Deploying Advanced Wireless Services using the Mobility Services Engine

BRKEWN-2012
Your Sessions Presenter

From Cisco Systems

- Yedunandan S
  - Consulting Systems Engineer - Mobility
  - Borderless Networks - India
Agenda

- Overview of MSE
- Context Aware Services
- Adaptive wIPS
- CleanAir interference Tracking
Overview of MSE
Overview of MSE

- Services Enabled Network
- MSE in CUWN Architecture
- MSE Services
- Licensing
Service-Enabled Network Requirements

Dedicated Processing Power
- Scalable service delivery requires a robust, purpose-built processing engine

Centralised Management
- Simplifying the IT burden for mobility requires unified services management

Breaking Network Silos
- Mobility applications must not be limited to Wi-Fi networks only

Open Architecture
- The mobility services platform must provide a common, open interface for third party application development
Introducing A Practical Approach
Centralised, Scalable Mobility Services

3300 Series Mobility Services Engine

Services and Applications Platform
- Unified API enabling Enterprise 3.0 applications

Common Framework for Multiple Services
- Ease of deployment and efficient allocation of CapEx

Abstraction layer with CAPWAP/NMSP
- Allows Transport and Applications to evolve independently

Eco-system of Application Partners
- Accelerate development and deployment of customised solutions
Mobility Services Software Suite

**Context Aware**

- Optimise business process with context such as location and telemetry

**Adaptive Wireless IPS**

- Mitigate wireless threats with integrated intrusion prevention

**CleanAir Tracking**

- Tracking the location of Interfering devices and their impact areas

---

**Markets & Solutions**

- Healthcare
- Manufacturing
- Asset Tracking
- Condition Monitoring

**Markets & Solutions**

- Retail
- Financial Services
- Healthcare
- PCI, HIPAA, SOX

**Markets & Solutions**

- Manufacturing
- Healthcare
- Enterprise
- High Availability Networks
MSE in CUWN Architecture

Cisco Wireless LAN Controller

Switch/Routed Network

Access Points

Cisco Lightweight Access Point

CleanAir

Contextaware

wiIPS

Mobility Services Engine

Cisco Wireless Control System (WCS)

Client Devices (CCX and CSSC)
MSE Models

Cisco 3300 Series Mobility Services Engine
- Appliance based platform that delivers a suite of mobility services software, integrates with WLAN Controller and Cisco WCS

MSE 3350***
- Tracking 18000 Devices
- WIPS for 3000 APs

MSE 3310
- Tracking 3000 Devices
- WIPS for 2000 APs
Mobility Services Licensing

Mobility Services (MSE Platform)**

**Context-Aware**

- Engine for Client & Tag tracking
- License Bundles of 1K, 3K, 6K & 12K*

**Wireless Intrusion Prevention (WIPS)**

- License Bundles of 5, 25, 100, 2000 & 3000 Monitor Mode APs*

* All SKUs of the individual mobility services are additive
MSE Evaluation Mode

- Evaluation license ships by default on MSE
- Without a license, MSE provides “try before you buy” functionality for 60 days
  - 20 wIPS APs
  - 100 Location clients
  - 100 tags
- 100 Permanent Interferers licenses are embedded in MSE. These Interferer Licenses open up as Clean Air APs (AP3500) are detected, in stages of 5 per 3500 AP
- Once the license is installed it is usage based, depending upon the service is enabled/disabled

Licenses are tied to MSE UDI
# MSE-3310 Service Support Matrix

## wIPS and Context Aware

<table>
<thead>
<tr>
<th>Clients / Tags</th>
<th>wIPS Monitor Mode APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>2000</td>
<td>2000</td>
</tr>
</tbody>
</table>

Co-existence limit of services is enforced.
## MSE-3350 Service Support Matrix

### wIPS and Context Aware

**Co-existence limit of services is enforced**

<table>
<thead>
<tr>
<th>Clients / Tags</th>
<th>0</th>
<th>1000</th>
<th>2000</th>
<th>3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>18000</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12000</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6000</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>0</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

- wIPS Monitor Mode APs
Context Aware Solution
Overview of MSE

- Overview
- System Architecture
- Deploying CAS
- Improving Accuracy
- CleanAir Interference Tracking
Overview
Context Aware


- Asset Tracking
- Zone/Inventory Management
- Condition Tracking
- Presence
- Network Location Services
Context-Aware Services (CAS) Use Cases

Network Visibility & Control
Enhanced WLAN Security
CleanAir
Asset Management
Telemetry
Worker Safety/Workflow

ASSET VISIBILITY SOLUTIONS
NETWORK VISIBILITY SOLUTIONS
Context Aware Solution

- WCS
  - Plus License
- MSE
  - Context aware License for Clients/Tags
- WLC
  - Any WLC
- AP
  - Any AP in Local Mode / LOMM mode

Graphical Display
MSE with Context-aware License
WLC
Local mode Ap

CCX tags
Wi-Fi devices
Network Visibility
Context Aware Services provide a single view showing clients, rogues, tags

client: Rogue AP: Rogue clients:
tag: 
System Architecture
Context-Aware Architecture

Cisco MSE Context Aware Service

- Provides contextual information of wired and wireless IP enabled devices

- Contextual information provided through: SOAP/XML API
Indoor Tracking

Network Management Service Protocol (NMSP)

Cisco Wireless LAN Controller

Cisco Catalyst Switch

Access Point

Wireless Client

Active RFID Tag

Cisco WCS

(Client Browser)

WCS

HTTPS

SOAP/XML over HTTP/HTTPS

3rd-party location application

Location API via SOAP/XML over HTTPS

NMSP over SSL

Cisco Mobility Services Engine (MSE)

Wired Client

Cisco WCS over SSL

Cisco Mobility Services Engine (MSE)
Indoor Tracking
Tracking Tags and Clients

Tracking tags (indoor and outdoor/outdoor-like)

- Context-aware engine for tags (partner engine)

- Utilises:
  - CAPWAP infrastructure for indoor environments
  - Wi-Fi TDOA receivers for outdoor and outdoor-like environments
  - Partner HW/SW managed by System Manager (partner) and Cisco WCS

Tracking clients (indoor)

- Context aware engine for clients (Cisco engine)

- Utilises CAPWAP infrastructure

- Managed by Cisco WCS
Indoor Tracking

RSSI Overview

- Cisco RSSI-based location tracking solution based on “network-side” RSSI measurements
- Requires min. of three AP’s; optimal accuracy requires more than 3 AP’s
- Best suited for indoor office-like environments (carpeted, low ceiling, i.e. < 20 feet)
- Main factors affecting accuracy:
  - AP density
  - AP placement
  - RF environment
Rogue Location
In real-time with WCS and MSE Context-Aware

- Track of multiple rogues in real-time (up to MSE limits)
- Can track and store rogue location historically
- Provides location of rogue clients
- Provides location of rouge ad-hoc networks
Outdoor Tracking

TDoA Overview

- Based upon relative differences in time measurement
- Requires clock synchronisation at receivers, but not the mobile device
- Requires min. of three time-synchronised TDoA receivers
- Time for message to be received at different receivers is proportional to length of transmission path between the mobile device and each receiver
Outdoor Tracking

- TDOA Receivers challenges
  - are costly, require extra synchronisation, require licences
  - require third party software platform for configuration

- Recommendations
  - RFID tags should be placed at some height (4 to 5 ft) above ground to avoid any blockage

- Cisco Outdoor Mesh APs can be used
  - MSE successfully connects to Controller with Mesh APs
  - RFID tags are detected by Mesh APs and are shown on the campus map
  - Location Accuracy Tool works with Mesh APs
  - Nearest AP support
  - Device will be displayed near the AP (with higher RSSI)
### Important Points

- Only CCX Tags can be tracked
- Tags vendors have implemented CCXv1
- Tags only operate in 2.4 GHz band
- Need Third Party “Tag Activator” to program Tags
- May need Third Party tools for “Calibration”

### Calculation Method

Received Signal Strength Indication Chokepoint for Zone Level Location

### Wi-Fi Devices or Active Tags

**Battery Powered**

Price Between $50–$80

Telemetry Capabilities

---

[http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html](http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html)
System Scalability

- MSE can be managed by only 1 WCS
- WCS can manage up to 5 MSE’s
- 1 WLC can have up to 10 NMSP sessions
  - WLC with wIPS AP’s cannot establish NMSP session with multiple MSE’s
- MSE can have up to 500 NMSP sessions (i.e. 500 WLC’s)
  - Max. limit is based on client/tag count supported per WLC
- Max. number of moving elements
  - MSE-3310: 150 elements/sec
  - MSE-3350: 900 elements/sec
- Max. number of coverage areas: 50/floor
- End-to-end latency: up to 6 seconds under full load
- APs per Floor: 100 (Limit on WCS side)
- Floors per Building in a campus: 20
## WLC – Device Tracking Capacity

<table>
<thead>
<tr>
<th>WLC Model</th>
<th>Client Capabilities</th>
<th>Tag Capabilities</th>
<th>Rogue AP Capabilities</th>
<th>Rouge Client Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLCM</td>
<td>500</td>
<td>256</td>
<td>125</td>
<td>100</td>
</tr>
<tr>
<td>2106/12/25</td>
<td>256</td>
<td>500</td>
<td>125</td>
<td>100</td>
</tr>
<tr>
<td>Catalyst 3750G with Integrated WLC</td>
<td>2,500</td>
<td>1,250</td>
<td>625</td>
<td>500</td>
</tr>
<tr>
<td>4402</td>
<td>2,500</td>
<td>1,250</td>
<td>625</td>
<td>500</td>
</tr>
<tr>
<td>4404</td>
<td>2,500</td>
<td>5,000</td>
<td>625</td>
<td>500</td>
</tr>
<tr>
<td>5508</td>
<td>7,000</td>
<td>5,000</td>
<td>2,000</td>
<td>2,500</td>
</tr>
<tr>
<td>WiSM</td>
<td>10,000</td>
<td>5,000</td>
<td>1,300</td>
<td>1,000</td>
</tr>
</tbody>
</table>
Deploying Context-Aware Services
Deploying a Context Aware Capable Infrastructure - WLAN Design

Access Point Density (Office)

- Use smaller, overlapping cells
  - For wireless data only deployments: 10% AP cell overlap
  - For wireless data + voice deployments: 20% AP cell overlap
- For good location fidelity, access points should be located 50-70 linear feet apart (15-22m)
- Typically about one access point every 2500 – 5000 square feet (230 – 460 sqm)
- Aps/Antennas height should be from 10 ft to 20 ft
- Enable Antenna Diversity
- AP’s placed too close can cause co-channel interference

Location coverage & capacity

Graphic is using only 3 channels to show option to avoid interference
AP Positioning

“Location Ready”

- Optimal AP positioning can greatly improve accuracy.
- Even distribution of APs provides better stability and repeatability of the data points.
- Four AP’s minimum <70ft (20m) with one in each quadrant of the object being tacked.
Coverage Gaps – Voice and Location

Tracking Optimised Monitor Mode APs

- Local mode AP placement and density may be sufficient for data/voice applications
- Normal Coverage Deployment places the Local Mode Aps in the Centre of the Bldg
- Good for periphery of buildings to improve location accuracy without adding extra traffic that may impact voice or client services
- Use TOMM AP’s to fill in coverage gaps

TOMMMs act as dedicated sensors for location tracking

Channels on TOMM AP’s should be same as the local mode AP’s
CleanAir Deployment Recommendations

Customer Needs/Has:
- New or Upgrading to 802.11n
- New areas for ongoing 802.11n deployments
- Networks severely impacted by non-WiFi interference

Deploy:
- Pervasively deploy 3500 in local mode
  - Self Healing
  - Troubleshooting
  - Location
  - Do not ‘sprinkle in’ local mode 3500s. Local mode 3500s scan data serving channel only.

Customer Needs/Has:
- Existing 802.11n deployments 1140, 1250
- Competitive Installed 802.11n deployments

Deploy:
- Sprinkle In 3500 in monitor mode (1 monitor AP for 5 data APs)
  - Self Healing
  - Troubleshooting
  - Location
  - CleanAir Technology required in AP for Self Healing
Rails and Regions

- Allows for certain regions in map to be defined as within or outside the scope of valid location area – improving location accuracy

- Corridors or rooms where people or assets are constantly changing positions can be especially challenging

- Three types of regions can be specified
  - Location inclusion region: tracked device cannot be outside of this polygon (examples: outside of building outer walls)
  - Location exclusion region: tracked device cannot be inside of this polygon (examples: open atrium)
  - Rails: tracked device must be within defined area with narrow band. Typically used within exclusion region (examples: conveyor belt).

- Regions defined in WCS and “pushed” (via synchronisation process to MSE)

- In MSE it works for only clients. “Cells & Masks” feature in Aero Scout – Systems Manager can be used for tags
Rails and Regions

- Rails can be used to produce a weighting effect to the devices being tracked
  - e.g. Tracking a device or person along a narrow corridor could result in the object jumping from room to room and not following a straight line.
Adding Rails
Map Editor

- Note! The rail width is doubled therefore in the example below the value required is 1.75 meters not 3.5 meters!
Rails and Regions

- Tracked device are pulled onto the rail without introducing latency
Rails and Regions

- Regions can be used to create inclusion or exclusion zones

To resize based on available browser space [click here].

Note: Please recompute RF prediction (Command -> Recompute Prediction) when Rails or Regions are modified for WCS Location.
Location Accuracy

WCS Location Readiness Tool

Yes – 7m, 90%
WCS Location Quality Tool

- Under tools select Location accuracy tool
- Define On-Demand or Scheduled scan
- Select and position device
  - Wait for 60 sec
  - Run the test for 2 minutes
- Report in CSV or PDF file format

Accuracy Test Result:
- 90% Accuracy - 3.21 meters
- 100% Accuracy - 400%

Accuracy Test Summary:
- Error Range (Meters):
  - 3.09 or less
  - 3.01 to 5.00
  - 5.01 to 7.00
  - 7.01 to 10.00
  - 10.01 or more

Accuracy Test Histogram
- Error Distance Histogram
- Accuracy Test CDF
- Cumulative Error Distribution

Result: 7m, 90%
Understanding Cumulative Probability Distribution

~60% of devices within 7m

Accuracy Test Result (%)

98.14 \((49.31+25.86+17.53+5.11+1.86)\)

<table>
<thead>
<tr>
<th>Error Range (Meters)</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.00 or less</td>
<td>49.31</td>
</tr>
<tr>
<td>3.01 to 5.00</td>
<td>25.86</td>
</tr>
<tr>
<td>5.01 to 7.00</td>
<td>17.53</td>
</tr>
<tr>
<td>7.01 to 10.00</td>
<td>5.11</td>
</tr>
<tr>
<td>10.01 or more</td>
<td>1.86</td>
</tr>
</tbody>
</table>
# Network Visibility

Context Aware Services allows creation of alarm conditions & trigger notifications

<table>
<thead>
<tr>
<th>Absence</th>
<th>Last Hour</th>
<th>24 Hours</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Notifications</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Client Stations</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rogue AccessPoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>In/Out Area</th>
<th>Last Hour</th>
<th>24 Hours</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Notifications</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Client Stations</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rogue AccessPoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location Changes</th>
<th>Last Hour</th>
<th>24 Hours</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Notifications</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Client Stations</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rogue AccessPoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Movement from Marker</th>
<th>Last Hour</th>
<th>24 Hours</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Notifications</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Client Stations</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rogue AccessPoints</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Battery Level</th>
<th>Last Hour</th>
<th>24 Hours</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Notifications</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

© 2011 Cisco and/or its affiliates. All rights reserved.
**Network Visibility**

**Context Aware Services** provide stats, usage pattern for clients/tags/rogues/interferers and location history with play back.

### Context Aware Service: Alpha-mse1

<table>
<thead>
<tr>
<th>Services &gt; Mobility Services &gt; Context Aware Service &gt; General</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>General Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Operational Status</td>
</tr>
<tr>
<td>Number of Tracked Clients</td>
</tr>
<tr>
<td>Number of Tracked Tags</td>
</tr>
<tr>
<td>Number of Tracked Rogues</td>
</tr>
<tr>
<td>Number of Tracked Interferers</td>
</tr>
<tr>
<td>Total Elements Tracked</td>
</tr>
<tr>
<td>Tracked Elements (Clients, Rogues and Interferers) Limit</td>
</tr>
<tr>
<td>Tracked Tags Limit</td>
</tr>
</tbody>
</table>

### Client Location History

<table>
<thead>
<tr>
<th>Change selection every</th>
<th>2 secs</th>
<th>Play</th>
<th>Stop</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Floor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Aug 17 07:58:20 PDT 2009</td>
<td>Cisco San Jose - Site 5&gt;BLD 14&gt;3rd floor</td>
</tr>
<tr>
<td>Thu Aug 13 08:55:31 PDT 2009</td>
<td>Cisco San Jose - Site 5&gt;BLD 14&gt;3rd floor</td>
</tr>
<tr>
<td>Wed Aug 12 12:05:16 PDT 2009</td>
<td>Cisco San Jose - Site 5&gt;BLD 14&gt;3rd floor</td>
</tr>
<tr>
<td>Wed Aug 12 10:39:14 PDT 2009</td>
<td>Cisco San Jose - Site 5&gt;BLD 14&gt;3rd floor</td>
</tr>
<tr>
<td>Wed Aug 12 09:21:12 PDT 2009</td>
<td>Cisco San Jose - Site 5&gt;BLD 14&gt;3rd floor</td>
</tr>
<tr>
<td>Wed Aug 12 09:06:12 PDT 2009</td>
<td>Cisco San Jose - Site 5&gt;BLD 14&gt;3rd floor</td>
</tr>
</tbody>
</table>

### Client Location

Location Calculated at: Cisco San Jose - Site 5>BLD 14>3rd floor
Improving Accuracy
Enabling Accurate Location

802.11 doesn’t require mobile devices to constantly advertise their presence to the network. A “silent” mobile becomes invisible to the network.

How to ensure continuous location of Mobile devices!?

CCX Mobile devices *always* send periodic location track frames to the Cisco Unified Wireless Network including transmit channel and transmit power info.

Network can compute accurately the mobile device position.

Benefits: Ensures mobile device can be accurately localised.
Comparison of Client Drivers Features

<table>
<thead>
<tr>
<th>Legacy</th>
<th>S36</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non – CCX Or CCXv1</td>
<td>CCXv2 or higher</td>
</tr>
<tr>
<td>Aps do not know Tx Power of the probes</td>
<td>Aps do not know Tx Power of the probes</td>
</tr>
<tr>
<td>Aps do not know channel frequency of the probes</td>
<td>Aps do not know channel frequency of the probes</td>
</tr>
<tr>
<td>Probes can be detected on a wrong channel at a reduced power</td>
<td>Probes can be detected on a wrong channel at a reduced power</td>
</tr>
<tr>
<td>Probes transmitted infrequently</td>
<td>Frames scheduled periodically</td>
</tr>
<tr>
<td>Path Loss Model can show very large scale RSSI variations</td>
<td>Path Loss Model can show RSSI variations- but variations are averaged as more frequent info available</td>
</tr>
</tbody>
</table>

**S36 is a feature of CCX applicable to CCXv2 & higher**

**S60 is a feature of CCX applicable to CCXv4 or higher**
WCS Planning Tool

- WCS has the ability for planning and simulating RF propagation for data, voice and location services primarily in indoor office or similar areas
  - Supports Cisco AP’s and antenna only
  - Provides a 2 dimensional prediction model and report
  - Automatic or manual AP deployment
  - Does not consider obstacles or wall attenuation when calculating AP positions
  - True RF coverage pattern including obstacles and wall attenuation
WCS Map Editor

1st Verify map is to scale

Use scaling tab to reset map scale

Use horizontal or vertical drag & drop to select distance

Note! A warning notification usually indicates the building requires resizing
Wall and partition properties

- Use obstacle type to define dB loss Note! These values are recommendation only

- Multiple lines can be combined to obtain required loss!

Use obstacle tab to Select wall properties

- 1dB Cubicle
- 1.5dB Glass
- 2dB Light Wall
- 4dB Light door
- 13dB Thick Wall
- 15dB Heavy Door
Calibration Models

- After implementation, calibration function available within WCS can be used for higher location accuracy.

- WCS provides a way for user to calibrate signal characteristics for a particular indoor environment or similar areas.

- More accurate the model used — more better is the Location Accuracy.

- Point calibration: client at fixed location. One location at a time.

- Linear calibration: data collected between two different points (straight line).

- Aero Scout-Systems Manager should be utilised to do the calibration function for Tags.

- Calibration with non CCX clients Not supported.

- CCX version check Monitor>Clients>Client Details.
Calibration – Point Mode

Disable RRM AP Power mode
Calibration should be performed for every band

Represented completed calibration area
Calibration – Point Mode

After calibration model is created following steps are essential:

- Apply this model to the floor map(s)
- Synchronise WCS with MSE

**MSE is not involved during Calibration process**

Calibration date collected for entire floor space
Launch this from Calibration Detail Page after calibration to check on how good the data points collected are and how much improvement is achieved for the desirable accuracy.

Calculated Location
Test Point
Participating Aps displayed with RSSI values

Scrolling Mouse on the area displays test points and also identifies the Aps (who participated in calibration) as "blue" with RSSI values.
Summary of Best Practices for Location Deployment

Design 802.11 Network for Context Aware Services

- Proper AP density and placement
- Create an AP Perimeter
- Use S36/S60 clients (S36/S60 is a CCX feature)
- Calibrate the environment
- Use rails & regions
- Make sure interference level is low
- Chokepoints will help prevent inter-floor problem and provide room level accuracy
- When using tags config ch 1, 6 and 11 with 3 repetitions/channel (motion enabled & chirp rate configured)
CleanAir Interference Tracking
What is CleanAir Technology?

- Classification processed on Access Point
- Interference impact and data sent to WLC for real-time action
- WCS and MSE store data for location, history, and troubleshooting
Network Visibility

Context Aware Services enable WCS to show Interferer’s location

NEW

Map – Air Quality View

Interferer Details

DECT Like Phone

Bluetooth Link

AP3500

Zone of Impact

Contributing APs

Heatmap Type: 
- IDS
- Coverage
- Air Quality

Use: 
- Average AQ
- Minimum AQ

Interferer Filter

Filter:
- Interferer Status: All
- Severity greater than: 0
- Interference Type: All Interferers

Display:
- Show Small Icons: No
- Show Zone of Impact: Yes

Type: DECT Like Phone
State: Active
Affected Channels: 6
Detecting AP(s): S3C14+41A+6A+6 (Cluster Center)
Duty Cycle: 1
Severity: 1
First Detected: 4/25/10 9:02:52 PM
Last Reported: 4/25/10 9:25:20 PM
Zone of Impact: 110.60 feet
# Cisco CleanAir Components

<table>
<thead>
<tr>
<th>Product</th>
<th>Licensing Requirements</th>
<th>Functionality</th>
</tr>
</thead>
</table>
| AP3500                | ▪ None                                                      | ▪ Multi-interferer Detection & Classification  
▪ AirQuality Monitoring  
▪ Self-Healing Event Driven RRM |
| Wireless LAN Controller | ▪ Standard per AP                                           | ▪ AirQuality Aware RRM  
▪ Self-Learning Persistent Device Avoidance  
▪ Spectrum Expert Connect  
▪ AirQuality and Interferer Alerts |
| MSE                   | ▪ Context Aware “endpoints” required for each interferer tracked  
▪ MSE adds support for 100 interferers when AP3500 present (5 per AP, additive) | ▪ Interferer Tracking & Zone of impact  
▪ Merging or correlating interferers from multiple WLCs (pseudo MAC)  
▪ Location Calculations  
▪ History Storage |
| WCS                   | ▪ Standard per AP count  
▪ WCS Plus required for MSE                                 | ▪ Remote Client Troubleshooting  
▪ AirQuality Visualisation and Mapping  
▪ Forensics Tools  
  ➢ Location Visualisation  
  ➢ Impact Analysis  
  ➢ History Playback |
Adaptive wIPS
Wireless Security Threats

**Top Attacks**

**On-Wire Attacks**

- Ad-hoc Wireless Bridge
  - HACKER
  - Client-to-client backdoor access

- Rogue Access Points
  - HACKER
  - Backdoor network access

**Over-the-Air Attacks**

- Evil Twin/Honeypot AP
  - HACKER'S AP
  - Connection to malicious AP
  - Service disruption

- Reconnaissance
  - HACKER
  - Seeking network vulnerabilities
  - Sniffing and eavesdropping

**Cisco wIPS Detects These Attacks**

- Non-802.11 Attacks
  - Backdoor access
  - Service disruption
  - Cisco Spectrum Intelligence
  - Detects These Attacks

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public
# Security Features in Different AP modes

<table>
<thead>
<tr>
<th></th>
<th>Local</th>
<th>Monitor</th>
<th>wIPS Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Servicing</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Rogue Detection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rogue Containment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rogue Detection and containment</td>
<td>Slow</td>
<td>Fast</td>
<td>Fast</td>
</tr>
<tr>
<td>Attack Detection</td>
<td>17</td>
<td>17</td>
<td>40+</td>
</tr>
<tr>
<td>MSE Needed</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Attack Encyclopedia in Alerts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Forensics or Packet captures</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Event Correlation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WCS needed</td>
<td>No</td>
<td>No</td>
<td>Yes (Plus license)</td>
</tr>
</tbody>
</table>
Cisco’s Attack Detection Mechanisms

Base IDS

- Built-in to controller software
- Uses Local and Monitor Mode APs

Adaptive wIPS

- Requires MSE
- Uses wIPS Monitor Mode APs
## Adaptive wIPS Differences from Base Controller IDS

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Correlation</td>
<td>- Reduced false alarms</td>
</tr>
<tr>
<td>Number of attacks</td>
<td>- Only 17 on base controller IDS</td>
</tr>
<tr>
<td>Forensics</td>
<td>- Packet capture of attack</td>
</tr>
<tr>
<td>Historic Reporting</td>
<td>- Longer attack archives</td>
</tr>
</tbody>
</table>
Adaptive wIPS
Components and Functions

AP
- Attack Detection
- 24x7 Scanning

WLC
- Configuration

MSE
- Alarm Archival
- Capture Storage

WCS
- Centralised Monitoring
- Historic Reporting

Over-the-Air Detection

wIPS AP Management

Complex Attack Analysis, Forensics, Events

Monitoring, Reporting
MSE System Configuration

- Use the following command which starts wizard to guide the user in setting the system parameters
  - `/opt/mse/setup/setup.sh`

- `/opt/mse/setup/setup.sh` must be used for –
  - Host name / Domain name changes
  - Changing system IP address/subnet
  - Dual homing
  - Routes configuration
  - Console/ssh access settings
  - Root password changes
  - WCS user password changes

- For managing Context Aware Engine for Clients
  - Start command: `/etc/init.d/msed start`
  - Status command: `/etc/init.d/msed status`
  - Stop command: `/etc/init.d/msed stop`
  - Restart command: `/etc/init.d/msed restart`
“getserverinfo” Command

---

Context Aware Service

---

Total Active Elements (Clients, Rogues, Interferers): 129
Active Clients: 34
Active Tags: 29
Active Rogues: 66
Active Interferers: 0
Active Wired Clients: 0
Active Elements (Clients, Rogues, Interferers) Limit: 100
Active Tag Limit: 100
Active Wired Clients Limit: 0
Active Sessions: 1

Clients Not Tracked due to the limiting: 481
Tags Not Tracked due to the limiting: 0
Rogues Not Tracked due to the limiting: 1306
Interferers Not Tracked due to the limiting: 0
Wired Clients Not Tracked due to the limiting: 0
Total Elements (Clients, Rogues, Interferers) Not Tracked due to the limiting: 1787

---

Context Aware Sub Services

---

Sub Service Name: aeroscout
Version: 3.2.0 - 4.0.14.13
Description: AeroScout® Location Engine for RSSI and TDOA asset tracking
Registered: true
Active: true
Watchdog Process ID: 25579
Engine Process ID: 25761
Troubleshooting NMSP Issues

Common Issue (certificate exchange) seen with NMSP

- Time synchronisation/configuration
- Key hash template
- Key exchange
- WCS Communication Password mismatch
- NMSP Status on the WLC
- NMSP Status on the MSE
- NMSP Status on the WCS
Time Synchronisation/Configuration

- Possible symptom of clock discrepancy between WLC and MSE: can’t establish NMSP connection after adding MSE to the system

- Suggested course of action:
  - Use NTP server for synchronising clocks (recommended)
  - Manual configuration (controller time should be ahead of time on MSE)
Establishing NMSP Connection

MSE

root@mse ~]# cmdshell
cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
Server Auth Info

MAC Address: 00:1e:0b:61:35:60
Key Hash: 5384ed3cedc68eb9c05d36d98b62b06700c707d9
Certificate Type: SSC

WLC

(Cisco controller) >config auth-list add lbs-ssc <MSE Ethernet MAC> <MSE key hash>

(Cisco Controller) >show auth-list
Mac Addr    Cert Type    Key Hash
-----------------------   -------   ------------------------------
00:1e:0b:61:35:60  LBS-SSC  5384ed3cedc68eb9c05d36d98b62b06700c707d9

Note: WCS template for adding MSE should create association between MSE and WLC automatically. Manual process should not be required.
WCS Communication password mismatch

- WCS communication password is set in MSE during initial setup running “setup script”. Default is “admin/admin

- Use the same password while adding MSE to the WCS

To fix the mismatch, run the set up script again using /opt/mse/setup/setup.sh
Verifying NMSP Connection Status (WLC/MSE)

(Cisco Controller) > show nmsp status

<table>
<thead>
<tr>
<th>LocServer IP</th>
<th>TxEchoResp</th>
<th>RxEchoReq</th>
<th>TxData</th>
<th>RxData</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.20.224.17</td>
<td>18006</td>
<td>18006</td>
<td>163023</td>
<td>10</td>
</tr>
</tbody>
</table>

Context Aware Service

Total Active Elements (Clients, Rogues, Interferers): 129
  - Active Clients: 34
  - Active Tags: 29
  - Active Rogues: 66
  - Active Interferers: 0
  - Active Wired Clients: 0

Active Elements (Clients, Rogues, Interferers) Limit: 100
  - Active Tag Limit: 100
  - Active Wired Clients Limit: 0

Active Sessions: 1

root@mse ~]# getserverinfo | more

# of active NMSP sessions
NMSP Status on WCS for MSE

- Navigate to Services>Mobility Services>MSE>Status
- WLC could have been added, but NMSP status can be “Inactive”
NMSP Status Troubleshooting Tab on WCS

- Click on the NMSP Troubleshooting Tab
- Provides you the status of the common NMSP issues
1. From WCS, Navigate to **Services > Synchronisation Services**
2. Tabs for Network Design, Event Groups, Controllers, Wired Switches placed on left
3. GUI is more interactive with clear messaging
4. Click on Controllers, and select the Controller to be assigned to the MSE

5. Click on “Change MSE Assignment”, select the services (CAS/WIPS) on each MSE

**Service based assignment:** MSE can be assigned to any WLC on a per-Service basis
Synchronisation- Interactive GUI contd.

6. Selected services (CAS/WIPS) are displayed

7. Clear message showing that Synchronisation is pending for the Controller
Synchronisation - Interactive GUI contd..

8. Select Controller, and Click on “Synchronisation” Tab on top left corner

9. Controllers and MSE are completely synchronised
Synchronisation - Interactive GUI contd..

8. Click on “NMSP Status” TAB

9. Verify if MSE is communicating with each Controller for chosen services only

### NMSP Connection Status Details: 50.50.1.11

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>50.50.1.11</td>
</tr>
<tr>
<td>Version</td>
<td>7.0.94.33</td>
</tr>
<tr>
<td>Target Type</td>
<td>Controller</td>
</tr>
<tr>
<td>NMSP Status</td>
<td>Active</td>
</tr>
<tr>
<td>Echo Request Count</td>
<td>1</td>
</tr>
<tr>
<td>Echo Response Count</td>
<td>1</td>
</tr>
<tr>
<td>Last Activity Time</td>
<td>December 14, 2009 5:00:46 PM PST</td>
</tr>
<tr>
<td>Last Echo Request Message Received At</td>
<td>December 14, 2009 5:00:45 PM PST</td>
</tr>
<tr>
<td>Last Echo Response Message Received At</td>
<td>December 14, 2009 5:00:45 PM PST</td>
</tr>
<tr>
<td>Model</td>
<td>4400</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:10:73:36:00:40</td>
</tr>
</tbody>
</table>

### Capable NMSP Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Subservices</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS</td>
<td>WIRELESS IDS</td>
</tr>
</tbody>
</table>
Synchronisation - Interactive GUI contd..

Similarly Network Designs, Wired Switches and Event Groups can be Synchronised

Network Designs

Modifying assignments for Network Designs will auto assign the Controllers for CAS. Modifying assignments at Campus or Building level always overrides any previous assignments of their children maps.

Choose MSEs

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>CAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE 1</td>
<td>10.51.1.30</td>
<td></td>
</tr>
</tbody>
</table>

Save | Cancel
Enhanced Synchronisation History

- Synchronisation History shows
  - Automatic Synchronisation
  - Automatic Controller Selection/Assignment
  - Smart Synchronisation

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Server</th>
<th>Element Name</th>
<th>Type</th>
<th>Sync Operation</th>
<th>Generated By</th>
<th>Status</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/10 2:59 PM</td>
<td>MSE 1</td>
<td>SEVT CONTROLLER (10.01.1.10)</td>
<td>Controller</td>
<td>Add</td>
<td>Manual</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>2/1/10 2:03 PM</td>
<td>MSE 1</td>
<td>SEVT CONTROLLER (10.01.1.10)</td>
<td>Controller</td>
<td>Add</td>
<td>Automatic</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>2/1/10 1:56 PM</td>
<td>MSE 1</td>
<td>Cisco Controller (1.05.1.1.15)</td>
<td>Controller</td>
<td>Delete</td>
<td>Automatic</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>2/1/10 1:58 PM</td>
<td>MSE 1</td>
<td>SEVT CONTROLLER (10.01.1.10)</td>
<td>Controller</td>
<td>Delete</td>
<td>Automatic</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>1/28/10 12:58 PM</td>
<td>MSE 1</td>
<td>Cisco Controller (1.05.1.1.15)</td>
<td>Controller</td>
<td>Update</td>
<td>Manual</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>1/28/10 11:22 AM</td>
<td>MSE 1</td>
<td>Cisco Network Design</td>
<td></td>
<td>Update</td>
<td>Automatic</td>
<td>Success</td>
<td></td>
</tr>
</tbody>
</table>
Enable Element Tracking

If checked (Enabled), only then:

- Devices will be tracked
- History will be available

Special Check for wired clients

Client Lic. Include interferers
History Parameters

- Number of days to save history is not limited in WCS UI
  - Limited by disk space and system performance
- History of an element is recorded only if:
  - Element moves more than 10m (30 ft)
  - Tag: emergency or panic button is pressed
  - Tag: passes by an exciter
  - Floor changes, i.e. element moves between floors
- Element is declared inactive if it remains inactive for an hour. If it remains inactive for 24 hours, it is removed from "tracking table", and it is not possible to see element’s historical location on the WCS Monitoring page. "Absent Data Cleanup Interval" helps to control “tracking table”
Intuitive Logging with 7.0 code

- **Mac address based logging**: Max of 5 mac adds. at a time, 2 files/mac add

- **Configurable Log Files**: Number of files and the file size is configurable. Max size of the combined log files is 1 GB (20 files x 50 Mb)

- **Persistent Logging**: Log Modules, Logging levels, Log file parameters are preserved after MSE upgrade or reboot

Logging options moved under one tab
Logs go to opt/mse/logs/locserver
## Intuitive Log File Indexing

Log file now includes output of `getserverinfo`, licensing info, sys parameters, run `diag`, solid crash, etc.

### Licensing Information

<table>
<thead>
<tr>
<th>License Elements</th>
<th>Licensing Limit</th>
<th>License Status</th>
<th>License Type</th>
<th>Count</th>
<th>Unlicensed Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Limit</td>
<td>100</td>
<td>Active</td>
<td>Permanent</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>License status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Licensing Information (client)

<table>
<thead>
<tr>
<th>License Elements</th>
<th>Licensing Limit</th>
<th>License Status</th>
<th>License Type</th>
<th>Count</th>
<th>Unlicensed Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Limit</td>
<td>1000</td>
<td>Active</td>
<td>Permanent</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>License status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Licensing Information (WIPS Monitor Mode APs)

<table>
<thead>
<tr>
<th>License Elements</th>
<th>Licensing Limit</th>
<th>License Status</th>
<th>License Type</th>
<th>Count</th>
<th>Unlicensed Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Limit</td>
<td>100</td>
<td>Inactive</td>
<td>Evaluation</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>License status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Licensing Information (WIPS Enhanced Local Mode APs)

<table>
<thead>
<tr>
<th>License Elements</th>
<th>Licensing Limit</th>
<th>License Status</th>
<th>License Type</th>
<th>Count</th>
<th>Unlicensed Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Limit</td>
<td>10</td>
<td>Active</td>
<td>Evaluation</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>License status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Log Files

- **Solid DB Log File**
  - `/solmsg.out` - Solid DB

- **MSE Context Aware Service Log File**
  - `/locserver-0-0.log`
  - `/locserver-1-0.log`
  - `/locserver-2-0.log`
  - `/locserver-3-0.log`
  - `/locserver-4-0.log`

- **Installation Log File**
  - `/locserver-error-0-0.log`
  - `/locserver-error-1-0.log`
  - `/locserver-error-2-0.log`
  - `/locserver-error-3-0.log`
  - `/locserver-error-4-0.log`
  - `/locserver-error-5-0.log`
  - `/locserver-error-6-0.log`
  - `/locserver-error-7-0.log`
  - `/locserver-error-8-0.log`
  - `/locserver-error-9-0.log`

### MSE rundiag Log File

- `/rundiag.out`

- **MSE Framework Log File**
  - `/mse-framework.log`
  - `/mse-framework.log.1`
  - `/AeroScoutEngine.log`

### Session Information

- **Session ID**: 7058
- **Session User ID**: 1
- **Session IP Address**: 10.51.1.30
- **Session start time**: Mon Feb 01 13:37:44 PST 2016
- **Session last access time**: Tue Feb 02 16:45:55 PST 2010
Minimising Latency

- Tag notification frame interval for stationary tag 3-5 minutes
- Tag notification frame interval for moving tags <10sec
- WLC NMSP aggregation window is 2 sec by default
- Correct aggregation window should be set to make sure that WLC has received updates from all the APs, before sending data to MSE via NMSP
- From WLC CLI aggregation window can be set independently for clients, tags, rogue APs, rogue clients and RFids

(Cisco Controller) >config nmmsp notification interval rssi ?

clients       Measurement interval for clients.
rfid          Measurement interval for rfid tags.
rogues        Measurement interval for rogue APs and rogue clients
Latency settings from WCS

Example:
WLC 1 has a 5 seconds aggregation window
WLC 2 has 2 seconds aggregation window
The AES engine will set its window to 5 sec to match with the biggest window on all WLC(s)

Auto-sync, sends the changes automatically to MSE, if WLC was already synchronised
Immediate Notification from MSE

Business Application

SOAP/XML API

Context-Aware Software

Context Aware Engine for Clients

RSSI

RSSI / TDOA

Context Aware Engine for Tags

Indoor Environment

Mobile User
Voice over 802.11

Smart Phone

802.11 Clients

Indoor & Outdoor Environments

802.11 CCX Tags

Back and forth travel of Information between MSE to AES can be skipped with 7.0 code
Immediate Notification from MSE

- With 7.0 code MSE can forward the tag info straight to third party, bypassing the AES engine.

- Configuration available from aes-config.xml file (dir: /opt/mse/locserver/conf/) with parameters:
  1. Enable-immediate-notification-Default value False
  2. Forward-notification-without-location- Default value False

- Setting the first parameter to true will cause the MSE to immediately send the notification to Mobile View or any other application. This however will have old or no location.

- After the location calculation another notification will be fired with the latest location value.

- If the location is not needed at all, then the second parameter should be set to true. Note the MSE will just act as a forwarding engine in this case and no location calculations will be computed.
Wired Location Detection

- Switches report to MSE switch port mapping of connected devices
- MSE actively tracks communicated information and location of both devices and chassis
  - MSE maintains history of device connect, connection location, and device disconnect
- MSE provides SOAP XML API to external systems that are interested in location of chassis or endpoint devices
- Applications can query or receive async events when devices or chassis move location
Wired Location with MSE

- MSE tracks location history of wired clients
- WCS configures MSE with list of switches
  - Add Ethernet switches { add IP addresses, add SNMP Community (read-write), enable location capability}
- Location information configured using switch CLIs
  - Define the location identifier
  - Enable ip device tracking
  - Attach the identifier to the switch interface
- Switch and MSE communicate using NMSP
- Switches notify MSE of wired client association / disassociation
- Switches supported - Catalyst 2960, 3750, 3750E, 3560, 3560E, 4500, 4900

Required software versions –

- Catalyst switches – 12.2(50)SE
- WCS – 6.0.x onwards
- MSE – 6.0.x onwards

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>nmsp enable</td>
<td>Enable the NMSF features on the switch</td>
</tr>
<tr>
<td>3</td>
<td>nmsp notification interval (attachment</td>
<td>Specify the NMSF notification interval. location), interval-seconds</td>
</tr>
<tr>
<td></td>
<td>attachment—</td>
<td>Specify the attachment notification interval.</td>
</tr>
<tr>
<td></td>
<td>location—</td>
<td>Specify the location notification interval.</td>
</tr>
<tr>
<td></td>
<td>interval-seconds—</td>
<td>Duration in seconds before the switch sends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the MSE the location or attachment updates. The range is 1 to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30; the default is 30.</td>
</tr>
</tbody>
</table>

This example shows how to enable NMSF on a switch and to set the location notification time to 10 seconds:

```
Switch(config)# nmsp enable
Switch(config)# nmsp notification interval location 10
```
Deployment Checklist

- Follow proper AP placement guidelines (location and density)
- Configure NTP server on both WLC and MSE or manually synchronise both the devices (and preferably WCS) with the correct time and time zone.
  - Note: controllers use GMT (UTC) time with correct time zone to derive local time. Consequently, time needs to be entered in UTC and the correct time zone specified.
- Specify which controllers should talk to which MSE using the WCS MSE Synchronisation page
- Check that certificates are exchanged correctly
- Check the NMSP connection status on the controller
- Ensure that tracking is enabled for the right devices
- Ensure that the maps and AP positions are synchronised between the WCS and MSE
- Ensure that location calculations are taking place either on the tracking page or the MSE console using `getserverinfo` command

For Clients

- Verify tracking is enabled on MSE
- Verify clients are detected by controller
- Max calculation time taken into account

For Tags

- Verify tracking is enabled on MSE
- Verify tags are detected by controller
- Max calculation time taken into account
Recommended Reading

- Cisco Mobility Services Engine - Context Aware Mobility Solution Deployment Guide

- Cisco Context-Aware Service Configuration Guide

- Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide

- Location Appliance to MSE Migration Guide

- WiKi Page External

- AeroScout Support Page
  http://support.aeroscout.com
Q & A
Complete Your Online Session Evaluation

Complete your session evaluation:

- Directly from your mobile device by visiting www.ciscoliveaustralia.com/mobile and login by entering your badge ID (located on the front of your badge)

- Visit one of the Cisco Live internet stations located throughout the venue

- Open a browser on your own computer to access the Cisco Live onsite portal