



AeroScout – Meru Interop Config Guide

Version History

Version	Status	Revision Date	Details of Changes	Author
1.0	Draft	10/14/2010	Initial Version	Vikram Bains
2.0	Draft	03/13/2013	Updated SD/platform support	Vikram Bains

Table of Contents

Version History	2
Table of Contents	3
1. Setup Details:	5
1.1 Meru System Details:	5
1.2 AeroScout System Details:	5
2. Supported Platforms and Firmware	6
2.1 Meru AP Platforms Supported	6
2.2 Meru Software Platforms Supported	6
3. Acronyms and Abbreviations	7
4. Overview	8
4.1. The AeroScout Solution	8
4.2 AeroScout's General Architecture	8
5. Location Based Services/Components	10
5.1 Locating Tags	10
5.2 Locating Wi-Fi Enabled Mobile Units	11
5.3 AeroScout Engine	13
5.4 AeroScout MobileView™	13
5.5 RSSI Variance and Noise Floor Measurement	13
5.6 Network Infrastructure	14
6. Communication Between AE/AP	15
6.1 Interface Messages	15
6.2 AE Messages	15
6.3 AP Messages	15
6.4 Request/Reply Mechanisms and IP Addressing	15
6.5 ACK/NACK Mechanism	16
6.6 Communication Scheme	16
6.7 Generic AP Notifications	17
7. Configuring the AE for LBS	20
7.1 Configure the controller for AE	20
7.2 Activating tags	20
7.3 Calibrating the map	21
7.4 Adding APs on the map	21
7.5 Starting LBS for tags and MUs	22
8. Interop Notes	25
8.1 Compounded Reports	25
8.2 Dilution Timeout	27
8.3 AeroScout Integration Tool and Generic AP Notifications	29
8.4 AE -> AP Sample Message	30
8.5 AP -> AE Sample Message	30
9. Design/Deployment Considerations	31
9.1 Accuracy Basics	31
9.2 Factors that Affect Accuracy	32
9.3 General Deployment Guidelines	32
10. Geometric Dilution of Precision	35
10.1 Presence and Choke-Point Location	35
11. Limitations	37
12. References	38

1. Setup Details:

1.1 Meru System Details:

Controller Type: MC1500, MC3000

Meru Firmware: 4.0-123, -124, -129, -131 MR2

Main AP Type tested: AP300

1.2 AeroScout System Details:

AeroScout Engine Firmware: 03.02.42.03

AeroScout System Manager version: 03.02.42.02

AeroScout Positioning Server version: 03.02.42.03

AeroScout Integration Tool version: 1.0.1

AeroScout Tag Manager version: 3.01.06

AeroScout Tag Hardware : T2, T3 & T5

2. Supported Platforms and Firmware

2.1 Meru AP Platforms Supported

AP300 family (AP301, AP310, AP311, AP320)

AP332

AP1000 family (AP1010, AP1020)

AP1014

AP110

AP433

2.2 Meru Software Platforms Supported

All System Director versions later than 4.0-MR2

3. Acronyms and Abbreviations

Acronym	Description
AE	AeroScout Engine
AP	Access Point
DHCP	D ynamic H ost C onfiguration P rotocol
DS	D istribution S ystem
IBSS	I ndependent B asic S ervice S et
IP	I nternet P rotocol
LAN	L ocal A rea N etwork
LBS	L ocation B ased S ervices
MPDU	802.11 M AC P rotocol D ata U nit
MU	Wi-Fi M obile U nit
PDU	P rotocol D ata U nit
PS	AeroScout P ositioning S erver
RSSI	R eceived S ignal S trength I ndication
SM	AeroScout S ystem M anager
UDP	U ser D atagram P rotocol
WDS	W ireless D istribution S ystem

4. Overview

4.1. The AeroScout Solution

The AeroScout suite of products provides Enterprise Visibility Solutions using Wi-Fi wireless networks as an infrastructure. AeroScout solutions use standard wireless networks to accurately locate any asset, and utilize that location to deliver direct benefits such as asset tracking, process automation, theft prevention and increased utilization.

The AeroScout system locates both AeroScout Tags and any Wi-Fi mobile units. AeroScout Tags are small, battery-powered devices that may be mounted on equipment or carried by personnel, delivering real-time location of the tracked asset or person. In addition, Wi-Fi mobile units (MUs) may be located if they are associated to some access point, or when transmitting broadcast messages.

The messages transmitted by the AeroScout Tags or Wi-Fi mobile units are received by access points, and are passed along with additional information (e.g. signal strength measurements) to the AeroScout Engine, a core component of the AeroScout visibility system, that calculates the accurate location of the Tag or Wi-Fi device.

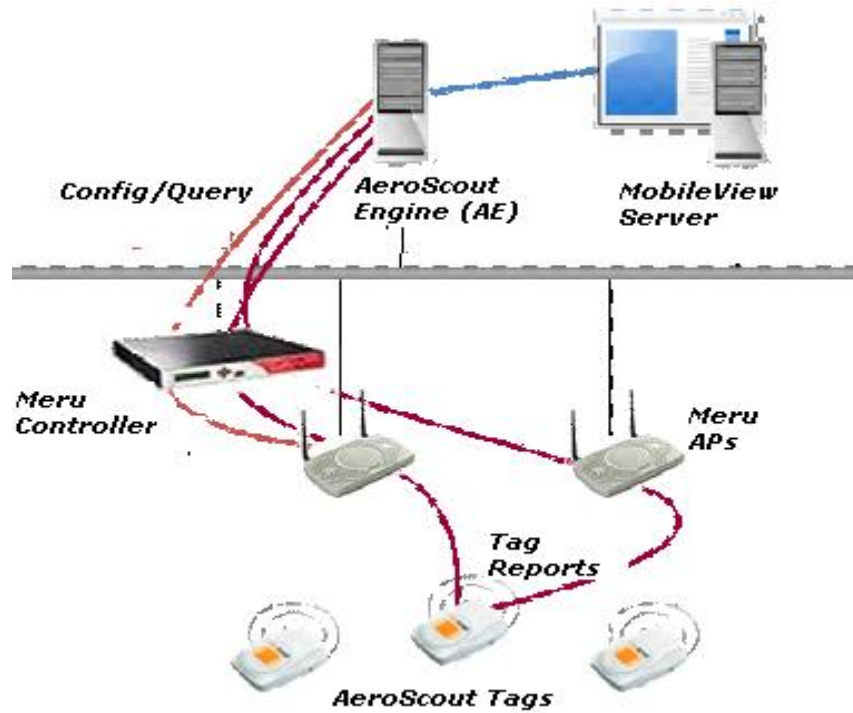
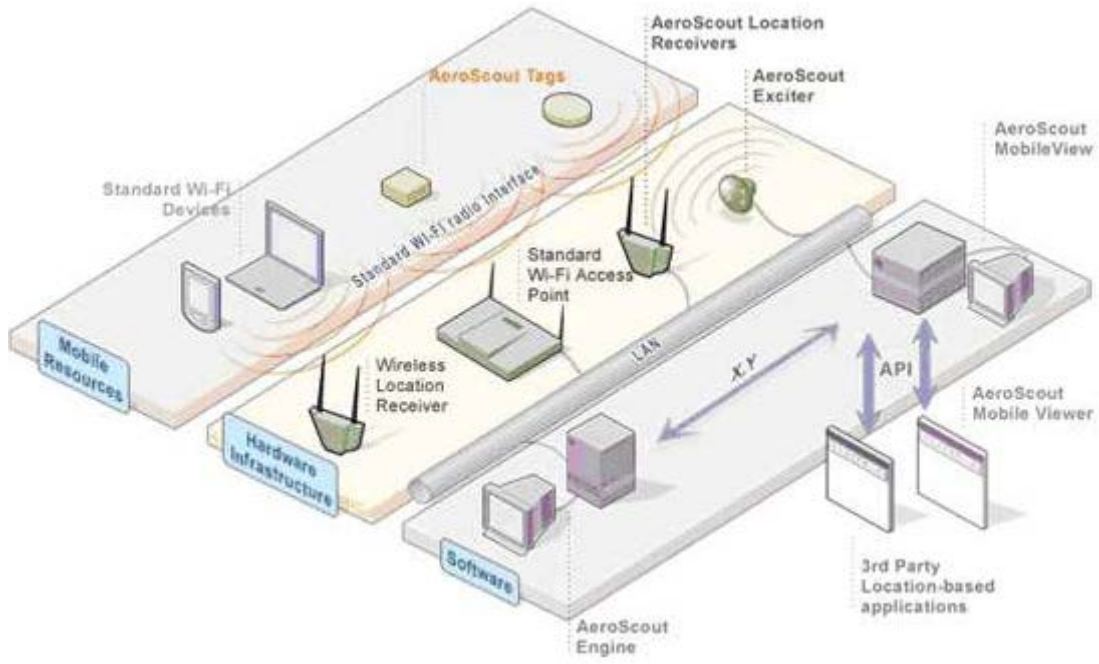
Reporting Tags and/or Wi-Fi mobile units should not affect the normal operation of the AP, that is, the AP should be able to keep performing in all its supported modes – normal 802.11a/b/g/n communication, monitor, and bridge modes.

4.2 AeroScout's General Architecture

How does the AeroScout system work?

AeroScout Tags and/or standard Wi-Fi devices send short wireless messages at a regular interval. The signal is received by standard wireless access points, and is sent to the AeroScout Engine along with its measured signal strength.

The AeroScout Engine uses signal strength and/or time of arrival algorithms to determine the coordinates of the reported location, and sends this data to AeroScout MobileView. AeroScout MobileView uses location data to display maps, enable searches, create alerts, manage assets etc.



5. Location Based Services/Components

5.1 Locating Tags

AeroScout Tags periodically transmit a short Wi-Fi message that is received by access points within range. Each access point measures the Received Signal Strength of the message, and forwards the message, with its Received Signal Strength Indication (RSSI) to the AeroScout Engine. After receiving several RSSI values from several access points for the same Tag, the AeroScout Engine calculates the accurate location of the Tag.

AeroScout T2 and T3 tags do not associate with access points and do not have an IP address.

Their messages are pure 802.11 messages. The Tags are unidirectional in the sense that they only transmit 802.11 messages; they do not listen to incoming 802.11 messages. Each Tag transmits its MAC address as the source address (SA) of the message. The Tags can transmit each message on several Wi-Fi channels, to support environments where access points work on different channels.

Access points can differentiate an AeroScout Tag message from any other Wi-Fi message according to the message's destination address (DA), which is a specific multicast address. This multicast address is configurable.

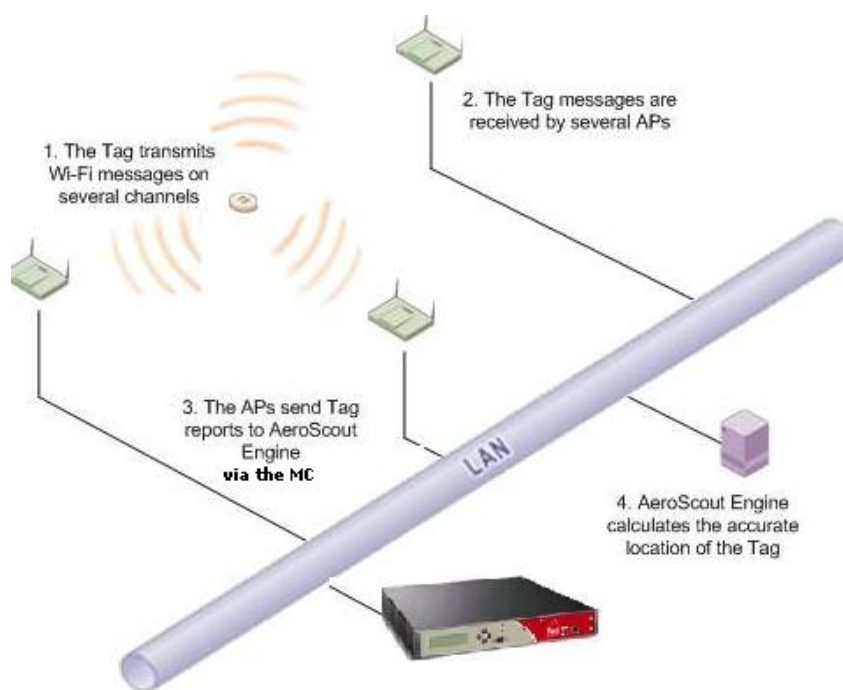
Every Tag message received by an AP must be reported to the AE.

Access points can receive and process Wi-Fi messages that were not transmitted on the same channel as the one the access point uses (the closer the transmission channel to the access point's operation channel, the better the chances that the message will be successfully received by the access point). Such messages have lower RSSI measurements than messages received through the correct channel, because of the channel difference. Since the RSSI values are the basis of the location calculation, the access point must match its channel with the Tag's transmission channel, i.e. drop every Tag message that was transmitted on a channel other than that of the access point's. This matching can be done because the Tag reports its transmission channel in its message.

For the location of a Tag to be calculated accurately, at least 3 access points need to report the Wi-Fi message transmitted by the Tag. A message received and reported by less than 3 access points provides only a very general location (which, in most cases, is the location of the AP closest to the Tag; In other cases, the tags may appear between the two reporting APs).

When AeroScout Exciters are used for choke-point locationing (a situation where alerts need to be generated based on an asset exiting or passing through a particular

area/portal; for example, Asset X has just passed Door Y), one AP receiving the Tag message is enough to deliver an accurate location report.



5.2 Locating Wi-Fi Enabled Mobile Units

The location of MUs is based on the fact that as long as they are associated with an access point, they transmit Wi-Fi messages. In order to locate mobile units, access points that receive their messages need to pass the RSSI values of each message (along with SSID and channel) to the AeroScout Engine.

As with locating Tags, at least 3 access points need to report the RSSI values for each MU in order to calculate the location. Unlike Tags, however, MUs are associated with a certain access point and do not communicate with other access points simultaneously. In order to locate MUs, access points must be able to collect data messages from MUs not associated with them, and pass the RSSI values to the AeroScout Engine.

Channel-matching is important for MU location as it is for Tag location. However, unlike Tags, MUs do not report their transmission channel in their messages. The most effective way to know the transmission channel of a MU is to know the operation channel of the AP it is associated with. When possible, APs should only pass MU reports when their own channel is the same as the channel that the AP associated with the MU operates on.

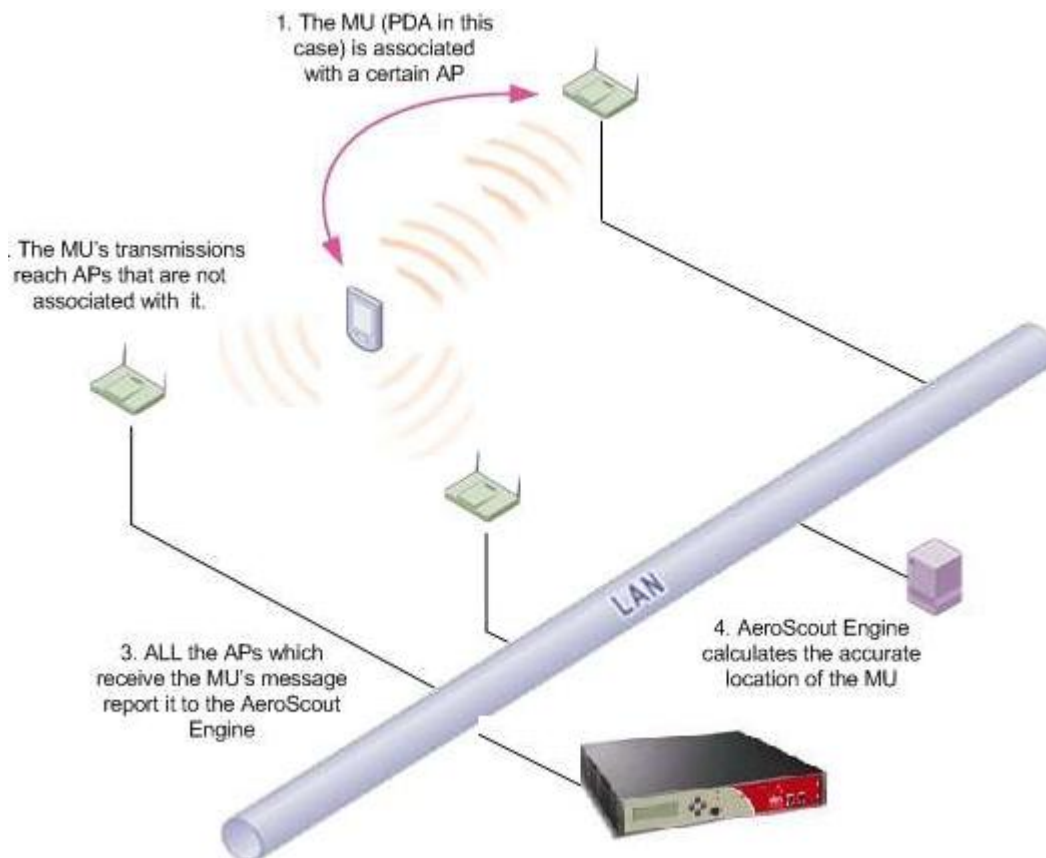
For example, if a MU is associated with an AP operating on channel 1 ("AP1") sends a packet, and its message is received by an AP operating on channel 2 ("AP2"), the

message will be dropped by AP2 and not reported to AeroScout Engine. In case the AP can not make this comparison (i.e. does not know which AP the MU is associated with), it will report it to AeroScout Engine and the Engine will disregard it (the advantage of having this mechanism in the APs rather than in the AeroScout Engine is that unnecessary messages are not passed through the network, which reduces the network load).

Because MU traffic may be high, it is possible to dilute the MU messages that are sent to AeroScout Engine by some Dilution Factor/Timeout.

MUs transmit messages even when they are not associated with APs. While scanning for available APs, for example, an MU may send "probe requests" across all channels. The RSSI of messages received from an MU should be passed to the AeroScout Engine regardless of whether the MU is associated with an AP or not.

For the purpose of the interface, Rogue APs are a special type of MU, although they do not associate with any AP. The reporting of MUs contains inherent support for the reporting of Rogue APs.



5.3 AeroScout Engine

AeroScout Engine (AE) is a sophisticated, algorithm-based software intended to calculate the location of AeroScout Tags and MUs, given RSSI reports received from standard access points.

AE is comprised of two components:

Positioning Server (PS): A Microsoft Windows service that receives messages with their RSSI values from access points, and outputs location reports.

System Manager (SM): A Microsoft Windows application that enables configuration of the PS and visual representation of the real-time location of AeroScout Tags and MUs.

Although RSSI location is a major function of the AeroScout Engine, the Engine offers additional important features:

TDOA Location: Inferring location from RSSI measurements is suitable for indoor environments. Outdoor environments, in which the density of APs is smaller than indoors, need a different suite of algorithms to calculate location accurately. The combination of AeroScout Location Receivers and the AeroScout Engine enables location calculations according to Time Difference of Arrival (TDOA), especially for outdoor environments.

AeroScout Exciters: In addition to X, Y location, some sites require accurate chokepoint capabilities ("Asset X has just passed Door Y"). In such cases AeroScout Exciters are utilized, and together with AeroScout Engine, they provide a full-fledged choke-point solution.

5.4 AeroScout MobileView™

AeroScout MobileView™ is a Web-based asset visibility platform. MobileView™ receives location data from the AeroScout Engine and other sources, and turns raw asset location information into real business solutions. The application includes user-friendly online asset location search (current and historical), sophisticated mapping, a variety of rule-based alerting and multiple reporting functions. MobileView™ also offers a standards-based, open API to integrate valuable location data with existing or new third-party applications.

5.5 RSSI Variance and Noise Floor Measurement

The AeroScout Engine uses the RSSI values measured and reported by the access points to infer the distance of the transmitting unit from the receiving access point.

Errors in the measurement of RSSI yield errors in the location accuracy.

The stability of the RSSI measurements follows the same logic. If the reported RSSI values have high variance (assuming a unit transmits with constant power), there will be a variance in the location accuracy.

Although the accuracy of RSSI values and their variance is not relevant to normal Wi-Fi data communication, it is crucial for accurate location.

Provided with a constant power signal (e.g. a source directly connected to the antenna), an access point needs to measure RSSI with a peak-to-peak deviation not higher than 2.0dBm.

Testing the RSSI peak-to-peak deviation is a prerequisite to the integration.

In some cases the AP module does not measure absolute RSSI values, but RSSI values that are relative to a momentary noise floor. Such RSSI values, by themselves, have high variance since the noise floor can change between measurements. It is possible to report the measured noise floor along with the RSSI value, to enable higher location accuracy.

5.6 Network Infrastructure

In order for the AeroScout Engine to send configuration messages to the APs, it needs to know their IP address. Therefore, every AP should preferably have a fixed IP address defined for it in the DHCP server (or use static IP).

In an architecture where APs do not have an IP address, the wireless controllers need to have a fixed IP defined in the DHCP server (or use static IP).

6. Communication Between AE/AP

The communication between the APs and the AE is conducted using UDP over IP. The AE configures the location related properties of the AP ("LBS configuration"), and the AP passes to the AE messages received from AeroScout Tags and MUs, along with the RSSI values and other parameters.

The APs listen on a specific port for the incoming AE message (Port 1144).

6.1 Interface Messages

The messages in this protocol are divided into two groups:

AE Messages: sent from the AE to the AP

AP Messages: sent from the AP to the AE

AP Messages are further divided into two groups:

Reply Messages: sent as responses to AE messages

Unsolicited Messages: sent autonomously by the AP

6.2 AE Messages

AE messages contain:

- Configuration messages
- Status querying messages
- Debug information querying messages

6.3 AP Messages

AP messages contain:

Comm Message	Type
Tag reports	Unsolicited
MU reports	Unsolicited
Status reports	Reply
ACKs and NACKs to AE	Reply
Compounded reports messages (several Tag reports and/or MU reports in one message)	Unsolicited
Debug information messages	Reply
Generic Notification Messages	Unsolicited

6.4 Request/Reply Mechanisms and IP Addressing

As noted earlier, there are two types of AP Messages: Reply Messages and

Unsolicited Messages. This section describes the destination address to which an AP needs to send its messages (both types).

The destination address of Reply Messages should be taken from the incoming AE message. Each AE message contains two fields: "Response IP Address" and "Response Port". Upon receiving an AE message the AP should either send its reply to the address stated in those fields or to the source IP and port of the incoming UDP packet, depending on the value of these fields. The address of the Response Message will be constructed as follows:

IP address: If the "Response IP Address" field has the value 0.0.0.0, the response IP address should be taken from the incoming UDP packet's source IP; otherwise the response IP should be the "Response IP Address" value.

Port: If the "Response Port" field has the value 0, the response port should be taken from the incoming UDP packet's source port; otherwise the response port should be the "Response Port" value.

A special case of an incoming AE message with respect to IP and port is "Set Configuration" message. When an AP receives a "Set Configuration" message, it should save the IP/Port to which it replied for that message. The saved IP/Port pair will be used as the destination address for Unsolicited Messages.

Note that the destination address for Unsolicited Messages can be changed only by a "Set Configuration" message; no other AE message changes this address.

6.5 ACK/NACK Mechanism

Every AE message will be acknowledged by an AP message.

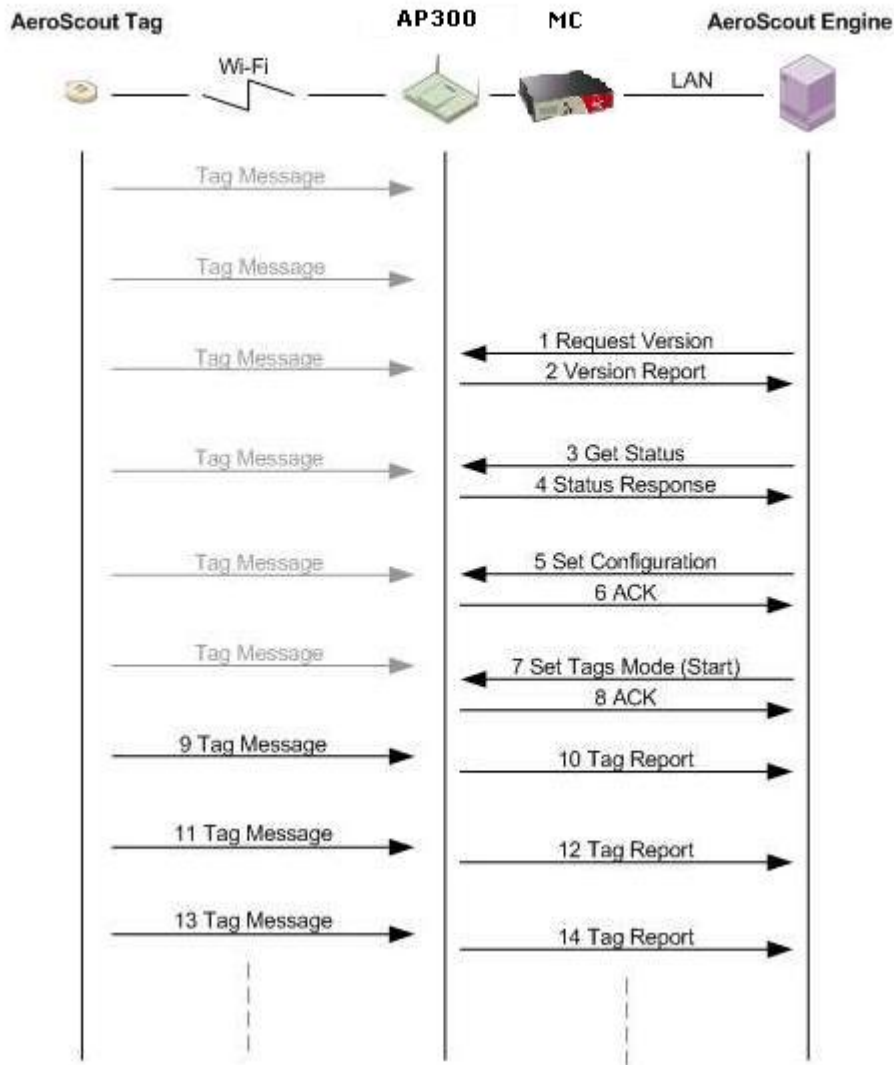
Some AE messages have specific response messages; others will expect an ACK message in response.

In case the AP has a problem and can not execute a specific AE message, it will send a NACK specifying the problem.

The AE does not acknowledge AP messages, except in one case. The AP may autonomously send a "Generic AP Notification" message, that can be used to pass to AE important information, such as an IP change or an error. In this message, the AP may request an ACK for the message (in which case the AE acknowledges by sending a "Request AP status" message to the AP, and the AP responds with a AP Status message).

6.6 Communication Scheme

The figure below describes the initial communication scheme for Tag location. Note that the Tag always transmits, regardless of whether the AP is configured to report its messages. The AE periodically queries the AP for status.



6.7 Generic AP Notifications

In the Meru solution, Generic AP notifications are sent out from the controller to the AeroScout Engine when the AP connectivity state changes or when AeroScout configurations on the controller change. The AeroScout Engine ACKs all Generic AP notification messages sent by the controller.

In general, a Generic AP notification is used to communicate an IP address change, a “wake up” from reboot, and/or any error conditions that need to be communicated to the AeroScout engine.

The following use cases describe the contexts in which a Generic AP report is generated.

Use Case 1: AP comes online

1. AP comes online
2. Controller sends out a Generic AP notification with the “AP’s IP changed”, “Wake up” and “ACK required” bits set
3. AeroScout Engine sends an ACK message back to the controller.

Use Case 2: AP goes offline temporarily

1. AP goes offline
2. Controller sends out a Generic AP notification with the “AP Encountered an Error” and “ACK required” bits set.
3. AeroScout Engine sends an ACK message back to the controller
4. AP comes back up online
5. Controller sends out a Generic AP notification with the “AP’s IP changed”, “Wake up” and “ACK required” bits set
6. AeroScout Engine sends an ACK message back to the controller.

Use Case 3: Controller comes online

1. Controller sends out a Generic AP notification for each AP connected to the controller with the “AP’s IP changed”, “Wake up” and “ACK required” bits set.
2. AeroScout Engine sends ACK messages back to the controller for each Generic AP notification that the controller sent out.

Use Case 4: WNC agent restarts or AeroScoutd restarts

1. Controller sends out a Generic AP notification for each AP connected to the controller with the “AP’s IP changed”, “Wake up” and “ACK required” bits set.
2. AeroScout Engine sends ACK messages back to the controller for each Generic AP notification that the controller sent out.

Use Case 5: AP moves from controller#1 to controller#2

1. AP goes offline on controller#1
2. Controller#1 sends out a Generic AP notification with the “AP Encountered an Error” and “ACK required” bits set.
3. AeroScout Engine sends an ACK message back to controller#1

4. AP comes back online on controller#2
5. Controller sends out a Generic AP notification with the “AP’s IP changed”, “Wake up” and “ACK required” bits set
6. AeroScout Engine sends an ACK message back to controller#2.

7. Configuring the AE for LBS

Setup/Install the AeroScout Engine, then follow these steps for activating location-based services.

7.1 Configure the controller for AE

1. # config terminal
2. # AeroScout enable
3. # AeroScout ip-address x.x.x.x. (this should be the AE IP add.)
4. # AeroScout port 12092
5. # end
6. # sh AeroScout

```

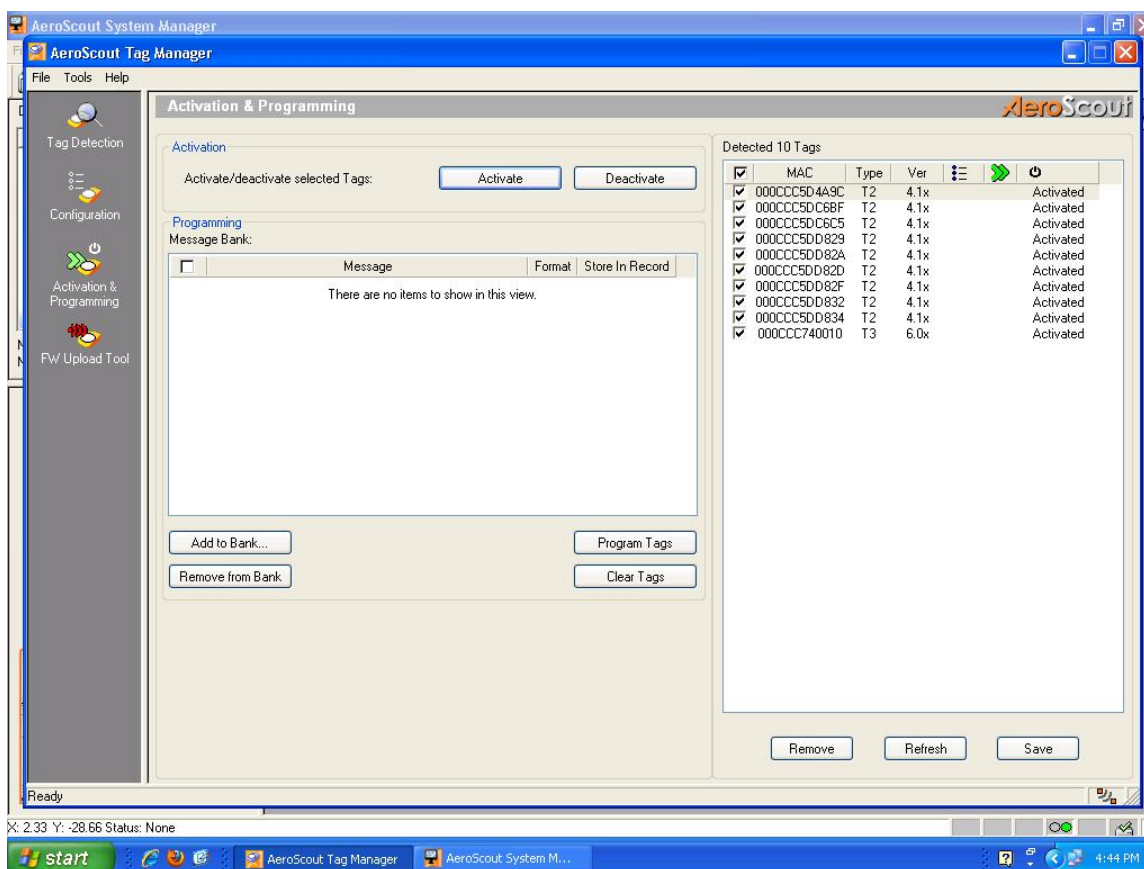
MC1500-Interop#
MC1500-Interop#
MC1500-Interop#
MC1500-Interop#
MC1500-Interop# config terminal
MC1500-Interop(config)# aeroscout enable
MC1500-Interop(config)# aeroscout ip-address 172.18.37.222
MC1500-Interop(config)# aeroscout port 12092
MC1500-Interop(config)# end
MC1500-Interop# sh aeroscout
Aeroscout Parameters

Enable/Disable           : enable
Aeroscout Engine IP Address : 172.18.37.222
Aeroscout Engine Port    : 12092
MC1500-Interop#
MC1500-Interop#

```

7.2 Activating tags

1. Start the AeroScout Tag Manager app.
2. Ensure all tags to be configured/used are placed in close proximity to the Tag Manager hardware.
3. In the Tag Manager app, click the Detect Tags button to display all discovered tags.
4. Ensure all the checkboxes next to the tag IDs are checked.
5. Click on the "Activate" button. All successfully activated tags should display a green checkmark in the last field (or display "Activated"). If certain tags show a red cross, repeat steps 4 and 5.
6. Click on the "Configuration" tab on the left of the screen.
7. Under the "General" subsection, click "Options" and define channel number to be used by the tags.

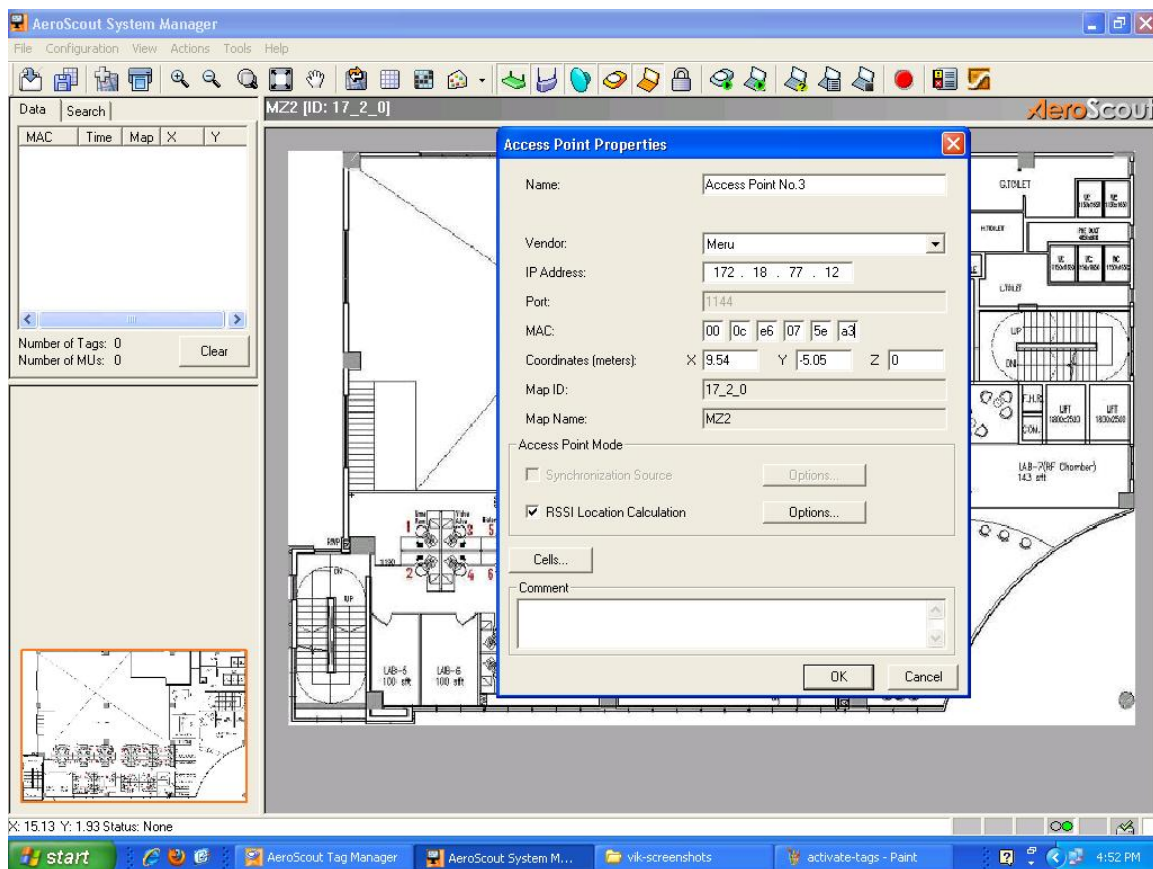


7.3 Calibrating the map

1. Start the AeroScout System Manager app.
2. Click on "Config" -> "Maps" -> "Add" to select a jpg/bmp image to import as a map.
3. Calibrate the map by right-clicking on it and choosing a (0,0) reference point. (This should usually be the top or bottom left corner of the floor map, to allow the entire grid to have positive values).
4. Right-click on the map again. Choose Calibrate -> Distance (or X,Y coordinates). Drag a point to point link between any two points on the map and enter the distance (in meters). This information needs to be accurate as the positioning will be calculated based on these values. Refer to your floor plans for further info on calibrating X,Y coordinates.

7.4 Adding APs on the map

1. Right-click any location on the map where there is an AP present.
2. Select the "Add Access Point" option.
3. Enter the controller IP in the "IP address" field.
4. Enter the AP's MAC address in the relevant field. Click "OK".
5. Repeat steps 1-4 for adding additional APs.

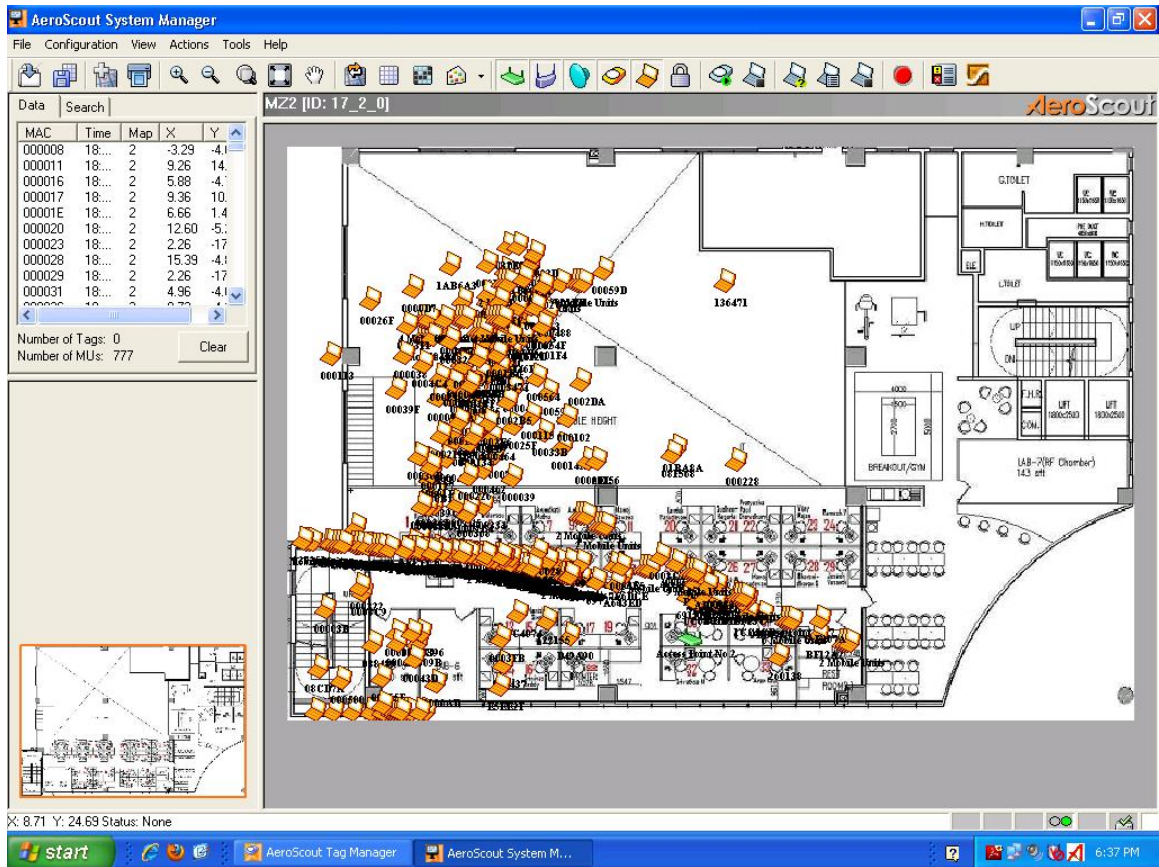


7.5 Starting LBS for tags and MUs

1. In AeroScout System Manager, Click Actions -> Start Tag Positioning.

MAC	Time	Map	X	Y
5D4A9C	17:...	2	28.61	-9.37
5D66BF	17:...	2	30.36	-8.67
5D6C5	17:...	2	32.91	-9.54
5D829	17:...	2	28.48	-8.81
5D82A	17:...	2	30.86	-9.02
5D82D	17:...	2	28.79	-8.99
5D82F	17:...	2	25.44	-8.99
5D832	17:...	2	27.79	-10...
5D834	17:...	2	27.37	-8.62
740010	17:...	2	19.60	-7.15

2. Similarly, for MUs, go to Configuration -> System Parameters -> Access Points. Check the "Enable mobile-unit location with Access Points" checkbox. Then, Actions -> Start MU positioning.



Beyond this basic configuration, for using additional features available on the AE (Recorder, Event Manager et al.), please refer to AeroScout documentation.

8. Interop Notes

MUs can be tracked in both 2.4 GHz and 5 GHz bands, AeroScout tags use only the 2.4GHz band for their transmissions.

The AeroScout Tag location is not supported on AP150s with Virtual Cell enabled.

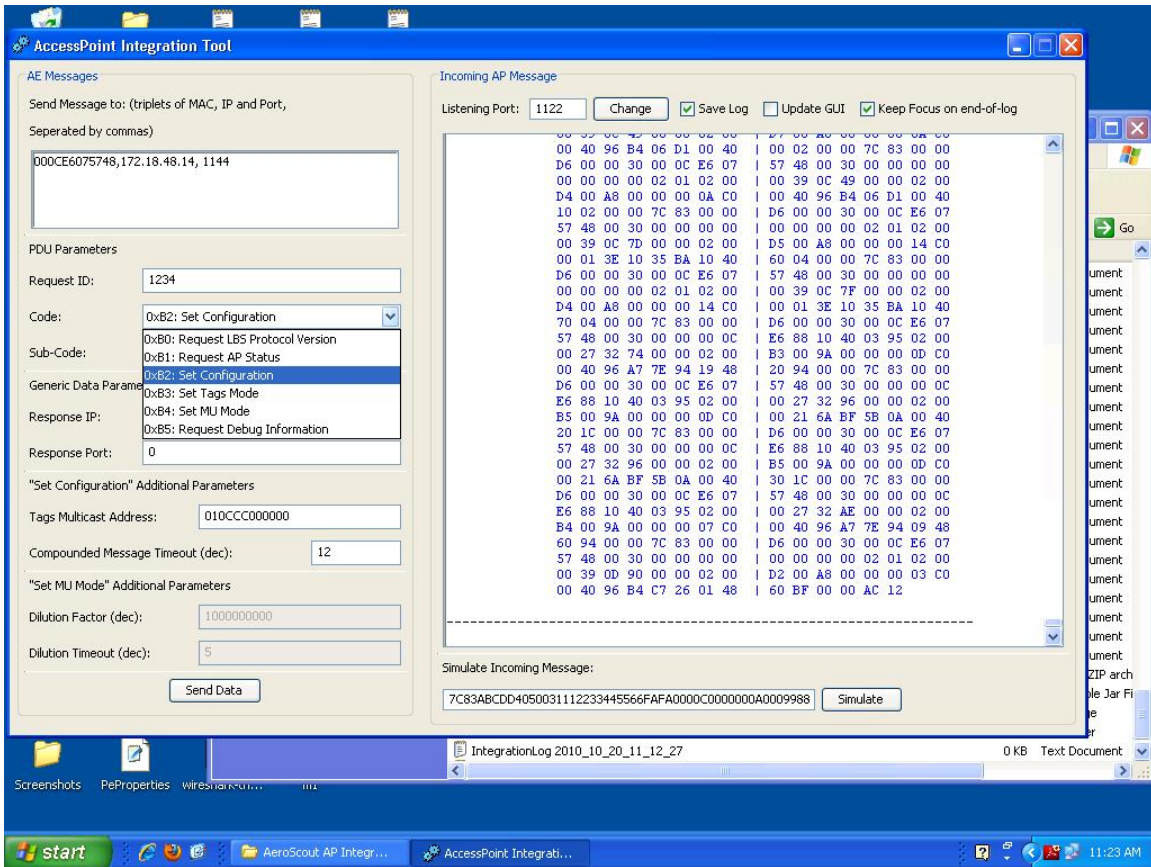
8.1 Compounded Reports

Wi-Fi mobile units (MUs) may be located if they are associated to some access point, or when transmitting broadcast messages. The messages transmitted by Wi-Fi mobile units are received by access points, and are passed along with additional information (e.g. signal strength measurements) to the AeroScout Engine, that calculates the accurate location of the Wi-Fi device.

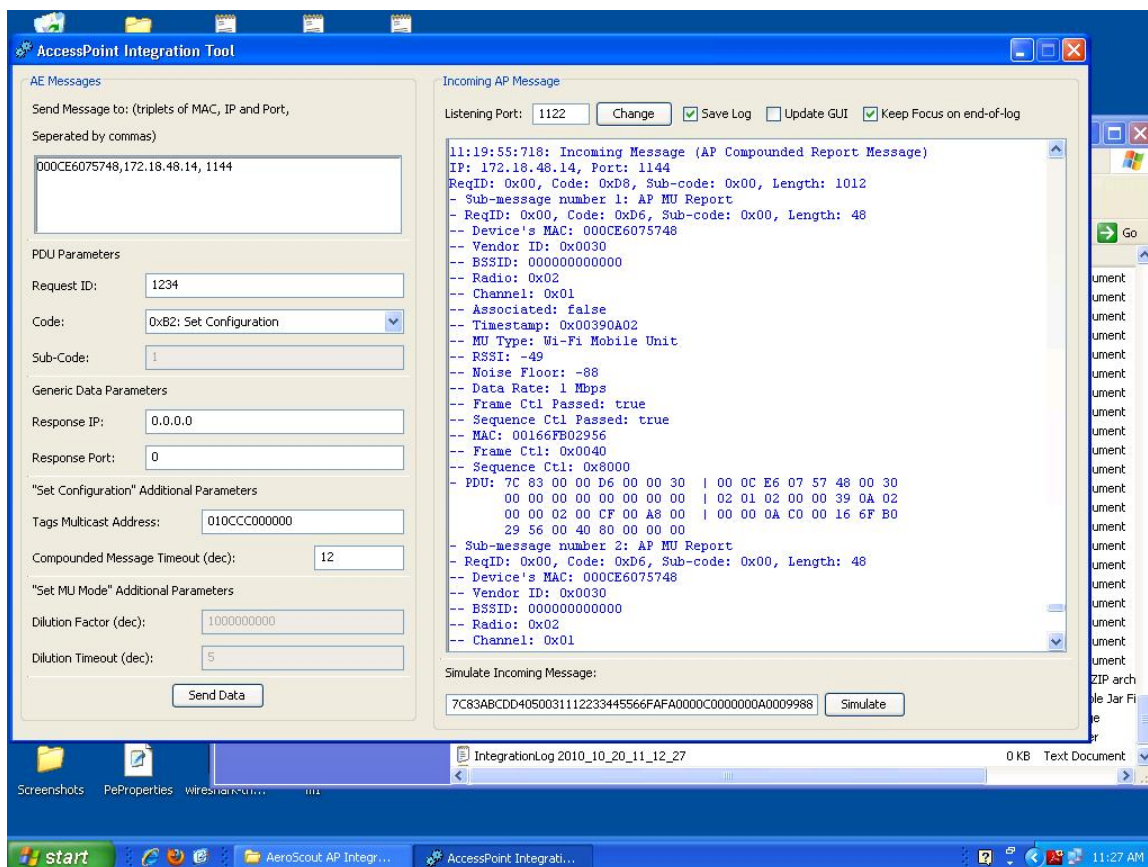
For better performance (avoiding overhead), Several MU reports can be combined within a fixed pre-defined period in Compounded Reports.

The Meru implementation combines a maximum of 18 MU Reports in 1 Compounded Report. The number of Compounded Reports may vary as per the Compounded Message Timeout configured on the AeroScout Integration tool . 'Compounded Message timeout' can be configured on the AeroScout Integration tool under 'Set Configuration' .

Important: See Section 5.3.



Compounded Report sample output:



Note : Pay attention to the "Sub-message number" values. In Meru's implementation, the Sub-message numbers can reach a max of 18, in a single compounded report.

8.2 Dilution Timeout

The AeroScout protocol provides two parameters to help APs dilute messages from each MU: 1. Dilution Factor 2. Dilution Timeout.

Meru MU reporting supports only Dilution Timeout. The Dilution Timeout is used to reduce excessive MU Report traffic between AP300s and the AE. These messages are unsolicited and no ACK/NACK is sent by the AeroScout Location Engine.

Dilution Timeout represents the number of seconds after which a MU message will be reported, regardless of the dilution factor. In other words, the value of the dilution timeout (in secs) is essentially the time interval between successive MU reports sent to the AE, on a per-MU basis.

For example, if this value is set to 60 seconds and, if the AP receives a message from a MU for which it has not reported a message to the AE for more than 60 seconds, the new message will be reported to the AE immediately regardless of the dilution factor, and the dilution counter will be initialized.

Commands broadcasted by a MU (e.g. Probe Requests) are required to be forwarded to the AE regardless of the dilution parameters. When a probe request is heard by the AP for a particular MU, the dilution counter is re-initialized.

Sample Message:

```
-----Outgoing Message (Set MU Mode)
16:43:32:265: Outgoing Message (AP Set MU Mode, Start: 0x01)
IP: 172.18.37.202, Port: 1144
ReqID: 0x4D2, Code: 0xB4, Sub-code: 0x01, Length: 24
- Device's MAC: 000CE6060D20
- Response IP: 0.0.0.0
- Response Port: 0
- _mode: Start
- Delution Factor: 0x3B9ACA00
- Delution Timeout: 0x0005
PDU: 7C 83 04 D2 B4 01 00 18 | 00 0C E6 06 0D 20 00 00
      00 00 00 00 00 00 00 00 | 3B 9A CA 00 00 05 00 00
-----

16:43:32:265: Incoming Message (AP ACK)
IP: 172.18.37.202, Port: 1144
ReqID: 0x4D2, Code: 0xD0, Sub-code: 0x00, Length: 8
- Device's MAC: 000CE6060D20
PDU: 7C 83 04 D2 D0 00 00 08 | 00 0C E6 06 0D 20 00 00
-----

16:43:32:281: Incoming Message (AP ACK)
IP: 172.18.37.202, Port: 1144
ReqID: 0x4D2, Code: 0xD0, Sub-code: 0x00, Length: 8
- Device's MAC: 000CE6060D20
PDU: 7C 83 04 D2 D0 00 00 08 | 00 0C E6 06 0D 20 00 00
-----

16:43:32:281: Incoming Message (AP MU Report)
IP: 172.18.37.202, Port: 1144
ReqID: 0xEF37, Code: 0xD6, Sub-code: 0x00, Length: 48
- Device's MAC: 000CE6060D20
- Vendor ID: 0x0030
- BSSID: 000CE66EE830
- Radio: 0x02
- Channel: 0x01
- Associated: false
- Timestamp: 0x48316C03
- MU Type: Wi-Fi Mobile Unit
- RSSI: -19
- Noise Floor: -85
- Data Rate: 1 Mbps
- Frame Ctl Passed: true
- Sequence Ctl Passed: true
- MAC: 001A739D9D1C
- Frame Ctl: 0x0988
- Sequence Ctl: 0xA03A
PDU: 7C 83 EF 37 D6 00 00 30 | 00 0C E6 06 0D 20 00 30
      00 00 00 0C E6 6E E8 30 | 02 01 02 00 48 31 6C 03
      00 00 02 00 ED 00 AB 00 | 00 00 0A C0 00 1A 73 9D
      9D 1C 09 88 A0 3A 00 00 | AC 12
-----
```

8.3 AeroScout Integration Tool and Generic AP Notifications.

The AeroScout Integration tool is primarily a Dev tool to test/simulate packet exchanges between the AE and APs. This is not considered a part of the standard user-level AeroScout Engine implementation. All examples/sample output shown in this document, that has originated from the Integration Tool is mainly for demonstration purposes, to show info exchange at the packet level. Do not use the AeroScout AP Integration Tool, unless asked to do so by Support.

Generic AP notifications are autonomous messages sent to the AeroScout Integration Tool on port 12092 to report the AP connectivity state (AP comes online, goes down etc). The AeroScout Engine ACKs all Generic AP notification messages sent by the controller. See section 3.8-Generic AP notifications.

Note – When AeroScout config parameters are changed (for example, AeroScout is enabled/disabled on the controller), in Meru's implementation, NO generic AP messages are sent to the AE.

Open the AeroScout Integration Tool. To view Generic AP notifications, configure the port on the tool to '12092' from '1122' (default). Now whenever AP's come online/go offline or when the controller is going down/coming back online, we will see the generic AP Notifications sent from the controller for all the APs on the controller and the AeroScout Integration Tool will send ACKs back to the controller for each Generic AP Notification.

Sample Generic Notification:

```
Sample for AP Generic Report :
Generic Notification -1
-----
11:06:11:578: Incoming Message (Generic Notification)
IP: 172.18.48.14, Port: 1144
ReqID: 0x00, Code: 0xD9, Sub-code: 0x00, Length: 24
- Device's MAC: 000CE6075748
- Vendor ID: 0x0030
- Ack Required: true
- Error Occurs: true
- AP Changed: false
- Wake UP: false
- Aux Data:
PDU: 7C 83 00 00 D9 00 00 18 | 00 0C E6 07 57 48 00 30
      00 00 C0 00 00 00 00 00 | 00 00 00 00 00 00 00 00
-----
Generic Notification -2

11:10:17:656: Incoming Message (Generic Notification)
IP: 172.18.48.14, Port: 1144
ReqID: 0x00, Code: 0xD9, Sub-code: 0x00, Length: 24
- Device's MAC: 000CE6075748
- Vendor ID: 0x0030
- Ack Required: true
- Error Occurs: false
- AP Changed: true
- Wake UP: true
- Aux Data:
```

```
PDU: 7C 83 00 00 D9 00 00 18 | 00 0C E6 07 57 48 00 30
      00 00 B0 00 00 00 00 00 | 00 00 00 00 00 00 00 00
```

8.4 AE -> AP Sample Message

```
-----
14:43:37:656: Outgoing Message (AP Set Configuration)
IP: 192.168.220.52, Port: 1144
ReqID: 0x4D2, Code: 0xB2, Sub-code: 0x00, Length: 24
- Device's MAC: 000CE6003771
- Response IP: 0.0.0.0
- Response Port: 0
- Tag's Multicast Address: 010CCC000000
- Message Timeout: 0x000C
PDU: 7C 83 04 D2 B2 00 00 18 | 00 0C E6 00 37 71 00 00
      00 00 00 00 00 00 01 0C | CC 00 00 00 00 0C 00 00
```

```
-----
14:43:37:666: Incoming Message (AP ACK)
IP: 192.168.220.52, Port: 1144
ReqID: 0x4D2, Code: 0xD0, Sub-code: 0x00, Length: 8
- Device's MAC: 000CE6003771
PDU: 7C 83 04 D2 D0 00 00 08 | 00 0C E6 00 37 71 00 00
```

8.5 AP -> AE Sample Message

```
-----
16:43:32:281: Incoming Message (AP MU Report)
IP: 172.18.37.202, Port: 1144
ReqID: 0xEF37, Code: 0xD6, Sub-code: 0x00, Length: 48
- Device's MAC: 000CE6060D20
- Vendor ID: 0x0030
- BSSID: 000CE66EE830
- Radio: 0x02
- Channel: 0x01
- Associated: false
- Timestamp: 0x48316C03
- MU Type: Wi-Fi Mobile Unit
- RSSI: -19
- Noise Floor: -85
- Data Rate: 1 Mbps
- Frame Ctl Passed: true
- Sequence Ctl Passed: true
- MAC: 001A739D9D1C
- Frame Ctl: 0x0988
- Sequence Ctl: 0xA03A
PDU: 7C 83 EF 37 D6 00 00 30 | 00 0C E6 06 0D 20 00 30
      00 00 00 0C E6 6E E8 30 | 02 01 02 00 48 31 6C 03
      00 00 02 00 ED 00 AB 00 | 00 00 0A C0 00 1A 73 9D
      9D 1C 09 88 A0 3A 00 00 | AC 12
```

9. Design/Deployment Considerations

9.1 Accuracy Basics

Note the following basic points:

- Indoors, the maximum effective distance between a tag and an access point (transmission range) is 200ft (61m). For ideal performance in most sites, this distance should not be more than 150ft (46m). In sites with thick concrete walls, the distance should not be more than 100ft (30.5m).
- To obtain an accurate location report, at least three access points need to be within the transmission range of every tag. For redundancy purposes, it is recommended that at least four access points be positioned within the transmission range of every tag.
- In a quadrilateral area, at least four access points should be installed at the four corners of the area, regardless of how small an area is and regardless of the fact that three access points in transmission range are sufficient to deliver an accurate location report.
- As the density of APs grows, the accuracy of the location reports increases.
- The distance of APs from the tags has an impact on accuracy. High ceilings (higher than 20ft [6 m]) yield lower accuracy. TDOA location technology is recommended in such cases.
- Electromagnetic interference, wall materials and wall thickness affect accuracy.
- In a site that has an extreme dynamic nature, accuracy may shift. For example, in sites where walls are being constantly built and torn down, accuracy may change. Another example is sites where large moving objects, such as commercial airplanes, block the line-of-sight between APs and tags.
- Accuracy measurement is probabilistic. When discussing accuracy rates, the rate refers to a 90% statistic order. For example, when referring to an accuracy of 12 feet, it means that 90% of the readings in that area are within 12 feet from the real location of the tag (that is, inside a circle of radius 12 feet whose center is the real location of the tag) and 10% of the readings return a location farther than 12 feet from the real location of the tag.

9.2 Factors that Affect Accuracy

AP density - The higher the density, the better the accuracy is.

Wall materials - Walls attenuate the signals transmitted by the tags, and therefore reduce the transmission range.

Large moving objects - When the RF environment changes, it is expected that the accuracy will also shift temporarily.

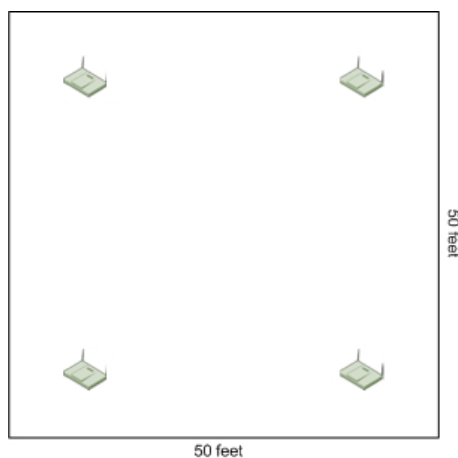
RSSI location determination over Wi-Fi achieves an accuracy of ~9ft (3m) in dense and interference-free environments. Depending on the density of the AP deployment, an accuracy of 9-30ft (3-10m) can be expected. Accuracy better than 9ft (3m) can be reached in some cases, but in most sites the best possible accuracy is 9ft (3m). On the other hand, in some harsh environments it is impossible to reach 9ft accuracy.

9.3 General Deployment Guidelines

Following are guidelines for good deployments. Most sites have limitations and restrictions that do not allow for an ideal installation, but by using the following guidelines accuracy levels can be increased significantly.

Minimum of Four Access Points

For a location to be calculated accurately, at least four access points are required, regardless of how small an area is. For example, in the following 2500ft² (232m²) area, four access points are required. This does not mean that every room needs four APs but that stand-alone small areas need at least four APs. Several rooms should be treated as one big space.

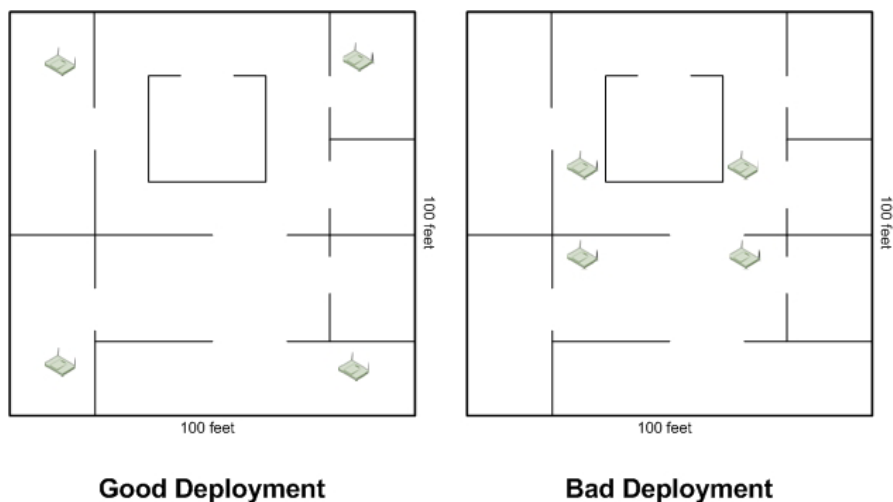


Access Points in a Small Area

Perimeter Deployment

APs should preferably be positioned along and within the perimeter on an enclosed area. Depending on the size of the area, more APs may be needed inside (not on the perimeter).

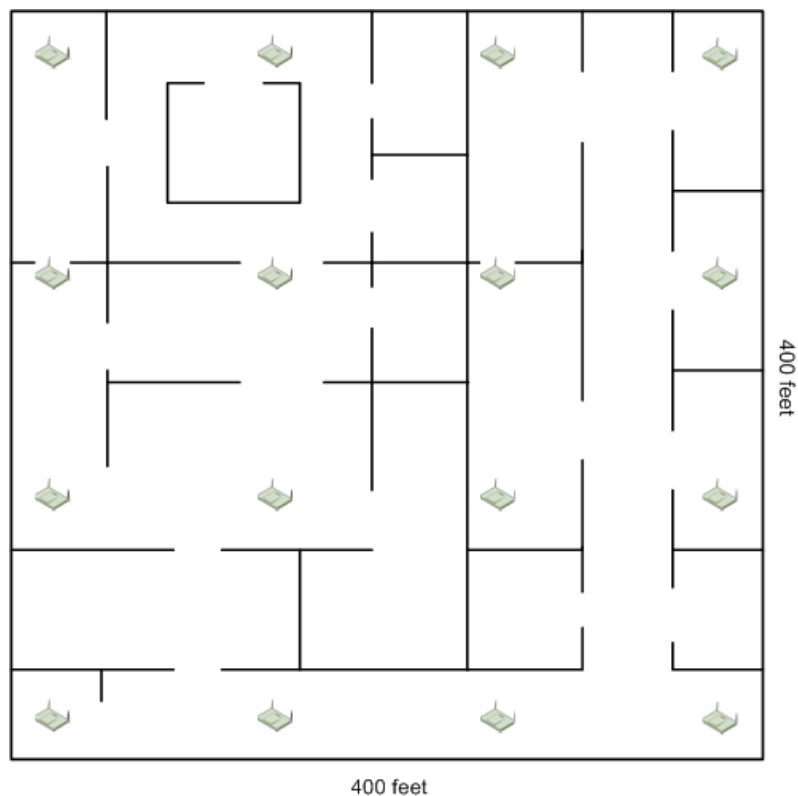
For example, assuming an area of 10000ft² (930m²), the following figure shows the ideal deployment (“good deployment”) and a deployment that should be avoided (“bad deployment”).



Note that the perimeter does not have to correspond to walls and the area covered may include walls.

Even Distribution

In a large area, distribute the APs evenly, so that APs are placed at relatively equal distances from each other.



Even distribution over a wide area

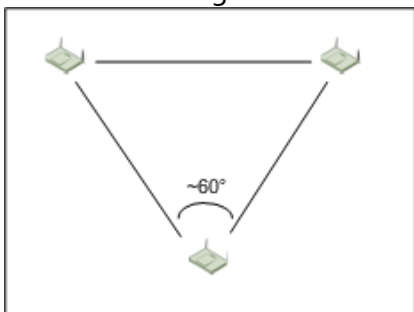
Such ideal distribution is usually difficult to achieve. However, in narrow hallways, the APs should not be arranged in a straight line even if placed at equal distances from each other.

Dealing with Sub-Areas

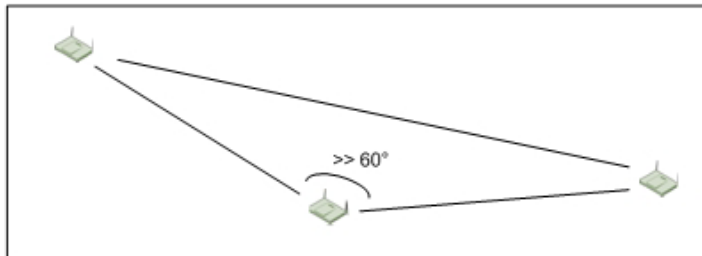
When considering areas and the number of APs that is appropriate for a given size, pay attention to the subdivision of an area. For example, a large warehouse divided into two sections by a wall likely to obstruct signals should be considered as two independent areas and should be equipped accordingly. In other words, if the warehouse has an area of 2000ft² it should be considered as two areas of 1000ft² and the number of APs to install should be calculated for each section of 1000ft² and not for 2000ft² (a minimum of four APs must be deployed in each part regardless of its size).

10. Geometric Dilution of Precision

The geometric shapes formed by the distribution of APs affect accuracy. APs arranged in equilateral triangles yield better accuracy than APs that form an obtuse triangle.

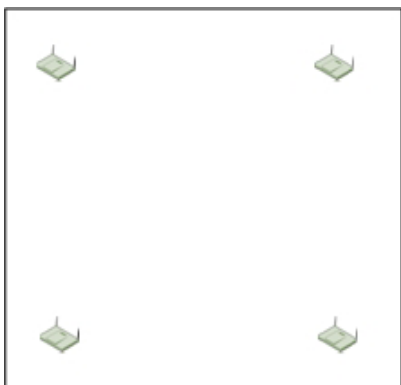


Good Deployment



Bad Deployment

Similarly, APs arranged in squares yield better results than APs that form rectangles.



Good Deployment



Bad Deployment

10.1 Presence and Choke-Point Location

Deployment considerations notwithstanding and depending on the needs, acceptable levels of accuracy can also be obtained with a very small number of devices, using the presence and choke-point location technologies. These technologies do not use triangulation and therefore do not require signals coming from at least three APs in order to deliver a location report.

Often, it is sufficient to just know that a tag is located in the vicinity of a given AP. In such cases, the presence method delivers the desired results based on a report coming from a single AP – the AP to which the tag is closest. In this case, whole areas may be covered by a single AP.

In the choke-point method, the location report indicates that the tag has passed

through a given point, such as the entrance to an area or the exit point of an area. This information is obtained through AeroScout Exciters (proprietary hardware).

Another option is to perform location calculations with pairs of APs. When a tag message is received by only two APs, it is located somewhere along the line connecting the two APs. In sites divided into sub-areas, this may be enough.

11. Limitations

1. AP200s and AP150s support tag positioning only.
2. Devices tested include Tags (T2 and T3 only) and MUs (laptops, Cisco/Ascom phones).
3. Support for MUs is available from Meru firmware 4.0-MR2 onwards (AP300). Prior to this firmware release, only tags are supported.
4. Location based accuracy has a margin of error of ~ 3-5 meters.
5. For the Dilution mechanism, Meru only supports Dilution Timeout. Dilution Factor is not implemented.
6. In the Meru implementation, there is no retry mechanism for generic AP messages/notifications, in a situation where the AE does not send an ACK/Req AP Status for the generic AP messages.
7. When AeroScout config parameters are changed (for example, AeroScout is enabled/disabled on the controller), in Meru's implementation, NO generic AP messages are sent to the AE.
8. As of 4.0MR2, the Dilution Timeout value is offset by 1. So, if the DT value is configured as 5, it is effective as a value of 6.
9. The T4 tag is the only model that sustains bi-directional comm. It has not been tested, or documented here.

12. References

- AeroScout Engine-AP Interface Protocol ver 2.01
- AeroScout_GenericAPNotify_SFS_SDS