HP MSM Wireless Deployment – Step by Step Walkthrough

Written by: Jesse Rink

Revision: 0.4H

Send questions/comments to jrink@sourceonetechnology.com

Source One Technology, Inc.
HP Partner
(414) 475 4037 (phone)
(888) 475 6037 (fax)
http://www.sourceonetechnology.com

Note – *This Step by Step Walkthrough is NOT approved by HP, nor is it official HP documentation*. It is meant solely to help customers better understand the steps involved in an HP MSM wireless deployment. The HP MSM product can be configured numerous ways for different scenarios, this is but one example.

Table of Contents

I. Background Information

Current Network Layout

Customer wants to deploy an HP wireless infrastructure to meet their growing wireless needs. The network infrastructure currently consists of an HP 5406ZL core chassis and two HP E2520G-POE-24 switches. Currently there are 3 VLANs implemented for various purposes and management. The servers and network infrastructure are located on VLAN 1, wired computers are located on VLAN 130, and IP Phones are located on VLAN 140.

The following diagram (*Figure 1*) depicts the current network topology layout.

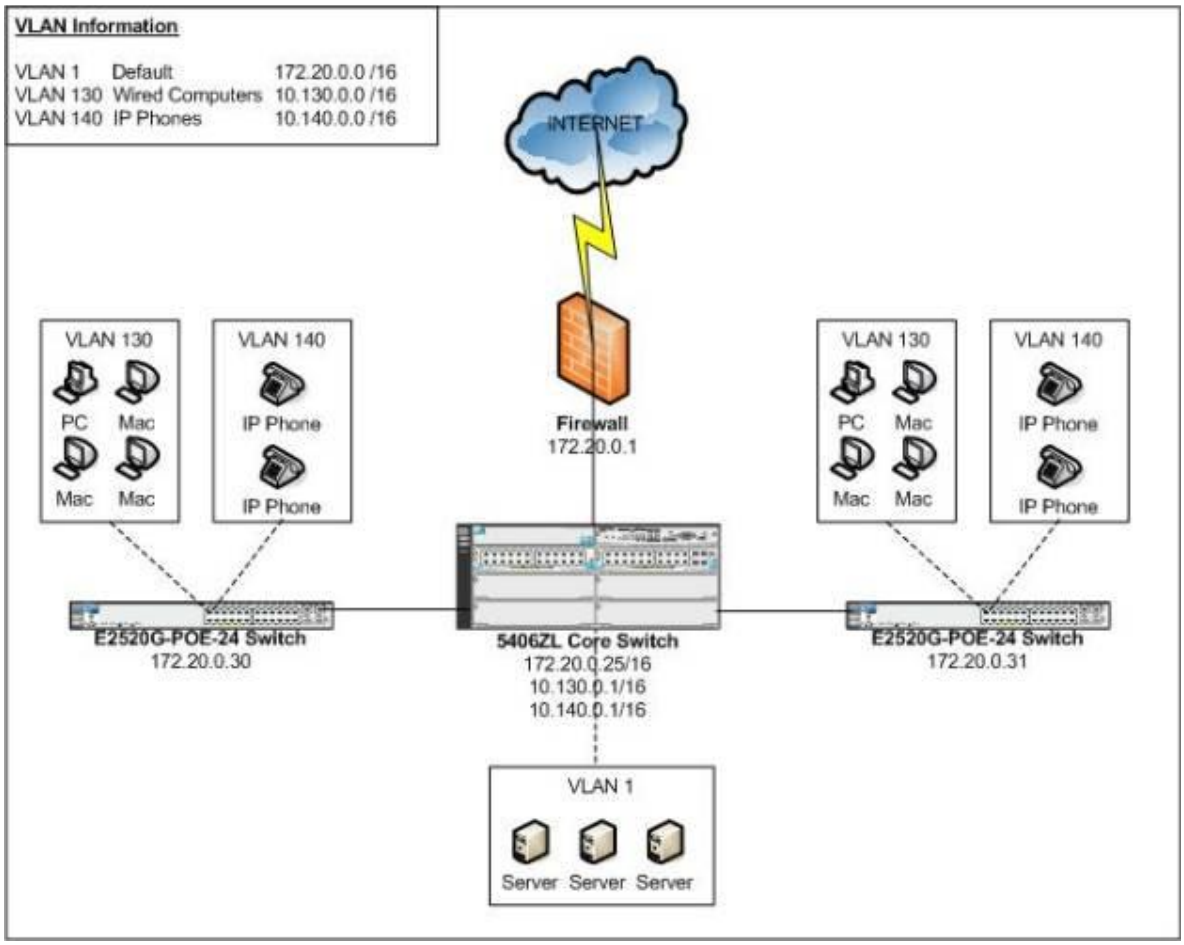


Figure 1

Proposed Network Layout

With the addition of an HP MSM wireless network, the customer wants to provide two different wireless networks: a Private wireless network, and a Public wireless network. The following highlights the design goals for each particular wireless network that will be implemented:

Private Wireless

- Allow only company-owned, or IT-managed, devices on the Private wireless network.
- Use WPA2-PSK security for data encryption.

- Enable Broadcast Filtering to improve wireless performance and reduce unnecessary wireless traffic.
- Enable Band Steering so dual-band capable clients are directed to the 5GHz radios instead of 2.4GHz radios.
- Allow communication between wireless client devices.
- IP addresses for wireless clients are issued by a local Windows DHCP server.

Public Wireless

- Allow any wireless device on the Public wireless network.
- No data encryption – for easier client configuration.
- Prevent guest users from accessing ANY network resources – ONLY allow direct internet access.
- Enable a splash page that forces guest users to authenticate before given access to browse the internet.
- Enable Broadcast Filtering to improve wireless performance and reduce unnecessary wireless traffic.
- Prevent all communication between wireless devices.
- IP addresses for wireless clients are issued by the DHCP Server on the MSM 760 controller.

To accommodate the goals of the two additional wireless networks, two additional VLANs will need to be created in the current network infrastructure.

VLAN ID	VLAN Name	Network ID	Purpose
VLAN 200	MSM-Private	10.200.0.0/16	Used specifically by Private wireless clients
VLAN 210	MSM-Public	10.210.0.0/16	Used specifically by Public wireless clients

The following diagram (*Figure 2*) depicts the <u>proposed</u> network topology layout and changes.

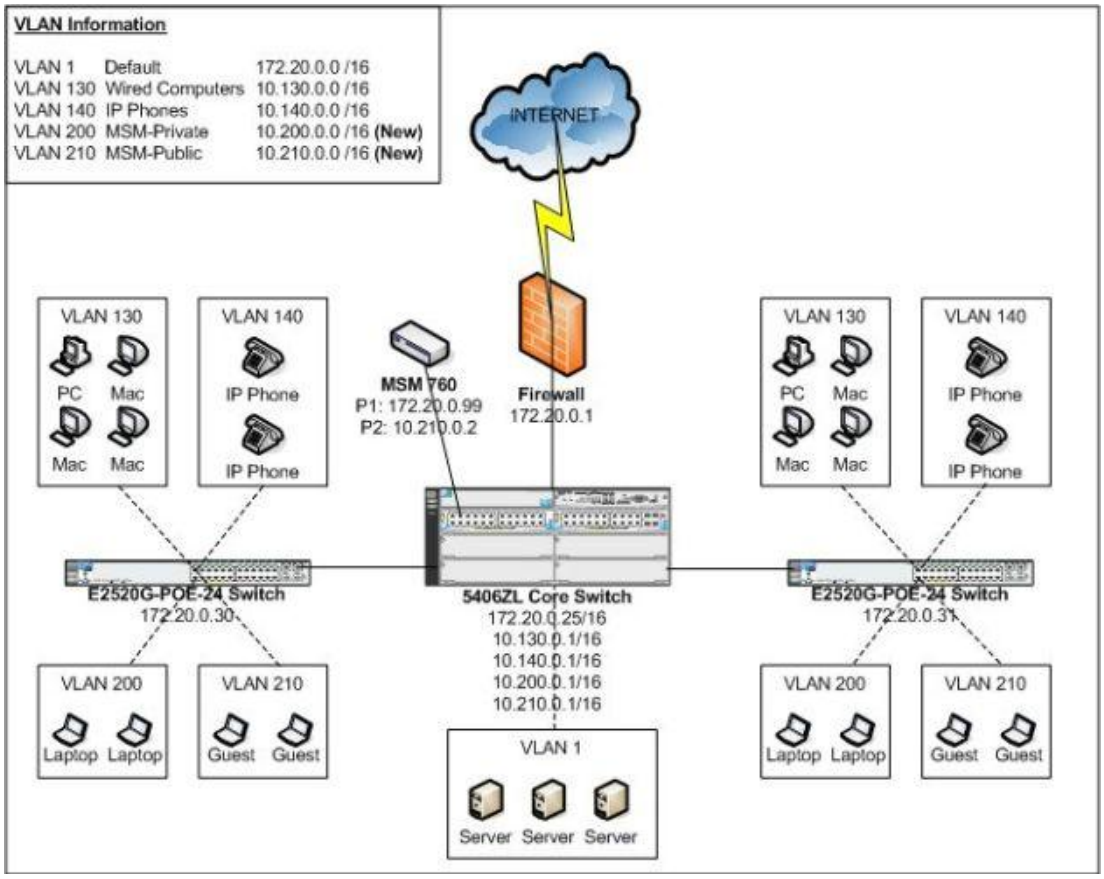


Figure 2

Several changes, including IP addressing and VLAN information will need to be implemented at the core HP 5406ZL switch and at the various HP E2520G edge switches to accommodate the proposed wireless network changes. The changes can be put in place with causing any disruption or outages to the network.

This scenario will sometimes to refer to (2) local Windows Servers. For the purpose of this scenario, these Windows Servers will provide DNS and DHCP functionality. The IP addresses are 172.20.100.22 and 172.20.100.23 and are located on VLAN 1.

II. Switch Configuration Changes

Core switch Configuration

The 5406ZL core switch will need to have the following configuration changes made to accommodate the new MSM wireless deployment:

- Creation of VLAN 200 and VLAN 210.
- Add IP addresses assigned to VLAN 200 and VLAN 210 for routing purposes.
- Add Proper VLAN tagging for the uplink ports between the 5406ZL Core and edge E2520G-POE-24 switches.
- Add Proper VLAN tagging for the MSM 760 controller's Internet and LAN Ports.

When complete, your configuration of the core switch should reflect the configuration shown in *Figure 3* below.

Create VLAN 200 and VLAN 210 and Assign IPs on the Core switch

1. Access the switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials.
3. Enter the Command Line (CLI) interface of the switch.
4. Type "config" at the prompt to enter Configuration Mode.
5. Type "vlan 200 name MSM-Private" to create the VLAN used by the Private wireless.
6. Type "vlan 200 ip address 10.200.0.1 255.255.0.0" to set the IP address for VLAN 200.
7. Type "vlan 210 name MSM-Public" to create the VLAN used by the Public wireless.
8. Type "vlan 210 ip address 10.210.0.1 255.255.0.0" to set the IP address for VLAN 210.
9. Type "write mem" to save the switch configuration.

Configure the Uplink ports (Port B23 and B24) on the Core switch to the Edge switches

1. Access the switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials.
3. Enter the Command Line (CLI) interface of the switch.
4. Port B23 is the uplink port to the 172.20.0.30 (E2520G-POE-24) switch – set applicable VLAN tagging for the newly created VLAN 200 and VLAN 210.
    a. Type "config" at the prompt to enter Configuration Mode.
    b. Type "vlan 200 tagged b23".
    c. Type "vlan 210 tagged b23".

5. Port B24 is the uplink port to the 172.20.0.31 (E2520G-POE-24) switch – set applicable VLAN tagging for the newly created VLAN 200 and VLAN 210.
    a. Type “vlan 200 tagged b24”.
    b. Type “vlan 210 tagged b24”.
6. Type “write mem” to save the switch configuration.

Configure the MSM 760 LAN Port and Internet Ports (A1 and A2) on the Core switch

1. Access the switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials.
3. Enter the Command Line (CLI) interface of the switch.
4. Type “config” at the prompt to enter Configuration Mode.
5. Type “vlan 210 untagged a1”
6. Type “vlan 1 untagged a2”
7. Type “write mem” to save the switch configuration.

Edge Switches Configuration

The two HP E2520G-POE-24 switches shown in *Figure 2* will need to have the following configuration changes made to accommodate the new MSM wireless deployment:

- Creation of VLAN 200 and VLAN 210
- Proper VLAN tagging for Port 24 (the Uplink port to the 5406ZL core switch)
- Proper VLAN tagging for Ports 1-10 (the ports used by the MSM 460 Access Points)

When complete, your configuration of the Edge switches should reflect the configuration show in *Figure 3 below.*

Create VLAN 200 and VLAN 210 on both Edge switches

1. Access the switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials.
3. Enter the Command Line (CLI) interface of the switch.
4. Type “config” at the prompt to enter Configuration Mode.
5. Type “vlan 200 name MSM-Private” to create the VLAN used by the Private wireless.
6. Type “vlan 210 name MSM-Public” to create the VLAN used by the Public wireless.

Configure the Uplink ports (Port 24) on both Edge switches to the 5406ZL Core switch

1. Access the switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials
3. Enter the Command Line (CLI) interface of the switch.
4. Type “config” at the prompt to enter Configuration Mode.
5. Type “vlan 200 tagged 24” to tag Uplink Port 24 for VLAN 200 traffic.
6. Type “vlan 210 tagged 24” to tag Uplink Port 24 for VLAN 210 traffic.

When VLAN tagging for the switches and uplink ports are complete, your switch configuration should resemble this diagram (*see Figure 3*).

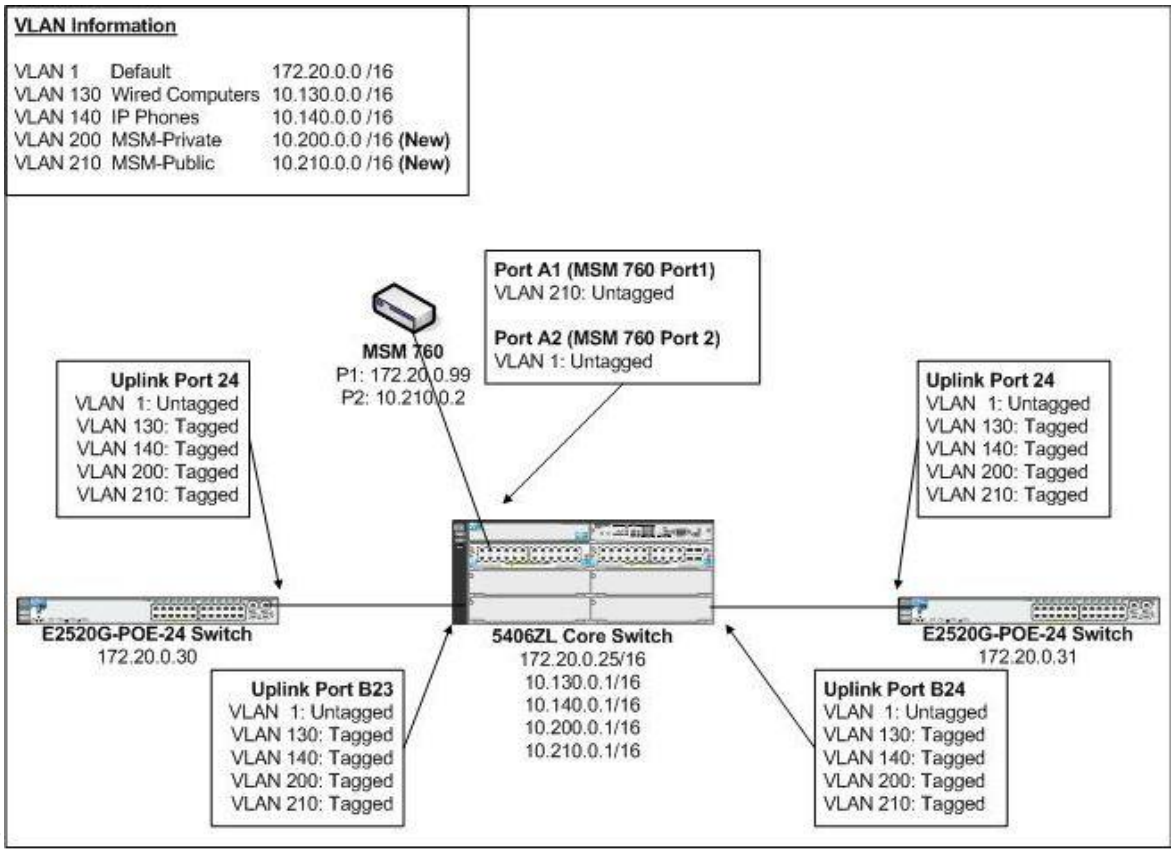


Figure 3

Configure the Edge ports on both Edge switches for the MSM 460 APs (Ports 1-10)

Each Edge switch will have MSM 460 APs directly connected on ports 1-10. AP's will be configured for VLANs in the following manner:

- Untagged on VLAN 1 - for purposes of receiving an IP address and management.
- Tagged on VLAN 200 – for purposes of the Private VSC
- Tagged on VLAN 210 – for purposes of the Public VSC

1. Access the switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials.
3. Enter the Command Line (CLI) interface of the switch.
4. Type "config" at the prompt to enter Configuration Mode.
5. Type "vlan 1 untagged 1-10" to untag ports designated for MSM 460 APs on VLAN 1.
6. Type "vlan 200 tagged 1-10" to tag ports designated for MSM 460 APs on VLAN 200.
7. Type "vlan 210 tagged 1-10" to tag ports designated for MSM 460 APs on VLAN 210.

Type "show vlan 200" on both Edge switches and verify you see the following configuration as shown in *Figure* 4:

Figure 4

```
VLAN ID : 200
Name : MSM-Private
Status : Port-based  Voice : No
Jumbo : No

Port Information Mode     Unknown VLAN Status
---------------- -------- ------------ ----------
1                Tagged   Learn        Up
2                Tagged   Learn        Up
3                Tagged   Learn        Up
4                Tagged   Learn        Down
5                Tagged   Learn        Down
6                Tagged   Learn        Down
7                Tagged   Learn        Down
8                Tagged   Learn        Down
9                Tagged   Learn        Down
10               Tagged   Learn        Down
24               Tagged   Learn        Up
```

Type “show vlan 210” on both Edge switches and verify you see the following configuration as shown in *Figure* 5:

Figure 5

```
VLAN ID : 210
Name : MSM-Public
Status : Port-based  Voice : No
Jumbo : No

Port Information Mode     Unknown VLAN Status
---------------- -------- ------------ ----------
1                Tagged   Learn        Up
2                Tagged   Learn        Up
3                Tagged   Learn        Up
4                Tagged   Learn        Down
5                Tagged   Learn        Down
6                Tagged   Learn        Down
7                Tagged   Learn        Down
8                Tagged   Learn        Down
9                Tagged   Learn        Down
10               Tagged   Learn        Down
24               Tagged   Learn        Up
```

Also verify that the edge ports used for the MSM APs and the uplink ports are also untagged for VLAN 1 (the Default VLAN) as shown in *Figure 3*. When complete, type “write mem” to save the switch configuration on both Edge switches.

III. DHCP Setup

Windows DHCP Server Setup and Configuration of IP Helper

The Private wireless VSC will be egressed to the network on VLAN200. We will need to make the following configuration changes in order to allow wireless clients connected to the Private wireless VSC to receive an IP address from the local Windows Server:

- Configure an IP Helper address for VLAN 200 on the core 5406ZL switch
- Create a DHCP Scope for VLAN 200 on the local Windows Server

Configure the appropriate IP Helper address

1. Access the 5406ZL core switch via a console port cable, telnet, or SSH connection as applicable.
2. Provide applicable login credentials.

3. Enter the Command Line (CLI) interface of the switch.
4. Type “config” at the prompt to enter Configuration Mode.
5. Type “vlan 200 ip helper-address 172.20.100.23” (our local Windows Server hosting DHCP).
6. Type “write mem” to save the switch configuration.

VLAN 200 should now show the following IP Helper information when issuing a “show run” command on the core 5406ZL switch (see *Figure* 6)

Figure 6

Create the DHCP Scope for VLAN 200 on the Windows Server

1. Logon to the local Windows Server (172.20.100.23 in this scenario) and start the DHCP management console application from Administrative Tools.
2. Expand DHCP -> Your Server -> IPv4 and select New Scope from the Action toolbar menu.
3. Assign a name to the Scope (for example, MSM-Private).
4. Enter the appropriate range of IP addresses.
    a. Starting address 10.200.1.0
    b. Ending address 10.200.9.255
    c. Subnet Mask 255.255.0.0
5. No IP exclusions are necessary as part of this scenario.
6. Set a lease duration of 8 hours.
7. When asked to configure scope option now, choose Yes.
    a. Default gateway – 10.200.0.1 (the 5406ZL core switch)
    b. Parent domain – mycompany.com
    c. DNS Server - 172.20.100.23 (the local Windows DNS server)
    d. Activate the DHCP Scope and click Finish when completing the wizard

IV. MSM 760 Controller – Initial Setup

Initial Setup

Start by setting up the basic one-time configuration options that require input the first time you log on to the MSM 760 controller. It would also be advisable to update to the latest version of production firmware code that is available through HP Procurve Support services.

1. Change your PC’s network card IP from DHCP to a Static IP address of 192.168.1.50 with a 255.255.255.0 Subnet Mask.
2. Physically connect your PC’s network card to Port 2 (LAN Port) of the MSM 760 controller.
3. Access the MSM 760 controller via a web browser at address https://192.168.1.1
4. Login using the default username of *admin* and password of *admin*.
5. Agree to the HP End User License Agreement.

6. When asked to Register, select the Register Later option.
7. Select the appropriate Country Code and click Save.
8. Change the default administrator password from *admin* to your preference and click Save.
9. Update the firmware to the latest production release.
    a. From the main interface menu, select Controller ->Maintenance -> Firmware updates.
    b. Click Browse and select the applicable firmware release.
    c. Click Install to install the firmware.
    d. Wait for MSM 760 to install firmware and reboot the controller.
    e. Connect to the MSM 760 controller via a web browsing at address https://192.168.1.1
    f. Login using applicable username and password that was set in earlier steps.

IP Configuration

The next step is to configure both the LAN and Internet Ports of the MSM 760 controller for proper IP address as we defined earlier in our wireless deployment scenario (*see Figure 2*) and plugging in the LAN Port and Internet Port to the Core 5406ZL switch.

1. Connect to the MSM 760 controller via a web browsing at address https://192.168.1.1
2. Login using applicable username and password that was set in earlier steps
3. Setup the LAN Port IP address (172.20.0.99)
    a. From the main interface menu, select Controller -> Network -> Ports
    b. Click LAN Port – Set IP address to 172.20.0.99 with a Subnet Mask of 255.255.0.0 then click Save. (At this time, your PC will lose access to the controller because of the IP/network change)
    c. Disconnect your PC from Port 2 (LAN Port) of the MSM 760 controller.
    d. Change your PC's network card from the previously assigned Static IP address of 192.168.1.50 to a DHCP address.
    e. Connect your PC's network card to the network on VLAN 1.
    f. Verify your PC is given a DHCP address on VLAN 1 from your local DHCP server.
    g. Connect port 2 (LAN Port) of the MSM 760 controller to port A2 of the Core 5406ZL switch.
    h. Ping the LAN Port of the MSM 760 controller (172.20.0.99) to verify connectivity.
    i. Access the MSM 760 controller via a web browser at address https://172.20.0.99
    j. Login using applicable username and password that was set in earlier steps.
4. Setup the Internet Port IP address (10.210.0.2)
    a. From the main interface menu, select Controller -> Network -> Ports
    b. Click Internet Port – Change from DHCP Client to Static, and then click on Configure.
    c. Specify IP address as specified earlier, 10.210.0.2 with Subnet Mask of 255.255.0.0 and click Save, and then click Save again, to return to the Port Configuration page (see *Figure 7*).

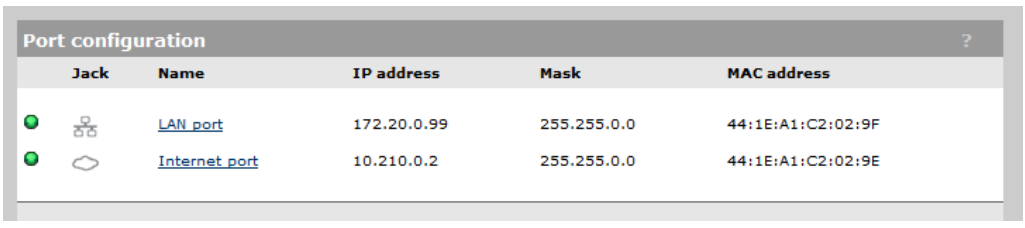


Figure 7

    d. Connect port 1 (Internet port) of the MSM 760 controller to port A1 of the Core 5406ZL switch.

V. MSM 760 Controller – Configuration

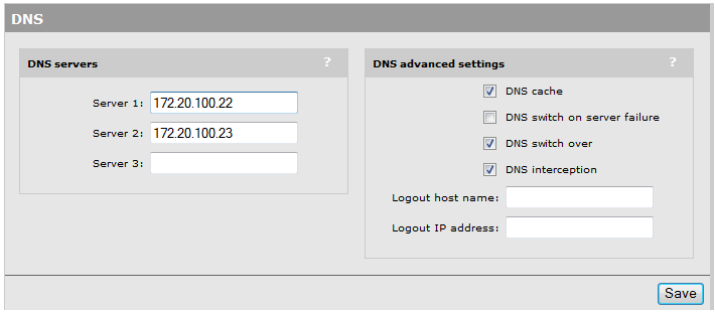
Setup DNS

Proper DNS Server configuration is needed for successful deployment of our future Public wireless network.

1. From the main interface menu, select Controller -> Network -> DNS
2. Specify the DNS servers on the network, in this case we will use two Microsoft AD DNS servers.
    a. Server 1: 172.20.100.22
    b. Server 2: 172.20.100.23
3. Specific DNS advanced settings.
    a. DNS Cache – Enable
    b. DNS Switch Over – Enable
    c. DNS Interception – Enable
4. Click Save.

Your DNS information should be defined as follows (see *Figure 8*):

Figure 8



Setup IP Routing

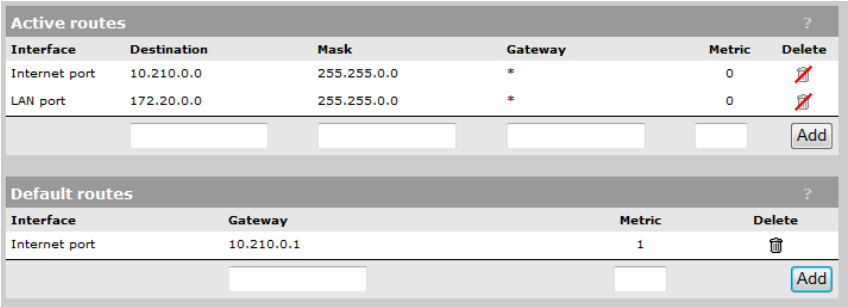
In our scenario, we need to setup a Default Gateway route on the MSM 760 controller so data can be sent across the various networks defined when we documented our wireless deployment.

1. From the main interface menu, select Controller -> Network -> IP Routes
2. Add a default route of 10.210.0.1 (IP address of VLAN 210 on the 5406ZL Core) with metric 1 and click Add.

Note -- Until the Default route is added, you will not be able ping the Internet Port's IP address from any network except the 172.20.0.0/16 and 10.210.0.0/16 networks. After the Default route has been added, you should be able to ping the Internet Port's IP address from any network.

Your IP and Routing information should be defined as follows (see *Figure 9):*

Figure 9



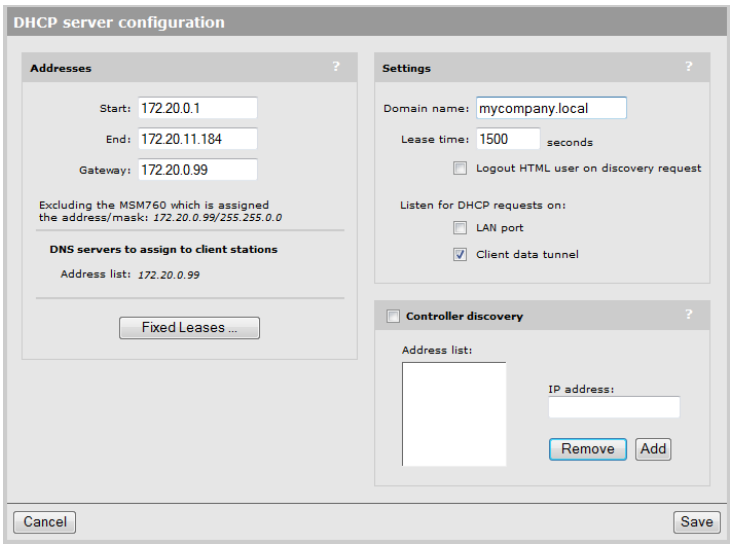
Address Allocation and DHCP Services

Because we will be using the MSM 760 controller to hand out DHCP addresses to wireless clients on the Public VSC, we need to activate the DHCP services on the controller. (Please note – we will define the actual IP address range that is handed out by the MSM 760 controller later on when we configure the Public VSC)

1. From the main interface menu, select Controller -> Network -> Address Allocation
2. Change DHCP services option to DHCP Server and click Configure.
3. Enter a domain name, such as “mycompany.local”.
4. Change the lease time duration to 1500 seconds (or to custom value you prefer).
5. Set the Listen for DHCP requests on:
    a. LAN Port – Disabled (You must disable this if you already have a DHCP server on the LAN Port network)
    b. Client data tunnel – Enabled

Your DHCP Services information should be defined as follows (see Figure *10*):

Figure 10



Remote Logging

If you wish to define a remote Syslog server for logging purposes you can define this in the MSM 760 controller. Setting up a remote Syslog server will allow you to maintain a much longer retention period for various warnings, errors, and other event log entries.

1. From the main interface menu, select Controller -> Tools -> Remote Log

2. Specify a name for the Remote Syslog server.
3. Specify the Syslog Server address. In this case we will use a Syslog server which is already setup on IP address 172.20.100.54.
4. Specific the Filter definitions. Enable the checkbox next to Severity Level option and set for Higher or Equal to:
    a. Warning – for basic logging
    b. Debug – for detailed logging when you are actively troubleshooting a support issue.
5. Click Save.

Your Remote Logging information should be defined as follows (see *Figure 11*):

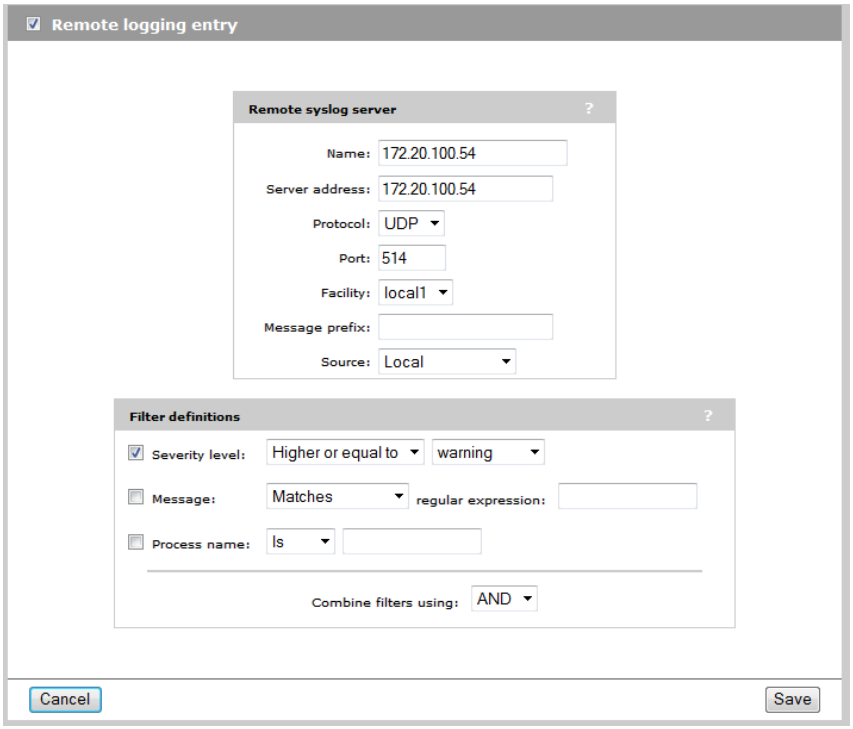


Figure 11

SNMP Configuration

If you wish to monitor the MSM 760 controller via SNMP management, you can define these settings.

1. From the main interface menu, select Controller -> Management -> SNMP
2. Enter in the applicable information for Location and Contact attributes.
3. Select your SNMP protocol versions (Version 1 and 2C are selected by default)
4. Specify the applicable Community Names used for SNMP monitoring in your network.
5. Specify the Notification Receiver for SNMP trap notification.
6. Click Save when completed.

Time Configuration

Setting the appropriate system time is important for reviewing Event Logs on the MSM 760 controller to aid in various troubleshooting steps and procedures. An external NTP server, or an internal NTP server, can be used. In

this scenario we will specify the internal Domain Controller servers on the local network to be used for time synchronization.

1. From the main interface menu, select Controller -> Management -> System Time.
2. Change the Time Zone to the appropriate value.
3. Remove any previous Time Server entries.
4. Add 172.20.100.22 and 172.20.100.23 as our local Time Servers.

Your Time Configuration should be defined as follows (see *Figure 12*):

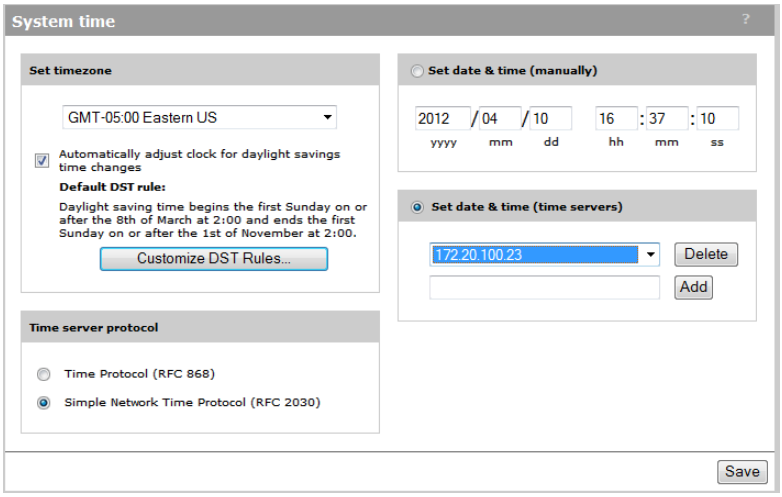


Figure 12

Bandwidth Control

In some scenarios, we may want to limit the data rate of the Public wireless traffic that will be tunneled through the controller's Client Data Tunnel and Internet Port. In this deployment scenario, our internet pipe is 75Mb, so we will set a limitation of 20Mb for all Public wireless traffic to the internet so Public wireless traffic doesn't saturate our internet bandwidth.

1. From the main interface menu, select Controller -> Network -> Bandwidth Control
2. Enable the checkbox for Internet port data rate limits.
3. Specify a maximum transmit and receive rate for 20480 kbps.
4. Click Save.

Your Bandwidth Control should be defined as follows (see *Figure 13*):

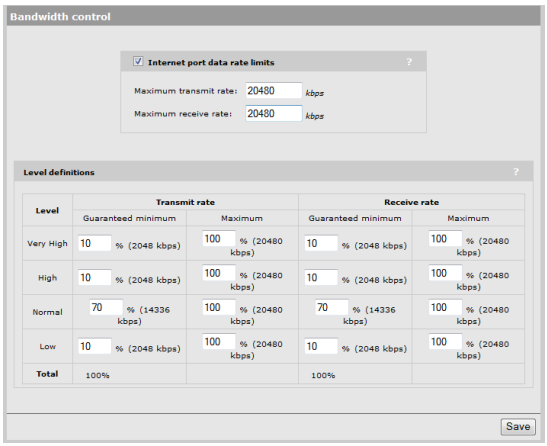


Figure 13

VI. VSC Setup

VSC Creation – Private Wireless

The goals for the Private wireless VSC were determined to be as follows:

- Allow only company-owned, or IT-managed, devices on the Private wireless network.
- Use WPA2-PSK security for data encryption.
- Enable Broadcast Filtering to improve wireless performance and reduce unnecessary wireless traffic.
- Enable Band Steering so dual-band clients are directed to the 5GHz radios instead of 2.4GHz radios.
- Allow communication between wireless client devices.

To configure the Private wireless VSC, perform the following steps:

1. From the main interface menu, select Controller -> VSCs -> HP (this is the default VSC which we will edit)
2. Change the Profile name from HP to Private.
3. Uncheck the Authentication and Access Control check boxes.
4. Change the SSID name from HP to Private.
5. Enable the Broadcast Filtering check box.
6. Disable the Wireless Security Filters checkbox.
7. Enable wireless protection modes:
    a. Set Mode as WPA2 (AES/CCMP).
    b. Set Key Source as Preshared Key.
    c. Define a Key password.
    d. Confirm the Key password.
8. Click the Save button.

Your Private VSC should be defined as follows (see *Figure 14*):

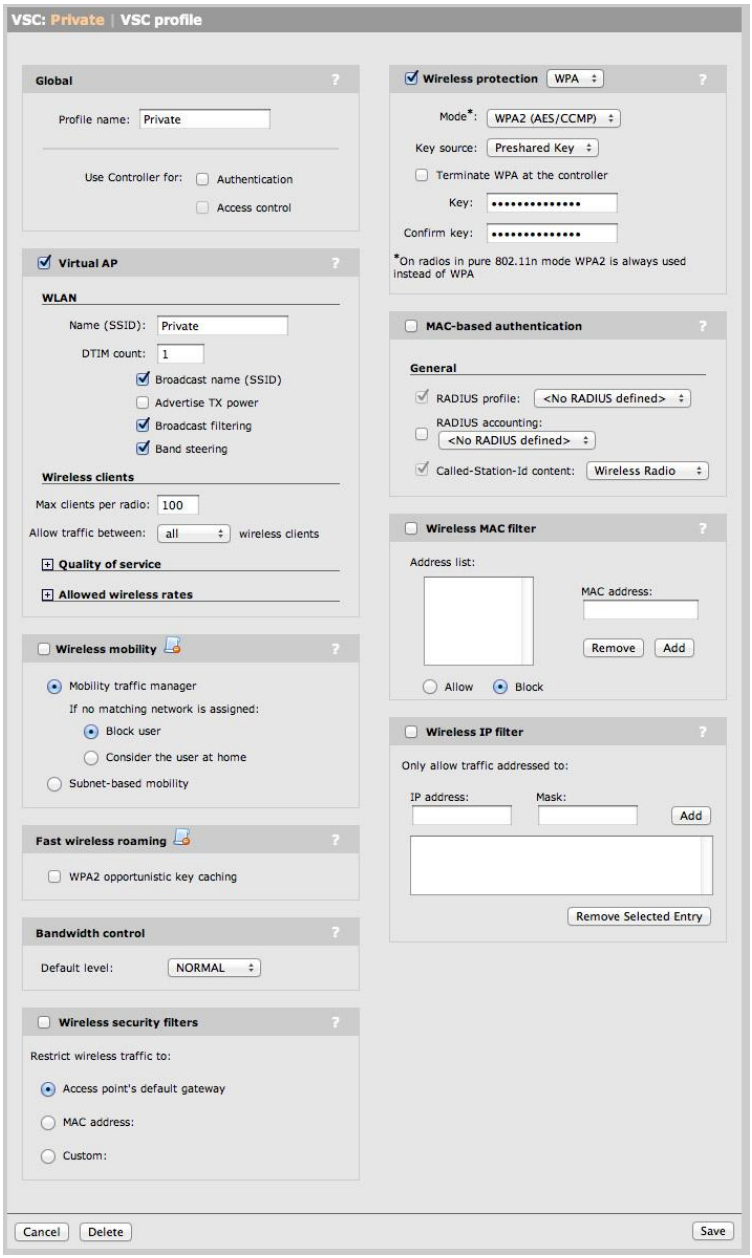


Figure 14

VSC Creation – Public Wireless

The goals for the Public wireless VSC were determined to be as follows:

- No wireless encryption so any guest device can connect.
- Enable a splash page redirection that forces guest users to provide authentication credentials before being allowed to browse the internet.
- Prevent guest users from accessing any network resources – only allow them access directly to the internet (this will be accomplished later through the use of setting up Access Lists in the MSM 760 controller)
- Enable Broadcast Filtering to improve wireless performance and reduce unnecessary wireless traffic.
- Prevent any client-to-client wireless traffic so users cannot access other devices on the Public network.

- Allow the MSM 760 Controller to hand out IP addresses via DHCP to Public wireless users

To configure the Public wireless VSC, perform the following steps:

1. From the main interface menu, select Controller -> VSCs
2. Click Add New VSC Profile
3. Change the Profile name from HP to Public.
4. Leave the Authentication and Access Control check boxes enabled.
5. Change the SSID name from HP to Public.
6. Enable the Broadcast Filtering check box.
7. Change 'Allow Traffic Between [All|No] Wireless Clients' to No.
8. Expand Client Data Tunnel and enable the 'Always Tunnel Client Traffic' check box.
9. Disable any Wireless Protection is used (WPA/WEP) so the VSC is Open.
10. Verify HTML-based User logins is enabled using Local authentication (note – we will create a guest user later in this document).
11. Enable the DHCP Server option in the VSC. This will allow the MSM 760 controller to hand out DHCP addresses to the Public wireless clients in a NAT'd IP range. Since we already enabled the MSM 760 DHCP Server in previous steps, we will now configure the following DHCP Server options for the Public VSC:
    a. DNS – 10.220.0.1
    b. Start – 10.220.0.100
    c. End – 10.220.9.255
    d. Gateway – 10.220.0.1
    e. Netmask – 255.255.0.0
    f. Subnet – 10.220.0.0
12. Save VSC Settings.

Your Public VSC should be defined as follows (see *Figure 15*):

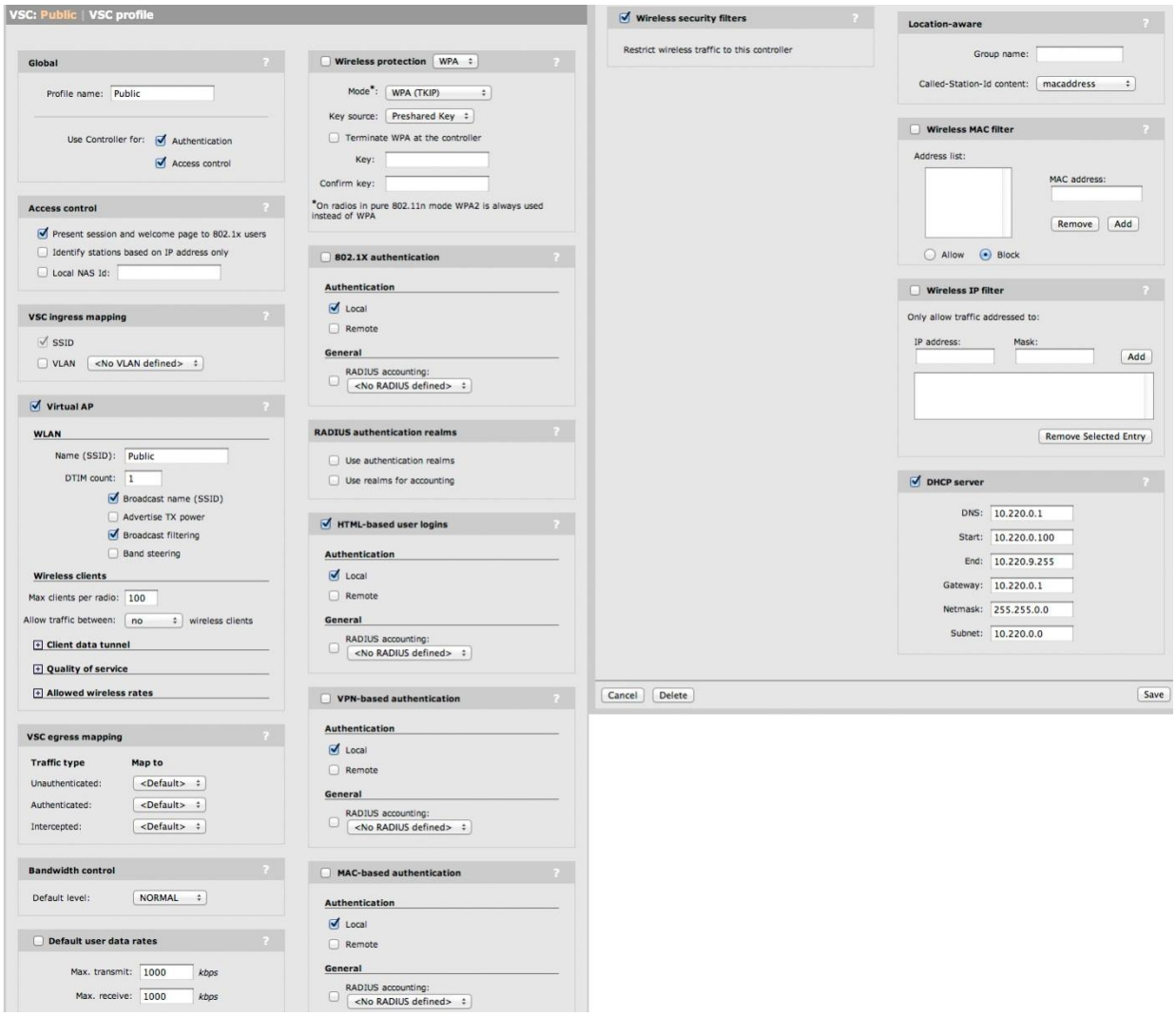


Figure 15

VII. Network Profiles and VSC Bindings

Network Profiles

Now that our VSC's have been created, we will define the Network Profiles. Our wireless deployment scenario called for setting up two different VSCs (Private and Public), each configured on their own independent VLAN.

1. From the main interface menu, select Controller -> Network -> Network Profiles
2. Create the Network Profile to be used for the Private VSC
    a. Click on Add New profile.
    b. Specify the name as Private.
    c. Enable the VLAN check box and specify the VLAN ID as 200.
    d. Click Save.
3. Create the Network Profile to be used for the Public VSC

a. Click on Add New Profile.
b. Specify the name as Public.
c. Enable the VLAN check box and specify the VLAN ID as 210.
d. Click Save.

Your Network Profiles should now be defined as follows (see *Figure 16*):

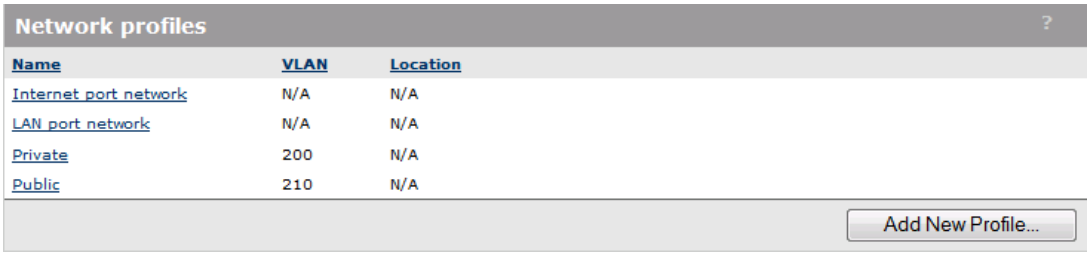


Figure 16

We will use these Network Profiles as we bind the Private VSC and Public VSC to the Default Group for our APs.

Default Group Binding

We are now ready to bind our newly created VSCs to the Default AP Group where our MSM 460 APs are located by default. To bind the VSCs to the Default AP Group, perform the following steps:

1. From the main interface menu, expand Controller -> Controlled APs -> Default Group
2. Click on VSC Bindings
3. Create VSC Binding for the Private VSC
    a. Click Add New Binding
    b. Select the previously created VSC Profile "Private"
    c. Enable the Egress Network checkbox and select the Network Profile "Private"
    d. We will broadcast the Private VSC on both radios, 2.4Ghz and 5Ghz, so leave the Dual Radio Behavior at the default setting.
    e. Click Save
4. Create the VSC Binding for the Public VSC
    a. Click Add New Binding
    b. Select the previously created VSC Profile "Public"
    c. Enable the Egress Network checkbox and select the Network Profile "Public"
    d. We will broadcast the Private VSC on both radios, 2.4Ghz and 5Ghz, so leave the Dual Radio Behavior at the default setting.
    e. Click Save

Your VSC Bindings to the Default AP Group should be defined as follows (see *Figure 17*):

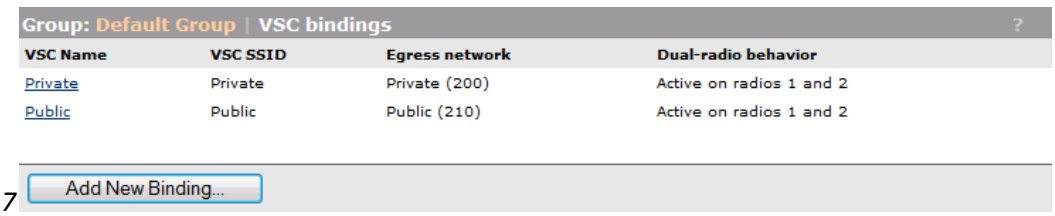


Figure 17

VIII. MSM 460 AP Defaults – Configuration

MSM 460 Radio Settings

For this scenario, we will pretend this wireless AP rollout and site survey was designed for capacity, as opposed to coverage. With that in mind, we will make several adjustments to the default radio configuration of the MSM 460s in an effort to reduce potential RF problems with channel overlap and signal saturation. The following MSM 460 radio configuration changes will be applied to the "Controlled APs" group, which all other AP groups, including the Default Group, inherit their settings from by default.

- Specify Radio 1 and Radio 2 auto-channel selection to occur once/day at 02:00 hours
- Exclude all Radio 2 channels except 1, 6, and 11 to minimize co-channel interference
- Set the maximum number of clients that can connect to a given radio at 75 for each radio
- Set the Distance Between APs value to Small for each radios as we have a rather dense AP rollout
- Change the power output for each radio from Maximum Power (100%) to 25% power

To implement these configuration changes, perform the following steps:

1. From the main interface menu, expand Controller -> Controlled APs -> Configuration -> Radio List and click on E-MSM460
2. Make the following changes on Radio 1 (5GHz Radio)
    a. Change Time Interval to Time of Day at 02:00 hours
    b. Set Max clients to 75
    c. Change Distance Between APs to Small
    d. Select the "Set power to" radio button and specific 25% of max power
3. Make the following changes on Radio 2 (2.4GHz Radio)
    a. Change Time Interval to Time of Day at 02:00 hours
    b. Select channels 2, 3, 4, 5, 7, 8, 9, 10 (using ctrl-click) in the Automatic Channel Exclusion List settings
    c. Set Max clients to 75
    d. Change Distance Between APs to Small
    e. Select the "Set power to" radio button and enter 14 dBm (25% power)
4. Click Save

Your E-MSM460 Radio Configuration settings should be defined as follows (see *Figure 18*):

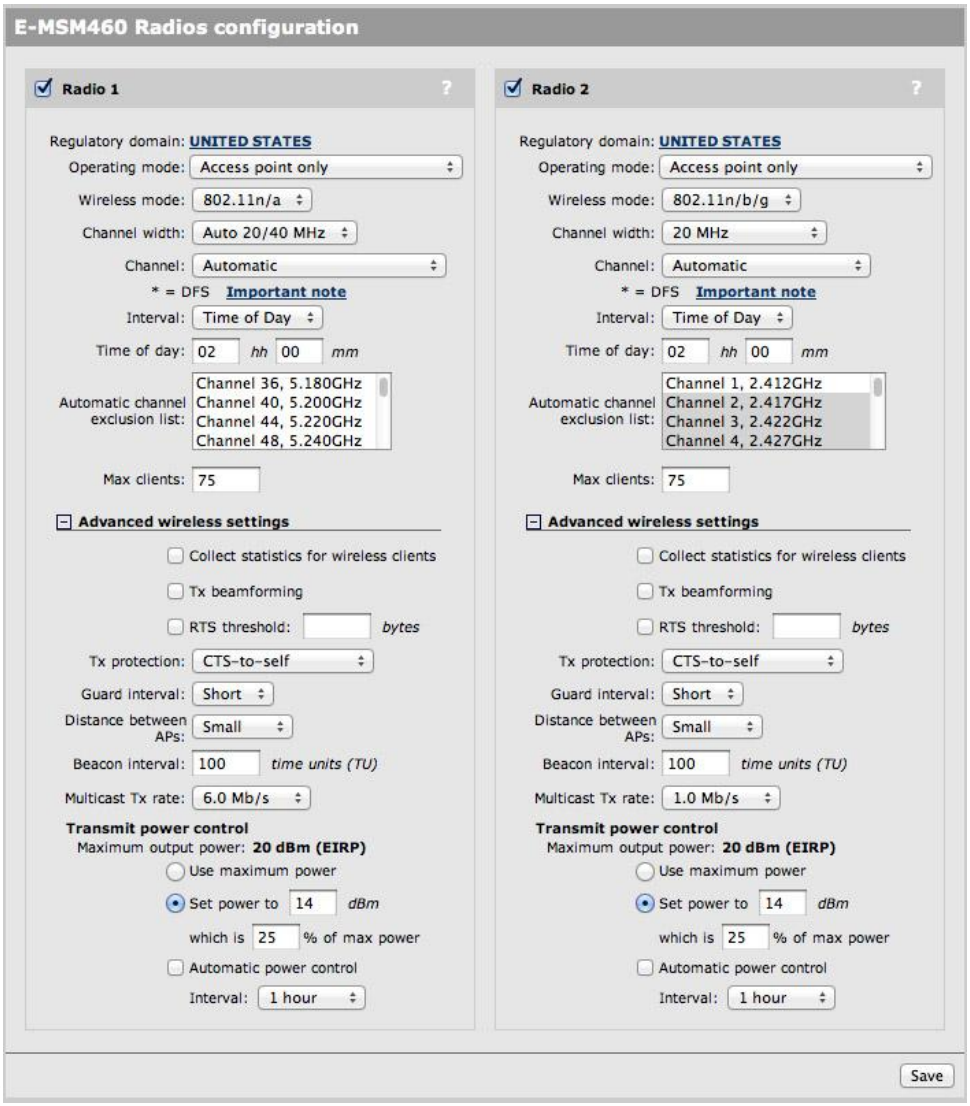


Figure 18

IX. Public Wireless – Creating User Accounts

Creating Users Accounts for use on the Public VSC wireless network

During the creation of our Public VSC, we enabled "HTML-based User Logins" so any guest users connecting to the Public VSC will be redirected to a splash page requiring logon credentials before they can access the internet. We need to define those user accounts now. In this particular scenario, we will create a single user account called "guest" that is will be shared by all users connecting to the Public VSC. To create the "guest" user account on the MSM 760 controller, perform the following steps:

1. From the main interface menu, click Users -> User Accounts
2. Click Add New Account
    a. Specify the User Name as "guest"

b. Specify the Password and Confirm Password as “guest1”
c. Since this is a shared account used by than one concurrent guest user, change the Max Concurrent Sessions to 255.
d. Enable the VSC Usage checkbox and restrict this account to the Public VSC only by selecting Public and clicking the right arrow button.
e. Verify your User Account settings reflect the following settings (see *Figure 19):*

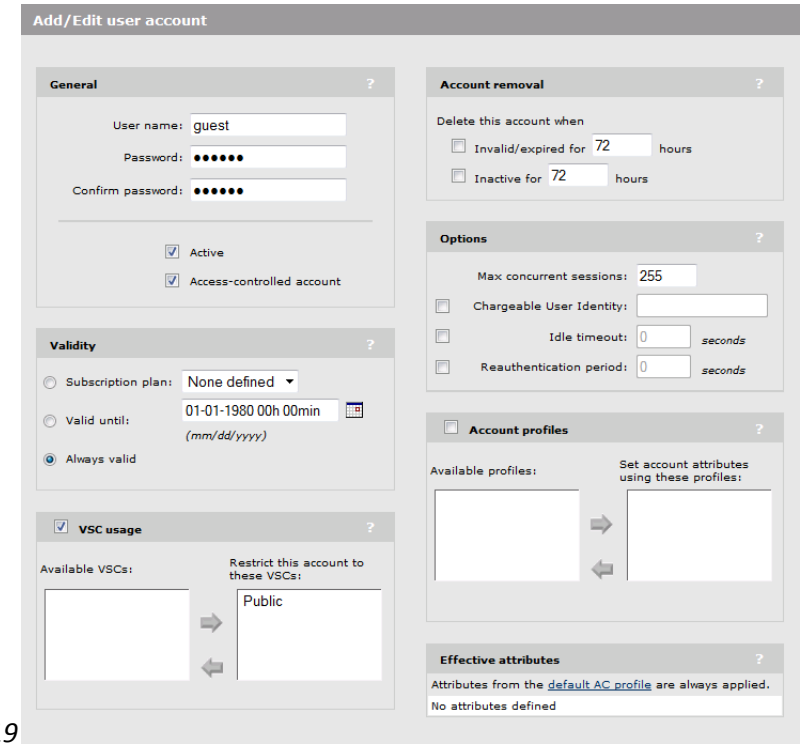


Figure 19

f. Click Save.

This “guest” user account can now be used to authenticate guest users connected to the Public VSC. Guest users will be automatically redirected to the splash page and required to enter the proper credentials before receiving internet access.

X. Public Wireless - Setup Access Control Lists

Create ACLs to limit access from the Public VSC to only specific network resources

With the creation of the Public VSC and creation of a “guest” user account, users with the appropriate logon information will be connected to the Public VSC after successfully authenticating on the HTML login redirect page. Since we specified the Public VSC to enforce the use of the Client Data Tunnel all traffic on the Public VSC will be tunneled through the controller. It is important we ensure that guest wireless users are prevented from accessing the production network and all related network resources. We will use the MSM 760 controller’s built-in ACL functionality to provide the following goals and restrictions for all guest wireless traffic.

- Allow the “guest” account direct access to the Internet

- Allow the “guest” account access to the company’s internal Web Server (172.20.100.50) on port 80
- Allow the “guest account access to the company’s internal Web Server (172.20.100.50) on port 443
- Deny the “guest” account access to ALL other production network and network resources

To achieve the goals mentioned above, perform the following steps for creating the ACLs:

1. From the main interface menu, click Public Access -> Attributes
2. Click Add New Attribute
    a. Select Default-User-Use-Access-List from the dropdown box and specify a value of Public (this will assign an access list called Public to ALL users authenticated by the MSM 760 Controller, including the “guest” account we created earlier and any new accounts we might create in the future).
    b. Click Add.
3. Click Add New Attribute
    a. Verify Access-List is selected in the Name dropdown box.
    b. Type “public,accept,tcp,172.20.100.50/32,80” (allow HTTP traffic to company’s internal web server).
    c. Click Add.
4. Click Add New Attribute
    a. Verify Access-list is selected in the Name dropdown box.
    b. Type “public,accept,tcp,172.20.100.50/32,443” (allow SSL traffic to company’s internal web server).
    c. Click Add.
5. Click Add New Attribute
    a. Verify Access-list is selected in the Name dropdown box.
    b. Type “public,deny,all,172.0.0.0/8,all” (block all traffic from the Public VSC to network resources).
    c. Click Add.
6. Click Add New Attribute
    a. Verify Access-list is selected in the Name dropdown box.
    b. Type “public,deny,all,10.0.0.0/8,all” (block all traffic from the Public VSC to network resources).
    c. Click Add.
7. Click Add New Attribute
    a. Verify Access-list is selected in the Name dropdown box.
    b. Type “public,accept,all,all,all” (allow all remaining traffic from the Public VSC)
    c. Click Add.

When complete, your ACLs should reflect the settings as shown in *Figure 20:*

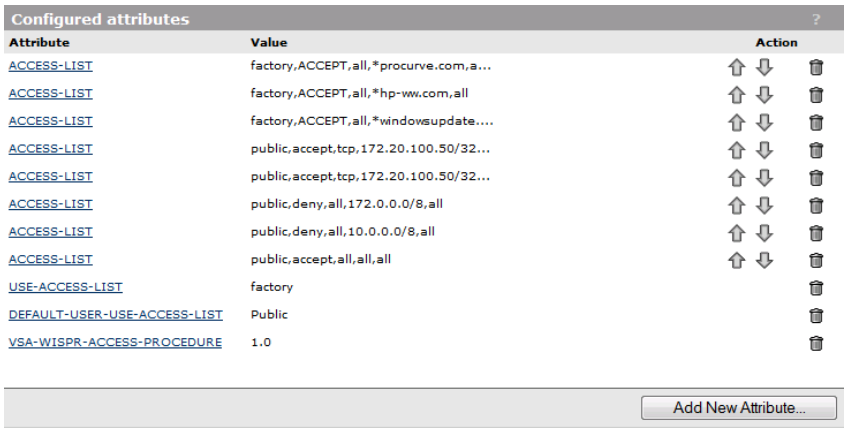


Figure 20

XI. Synchronize Changes and Test

Synchronize Changes and Test Implementation

Once all the configuration changes have been made on the MSM 760 controller, make sure to synchronize the changes to your Access Points.

1. From the main interface menu, in the Summary section on the left side, click on Unsynchronized.
2. Change the action to Synchronize Configuration.
3. Click Apply.

This may be a good time to take a backup configuration of the MSM 760 controller settings. Once complete, begin testing your wireless implementation by connecting clients to each of the VSCs that were created and verify successful connectivity.