# VIEW Certified Configuration Guide

# Trapeze Smart Mobile

## Mobility System for MP-372/422 APs

June 2009 Edition
1725-36194-001
Version C

## Trademark Information

Polycom® and the logo designs
SpectraLink®
LinkPlus
Link
NetLink
SVP
Are trademarks and registered trademarks of Polycom, Inc. in the United States of America and various countries. All other trademarks used herein are the property of their respective owners.

## Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

## Copyright Notice



Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

## Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY POLYCOM FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF POLYCOM WHATSOEVER.

## Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.
4750 Willow Road,
Pleasanton, CA 94588
http://www.polycom.com

# Introduction

Polycom's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink Wireless Telephones and wireless LAN (WLAN) infrastructure products.

The products listed below have been thoroughly tested in Polycom's lab and have passed VIEW Certification. This document details how to configure the Trapeze Networks Mobility Exchange (MX) switch and Mobility Point (MP) access point (AP) with SpectraLink Wireless Telephones***.

## Product Summary

| | | |
|---|---|---|
| Manufacturer: | Trapeze Networks: www.trapezenetworks.com | |
| Certified products: | Controllers:<br>MXR-2<br>MX-8†<br>MX-20<br>MX-200<br>MX-216†<br>MX-400<br>MX-2800 | Access Points:<br>MP-372†<br>MP-422† |
| Radio: | 2.4 GHz (802.11b), 5 GHz (802.11a) | |
| Security : | WEP, WPA-PSK, WPA2-PSK, and WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2)*** | |
| QoS: | SVP, Wi-Fi Standard*** | |
| AP and WLC software version tested: | 7.0.9.8.0 | |
| Handset models tested: | SpectraLink 8020/8030 Wireless Telephone* | |
| Handset software tested: | 131.019 | |
| Radio mode: | 802.11b | 802.11a |
| Maximum calls tested per AP: | 10 (SVP),<br>8 (Wi-Fi Standard QoS)*** | 12** (SVP),<br>9 (Wi-Fi Standard QoS)*** |
| Network topology: | Switched Ethernet (recommended) | |

† Denotes products directly used in VIEW Certification testing

*SpectraLink handset models 8020/8030 and their OEM derivates are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as "SpectraLink Wireless Telephones" or "handsets".

** Maximum calls tested during VIEW Certification. The certified product may actually support a higher number of maximum calls for 802.11a radio modes.

*** ONLY Release 3.0 capable handsets support WPA2-Enterprise and Wi-Fi Standard QoS. Release 3.0 may not be available for all Polycom or OEM branded handset models. To confirm that the proposed handsets support this capability, contact Polycom Customer Service.

## Service Information

If you encounter difficulties or have questions regarding the configuration process of the Mobility Exchange, please contact Trapeze Networks by calling 866 TRPZ TAC or 925 474 2400 or by e-mailing support@trapezenetworks.com.

## Known Limitations

- Only SpectraLink Wi-Fi Release 3.0 capable handsets support WPA2-Enterprise and Wi-Fi Standard QoS. Release 3.0 may not be available for all Polycom or OEM branded handset models. To confirm that the proposed handsets support this capability, contact Polycom Customer Service.
- All handsets operating on a given AP radio must have the same QoS setting. The APs must be configured to enable the corresponding features to support the handset QoS setting.
- Heavy multicast, broadcast or push-to-talk (PTT) traffic may impair voice quality.
- Voice and data must be separated onto separate service set identifiers (SSIDs) to obtain the best voice performance.
- You must disable Internet Group Management Protocol (IGMP) snooping when running SpectraLink Radio Protocol (SRP), which is used with the SpectraLink 8000 Telephony Gateway. SRP uses multicast packets to do an SRP Check-In, which are not forwarded through the Mobility Exchange Switch when IGMP snooping is enabled. NOTE: SRP does not support SpectraLink Wi-Fi Release 3.0 features, which means that neither Wi-Fi Standard QoS nor WPA2-Enterprise may be used in these deployments.

This document does not cover the steps involved to configure a RADIUS server required for using WPA2-Enterprise.

# Access Point Capacity and Positioning

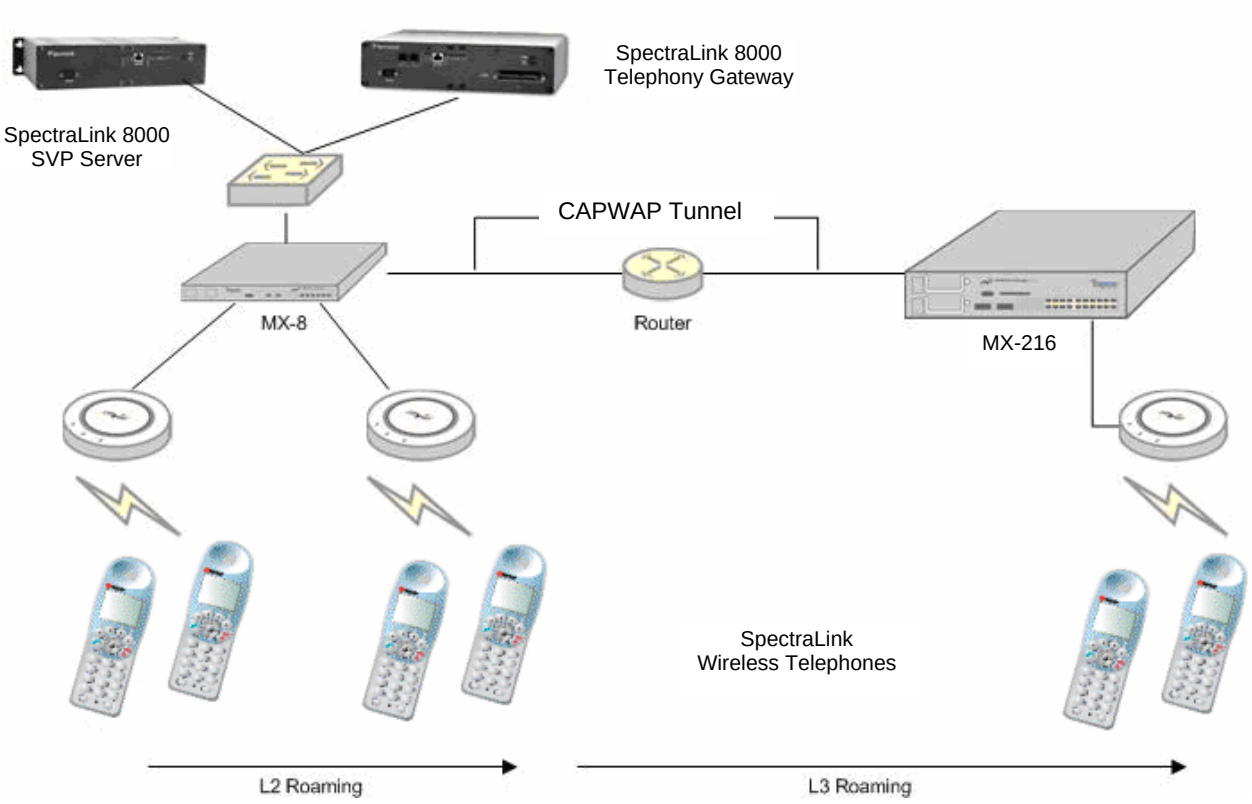
Please refer to the Polycom *Deploying Enterprise-Grade Wi-Fi Telephony* white paper. This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide for Deploying SpectraLink 8020/8030 Wireless Telephones*. This document identifies solutions based on Polycom's extensive experience in enterprise-class Wi-Fi telephony and provides recommendations for ensuring that a network environment is adequately optimized for use with SpectraLink 8020/8030 Wireless Telephones.

# Network Topology

It is important to note that this configuration is not necessarily applicable to all customer environments.

Both Layer-2 and Layer-3 roaming were tested. Layer-3 roaming of SpectraLink Wireless Telephones requires the use of Trapeze Networks Mobility Domain vlan tunneling.



# High-Level Concepts

Trapeze Mobility Controller configuration has two profiles:

- Radio
- Service

## Radio Profile

This is where parameters like DTIM interval and QoS mechanisms are customized. There can be only one radio profile assigned to one of the two radios in an AP. However, as can be seen in the example below there can be more than one service profile assigned to a radio profile. In this case the service profiles **common** and **wpa2** have been associated with the radio profile **wmmps**.

The output of the show command below provides an example of a radio profile configured for WMM-Power Save QoS mode:

```
# show radio-profile wmmps
Options
  802.11:       WMM-powersave
  QoS:          None
  Auto tune:    None
  RF-scanning:  None
  Other:        None

802.11
  Beacon interval:                100    Max Tx lifetime:                2000
  DTIM interval:                    2    Max Rx lifetime:                2000
  RTS threshold:                 2347    Frag threshold:                 2346

11n
  Channel width (11na):          40MHz

Auto tune
  Tune channel range (11a): lower-bands  Tune power interval:             600
  Tune channel interval:          3600   Power ramp interval:              60
  Channel holddown:                900

RF-scanning
  Mode:                        PASSIVE   Channel-scope:             OPERATING

Other
  Countermeasures:                none
  DFS channels:                 enabled
  QoS mode:                        wmm
    Queue       ACM  Max %  Police
```

```
    Background    NO       0       NO
    BestEffort    NO       0       NO
    Video        YES       0       NO
    Voice        YES       0       NO

Service profiles: common, wpa2e
Snoop filters: none
```

## Service Profile

The service profile is where attributes like the SSID name and security options are defined. A service profile is never directly associated with a particular radio on an AP. A service profile is only active when it is associated with a radio profile and the radio profile is associated with an AP.

The output of the show command below provides an example of a service profile with settings specific to WMM-Power Save QoS:

```
# show service-profile wpa2e
General attributes
  SSID name:  TALPHAX
  SSID type:  crypto

11n attributes
  11n Mode (na):           enabled
  11n Mode (ng):           enabled
  Guard Interval:          short
  Frame aggregation mode:  all
  MSDU Max length:         4k
  MPDU Max length:         64k

Options
  Auth:    Fallthru none
  Mesh:    None
  CAC:     None
  L2:      Proxy-ARP
  802.11:  Beacon, Idle-client-probing

Crypto
  Authentication:  802.1X
  Encryption:      RSN
  Cipher:          CCMP

SSID attributes
  Vlan name:  default

WEP
  Active-unicast-index:    1
  Active-multicast-index:  1
  Preset keys:             None

Web Portal
```

```
  Logout mode:      disabled
  Session timeout:  5

SODA
  Enforce checks:  enabled

Miscellaneous
  CAC max-sessions:     48
  Short retry counter:  5
  Long retry counter:   5
  Max bandwidth:        unlimited
  User idle timeout:    180 s

802.11 settings
  11a
    Beacon     rate:  6
    Multicast  rate:  AUTO
    Mandatory rates:  6, 12, 24
    Standard  rates:  9, 18, 36, 48, 54
    Disabled  rates:  None
  11b
    Beacon     rate:  2
    Multicast  rate:  AUTO
    Mandatory rates:  1, 2
    Standard  rates:  5.5, 11
    Disabled  rates:  None
  11g
    Beacon     rate:  2
    Multicast  rate:  AUTO
    Mandatory rates:  1, 2, 5.5, 11
    Standard  rates:  6, 9, 12, 18, 24, 36, 48, 54
    Disabled  rates:  None
  11na
    Beacon     rate:  6
    Multicast  rate:  AUTO
    Mandatory rates:  6, 12, 24
    Standard  rates:  9, 18, 36, 48, 54, m0, m1, m2, m3, m4, m5, m6, m7
                      m8, m9, m10, m11, m12, m13, m14, m15
    Disabled  rates:  None
  11ng
    Beacon     rate:  2
    Multicast  rate:  AUTO
    Mandatory rates:  1, 2, 5.5, 11
    Standard  rates:  6, 9, 12, 18, 24, 36, 48, 54, m0, m1, m2, m3, m4
                      m5, m6, m7, m8, m9, m10, m11, m12, m13, m14, m15
    Disabled  rates:  None
```

## Radio Profiles on an AP

This summary shows seven APs and the radio profiles associated with the two radios. **Radio 1** is the 2.4GHz (802.11b/g) radio band and **Radio 2** is the 5GHz (802.11a) radio band. In the configuration below the **wmmps** radio profile is associated with all of the A-Band radios and the **default** radio profile is associated with the B/G-Band radios.

To view which radio profiles are configured on the APs, use the following show command:

```
# show ap config
AP   AP Name          Model      Mode     Radio 1 profile  Radio 2 profile
---- ---------------- ---------- -------- ---------------- ----------------
   1 AP01             MP-422              default          wmmps
   2 AP02             MP-422              default          wmmps
   3 AP03             MP-422              default          wmmps
   4 AP04             MP-372              default          wmmps
   5 AP05             MP-372              default          wmmps
   6 AP06             MP-372              default          wmmps
  16 AP16             MP-432              default          wmmps
```

# Configure Controller from Factory Defaults

## Configuring Communication through the Console Port

1. Using a standard RS-232 cable, connect the **Mobility Exchange Switch** to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as Putty or HyperTerminal) or use a VT-100 terminal with the following configuration:

| | |
|---|---|
| Bits per second: | 9600 |
| Data bits: | 8 |
| Parity: | None |
| Stop bits: | 1 |
| Flow control: | None |

3. Press Enter three times to display the **Mobility Exchange Switch** login screen, and to get past the **Username** prompt and the **Password** prompt. There are no default usernames or passwords.
4. Type **enable** to enter privileged mode. The default password is blank.

## Configuring Communication through the Web Server

The Trapeze Web interface is known as WebView. This interface provides rudimentary configuration and monitoring, but many of the advanced configuration options need to be set through the command line interface.

Below is the set of commands enabling WebView. Note that the embedded Web server uses HTTPS, so the configuration of the crypto functions is required.

**Purpose**: Enable Web server.

**Command**: **set ip https server enable**

**Purpose**: Generate keys for security. Assuming username of **admin**, which is the default. Answer prompts as needed. Answer to Common Name prompt must be **admin.cert**

**Command**: **crypto generate key admin 1024**

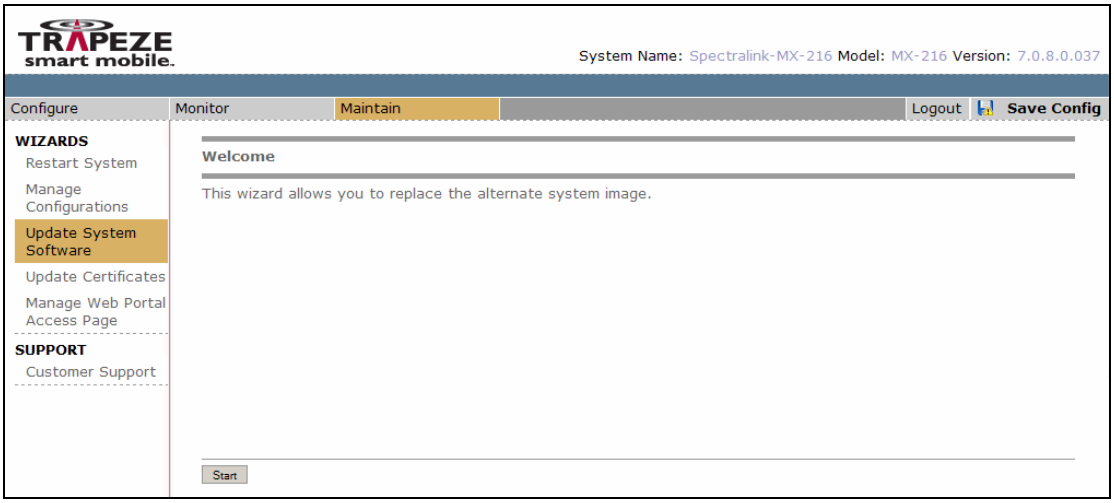
**Purpose**: Generate self-signed certificate.

**Command**: **crypto generate self-signed admin**

The username for WebView is "admin" and the password the enable password. The password for the "admin" user will not work as the password for WebView.

## Upgrade Firmware using WebView

Using WebView, click the **Maintain** tab and select **Update System Software** in the navigation pane on the left (see below). The wizard will guide you through the upgrade process.



# Configure VLAN, Ports and Security

## Common Parameters

### Purpose
Set controller name.

### Command
```
set system name <Name>
```

### Purpose
Set controller IP address.

### Command
```
set system ip-address <IP Address>
```

### Purpose
Set controller default route.

### Command
```
set ip route default <IP Address> <VLAN Number>
```

### Purpose
Configure VLAN IP address.

### Command
```
set interface <VLAN Number> ip <IP Address> <IP Mask>
```

### Purpose
Configure VLAN on ports used for APs and connected to the LAN.

### Command
```
set vlan 1 port <Port Number>
```

### Purpose
Enable Power-Over-Ethernet on ports used for APs.

### Command
```
set port poe <Port Number> enable
```

### Purpose
Enable Telnet. This is optional, but allows configuration through the CLI without requiring a serial cable.

### Command
```
set ip telnet server enable
```

## WMM Parameters

(No WMM specific VLAN or security settings required.)

## SVP Parameters

### Purpose
Place all SVP traffic (protocol 119) traffic in the class-of-service (CoS) queue 7.

### Command
```
set security ac lip SVP permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
```

### Purpose
(Optional) If data traffic is to be shared with voice traffic, it must be explicitly enabled.

### Commands
```
set security acl name svp permit 0.0.0.0 255.255.255.255
commit security acl svp
set security acl map svp vlan 1 out
set security acl map svp vlan 1 in
```

### Purpose
Disable Internet Group Management Protocol (IGMP) snooping on a designated VLAN. IGMP snooping must be disabled only when running SpectraLink Radio Protocol (SRP), which is used with the SpectraLink 8000 Telephony Gateway. SRP uses multicast packets to do an SRP Check-In. These packets are not forwarded through the Mobility Exchange Switch when IGMP snooping is enabled. NOTE: SRP does not support SpectraLink Wi-Fi Release 3.0 features, which means that neither Wi-Fi Standard QoS nor WPA2-Enterprise may be used in these deployments.

When a tunneled virtual LAN (VLAN) is configured over a Layer-3 network, IGMP snooping is turned on by default. IGMP snooping must be disabled each time the tunnel is established.

## Command

```
set igmp disable vlan <name of vlan>
```

# Configure Radio Profile

The radio profile configuration is described below and divided between the two types of QoS supported by the handsets. The handsets and an AP radio can only support one type of QoS mode (WMM-Power Save or SVP) at one time. There is a section for configuring the AP radios common radio-profile to both QoS modes and for each of the QoS modes.

The string **<profile name>** should be substituted with the radio profile name desired. The example configuration in the appendix uses **wmmps** for the WMM-Power Save QoS mode radio profile and **svp** for the SVP QoS mode radio profile.

## Common Parameters

### Purpose
Setting the DTIM interval to 2.

### Command
```
set radio-profile <profile name> dtim-interval 2
```

### Purpose
Prevent the AP from going off-channel to scan.

### Commands
```
set radio-profile <profile name> rf-scanning channel-scope
operating

set radio-profile <profile name> active-scan disable
```

### Purpose
Disable auto tune power.

### Command
```
set radio-profile <profile name> auto-tune power-config
disable
```

# WMM Parameters

### Purpose
Enable WMM-Power Save (UAPSD).

### Command
```
set radio-profile <profile name> wmm-powersave enable
```

### Purpose
Enable WMM QoS.

### Command
```
set radio-profile <profile name> qos-mode wmm
```

### Purpose
Enable Voice/Video admission control, disable policing, and configure max-utilization for each of the WMM access category queues. This setting is required if the handset is configured for **Mandatory** admission control (recommended) and optional if the handset is configured for **Optional** admission control. Enabling admission control for Voice/Video provides enterprise grade quality of service. Admission control is disabled by default for all access categories.

### Commands
```
set radio-profile <profile name> cac voice mode enable
set radio-profile <profile name> cac video mode enable
```

### Purpose
Disable policing for all access categories. The maximum utilization settings are set to recommended values for each access category. Policing is enabled by default on all access categories.

### Commands
```
set radio-profile <profile name> cac voice policing disable
set radio-profile <profile name> cac video policing disable
set radio-profile <profile name> cac best-effort policing
disable
set radio-profile <profile name> cac background policing
disable
```

### Purpose
Set the maximum utilization settings are set to recommended values for each access category. Maximum utilization is disabled (set to 0) by default.

### Commands

```
set radio-profile <profile name> cac voice max-utilization
80
set radio-profile <profile name> cac video max-utilization
20
set radio-profile <profile name> cac best-effort max-
utilization 0
set radio-profile <profile name> cac background max-
utilization 0
```

# SVP Parameters

## Purpose

Enable SVP QoS.

## Command

```
set radio-profile <profile name> qos-mode svp
```

# Review Settings

## Purpose

Review the radio profile settings. The results below are shown for a radio profile configured for WMM-Power Save.

## Command

**show radio-profile <profile name>**

## Result

```
Options
  802.11:       WMM-powersave
  QoS:          None
  Auto tune:    None
  RF-scanning:  None
  Other:        None

802.11
  Beacon interval:                  100    Max Tx lifetime:                 2000
  DTIM interval:                      2    Max Rx lifetime:                 2000
  RTS threshold:                   2347    Frag threshold:                  2346

11n
  Channel width (11na):           40MHz

Auto tune
  Tune channel range (11a): lower-bands    Tune power interval:              600
  Tune channel interval:            3600    Power ramp interval:              60
  Channel holddown:                  900

RF-scanning
  Mode:                          PASSIVE    Channel-scope:              OPERATING

Other
  Countermeasures:                  none
  DFS channels:                  enabled
  QoS mode:                          wmm
    Queue       ACM  Max %  Police
    Background   NO      0      NO
    BestEffort   NO      0      NO
    Video       YES     20      NO
    Voice       YES     80      NO

Service profiles: common, wpa2e
Snoop filters: none
```

# Configure Service Profile

## Common Parameters

### Purpose
Disable 11n aggregation.

### Command
```
set service-profile <profile-name> 11n frame-aggregation
disable
```

## WMM Parameters

### Purpose
Enable Proxy-ARP. This eliminates delays in audio at the start of a call and may be necessary for a phone in standby to ring when called.

### Command
```
set service-profile <profile name> proxy-arp enable
```

## SVP Parameters

### Purpose
Sets the number of short retires to 3

### Command
```
set service-profile <profile name> short-retry-count 3
```

## WEP Parameters

### Purpose
Configure SSID name.

### Command
```
set service-profile <profile name> ssid-name <SSID Name>
```

### Purpose
Authentication set to open access.

### Command

```
set service-profile <profile name> auth-fallthru last-
resort
```

### Purpose

Authentication set to shared access.

### Command

```
set service-profile <profile name> shared-key-auth enable
```

### Purpose

Set to 40-bit WEP security.

### Command

```
set service-profile <profile name> cipher-wep40 enable
```

### Purpose

Set to 104-bit WEP security (called 128-bit in the phone).

### Command

```
set service-profile <profile name> cipher-wep104 enable
```

### Purpose

Choose the key index and the key. Note: if a key index greater than 1 is used, the lower keys must be filled with a value of the correct number of digits.

### Command

```
set service-profile <profile name> wep key-index 1 key
<either 10 or 26 ASCII characters representing hexadecimal
digits>
```

### Purpose

Disable 802.1X Authentication

### Command

```
set service-profile <profile name> auth-dot1x disable
```

### Purpose

Associate the service profile with a VLAN

### Command

```
set service-profile <profile name> attr vlan-name <VLAN
Name>
```

# WPA-PSK Parameters

### Purpose
Configure SSID name.

### Command
```
set service-profile <profile name> ssid-name <SSID Name>
```

### Purpose
Authentication set to open access.

### Command
```
set service-profile <profile name> auth-fallthru last-
resort
```

### Purpose
Set to WPA security.

### Command
```
set service-profile <profile name> cipher-tkip enable
```

### Purpose
Enable WPA Security.

**Command**: `set service-profile <profile name> wpa-ie enable`

### Purpose
Configure Pre-Shared Key passphrase.

### Command
```
set service-profile <profile name> psk-phrase <passphrase>
```

### Purpose
Enable Pre-Shared Key Authentication.

### Command
```
set service-profile <profile name> auth-psk enable
```

### Purpose
Disable 802.1X Authentication.

### Command
```
set service-profile <profile name> auth-dot1x disable
```

### Purpose
Associate the service profile with a VLAN.

### Command
```
set service-profile <profile name> attr vlan-name <VLAN
Name>
```

## WPA2-PSK Parameters

### Purpose
Configure SSID name.

### Command
```
set service-profile <profile name> ssid-name <SSID Name>
```

### Purpose
Authentication set to open access.

### Command
```
set service-profile <profile name> auth-fallthru last-
resort
```

### Purpose
Enable WPA2-PSK Security cipher (AES-CCMP).

### Command
```
set service-profile <profile name> cipher-ccmp enable
```

### Purpose
Enable WPA2 Security.

### Command
```
set service-profile <profile name> rsn-ie enable
```

### Purpose
Configure PSK passphrase.

### Command
```
set service-profile <profile name> psk-phrase <passphrase>
```

### Purpose
Enable Pre-Shared Key Authentication.

### Command
```
set service-profile <profile name> auth-psk enable
```

### Purpose
Disable 802.1X Authentication.

### Command
```
set service-profile <profile name> auth-dot1x disable
```

### Purpose
Associate the service profile with a VLAN.

### Command
```
set service-profile <profile name> attr vlan-name default
```

## WPA2-Enterprise Parameters

### Purpose
Configure the SSID name.

### Command
```
set service-profile <profile name> ssid-name <SSID Name>
```

### Purpose
Enable WPA2-Enterprise (802.1X) Security.

### Commands
```
set service-profile <profile name> cipher-ccmp enable
set service-profile <profile name> rsn-ie enable
set service-profile <profile name> attr vlan-name default
```

## Review Settings

### Purpose
Review the service profile settings. The results below are shown for a radio profile configured for WMM-Power Save and WPA2-Enterprise security.

### Command
```
show service-profile <profile name>
```

## Result

```
General attributes
  SSID name:  TALPHAX
  SSID type:  crypto

11n attributes
  11n Mode (na):           enabled
  11n Mode (ng):           enabled
  Guard Interval:          short
  Frame aggregation mode:  all
  MSDU Max length:         4k
  MPDU Max length:         64k

Options
  Auth:    Fallthru none
  Mesh:    None
  CAC:     None
  L2:      Proxy-ARP
  802.11:  Beacon, Idle-client-probing

Crypto
  Authentication:  802.1X
  Encryption:      RSN
  Cipher:          CCMP

SSID attributes
  Vlan name:  default

WEP
  Active-unicast-index:    1
  Active-multicast-index:  1
  Preset keys:             None

Web Portal
  Logout mode:      disabled
  Session timeout:  5

SODA
  Enforce checks:  enabled

Miscellaneous
  CAC max-sessions:     48
  Short retry counter:  5
  Long retry counter:   5
  Max bandwidth:        unlimited
  User idle timeout:    180 s

802.11 settings
  11a
    Beacon     rate:  6
    Multicast  rate:  AUTO
    Mandatory rates:  6, 12, 24
    Standard  rates:  9, 18, 36, 48, 54
    Disabled  rates:  None
  11b
```

```
    Beacon     rate:  2
    Multicast  rate:  AUTO
    Mandatory rates:  1, 2
    Standard  rates:  5.5, 11
    Disabled  rates:  None
  11g
    Beacon     rate:  2
    Multicast  rate:  AUTO
    Mandatory rates:  1, 2, 5.5, 11
    Standard  rates:  6, 9, 12, 18, 24, 36, 48, 54
    Disabled  rates:  None
  11na
    Beacon     rate:  6
    Multicast  rate:  AUTO
    Mandatory rates:  6, 12, 24
    Standard  rates:  9, 18, 36, 48, 54, m0, m1, m2, m3, m4, m5, m6, m7
                      m8, m9, m10, m11, m12, m13, m14, m15
    Disabled  rates:  None
  11ng
    Beacon     rate:  2
    Multicast  rate:  AUTO
    Mandatory rates:  1, 2, 5.5, 11
    Standard  rates:  6, 9, 12, 18, 24, 36, 48, 54, m0, m1, m2, m3, m4
                      m5, m6, m7, m8, m9, m10, m11, m12, m13, m14, m15
    Disabled  rates:  None
```

# Configure APs

### Purpose
Set AP model and port.

### Command
```
set ap <ap #> port <port #> model <AP model>
```

### Purpose
Configure B-Band Radio (known as radio 1). In this example, the B-Radio is disabled.. The A-Band radio is known as radio 2.

### Command
```
set ap <ap #> radio 1 mode disable
```

### Purpose
Disable load balancing between APs. Repeat for all APs and radios.

### Command
```
set ap <ap #> radio <radio #> load-balancing disable
```

### Purpose
Configure A-Band Radio (known as radio 2). In this example, the A-Band radio is enabled, set to Channel 161 at 15dBm. The radio profile associated with the radio will be one that was configured for SVP or WMM-Power Save QoS.

### Command
```
set ap <ap #> radio 2 channel 161 radio-profile <radio
profile> mode enable tx-power 15
```

## Review Settings

### Purpose
Review AP configuration settings.

### Command
```
show ap config <ap #>
```

## Result

```
AP 16 (AP16)
  Model:                    MP-432
  Mode:
  Bias:                     high
  Power mode:               auto
  Options:                  upgrade-firmware
  Connection:               port 16
  Serial number:
  Fingerprint:
  Communication timeout:    25
  Location:
  Contact:
  Vlan-profile:
Radio 1 (802.11ng)
  Mode:                  disabled          Radio profile:          default
  Channel:               6                 Load balancing:         NO
  Tx power:              18                Load balancing group:
  Auto tune max power:   default           Force rebalance:        NO
  Antenna location:      indoors           Antenna type:           INTERNAL
  Service profiles:
    s1
    wpa2
    wpa2e
Radio 2 (802.11na)
  Mode:                  enabled           Radio profile:          wmmps
  Channel:               153               Load balancing:         NO
  Tx power:              11                Load balancing group:
  Auto tune max power:   default           Force rebalance:        NO
  Antenna location:      indoors           Antenna type:           INTERNAL
  Service profiles:
    common
    wpa2e
```

## Purpose

Summary of all APs' configuration settings. When the AP number is left out of the command a brief summary is displayed, as shown below.

## Command

**show ap config**

## Result

```
AP   AP Name          Model      Mode     Radio 1 profile  Radio 2 profile
---- ---------------- ---------- -------- ---------------- ----------------
   1 AP01             MP-422              default          wmmps
   2 AP02             MP-422              default          wmmps
   3 AP03             MP-422              default          wmmps
   4 AP04             MP-372              default          wmmps
   5 AP05             MP-372              default          wmmps
   6 AP06             MP-372              default          wmmps
  16 AP16             MP-432              default          wmmps
```

# Configure RADIUS Server Example (WPA2-Enterprise Only)

### Purpose

Configure a RADIUS server to be used by the Trapeze controller. Timeout, retransmit, and deadtime parameters may be customized as desired. The values in the command example are valid, but other values may also be used.

### Command

```
set radius server <Name of RADIUS Server> address <IP
Address of RADIUS Server> timeout 5 retransmit 3 deadtime 0
key <shared secret key>
```

### Purpose

Create a server group.

### Command

```
set server group CiscoACS members CiscoACSBoulder
```

### Purpose

Associate server group with an SSID configured for WPA2-Enterprise security using a server group as an external RADIUS server.

### Command

```
set authentication dot1x ssid <SSID Name> ** pass-through
CiscoACS
```

# Configure QoS

In addition to QoS parameters present in the radio and service profiles, there are system-wide settings. Only ingress (packets from the wire side of the switch) needs to be configured.

### Purpose

Set COS/DSCP Mappings for Voice packets. The specific values depend on how the call server is configured. Common values for DSCP values are 46 and 48.

### Command

```
set qos dscp-to-cos-map <DSCP Value> cos 6
```

### Purpose

Set COS/DSCP Mappings for Control packets. The specific values depend on how the call server is configured. Common values for DSCP values are 26 and 40.

### Command

```
set qos dscp-to-cos-map <DSCP Value> cos 4
```

# Configure Subnet Roaming

If more than one MX switch is used, then subnet roaming needs to be configured.

To set up subnet roaming between two switches, a mobility domain must be configured on both switches. Choose one of the switches to be the "seed MX switch."

The IP addresses used in mobility domain configuration must use the system IP address of each switch).

The following commands are performed on the "seed MX switch"

### Purpose

Configure the "seed MX switch" for a domain member.

### Commands

```
set system ip-address <system ip address>
set mobility-domain mode seed domain-name <domain name>
set mobility-domain member <member ip address>
```

The following commands are performed on the other (member) MX switch:

### Purpose

Configure the "member MX switch" for a seed MX switch.

### Commands

```
set system ip-address <system ip address>
set mobility-domain mode member seed-ip <member ip address>
```

### Purpose

Disable IGMP snooping temporarily on the MX that does NOT have the VLAN statically configured.

### Command

```
set igmp disable vlan <vlan name>
```

### Purpose

Clear an existing mobility domain before defining a new one.

### Command

```
clear mobility-domain
```

## Purpose

Check the mobility domain.

## Command

**show mobility-domain**

## Response

```
Mobility Domain name:  default
Member          State
1.1.1.1         STATE_UP     SEED
1.1.3.1         STATE_UP     MEMBER
```

# Monitoring

## QoS

### Purpose

Monitor which CoS queue traffic is being sent. Most of the traffic should be in the voice queue. If there is no traffic in the voice queue when voice traffic is present, then the DSCP mapping isn't working properly. This could be a result of missing DSCP values in the packets or a misconfigured Trapeze controller.

### Command

**show ap qos-stats**

### Response

```
CoS  Queue       Rx      Rx     Tx      Tx     Tx     Tx    Tx          Tx
                 kb/s    %      kb/s    %      %Req   %Max  Packets     Dropped
================================================================================
1,2  Background      <1    0       <1    0      0      0           0         0
0,3  BestEffort      <1    0       <1    0      0      0           0         0
4,5  Video           <1    0       <1    0      0      0           0         0
6,7  Voice           <1    0       <1    0      0      0           0         0
===> AP:0001 R:1     <1    0       <1    0

1,2  Background      <1    0       <1    0      0      0          13         2
0,3  BestEffort      <1    0       <1    0      0      0      211093       103
4,5  Video           98    3       <1    0      0      0           0         0
6,7  Voice          224    1      254    1      0      0       81192        42
===> AP:0001 R:2    322    4      254    1

1,2  Background      <1    0       <1    0      0      0           0         0
0,3  BestEffort      <1    0       <1    0      0      0           0         0
4,5  Video           <1    0       <1    0      0      0           0         0
6,7  Voice           <1    0       <1    0      0      0           0         0
===> AP:0016 R:1     <1    0       <1    0

1,2  Background      <1    0       <1    0      0      0          15         4
0,3  BestEffort      <1    0       <1    0      0      0       34159         1
4,5  Video           <1    0       <1    0      0      0           0         0
6,7  Voice           80    0       95    0      0      0        8488         4
===> AP:0016 R:2     80    0       95    0
```

# WPA2-Enterprise

### Purpose

View clients authenticated with the Trapeze controller APs. The response below shows two clients authenticated with WPA2-Enterprise and four with no WPA2-Enterprise-based authentication and no cipher for encrypting data.

### Command

**show dot1x clients**

### Response

```
   MAC Address        State          Vlan      Identity          cipher
  -------------      -------        ------    ----------        --------
00:90:7a:06:e8:9c Authenticated   default    eapuser           CCMP (RSN)
00:90:7a:06:e7:ad Authenticated   default    eapuser           CCMP (RSN)
00:90:7a:07:95:8a Authenticated   default    last-resort       NO-CIPHER
00:90:7a:05:42:fb Authenticated   default    last-resort       NO-CIPHER
00:90:7a:05:42:eb Authenticated   default    last-resort       NO-CIPHER
00:90:7a:07:11:c1 Authenticated   default    last-resort       NO-CIPHER
```

# Radio Performance

### Purpose

View counters on an AP and radio basis to inspect radio and other 802.11-related performance counters.

### Command

**show ap counters 16**

### Response

```
show ap counters 16

AP: 16               radio: 1
================================
Last packet transfer rate:       <unknown>
Tx packets count:                0         Rx packets count:        0
Clients in power save mode:      0         Multi packets drop:      0
Last packet Rx signal strength:  <unknown> Multi bytes drop:        0
Last packet signal noise ratio:  0         User sessions:           0
TKIP packets transfer count:     0         MIC error count:         0
TKIP packets replays:            0         TKIP decrypt errors:     0
CCMP packets decrypt errors:     0         CCMP packets replays:    0
CCMP packets transfer count:     0         Radio resets:            0
Radio receive physical errors:   0         Transmit retries:        0
Radio adjusted Tx power:         0         Noise floor:             0
802.3 Tx packets count:          0         802.3 Rx packets count:  0
No receive descriptor:           0         Invalid Rates            0
```

```
       TxUnicast TxMulticast                  Undcrypt
      Pkts Bytes Pkts Bytes RxPkts RxBytes Pkts Bytes PhyErr
-------------------------------------------------------------
 1.0:    0     0    0     0      0       0    0     0      0
 2.0:    0     0    0     0      0       0    0     0      0
 5.5:    0     0    0     0      0       0    0     0      0
 6.0:    0     0    0     0      0       0    0     0      0
 9.0:    0     0    0     0      0       0    0     0      0
11.0:    0     0    0     0      0       0    0     0      0
12.0:    0     0    0     0      0       0    0     0      0
18.0:    0     0    0     0      0       0    0     0      0
24.0:    0     0    0     0      0       0    0     0      0
36.0:    0     0    0     0      0       0    0     0      0
48.0:    0     0    0     0      0       0    0     0      0
54.0:    0     0    0     0      0       0    0     0      0
  m0:    0     0    0     0      0       0    0     0      0
  m1:    0     0    0     0      0       0    0     0      0
  m2:    0     0    0     0      0       0    0     0      0
  m3:    0     0    0     0      0       0    0     0      0
  m4:    0     0    0     0      0       0    0     0      0
  m5:    0     0    0     0      0       0    0     0      0
  m6:    0     0    0     0      0       0    0     0      0
  m7:    0     0    0     0      0       0    0     0      0
  m8:    0     0    0     0      0       0    0     0      0
  m9:    0     0    0     0      0       0    0     0      0
 m10:    0     0    0     0      0       0    0     0      0
 m11:    0     0    0     0      0       0    0     0      0
 m12:    0     0    0     0      0       0    0     0      0
 m13:    0     0    0     0      0       0    0     0      0
 m14:    0     0    0     0      0       0    0     0      0
 m15:    0     0    0     0      0       0    0     0      0
-------------------------------------------------------------
TOTL:    0     0    0     0      0       0    0     0      0

AP: 16               radio: 2
================================
Last packet transfer rate:       54
Tx packets count:                429034    Rx packets count:        70280
Clients in power save mode:      2         Multi packets drop:      0
Last packet Rx signal strength:  -27       Multi bytes drop:        0
Last packet signal noise ratio:  68        User sessions:           2
TKIP packets transfer count:     0         MIC error count:         0
TKIP packets replays:            0         TKIP decrypt errors:     0
CCMP packets decrypt errors:     0         CCMP packets replays:    0
CCMP packets transfer count:     76        Radio resets:            0
Radio receive physical errors:   0         Transmit retries:        3328
Radio adjusted Tx power:         11        Noise floor:             -96
802.3 Tx packets count:          0         802.3 Rx packets count:  0
No receive descriptor:           0         Invalid Rates            0
```

| | TxUnicast | | TxMulticast | | | | Undcrypt | | |
|---|---|---|---|---|---|---|---|---|---|
| | Pkts | Bytes | Pkts | Bytes | RxPkts | RxBytes | Pkts | Bytes | PhyErr |
| 6.0: | 11314 | 2660308 | 288678 | 77221365 | 0 | 0 | 0 | 0 | 17982 |
| 9.0: | 1 | 236 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12.0: | 173 | 42410 | 2787 | 360393 | 0 | 0 | 0 | 0 | 4 |
| 18.0: | 186 | 42606 | 2315 | 296529 | 0 | 0 | 0 | 0 | 8 |
| 24.0: | 170 | 33708 | 1435 | 189818 | 1289 | 134889 | 0 | 0 | 122 |
| 36.0: | 170 | 27604 | 2687 | 344545 | 377 | 66766 | 0 | 0 | 17 |
| 48.0: | 1476 | 294852 | 3058 | 389195 | 389 | 67417 | 0 | 0 | 5 |
| 54.0: | 89123 | 16205320 | 24641 | 3207296 | 68225 | 14064722 | 0 | 0 | 161 |
| m0: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 |
| m1: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m2: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m3: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m4: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m5: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m6: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m7: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m8: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m9: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m10: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| m11: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m12: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m13: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m14: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| m15: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| TOTL: | 102613 | 19307044 | 325601 | 82009141 | 70280 | 14333794 | 0 | 0 | 18308 |

# Appendix

## Configuration Example #1
## Minimal Configuration on a Single MX with WMM and SVP

Use the command sh**ow configuration** to display all non-default configuration parameters, as shown below. To include the default parameters in this output, use the command **show configuration all**.

This configuration contains radio profiles for both QoS methods supported on the Trapeze (WMM and SVP); however, recall that only one method can be used on any one radio at a time. This configuration shows only WMM QoS being used on APs "4" and "5" on the 2.4GHz radio (radio "1") and the 5GHz radio (radio "2").

```
# Configuration nvgen'd at 2009-3-24 08:09:35
# Image 7.0.9.8.0
# Model MX-8
# Last change occurred at 2009-3-24 08:09:05
set ip route default 172.29.104.1 1
set system name SystemTestTrapeze
set system ip-address 172.29.104.150
set system location Battery
set system countrycode US
set timezone mountain -8 0
set service-profile 1X ssid-name 1X
set service-profile 1X proxy-arp enable
set service-profile 1X cipher-ccmp enable
set service-profile 1X rsn-ie enable
set service-profile 1X 11n frame-aggregation disable
set service-profile 1X attr vlan-name default
set service-profile OPEN ssid-name OPEN
set service-profile OPEN ssid-type clear
set service-profile OPEN proxy-arp enable
set service-profile OPEN auth-fallthru last-resort
set service-profile OPEN auth-dot1x disable
set service-profile OPEN 11n frame-aggregation disable
set service-profile OPEN attr vlan-name default
set service-profile WEP0128 ssid-name WEP0128
set service-profile WEP0128 proxy-arp enable
set service-profile WEP0128 auth-fallthru last-resort
set service-profile WEP0128 wep key-index 1 key encrypted
12485744465a5e577e7a767b6764704053475152020 80a00005b55
set service-profile WEP0128 wep key-index 2 key encrypted
12485744465a5e577e7a767b6764704053475152020 80a00005b55
set service-profile WEP0128 wep key-index 3 key encrypted
1446405858517c7c7c71636470405343555 60e000802065d574d40
set service-profile WEP0128 wep active-unicast-index 3
```

```
set service-profile WEP0128 wep active-multicast-index 3
set service-profile WEP0128 cipher-wep104 enable
set service-profile WEP0128 auth-dot1x disable
set service-profile WEP0128 11n frame-aggregation disable
set service-profile WEP0128 attr vlan-name default
set service-profile WEP040 ssid-name WEP040
set service-profile WEP040 proxy-arp enable
set service-profile WEP040 auth-fallthru last-resort
set service-profile WEP040 wep key-index 1 key encrypted 014254570f5e505879151e
set service-profile WEP040 cipher-wep40 enable
set service-profile WEP040 auth-dot1x disable
set service-profile WEP040 11n frame-aggregation disable
set service-profile WEP040 attr vlan-name default
set service-profile WEPS128 ssid-name WEPS128
set service-profile WEPS128 auth-fallthru last-resort
set service-profile WEPS128 wep key-index 1 key encrypted
091d1c5a4d5041455355547b79777c6663754b5e465253050d0d05
set service-profile WEPS128 wep key-index 2 key encrypted
075e731f1a5c4f524f4b5b5d56797f717e646d7b4356445055030f
set service-profile WEPS128 wep key-index 3 key encrypted
1446405858517c7c7c71636470405343556560e000802065d574d40
set service-profile WEPS128 wep key-index 4 key encrypted
014254570f5e505879151e584b5643475d5b5c737b757a60617745
set service-profile WEPS128 wep active-unicast-index 4
set service-profile WEPS128 wep active-multicast-index 4
set service-profile WEPS128 cipher-wep104 enable
set service-profile WEPS128 shared-key-auth enable
set service-profile WEPS128 auth-dot1x disable
set service-profile WEPS128 attr vlan-name default
set service-profile WEPS40 ssid-name WEPS40
set service-profile WEPS40 proxy-arp enable
set service-profile WEPS40 auth-fallthru last-resort
set service-profile WEPS40 wep key-index 1 key encrypted 06575d72181b5f4e5d4e42
set service-profile WEPS40 wep key-index 2 key encrypted 101f5b4a5142445c545d7a
set service-profile WEPS40 wep active-unicast-index 2
set service-profile WEPS40 wep active-multicast-index 2
set service-profile WEPS40 cipher-wep40 enable
set service-profile WEPS40 shared-key-auth enable
set service-profile WEPS40 auth-dot1x disable
set service-profile WEPS40 11n frame-aggregation disable
set service-profile WEPS40 attr vlan-name default
set service-profile WMM ssid-name WMM
set service-profile WMM proxy-arp enable
set service-profile WMM cipher-ccmp enable
set service-profile WMM wpa-ie enable
set service-profile WMM rsn-ie enable
set service-profile WMM attr vlan-name default
set service-profile WPA ssid-name WPA
set service-profile WPA proxy-arp enable
set service-profile WPA auth-fallthru last-resort
set service-profile WPA cipher-tkip enable
set service-profile WPA wpa-ie enable
set service-profile WPA psk-encrypted
091c4f5d4a5c1644085a557a737d2c3165744a544e005803010e060256014e130d0e51005357025f5
d07535a525315
5f000209055d78141c5c41064247520a507d
set service-profile WPA auth-psk enable
```

```
set service-profile WPA auth-dot1x disable
set service-profile WPA 11n frame-aggregation disable
set service-profile WPA attr vlan-name default
set service-profile WPA2 ssid-name WPA2
set service-profile WPA2 proxy-arp enable
set service-profile WPA2 auth-fallthru last-resort
set service-profile WPA2 cipher-ccmp enable
set service-profile WPA2 rsn-ie enable
set service-profile WPA2 psk-encrypted
045f5a575b7319165f4c004e135c0d017f28212a67367a4253415154520b0f0a0508521e460801550
40a57055e5a0
2515d000042525408525059781548 5c1f0041
*AlcatrazTrapeze# show config
# Configuration nvgen'd at 2009-3-24 08:17:22
# Image 7.0.8.4.0
# Model MX-8
# Last change occurred at 2009-3-24 08:09:05
set ip route default 172.29.104.1 1
set system name AlcatrazTrapeze
set system ip-address 172.29.104.150
set system location Battery
set system countrycode US
set timezone mountain -8 0
set service-profile 1X ssid-name 1X
set service-profile 1X proxy-arp enable
set service-profile 1X cipher-ccmp enable
set service-profile 1X rsn-ie enable
set service-profile 1X 11n frame-aggregation disable
set service-profile 1X attr vlan-name default
set service-profile OPEN ssid-name OPEN
set service-profile OPEN ssid-type clear
set service-profile OPEN proxy-arp enable
set service-profile OPEN auth-fallthru last-resort
set service-profile OPEN auth-dot1x disable
set service-profile OPEN 11n frame-aggregation disable
set service-profile OPEN attr vlan-name default
set service-profile WEP0128 ssid-name WEP0128
set service-profile WEP0128 proxy-arp enable
set service-profile WEP0128 auth-fallthru last-resort
set service-profile WEP0128 wep key-index 1 key encrypted
12485744465a5e577e7a767b6764704053 47515202080a00005b55
set service-profile WEP0128 wep key-index 2 key encrypted
12485744465a5e577e7a767b6764704053 47515202080a00005b55
set service-profile WEP0128 wep key-index 3 key encrypted
1446405858517c7c7c71636470405343555 60e000802065d574d40
set service-profile WEP0128 wep active-unicast-index 3
set service-profile WEP0128 wep active-multicast-index 3
set service-profile WEP0128 cipher-wep104 enable
set service-profile WEP0128 auth-dot1x disable
set service-profile WEP0128 11n frame-aggregation disable
set service-profile WEP0128 attr vlan-name default
set service-profile WEP040 ssid-name WEP040
set service-profile WEP040 proxy-arp enable
set service-profile WEP040 auth-fallthru last-resort
set service-profile WEP040 wep key-index 1 key encrypted 014254570f5e505879151e
set service-profile WEP040 cipher-wep40 enable
set service-profile WEP040 auth-dot1x disable
```

```
set service-profile WEP040 11n frame-aggregation disable
set service-profile WEP040 attr vlan-name default
set service-profile WEPS128 ssid-name WEPS128
set service-profile WEPS128 auth-fallthru last-resort
set service-profile WEPS128 wep key-index 1 key encrypted
091d1c5a4d5041455355547b79777c6663754b5e465253050d0d05
set service-profile WEPS128 wep key-index 2 key encrypted
075e731f1a5c4f524f4b5b5d56797f717e646d7b4356445055030f
set service-profile WEPS128 wep key-index 3 key encrypted
1446405858517c7c7c7163647040534355560e000802065d574d40
set service-profile WEPS128 wep key-index 4 key encrypted
014254570f5e505879151e584b5643475d5b5c737b757a60617745
set service-profile WEPS128 wep active-unicast-index 4
set service-profile WEPS128 wep active-multicast-index 4
set service-profile WEPS128 cipher-wep104 enable
set service-profile WEPS128 shared-key-auth enable
set service-profile WEPS128 auth-dot1x disable
set service-profile WEPS128 attr vlan-name default
set service-profile WEPS40 ssid-name WEPS40
set service-profile WEPS40 proxy-arp enable
set service-profile WEPS40 auth-fallthru last-resort
set service-profile WEPS40 wep key-index 1 key encrypted 06575d72181b5f4e5d4e42
set service-profile WEPS40 wep key-index 2 key encrypted 101f5b4a5142445c545d7a
set service-profile WEPS40 wep active-unicast-index 2
set service-profile WEPS40 wep active-multicast-index 2
set service-profile WEPS40 cipher-wep40 enable
set service-profile WEPS40 shared-key-auth enable
set service-profile WEPS40 auth-dot1x disable
set service-profile WEPS40 11n frame-aggregation disable
set service-profile WEPS40 attr vlan-name default
set service-profile WMM ssid-name WMM
set service-profile WMM proxy-arp enable
set service-profile WMM cipher-ccmp enable
set service-profile WMM wpa-ie enable
set service-profile WMM rsn-ie enable
set service-profile WMM attr vlan-name default
set service-profile WPA ssid-name WPA
set service-profile WPA proxy-arp enable
set service-profile WPA auth-fallthru last-resort
set service-profile WPA cipher-tkip enable
set service-profile WPA wpa-ie enable
set service-profile WPA psk-encrypted
091c4f5d4a5c1644085a557a737d2c3165744a544e005803010e060256014e130d0e51005357025f5
d07535a525315
5f000209055d78141c5c41064247520a507d
set service-profile WPA auth-psk enable
set service-profile WPA auth-dot1x disable
set service-profile WPA 11n frame-aggregation disable
set service-profile WPA attr vlan-name default
set service-profile WPA2 ssid-name WPA2
set service-profile WPA2 proxy-arp enable
set service-profile WPA2 auth-fallthru last-resort
set service-profile WPA2 cipher-ccmp enable
set service-profile WPA2 rsn-ie enable
set service-profile WPA2 psk-encrypted
045f5a575b7319165f4c004e135c0d017f28212a67367a4253415154520b0f0a0508521e460801550
40a57055e5a0
```

```
2515d000042525408525059781548 5c1f0041
set service-profile WPA2 auth-psk enable
set service-profile WPA2 auth-dot1x disable
set service-profile WPA2 11n frame-aggregation disable
set service-profile WPA2 attr vlan-name default
set radius server ciscoacs address 172.29.65.9 encrypted-key 121d001b04021e05
set server group ciscoacsgrp members ciscoacs
set enablepass password b6b706525e1814394621eeb2a1c4d5803fcf
set authentication mac ssid any * local
set authentication dot1x ssid WMM ** pass-through ciscoacsgrp
set authentication dot1x ssid 1X ** pass-through ciscoacsgrp
set user admin password encrypted 11081d081e1c
set user eapuser password encrypted 011607144b1c
set radio-profile SVP
set radio-profile SVP dtim-interval 2
set radio-profile SVP rts-threshold 2347
set radio-profile SVP auto-tune channel-config disable
set radio-profile SVP rf-scanning mode passive
set radio-profile SVP rf-scanning channel-scope operating
set radio-profile SVP qos-mode svp
set radio-profile SVP service-profile OPEN
set radio-profile SVP service-profile WPA2
set radio-profile SVP service-profile WEP040
set radio-profile SVP service-profile 1X
set radio-profile SVP service-profile WEP0128
set radio-profile SVP service-profile WEPS40
set radio-profile SVP service-profile WEPS128
set radio-profile SVP service-profile WPA
set radio-profile WMM
set radio-profile WMM dtim-interval 2
set radio-profile WMM rf-scanning mode passive
set radio-profile WMM rf-scanning channel-scope operating
set radio-profile WMM wmm-powersave enable
set radio-profile WMM cac video mode enable
set radio-profile WMM cac voice mode enable
set radio-profile WMM cac video max-utilization 20
set radio-profile WMM cac voice max-utilization 80
set radio-profile WMM cac background policing disable
set radio-profile WMM cac best-effort policing disable
set radio-profile WMM cac video policing disable
set radio-profile WMM cac voice policing disable
set radio-profile WMM service-profile OPEN
set radio-profile WMM service-profile WEP040
set radio-profile WMM service-profile 1X
set radio-profile WMM service-profile WEPS40
set radio-profile WMM service-profile WEP0128
set radio-profile WMM service-profile WEPS128
set radio-profile WMM service-profile WPA
set radio-profile WMM service-profile WPA2
set ap 4 port 4 model MP-372
set ap 4 radio 1 radio-profile WMM mode disable
set ap 4 radio 2 radio-profile WMM mode disable
set ap 5 port 5 model MP-372
set ap 5 radio 1 radio-profile WMM mode disable
set ap 5 radio 1 load-balancing disable
set ap 5 radio 2 channel 60 radio-profile WMM mode disable tx-power 5
set ip telnet server enable
```

```
set port poe 1 enable
set port poe 2 enable
set port poe 3 enable
set port poe 4 enable
set port poe 5 enable
set port poe 6 enable
set vlan 1 port 3
set vlan 1 port 6
set vlan 1 port 7
set vlan 1 port 8
set interface 1 ip 172.29.104.150 255.255.255.0
set security acl name SVP permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
set security acl name SVP permit 0.0.0.0 255.255.255.255
commit security acl SVP
set security acl map SVP vlan 1 out
set security acl map SVP vlan 1 in
set qos dscp-to-cos-map 40 cos 4
set qos dscp-to-cos-map 46 cos 6
set ntp enable
set ntp server 172.29.65.2
```

# Configuration Example #2
# SVP Configuration for Single MX

For Reference Only

```
# General Configuration
set ip dns domain trpz.com
set ip dns enable
set ip route default 172.16.1.1 1
set log console enable severity error
set log session disable severity info
set log buffer enable severity error
set log trace enable severity debug
set log mark disable severity notice interval 300
set web-portal enable
set dot1x timeout supplicant 30
set dot1x timeout auth-server 30
set dot1x quiet-period 0
set dot1x reauth-max 2
set dot1x tx-period 5
set dot1x reauth-period 3600
set dot1x max-req 2
set dot1x key-tx enable
set dot1x reauth enable
set dot1x authcontrol enable
set dot1x wep-rekey-period 1800
set dot1x wep-rekey enable
set dot1x bonded-period 0
set system name VIEW
set prompt ""
set system ip-address 172.16.1.22
set system idle-timeout 0
```

```
set domain security none
set auto-config disable
set system countrycode US

# Security Profile
set service-profile SvpVoip ssid-name voip
set service-profile SvpVoip ssid-type clear
set service-profile SvpVoip beacon enable
set service-profile SvpVoip proxy-arp disable
set service-profile SvpVoip dhcp-restrict disable
set service-profile SvpVoip no-broadcast disable
set service-profile SvpVoip short-retry-count 3
set service-profile SvpVoip long-retry-count 5
set service-profile SvpVoip auth-fallthru last-resort
set service-profile SvpVoip soda mode disable
set service-profile SvpVoip soda enforce-checks enable
set service-profile SvpVoip max-bw 0
set service-profile SvpVoip cac-mode none
set service-profile SvpVoip cac-session 14
set service-profile SvpVoip user-idle-timeout 180
set service-profile SvpVoip idle-client-probing enable
set service-profile SvpVoip keep-initial-vlan enable
set service-profile SvpVoip web-portal-session-timeout 5
set service-profile SvpVoip wep active-unicast-index 1
set service-profile SvpVoip wep active-multicast-index 1
set service-profile SvpVoip cipher-tkip disable
set service-profile SvpVoip cipher-ccmp enable
set service-profile SvpVoip cipher-wep104 disable
set service-profile SvpVoip cipher-wep40 disable
set service-profile SvpVoip wpa-ie disable
set service-profile SvpVoip rsn-ie enable
set service-profile SvpVoip psk-encrypted  <password>
set service-profile SvpVoip auth-psk enable
set service-profile SvpVoip shared-key-auth disable
set service-profile SvpVoip tkip-mc-time 60000
set service-profile SvpVoip auth-dot1x disable
set service-profile SvpVoip mesh mode disable
set service-profile SvpVoip bridging disable
set service-profile SvpVoip load-balancing-exempt disable
set service-profile SvpVoip web-portal-logout mode disable
set service-profile SvpVoip 11n mode-na enable
set service-profile SvpVoip 11n mode-ng enable
set service-profile SvpVoip 11n short-guard-interval enable
set service-profile SvpVoip 11n frame-aggregation all
set service-profile SvpVoip 11n a-msdu-max-length 4k
set service-profile SvpVoip 11n a-mpdu-max-length 64k
set service-profile SvpVoip active-call-idle-timeout 120
set service-profile SvpVoip transmit-rate 11a mandatory 6.0,12.0,24.0 beacon-rate
6.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11b mandatory 1.0,2.0 beacon-rate 2.0
multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11g mandatory 1.0,2.0,5.5,11.0 beacon-
rate 2.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11na mandatory 6.0,12.0,24.0 beacon-
rate 6.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11ng mandatory 1.0,2.0,5.5,11.0 beacon-
rate 2.0 multicast-rate AUTO
```

```
set service-profile SvpVoip attr vlan-name Vln
set radius deadtime 0
set radius timeout 5
set radius retransmit 3
set radius das-port 3799
set enablepass password <password>
set authentication mac ssid any * local
set user admin password encrypted <password>

# AP Radio Profile
set radio-profile default beacon-interval 100
set radio-profile default dtim-interval 3
set radio-profile default max-tx-lifetime 2000
set radio-profile default max-rx-lifetime 2000
set radio-profile default rts-threshold 65535
set radio-profile default frag-threshold 2346
set radio-profile default preamble-length short
set radio-profile default auto-tune channel-config disable
set radio-profile default auto-tune 11a-channel-range lower-bands
set radio-profile default auto-tune ignore-clients disable
set radio-profile default auto-tune power-config disable
set radio-profile default auto-tune channel-interval 3600
set radio-profile default auto-tune power-interval 600
set radio-profile default auto-tune power-ramp-interval 60
set radio-profile default auto-tune channel-holddown 900
set radio-profile default countermeasures none
set radio-profile default rf-scanning mode active
set radio-profile default rf-scanning channel-scope operating
set radio-profile default rf-scanning cts-to-self disable
set radio-profile default rfid-mode disable
set radio-profile default wmm-powersave disable
set radio-profile default qos-mode svp
set radio-profile default weighted-fair-queuing disable
set radio-profile default rate-enforcement disable
set radio-profile default dfs-channels disable
set radio-profile default 11n channel-width-na 40MHz
set radio-profile default cac background mode disable
set radio-profile default cac best-effort mode disable
set radio-profile default cac video mode disable
set radio-profile default cac voice mode disable
set radio-profile default cac background max-utilization 0
set radio-profile default cac best-effort max-utilization 0
set radio-profile default cac video max-utilization 0
set radio-profile default cac voice max-utilization 0
set radio-profile default cac background policing disable
set radio-profile default cac best-effort policing disable
set radio-profile default cac video policing disable
set radio-profile default cac voice policing disable
set radio-profile default service-profile SvpVoip

# AP Basic Configuration
set ap 1 port 4 model MP-422 radiotype 11g
set ap 1 name AP04
set ap 1 bias high
set ap 1 blink disable
set ap 1 upgrade-firmware enable
set ap 1 force-image-download disable
```

```
set ap 1 time-out 25
set ap 1 power-mode auto
set ap 1 radio 1 channel 6 radio-profile default mode enable antenna-location
indoors antennatype INTERNAL tx-power 9
set ap 1 radio 1 auto-tune max-power default
set ap 1 radio 1 load-balancing enable
set ap 1 radio 2 channel 36 radio-profile default mode disable antenna-location
indoors antennatype INTERNAL tx-power 18
set ap 1 radio 2 auto-tune max-power default
set ap 1 radio 2 load-balancing enable
set ap 1 local-switching mode disable vlan-profile default

# IP services and port configuration
set arp agingtime 1200
set ip https server enable
set ip telnet server enable
set ip telnet 23
set ip snmp server disable
set ip ssh server enable
set ip ssh 22
set load-balancing mode disable
set load-balancing strictness low
set band-preference none
set port enable 1
set port speed 1 AUTO
set port duplex 1 full
set port trap 1 disableset port trap 1 NO
# Set additional ports as appropriate.

# SNMP Configuration
set snmp protocol v1 enable
set snmp protocol v2c disable
set snmp protocol usm disable

# VLAN Configuration
set vlan tagtype dot1q
set vlan 1 name Vln tunnel-affinity 5
set vlan 1 port 1
set vlan 1 port 2
# add ports to vlan as appropriate

set spantree backbonefast disable
set spantree uplinkfast disable
set spantree fwddelay 15 vlan 1
set spantree hello 2 vlan 1
set spantree maxage 20 vlan 1
set spantree priority  32768 vlan 1
set spantree disable vlan 1
set spantree enable port 1 1
set spantree portpri 1 priority 128
set spantree portfast 1 disable
set igmp disable vlan 1
set igmp proxy-report enable vlan 1
set igmp querier disable vlan 1
set igmp mrsol disable vlan 1
set igmp version 2 vlan 1
set igmp mrsol mrsi 30 vlan 1
```

```
set igmp qi 125 vlan 1
set igmp oqi 255 vlan 1
set igmp qri 100 vlan 1
set igmp lmqi 10 vlan 1
set igmp rv 2 vlan 1
set igmp mrouter port 1 disable
set igmp receiver port 1 disable
# disable router and receivers on other ports as appropriate
set fdb agingtime 1 age 300
set interface 1 ip 172.16.1.22 255.255.255.0
set interface 1 ip dhcp-server disable start 192.168.100.2 stop 192.168.100.254
set snmp notify profile default drop all
set mobility-domain mode seed domain-name mobdom
set mobility-domain member 172.16.2.20
set rfdetect classification ssid-masquerade rogue
set rfdetect classification seen-in-network rogue
set rfdetect classification ad-hoc skip-test
set rfdetect classification default-classification suspect
set rfdetect log enable
set rfdetect countermeasures mode normal
set rfdetect signature enable
set rfdetect voice-ext snr-threshold 12
set security acl hit-sample-rate 0
set security acl name svp permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
set security acl name svp permit 0.0.0.0 255.255.255.255
commit security acl svp
set security acl map svp vlan 1 in
set security acl map svp vlan 1 out
set qos dscp-to-cos-map 1 cos 0
set qos dscp-to-cos-map 2 cos 0
set qos dscp-to-cos-map 3 cos 0
set qos dscp-to-cos-map 4 cos 0
set qos dscp-to-cos-map 5 cos 0
set qos dscp-to-cos-map 6 cos 0
set qos dscp-to-cos-map 7 cos 0
set qos dscp-to-cos-map 8 cos 1
set qos dscp-to-cos-map 9 cos 1
set qos dscp-to-cos-map 10 cos 1
set qos dscp-to-cos-map 11 cos 1
set qos dscp-to-cos-map 12 cos 1
set qos dscp-to-cos-map 13 cos 1
set qos dscp-to-cos-map 14 cos 1
set qos dscp-to-cos-map 15 cos 1
set qos dscp-to-cos-map 16 cos 2
set qos dscp-to-cos-map 17 cos 2
set qos dscp-to-cos-map 18 cos 2
set qos dscp-to-cos-map 19 cos 2
set qos dscp-to-cos-map 20 cos 2
set qos dscp-to-cos-map 21 cos 2
set qos dscp-to-cos-map 22 cos 2
set qos dscp-to-cos-map 23 cos 2
set qos dscp-to-cos-map 24 cos 3
set qos dscp-to-cos-map 25 cos 3
set qos dscp-to-cos-map 26 cos 3
set qos dscp-to-cos-map 27 cos 3
set qos dscp-to-cos-map 28 cos 3
```

```
set qos dscp-to-cos-map 29 cos 3
set qos dscp-to-cos-map 30 cos 3
set qos dscp-to-cos-map 31 cos 3
set qos dscp-to-cos-map 32 cos 4
set qos dscp-to-cos-map 33 cos 4
set qos dscp-to-cos-map 34 cos 4
set qos dscp-to-cos-map 35 cos 4
set qos dscp-to-cos-map 36 cos 4
set qos dscp-to-cos-map 37 cos 4
set qos dscp-to-cos-map 38 cos 4
set qos dscp-to-cos-map 39 cos 4
set qos dscp-to-cos-map 40 cos 5
set qos dscp-to-cos-map 41 cos 5
set qos dscp-to-cos-map 42 cos 5
set qos dscp-to-cos-map 43 cos 5
set qos dscp-to-cos-map 44 cos 5
set qos dscp-to-cos-map 45 cos 5
set qos dscp-to-cos-map 46 cos 5
set qos dscp-to-cos-map 47 cos 5
set qos dscp-to-cos-map 48 cos 6
set qos dscp-to-cos-map 49 cos 6
set qos dscp-to-cos-map 50 cos 6
set qos dscp-to-cos-map 51 cos 6
set qos dscp-to-cos-map 52 cos 6
set qos dscp-to-cos-map 53 cos 6
set qos dscp-to-cos-map 54 cos 6
set qos dscp-to-cos-map 55 cos 6
set qos dscp-to-cos-map 56 cos 7
set qos dscp-to-cos-map 57 cos 7
set qos dscp-to-cos-map 58 cos 7
set qos dscp-to-cos-map 59 cos 7
set qos dscp-to-cos-map 60 cos 7
set qos dscp-to-cos-map 61 cos 7
set qos dscp-to-cos-map 62 cos 7
set qos dscp-to-cos-map 63 cos 7
set qos cos-to-dscp-map 1 dscp 8
set qos cos-to-dscp-map 2 dscp 16
set qos cos-to-dscp-map 3 dscp 24
set qos cos-to-dscp-map 4 dscp 32
set qos cos-to-dscp-map 5 dscp 40
set qos cos-to-dscp-map 6 dscp 48
set qos cos-to-dscp-map 7 dscp 56
set ntp disable
set ntp update-interval 64
```

# Configuration Example #3
# SVP Configuration For Multiple MX's (Subnet Roaming)

For Reference Only

SEED MX

```
# General Configuration
set ip dns domain trpz.com
set ip dns disable
set ip route default 172.16.1.1 1
set log console enable severity error
set log session disable severity info
set log buffer enable severity error
set log trace enable severity debug
set log mark disable severity notice interval 300
set web-portal enable
set dot1x timeout supplicant 30
set dot1x timeout auth-server 30
set dot1x quiet-period 0
set dot1x reauth-max 2
set dot1x tx-period 5
set dot1x reauth-period 3600
set dot1x max-req 2
set dot1x key-tx enable
set dot1x reauth enable
set dot1x authcontrol enable
set dot1x wep-rekey-period 1800
set dot1x wep-rekey enable
set dot1x bonded-period 0
set system name VIEW_Seed
set prompt ""
set system ip-address 172.16.1.22
set system idle-timeout 0
set domain security none
set auto-config disable
set system countrycode US



# Security Profile
set service-profile SvpVoip ssid-name voip
set service-profile SvpVoip ssid-type clear
set service-profile SvpVoip beacon enable
set service-profile SvpVoip proxy-arp disable
set service-profile SvpVoip dhcp-restrict disable
set service-profile SvpVoip no-broadcast disable
set service-profile SvpVoip short-retry-count 3
set service-profile SvpVoip long-retry-count 5
set service-profile SvpVoip auth-fallthru last-resort
set service-profile SvpVoip soda mode disable
set service-profile SvpVoip soda enforce-checks enable
set service-profile SvpVoip max-bw 0
set service-profile SvpVoip cac-mode none
set service-profile SvpVoip cac-session 14
set service-profile SvpVoip user-idle-timeout 180
set service-profile SvpVoip idle-client-probing enable
set service-profile SvpVoip keep-initial-vlan enable
set service-profile SvpVoip web-portal-session-timeout 5
```

```
set service-profile SvpVoip wep active-unicast-index 1
set service-profile SvpVoip wep active-multicast-index 1
set service-profile SvpVoip cipher-tkip disable
set service-profile SvpVoip cipher-ccmp enable
set service-profile SvpVoip cipher-wep104 disable
set service-profile SvpVoip cipher-wep40 disable
set service-profile SvpVoip wpa-ie disable
set service-profile SvpVoip rsn-ie enable
set service-profile SvpVoip psk-encrypted <password>
set service-profile SvpVoip auth-psk enable
set service-profile SvpVoip shared-key-auth disable
set service-profile SvpVoip tkip-mc-time 60000
set service-profile SvpVoip auth-dot1x disable
set service-profile SvpVoip mesh mode disable
set service-profile SvpVoip bridging disable
set service-profile SvpVoip load-balancing-exempt disable
set service-profile SvpVoip web-portal-logout mode disable
set service-profile SvpVoip 11n mode-na enable
set service-profile SvpVoip 11n mode-ng enable
set service-profile SvpVoip 11n short-guard-interval enable
set service-profile SvpVoip 11n frame-aggregation all
set service-profile SvpVoip 11n a-msdu-max-length 4k
set service-profile SvpVoip 11n a-mpdu-max-length 64k
set service-profile SvpVoip active-call-idle-timeout 120
set service-profile SvpVoip transmit-rate 11a mandatory 6.0,12.0,24.0 beacon-rate
6.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11b mandatory 1.0,2.0 beacon-rate 2.0
multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11g mandatory 1.0,2.0,5.5,11.0 beacon-
rate 2.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11na mandatory 6.0,12.0,24.0 beacon-
rate 6.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11ng mandatory 1.0,2.0,5.5,11.0 beacon-
rate 2.0 multicast-rate AUTO
set service-profile SvpVoip attr vlan-name VlnSeed
set radius deadtime 0
set radius timeout 5
set radius retransmit 3
set radius das-port 3799
set enablepass password <password>
set authentication mac ssid any * local
set user admin password encrypted <password>

# AP Radio Profile
set radio-profile default beacon-interval 100
set radio-profile default dtim-interval 3
set radio-profile default max-tx-lifetime 2000
set radio-profile default max-rx-lifetime 2000
set radio-profile default rts-threshold 65535
set radio-profile default frag-threshold 2346
set radio-profile default preamble-length short
set radio-profile default auto-tune channel-config disable
set radio-profile default auto-tune 11a-channel-range lower-bands
set radio-profile default auto-tune ignore-clients disable
set radio-profile default auto-tune power-config disable
set radio-profile default auto-tune channel-interval 3600
set radio-profile default auto-tune power-interval 600
```

```
set radio-profile default auto-tune power-ramp-interval 60
set radio-profile default auto-tune channel-holddown 900
set radio-profile default countermeasures none
set radio-profile default rf-scanning mode active
set radio-profile default rf-scanning channel-scope operating
set radio-profile default rf-scanning cts-to-self disable
set radio-profile default rfid-mode disable
set radio-profile default wmm-powersave disable
set radio-profile default qos-mode svp
set radio-profile default weighted-fair-queuing disable
set radio-profile default rate-enforcement disable
set radio-profile default dfs-channels disable
set radio-profile default 11n channel-width-na 40MHz
set radio-profile default cac background mode disable
set radio-profile default cac best-effort mode disable
set radio-profile default cac video mode disable
set radio-profile default cac voice mode disable
set radio-profile default cac background max-utilization 0
set radio-profile default cac best-effort max-utilization 0
set radio-profile default cac video max-utilization 0
set radio-profile default cac voice max-utilization 0
set radio-profile default cac background policing disable
set radio-profile default cac best-effort policing disable
set radio-profile default cac video policing disable
set radio-profile default cac voice policing disable
set radio-profile default service-profile SvpVoip

# AP Basic Configuration
set ap 1 port 4 model MP-422 radiotype 11g
set ap 1 name AP04
set ap 1 bias high
set ap 1 blink disable
set ap 1 upgrade-firmware enable
set ap 1 force-image-download disable
set ap 1 time-out 25
set ap 1 power-mode auto
set ap 1 radio 1 channel 6 radio-profile default mode enable antenna-location
indoors antennatype INTERNAL tx-power 9
set ap 1 radio 1 auto-tune max-power default
set ap 1 radio 1 load-balancing enable
set ap 1 radio 2 channel 36 radio-profile default mode disable antenna-location
indoors antennatype INTERNAL tx-power 18
set ap 1 radio 2 auto-tune max-power default
set ap 1 radio 2 load-balancing enable
set ap 1 local-switching mode disable vlan-profile default

# IP services and port configuration
set arp agingtime 1200
set ip https server enable
set ip telnet server enable
set ip telnet 23
set ip snmp server disable
set ip ssh server enable
set ip ssh 22
set load-balancing mode disable
set load-balancing strictness low
set band-preference none
```

```
set port enable 1
set port speed 1 AUTO
set port duplex 1 full
set port trap 1 disable
# Set additional ports as appropriate.

# SNMP Configuration
set snmp protocol v1 enable
set snmp protocol v2c disable
set snmp protocol usm disable


# VLAN Configuration
set vlan tagtype dot1q
set vlan 1 name VlnSeed tunnel-affinity 5
set vlan 1 port 19
set vlan 1 port 1
set vlan 1 port 2
# Add ports to vlan as appropriate.

# Spanning Tree Configuration
set spantree backbonefast disable
set spantree uplinkfast disable
set spantree fwddelay 15 vlan 1
set spantree hello 2 vlan 1
set spantree maxage 20 vlan 1
set spantree priority  32768 vlan 1
set spantree disable vlan 1
set spantree enable port 1 1
set spantree portpri 1 priority 128
set spantree portfast 1 disable
set spantree enable port 2 1
set spantree portpri 2 priority 128
set spantree portfast 2 disable
#Configure ports as needed.

# IGMP Configuration
set igmp disable vlan 1
set igmp proxy-report enable vlan 1
set igmp querier disable vlan 1
set igmp mrsol disable vlan 1
set igmp version 2 vlan 1
set igmp mrsol mrsi 30 vlan 1
set igmp qi 125 vlan 1
set igmp oqi 255 vlan 1
set igmp qri 100 vlan 1
set igmp lmqi 10 vlan 1
set igmp rv 2 vlan 1
set igmp mrouter port 19 disable
set igmp receiver port 19 disable
set igmp mrouter port 1 disable
set igmp receiver port 1 disable
set igmp mrouter port 2 disable
set igmp receiver port 2 disable
# Configure additional ports as needed
```

```
set fdb agingtime 1 age 300
set interface 1 ip 172.16.1.22 255.255.255.0
set interface 1 ip dhcp-server disable start 192.168.100.2 stop 192.168.100.254
set snmp notify profile default drop all

# Mobility Domain configuration
set mobility-domain mode seed domain-name mobdom
set mobility-domain member 172.16.2.20
set rfdetect classification ssid-masquerade rogue
set rfdetect classification seen-in-network rogue
set rfdetect classification ad-hoc skip-test
set rfdetect classification default-classification suspect
set rfdetect log enable
set rfdetect countermeasures mode normal
set rfdetect signature enable
set rfdetect voice-ext snr-threshold 12
set security acl hit-sample-rate 0

# VIEW ACL configuration
set security acl name svp permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
set security acl name svp permit 0.0.0.0 255.255.255.255
commit security acl svp
set security acl map svp vlan 1 in
set security acl map svp vlan 1 out

# QoS Settings
set qos dscp-to-cos-map 1 cos 0
set qos dscp-to-cos-map 2 cos 0
set qos dscp-to-cos-map 3 cos 0
set qos dscp-to-cos-map 4 cos 0
set qos dscp-to-cos-map 5 cos 0
set qos dscp-to-cos-map 6 cos 0
set qos dscp-to-cos-map 7 cos 0
set qos dscp-to-cos-map 8 cos 1
set qos dscp-to-cos-map 9 cos 1
set qos dscp-to-cos-map 10 cos 1
set qos dscp-to-cos-map 11 cos 1
set qos dscp-to-cos-map 12 cos 1
set qos dscp-to-cos-map 13 cos 1
set qos dscp-to-cos-map 14 cos 1
set qos dscp-to-cos-map 15 cos 1
set qos dscp-to-cos-map 16 cos 2
set qos dscp-to-cos-map 17 cos 2
set qos dscp-to-cos-map 18 cos 2
set qos dscp-to-cos-map 19 cos 2
set qos dscp-to-cos-map 20 cos 2
set qos dscp-to-cos-map 21 cos 2
set qos dscp-to-cos-map 22 cos 2
set qos dscp-to-cos-map 23 cos 2
set qos dscp-to-cos-map 24 cos 3
set qos dscp-to-cos-map 25 cos 3
set qos dscp-to-cos-map 26 cos 3
set qos dscp-to-cos-map 27 cos 3
set qos dscp-to-cos-map 28 cos 3
set qos dscp-to-cos-map 29 cos 3
set qos dscp-to-cos-map 30 cos 3
```

```
set qos dscp-to-cos-map 31 cos 3
set qos dscp-to-cos-map 32 cos 4
set qos dscp-to-cos-map 33 cos 4
set qos dscp-to-cos-map 34 cos 4
set qos dscp-to-cos-map 35 cos 4
set qos dscp-to-cos-map 36 cos 4
set qos dscp-to-cos-map 37 cos 4
set qos dscp-to-cos-map 38 cos 4
set qos dscp-to-cos-map 39 cos 4
set qos dscp-to-cos-map 40 cos 5
set qos dscp-to-cos-map 41 cos 5
set qos dscp-to-cos-map 42 cos 5
set qos dscp-to-cos-map 43 cos 5
set qos dscp-to-cos-map 44 cos 5
set qos dscp-to-cos-map 45 cos 5
set qos dscp-to-cos-map 46 cos 5
set qos dscp-to-cos-map 47 cos 5
set qos dscp-to-cos-map 48 cos 6
set qos dscp-to-cos-map 49 cos 6
set qos dscp-to-cos-map 50 cos 6
set qos dscp-to-cos-map 51 cos 6
set qos dscp-to-cos-map 52 cos 6
set qos dscp-to-cos-map 53 cos 6
set qos dscp-to-cos-map 54 cos 6
set qos dscp-to-cos-map 55 cos 6
set qos dscp-to-cos-map 56 cos 7
set qos dscp-to-cos-map 57 cos 7
set qos dscp-to-cos-map 58 cos 7
set qos dscp-to-cos-map 59 cos 7
set qos dscp-to-cos-map 60 cos 7
set qos dscp-to-cos-map 61 cos 7
set qos dscp-to-cos-map 62 cos 7
set qos dscp-to-cos-map 63 cos 7
set qos cos-to-dscp-map 1 dscp 8
set qos cos-to-dscp-map 2 dscp 16
set qos cos-to-dscp-map 3 dscp 24
set qos cos-to-dscp-map 4 dscp 32
set qos cos-to-dscp-map 5 dscp 40
set qos cos-to-dscp-map 6 dscp 48
set qos cos-to-dscp-map 7 dscp 56
set ntp disable
set ntp update-interval 64
```

MEMBER MX

```
# Model MX-8
set command-audit level default size 500
set ip dns disable
set ip route default 172.16.2.1 1
set log console enable severity error
set log session disable severity info
set log buffer enable severity error
set log trace enable severity debug
set log mark disable severity notice interval 300
set web-portal enable
```

```
set dot1x timeout supplicant 30
set dot1x timeout auth-server 30
set dot1x quiet-period 0
set dot1x reauth-max 2
set dot1x tx-period 5
set dot1x reauth-period 3600
set dot1x max-req 2
set dot1x key-tx enable
set dot1x reauth enable
set dot1x authcontrol enable
set dot1x wep-rekey-period 1800
set dot1x wep-rekey enable
set dot1x bonded-period 0
set system name VIEW_Member
set prompt ""
set system ip-address 172.16.2.20
set system idle-timeout 0
set domain security none
set auto-config disable
set system countrycode US
set service-profile SvpVoip ssid-name voip
set service-profile SvpVoip ssid-type clear
set service-profile SvpVoip beacon enable
set service-profile SvpVoip proxy-arp disable
set service-profile SvpVoip dhcp-restrict disable
set service-profile SvpVoip no-broadcast disable
set service-profile SvpVoip short-retry-count 3
set service-profile SvpVoip long-retry-count 5
set service-profile SvpVoip auth-fallthru last-resort
set service-profile SvpVoip soda mode disable
set service-profile SvpVoip soda enforce-checks enable
set service-profile SvpVoip max-bw 0
set service-profile SvpVoip cac-mode none
set service-profile SvpVoip cac-session 14
set service-profile SvpVoip user-idle-timeout 180
set service-profile SvpVoip idle-client-probing enable
set service-profile SvpVoip keep-initial-vlan enable
set service-profile SvpVoip web-portal-session-timeout 5
set service-profile SvpVoip wep active-unicast-index 1
set service-profile SvpVoip wep active-multicast-index 1
set service-profile SvpVoip cipher-tkip disable
set service-profile SvpVoip cipher-ccmp disable
set service-profile SvpVoip cipher-wep104 disable
set service-profile SvpVoip cipher-wep40 disable
set service-profile SvpVoip wpa-ie disable
set service-profile SvpVoip rsn-ie disable
set service-profile SvpVoip auth-psk disable
set service-profile SvpVoip shared-key-auth disable
set service-profile SvpVoip tkip-mc-time 60000
set service-profile SvpVoip auth-dot1x disable
set service-profile SvpVoip mesh mode disable
set service-profile SvpVoip bridging disable
set service-profile SvpVoip load-balancing-exempt disable
set service-profile SvpVoip web-portal-logout mode disable
set service-profile SvpVoip 11n mode-na enable
set service-profile SvpVoip 11n mode-ng enable
set service-profile SvpVoip 11n short-guard-interval enable
```

```
set service-profile SvpVoip 11n frame-aggregation all
set service-profile SvpVoip 11n a-msdu-max-length 4k
set service-profile SvpVoip 11n a-mpdu-max-length 64k
set service-profile SvpVoip active-call-idle-timeout 120
set service-profile SvpVoip transmit-rate 11a mandatory 6.0,12.0,24.0 beacon-rate
6.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11b mandatory 1.0,2.0 beacon-rate 2.0
multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11g mandatory 1.0,2.0,5.5,11.0 beacon-
rate 2.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11na mandatory 6.0,12.0,24.0 beacon-
rate 6.0 multicast-rate AUTO
set service-profile SvpVoip transmit-rate 11ng mandatory 1.0,2.0,5.5,11.0 beacon-
rate 2.0 multicast-rate AUTO
set service-profile SvpVoip attr vlan-name VlnMember
set radius deadtime 0
set radius timeout 5
set radius retransmit 3
set radius das-port 3799
set enablepass password <password>
set authentication mac ssid any * local
set user admin password encrypted 070e25414707
set radio-profile default beacon-interval 100
set radio-profile default dtim-interval 3
set radio-profile default max-tx-lifetime 2000
set radio-profile default max-rx-lifetime 2000
set radio-profile default rts-threshold 65535
set radio-profile default frag-threshold 2346
set radio-profile default preamble-length short
set radio-profile default auto-tune channel-config disable
set radio-profile default auto-tune 11a-channel-range lower-bands
set radio-profile default auto-tune ignore-clients disable
set radio-profile default auto-tune power-config disable
set radio-profile default auto-tune channel-interval 3600
set radio-profile default auto-tune power-interval 600
set radio-profile default auto-tune power-ramp-interval 60
set radio-profile default auto-tune channel-holddown 900
set radio-profile default countermeasures none
set radio-profile default rf-scanning mode active
set radio-profile default rf-scanning channel-scope operating
set radio-profile default rf-scanning cts-to-self disable
set radio-profile default rfid-mode disable
set radio-profile default wmm-powersave disable
set radio-profile default qos-mode svp
set radio-profile default weighted-fair-queuing disable
set radio-profile default rate-enforcement disable
set radio-profile default dfs-channels disable
set radio-profile default 11n channel-width-na 40MHz
set radio-profile default cac background mode disable
set radio-profile default cac best-effort mode disable
set radio-profile default cac video mode disable
set radio-profile default cac voice mode disable
set radio-profile default cac background max-utilization 0
set radio-profile default cac best-effort max-utilization 0
set radio-profile default cac video max-utilization 0
set radio-profile default cac voice max-utilization 0
set radio-profile default cac background policing disable
```

```
set radio-profile default cac best-effort policing disable
set radio-profile default cac video policing disable
set radio-profile default cac voice policing disable
set radio-profile default service-profile SvpVoip
set vlan-profile default vlan default
set ap security none
set ap auto mode disable
set ap auto radiotype 11g
set ap auto bias high
set ap auto blink disable
set ap auto upgrade-firmware enable
set ap auto force-image-download disable
set ap auto time-out 25
set ap auto power-mode auto
set ap auto radio 1 radio-profile default mode enable antenna-location indoors
antennatype INTERNAL
set ap auto radio 1 auto-tune max-power default
set ap auto radio 1 load-balancing enable
set ap auto radio 2 radio-profile default mode enable antenna-location indoors
antennatype INTERNAL
set ap auto radio 2 auto-tune max-power default
set ap auto radio 2 load-balancing enable
set ap auto local-switching mode disable vlan-profile default
set ap 1 port 5 model MP-372 radiotype 11g
set ap 1 name AP01
set ap 1 bias high
set ap 1 blink disable
set ap 1 upgrade-firmware enable
set ap 1 force-image-download disable
set ap 1 time-out 25
set ap 1 power-mode auto
set ap 1 radio 1 channel 6 radio-profile default mode enable antenna-location
indoors antennatype INTERNAL tx-power 5
set ap 1 radio 1 auto-tune max-power default
set ap 1 radio 1 load-balancing enable
set ap 1 radio 2 channel 36 radio-profile default mode disable antenna-location
indoors antennatype INTERNAL tx-power 17
set ap 1 radio 2 auto-tune max-power default
set ap 1 radio 2 load-balancing enable
set ap 1 local-switching mode disable vlan-profile default
set arp agingtime 1200
set ip https server enable
set ip telnet server enable
set ip telnet 23
set ip snmp server disable
set ip ssh server enable
set ip ssh 22
set load-balancing mode disable
set load-balancing strictness low
set band-preference none
set port enable 1
set port speed 1 AUTO
set port duplex 1 full
set port trap 1 disable
set port enable 2
set port speed 2 AUTO
set port duplex 2 full
```

```
set port trap 2 disable
set port enable 3
set port speed 3 AUTO
set port duplex 3 full
set port trap 3 disable
set port enable 4
set port speed 4 AUTO
set port duplex 4 full
set port trap 4 disable
set port enable 5
set port speed 5 AUTO
set port poe 5 enable
set port duplex 5 full
set port trap 5 disable
set port enable 6
set port speed 6 AUTO
set port duplex 6 full
set port trap 6 disable
set port enable 7
set port speed 7 AUTO
set port duplex 7 full
set port trap 7 disable
set port enable 8
set port speed 8 AUTO
set port duplex 8 full
set port trap 8 disable
set snmp protocol v1 enable
set snmp protocol v2c disable
set snmp protocol usm disable
set vlan tagtype dot1q
set vlan 1 name VlnMember tunnel-affinity 5
set vlan 1 port 1
set vlan 1 port 2
set vlan 1 port 3
set vlan 1 port 4
set vlan 1 port 6
set vlan 1 port 7
set spantree backbonefast disable
set spantree uplinkfast disable
set spantree fwddelay 15 vlan 1
set spantree hello 2 vlan 1
set spantree maxage 20 vlan 1
set spantree priority  32768 vlan 1
set spantree disable vlan 1
set igmp disable vlan 1
set igmp proxy-report enable vlan 1
set igmp querier disable vlan 1
set igmp mrsol disable vlan 1
set igmp version 2 vlan 1
set igmp mrsol mrsi 30 vlan 1
set igmp qi 125 vlan 1
set igmp oqi 255 vlan 1
set igmp qri 100 vlan 1
set igmp lmqi 10 vlan 1
set igmp rv 2 vlan 1
set igmp mrouter port 1 disable
set igmp receiver port 1 disable
```

```
set igmp mrouter port 2 disable
set igmp receiver port 2 disable
set igmp mrouter port 3 disable
set igmp receiver port 3 disable
set igmp mrouter port 4 disable
set igmp receiver port 4 disable
set igmp mrouter port 6 disable
set igmp receiver port 6 disable
set igmp mrouter port 7 disable
set igmp receiver port 7 disable
set fdb agingtime 1 age 300
set interface 1 ip 172.16.2.20 255.255.255.0
set snmp notify profile default drop all
set mobility-domain mode member seed-ip 172.16.1.22
set rfdetect classification ssid-masquerade rogue
set rfdetect classification seen-in-network rogue
set rfdetect classification ad-hoc skip-test
set rfdetect classification default-classification suspect
set rfdetect log enable
set rfdetect countermeasures mode normal
set rfdetect signature enable
set rfdetect voice-ext snr-threshold 12
set security acl hit-sample-rate 0
set security acl name svp permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
set security acl name svp permit 0.0.0.0 255.255.255.255
commit security acl svp
set security acl map svp vlan 1 in
set security acl map svp vlan 1 out
set qos dscp-to-cos-map 1 cos 0
set qos dscp-to-cos-map 2 cos 0
set qos dscp-to-cos-map 3 cos 0
set qos dscp-to-cos-map 4 cos 0
set qos dscp-to-cos-map 5 cos 0
set qos dscp-to-cos-map 6 cos 0
set qos dscp-to-cos-map 7 cos 0
set qos dscp-to-cos-map 8 cos 1
set qos dscp-to-cos-map 9 cos 1
set qos dscp-to-cos-map 10 cos 1
set qos dscp-to-cos-map 11 cos 1
set qos dscp-to-cos-map 12 cos 1
set qos dscp-to-cos-map 13 cos 1
set qos dscp-to-cos-map 14 cos 1
set qos dscp-to-cos-map 15 cos 1
set qos dscp-to-cos-map 16 cos 2
set qos dscp-to-cos-map 17 cos 2
set qos dscp-to-cos-map 18 cos 2
set qos dscp-to-cos-map 19 cos 2
set qos dscp-to-cos-map 20 cos 2
set qos dscp-to-cos-map 21 cos 2
set qos dscp-to-cos-map 22 cos 2
set qos dscp-to-cos-map 23 cos 2
set qos dscp-to-cos-map 24 cos 3
set qos dscp-to-cos-map 25 cos 3
set qos dscp-to-cos-map 26 cos 3
set qos dscp-to-cos-map 27 cos 3
set qos dscp-to-cos-map 28 cos 3
```

```
set qos dscp-to-cos-map 29 cos 3
set qos dscp-to-cos-map 30 cos 3
set qos dscp-to-cos-map 31 cos 3
set qos dscp-to-cos-map 32 cos 4
set qos dscp-to-cos-map 33 cos 4
set qos dscp-to-cos-map 34 cos 4
set qos dscp-to-cos-map 35 cos 4
set qos dscp-to-cos-map 36 cos 4
set qos dscp-to-cos-map 37 cos 4
set qos dscp-to-cos-map 38 cos 4
set qos dscp-to-cos-map 39 cos 4
set qos dscp-to-cos-map 40 cos 5
set qos dscp-to-cos-map 41 cos 5
set qos dscp-to-cos-map 42 cos 5
set qos dscp-to-cos-map 43 cos 5
set qos dscp-to-cos-map 44 cos 5
set qos dscp-to-cos-map 45 cos 5
set qos dscp-to-cos-map 46 cos 5
set qos dscp-to-cos-map 47 cos 5
set qos dscp-to-cos-map 48 cos 6
set qos dscp-to-cos-map 49 cos 6
set qos dscp-to-cos-map 50 cos 6
set qos dscp-to-cos-map 51 cos 6
set qos dscp-to-cos-map 52 cos 6
set qos dscp-to-cos-map 53 cos 6
set qos dscp-to-cos-map 54 cos 6
set qos dscp-to-cos-map 55 cos 6
set qos dscp-to-cos-map 56 cos 7
set qos dscp-to-cos-map 57 cos 7
set qos dscp-to-cos-map 58 cos 7
set qos dscp-to-cos-map 59 cos 7
set qos dscp-to-cos-map 60 cos 7
set qos dscp-to-cos-map 61 cos 7
set qos dscp-to-cos-map 62 cos 7
set qos dscp-to-cos-map 63 cos 7
set qos cos-to-dscp-map 1 dscp 8
set qos cos-to-dscp-map 2 dscp 16
set qos cos-to-dscp-map 3 dscp 24
set qos cos-to-dscp-map 4 dscp 32
set qos cos-to-dscp-map 5 dscp 40
set qos cos-to-dscp-map 6 dscp 48
set qos cos-to-dscp-map 7 dscp 56
set ntp disable
set ntp update-interval 64
```