

A NAT router typically operates at the border of a stub network.

When a device inside the stub network wants to communicate with a device outside of its network, the packet is forwarded to the border router which performs the NAT process, translating the internal private address of the device to a public, outside, routable address.

we applied NAT in all branches, each branches has one public IP.



**Figure8: NAT**

* 1. **DTP: Dynamic Trucking Protocol (DTP)**

Is a proprietary Cisco protocol.

DTP characteristics are as follows:

* On by default on Catalyst 2960 and 2950 switches
* Dynamic-auto is default on the 2960 and 2950 switches
* May be turned back on by setting the interface to dynamic-auto
* Setting a switch to a static trunk or static access will avoid negotiation issues with the switchport mode trunk or the switchport mode access commands

we used it in all switches port trunk and access to avoid negotiation issues.

* 1. **NTP and SYSLOG:**

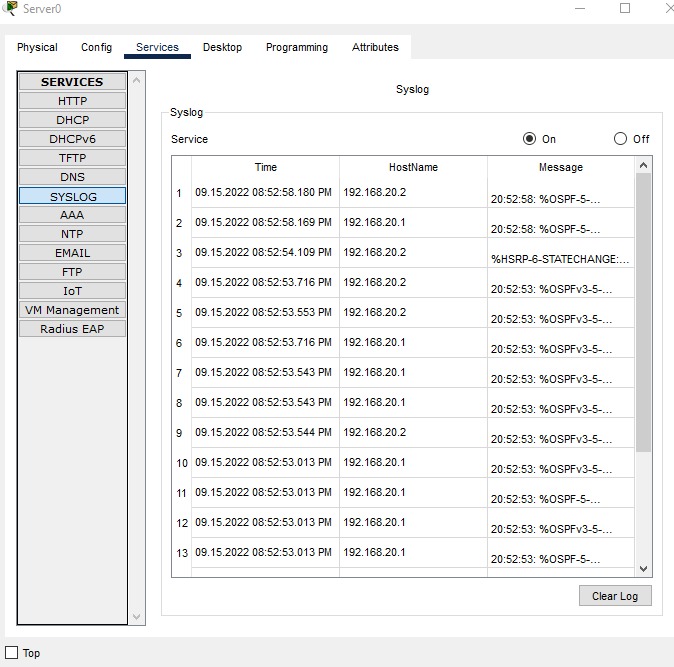
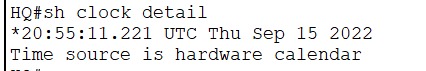
The software clock on a router or switch starts when the system boots. It is the primary source of time for the system. It is important to synchronize the time across all devices on the network. When the time is not synchronized between devices, it will be impossible to determine the order of the events and the cause of an event.​

If a violation happened send a log message to syslog server.

we gather network devices traps and messages and save them to a

Syslog server on both HQ and BO sites.

Typically, we configure the Network Time Protocol (NTP) and SYSLOG on server (192.168.20.20 | fc00:20::20) and connected it to all devices



**Figure9: NTP and SYSLOG**

* 1. **Security**

SSH:

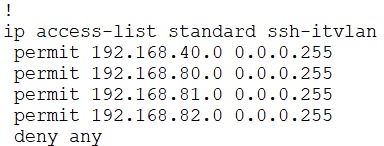
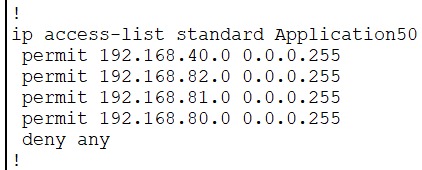
* Access all routers and switches with only SSH, use RSA with 2048.
* Use (laith) as a username and (obeidat) as the password.
* Access in IPv4 and IPv6.

Port Security:

* All unused ports need to be shutdown.
* In port security maximum mac address learned is 4, and learned the mac address sticky.
* Disable BPDU messages on all access ports and enable port fast.

ACL in IPv4 and IPv6:

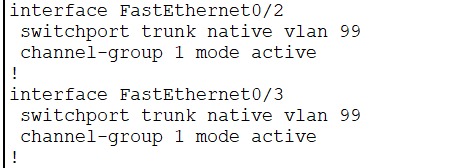
* Only IT VLAN can access Application VLAN in HQ
* Only IT VLAN can SSH network devices in Branch Irbid



**Figure10: ACL**

Native VLAN:

The use of a native VLAN was designed for legacy use, like the hub in the example.



**Figure 11: Native VLAN**

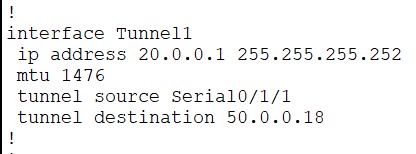
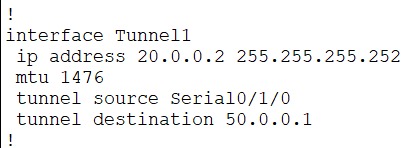
* 1. **VPN:**

Virtual private networks (VPNs) to create end-to-end private network connections.

A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network.

A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.

In VPN site-to-site use GRE protocol between HQ and Branch Amman.

****

**Figure 12: VPN**

# Chapter 5: Results and Discussion

**Results:**

The network infrastructure has the many phases: availability, Security, Speed, connectivity, redundancy, scalability and performance which will give the Company the full ability to interact with each other fast and securely.

**Strengths and weaknesses of the solution:**

The network infrastructure design provides the necessary requirements for the full operation of the company with high speed and secure process, and it gives the ability to expand it in time which will make the company grow as comfortable as it needs, but it needs more time to implement and maintain it.

# Chapter 6: Economical, Cost and Environment

**Relevant Environmental Considerations:**

In our project we used the simulation which provide the necessary environment for the infrastructure but in real world implementation many Environmental Considerations should be considered like temperature and humidity.

**Preliminary Cost Estimation and Justification**

Since our project is a simulation project and we did not use any tangible equipment, so there is no any cost except the time and effort cost, but if it is going to be deployed in real world it will need a whole economical plan.

Table slandered :

|  |  |  |
| --- | --- | --- |
| **No.** | **Description** | **Price (USD)** |
| 1 | Catalyst 2960 24 Port Ethernet 10/100 | 1500 |
| 2 | Catalyst 2960 48 Port Ethernet 10/100 | 2500 |
| 3 | Catalyst 3560 24 Port Ethernet 10/100 | 4000 |
| 4 | Catalyst 3650 48 Port Ethernet 10/100 | 6000 |
| 5 | ISR 4331 Router with 2 Port 1GB per port | 1500 |
| 6 | High Wan Interface Card | 1000 |
| 7 | Workstation for service (Syslog, NTP, DHCP, etc.) | 600 |
| 8 | WLC 3504 | 5000 |
| 9 | Access Point AP(LAP) | 300 |
| 10 | Wireless adapter | 50 |

**Table Cost:**

|  |  |  |
| --- | --- | --- |
| **Description** |  | **Price (USD)** |
| Catalyst 2960 24 Port Ethernet 10/100 | 10 | 15000 |
| Catalyst 2960 48 Port Ethernet 10/100 | 0 | 0 |
| Catalyst 3560 24 Port Ethernet 10/100 | 1 | 4000 |
| Catalyst 3650 48 Port Ethernet 10/100 | 0 | 6000 |
| ISR 4331 Router with 2 Port 1GB per port | 11 | 16500 |
| High Wan Interface Card | 12 | 12000 |
| Workstation for service (Syslog, NTP, DHCP, etc.) | 1 | 600 |
| WLC 3504 | 1 | 5000 |
| Access Point AP(LAP) | 1 | 300 |
| Wireless adapter | 2 | 100 |
| Total |  | 59500 |

# Chapter 7: Project Management

**Time Management:**

|  |  |
| --- | --- |
| Task | Time |
| Planning | 5-6/9/2022 |
| Assign Roles to Team | 7/9/2022 |
| Research | 8/9/2022 |
| Design | 9-10/9/2022 |
| Implementation and Configuration | 11-15/9/2022 |
| Documentation | 16-17/9/2022 |
| Troubleshooting | 18-20/9/2022 |
| Presentation | 21/9/2022 |

**Quality Management**

We used the latest version of packet tracer and assigned the best devices for the project.

**Risk Management**

We tried to manage the risks as possible, by saving a couple of copies of the project each time we added something.

**Project Procurement**

We did not have any procurement, we used free simulation tool.

# Chapter 8: Conclusion and Future Work

**Further future work someone should do to make the solution better.**

Add more technological solutions and protocols and adopt new ways to make the system more fast and reliable and secure.

**Lessons learned.**

The more we learn the more we rise with our self’s and the community.