

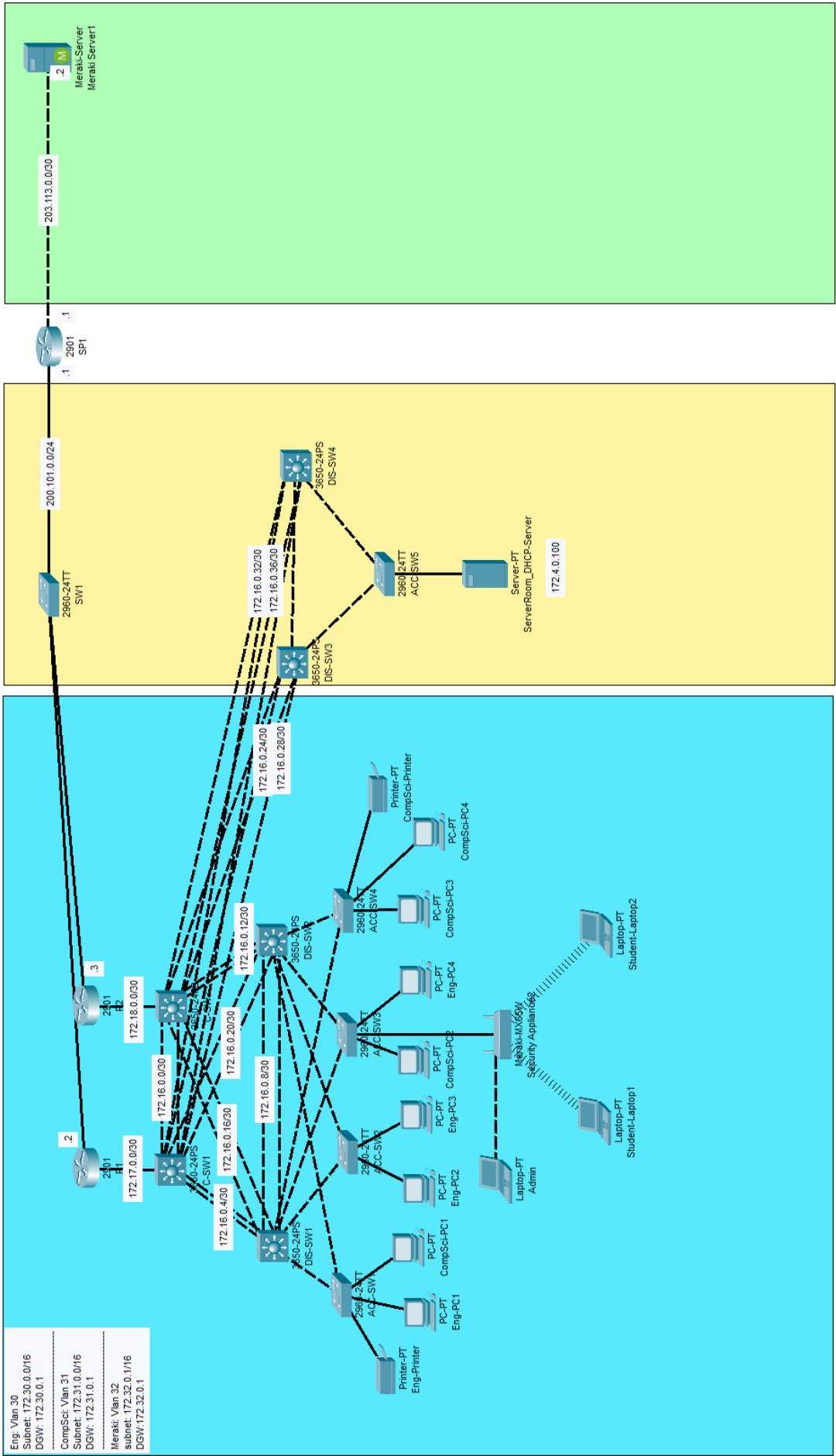
Cisco Meraki Centralized WLC on a 3-Tier Campus LAN Architecture

Table of Contents

ABSTRACT	3
INTRODUCTION	5
METHOD AND EQUIPMENT.....	5
HOSTNAME CONFIGURATION	5
IP SUBNET CONFIGURATION	6
OSPF CONFIGURATION	6
SERVICE PROVIDER STATIC IP ROUTE CONFIGURATION	7
VLAN, DHCP & HSRP CONFIGURATION	7
MERAKE SERVER CONFIGURATION	10
MERAKE-MX65W SECURITY APPLIANCE CONFIGURATION	12
WIRELESS END HOST CONFIGURATION	21
VERIFICATION & DISCUSSION	22

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](#)." 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.



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](#)." 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)#standby 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 its IP address on the internet interface from the serverPool configured on the DHCP server at 172.4.0.100.

SERVICES
 HTTP
DHCP
 DHCPv6
 TFTP
 DNS
 SYSLOG
 AAA
 NTP
 EMAIL
 FTP
 IoT
 VM Management
 Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 172.32.0.1

DNS Server: 203.113.0.2

Start IP Address: 172 32 0 4

Subnet Mask: 255 255 0 0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add
Save
Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	172.32.0.1	203.113.0.2	172.32.0.4	255.255....	512	0.0.0.0	0.0.0.0

Figure 1-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.

The image shows a web interface for configuring a Meraki server. On the left is a sidebar with a menu. The main area is titled 'Global Settings' and contains configuration fields for the device 'Meraki Server1'.

GLOBAL

- Settings
- Algorithm Settings

INTERFACE

- FastEthernet0

Global Settings

Display Name: Meraki Server1

Gateway/DNS IPv4

- ☐ DHCP
- ☒ Static

Default Gateway: 203.113.0.1

DNS Server:

Gateway/DNS IPv6

- ☐ Automatic
- ☒ Static

Default Gateway:

DNS Server:

Figure 2-Meraki server gateway configuration

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0000.0C97.C649

IP Configuration

☐ DHCP
☒ Static

IPv4 Address 203.113.0.2

Subnet Mask 255.255.255.252

IPv6 Configuration

☐ Automatic
☒ Static

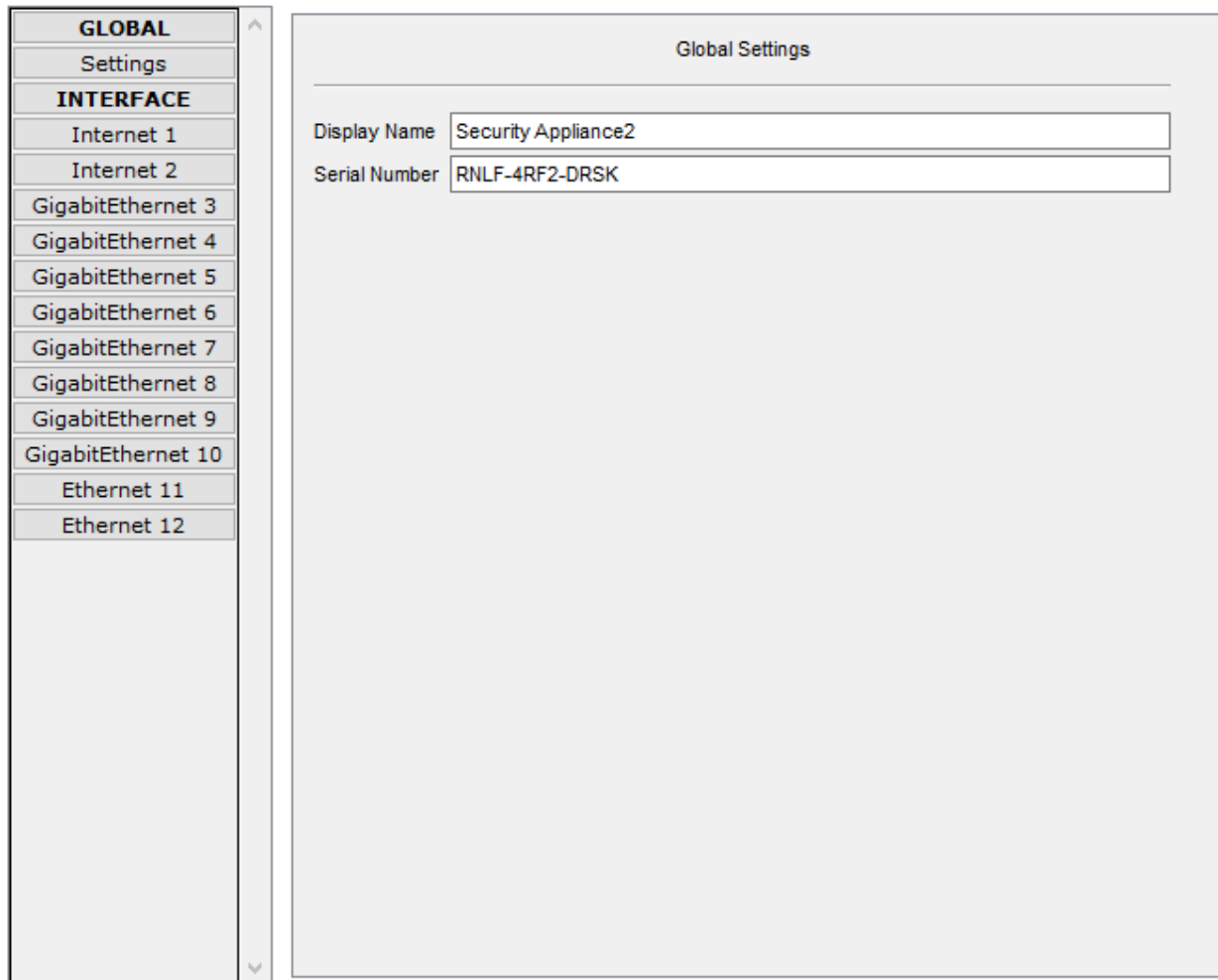
IPv6 Address

Link Local Address: FE80::200:CFF:FE97:C649

Figure 3- 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.



Global Settings	
Display Name	Security Appliance2
Serial Number	RNLF-4RF2-DRSK

Figure 4-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.

The screenshot shows the Meraki Global Settings page for the 'Admin' interface. On the left is a sidebar with navigation links: 'GLOBAL' (selected), 'Settings', 'Algorithm Settings', 'INTERFACE', 'FastEthernet0', and 'Bluetooth'. The main content area is titled 'Global Settings' and contains the following configuration fields:

- Display Name:** Admin
- Interfaces:** FastEthernet0 (selected from a dropdown)
- Gateway/DNS IPv4:**
 - ☒ DHCP
 - ☐ Static
 - Default Gateway:** 192.168.0.1
 - DNS Server:** (empty field)
- Gateway/DNS IPv6:**
 - ☐ Automatic
 - ☒ Static
 - Default Gateway:** (empty field)
 - DNS Server:** (empty field)

Figure 5-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.

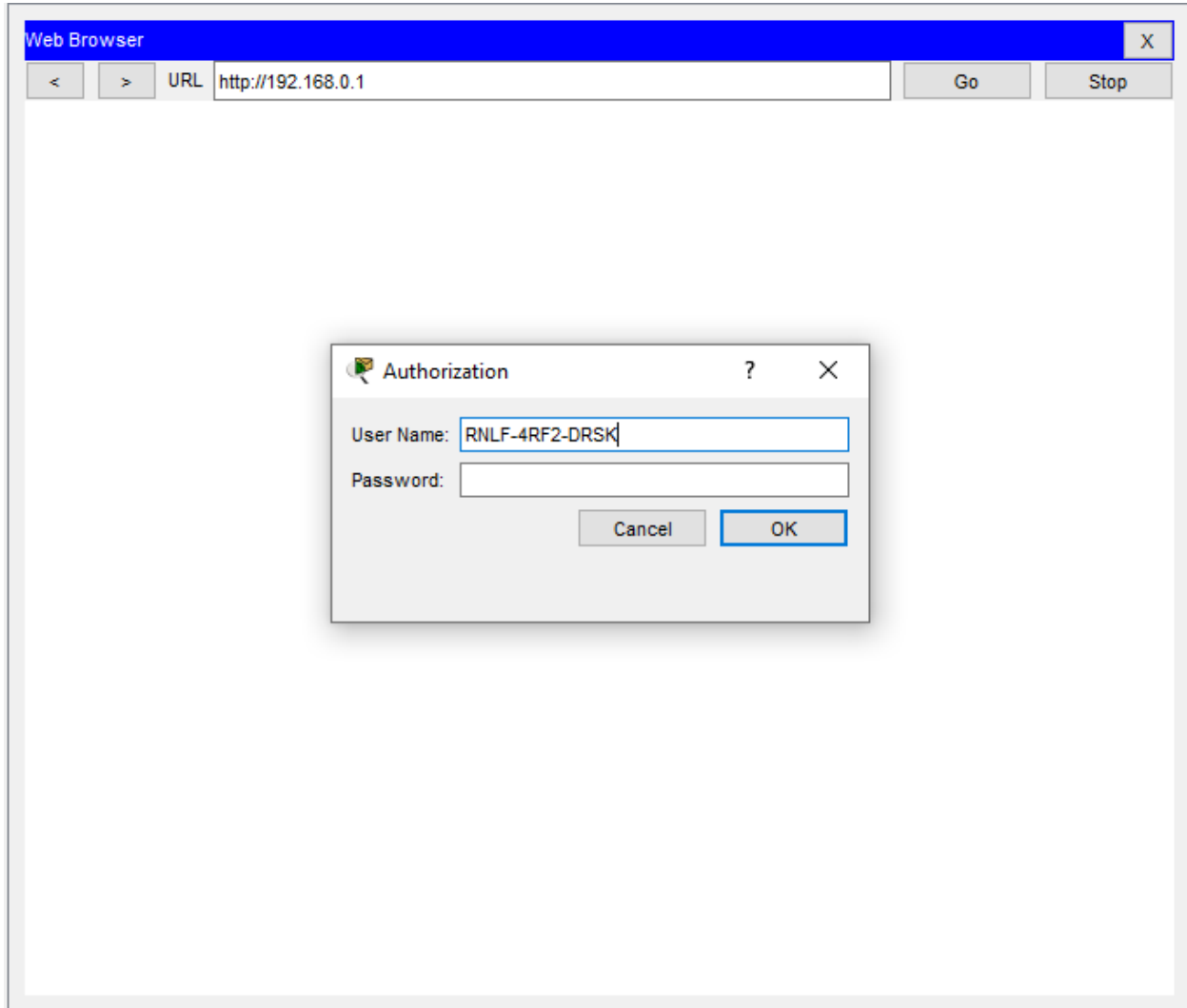


Figure 6-The web browser on the Admin end host is used to connect the Meraki appliance using the Appliance serial number as the User Name and the Password field is left blank

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

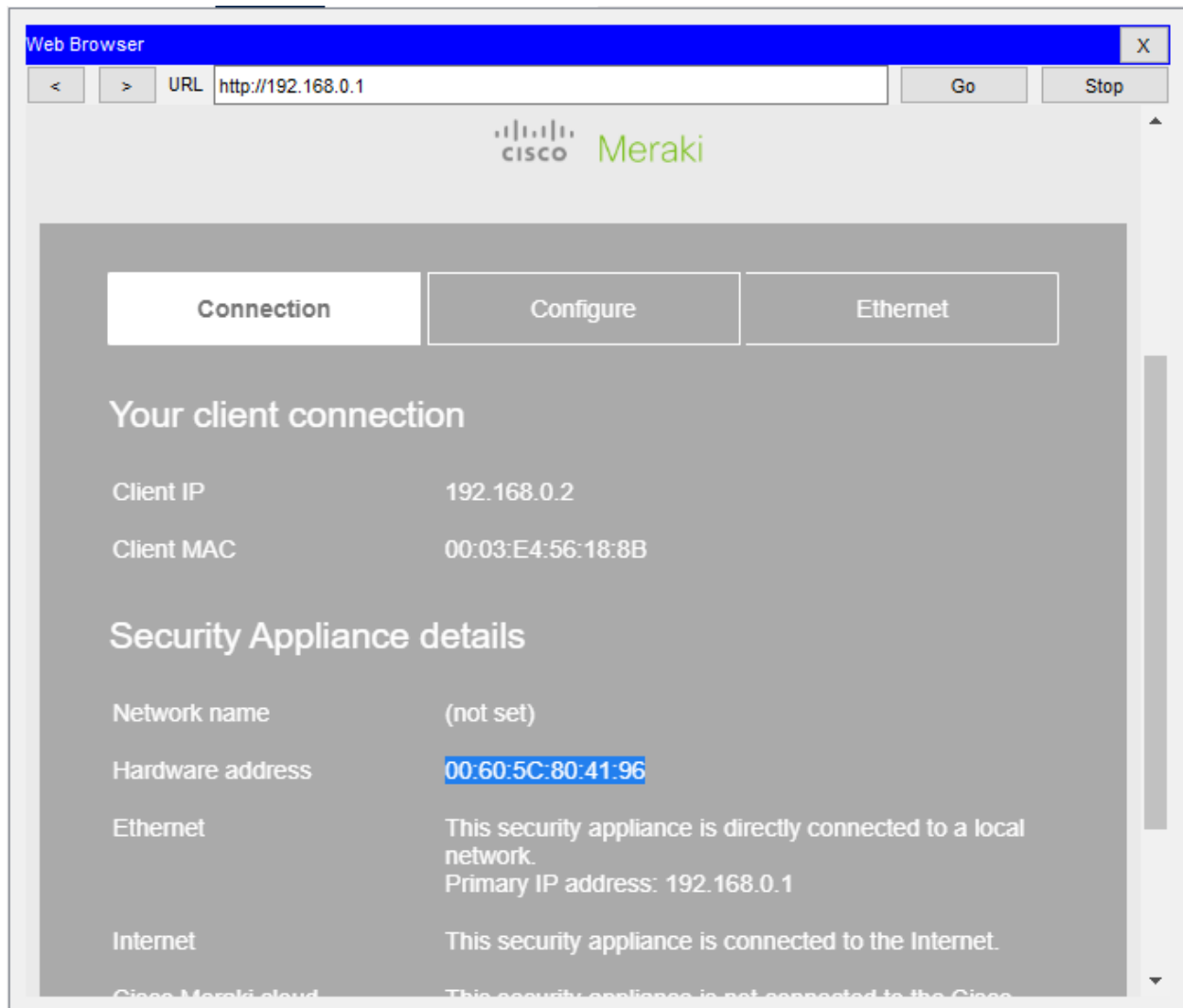


Figure 7-The Meraki Appliance MAC address on the connection page is used for further configuration

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.

The screenshot displays a web interface for configuring uplink connections. At the top, there are three tabs: 'Connection', 'Configure' (which is active), and 'Ethernet'. Below the tabs, the section is titled 'Uplink configuration' with a subtitle 'Configure the uplink Internet connection on this security appliance.' The configuration is divided into two sections: 'Internet 1' and 'Internet 2'. For 'Internet 1', the 'Connection type' is set to 'Direct' and the 'IP assignment' is set to 'DHCP'. For 'Internet 2', the 'Connection type' is set to 'Direct' and the 'IP assignment' is set to 'Static'. Below these settings, there are input fields for 'Address' and 'Netmask' for Internet 2, which are currently empty.

Tab	Connection	Configure	Ethernet
Uplink configuration Configure the uplink Internet connection on this security appliance.			
Internet 1			
Connection type	Direct ▼		
IP assignment	DHCP ▼		
Internet 2			
Connection type	Direct ▼		
IP assignment	Static ▼		
Address	<input type="text"/>		
Netmask	<input type="text"/>		

Figure 8-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.

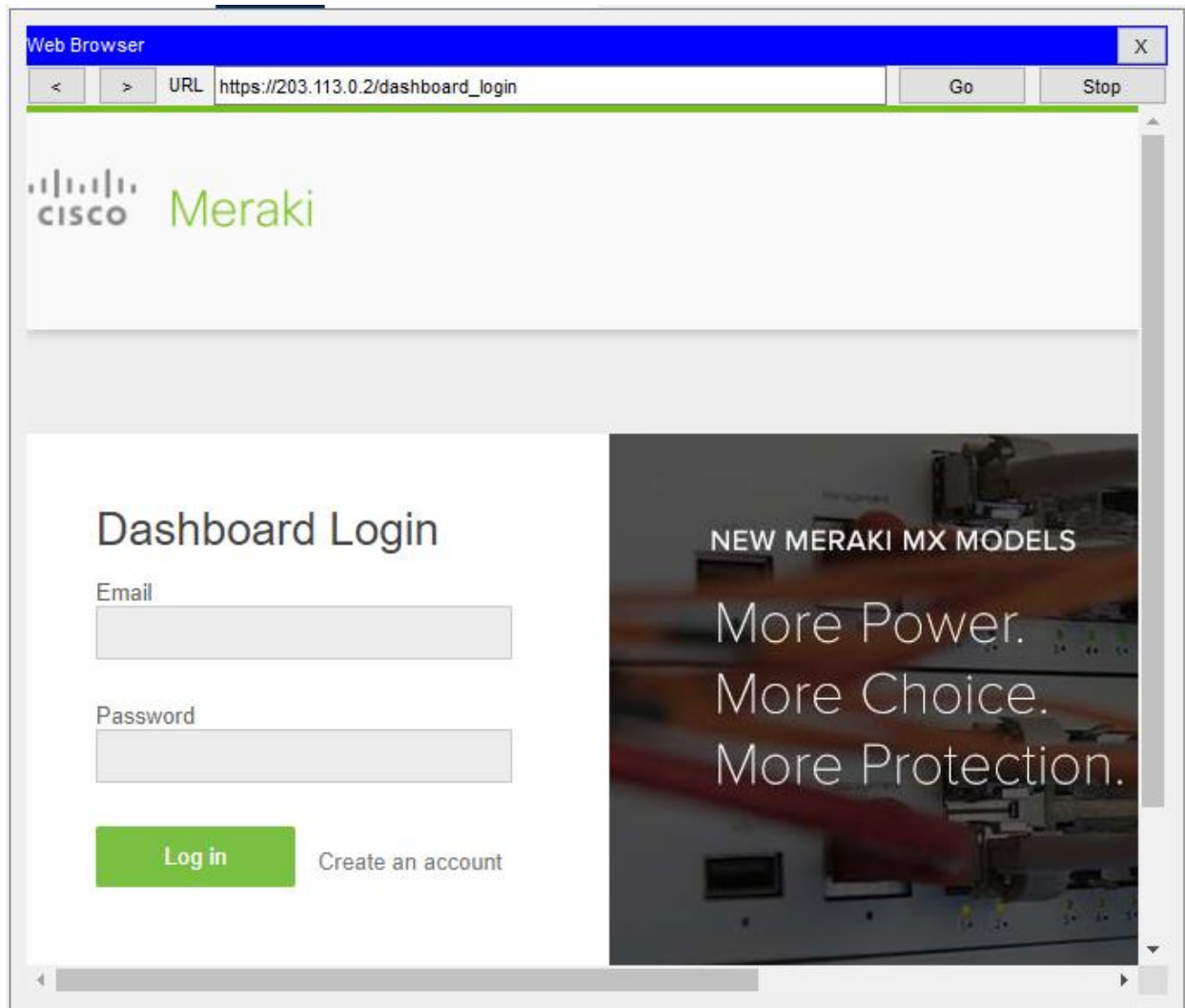
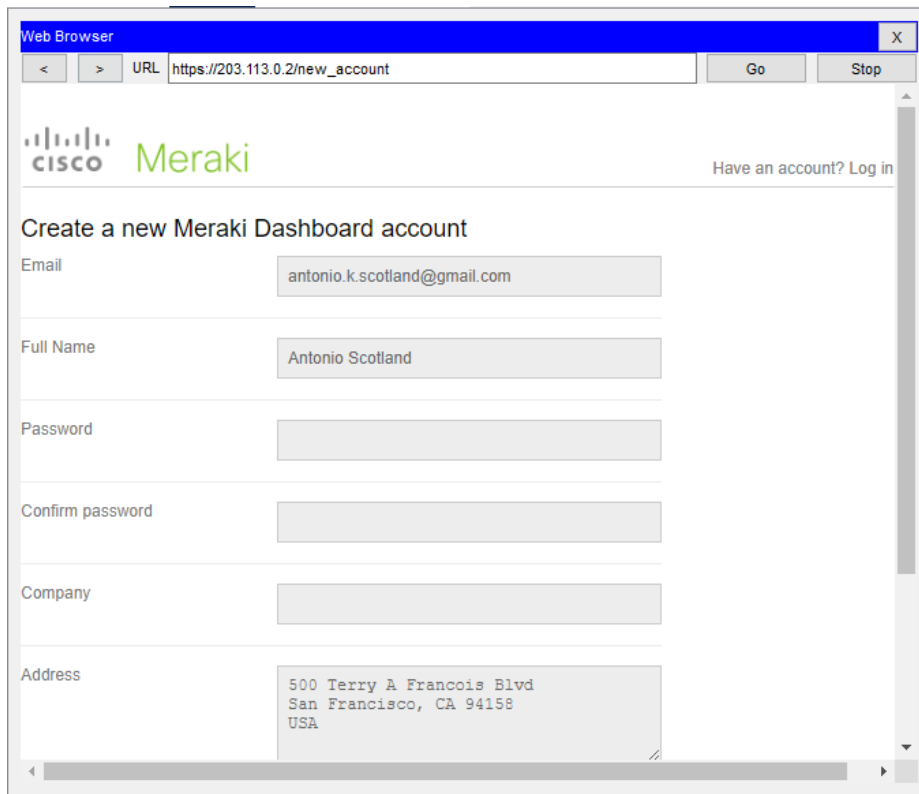


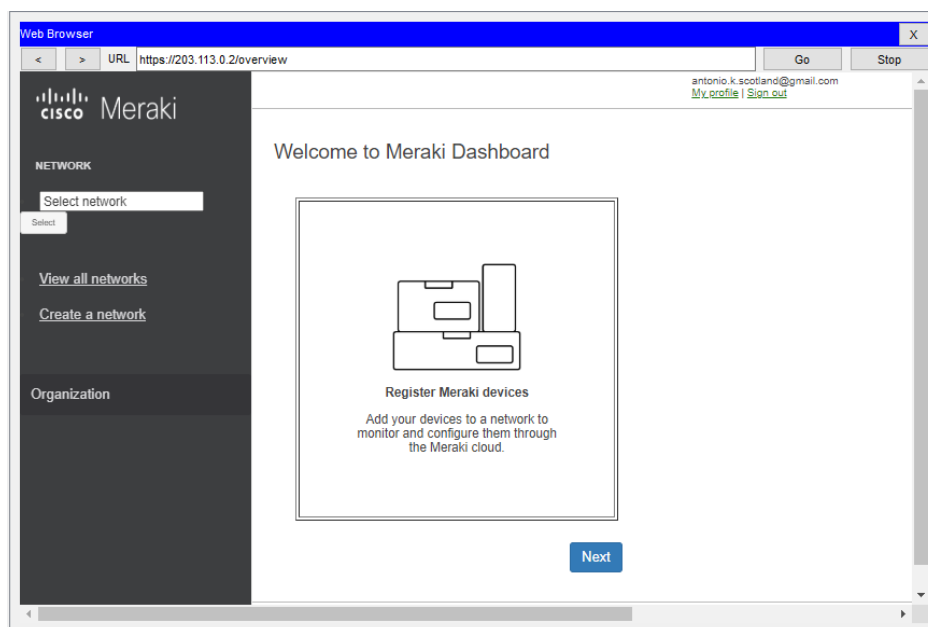
Figure 9-The Meraki Dashboard is accessed via the web browser on the Admin end host using the Meraki server IP (<https://203.113.0.2>), then an account must be created

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.



The screenshot shows a web browser window with the URL `https://203.113.0.2/new_account`. The page features the Cisco Meraki logo and a "Log in" link for existing users. The main heading is "Create a new Meraki Dashboard account". Below this, there are several input fields: "Email" (containing `antonio.k.scotland@gmail.com`), "Full Name" (containing "Antonio Scotland"), "Password", "Confirm password", "Company", and "Address" (containing "500 Terry A Francois Blvd", "San Francisco, CA 94158", and "USA").

Figure 10-The account creation page



The screenshot shows the Meraki Dashboard landing page in a web browser with the URL `https://203.113.0.2/overview`. The page has a dark sidebar on the left with the Cisco Meraki logo and navigation links: "NETWORK" (with "Select network" and "View all networks"), "Create a network", and "Organization". The main content area is titled "Welcome to Meraki Dashboard" and features a large box with a diagram of a Meraki device. Inside this box, the text reads: "Register Meraki devices", "Add your devices to a network to monitor and configure them through the Meraki cloud.", and a "Next" button.

Figure 11-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.

Web Browser

URL: https://203.113.0.2/new_network Go Stop

antonio.k.scotland@gmail.com
[My profile](#) | [Sign out](#)

Meraki

NETWORK

Select network

Select

[View all networks](#)

[Create a network](#)

Organization

Create Network

Setup network

Network name:

Network type:

Network configuration: ☒ Default Meraki configuration

[Create network](#)

Select devices from inventory

You have no unused devices
Add new devices or go to the inventory page to select devices that are already in networks

Add devices to inventory

Enter the individual device serial number:

Enter the device's model:

Figure 12-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.

Web Browser

URL: https://203.113.0.2/new_network Go Stop

Meraki

NETWORK

Select

[View all networks](#)

[Create a network](#)

Network-wide

Security Appliance

MONITOR

Appliance Status

CONFIGURE

Addressing & VLANs

Wireless Settings

DHCP

[Create network](#)

Select devices from inventory

You have no unused devices
Add new devices or go to the inventory page to select devices that are already in networks

Add devices to inventory

Enter the individual device serial number:

Enter the device's model:

Enter the device's mac address:

Enter the network the device belongs to:

[Add devices](#) [Go to inventory](#)

Privacy | Terms | © 2018 Cisco Systems, Inc.

Figure 13-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*.

The screenshot shows a web browser window with the URL `https://203.113.0.2/wireless_setting`. The page is the Cisco Meraki Wireless settings interface. On the left is a dark sidebar with the Meraki logo and navigation links: NETWORK, Quogem Engineering Buildi, View all networks, Create a network, Network-wide, Security Appliance, and Organization. The main content area is titled 'Wireless settings' and shows configuration for 'SSID 1'. The settings are: Status (Enabled), Name (Student), Security (WPA2 PSK), WPA key (masked with dots), WPA encryption mode (WPA2 only), and Visibility (Advertise this SSID publicly). A blue 'Save Changes' button is located below the visibility setting. At the bottom of the page, there are links for Privacy and Terms, and a copyright notice for © 2018 Cisco Systems, Inc.

Figure 14-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.

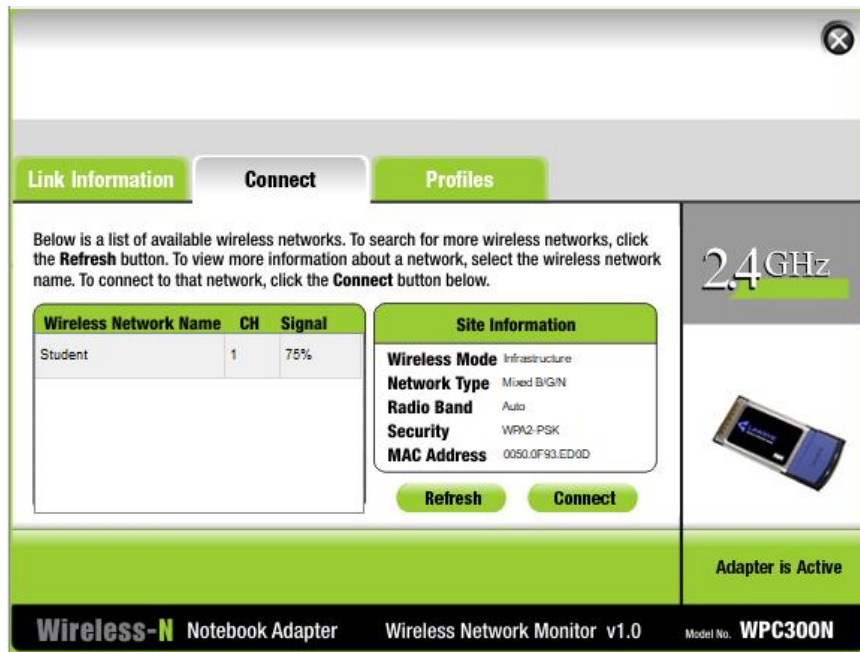


Figure 15-Student laptop wireless configuration GUI detecting the configured Students SSID



Figure 16-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.

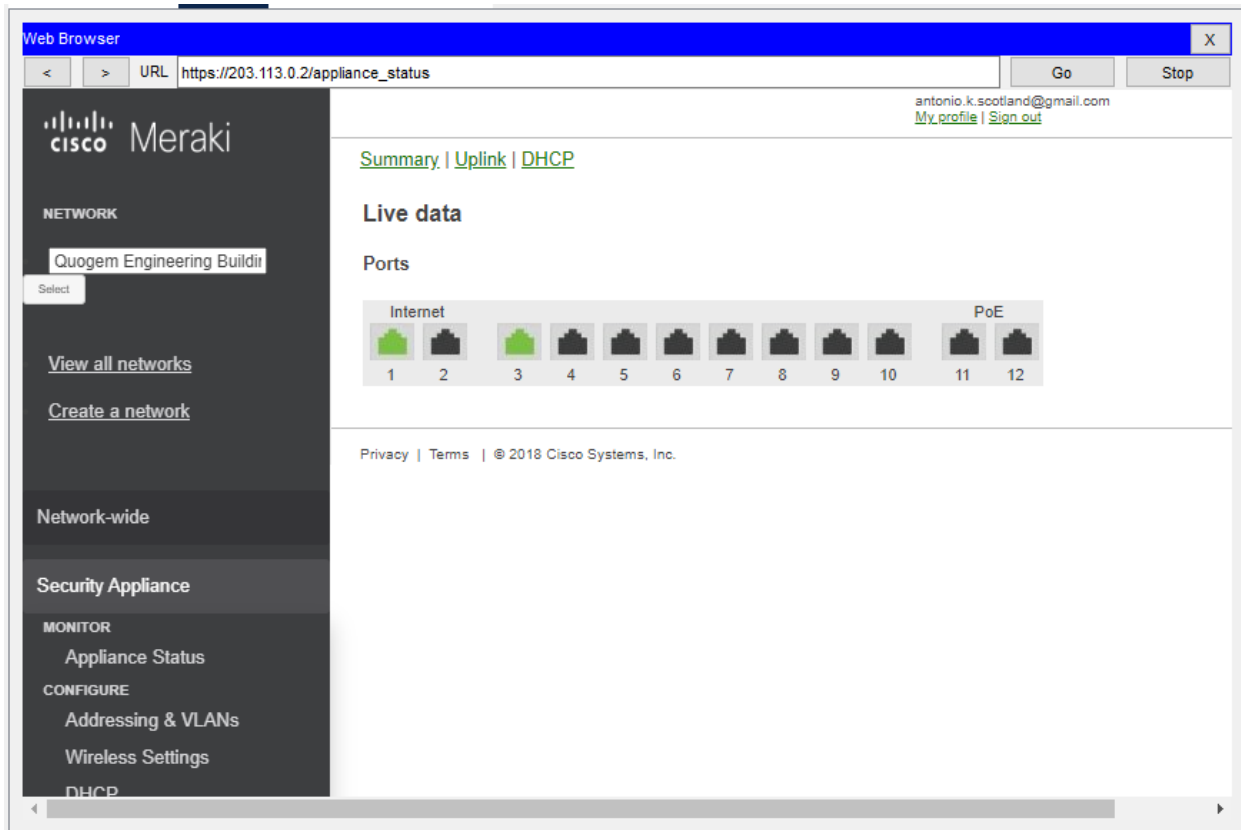


Figure 17-Appliance status on dashboard shows uplink and port 3 are now active

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 repsectively. This is shown in figure 20.

```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.0.1           0060.5c80.4196        dynamic

C:\>ipconfig

Wireless0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:5CFF:FE12:B964
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.0.3
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0
```

Figure 18-IP configuration on Student-Laptop 1

```
C:\>ping 200.101.0.1

Pinging 200.101.0.1 with 32 bytes of data:

Reply from 200.101.0.1: bytes=32 time=22ms TTL=251
Reply from 200.101.0.1: bytes=32 time=33ms TTL=251
Reply from 200.101.0.1: bytes=32 time=84ms TTL=251
Reply from 200.101.0.1: bytes=32 time=16ms TTL=251

Ping statistics for 200.101.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 84ms, Average = 38ms
```

Figure 19-Student-Laptop 1 has two connectivity to the service provider gateway

```
C:\>ping 172.30.0.15

Pinging 172.30.0.15 with 32 bytes of data:

Reply from 172.30.0.15: bytes=32 time=36ms TTL=126
Reply from 172.30.0.15: bytes=32 time=25ms TTL=126
Reply from 172.30.0.15: bytes=32 time=15ms TTL=126
Reply from 172.30.0.15: bytes=32 time=29ms TTL=126

Ping statistics for 172.30.0.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 36ms, Average = 26ms

C:\>ping 172.31.0.20

Pinging 172.31.0.20 with 32 bytes of data:

Reply from 172.31.0.20: bytes=32 time=17ms TTL=126
Reply from 172.31.0.20: bytes=32 time=34ms TTL=126
Reply from 172.31.0.20: bytes=32 time=7ms TTL=126
Reply from 172.31.0.20: bytes=32 time=26ms TTL=126

Ping statistics for 172.31.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 34ms, Average = 21ms

C:\>|
```

Figure 20-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