

## Meru Networks WLAN Controllers with AP100, AP201, AP208 Configuration and Deployment Guide

This document details the specifications for configuring the Meru Networks WLAN controllers and access points (APs).

### Product Summary

Manufacturer:	Meru Networks: <a href="http://www.merunetworks.com">www.merunetworks.com</a>	
Approved product(s):	WLAN Controllers	Access Points
	MC500	AP100
	MC1000	AP201
	MC3000	AP208
RF technology:	Direct-sequence spread spectrum (DS)	
Radio:	2.4 – 2.484 GHz	
Antenna Diversity:	Rx Diversity	
Security :	WEP, WPA-PSK	
AP software version:	3.1.1-24†	
Handset models	3616/3620/3626	3641/3645
Radio mode	802.11b	802.11b
Maximum telephone calls per AP:	8*	8*
Auto-learn function:	Yes	No
Recommended network topology:	Switched Ethernet (required)	

† Earlier and later software versions have not been tested for the Avaya™ Voice Priority Processor compliance. Refer to Wireless IP Telephone WLAN Compatibility List for field verified AP software versions.

\* Telephone calls per AP must be configured in the system per documentation provided by Avaya. Maximum 4 calls (when additional handsets are in a push-to-talk session)

### Known Limitations

Virtual Cell mode is incompatible with wireless IP telephone deployment. Please see the Virtual Cell information as detailed below in *Deployment Guidelines*.

### Notes on Configuration



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, please contact Avaya Technical Support at 1 800 242-2121 (USA only) or your local authorized Avaya dealer.

## Deployment Scenarios

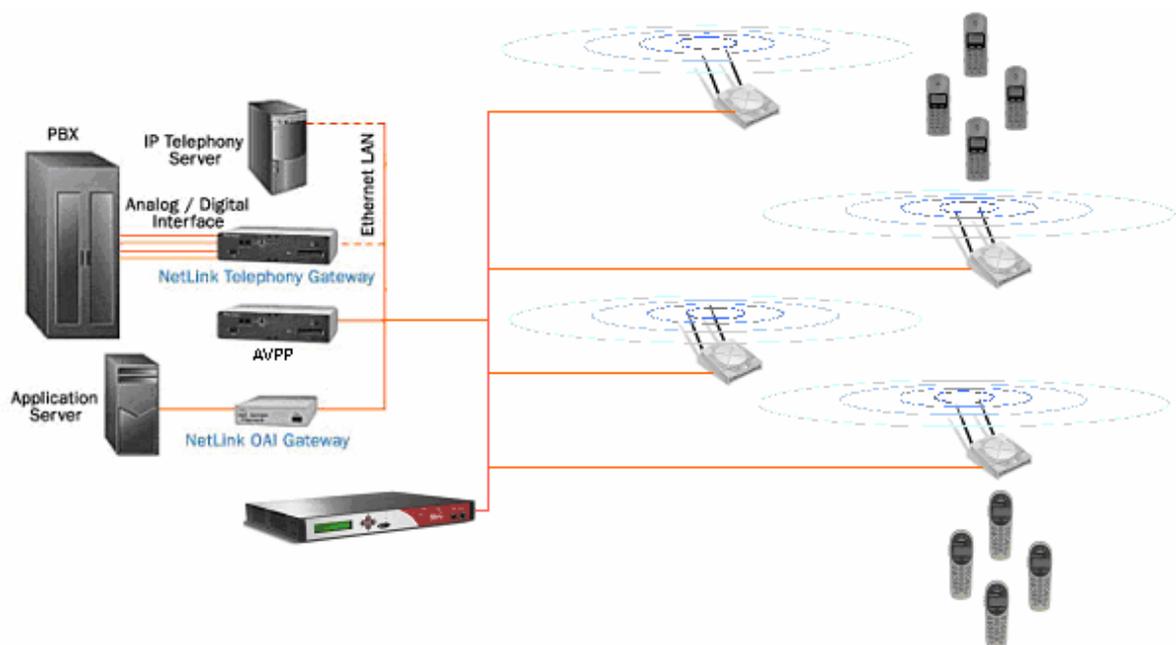
Wireless IP telephones can be deployed in a Meru Networks WLAN system where the access points are deployed within a subnet or across multiple layer 2 subnets.

The following figure shows the components in a typical deployment network with the Meru Networks WLAN and wireless IP telephone system.

When deploying the system you should determine which types of devices will require access and the mechanism of authentication/encryption that they support. This will drive the configuration of the system to support different user groups and security methods.

## Recommendations

- For a typical healthcare deployment, we recommend configuring one ESSID for the wireless IP telephones on a voice VLAN. In order to support the SVP Call Admission Control feature, this should be a non-Virtual Cell mode.
- For hospital staff tablets and laptop PC's, configure an additional ESSID utilizing strong authentication/encryption such as WPA, interfacing with a RADIUS server. This traffic should be separated onto a secure VLAN.
- If guest access is desired, configure an additional ESSID utilizing Captive Portal for web-based authentication. This traffic should be placed on a VLAN which terminates outside the hospital infrastructure firewall.



## Deployment Guidelines

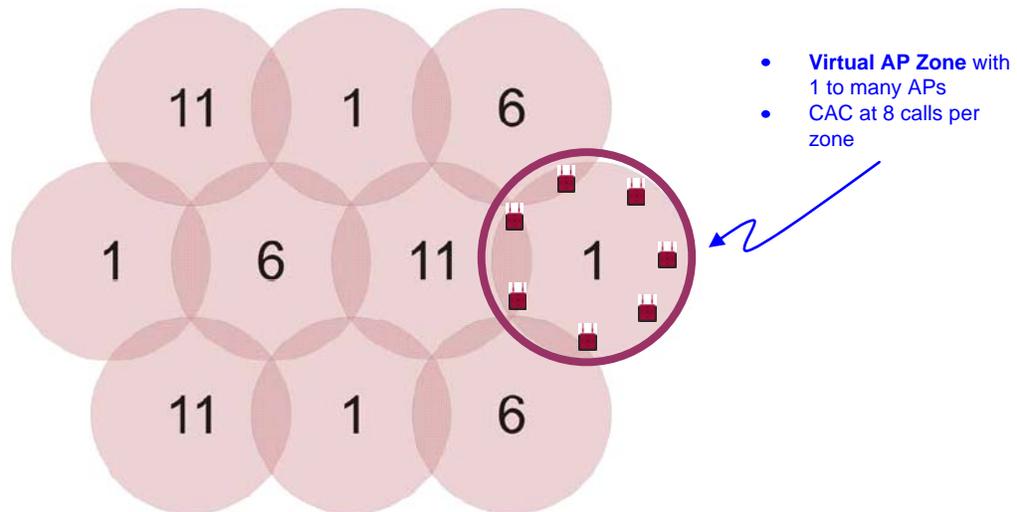
### Virtual Cell

Meru Virtual Cell technology allows for zero-handoff as the wireless IP telephones roam through the wireless environment. This dramatically improves the quality and consistency of client roam times. The bi-directional quality of service (QoS) provides a near toll-quality call experience regardless of the handsets' security context.

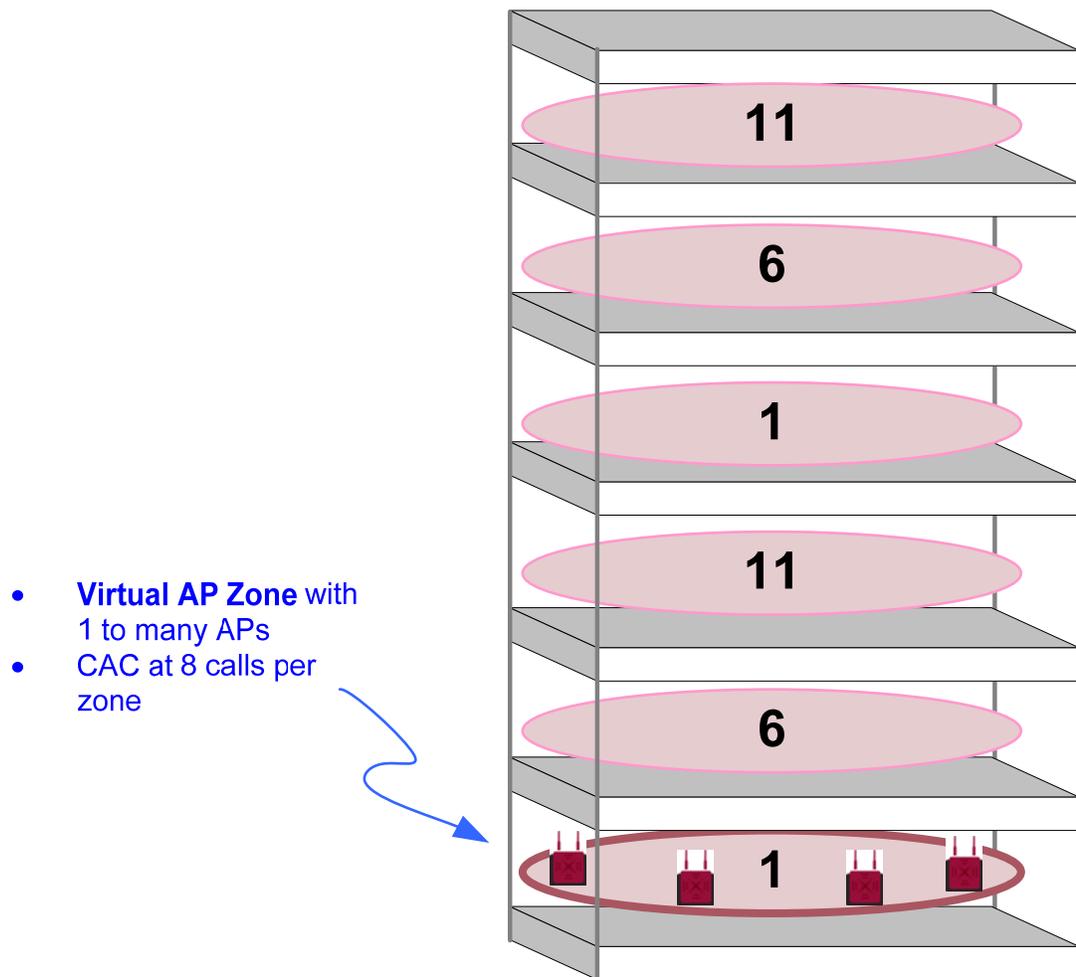
The Virtual Cell configuration does not provide a good configuration setting for dense wireless IP telephone deployment. This is because both Meru Networks and the wireless IP telephone system provide their own QoS schemes and are not centrally managed. For wireless IP telephones, the tolerance for packet retries is very low. Wireless handsets operate on a very tight delivery schedule and will often channel-scan elsewhere if those delivery expectations are not met.

To maintain the benefits of Virtual Cell just mentioned and to maximize calls, we recommend using Virtual Cell zones. A Virtual Cell zone is a zone area on a single channel containing one or more access points. The diagrams below provide further illustration of Virtual Cell zones. Depending on how many calls you expect to utilize per zone, the deployment may consist of one Virtual Cell zone (one channel deployment) or multiple virtual zones (multiple non-interfering channels 1,6,11) with each channel being a zone having one or more Virtual Cell access points.

Avaya recommends that no more than eight concurrent calls should exist in a zone, and that the Avaya Voice Priority Processor should be set to eight calls per access point



Single floor horizontal layout, non-interfering channels with overlap coverage



### Multiple floor vertical layout, non-interfering channel coverage

#### Push-to-talk feature

Push-to-talk (PTT) is a handset communication mechanism supported by the wireless IP telephone system. The mechanism uses multicast data delivery to communicate within the wireless neighborhood. With guaranteed coverage across all access points, push-to-talk often operates on a base rate as low as 1Mbps. Only a small set of handsets (3-4) can operate within a PTT channel on the Meru Wireless system. A recommended method of improvement, beyond multiple channel use for separation, is managing downlink data delivery at a higher rate than uplink by removing the 1 and 2 Mbps basic rates (**no base-tx-rates 802.11bg 1** and **no base-tx-rates 802.11bg 2**) for the ESS Profile. This provides some relief on channel space usage and potentially increases the number of calls within the channel space.

## Configuring the Meru Networks WLAN Controllers with CLI

Version 3.0 includes support for automatic QoS provision of SVP flows and does not require any specific AP settings. Specific parameters are required in the ESSID configuration to support various features of the wireless IP telephone system. For example, in order for the Avaya Voice Priority Processor discovery and push-to-talk features to function, multicast must be enabled for the ESSID.

### SVP QoS rules

In order to provide QoS mechanism for the wireless IP telephone system, a rule is required for the actual calls. If you have previously deleted a QoS rule, such as the one below, then you should add it back to the system.

```
qosrule 119 netprotocol 119 qosprotocol none
  action forward
  droppolicy head
  priority 0
  avgpacketrate 50
  tokenbucketrate 13400
  exit
```

## Security configuration

Meru Networks supports the following 802.11 security mechanisms for the wireless IP telephone system

- Open
- WEP (64 or 128)
- WPA-PSK (WPA Personal)

### Open

For Open (no 802.11 security) use the default security profile provided which has the “allowed-l2-modes clear” set.

### Static WEP

Sample WEP security profile:

```
Security-profile svp_wep
  allowed-l2-modes wep
    encryption-modes wep128

  static-wep key 0x1234567891234567890123456
  static-wep privacy auto
  exit
```

### WPA-PSK

Sample WPA-PSK security profile:

```
security-profile svp_wpapsk
  allowed-l2-modes wpa
    encryption-modes tkip

  psk key 0x6765747468656B3379

  exit
```

Note that you may enter the WPA-PSK key as either a string or the hexadecimal representation of the string. In the example above this could also have been entered as PSK key “**getthek3y**”. Note that on wireless IP telephones, you may enter this in the string format or hex format.

## VLAN configuration

It is often desirable to separate SVP packets from other data streams once the traffic enters the wired network. In the Meru solution, creating a VLAN entry in the controller and assigning it to the SVP ESSID achieves this. This is an optional configuration component.

```
vlan SVP_VLAN tag 1001
  ip address 10.4.0.250 255.255.0.0
  ip default-gateway 10.4.0.1
  ip dhcp-override
  ip dhcp-passthrough
  exit
```

## Deployment modes

The Meru Networks Air Traffic Control system supports two modes of deployment: Virtual Cell and non-Virtual Cell. In Virtual Cell mode, all of the access points on the same channel will utilize a single BSSID. This allows the system to perform client handoffs between access points without the client devices needing to perform 802.11 or 802.1X re-association procedures to the new access point. In a high density environment it is required that you use non-Virtual Cell mode with the wireless IP telephones, since they are optimized to work with a multi-channel deployment and perform admission control based on access point BSSID's. Following are the specific settings in order to run in non-Virtual Cell mode.

## ESSID configuration

The ESSID used by wireless IP telephones in production is of a similar configuration but would be configured for Virtual Cell and be assigned with the appropriate security profile.

It is important to note that when enabling the multicast support (for the server discovery and PTT feature) you must ensure that there is only one ESSID per VLAN otherwise multicast traffic is not passed.

If the deployment utilizes Avaya Call Servers on a software version older than 0.100 and does not have a Avaya Voice Priority Processor, then all 802.11 base rates higher than 1.2 Mbps must be disabled for the wireless IP telephone ESSID. If your deployment utilizes a Avaya Voice Priority Processor or is running version 0.100 or higher on the Avaya Call Server then 1,2,5.5, or 11 Mbps may be utilized as base and supported rates.

```
ssid  svp
      security-profile  chosen_security_profile
      vlan  svp_vlan (if required)
multicast-enable
      ap-discovery  join-ess
      no ap-discovery  join-virtual-ap
beacon dtim-period  2
beacon period  100
      no  publish-ssid
      exit
```

## AP configuration

Short preamble should be turned off per AP for wireless IP telephones. Under configuration of interface Dot11Radio this should be disabled.

```
Interface Dot11Radio <ap-id> <ap-idx>  
no preamble-short
```

A

An AP boot-script for AP configuration is required to support the SVP solution.

Create a file, **svpconfig.scr**, containing the following lines, and copy this to the controller into the directory **/opt/meru/ATS/scripts/**.

For Release 3.1.x and older, use the following settings in **svpconfig.scr**:

```
qos if wmac0 set qos_scheduling_discipline 1  
qos if wmac0 set mav 0  
wmac tx_rate decrease 2  
if 1 set be1_queue_len 48  
vayu queupackets wmac1 4  
vayu queuedspackets wmac0 4
```

For Release 3.2 and higher, use the following settings in **svpconfig.scr**:

```
qos if wmac0 set qos_scheduling_discipline 1  
qos if wmac0 set mav 0
```

Then configure the boot-script for each access point.

```
ap 1  
boot-script svpconfig
```

## References

*Meru Networks Configuration Reference*, available at <http://ftp.merunetworks.com/>

## Wireless IP Telephones

Wireless IP telephones use voice over IP (VoIP) technology on IEEE 802.11b-compatible wireless local area networks (WLANs). Access points utilize radio frequencies to transmit signals to and from the wireless IP telephones.

## Access Point Capacity and Positioning

Each site is unique in its AP requirements. 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 wireless LAN coverage wherever wireless IP telephones will be used. The typical range for a wireless IP telephone is comparable to that of a laptop computer utilizing a wireless LAN PC card. However, wireless IP telephones are likely to be used in areas where data devices are not typically used, such as stairwells and outdoor areas. Wireless IP telephones have a Site Survey mode that displays dBm levels to determine adequate WLAN coverage. Refer to the *Wireless IP Telephone Installation and Configuration* document for details about this feature.

### Number of handsets per access point

Estimate the number of wireless IP telephones and their anticipated call volume per AP area to ensure that the maximum number of calls per AP will not be exceeded. In this estimate, consider the data rates at which the handsets will operate. Higher data rates can only be sustained while well within the range of the AP. If the wireless IP telephones will be operating near the limits of the RF coverage from the AP, they will automatically drop to 1 Mb/s operation. Wireless IP 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 for 5.5 Mb/s operation, and 5% of available bandwidth for 11Mb/s operation.

Note: the maximum number of telephone calls per AP quoted in the summary table above is based on 11 Mb/s operation, and will be reduced if some or all wireless IP telephones are operating at 1, 2, or 5.5 Mb/s.

### LAN bandwidth

Estimate anticipated peak call volume to ensure that the LAN has enough bandwidth available to handle the network traffic generated by all of the wireless devices. Network traffic can be monitored/analyzed using a network sniffer or a simple network management protocol (SNMP) workstation.

### Number of other wireless devices per AP

The wireless IP telephones share bandwidth with other wireless devices. To ensure adequate RF bandwidth availability, consider the number of wireless data devices in use per AP.