VIEW Certified Configuration Guide

Trapeze Networks

Mobility System for MP-422 Access Points

June 2008 Edition
1725-36060-001
Version D

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.

Certified Product Summary

Manufacturer:	Trapeze Networks: www.trapezenetworks.com			
Approved products:	WLAN switches		Access points	
	MX-400 MX-216/216R MX-200/200R MX-20	MX-8 † MX-8R MXR-2	MP-422 †	
Security :	WPA-PSK and WPA2-PSK			
MX/MP software version certified:	Release 5.0.11.4			
SpectraLink handset models certified: **	e340/h340/i640	8020/8030		
SpectraLink handset software certified:	89.119	122.010 or greater		
SpectraLink radio mode:	802.11b	802.11b	802.11g	802.11a
Maximum telephone calls per MP:	10	10	12 *	12 *
Recommended network topology:	Switched Ethernet (required)			

† Denotes products directly used in VIEW Certification testing

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

** SpectraLink handset models 8020/8030, e340/h340/i640 and their OEM derivates are VIEW Certified 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".

Service Information

The AP must support SpectraLink Voice Priority (SVP). Contact your AP vendor if you need to upgrade the AP software.

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

During VIEW Certification testing, the following limitations were discovered.

- RF Active Scan must be disabled on MP radios that are providing voice services, including SpectraLink Wireless Telephones.
- 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. When a tunneled virtual LAN (VLAN) is configured over a Layer-3 network, IGMP snooping must be disabled each time the tunnel is established, because the virtual VLAN is established with IGMP snooping turned on by default.

Access Point Capacity and Positioning

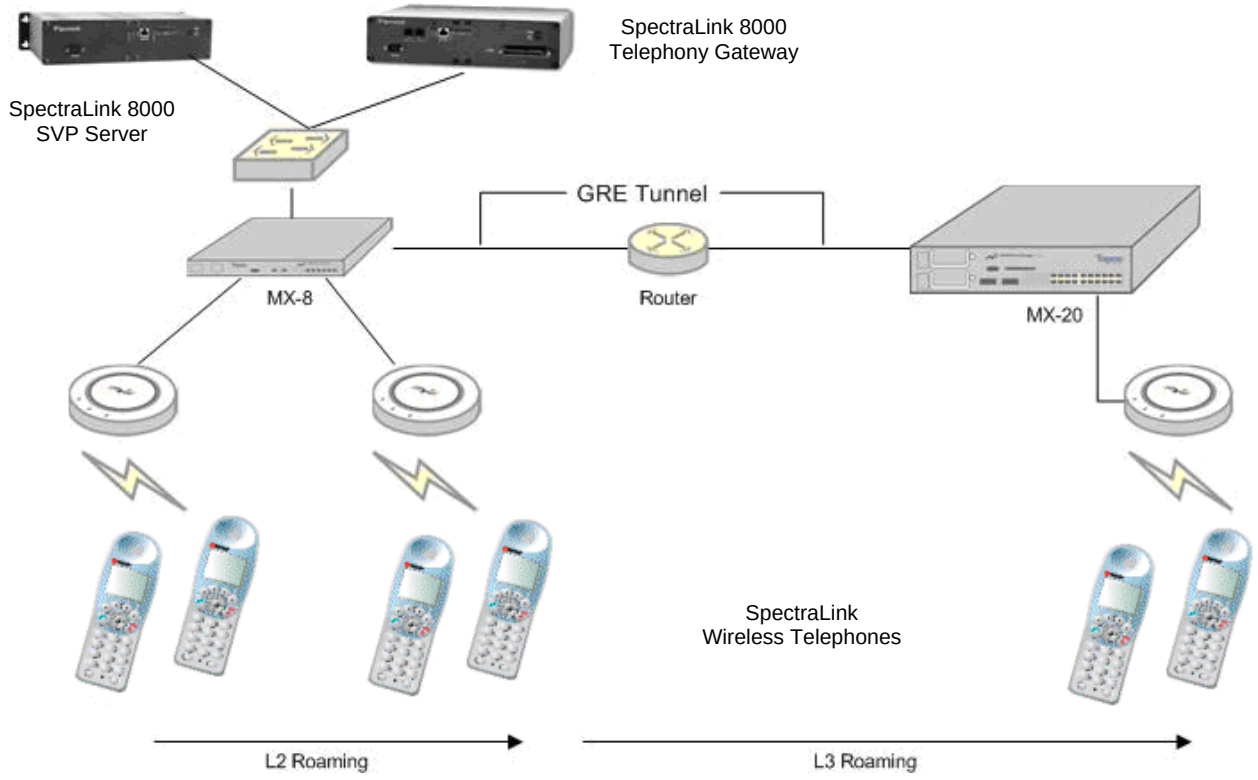
Please refer to the Polycom *Deploying Enterprise-Grade Wi-Fi Telephony* white paper. This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

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 issues and 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

The following topology was tested during VIEW Certification. It is important to note that these do not necessarily represent all "Certified" configurations.

Both Layer-2 and Layer-3 roaming were tested. Layer-3 roaming of SpectraLink Wireless Telephones requires the use of a generic routing encapsulation (GRE) tunnel.



Access Point Setup and Configuration

Installing software

Trapeze Mobility Exchange firmware cannot be downloaded from the SpectraLink website. Therefore, you must use the software that was shipped with your product, or contact Trapeze Networks for the latest software release.

Command, comment, and screen text key

In the sections below you will find commands, comments and system responses or other screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them..

Text Style	Denotes:
xxxxxxxx	Typed command
<xxxxxxxx>	Encryption key, domain name or other information specific to your system that needs to be entered
# xxxxxxxx	Comment about a command or set of commands
xxxxxxxx	System response or other displayed information

Configuring the Mobility Exchange Switch

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 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. There is no default password.

Service profile commands (SSID & security policy setup)

WPA2-PSK

Assume you are creating service profile "vowlan-wpa2" to define the ESSID "phones," as well as a WPA2-PSK security policy. The following commands are needed to setup the service for MP access points:

```
set service-profile Voice ssid-name vowlan-wpa2
   # sets the name of the service profile and SSID to
   vowlan-wpa2
set service-profile Voice auth-fallthru last-resort
   # specifies the authentication for the service
   profile to open access
set service-profile Voice rsn-ie enable
   # enables WPA2 security
set service-profile Voice cipher-tkip disable
   # disables TKIP
set service-profile Voice cipher-ccmp enable
   # enables AES / CCMP
set service-profile Voice psk-phrase <passphrase>
   # defines a passphrase
set service-profile Voice auth-psk enable
   # enables pre-shared key authentication
set service-profile Voice auth-dot1x disable
   # disables 802.1x authentication
set service-profile Voice attr vlan-name default
   # maps the handsets to the vlan named default
```

WPA-PSK

Assume you are creating service profile "vowlan-wpa" to define the ESSID "phones," as well as a WPA-PSK security policy. The following commands are needed to setup the service for MP access points:

```
set service-profile Voice ssid-name vowlan-wpa
   # sets the name of the service profile and SSID to
   vowlan-wpa
set service-profile Voice auth-fallthru last-resort
   # specifies the authentication for the service
   profile to open access
set service-profile Voice wpa-ie enable
   # enables WPA security
set service-profile Voice psk-phrase <passphrase>
```

```
   # defines a passphrase
set service-profile Voice auth-psk enable
   # enables pre-shared key authentication
set service-profile Voice auth-dot1x disable
   # disables 802.1x authentication
set service-profile Voice attr vlan-name default
   # maps the handsets to the vlan named default
```

Radio profile commands

Assume you are creating radio profile "voice" for all radios that will be providing voice services. The following commands are needed to setup the radio profile for the access points:

```
set radio-profile voice service-profile vowlan-wpa2
   # maps the service profile to the radio profile
set radio-profile voice dtim-interval 3
set radio-profile voice active-scan disable
   # prevents the AP from going off-channel to scan
set radio-profile voice auto-tune channel-config disable
   # disables dynamic channel tuning for radios in this
   profile.
set radio-profile voice qos-mode svp
   # qos mode SVP must be set for SVP to be supported
```

Network topology and MP access point hardware configuration

The network topology and access point hardware configuration can be configured using the Mobility System software. Please refer to the *Trapeze Networks Mobility System Software Configuration Quick Start Guide* or the *Trapeze Mobility Exchange Installation and Basic Configuration Guide* for more information. Some useful commands are:

To create VLAN "v1" and add port 3 as a member of "v1:"

```
set vlan 2 name v1 port 3
   # 2 is the VLAN ID (must be unique for every VLAN on
   the switch)
```

To create a configuration for a model MP-422 access point that is directly attached to port 1 of an MX switch:

```
set port type ap 1 model mp-422 poe enable
```

Radio configuration

During VIEW Certification, the MP access points were tested directly connected to a port on the MX (e.g. port 1). The following commands will configure a specific access point's radio to support the voice service:

```
set ap 1 radio 1 mode disable
   # if the radio is currently enabled. Radio 1 is the
   802.11b/g radio
set ap 1 radio 1 radio-profile voice mode enable
   # maps radio to the radio-profile and enables it
```

MP access points that are not directly connected to a port on the MX, which Trapeze calls a distributed access point (DAP), were not tested. If they are desired, the radio is configured with this command:

```
set dap 1 radio 1 mode disable
   # if the radio is currently enabled. Radio 1 is the
   802.11b/g radio
set dap 1 radio 1 radio-profile voice mode enable
   # maps radio to the radio-profile and enables it
```

SVP configuration

The following commands are needed to enable SpectraLink Voice Priority via access control list (ACL) "SVP."

This rule places all IP protocol 119 (SVP) traffic on class of service (CoS) queue 7 (SVP support):

```
set security acl ip SVP permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
```

(Optional) This rule permits all other data traffic. Do not use if the VLAN "v1" is dedicated to voice services. Note: There is an implicit "deny all" rule at the end of the ACL.

```
set security acl ip SVP permit 0.0.0.0 255.255.255.255
set security acl map SVP vlan v1 out
   # maps the ACL to VLAN v1 for outbound traffic
commit security acl SVP
   # activates the ACL
```

Be sure to disable IGMP snooping on VLAN "v1" by using the command:

```
set igmp disable vlan v1
```

Subnet roaming configuration between multiple MX switches

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" 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:

```
set system ip-address 1.1.1.1
set mobility-domain mode seed domain-name <domain name>
set mobility-domain member 1.1.3.1
   # configures the domain member
```

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

```
set system ip-address 1.1.3.1
set mobility-domain mode member seed-ip 1.1.1.1
```

Be sure to disable IGMP snooping temporarily on the MX that does NOT have the VLAN statically configured by using the command:

```
set igmp disable vlan v1
   # the VLAN name must be specified after the vlan
   keyword
```

If you have a previous mobility-domain configuration that is no longer valid, you must clear the existing mobility-domain before a new one can be defined:

```
clear mobility-domain
   # system will respond: Success: change accepted
show mobility-domain config
   # system will respond: There is no mobility domain
   configuration
```

To check the mobility domain, use the following command:

```
show mobility-domain
```

The system will respond:

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

Checking the configuration

Once the switch is configured, issue the following command at the command prompt to check the SVP settings:

```
sh ap qos-stats
```

The following information should be displayed (repeat the command to see changes):

```
CoS   Queue              Tx
==========================
    port: 1  radio: 1
1,2   Background          0
0,3   BestEffort        604
4,5   Video               0
6,7   Voice           79106      # Voice should have
                                 the most traffic.
    port: 1  radio: 2
1,2   Background          0
0,3   BestEffort          0
4,5   Video               0
6,7   Voice               0
```

The switch and AP are now ready for use with SpectraLink Wireless Telephones.

The network topology and other functions can also be configured using the Mobility System software. Please refer to the *Trapeze Networks Mobility System Software Configuration Quick Start Guide* or *Trapeze Mobility Exchange Installation and Basic Configuration Guide* for more information.

Configuration File (For Reference Only)

The following configuration file was used during VIEW Certification testing. The configuration below includes all configuration attributes, including defaults. Use the command **`show configuration all`** for this detailed version. To only see non-default configuration values, use the command **`show configuration`**.

Note: All of the lines below are commands, except for those preceded by the # symbol, which denotes a comment.

```
# General Configuration
set ip dns domain trpz.com
set ip dns enable
set log console enable severity error
set log session disable severity info
set log buffer enable severity error
set log trace enable severity debug mbytes 1
set web-aaa 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-key-period 1800
set dot1x wep-rekey enable
set dot1x bonded-period 0
set prompt
set system ip-address x.x.x.x
set system countrycode US
set auto-config disable

# Security Profile
set service-profile VoWLAN-WPA ssid-name <SSID name>
set service-profile VoWLAN-WPA shared-key-auth disable
set service-profile VoWLAN-WPA wep active-unicast-index
1
```

```
set service-profile VoWLAN-WPA wep active-multicast-
index 1
set service-profile VoWLAN-WPA wpa-ie disable
set service-profile VoWLAN-WPA rsn-ie enable
set service-profile VoWLAN-WPA cipher-tkip enable
   # for WPA this should be disabled
set service-profile VoWLAN-WPA cipher-ccmp enable
   # for WPA this should be enabled
set service-profile VoWLAN-WPA cipher-wep104 disable
set service-profile VoWLAN-WPA cipher-wep40 disable
set service-profile VoWLAN-WPA auth-dot1x disable
set service-profile VoWLAN-WPA auth-psk enable
set service-profile VoWLAN-WPA beacon enable
set service-profile VoWLAN-WPA ssid-type crypto
set service-profile VoWLAN-WPA auth-fallthru last-resort
set service-profile VoWLAN-WPA psk-phrase <passphrase>
set service-profile VoWLAN-WPA tkip-mc-time 60000
set radius deadtime 0
set radius timeout 5
set radius retransmit 3
set enablepass password <password>
set authentication admin * local

# AP Radio Profile
set radio-profile RealRadio service-profile VoWLAN-WPA
set radio-profile RealRadio 11g-only disable
set radio-profile RealRadio beacon-interval 100
set radio-profile RealRadio dtim-interval 3
set radio-profile RealRadio max-tx-lifetime 2000
set radio-profile RealRadio max-rx-lifetime 2000
set radio-profile RealRadio rts-threshold 2346
set radio-profile RealRadio short-retry 5
set radio-profile RealRadio long-retry 5
set radio-profile RealRadio frag-threshold 2346
set radio-profile RealRadio preamble-length short
set radio-profile RealRadio auto-tune channel-config
disable
set radio-profile RealRadio auto-tune power-config
disable
set radio-profile RealRadio auto-tune channel-interval
3600
set radio-profile RealRadio auto-tune power-interval 600
set radio-profile RealRadio auto-tune channel-holddown
300
```

```
set radio-profile RealRadio auto-tune power-backoff-
timer 10
set radio-profile RealRadio active-scan disable
set radio-profile RealRadio qos-mode svp
set radio-profile default 11g-only disable
set radio-profile default beacon-interval 100
set radio-profile default dtim-interval 1
set radio-profile default max-tx-lifetime 2000
set radio-profile default max-rx-lifetime 2000
set radio-profile default rts-threshold 2346
set radio-profile default short-retry 5
set radio-profile default long-retry 5
set radio-profile default frag-threshold 2346
set radio-profile default preamble-length short
set radio-profile default auto-tune channel-config
enable
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 channel-holddown 300
set radio-profile default auto-tune power-backoff-timer
10
set radio-profile default active-scan enable
set radio-profile default wmm enable
set dap security optional
set port type ap 1 model mp-422 poe enable

# AP Basic Configuration
set port type ap 1 model mp-422 poe enable
set ap 1 name <name>
set ap 1 bias high
set ap 1 blink disable
set ap 1 upgrade-firmware enable
set ap 1 group none
set ap 1 radio 1 channel 6 tx-power2 radio-profile
RealRadio mode enable
set ap 1 radio 1 auto-tune max-power default min-client-
rate 5.5 max-retransmissions 10
set ap 1 radio 2 channel 36 tx-power 17 radio-profile
default mode disable
set ap 1 radio 2 auto-tune max-power default min-client-
rate 24 max-retransmissions 10
set port type ap 2 model mp-422 poe enable
```

```
set ap 2 name MP02
set ap 2 bias high
set ap 2 blink disable
set ap 2 upgrade-firmware enable
set ap 2 group none
set ap 2 radio 1 channel 6 tx-power 2 radio-profile
default mode disable
set ap 2 radio 1 auto-tune max-power default min-client-
rate 5.5 max-retransmissions 10
set ap 2 radio 2 channel 36 tx-power 17 radio-profile
default mode disable
set ap 2 radio 2 auto-tune max-power default min-client-
rate 24 max_retransmissions 10
set arp agingtime 1200
set ip https server disable
set ip snmp server disable
set ip ssh server enable
set ip ssh 22
set ip telnet server enable
set ip telnet 23
set port enable 1
set port speed 1 AUTO
set port poe 1 enable
set port trap 1 NO
   # Set additional ports as appropriate.

# SNMP Configuration
set snmp notify profile default drop all
set snmp protocol v1 enable
set snmp protocol v2c disable
set snmp protocol usm disable
set snmp security unsecured

# VLAN Configuration
set vlan tagtype dot1q
set vlan 1 name v1
set vlan 1 port 3
set vlan 1 port 4
set vlan 1 port 5
set vlan 1 port 6
set vlan 1 port 7
set vlan 1 port 8
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 3 disable
set igmp receiver port 3 disable
   # disable router and receivers on other ports as
   appropriate
set fdb agingtime 1 age 300
set interface 1 ip 10.30.1.1 255.0.0.0
set mobility-domain mode seed domain-name mobdom
set mobility-domain member 10.30.1.2
set security acl ip SVP permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
set security acl ip SVP permit 0.0.0.0 255.255.255.255
set security acl map SVP vlan v1 out
commit security acl SVP
set ntp disable
set ntp update-interval 64
set igmp disable vlan v1
```