**Cisco Meraki Centralized WLC on a 3-Tier Campus LAN Architecture**

**Table of Contents**

[Abstract 3](#_Toc129271079)

[Introduction 5](#_Toc129271080)

[Method and Equipment 5](#_Toc129271081)

[Hostname Configuration 5](#_Toc129271082)

[IP subnet Configuration 6](#_Toc129271083)

[OSPF Configuration 6](#_Toc129271084)

[Service Provider Static IP Route Configuration 7](#_Toc129271085)

[VLAN, DHCP & HSRP Configuration 7](#_Toc129271086)

[Meraki Server Configuration 10](#_Toc129271087)

[Meraki-MX65W Security Appliance Configuration 12](#_Toc129271088)

[Wireless End Host Configuration 21](#_Toc129271089)

[Verification & Discussion 22](#_Toc129271090)

# Abstract

Using the Packet tracer software, I successfully implemented a centralized cloud based WLC on a 3-Tier LAN architecture, using the Cisco Meraki server and Meraki-MX65W security appliance. This is a continuation of work done on the project titled as “[DHCP configuration in a 3-Tier Campus LAN Architecture](https://github.com/ascotlan/DHCP-configuration-in-a-3-Tier-Campus-LAN-Architecture).” After configuring a DHCP pool for the Meraki Security Appliance, I created redundant virtual interfaces at the distribution layer for VLAN 32, for the Meraki appliance. Inter-VLAN routing was enabled and a route for all layer 3 traffic to/from the VLAN 32 virtual interface was also configured using OSPF. A default route to the service provider gateway was manually configured and thus a route to/from the Meraki server was implemented. Once the Meraki security appliance established a secure tunnel connection to the Meraki server, I successfully configured the appliance via the Meraki dashboard. LAN and WAN connectivity was then achieved for all wireless end hosts on the WLAN implemented on the Meraki Security Appliance.

Diagram, schematic

Description automatically generated

# Introduction

The objective is to implement a WLAN using a centralized cloud-based Meraki server and corresponding Meraki-MX65W security appliance. This will be executed using a 3-Tier Campus LAN architecture with DHCP that was previously configured in the project titled as “[DHCP configuration in a 3-Tier Campus LAN Architecture](https://github.com/ascotlan/DHCP-configuration-in-a-3-Tier-Campus-LAN-Architecture).” The objective will be achieved by first configuring hostnames on the additional network devices needed. Secondly, configuring an IP subnet for the WAN edge interfaces and the service provider interfaces. Thirdly, OSPF will be configured on the WAN edge interfaces, while static routes with load balancing will be implemented on the Service provider interfaces. Then an additional VLAN 32 for the Meraki appliance will be added to the VTP server already configured on ACC-SW1, and redundant virtual interfaces for VLAN 32 will be configured at the distribution layer using HSRP. Note that the IP addresses for the Virtual interfaces will fall within the 172.0.0.0/8 network that was pre-configured in the OSPF configuration. Next a DHCP pool for VLAN 32 will be set up on the DHCP server at 172.4.0.100. And finally, the Meraki Appliance will be configured via the Meraki dashboard on the Admin-Laptop connected to the Meraki security appliance via fast ethernet.

# Method and Equipment

## Hostname Configuration

### SP1

Router>en

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname SP1

SP1(config)#exit

SP1#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

### SW1

Switch>en

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname SW1

SW1(config)#int range fa0/3-24

SW1(config-if-range)#shutdown

SW1(config-if-range)#int g0/2

SW1(config-if)#shutdown

SW1#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

## IP subnet Configuration

### SP1

SP1#config t

Enter configuration commands, one per line. End with CNTL/Z.

SP1(config)#int g0/0

SP1(config-if)#ip address 203.113.0.1 255.255.255.252

SP1(config-if)#int g0/0

SP1(config-if)#no shutdown

!

SP1(config)#int g0/1

SP1(config-if)#ip address 200.101.0.1 255.255.255.0

SP1(config-if)#no shutdown

### R1

R1>en

R1#config t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#int g0/1

R1(config-if)#ip address 200.101.0.2 255.255.255.0

R1(config-if)#no shutdown

### R2

R2>en

R2#config t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#int g0/1

R2(config-if)#ip address 200.101.0.3 255.255.255.0

R2(config-if)#no shutdown

## OSPF Configuration

### R1

R1(config)#router ospf 1

R1(config-router)#network 200.101.0.0 0.0.0.255 area 0

R1(config-router)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 200.101.0.1

R1(config)#router ospf 1

R1(config-router)#default-information originate

### R2

R2(config)#router ospf 1

R2(config-router)#network 200.101.0.0 0.0.0.255 area 0

R2(config-router)#exit

R2(config)#ip route 0.0.0.0 0.0.0.0 200.101.0.1

## Service Provider Static IP Route Configuration

### SP1

SP1>en

SP1#config t

Enter configuration commands, one per line. End with CNTL/Z.

SP1(config)#ip route 172.0.0.0 255.0.0.0 200.101.0.2

SP1(config)#ip route 172.0.0.0 255.0.0.0 200.101.0.3

## VLAN, DHCP & HSRP Configuration

### ACC-SW1

ACC-SW1#config t

ACC-SW1(config)#vlan 32

ACC-SW1(config-vlan)#name Meraki

### DIS-SW1

DIS-SW1>en

DIS-SW1#config t

Enter configuration commands, one per line. End with CNTL/Z.

DIS-SW1(config)#vlan 32

DIS-SW1(config-vlan)#name Meraki

DIS-SW1(config-vlan)#exit

DIS-SW1(config)#int vlan 32

DIS-SW1(config-if)#ip address 172.32.0.2 255.255.0.0

DIS-SW1(config-if)#standby 32 ip 172.32.0.1

DIS-SW1(config-if)#standby 32 priority 110

DIS-SW1(config-if)#standy 32 preempt

%LINK-5-CHANGED: Interface Vlan32, changed state to up

DIS-SW1(config-if)#ip helper-address 172.4.0.100

### DIS-SW2

DIS-SW2>en

DIS-SW2#config t

Enter configuration commands, one per line. End with CNTL/Z.

DIS-SW2(config)#vlan 32

DIS-SW2(config-vlan)#name Meraki

DIS-SW2(config-vlan)#exit

DIS-SW2(config)#int vlan 32

DIS-SW2(config-if)#ip address 172.32.0.3 255.255.0.0

DIS-SW2(config-if)#standby 32 ip 172.32.0.1

DIS-SW2(config-if)#standby 32 priority 90

%LINK-5-CHANGED: Interface Vlan32, changed state to up

DIS-SW2(config-if)#ip helper-address 172.4.0.100

### ACC-SW3

ACC-SW3>en

ACC-SW3#config t

Enter configuration commands, one per line. End with CNTL/Z.

ACC-SW3(config)#int f0/2

ACC-SW3(config-if)#switchport mode access

ACC-SW3(config-if)#switchport access vlan 32

ACC-SW3(config-if)#no shutdown

The security appliance in VLAN 32 receives it IP address on the internet interface from the serverPool configured on the DHCP server at 172.4.0.100.

Graphical user interface, application

Description automatically generated

Figure -DHCP pool on DHCP server (172.4.0.100) for Meraki Appliances on VLAN 32

## Meraki Server Configuration

The Meraki server is on the subnet 203.113.0.0/30 as seen in figure 3 and is assigned the IP 203.113.0.2 with a default gateway of 203.113.0.1 as seen in figure 2.

Graphical user interface, text, application, email

Description automatically generated

Figure -Meraki server gateway configuration

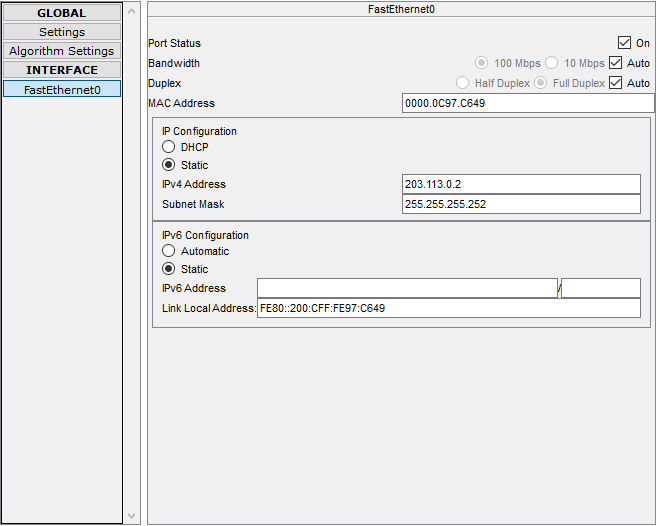


Figure - Meraki server fast ethernet interface configuration

## Meraki-MX65W Security Appliance Configuration

After the internet 1 interface was connected to the access layer switch ACC-SW3, the Meraki-MX65W security appliance was powered up, the serial number of the device was noted, as it is essential for further configuration of the device.

Graphical user interface, text, application, email

Description automatically generated

Figure -Meraki Appliance GUI shows the appliance serial number that is used by the Admin to configure the appliance

The Meraki security appliance was then connected to the Admin laptop via fast ethernet, and the DHCP server on the security appliance, operating in NAT mode, assigned an IP to the Admin laptop on a new subnet 192.168.0.0/24 with default gateway 192.168.0.1, as shown in figure 5. Note that the appliance itself received an IP from the DHCP server pool configured on the DHCP server at 172.4.0.100, as seen in figure 1. This was essential for the appliance to have a route to the Meraki server.

Graphical user interface, text, application, email

Description automatically generated

Figure -The Admin end host is set for DHCP and the received gateway is used for further configuration

The Meraki Security Appliance configuration menu was accessed via the web browser on the Admin laptop. The serial number of the appliance is entered as the User Name while the password field is left blank. The address of the configuration page is the default gateway on the appliance, as seen in figure 6.

Graphical user interface

Description automatically generated

Figure -The web browser on the Admin end host is used to connect the Meraki appliance using the Appliance serial number as the User Name and the Password field is left blank

Once logged in to the configuration page, the MAC address of the security appliance is noted for further configuration, as shown in figure 7.

Graphical user interface, text, application

Description automatically generated

Figure -The Meraki Appliance MAC address on the connection page is used for further configuration

The uplink interface i.e. Internet 1 is configured as a direct connection with DHCP for IP assignment in this case. This is done on the configure page, as shown in figure 8.

Graphical user interface, application

Description automatically generated

Figure -The uplink used (Internet 1) is set to DHCP on the Uplink configuration page

After it is confirmed that the Security Appliance interface Internet 1 has received an IP address via DHCP, then the Meraki cloud based server dashboard can be accessed via its IP address of 203.113.0.2, as seen in figure 9.

Graphical user interface, application

Description automatically generated

Figure -The Meraki Dashboard is accessed via the web browser on the Admin end host using the Meraki server IP (<https://203.113.0.2>), then an account must be created

A user account was first created, as shown in figures 10. And once authenticated you enter the landing page of the Meraki Dashboard as seen in figure 11.

Graphical user interface, text, application

Description automatically generated

Figure -The account creation page

Graphical user interface, application, Word

Description automatically generated

Figure -Meraki Dashboard landing page where the Meraki Security Appliance device must be registered

The network name and network type are then set and a network is created as seen in figure 12.

Graphical user interface, text, application

Description automatically generated

Figure -Page where a network can be created

The Meraki devices on the network are then added to the network via the dashboard using the device serial number, model number, MAC address and the name of the network the device is to be added to, as shown in figure 13.

Graphical user interface, text, application, email

Description automatically generated

Figure -The Meraki Appliance serial number and MAC address must be entered at this point

SSID’s are then created for each wireless device. The SSID, security encryption is configured as seen in figure 14. In this case WPA2 +PSK is selected as the authentication and encryption scheme for the SSID, *Student*.

Graphical user interface, application

Description automatically generated

Figure -Under the wireless settings page an authentication and encryption method are configured

## Wireless End Host Configuration

Once the Security Appliance is configured from the Meraki dashboard, wireless clients can now be added to the network using one of the SSIDs created. Figure 15 shows the, *Student,* SSID created on the dashboard. Once the pre-shared key is entered for the connection with SSID*, Student*, a connection to the WLAN is secured, as seen in figure 16.

Graphical user interface, text, application

Description automatically generated

Figure -Student laptop wireless configuration GUI detecting the configured Students SSID

Graphical user interface

Description automatically generated with medium confidence

Figure -The Student wireless end host is now securely connect using WPA2+PSK

# Verification & Discussion

In the appliance status menu of the Meraki Dashboard, a live data status can be seen on the uplink and access ports on the device. Figure 17 shows that the uplink internet 1 and Gigabit ethernet access port 3 are now active. Port 3 is connected to the Admin laptop while the internet uplink connects to the access layer switch, ACC-SW3.

Graphical user interface, text, application, email

Description automatically generated

Figure -Appliance status on dashboard shows uplink and port 3 are now active

Using NAT, the gateway 192.168.0.1 is mapped to IP address 172.32.0.6 assigned via DHCP to the internet 1 port. The Security Appliance DHCP sever assigns Student-Laptop1 an IP on the 192.168.0.0/24 subnet, as seen in figure 18. The wireless end hosts, including Student-Laptop1 now have two way connectivity to the service provide gateway of 200.101.0.1, as shown in figure 19. The wireless hosts also have access to networked resources on the Eng and CompSci VLANs, 30 and 31 repsctively. This is shown in figure 20.

Text

Description automatically generated

Figure -IP configuration on Student-Laptop 1

Text

Description automatically generated

Figure -Student-Laptop 1 has two connectivity to the service provider gateway

Text

Description automatically generated

Figure -Student-Laptop1 now has two-way connectivity to Eng-Printer at 172.30.0.15 in VLAN30 and CompSci-Printer at 172.31.0.20 in VLAN 31