Trapeze Networks Mobility System
Configuration and Deployment Guide

SpectraLink’s Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between NetLink Wireless Telephones and wireless LAN (WLAN) infrastructure products. The products listed below have been thoroughly tested in SpectraLink’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 NetLink Wireless Telephones.

Certified Product Summary

<table>
<thead>
<tr>
<th>Manufacturer: Trapeze Networks: [<a href="http://www.trapezenetworks.com">www.trapezenetworks.com</a>]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved products:</td>
</tr>
<tr>
<td>WLAN switches</td>
</tr>
<tr>
<td>MX-400</td>
</tr>
<tr>
<td>MX-20†</td>
</tr>
<tr>
<td>MX-8†</td>
</tr>
<tr>
<td>MX-8R</td>
</tr>
<tr>
<td>MXR-2</td>
</tr>
<tr>
<td>Access points</td>
</tr>
<tr>
<td>MP-372†</td>
</tr>
<tr>
<td>MP-352†</td>
</tr>
<tr>
<td>RF technology: 802.11b/g</td>
</tr>
<tr>
<td>Radio: 2.4 – 2.484 GHz</td>
</tr>
<tr>
<td>Security: WPA-PSK and WPA2-PSK</td>
</tr>
<tr>
<td>MX/MP software version tested: Release 4.0.3</td>
</tr>
<tr>
<td>NetLink Wireless Telephone software version tested: Version 2.0 (89.119)</td>
</tr>
<tr>
<td>Maximum telephone calls per MP: 10</td>
</tr>
<tr>
<td>Recommended network topology: Switched Ethernet (required)</td>
</tr>
</tbody>
</table>

† Denotes products directly used in Certification Testing

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.
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 NetLink Wireless Telephones requires the use of a tunnel.

Known Limitations

During VIEW Certification testing, the following limitations were discovered.

1. You cannot have WPA and WPA2 pre-shared key (PSK) configured on handsets simultaneously within the same ESSID. The phones will not check-in.

2. You must disable Internet Group Management Protocol (IGMP) snooping when running SpectraLink Radio Protocol (SRP), which is used with the NetLink Telephony Gateway. SRP uses multicast packets to 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.

3. RF Active Scan must be disabled on MP radios that are providing voice services, including NetLink Wireless Telephones.
Access Point Capacity and Positioning

Each site is unique in its AP requirements. Therefore, please take the following points into account when determining how many APs are needed and where they should be placed in the facility:

Handset range
There must be WLAN coverage wherever the NetLink Wireless Telephones will be used. Adequate coverage for a NetLink Wireless Telephone can be determined by using the Site Survey mode on the handset that displays dB levels and channel when the phones are in range of an AP (within approximately a -60dBm signal strength radius). Alternatively, you can make use of the planning capabilities built into Trapeze Network’s RingMaster network management software to perform a virtual site survey for voice services.

Number of Handset calls per AP
The number of handsets that can be in-call simultaneously was determined based on call quality within a lab environment. Since call quality is impacted by packet retry rate and missed packets, test criteria were established for the maximum data rate (11Mb/s) for phones in-range of the AP.

As the handsets move near the limits of optimal RF coverage from the AP, they will automatically drop to lower Mb/s operation. NetLink Wireless Telephones require approximately 15% of the available bandwidth per call for 1 Mb/s operation, approximately 10% of the available bandwidth per call for 2 Mb/s operation, approximately 7% of the available bandwidth per call for 5.5 Mb/s operation, and approximately 5% of the available bandwidth per call for 11 Mb/s operations.

LAN Bandwidth
Estimate anticipated peak call volume to ensure that the LAN has enough bandwidth to handle the network traffic generated by all of the wireless devices.

WLAN Bandwidth
The NetLink Wireless Telephones share bandwidth with other wireless devices. To ensure adequate RF bandwidth availability, consider the number of wireless data devices in use per AP when estimating the necessary number of devices.
Access Point Setup and Configuration

Installing Software
Trapeze Mobility Exchange firmware cannot be downloaded from the SpectraLink Web site. 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.

<table>
<thead>
<tr>
<th>Text Style</th>
<th>Denotes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxxxxxxx</td>
<td>Typed command</td>
</tr>
<tr>
<td>&lt;xxxxxxxxxx&gt;</td>
<td>Encryption key, domain name or other information specific to your system that needs to be entered</td>
</tr>
<tr>
<td># xxxxxxxxxx</td>
<td>Comment about a command or set of commands</td>
</tr>
<tr>
<td>xxxxxxxxxx</td>
<td>System response or other displayed information</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Bits per second:</th>
<th>9600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data bits:</td>
<td>8</td>
</tr>
<tr>
<td>Parity:</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits:</td>
<td>1</td>
</tr>
<tr>
<td>Flow control:</td>
<td>None</td>
</tr>
</tbody>
</table>

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 and 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:

```plaintext
set service-profile vowlan-wpa2 ssid-name phones
set service-profile vowlan-wpa2 wpa-ie disable
set service-profile vowlan-wpa2 rsn-ie enable
set service-profile vowlan-wpa2 cipher-tkip disable
set service-profile vowlan-wpa2 cipher-ccmp enable
set service-profile vowlan-wpa2 auth-dot1x disable
set service-profile vowlan-wpa2 auth-psk enable
set service-profile vowlan-wpa2 psk-raw <256-bit passkey>
```

**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:

```plaintext
set service-profile vowlan-wpa ssid-name phones
set service-profile vowlan-wpa wpa-ie enable
set service-profile vowlan-wpa rsn-ie disable
set service-profile vowlan-wpa cipher-tkip enable
set service-profile vowlan-wpa cipher-ccmp disable
set service-profile vowlan-wpa auth-dot1x disable
set service-profile vowlan-wpa auth-psk enable
set service-profile vowlan-wpa psk-raw <256-bit passkey>
```

**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:

```plaintext
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 wmm disable
    # wmm must be disabled 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-372 access point that is directly attached to port 1 of an MX switch:

```
set port type ap 1 model mp-372 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
```
Authentication, VLAN and SVP Configuration

Assume you want the voice traffic to run on VLAN “v1.” To specify that the “phone’s” SSID be trivially authenticated and placed on VLAN “v1,” type the following commands:

```
set authentication last-resort ssid phones local
set user last-resort-phones attr vlan-name v1
```

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. Note: 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):

<table>
<thead>
<tr>
<th>CoS</th>
<th>Queue</th>
<th>Tx</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,2</td>
<td>Background</td>
<td>0</td>
</tr>
<tr>
<td>0,3</td>
<td>BestEffort</td>
<td>604</td>
</tr>
<tr>
<td>4,5</td>
<td>Video</td>
<td>0</td>
</tr>
</tbody>
</table>
| 6,7 | Voice     | 79106 | # Voice should have the most traffic.

The switch and AP are now ready for use with NetLink 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-raw <256-bit passkey>
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 last-resort ssid <SSID name> local
set authentication admin * local
set user last-resort-<ssid_name> attr vlan-name v1

# 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 wmm disable
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-372 poe enable
# AP Basic Configuration

set port type ap 1 model mp-372 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-372 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 qr 100 vlan 1
set igmp lmqi 10 vlan 1
set igmp rv 2 vlan 1
set igmp mrout 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

# If you are performing cross-subnet roaming, this command
# must be issued on the "remote" MX (the one that doesn't have
# the VLAN statically configured). This command must be re-
# issued whenever the tunnel is re-established, since IGMP
# snooping is (re)enabled each time.
# A future Trapeze release will resolve this limitation.
set igmp disable vlan v1