

Final Project/ Technical Report

IIS Company

Instructor: Israa Saadeh

Course: CCNA

Mahmoud Saleh Sabobeh

[3180603002@htu.edu.jo](mailto:3180603002@htu.edu.jo)  
[mahmoud.sabobeh@hotmail.com](mailto:mahmoud.sabobeh@hotmail.com)

Training Period:   
27-Sep-2022 to 30-Dec-2022

Keywords:

OSPF, LAN, SSH, RSA, VLAN, DHCP, Ether Channel, VPN, Syslog, NTP, BPDU, IPv4, Wireless, NAT, Port Security, HSPR, DTP, SVI, Router on Stick, and others.

**ABSTRACT**

In today's world, networking have become extremely necessary for providing Communication and other services. Computer networks play a critical role in these services by communicating, administrating, automating, and processing information from one location to another. Hence most businesses and organizations consider computer networks to be the foundation of proper operation. Cisco packet tracer is used as a network simulator tool in this report to simulate and design a company's network project. The report discussed the interconnection between routers, switches, and other components in a data communication network and how they are programmed and configured.

**Introduction**

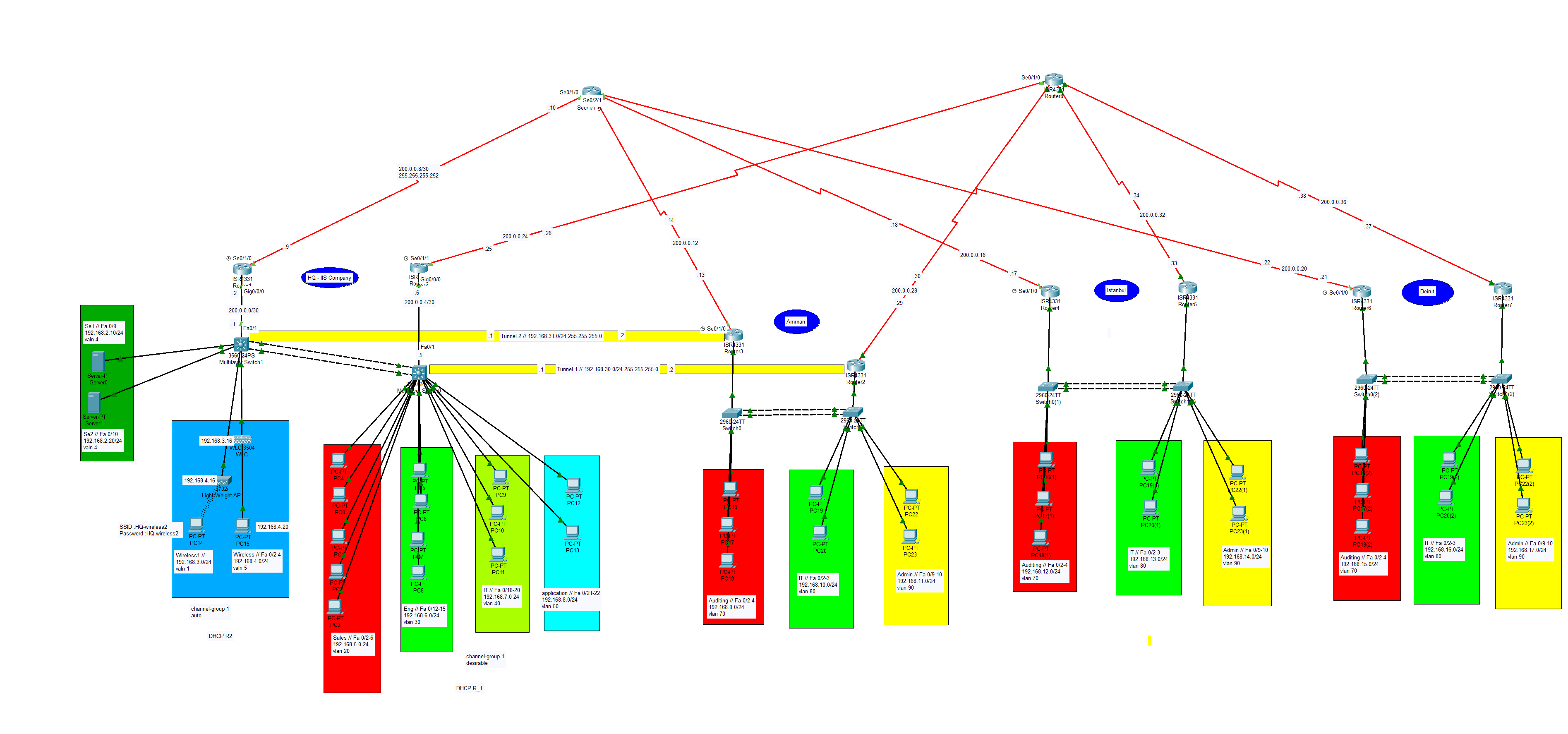
A computer network can be defined as a number of computer systems and other computing hardware devices that are linked together for sharing information in the form of messages, files, and data bases in an organization that may be in one building or spread over a large campus. In addition to that, the networks decrease cost, time, and effort and thereby increase productivity. Network connections: devices are connected together by using any type of communication medium, such as a copper coaxial cable, a twisted pair cable, a twisted pair cable, or wireless. In this project the network devices include PCs, NIM-2T, routers, multiplexers, switches, APs, WLC and others. Each one of these devices has various properties compared to others in terms of jobbing, security, and application. In this project, I will use Cisco Packet Tracer is a multi-tasking network simulation software that can be used to perform and analyze various network activities, such as the implementation of different topologies, the selection of the optimum path based on various routing algorithms, the creation of appropriate servers, subnetting, and the analysis of various network configuration and troubleshooting commands.

**Project Network Scenario**

In this technical report, I am a senior network engineer at IIS Company. The company is applying new infrastructure deployments, and new devices are needed to be brought to the Head Quarter (HQ) site and remote sites; they have three branches (Amman, Istanbul, and Beirut). It was requested to build a topology that could achieve full connectivity between the clients in HQ and all branch sites. It is also important not to exceed the budget for the company project when establishing a secure connection between the main site and the branch Amman site via VPN site-to-site connection.

# Requirements:

* High availability & redundancy.
* Restrict access using ACL (Security).
* Stick to budget. (85.000 JD)
* Scalability and easy of management.
* Creating VLANs and secure them
* Creating DHCP and secure the Scope
* Implement Dynamic Routing Protocol. (OSPF)
* Configuring Ether Channel and Port Security.
* Applying ACL and VPN
* Gathering Syslog messages.
* Client in HQ can ping clients located in all Branches (Amman, Istanbul, and Beirut).



**VLANS**:

HQ:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vlan No. | Name | Switch | Interfaces | Networks (IP) | Subnet |
| 99 | Native |  |  |  |  |
| 10 | Management |  |  |  |  |
| 4 | Server | Multi\_HQ1 | Fa 0/9-10 | 192.168.2.0 | 255.255.255.0 |
| 1 | Wireless1 | Multi\_HQ1 |  | 192.168.3.0 | 255.255.255.0 |
| 5 | Wireless | Multi\_HQ1 | Fa 0/2-4 | 192.168.4.0 | 255.255.255.0 |
| 20 | Sales | Multi\_HQ2 | Fa 0/2-6 | 192.168.5.0 | 255.255.255.0 |
| 30 | Eng. | Multi\_HQ2 | Fa 0/12-15 | 192.168.6.0 | 255.255.255.0 |
| 40 | IT | Multi\_HQ2 | Fa 0/18-20 | 192.168.7.0 | 255.255.255.0 |
| 50 | Application | Multi\_HQ2 | Fa 0/21-22 | 192.168.8.0 | 255.255.255.0 |

Amman:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vlan No. | Name | Switch | Interfaces | Networks (IP) | Subnet |
| 99 | Native |  |  |  |  |
| 10 | Management |  |  |  |  |
| 70 | Auditing | Sw1-Amman | Fa 0/2-3 | 192.168.9.0 | 255.255.255.0 |
| 80 | IT | Sw2- Amman | Fa 0/2-4 | 192.168.10.0 | 255.255.255.0 |
| 90 | Admin | Sw2- Amman | Fa 0/9-10 | 192.168.11.0 | 255.255.255.0 |

Istanbul:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vlan No. | Name | Switch | Interfaces | Networks (IP) | Subnet |
| 99 | Native |  |  |  |  |
| 10 | Management |  |  |  |  |
| 70 | Auditing | Sw1-Istanbul | Fa 0/2-3 | 192.168.12.0 | 255.255.255.0 |
| 80 | IT | Sw2-Istanbul | Fa 0/2-4 | 192.168.13.0 | 255.255.255.0 |
| 90 | Admin | Sw2-Istanbul | Fa 0/9-10 | 192.168.14.0 | 255.255.255.0 |

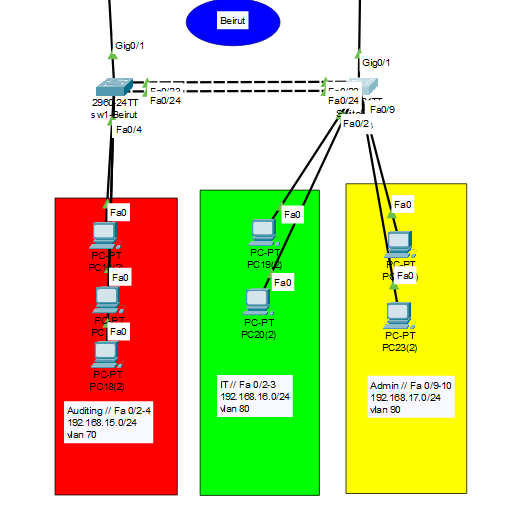
Beirut:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vlan No. | Name | Switch | Interfaces | Networks (IP) | Subnet |
| 99 | Native |  |  |  |  |
| 10 | Management |  |  |  |  |
| 70 | Auditing | Sw1-Beirut | Fa 0/2-3 | 192.168.15.0 | 255.255.255.0 |
| 80 | IT | Sw2- Beirut | Fa 0/2-4 | 192.168.16.0 | 255.255.255.0 |
| 90 | Admin | Sw2-Beirut | Fa 0/9-10 | 192.168.17.0 | 255.255.255.0 |

Note:

All the required things have been activated on the entire network/devices. In this report, I will review the ideas that have been applied to the network.

Switching Configuration:



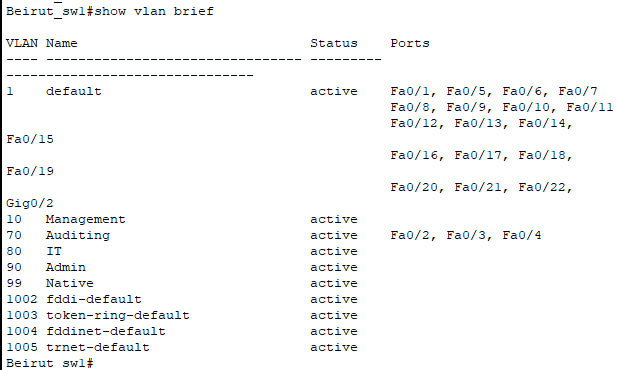
In the beginning set the name all devices (Routers, Switches, and Multilayers).  
And each of the **VLANs** is defined as a Name. And each of the VLANs token a Network.



**Both switches divided into VLANs and map the VLAN with the client ports:**

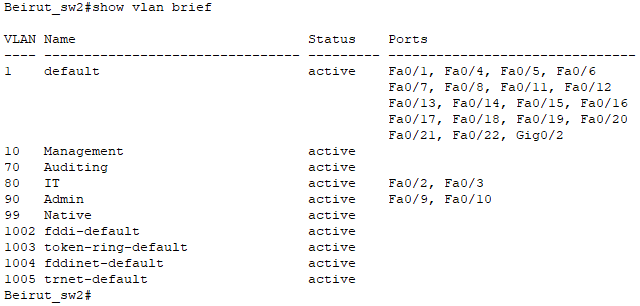
* **Beirut\_sw1**

Interfaces fa0/2, fa0/3, and fa0/4 specified to VLAN 70



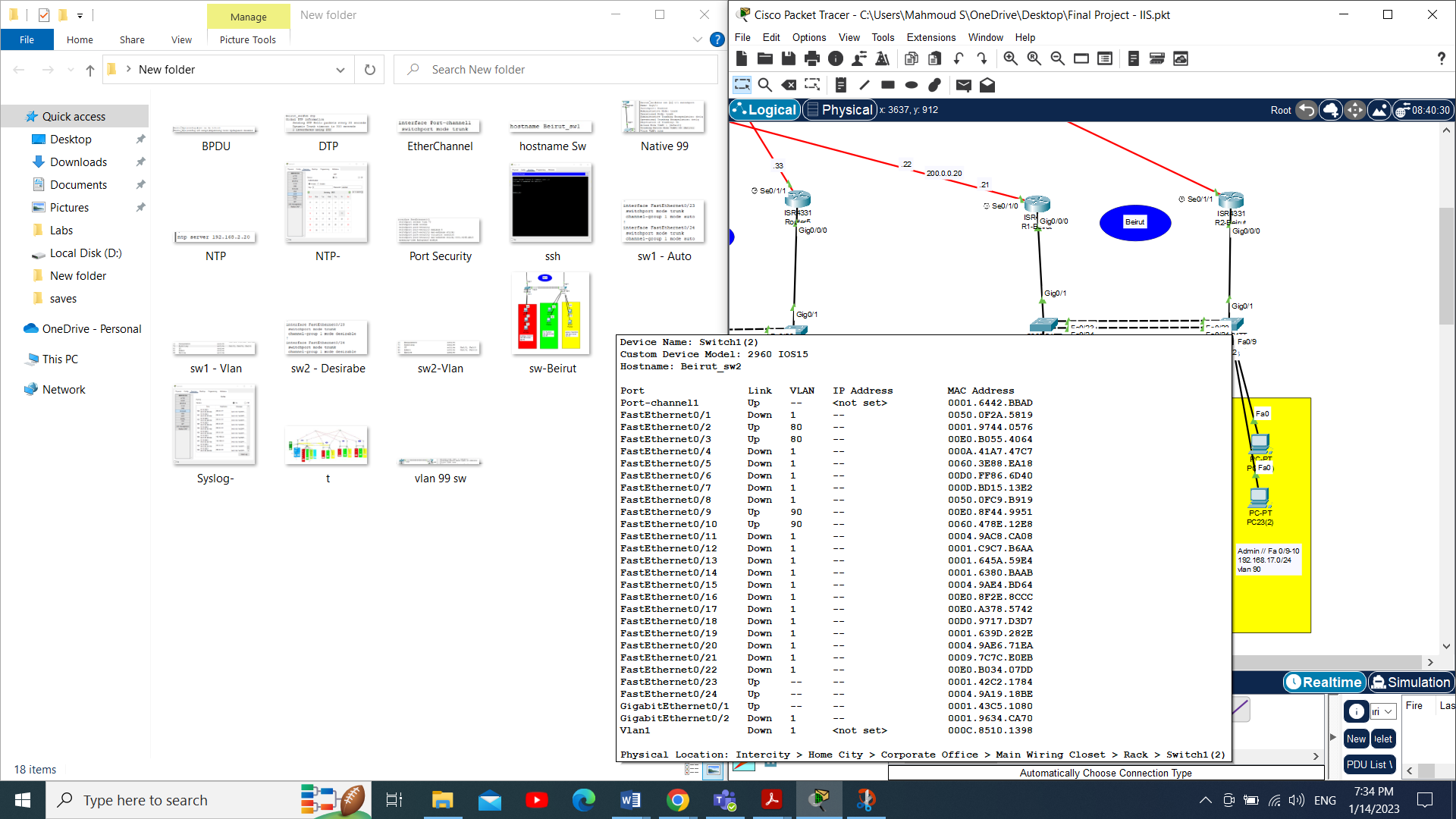
* **Beirut\_sw2 :**

Interfaces fa0/2 and fa0/3 specified to VLAN 80, fa0/9 and fa0/10 to VLAN 90.

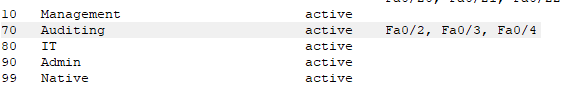


**Each VLAN have a redundant Gateway for their clients.**

* Ex: sw2-Beirut / VLAN 80 … Available from fa0/4 to fa0/8.



**Create all VLANs on both Switches.**



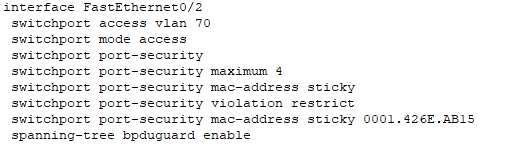
Sw2-Beirut - VLANs



Sw2-Beirut - VLANs

**Apply Port Security on both switches on an Interfaces UP.**

* Maximum mac address learned 4.
* Learned the mac address sticky.



Port Security

**Configure NTP and Syslog on both switches.  
Note:** applied this Command on alldevices (Routers, Switches, and Multilayers).

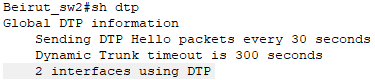
C:\Users\Mahmoud S\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Syslog.png



NTP Syslog

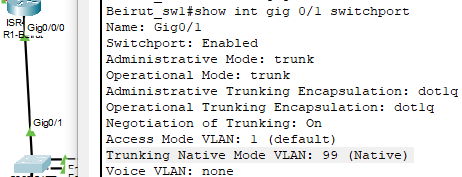
**Configure Dynamic Trunking Protocol (DTP) on ports per switch.**

* Apply On the interfaces outside from switch to Routers



DTP

**Apply Native VLAN 99 on All Trunk mode ports.**



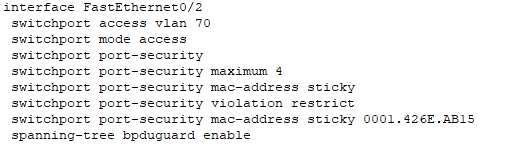
Native VLAN- 1



Native VLAN- 2

**Disable BPDU messages on all access ports.**

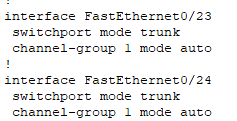
* Ports of the Clients



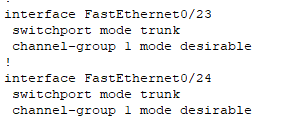
BPDU 1

**Configured EtherChannel between switches**

* Fa 0/23 and Fa 0/24
* pag-p (sw2-Beirut as a desirable and sw1-Beirut as an auto)



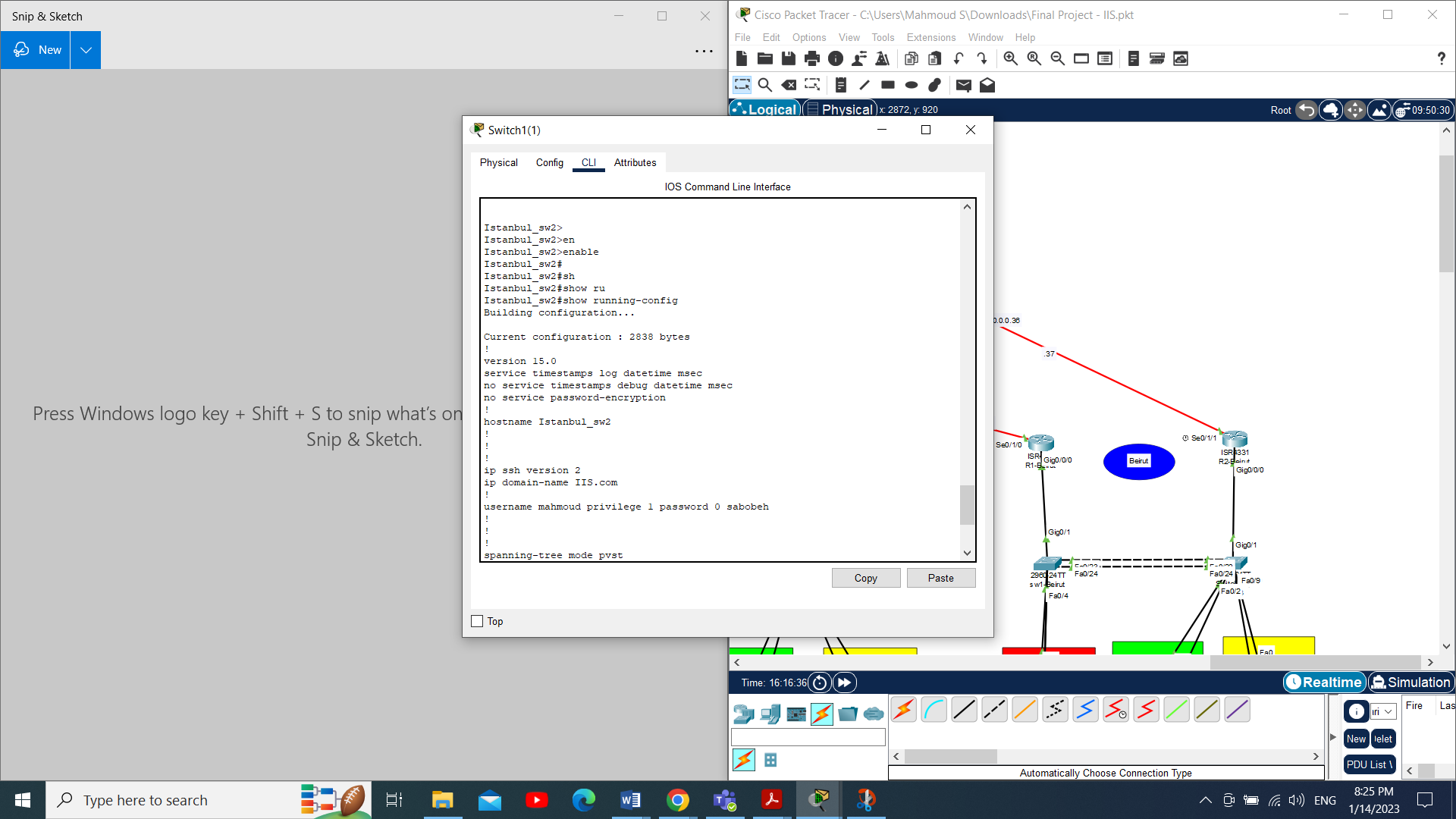
Ether Channel 1



Ether Channel 2

**Access both switches with only SSH.**

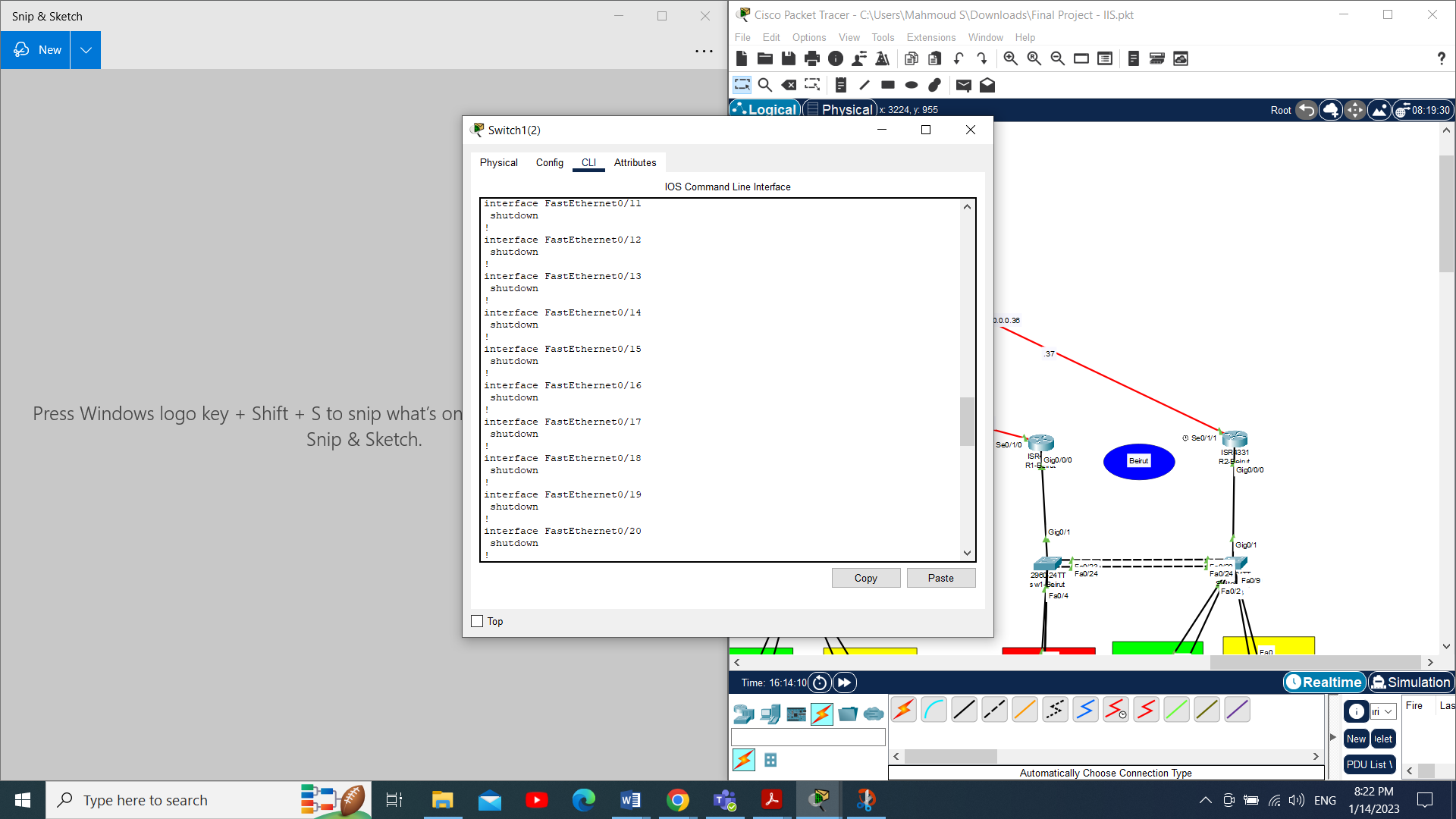
* Use RSA with 2048.



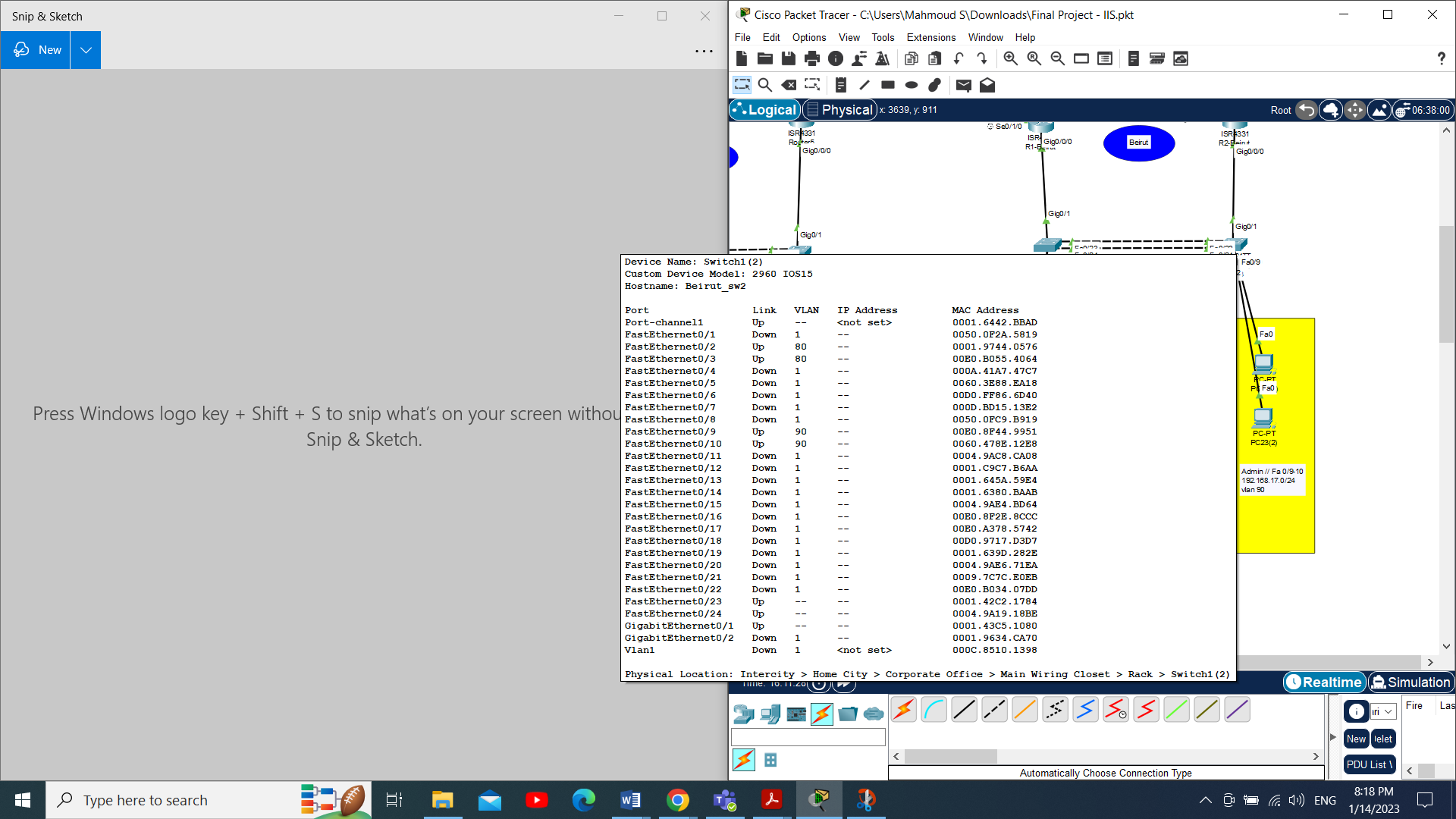
**All unused ports need to be shutdown.**

Interface Fa 0/1

Shutdown



Unused 1



Unused 2

Configuration Router:

Network with ISP – Standby

|  |  |  |
| --- | --- | --- |
| Network | Subnet | Wide |
| 200.0.0.0 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.8 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.12 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.16 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.20 | 255.255.255.252 | 0.0.0.3 |

Network with ISP - Active

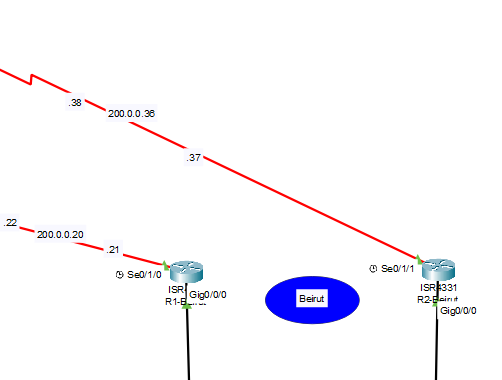
|  |  |  |
| --- | --- | --- |
| Network | Subnet | Wide |
| 200.0.0.4 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.24 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.28 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.32 | 255.255.255.252 | 0.0.0.3 |
| 200.0.0.36 | 255.255.255.252 | 0.0.0.3 |

IP Router – Standby:

|  |  |  |
| --- | --- | --- |
| Name Router | IP | Interfaces |
| ISP\_Standby | 200.0.0.10 | Se0/1/0 |
| HQ1 | 200.0.0.9 | Se0/1/0 |
| HQ1 | 200.0.0.2 | Gig0/0/0 |
| Multi\_HQ1 | 200.0.0.1 | Fa0/1 |
| ISP\_Standby | 200.0.0.14 | Se0/1/1 |
| Amman\_R1 | 200.0.0.13 | Se0/1/0 |
| ISP\_Standby | 200.0.0.18 | Se0/2/0 |
| Istanbul\_R1 | 200.0.0.17 | Se0/1/0 |
| ISP\_Standby | 200.0.0.22 | Se0/2/1 |
| Beirut\_R1 | 200.0.0.21 | Se0/1/0 |

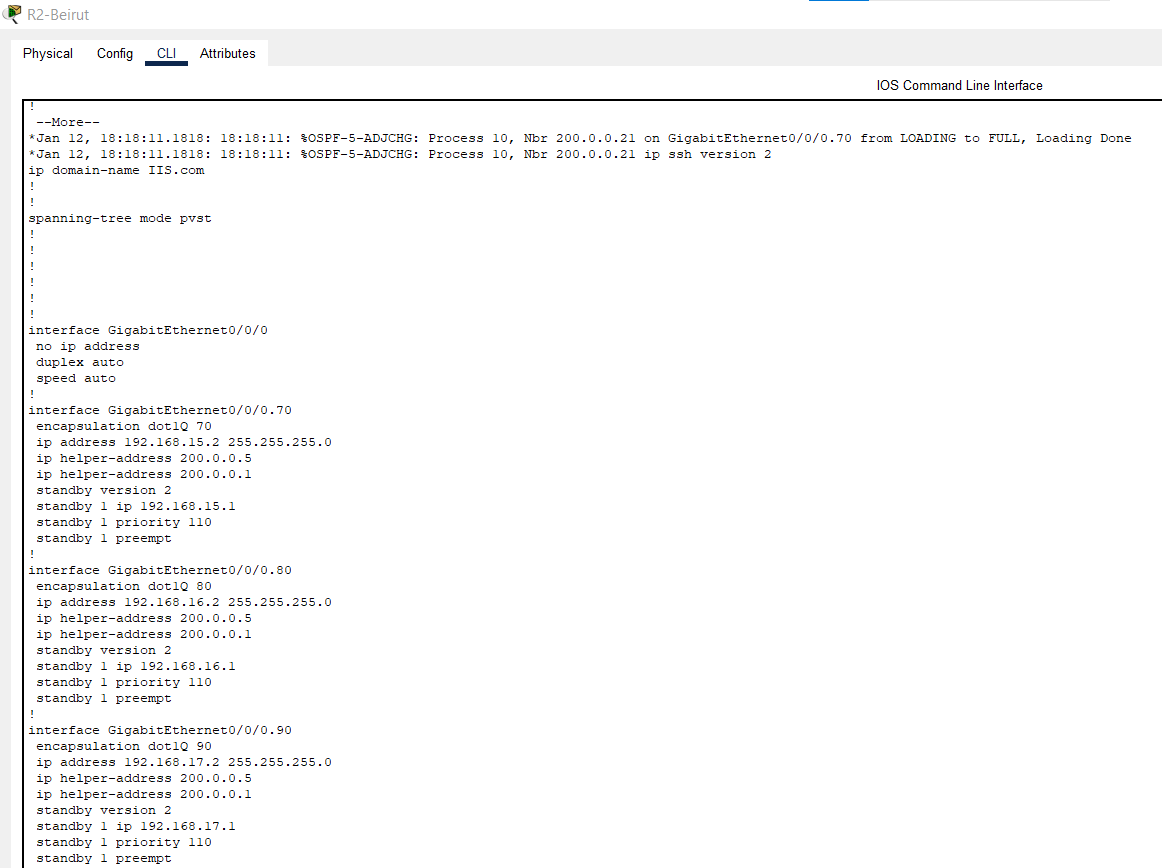
IP Router – Active:

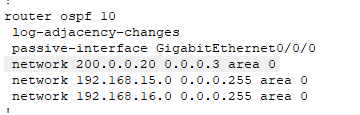
|  |  |  |
| --- | --- | --- |
| Name Router | IP | Interfaces |
| ISP\_Active | 200.0.0.26 | Se0/1/0 |
| HQ2 | 200.0.0.25 | Se0/1/1 |
| HQ2 | 200.0.0.4 | Gig0/0/0 |
| Multi\_HQ2 | 200.0.0.5 | Fa0/1 |
| ISP\_ Active | 200.0.0.30 | Se0/1/1 |
| Amman\_R2 | 200.0.0.29 | Se0/1/1 |
| ISP\_ Active | 200.0.0.34 | Se0/2/0 |
| Istanbul\_R2 | 200.0.0.33 | Se0/1/1 |
| ISP\_ Active | 200.0.0.38 | Se0/2/1 |
| Beirut\_R2 | 200.0.0.37 | Se0/1/1 |



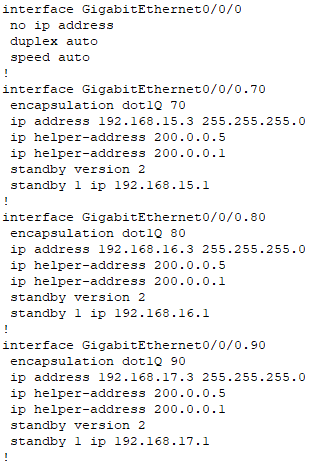
* **Sub-Interfaces , HSRP, IP Helper (DHCP) :**

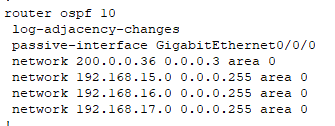
R2: **Active**





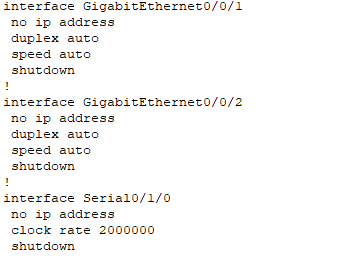
R2: **Standby**

: 



Note: Configure the **OSPF** on All Networks - Active and Standby (Redundancy).

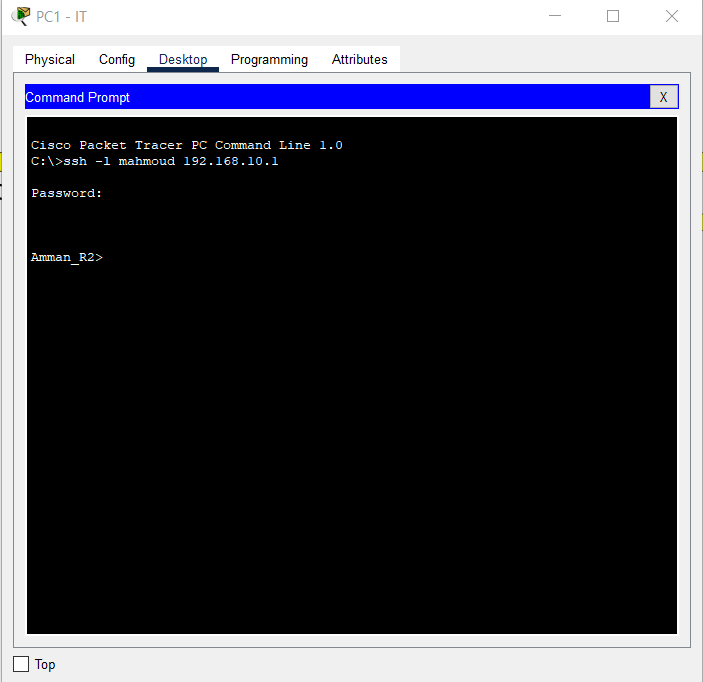
* **All Unused ports need to be shutdown.**

****

Note: Applied **Shutdown** in Unused portson all devices **-** Active and Standby (Redundancy).

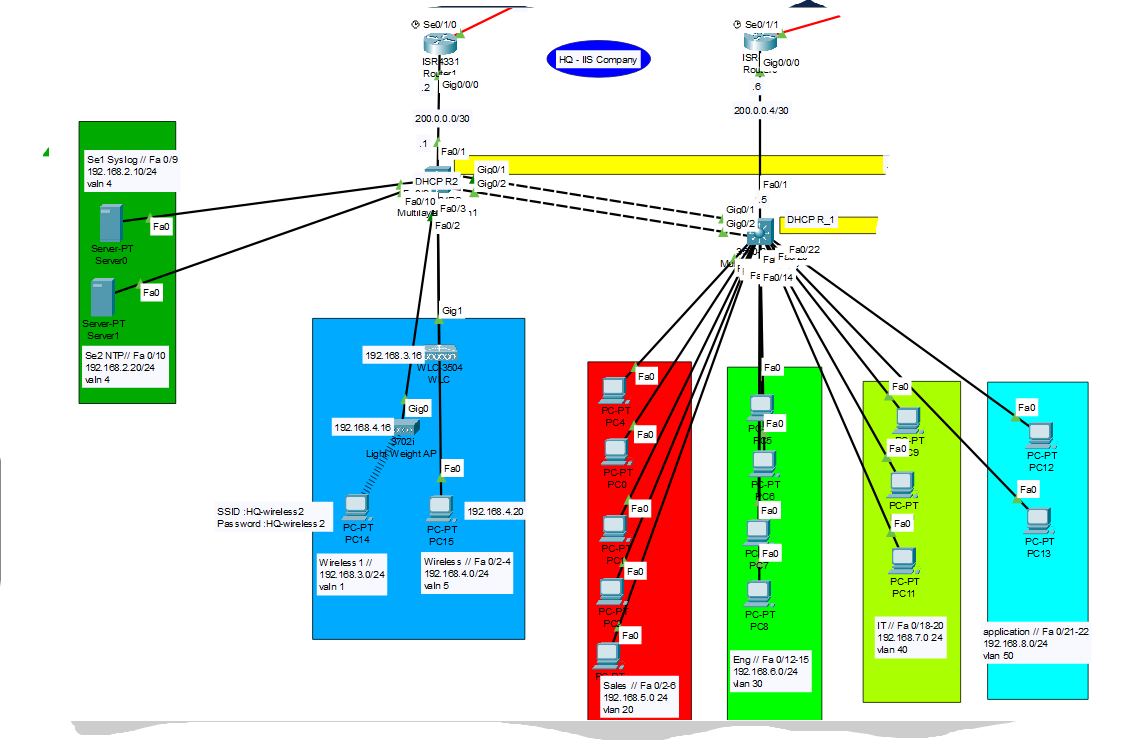
**Access all routers SSH.**

* RSA with 2048.



Note: Applied **SSH** in all devices **-** Active and Standby (Redundancy).

**Head Quarter (HQ):**

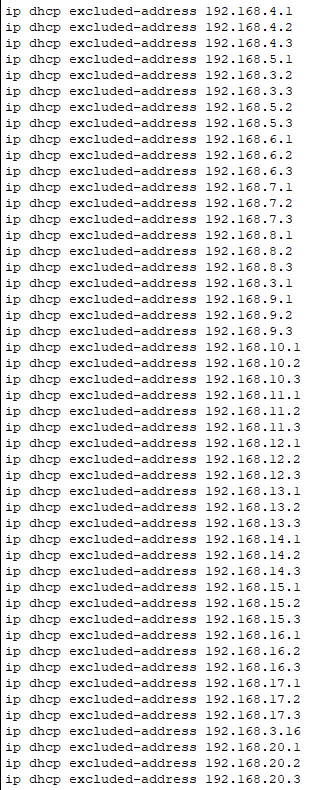
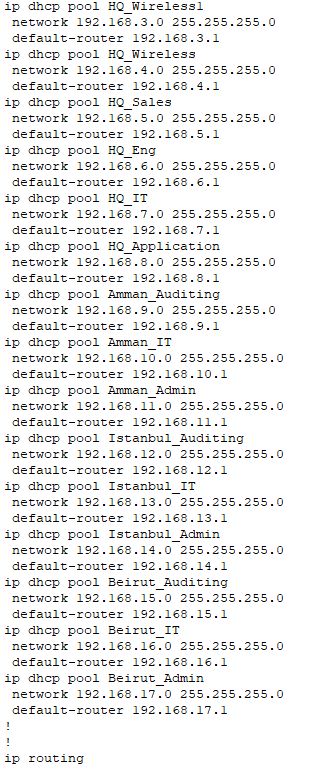


Configured:

* HSRP: Multi\_HQ1 (Standby) and Multi\_HQ2 (Active)
* OSPF.
* DHSP.
* Port Security.
* Wireless.
* Servers.
* SVI.
* VLAN.
* VPN.
* And Others

**DHCP Router on:**

* Multi\_HQ1 (as Redundancy)
* Multi\_HQ2 (as Active)

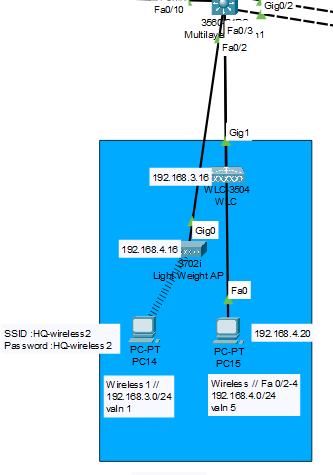


**IP Helper in All Routers:**

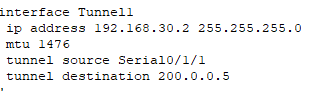
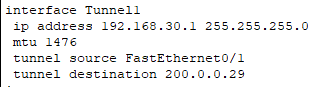
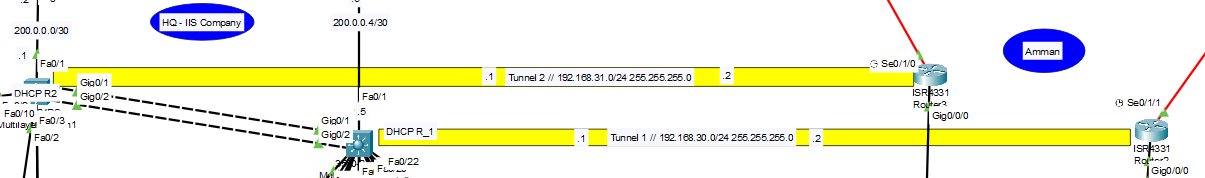


**Applied Wireless:**

* + Deploy a WLC one LAP for wireless clients in HQ.
  + Configure the WLC username “ADMIN” and password “Admin123”.
  + Configure one with SSID and name it HQ-wireless and map it to VLAN 5.



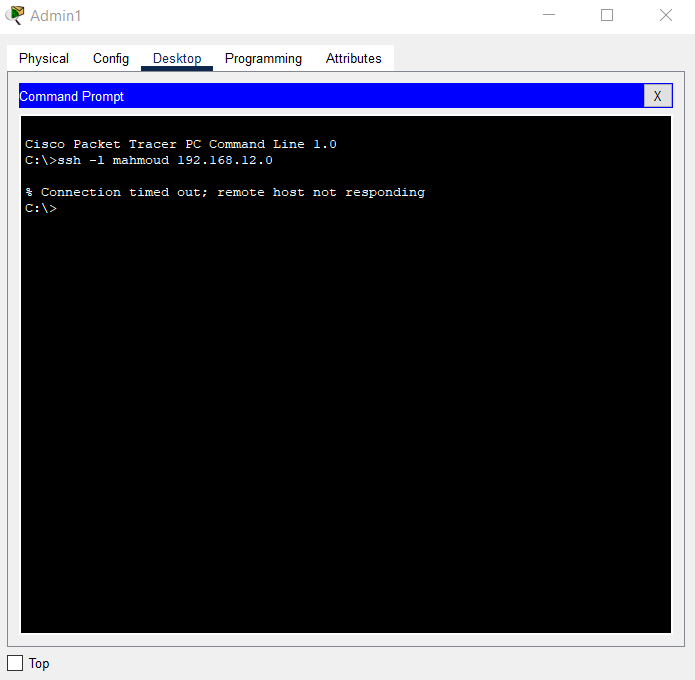
**VPN: (Two Tunnel)**



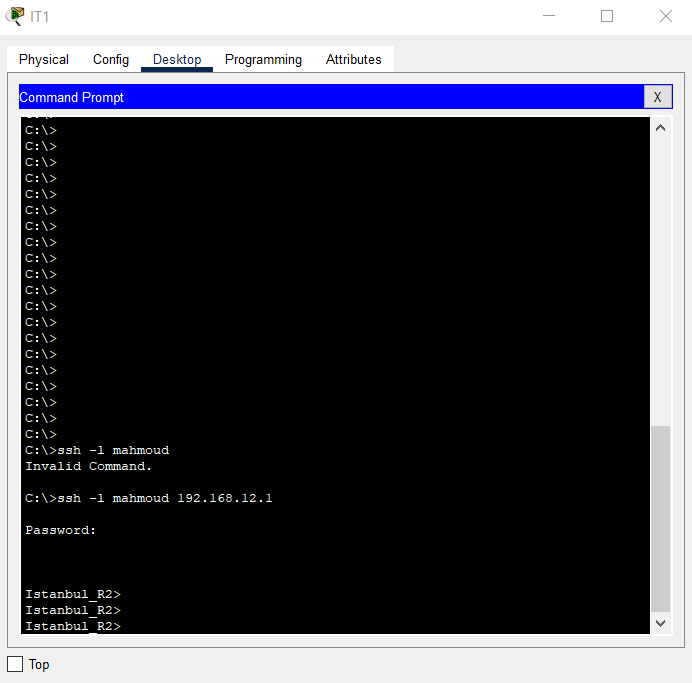
* **Only IT VLAN can SSH network devices in Branch Istanbul: (ACL with SSH)**

Network Auditing: 192.168.12.0

Network IT: 192.168.13.0  
Network Admin: 192.168.14.0



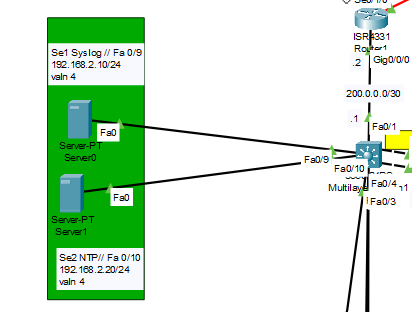
Others Vlan



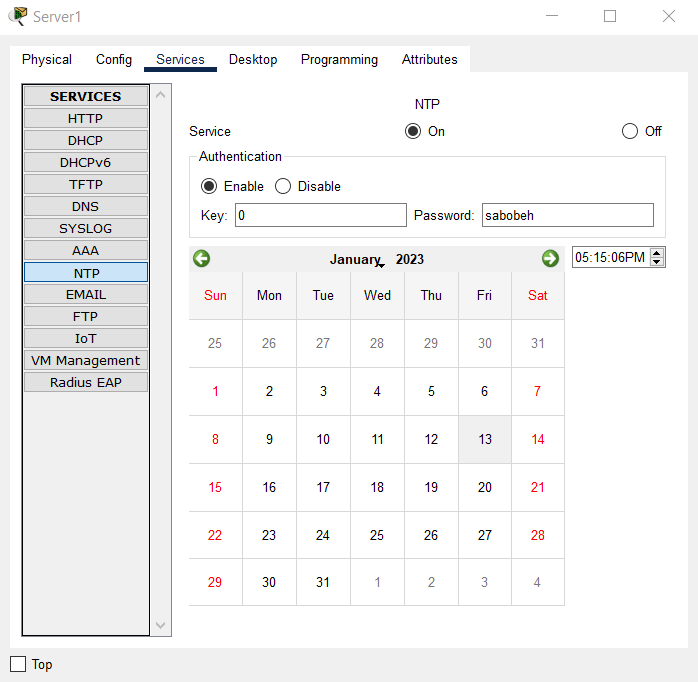
IT - SSH 1

**Server Configuration:**

* **NTP and Syslog: Applied in All Devices**



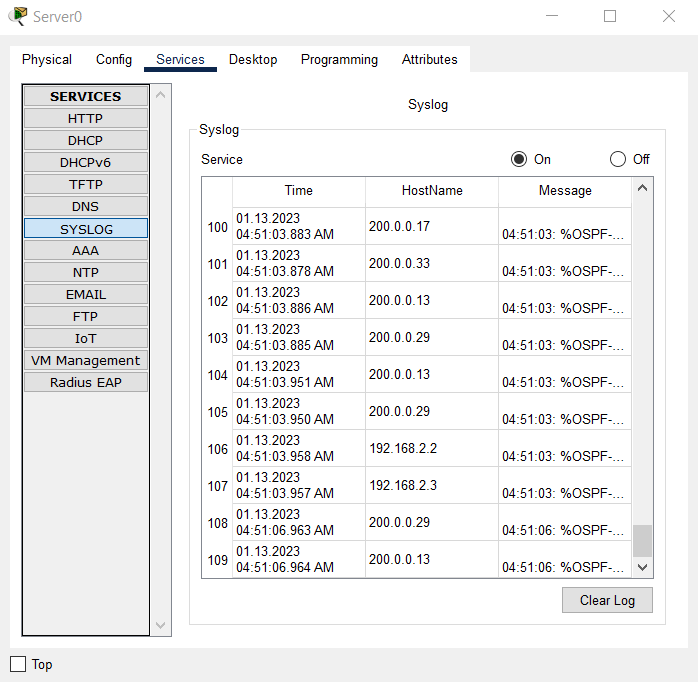
**NTP Server:**



On all devices



**Syslog Server:**



On all devices



Expected amount (Available): 85.000 USD

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Pieces** | **Price (USD)/ 1 Piece** | **Total** |
| 6 | 2960 Switch 24 Ports /2 GB | 2500 | 15.000 |
| 2 | 3560 Multilayer Switch | 3500 | 7.000 |
| 10 | ISR4331 Router with 2 Port 1GB per port | 1500 | 15.000 |
| 12 | High Wan Interface Card | 1000 | 12.000 |
| 2 | Workstation for service (Syslog, NTP) | 600 | 1.200 |
| 1 | WLC 3504 | 5000 | 5000 |
| 1 | Light weight AP(LAP) | 300 | 300 |
| 1 | Wireless adapter | 50 | 50 |
|  |  |  | **Total : 55.550 USD** |

The following illustrates the tools used to complete this project.

* Packet Tracer.
* MS Teams
* YouTube
* Office (Word, PowerPoint)
* Quillbut and Google Translate

Testing:

through Command Prompt :

* Ping “ip”
* **tracert “ip”**
* SSH –l “name” “ip”
* Ipconfig “ip”
* And Others …

Future Works:

* Only IT VLAN can access Application VLAN in HQ
* Apply NAT by using PAT.s
* Use IPv6 as redundant IP with IPv4 in your Address design.

CONCLUSION

The packet tracer is used to implement the network of the project and clarity the conception of the VLANs, DHCP, OSPF, NTP and Syslog server, and router configurations. Networking devices are expensive so the packet tracer is easy and best to implement structure of the network before implementing it on the real ground.