This document focuses on the application of general design best practices for the Cisco Context-Aware Services (CAS) and the Cisco Mobility Services Engine (MSE) when integrating into the Service Ready Architecture for Schools (SRA). It is intended as a guide to producing scalable and functional designs that incorporate CAS, where such inclusion can be seen to provide real-world benefits.

Note that while this document attempts to be as comprehensive as is warranted by the subject matter being discussed, it is not intended to be a comprehensive technical guide on Cisco Context-Aware Services, RFID technology, or the Cisco Mobility Services Engine in general. For comprehensive configuration and deployment information, the reader should refer to the in-depth configuration and deployment guides mentioned throughout this document.

Introduction

What Are Context-Aware Services?

Context-Aware Services provides the ability to dynamically capture and use contextual information about assets to optimize existing communications flows and organizational processes or facilitate the establishment of new ones. Contextual information can be collected for assets involved in almost any activity or process and this includes not just network endpoint devices (such as laptops and VoIP Phones) and products (such as microscopes and video projectors), but in some cases also the users that are associated with such devices.

In environments where the Cisco Unified Wireless Network has been deployed, Context-Aware Services makes use of embedded 802.11 network interface adapters (radios) in wireless client devices to accumulate contextual information about those assets or the user associated with the asset. For example, the location of a wireless laptop can be calculated via several different approaches or the user name associated with the laptop's user may be collected.

For assets that do not possess embedded wireless interfaces, external active Radio Frequency Identification (RFID) tags and sensors can be used to provide location input and monitor ambient environmental characteristics. Sensor capabilities can be directly embedded into active RFID tags in order to link the data captured (for instance, whether the asset is currently in motion) with the location of the asset. The algorithms used to determine location vary depending on the Radio Frequency (RF) environment and the accuracy required for a specific application.

In some cases, it may be necessary to track an asset with a high degree of accuracy throughout a school, such as when it is necessary to determine where a missing valuable asset is currently located). On the other hand, some applications using context-aware services may only require general indication of whether an asset is in or out of a permissible zone (such as the confines of a chemistry lab area for example).

Context-Aware Services can also provide location and other contextual information for wired devices attached to certain Cisco Catalyst LAN switches. With the correct level of software, switches such as the 2960G, 3560E, 3750E, 3750G, 4500, and 4900 series can become context-aware. Catalyst switches that are context-aware can provide civic location details for wired devices to the Cisco Mobility Services Engine based on pre-configured information specified for each switch port. This information can then be presented to users in a tabular format combined with other contextual information such as user name, device serial number and emergency location identifier numbers (ELINs).

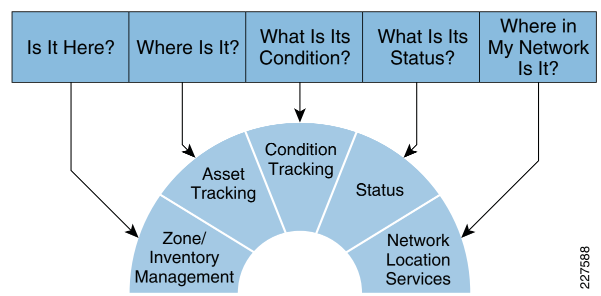
Note A civic location specifies the civic address and postal information for a physical location using fields such as the number, street or road name, community, and county assigned to residential, commercial, institutional, and industrial buildings (e.g., 31 Main Street, Alpharetta, Georgia 30004). An emergency location identifier number (ELIN) is a number that can be used by the local public safety answering point (PSAP) to look up the geographic location of the caller in a master database known as the automatic location information (ALI) database. The ELIN also allows the PSAP to call back the emergency caller directly in the event the phone call is disconnected.

For a more detailed overview of Context-Aware Services, refer to the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns788/solution_overview_c22-475173.html.

Why Use Context-Aware Services?

The information that can be provided by Context-Aware Services across its application API can generally be classified into five functional categories, as shown in Figure 1.

Figure 1 Five Functional Categories of Context-Aware Services



Is It Here?—Zone or Inventory Management

Zone or inventory management applications that utilize Cisco Context-Aware Services can define specific zones in which they monitor mobile assets that possess embedded wireless interfaces or have been outfitted with Cisco Compatible Extensions compliant RFID tags. These devices can be tracked and monitored when they enter and exit both permissible and non-permissible areas. Notifications can be generated when monitored assets stray away into areas where they should not enter. Examples of how zone or inventory management may be used in the school environment include:

- Issuing notifications to administrators or school resource officers when school assets are moved out of authorized areas
- Alerting appropriate parties when persons equipped with RFID-enabled ID badges enter unauthorized areas
- Providing indication to teachers and assistants upon the arrival of an authorized parent or guardian that has arrived to pick-up their children at the end of the day

Further details about zone or inventory management can be found at the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns788/solution_overview_c22-475178.html.

Where Is It?—Asset Tracking

Asset tracking applications that incorporate Context-Aware Services can help locate assets within the school, whether they are connected to wired or wireless infrastructure. In this way, Cisco Context-Aware Services can provide great value to school administrators, teachers, security personnel, or anyone who must quickly and effectively locate and recover missing assets. Examples of how asset tracking may be used in the School environment include:

- Locating wired and wireless portable assets (such as a portable video projector or flat panel display) for class use or faculty presentations
- Locating personnel possessing wireless VoWLAN phones or RFID-enabled badges in both emergency and non-emergency situations
- Identifying the past pattern of movement associated with an asset by enabling the review of archived location history information in both a tabular and a graphical format. Such audit trails can be especially useful when incorporated into security applications that can combine this information with other information sources, such as video surveillance.

Further detail regarding asset tracking can be found at the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns788/solution_overview_c22-475177.html.

What Is Its Condition?—Condition Tracking

Condition tracking applications utilizing Context-Aware Services can monitor select characteristics of an asset's internal or external environment, such as variations in temperature, humidity, pressure, quantity, fluid volume, etc. Any change in these characteristics beyond set thresholds can trigger alerts, notifications, or other application-dependent actions. Examples of how condition tracking may be used in the School environment include:

- Temperature and humidity telemetry passed by RFID tag sensors can be utilized in school food service applications to monitor the temperature of food refrigeration units, guarding against costly spoilage and premature replacement.
- Fluid level sensors placed in combination with RFID tags can be used to monitor critical fluid levels in school maintenance applications, such as fuel oil levels for school generators and remote fuel storage for building heating.
- Indication of excessive or insufficient pressure in systems such as school heating and cooling, school labs (vacuum, air, and various gases), and so on can be passed as telemetry data using properly equipped RFID tag sensors.

What Is Its Status?—Status Monitoring

Applications that monitor changes in user and asset status can use Context-Aware Services to detect status transitions, such as a change from a normal state to one indicating that an extraordinary event has occurred. Examples of how this may apply to the school environment include:

- RFID tags with user push buttons could be used to covertly pass indication of situations where assistance is needed, along with the location of the tag at the time of activation.
- Attempted asset tampering, such as the removal of RFID asset tags themselves or jostling of any type, can trigger status monitoring applications to generate alerts.
- The introduction of new assets into a school location, or any changes in the motion status of existing assets above a certain threshold, can serve as preliminary indication to building energy management systems regarding potential building environmental modifications, such as lighting, zone heating, or zone cooling.

Where Is It in My Network?—Network Location Services

Network location applications interfacing with the Context-Aware Services can help optimize the distribution of both wired and wireless network resources, reduce troubleshooting time, help eliminate waste due to use of network resources by unauthorized "rogue" devices, and help lower the overall total cost of network operation. Examples of how this may apply to the school environment include:

- Location and removal of unauthorized 802.11 wireless devices operating within a school building, which helps reduce the school system's exposure to the introduction of malicious external software as well as its liability to illegal file sharing activities.
- Ongoing tuning of the wireless network by identifying areas where the routine congregation of wireless users is heavier than expected. This may prompt adjustments in wireless network parameters, the number of access points deployed, or the placement of access points.

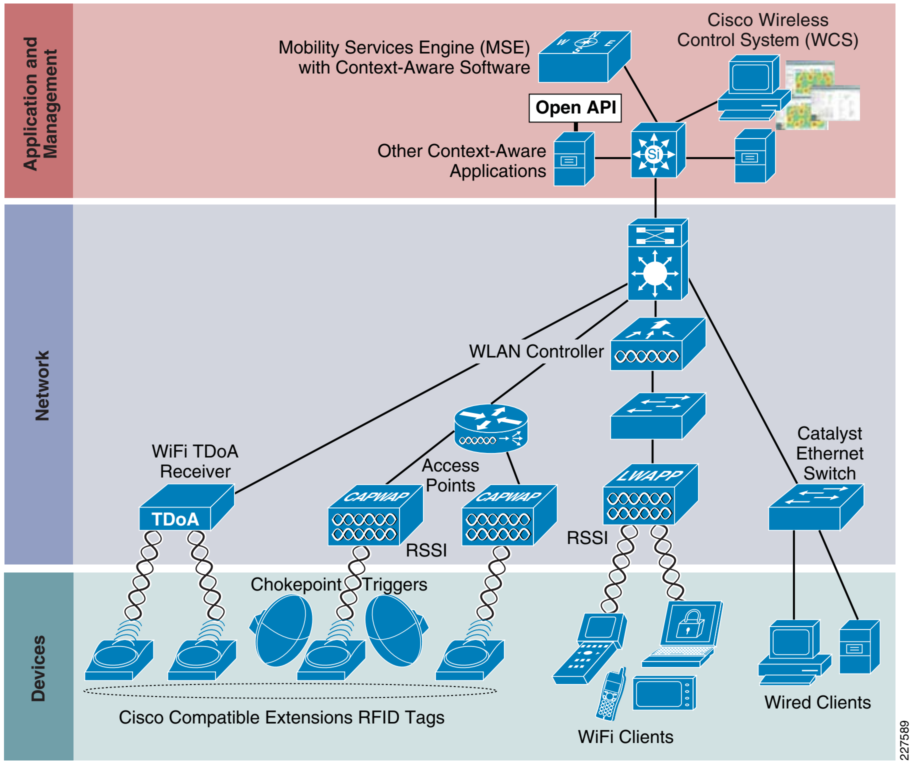
Further detail regarding network location services can be found at the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns788/solution_overview_c02-474514.html.

When combined with other applications constructed to take advantage of the Cisco Context-Aware Services API, Context-Aware Services can serve as an enabler for entirely new application functionality. For example, from their wired or wireless device, a teacher can consult a context-aware enabled application that makes use of such information to determine the location of other faculty team members (such as a nurse or resource school safety resource officer) and initiate contact with the nearest available team member qualified to assist them. Context-aware services enhance the experience of users while at the same time improving their overall efficiency and productivity.

Cisco Context-Aware Components

The components of the Cisco Context-Aware Services are shown in Figure 2.

Figure 2 Cisco Context-Aware Services Components



Wired and Wireless Client Devices

- Wired or wireless (Wi-Fi) devices—Mobile wireless devices (asset tags, WiFi equipped computers, mobile stations, etc.) that interact with the network and whose location and other contextual parameters can be monitored by Context-Aware Services. Wired devices are generally equipped with an Ethernet interface which is attached to a Cisco Ethernet switch (such as the 2960G, 3560E, 3750E, 3750G, 4500, and 4900 series) that supports context-aware services. In addition, some devices may possess both wired and wireless interfaces. Without context-aware services deployed, if a wired IP speakerphone is originally deployed in a school library, and a librarian moves this phone to classroom 206 across the hall, any location information with regard to this conference phone's whereabouts would need to be manually updated across all concerned systems. With Context-Aware Services and a context-aware Ethernet switch, the location of the phone can be dynamically updated to reflect its new location within seconds after it has been plugged into the wired network jack in classroom 206. Via the Mobility Services Engine's API, this information can be provided to various context-aware applications, including the Cisco Wireless Control System (WCS).
- Cisco Compatible Extensions RFID Tags—These RFID tags can be physically attached to assets (regardless of whether the asset itself contains a wired or wireless network interface adapter) and can pass contextual information on behalf of the asset to Cisco Context-Aware Services. Compliance with the Cisco Compatible Extensions program helps ensure that RFID tags comply with predefined information formats such that the contextual information they capture can be made readily available to other Context-Aware Services components, including safety and security applications from Cisco partners. Sensor capabilities can be externally mounted or directly embedded into tags in order to link the data captured (for instance, motion, or temperature data) with the location of the mobile asset. Externally mounted sensors can also be placed in fixed locations, like a refrigerator or a storage room.

  For more information about the Cisco Compatible Extensions for RFID Tags program, refer to the following URL:
  http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html.
- Chokepoint triggers—Chokepoint triggers (sometimes referred to as Exciters) are an optional component that can greatly enhance asset tag functionality, providing for finer tag location granularity and improved accuracy by localizing tagged assets within multi-floor structures, in presence detection scenarios, or when passing through chokepoint areas, such as entrances and exits. RFID asset tags that enter the proximity of a chokepoint trigger can change their normal behavior based on a set of pre-programmed instructions. RFID tags that have been stimulated by chokepoint triggers in this fashion send notifications and contextual information via the wireless infrastructure to the Cisco Mobility Services Engine.

Cisco Unified Network

This multipurpose network contains the wired and wireless infrastructure required to address converged data, voice, and video requirements, as well as providing the foundation for use of context-aware services.

- Context-Aware Ethernet switches—These are Ethernet switches (such as the 2960G, 3560E, 3750E, 3750G, and 4500 series) that support the specification of civic and emergency location identification number (ELIN) location information and the transmission of this information to Cisco Context-Aware Services. This functionality allows for contextual information associated with wired devices to be tracked using Context-Aware software on the Mobility Services Engine. Switches transmit relevant contextual information to the MSE for all of the devices attached to them. This information may include the physical mailing or street address location associated with the attached device (the civic address) as well as other information such as the IP address, MAC address, port, VLAN, and user name. Typically, this information is obtained using switch features such as IEEE 802.1x, Dynamic Host Configuration Protocol (DHCP) snooping, Dynamic Address Resolution Protocol (ARP) Inspection (DAI), and IP Source Guard. Additionally, if the end device runs the Cisco Discovery Protocol or Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED), additional information, such as the version number and serial number, can also be sent to the MSE.

Note At this time, serial numbers of attached devices are reported to the MSE Context-Aware Service if the device supports LLDP-MED.

- WLAN controllers—WLAN controllers (and the embedded software residing within them) provide for the aggregation and transfer of device tracking and statistics information for RFID tags, mobile wireless clients, and any rogue devices detected.

- Access points—In addition to their fundamental role in providing access for wireless clients, Cisco Aironet access points provide measurements of received signal strength from both wireless client devices and RFID tags and subsequently forward this information to the Mobility Services Engine via their registered WLAN controller.
- Received Signal Strength Indication (RSSI)—This is a mechanism used to determine device location by carefully considering the measured strength of a radio signal at several points in an indoor environment. Used by the Cisco Mobility Services Engine for WLAN clients, RFID tags, and rogue devices, this algorithm is based on the signal sent from the mobile asset to different access points deployed within the school. RSSI is usually preferred for indoor or low ceiling environments, both of which can result in high degrees of signal reflection.
- Wi-Fi Time Difference of Arrival (TDoA) Receiver—Wi-Fi TDoA receivers are optional components used in very large, open environments to locate assets equipped with RFID tags with greater accuracy and precision than is possible using other techniques.

Note Although useful in extending Context-Aware Services for RFID tagged assets in outdoor venues, the use of TDoA receivers were not included in the Schools SRA design.

For a more detailed explanation of both RSSI and other wireless location algorithms, refer to the *Wi-Fi Location-Based Services Design Guide 4.1* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/wifich2.html#wp1049520.

Management and Applications

- Cisco Mobility Services Engine (MSE) with Context Aware Services Software—The Cisco Mobility Services platform can host multiple independent services possessing high-level capabilities that can enhance both wireless and wired network infrastructures. One of these is Cisco Context-Aware Services which can capture, store, and analyze contextual information from multiple wired and wireless networks simultaneously. When Context-Aware Services is deployed in accordance with generally accepted best practices, both wired and wireless network infrastructure devices (controllers and switches) may send raw location measurement data, device attachment, and other contextual information to the MSE regarding the presence of any wired clients, wireless clients, RFID tags, or rogue devices. Both wired and wireless network infrastructures communicate with the MSE using the Cisco Network Management Services Protocol (NMSP), which is a Cisco-defined protocol used for secure communication between the MSE and other context-aware network infrastructure components. The MSE sits out of the data path of the wireless LAN and receives data from WLAN controllers and context-aware switches via the use of NMSP.

  The location of WLAN clients and RFID tags on the Cisco Mobility Service Engine is calculated by one of two software service modules:

  - Cisco Context-Aware Engine for Clients, which handles all context-aware operations involving RSSI location of Wi-Fi clients, rogue clients, and rogue access points. This engine also handles context-aware operations for wired clients.
  - Cisco Context-Aware Engine for Tags, which handles all context-aware operations involving TDoA and RSSI location of Cisco Compatible Extensions compliant RFID tags.

  Context-Aware Services software, when operating alone on the Cisco MSE, is capable of servicing up to a maximum of 18,000 simultaneously tracked devices per single MSE-3350 appliance and 2,000 simultaneously tracked devices per single MSE-3310 appliance.

  Refer to the following data sheet for more information regarding the Cisco 3300 Series Mobility Services Engines http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c78-475378.html

- Wireless Control System (WCS)—The Cisco Wireless Control System is a management platform that also contains a context-aware client application that interacts with the Mobility Services Engine. The primary role of the context-aware client application is to provide access to the contextual information contained on the MSE using the MSE's application programming interface (API). The application can then either present this information to the user directly (such as is seen in a graphical location map or a table of location values) or enable other processes to accomplish relevant tasks using this information that would otherwise be difficult to achieve. The Cisco WCS can also serve in a special secondary role as a control client that possesses the ability to configure MSE operational parameters.

  For more detailed information on the Cisco Wireless Control System management server and its capabilities, including its ability to serve as a context-aware application client, refer to the documentation at the following URL:

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html.

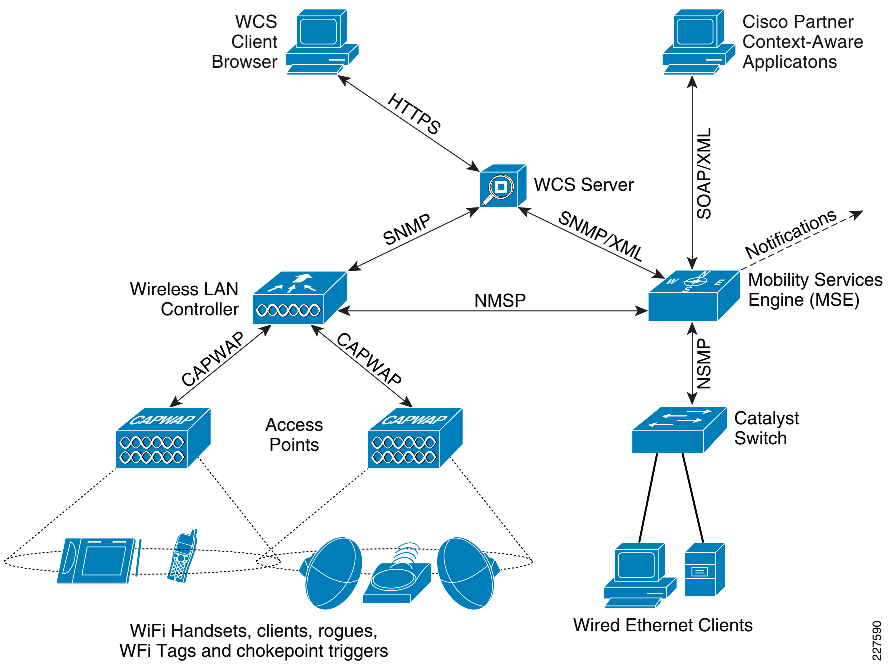
- Other Context-Aware Applications—Other context-aware client applications from third party Cisco Technology Development Partners may also access the MSE via its open API, which is based on Simple Object Access Protocol (SOAP) and XML protocol. Access to this API is available to any Cisco technology partner. Context-aware applications developed by Cisco Partners often deliver specifically targeted application functionality that is often not available from other sources.

  For more information on the Cisco Context-Aware Services API, refer to the following URL: http://developer.cisco.com/web/contextaware/home.

Context-Aware Component Interaction

Figure 3 provides a more detailed illustration of the protocol interaction between the various Context-Aware Service components.

Figure 3 Protocol Interaction Between Context-Aware Components



For wireless clients, tags, and rogues, Cisco Aironet access points use the Control and Provisioning of Wireless Access Points (CAPWAP) protocol to forward the RSSI of detected clients, tags, and rogues to the WLAN controller to which they are currently registered. The wireless LAN controller aggregates this information on a per device basis from all registered access points detecting the wireless device's signal. This information is then forwarded to the MSE using the NMSP protocol via an authenticated and encrypted session. The appropriate Context Aware software engine on the MSE then uses the RSSI data received from one or more WLAN controllers to determine the location of the wireless device

Note A rogue access point is any access point that is determined not to be a member of the same mobility group as the WLAN controller to which the detecting access points belong. A rogue client is any client that is currently associated to a rogue access point.

For wireless clients, rogue access points, and rogue clients, the Context-Aware Engine for Clients is used to process the received RSSI information. For operations involving RFID tags, however, the Context-Aware Engine for Tags is used instead. Using Context-Aware Services and the Mobility Services Engine, the Cisco Unified Network can readily detect 802.11 Wi-Fi active RFID tags that are compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification (such as those from AeroScout, WhereNet, G2 Microsystems, and others). Through the MSE and WCS, the location of these RFID tags can then be displayed on WCS floor maps using a yellow tag icon.

Note RFID tags that are not compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification are not tracked by Cisco Context-Aware Services Release 6.0.

Cisco Compatible Extensions compliant active RFID tags are detected on a Wi-Fi network based on periodic frames[1] that are sent by the tag using a Layer-2 multicast. The delay between these periodic frames can be programmed based on the specific application use case. In most cases, tags are configured to transmit periodic frames every three to five minutes in order to strike an equitable balance between location accuracy and good tag battery life.

RFID tags can also pass tag telemetry information upstream to the MSE as part of the tag message payload. This contextual information (battery status, motion, temperature, pressure, humidity, etc.) is received by access points and collected by WLAN controllers in a similar fashion as that described earlier in this section. WLAN controllers will aggregate telemetry traffic from multiple tags and eliminate any duplicate tag telemetry values that might be received. After the telemetry has been distilled and cleansed of any duplicate information, the WLAN controller passes it to the MSE. The MSE updates its internal databases with this information and in turn makes this information available to application programs.

Properly equipped RFID tags can also indicate the occurrence of a priority event, such as one that might result from the triggering of a tag tamper sensor or the depression of a tag call button. RFID tags indicate that these types of events have occurred via additional information embedded in the tag messages that are sent to the WLAN controller. This information is in turn passed northbound from the WLAN controller to the MSE and the MSE can make this information available to application programs.

RFID tags from various vendors include a secondary on-board magnetic signaling receiver, typically set up to respond to the magnetic field component of a 125 kHz RF carrier. This secondary receiver provides for additional tag functionality when tags enter into areas that are within close proximity to a magnetic signaling transmitter or chokepoint trigger. Chokepoint triggers are proximity communication devices that trigger asset tags to alter their configuration or behavior when the tag enters the chokepoint trigger's area of operation or stimulation zone. This alteration could be as simple as causing the asset tag to transmit its unique MAC address identifier. It could be significantly more complex, including causing the tag to change its internal configuration and status. One of the prime functions of a chokepoint trigger is to stimulate the asset tag such that it provides indication to the system that tag has entered (or exited) the confines of a constricted physical area known as a chokepoint. Typical chokepoints include entrances, exits or other types of physical constrictions that provide passage between connected regions of a facility (such as a corridor or hallway).

Note While chokepoint triggers are electronic devices that are typically deployed within physical chokepoints, it is not unusual to hear the term "chokepoint" used rather loosely to refer to both the physically constricted area and the associated electronic device.

Chokepoint triggers (including a very popular model manufactured by AeroScout Ltd. known as an Exciter) may be connected to the wired infrastructure and are configured using each vendor's configuration software. Once they have been configured, they can

1. These periodic frames are also sometimes referred to as "beacons". They should not be confused with the 802.11 beacons that are sent by access points.

either remain connected to the infrastructure full-time for management purposes or can be disconnected and operate in a standalone mode, requiring a source of electrical power but no actual connectivity to the network.

The chokepoint trigger address information contained in the tag packet provides the MSE with enough information to temporarily override any RSSI or TDoA localization currently in place for the tag and set the current location of the RFID tag to the location of the chokepoint trigger. The size of a chokepoint trigger's stimulation zone, or range, can extend from a radius one foot or less to over twenty feet, dependent upon the vendor and the capabilities of the particular model.

Catalyst switches supporting context-aware services also make use of NMSP to interact with the MSE similar to the manner described earlier for WLAN controllers. A major difference between how WLAN controllers and Catalyst switches interact with context-aware services lies with the method used to determine the location of switch attached wired devices. As explained earlier, localization of wireless devices is performed by the MSE using a signal or time based technique, whereas the location of wired devices is based on information sent to the MSE that originates in the switch configuration. The information recorded by the MSE for the wired device includes the device MAC address, switch MAC address, slot or port, IP address, and user name (if available). This information is sent whenever a device link changes state. Context-aware Cisco Catalyst switches provide the MSE with the latest relevant civic location and emergency location identification number (ELIN) information for all attached IP endpoints. These endpoints may include IP phones, PCs, access points and other devices.

In Release 6.0, all civic and ELIN location information is configured locally at the switch, and shortly after location changes are made using the CLI, they are propagated to the MSE. NMSP is used between the switches and the MSE to maintain synchronization, and alert the switch as to the connection or disconnection of devices.

Additional information regarding civic address location is available from the IETF in the following RFCs:

- DHCP Option for Civic Addresses Configuration Information http://www.rfc-editor.org/rfc/rfc4776.txt
- Revised Civic Location Format for Presence Information Data Format Location Object http://www.rfc-editor.org/rfc/rfc5139.txt

Note Proper validation of certificates between context-aware service components requires the participants to possess sane clocks (clocks whose configured time does not differ from one another by large amounts). In order to facilitate this, it is highly recommended that the clocks in the MSE, WCS, WLAN Controllers, and any context-aware Ethernet switches be synchronized to a common time base using the Network Time Protocol (NTP). The lack of clock sanity amongst context-aware components in the network can cause NMSP sessions to fail if the configured date and time fall outside of the certificate validity period, thereby causing certificate validation to fail.

Network Mobility Services Protocol (NMSP)

The Network Management Service Protocol (NMSP) was designed to define intercommunication between Mobility Service Engines and network access controllers over a switched or routed IP network. An access controller can provide network access for either wired or wireless endpoints. Within the scope of the Schools SRA design, access controllers are represented by WLAN controllers and context-aware Cisco Catalyst Ethernet switches.

NMSP is a two-way protocol that can be run over a connection-oriented or a connectionless transport. WLAN controllers and context-aware switches can use NMSP to communicate with one or more MSEs. NMSP is based upon a bidirectional system of requests and responses between the MSE and the access controllers.

MSP also provides for a keepalive feature that allows either partner in a NMSP session to determine if the adjacent partner is still active and responsive. Should an MSE fail, a WLAN controller or a context-aware Ethernet switch will try to contact another MSE with which to communicate. If the WLAN controller or context-aware Ethernet switch fails, all context-aware services being provided to that WLAN controller or context-aware Ethernet switch are disabled until that WLAN controller or context-aware Ethernet switch once again becomes active and re-establishes its NMSP session.

Note It is important to understand that the failure of an NMSP session has no direct impact on the ability of a WLAN controller or context-aware capable Ethernet switch to pass normal client session traffic to applications on the network. In other words, a failed NMSP session to a WLAN controller may affect the ability of the MSE to provide updated contextual information on that controller and its resources. But it does not affect the ability of the WLAN clients using that WLAN controller to logon to applications residing on the network. This also applies to wired clients and context-aware Ethernet switches.

NMSP uses Transport Layer Security (TLS) and TCP port 16113 on the WLAN controller or context-aware Ethernet switch. The MSE will initiate the connection to the WLAN controller or context-aware Ethernet switch, although once a secure session has been established between MSE and its session partner, messages may be initiated in either direction. The TCP port (16113) that the controller and mobility services engine communicate over must be open on any firewall that exists between the controller and mobility services engine.

The MSE and the WLAN controller or context-aware Ethernet switch use Echo Request and Echo Response control messages to maintain an active channel of communication so that the data messages can be sent. The Echo Request message is a keepalive mechanism that allows either NMSP session partner to determine if the other partner remains active and responsive. Echo Requests are sent periodically (upon expiration of a heartbeat timer) by the MSE or its session partner to determine the state of the NMSP session. When the Echo Request is sent, a NeighborDeadInterval timer is started. The NeighborDeadInterval timer specifies the minimum time a session partner must wait without having received Echo Responses to its Echo Requests, before the other session partner can be considered non-responsive and the NMSP session is placed in an idle state.

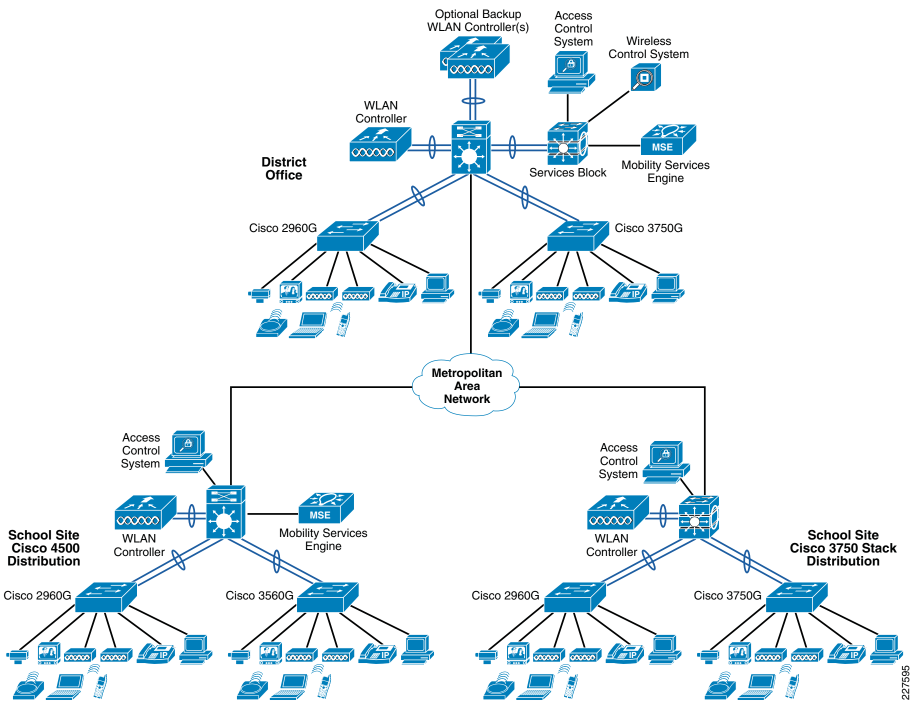
Context-Aware Services in the Schools Service Ready Architecture

Figure 4 provides a high level illustration of the integration of Cisco Context-Aware Services into the Schools Service Ready Architecture. The key points of this integration into a Metropolitan Area Network deployment are:

- The presence of a **centralized management entity** (the wireless control system (WCS) at the district office. In the case of Context-Aware Services, WCS also serves as a context-aware application client. District and school context-aware users can log into WCS and query the contextual characteristics (such as location) associated with wireless and wired client devices, rogues and asset tags. In some cases, third-party context-aware application servers may also contain context-aware applications that are located in the district office.

- The presence of a local Mobility Services Engine at larger schools used to provide Context-Aware Services to individual larger schools, where the anticipated number of total tracked devices is significantly higher (e.g., greater than 500 and most likely 1000 or more). A locally deployed MSE may also be justified if context-aware services are being utilized for school applications and tasks that are considered mission-critical to the function of the school or the safety and security of students or faculty.
- The option of a centralized Mobility Services Engine with Context Aware software at the district site used to provide the Context-Aware Services to smaller schools where the anticipated number of total tracked devices per school is relatively low (e.g., less than 500).

Figure 4 High-Level View of the Schools SRA With Hybrid Context-Aware Services Model



Except for very large or very small school districts, it is our understanding that the majority of School districts addressed by the Schools SRA design will contain a mix of large schools (such as high schools) and smaller schools (such as elementary and intermediate schools). We anticipate that many of the smaller schools in these districts may be well served by the 3750 switch stack used at the distribution layer, whereas larger school designs may be outfitted instead with the 4500 distribution switch. In situations such as this, the context-aware deployment model shown in Figure 4 can be used to provide context-aware services to both types of schools in a cost-effective manner.

Historically, context-aware services and the Cisco Mobility Services Engine (as well as its predecessor, the Cisco Wireless Location Appliance) have been deployed within modern switched LAN environments. In such deployments, FastEthernet speeds and capacity (at minimum) are assumed to be present throughout the network. However, many deployments make use of wide-area technologies in conjunction with LANs to connect geographically dispersed locations. When lower-speed WAN technologies (such as T1 and so on) are used to connect remote locations, due to the limited amount of WAN capacity available, it is typically not recommended to deploy the MSE across the WAN from where WLAN controllers are deployed. In such deployments, Cisco Systems has always recommended that the MSE be deployed locally on the LAN with WLAN controllers and any other components establishing NMSP sessions to the MSE. In such cases, designers may also wish to break up large WCS network designs into smaller designs to avoid time outs that can occur between WCS and the MSE during synchronization of very large network designs when using low-speed links[1].

A key difference (and major advantage) of the Schools SRA design is that the use of a modern high-speed metropolitan area network (MAN) instead of a traditional WAN offers far more bandwidth to each remote site. In this case, with modern LAN-like speeds available across the metropolitan area network, the concept of deploying an MSE remotely from the other context-aware components becomes much more feasible. Note however, this assumes sufficient bandwidth and infrastructure is in place to assure that FastEthernet-like speeds are available to each school and that proper network protocol identification, classification and QoS are all applied properly to manage congestion in the network.

Why might this be of consideration in the Schools SRA design? While the cost of a local MSE deployment can be often be easily justified in very large remote sites with large populations of devices and assets to track, this might not always be true in the case of smaller sites. Looking at the case of school districts that might contain a mix of larger and smaller schools, one can visualize situations where in spite of the fact that context-aware services can provide much desired functionality to schools of all sizes, the number of devices per smaller school makes it difficult to cost-justify deploying an MSE at each school. However, when taken in aggregate, the number of devices and assets to be tracked amongst a large group of small schools within the district can easily justify the deployment of a centralized, shared MSE. It is in cases such as this that the high-speed nature of the metropolitan area network can make the concept of a centralized MSE much more feasible.

In the context-aware services model shown in Figure 4, we take advantage of high-speed connectivity across the MAN to the remote schools and allow for a centralized MSE to provide context-aware services for smaller schools across the district. We assume here that on their own, a single small school might only have a maximum of 250 to 500 simultaneously tracked devices. An exception to the case made for using a centralized MSE for smaller schools might be for any schools where context-aware services are used for applications that are mission-critical to the safety and security of the school, its students, and the faculty and administration. An example of such an application might be a safety and security application used to ascertain the location of all faculty or students during a school lock-down security event using identification cards that are equipped with RFID technology. This type of application obviously must be available at all times, including any potential network outages, hence the use of a centralized MSE in this case

1. Or use a locally deployed WCS at each remote site that could optionally be managed by WCS-Navigator at a central site.

is not an option. Any other supporting applications that are required for such mission-critical deployments of context-aware services should also be deployed locally in this case as well.

Note Based on our analysis of MAN capacity, traffic flows, classification and QoS, we believe the centralized deployment of an MSE across a modern high speed metropolitan network is a viable concept. Although a great deal of intensive functional testing was performed during the preparation of this document, time constraints did not allow us to complete actual validation of centralized MSE deployments across metropolitan area networks.

Larger schools using a 4500 series Catalyst Ethernet switch for distribution are assumed to possess at least 500 or, more likely, 1000 or more simultaneously tracked wired or wireless devices. While it may be possible to service these larger schools using a centralized MSE, the larger number of clients and the increased amount of traffic placed onto the MAN between controllers, switches, and the MSE in this case can pose more of a challenge, especially when there are large device populations that move frequently and generate location updates on a regular basis. Careful analysis of data traffic and the judicious application of QoS in the network becomes especially important.

At the current time and based on our current level of validation, the most reliable solution in the case of larger schools with large tracked device populations is to deploy an MSE locally at the school. This MSE can in turn be managed via a remote WCS at the district office. Once again, in cases where context-aware services are regarded as mission critical for the school, other context-aware components (such as third-party context aware application servers or in some cases the WCS as well) should also be deployed locally in order to ensure that the context-aware solution is functional even in the rare case of a prolonged MAN failure.

In school districts where there are many schools with either large tracked device populations or mission-critical context-aware applications, it is important to keep in mind that at this time Cisco officially supports the management of up to five (5) MSE platforms from a single WCS system. While this is not a "hard" limitation on the number of MSE platforms that can be assigned to a single WCS system, it is the limit to which testing has been performed. Therefore, in designs where there may be greater than five large schools equipped with locally deployed MSE platforms, you may wish to consider using additional WCS systems as necessary. In this case, the use of WCS-Navigator (not shown in Figure 4) should be considered at the district office to provide a single interface portal to as many as twenty (20) WCS management systems and their associated Mobility Services Engines. WCS-Navigator is a management aggregation platform that delivers enhanced scalability, manageability, and visibility of large-scale implementations of Cisco WCS and the Cisco Unified Network. WCS-Navigator provides straightforward access to information from multiple Cisco WCS management platforms. A single WCS-Navigator management aggregator can support up to twenty (20) WCS management systems and 30,000 access points.

Note Due to time constraints, scalability testing of WCS-Navigator in the Schools SRA design beyond four WCS systems was not able to be completed. Further information on WCS-Navigator can be found at http://www.cisco.com/en/US/products/ps7305/index.html.

Component Capacities

Mobility Services Engine

Each Cisco Mobility Services Engine has a maximum device tracking capacity, defined as the maximum number of active wired and wireless (clients, rogues, and RFID tags) that can be tracked by a single Mobility Services Engine. This is a "hard" limit that is dictated by the licensing purchased for the Context-Aware software as well as the presence of any other applications on the MSE. Once a Mobility Services Engine has reached its maximum tracking capacity, any new devices that the MSE becomes aware of beyond that limit are simply not tracked. It is important to note that while this section discusses the maximum device tracking limits for the MSE, MSE licenses can be purchased supporting a lower maximum number of tracked devices than those shown here. Refer to the *MSE Licensing and Ordering Guide* (http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html) for more information regarding the various combination of client and RFID tag tracking capacities available for the MSE.

For Release 6.0, the maximum device tracking limits when using only the Context-Aware Services software on the MSE are shown in Table 1.

Table 1 MSE Maximum Tracked Device Capacities (Context-Aware Software Only)

Mobility Service Engine	Maximum Tracked Device Capacity
MSE-3350	18,000
MSE-3310	2,000

If you intend to use the MSE-3350 to deliver other services in addition to Context-Aware, the maximum capacity shown above in Table 2 will likely be reduced. See the *MSE Licensing and Ordering Guide* (http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html) for information on Context-Aware maximum tracked device limits with other co-resident MSE services.

When working within these maximum capacities, it is important to note that further category-specific limits can be instituted at the designer's discretion via the MSE configuration. This allows, for example, a maximum capacity of 2,000 tracked devices on a MSE-3310 to be further limited as 1,000 wired and wireless clients, 500 RFID tags, and 500 rogue access points and clients. Partitioning the maximum tracking capacity of the context-aware software in this manner prevents any single device category from consuming more than its authorized share of the maximum tracking capacity of the system.

In the high-level diagram shown in Figure 4, the MSE-3310 might be a good design choice for a locally deployed MSE at our 4500-based school site. Its maximum tracked device capacity of 2000 devices should scale well to a larger school site with an estimated 1000-1250 total tracked devices. This would leave ample MSE capacity in reserve for future growth in tracked devices at this location. Of course, you could deploy with less capacity in reserve should you choose to, and elect to address future tracked device growth at a later date via a hardware addition or upgrade. 4500-based schools that possess or anticipate near-term tracked device needs beyond 2000 devices should consider the MSE-3350 instead.

Except for very small school districts, the MSE-3350 would typically be the best overall choice when considering a centralized deployment using a high-speed metropolitan area network. In this way, it can provide context-aware services for several smaller school sites, each of which might possess an estimated 500 or fewer tracked devices. In very small school districts (e.g., a district containing up to four small schools for example) a centralized MSE-3310 may prove to be even more cost-effective.

WLAN Controllers

WLAN controllers also possess limitations on the maximum number of devices for which the controller will track and aggregate contextual information. In Release 6.0, these limits are shown in Table 2.

Table 2 WLAN Controller Maximum Tracked Device Capacities

WLAN Controller	Clients	Tags	Rogue Access Points	Rogue Clients
4404	5000	2500	625	500
4402	2500	1250	625	500
2106	500	256	125	100

Note that these are indeed “hard” limits. In other words, once these limits have been achieved on a WLAN controller, contextual tracking information for any new clients, RFID tags, rogue access points, or rogue clients beyond these limits will be dropped until such time that older entries are pruned from the controller's internal database. The client and tag limits are quite high and should not prove to be easily exceeded for a single school. Unless students are allowed to operate their own unauthorized rogue WiFi equipment during school hours (which is typically not the case as per our understanding), the limitation on the number of rogue devices tracked by a single controller should not be routinely exceeded in a single school.

The Context-Aware System Performance chapter of the *Mobility Services Engine Context Aware Deployment Guide* (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#casysperf) also points out that a single MSE can support up to 500 total NMSP connections. Keep in mind this includes not only the NMSP sessions to WLAN controllers, but NMSP sessions to any context-aware Ethernet switches conducted from that MSE.

1. Although a single MSE can technically support up to 500 NMSP sessions, scalability testing constraints have only allowed for testing of 100 simulated NMSP connections to a single MSE at this time.

Wireless Control System (WCS)

With regard to the MSE, WCS interacts as a context-aware client and does not track devices itself when used in conjunction with the MSE. Thus, there are no direct constraints on the maximum number of tracked devices imposed by WCS itself.

In addition to established WCS sizing and capacity guidelines for the number of supported controllers and access points (listed in the *System Requirements section of the Wireless Control System Configuration Guide*, Release 6.0, http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0wst.html#wp1061082), there are a few indirect constraints relating to Context-Aware services that you should be aware of:

- To maintain clarity and the speed of its graphical user interface, WCS only displays the first 250 wireless clients, RFID tags, rogue clients, or access points on a single floor map. To view graphical location displays for any of these device categories beyond this limit, filtering (based on MAC address, asset name, asset group, asset category, or controller) should be used to limit the number of devices displayed at once (see the Floor Settings section of the *Wireless Control System Configuration Guide*, Release 6.0, http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0maps.html#wp1210969).
- Currently, a single WCS can manage Context-Aware Services on up to five (5) Mobility Service Engines. While defining more than five MSEs to a single WCS is possible, Cisco Systems has not validated this level of operation.
- Currently, Context-Aware Services on the Mobility Services Engine can be managed by only one Wireless Control System.
- In Release 6.0, WCS supports the creation of up to 124 WCS virtual domains.

Context-Aware Engine for Tags (AeroScout)

The Context-Aware Engine for Tags used in version 6.0.85.0 of the MSE Context-Aware Services software supports network designs containing up to 255 floor maps. A network design typically consists of campus, buildings, and floor maps. Thus, in the Schools SRA, a network design might be used to describe a school district. This limitation could be interpreted as saying that a school district should not contain more than 255 floor maps. If more than 255 floor maps are required, it is necessary to break the school district up into two or more network designs.

Obviously, the degree of restriction here will vary with the number of floors in each school in your district, multiplied by the number of schools. For example, if all schools in a district contain only a single floor, then up to 255 schools could be defined in a single network design before the conditions of this restriction are encountered. If schools each contained three floors however, then only 85 schools could be defined before being subject to this limitation.

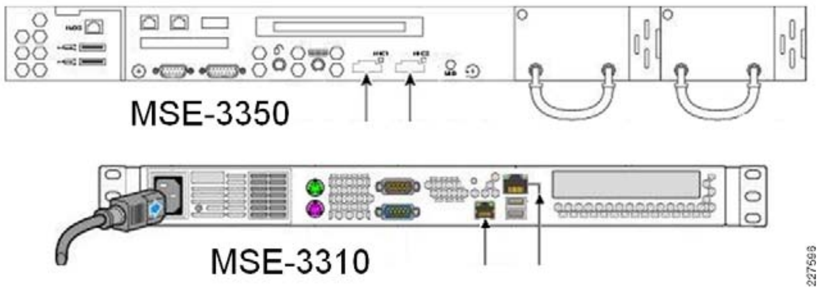
Integration with the Schools Service-Ready Architecture

MSE Connection to the Network

Figure 5 is an illustration of the rear panel of both the MSE-3350 and the MSE-3310. The Cisco Mobility Services Engine is equipped with two 10/100/1000BASE-T Gigabit Ethernet ports (shown in Figure 5 by the solid arrows) that can be used to directly connect the MSE to two different IP networks (dual-homed). This makes it a simple affair, for example, to configure a MSE for service on network A while affording it the capability to be managed out-of-band on network B if the need arises.

In the Schools SRA design, we attach the MSE to the network via a single connection to the NIC0 interface.

Figure 5 Rear Panel Illustration of MSE-3350



Note The dual on-board Ethernet controllers on the MSE are not intended for redundant or simultaneous connections to the same IP network. Any attempt to manually configure the MSE in order to try and establish parallel, load balancing, or redundant Ethernet connections to the same IP network is not recommended or supported at this time.

Clock Synchronization

The Mobility Services Engine, WCS, WLAN controllers, and any switches that support context-aware services use Coordinated Universal Time (UTC)[1] in their interaction. Because proper certificate authentication relies on time base consistency between participating components, it is important to ensure that these components are synchronized to a common time base throughout the Schools SRA design. In addition, having components synchronized to a common time source makes troubleshooting much easier, especially when having to look at events occurring within the logs of different network components. And the output of coordinated information by a central source, such as WCS, makes much more sense when the time stamps of all information displayed follow a logical flow and make sense to the user.

Once time and date in each network component has been set initially, time synchronization should be maintained using the Network Time Protocol (NTP). In the Schools SRA design, these components should be synchronized to the local school or district ISR router.

NTP Configuration of the Mobility Services Engine

Configuration of the NTP server addresses used by the MSE is handled during installation and the execution of the MSE automatic configuration script. An excerpt of that script is shown below. Detailed information regarding the automatic configuration script can be found in the Automatic Installation Script section (http://www.cisco.com/en/US/docs/wireless/mse/3350/quick/guide/mse_qsgmain.html#wp1057105) of the Mobility Services Engine Getting Started Guide, http://www.cisco.com/en/US/docs/wireless/mse/3350/quick/guide/mse_qsgmain.html#wp1057105, and in Appendix A (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#appena) of the Mobility Services Engine Context Aware Deployment Guide, http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#appena.

```
If you choose to enable NTP, the system time will be configured from NTP
servers that you select. Otherwise, you will be prompted to enter the
current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default (S)kip: Y

Enter whether or not you would like to set up the Network Time Protocol
(NTP) for this
machine.

If you choose to enable NTP, the system time will be configured from NTP
servers that you
select. Otherwise, you will be prompted to enter the current date and
time.

Enable NTP (yes/no) no : yes
Enter NTP server name or address: <IP address or DNS name of NTP server>
Enter another NTP server IP address (or none) none: none
```

NTP Configuration of WLAN Controllers

Configuration of the internal clock and the specification of which NTP servers to use for periodic time synchronization can be performed on the WLAN controller using either the web GUI interface or the command line interface.

If you did not configure the system date and time through the configuration wizard when the controller was initially configured, or if you want to change your configuration, you can follow the instructions located in the section entitled Managing the System Date and Time (http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/c60intf.html) in the WLAN Controller Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/c60intf.html#wp1144340) in order to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server.

NTP Configuration of the Wireless Control System (WCS) Server

Configuration of the internal clock and the specification of which NTP servers to use for periodic time synchronization must be performed on the WCS server using the time and date capabilities of the WCS host operating system in use (either Windows or Linux).

RHEL-Based WCS Server

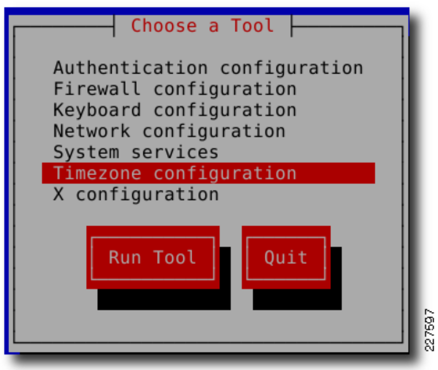
For a Redhat Linux-based WCS server, login to the host OS as root and use the following procedure to synchronize the internal software clock to the NTP server, synchronize the software clock to the server's hardware clock, and then maintain synchronization by starting the ntpd client daemon:

1. clock—Displays the current setting of the software clock.

1. For applications such those anticipated in the Schools SRA, Universal Coordinated Time may be considered as equivalent to Greenwich Mean Time (GMT).

2. /etc/init.d stop—Stops the ntpd client if it is already running.
3. ntpdate <*ntp server name or address*>—Synchronizes the system software clock with the NTP server.
4. setup—Brings up a setup utility that allows you to choose to set the time zone (shown in Figure 6).
5. hwclock-systohc—Writes the software clock settings to the hardware clock.
6. /etc/init.d/ntpd start—Starts the ntpd daemon to keep the clock synchronized going forward.[1]

Figure 6 RHEL Setup Utility



Note There are various other approaches that can be used to set the time zone on a Linux system. The reader is encouraged to consult the Redhat documentation for methods involving the use of the TZ variable or symbolic links to the localtime file or a particular time zone file in the system's time zone directory.

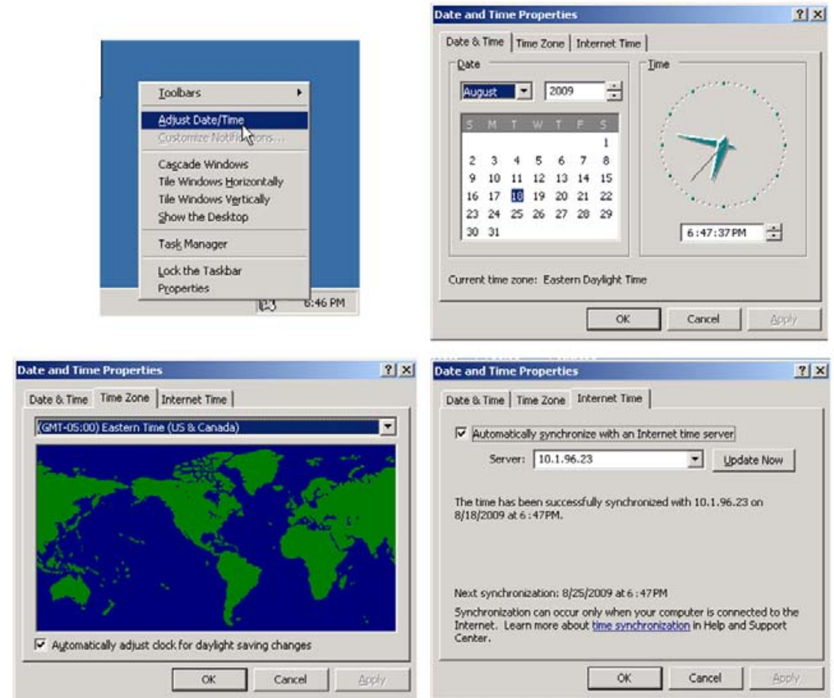
Windows 2003-Based WCS Server

For a WCS server based on the Microsoft Windows 2003 Server OS, use the following procedure to synchronize and maintain the correct system time via the Windows Time service (see Figure 7):

1. Check Settings>Control Panel >Administrative Tools>Services for the Windows Time service and ensure that it has been started.
2. Right click on the Task Bar clock and select Adjust Date/Time.
3. Under the Date & Time tab, set the current date and clock time to the approximate time of your NTP server.
4. Set the Time Zone and Daylight Savings time selections appropriately.
5. Select the Internet Time tab, check the box to Automatically Synchronize With An Internet Time Server, type in the DNS name or address of your NTP server, and then Apply.

1. If ntpd does not start as part of your system boot script, you might want to add it using the command chkconfig --add ntpd.

Figure 7 Setting Time and NTP Server on Windows 2003



NTP Configuration of Context-Aware Catalyst Ethernet Switches

In order to prevent any issues with authentication and NMSP session initiation, Catalyst Ethernet switches participating in context-aware services should be configured to utilize NTP in order to keep their clocks in synchronization with other context-aware components. NTP is configured similarly amongst the various switch models discussed in this document, and the most comprehensive information on how to configure a Catalyst switch as an NTP client can usually be found in the configuration guide for the particular switch model. For example, for the Catalyst 2960G NTP configuration is documented in Configuring NTP section of the Catalyst 2960 Switch Software Configuration Guide (http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/swadmin.html#wp1053923).

It is good general best practice to ensure time synchronization of all network components when possible. However, from the perspective of context-aware services in the Schools SRA, only those switches that are actually participating in an NMSP session with the MSE require clock synchronization.

Schools SRA Wireless Control System (WCS) Context-Aware Considerations

The Wireless Control System is used for several important configuration tasks relating to context-aware services in the Schools SRA:

- Creation of a School or School District Network Design, which may include campus, building, floor, and outdoor level maps.

- Definition of WCS User Groups, which are used to define what management actions school context-aware users are authorized to perform with regard to network resources.
- Definition of Virtual Domains, which can be used to restrict which network resources school and other users have the ability to manage via WCS.
- Configuration of Mobility Service Engine operating parameters. This represents the next level of MSE setup beyond that performed by the MSE automatic configuration script discussed in section NTP Configuration of the Mobility Services Engine.
- Definition of Context-Aware Conditional Notifications, which defines how applications and parties external to the School might receive notification of specific events pertaining to changes in contextual characteristics associated with clients, tags or rogue devices.

In this section, we discuss only those areas where, in our testing of the Schools SRA design, we made use of significant WCS features relevant to the integration of context-aware services in our design, or where important configuration changes were made that significantly differ from the defaults. This is not meant to serve as a comprehensive configuration guide to all aspects of the WCS and MSE. Readers should refer to the WCS and MSE configuration documents already cited throughout this document (including Context-Aware Services General Best Practice References) for additional information regarding configuration parameters and procedures that, while not discussed in detail here, must still be configured or performed properly.

Creation of a Network Design

Once access points have been installed and have registered with a controller, WCS can be configured to manage the controllers and a network design can be set up. A network design is a representation within WCS of the physical placement of access points and other context-aware components throughout a facility or group of facilities. A hierarchy consisting of a single campus, the buildings that compose that campus, the floors of each building, and any outdoor areas constitutes a single network design.

In the Schools SRA, the choice of whether to configure the school district or each individual school at the campus layer depends to a large part on the on whether the schools in the district each contain a single building, or multiple buildings. If each school is comprised of one building and one building only, then the campus layer of the network design can be the entire school district. On the campus map, each school would be represented by a single building with one or more floors per building. This might be seen where:

- Schools are of more recent vintage and may have been sized accordingly for larger student populations. School temporary or portable outbuildings are not seen in this type of scenario.
- Areas where student population is relatively low, and there is no need for any secondary outbuilding structures at schools to meet student population demands.

In other cases, schools might be composed of multiple buildings, such as:

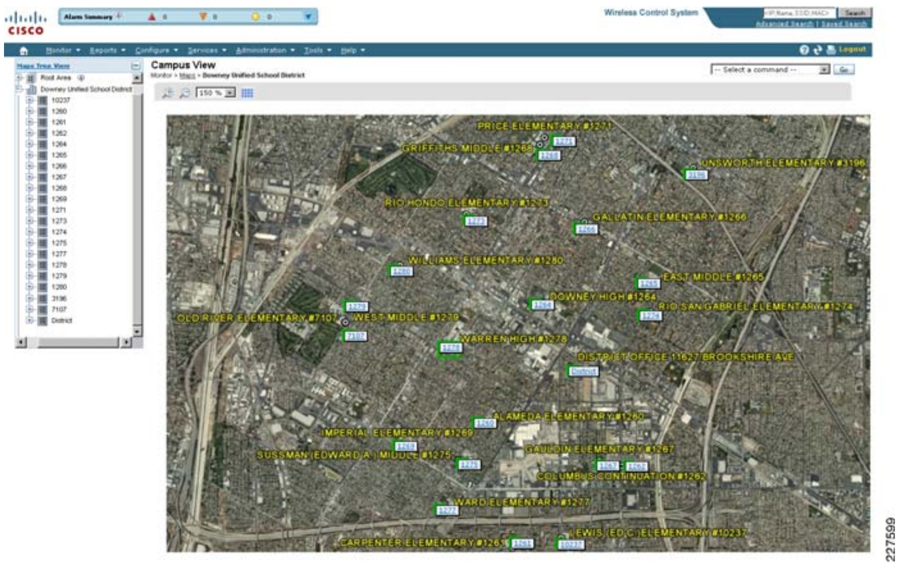
- An older school which has been expanded via the use of one or more secondary outbuildings. This might also be the case despite the age of the school if the surrounding communities have experienced explosive population growth.
- Larger schools that were architecturally designed to be small campuses, with multiple buildings, outdoor venues and the potential for large student populations. In some areas, this may be seen in high school settings.

In these scenarios, it makes more sense to define the school as a campus in and of itself.

A step-by-step set of configuration instructions regarding how to configure network designs consisting of campus, building, and floor maps can be found in Chapter 5 of the *Cisco Wireless Control System Configuration Guide*, Release 6.0, http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0maps.html #wp1203275.

Figure 8, Figure 9, and Figure 10 give an example of what a campus, building, and floor level network design might look like for a school district where all schools are assumed to be comprised of single buildings. In Figure 8, we use satellite imagery of the school district area as the backup for the campus map. Clicking on any of the icons takes us to the building map for the school. In this case, we select school number 1278, Warren High School, which then brings us to Figure 9.

Figure 8 Campus Level



The building map shown in Figure 9 indicates that this school is composed of a single floor. Clicking directly on the building map takes us to the floor definition shown in Figure 10. This is where we would actually see the location of wireless clients, active RFID tags and rogues displayed. Wired devices that are attached to context-aware Ethernet switches are not displayed on floor maps in Release 6.0 of Context-Aware Services.

Figure 9 Building Level for School #1278

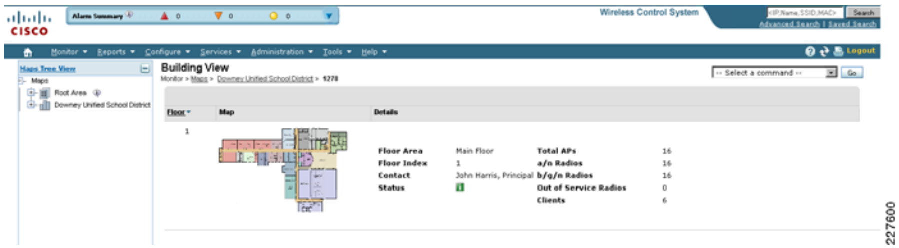
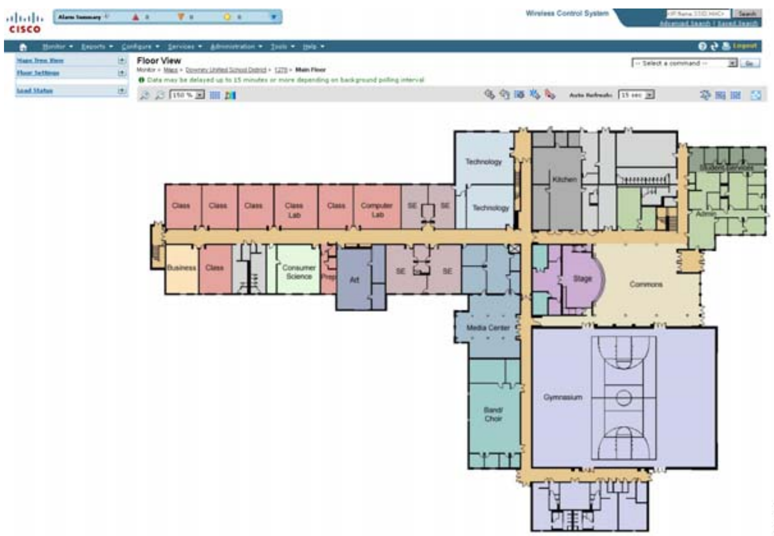


Figure 10 Floor Level for School #1278



Note Network designs are created in WCS, but they are not actually used for device tracking until they are transmitted to the MSE via a process known as network design synchronization. Only after network design synchronization has successfully occurred between WCS and its associated MSE will the network design actually be used by the Context-Aware Engine for Clients and the Context-Aware Engine for Tags. Synchronization of network designs and other components with the MSE is discussed in detail in the chapter entitled *"Synchronizing Mobility Services Engines" in the Context-Aware Service Configuration Guide* 6.0, http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch3_CAS.html.

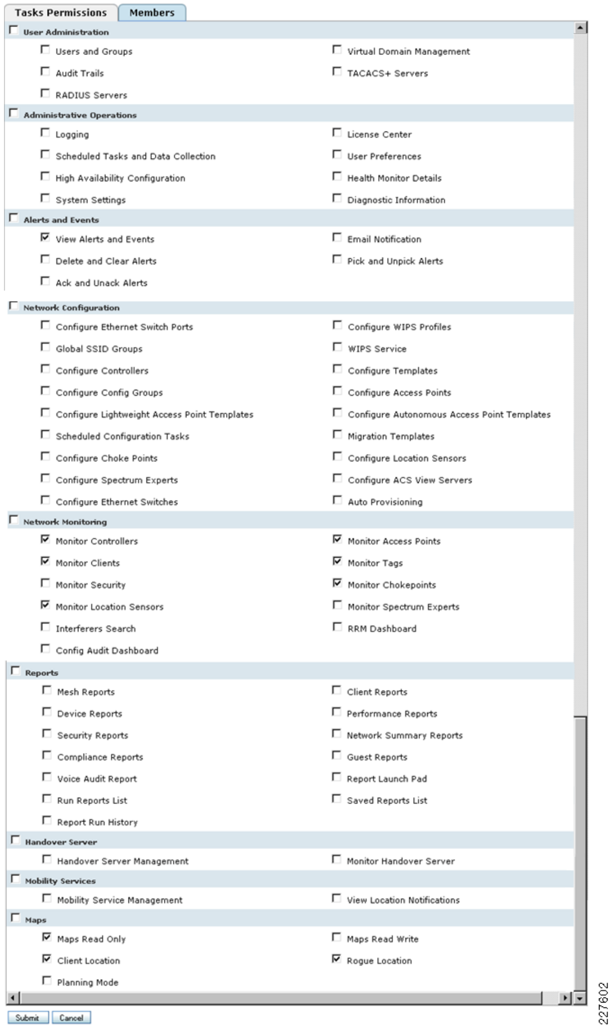
WCS Users, User Groups, and Virtual Domains

When installed, WCS provides for a single root user, which will have access to all WCS functions. The password for this root user should be protected and only known by those personnel at the district data center with a true need to know (e.g. those personnel responsible for the installation, maintenance, and detailed administration of WCS). Instead of using the root user password for routine access to WCS, you should create other users and grant them administrative access with privileges assigned as necessary via the use of WCS user groups. Chapter 7 of the *Cisco Wireless Control System Configuration Guide*, Release 6.0 (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0manag.html) provides comprehensive instructions with regard to the proper procedure for configuring users and group privileges on your WCS server. This chapter also contains a complete listing of the user groups available in WCS as well as the privileges contained in each group.

Common sense should be applied in the assignment of user privileges in the Schools SRA. For example, while only a very small set of key technical personnel should have access to the actual WCS root user ID and password, you may wish to assign the ability to make WCS configuration changes to a somewhat larger audience. This larger group can be assigned as WCS "admin" users or assigned to the "superuser" group. Most school users that are only interested in viewing the information available to them on WCS will not need more than the ability to simply monitor network activity in WCS. For these users, the privileges accorded them by the WCS System Monitoring or Monitor Lite user groups may be all that is required, depending upon the specific WCS monitoring functions you wish to grant those users.

In our validation of the Schools SRA, the custom user-defined group shown in Figure 11 was found to be very useful in limiting users to only monitoring context-aware information, as well as some basic WCS alerts and events. Note that the user is not allowed free rein to use any of the monitoring functions provided by WCS. For example, we may wish to allow a librarian in a school to access the context-aware functions listed under the WCS "Maps" function or search for a device by name. But this same school librarian probably has no need to monitor school network security compliance reports, thus we have not enabled access to those reports for this librarian's WCS account. Keep in mind that the requirements of school users in your environment may be different, so it may make sense for you to develop a custom WCS user group that closely fits your needs.

Figure 11 Custom User Group to Allow Context-Aware Monitoring



While WCS user groups define the WCS functionality users have been granted, WCS virtual domains allow the network administrator logically partition the WCS management domain and limit management access. In this way, the group of resources that the WCS functionality assigned to a user group may be exercised against is restricted. A WCS virtual domain consists of a set of assigned devices and maps, and restricts a user's scope to only information that is relevant to those devices and maps. Through a assigned virtual domain, users are only able to utilize WCS functionality against a pre-defined subset of the devices managed by WCS.

Users can be assigned one or more virtual domains, however only one assigned virtual domain may be active for a user at WCS login. The user can change the current virtual domain in use by selecting a different permitted virtual domain using the WCS Virtual Domain drop-down menu.

The WCS virtual domain can be used to limit the user's ability to even view certain resources inside WCS that are not contained in their active assigned virtual domain. For example, the Physics department chairman of a high school may have the ability to view the location and other context-aware characteristics of wireless assets due to his WCS user account being assigned to an appropriate user group permitting this level of WCS functionality. But the virtual domain that this department chairman director is assigned may only allow such functionality to be exercised against these assets if they are located within his assigned school. Thus, if the chairman of the physics department for school "A" attempted to use WCS to discover the quantity and location of RFID-tagged equipment in school "B", his assigned virtual domain would not allow access to school B's resources.

Administrative personnel with district-wide responsibilities, on the other hand, would be assigned a virtual domain that includes all resources in the district, including those in each school, and could exercise the functionality assigned to them by their user group against any of these resources. In this way, the virtual domain assignment can be useful in prevent unnecessary inter-school WCS traffic, especially traffic whose nature might be based more upon curiosity rather than actual need.

Note WCS user groups assign what actions a user can take against a resource, whereas WCS virtual domains determine what resources those user group actions can be applied towards.

There are two basic steps necessary to enable the use of virtual domains within WCS:

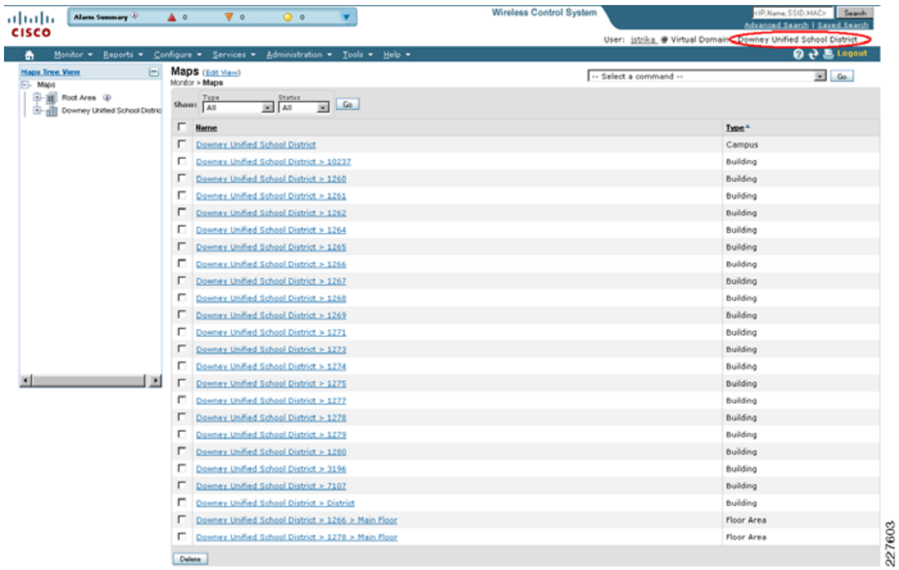
1. A virtual domain must be created, and the resources that we wish to include assigned to the virtual domain. The process for creating and assigning network resources to the virtual domain is detailed in Chapter 20 *Virtual Domains of the WCS Configuration Guide 6.0* (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0virtual.html#wp1040002).
2. The virtual domain must be assigned to the user. The process for assigning a virtual domain to a user is detailed in Chapter 7 Managing WCS User Accounts (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0manag.html#wp1097733).

Note It is important to note that in Release 6.0, non-root WCS virtual domain users cannot access WCS functions listed under the Services > Mobility Services main menu heading. This includes wired switch and device location. Refer to Understanding Virtual Domains as a User, WCS Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0virtual.html#wp1120787) for a complete list of WCS functions that are not available in non-root virtual domains.

In Release 6.0, since wired devices attached to context-aware Ethernet switches are displayed using Services > Mobility Services > Context Aware Service > Wired > Wired Clients, only users that are assigned to the root virtual domain are able to display context-aware information for these devices.

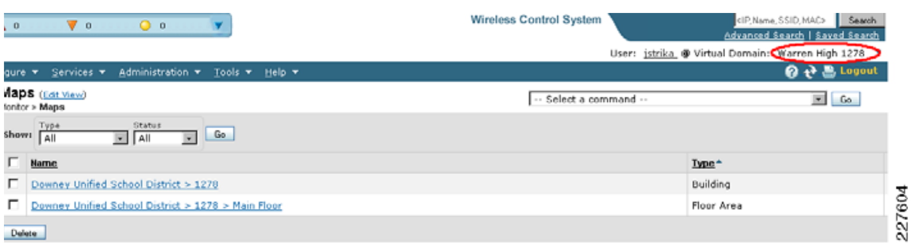
Figure 12, Figure 13, and Figure 14 demonstrate the effectiveness of WCS virtual domains (note that the current virtual domain in use by the logged-in WCS user is highlighted in each figure by the red oval). In Figure 12, we can see from the left hand margin that the root virtual domain user can see the entire set of schools comprising the Downey School District, and is capable of applying any of the WCS functionality accorded to them by their WCS user group assignment. This virtual domain setting might be appropriate, for example, in the case of a person requiring the ability to view and potentially take action upon all resources in the network. An example of a person in a school district that might require such capability could be a school district administrator.

Figure 12 Virtual Domain for Entire School District



In contrast, Figure 13 and Figure 14 each illustrate how the user's view of the school district in WCS can be severely curtailed when a WCS virtual domain is applied. A virtual domain setting such as this might be appropriate for most of the personnel within a school that might only need to work with school resources located in their school only. Figure 13 illustrates what a user in Warren High School #1278 would see if they were assigned a WCS virtual domain that limited their resource visibility to only those resources associated with Warren High School.

Figure 13 Virtual Domain Limited to School 1278 (Warren High School)



In Figure 14, we see the results of a WCS virtual domain for a user in Gallatin Elementary, School #1266. Note that a user that is assigned a virtual domain for school 1266 does not have visibility to any resources associated with other schools. All that is visible to the school 1266 user in this case are the buildings and floor maps associated with school 1266.

Figure 14 Virtual Domain Limited to School 1266 (Gallatin Elementary)

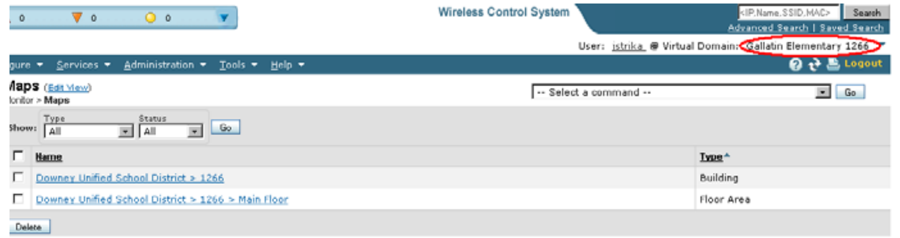


Figure 15 illustrates the typical result that occurs when a user attempts to view information for resources outside the scope of their assigned virtual domain. In this case, we see the result of a user in school 1266 attempting to access resources in another school, #1278.

Figure 15 Virtual Domain Permission Error

Mobility Services NMSP Parameters

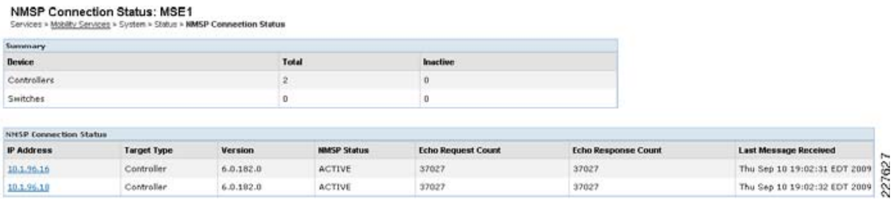
WCS 6.0 provides us with several NMSP parameters available that affect various NMSP protocol timing characteristics between the MSE and its session partners. These parameters can be found at **Services > Mobility Services > System > NMSP Parameters**, and apply globally to all NMSP sessions between the selected MSE and any of its WLAN controller or Ethernet switch session partners. Complete configuration information for configuring NMSP session timing parameters, as well as the default values for these parameters, can be found at Configuring Mobility Services Engine Properties section of the *Context-Aware Service Configuration Guide* (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch4_CAS.html#wp1014368).

When deploying an MSE locally in the school, it is unlikely that these parameters will require changes from the default values, except perhaps in the very largest of schools where there might be several thousand tracked devices, and a large quantity of wireless devices moving about on a regular basis. However, in a centralized deployment, there is more of a chance that network congestion or other factors may cause delays that could cause NMSP session timeouts. While this should be minimized by the appropriate identification and classification of NMSP data flows in the network along with properly defined network QoS, there may be instances where adjustments to NMSP timing are required. In these cases, the NMSP echo interval, neighbor dead interval, and response timeout values can be increased to limit the number of failed echo acknowledgments that may occur, especially in a centralized MSE deployment.

Note Readers are advised that a tremendous amount of functional validation was performed in association with the content contained in this document. However, time constraints limited the degree of performance validation that could be completed for Context-Aware Services across a simulated Metropolitan Area Network (MAN). The deployment of Mobility Services Engines in a centralized fashion across a MAN was not able to be fully validated due to these time constraints.

To aid in determining whether echo packets are being dropped, you can use the WCS function **Services > Mobility Services > System > Status > NMSP Connection Status** as shown in Figure 16. This WCS menu panel displays all the NMSP session partners for this MSE, along with echo request and response counts. For example, in the figure for the Mobility Services Engine with the hostname MSE1, we see that there are currently two NMSP sessions to two different school WLAN controllers.

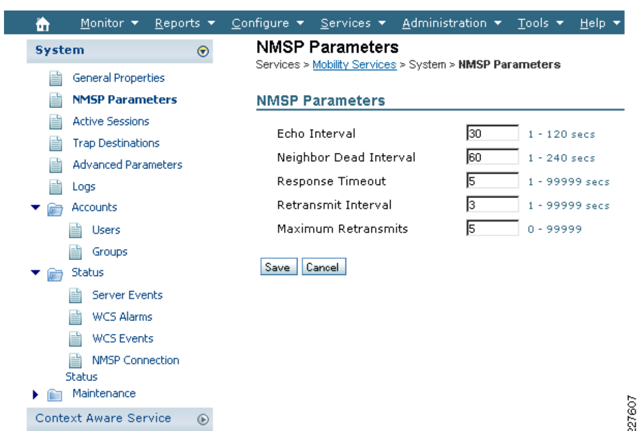
Figure 16 NMSP Connection Status



We can see in Figure 16 that both of the NMSP WLAN controller sessions appear to be functioning properly, as the number of Echo Requests issued is seen to be exactly equal to the number of Echo Responses received. This might not always be the case and small static differences over a long period of time do not necessarily indicate a serious problem. However, sluggish performance combined with a regularly increasing discrepancy in the delta between the number of requests issued and responses received could be indicative of the NMSP session timing out. In a centralized deployment, this may be due to unforeseen levels of congestion or other resource constraint. In this case, raising the response timeout may assist in alleviate the timeouts. Keep in mind, however, that a successful centralized deployment assumes that there is sufficient MAN capacity available to each school and that QoS has been applied appropriately.

Figure 17 gives an example of the NMSP Parameter screen that is located at **Services > Mobility Services > System > NMSP Parameters**, which we can use to change the system defaults. In Figure 17, the network administrator or network technician has instituted the following changes from the defaults: the echo interval has been raised to 30 seconds, the neighbor dead interval has been raised to 60 seconds, and the response timeout has been raised to 5 seconds.

Figure 17 Example of NMSP Parameter Modification



Note Although the NMSP configuration worked well for us in our lab testing, we cannot predict and simulate each and every condition that might occur in a production deployment. Therefore, it is important that you take the time to understand the function of these parameters and especially the fact that they can be adjusted beyond the values illustrated here in order to promote improved NMSP session stability and network performance.

Further information on these NMSP parameters can be found in the Configuring Mobility Services Engine Properties section of the *Context-Aware Service Configuration Guide* (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch4_CAS.html#wp1014368).

Context-Aware Service Parameters—Tracking

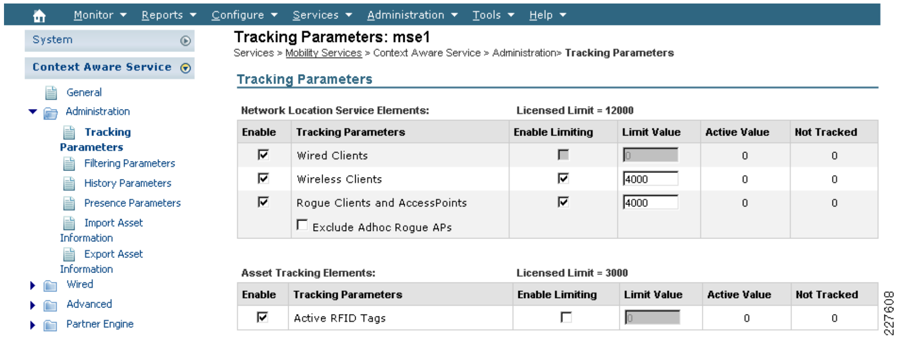
As mentioned earlier, Context-Aware Services can track up to a maximum of 18,000 licensed devices when using the MSE-3350 hardware platform, and up to a maximum of 2,000 licensed devices when using the MSE-3310 platform. The absolute limit on the number of clients or tags that can be tracked is determined by the hardware platform used, the presence of any other applications co-residing on the MSE, and the level of licensing purchased. The WCS tracking parameters configuration panel (located at **Services > Mobility Services > Context Aware Service > Administration> Tracking Parameters**) allows the administrator to pre-determine just how much of the MSE's maximum licensed tracking capacity will be allocated towards the tracking of specific device categories. This is useful in the Schools SRA environment in order to allow the tracking of device categories such as nearby rogue access points and rogue clients, but also limit these categories such that an uncontrolled introduction of rogues is not allowed to consume all of the remaining context-aware tracking capacity on the MSE.

We can use the Context-Aware Service Tracking configuration to:

- Entirely enable or disable the tracking of wired and wireless client stations, asset tags, rogue access points, and rogue clients.
- Set limits on how much MSE tracked device capacity will be allocated to certain device categories. Figure 18 provides us with an example of how this can be achieved, where the maximum number of tracked clients and rogue clients/APs are capped at 4,000 devices each. No limit is placed on the number of RFID tags tracked, which in effect means that the maximum number of tags tracked will be allowed to rise until the tag licensing limit is reached (3,000 tags).

Note that any devices that are detected but excluded from tracking due to the enforcement of a tracking limit will be reflected in the "Not Tracked" device count column shown on the right side of the display.

Figure 18 Context-Aware Service Tracking Parameters



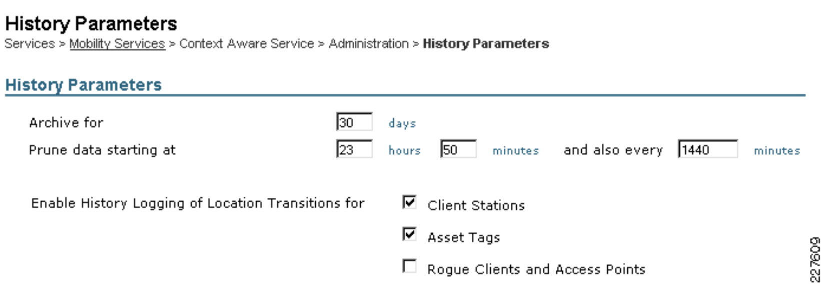
Note In Release 6.0, wired client tracking can be enabled or disabled, but imposing a limit solely on the number of wired clients tracked is not supported at this time. As a workaround, use switch CLI commands such as the global nmsp disable or the interface nmsp suppress attachment commands to limit the number of tracked wired clients that are presented to the MSE.

Context-Aware Service Parameters—History

The MSE records and maintains historical location and statistics information for wireless clients, tags, rogue access points, and rogue clients. This information is available for viewing through WCS or via third-party context-aware application clients, and can be very valuable in helping establish patterns of movement for tracked assets and rogues. Historical information can be used for location trending, asset loss investigation, RF capacity management, and facilitation of network problem resolution. Contextual information such as whether an emergency button was depressed or whether an asset tag has moved into close proximity to a chokepoint trigger is also tracked in the history data.

The collection of historical information must be explicitly enabled for each desired category of device (as shown in Figure 19). By default, 30 days of historical data are stored in the MSE.

Figure 19 MSE History Parameters



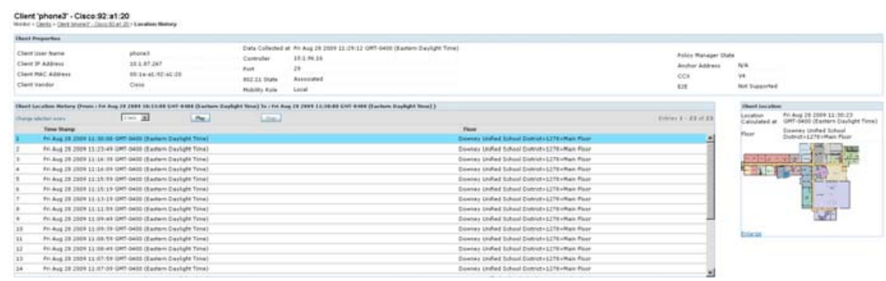
There are several variables that can affect how much historical information can be stored by the MSE for the tracked assets in your school or school district. Among these variables are the average number of elements that move, average distance covered every time there is a movement, information transitions, telemetry information from tags, and so on.

Depending on these variables as well as the number of items for which you are tracking history information in your school, you may wish to decrease the number of days of historical data to a value below 30 days.

Changes to the default history archive period should be done with careful consideration, since longer history periods typically increase the amount of space consumed by the history database. Users unfamiliar with the way in which Context-Aware Services on the Cisco MSE archives historical information for tracked devices may wish to consult with your Cisco field technical representative or the Cisco Technical Assistance Center

Figure 20 illustrates what you can expect to see when recalling the history for a tracked device. Here, we recall the history for a specific WLAN client. As shown in Figure 20, the focus of the display is the list of past locations recorded for the client. Setting the "change selection time" parameter on the screen and then clicking play displays the various client locations on the small floor map at the right side of the image (this can be enlarged for easier viewing). In this way, you can step back through all of the stored locations for the client within the history database. Obviously, this information could be very useful to school administrators, district and school WLAN engineers, as well as school resource officers and other law enforcement officials that may be looking for information useful in recreating a sequence of events that may have take place in the past.

Figure 20 Display of Location History for a WLAN Client in the School



Further information on the procedure to follow when making adjustments to history parameters can be found in the following documents:

Context Aware Solution Deployment Guide
http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#rfid

Context Aware Service Configuration Guide 6.0
http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html#wp1128896

Context Aware Service Parameters—Notifications

Cisco WCS allows you to define certain conditions for tags, WLAN clients, and rogues that cause the MSE to send notifications to application programs that are monitoring specific ports. You can use Cisco WCS to define and enable both conditional notifications and northbound notifications.

Conditional notifications are those notifications that the mobility services engine sends to Cisco WCS and other applications that can receive short, relatively simple messages via SOAP/XML (either HTTP or HTTPS), SMTP, UDP Syslog, or as an SNMP trap. Conditional notifications can be triggered by WLAN clients, tags, or rogue devices. The conditions available include:

- Missing—The MSE generates a Missing Asset conditional notification if it has not located the asset for more than a specified number of minutes.
- In/Out—The MSE generates an In/Out conditional notification if the asset is found to be inside of, or outside of, a selected area.
- Distance From Marker—The MSE generates a Distance From Marker conditional notification if the asset is found to be beyond a specified distance from a designated marker.
- Battery Level—The MSE generates a Battery Level conditional notification if the battery level reported by an asset tag is equal to a selected value.
- Location Change—The MSE generates a Location Change conditional notification if the asset experiences a change in location.
- Emergency—The MSE generates an Emergency conditional notification if a tag button, tamper or detached event is detected.
- Chokepoint—The MSE generates a Chokepoint Conditional notification if a tag enters into the proximity of a chokepoint trigger.

Northbound notifications are a special category of notification that is specific to RFID tags only. They define which tag notifications the MSE will send to third-party applications using SOAP/XML. Northbound notifications can include chokepoint, telemetry, emergency, battery, and tag vendor data. Optionally, the tag's location coordinates can be included within the northbound notifications as well. An important difference between conditional notifications and northbound notifications is that northbound notifications can contain considerably more information. The information sent in the northbound notification is sent in a pre-defined data format. Details regarding the data format for northbound notifications are available on the Cisco developers support portal at http://developer.cisco.com/web/contextaware.

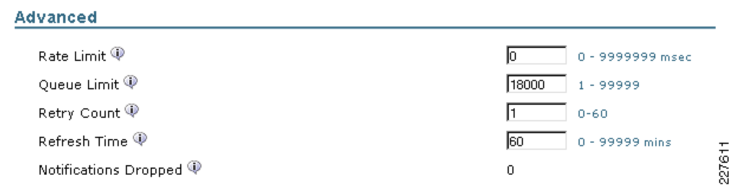
Note In Release 6.0, neither conditional nor northbound notifications can be applied to tracked wired devices.

Complete and detailed information regarding how to configure Context-Aware Notifications can be found in the following locations:

- Configuring Event Notifications chapter of the *Context-Aware Configuration Guide 6.0* (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch6_CAS.html).
- Enabling Notifications and Configuring Notification Parameters section of the *Context-Aware Configuration Guide 6.0* (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html#wp1129909).
- Context-Aware System Performance section of the *Context-Aware Solution Deployment Guide* (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#casysperf).

Via the menu panel located at Services > Mobility Services > Context Aware Service > Advanced> Notification Parameters (Figure 21),WCS allows the user to modify several advanced timing parameters pertaining to conditional notifications and northbound notifications. For example, you can limit the rate at which the MSE generates notifications, set a maximum queue size for notifications, and set a retry limit for notifications with in a certain period.

Figure 21 Context Aware Advanced Notification Parameters



Note Modify advanced notification parameters only when you can reasonably expect the Mobility Services Engine to transmit a large number of notifications or when it is noticed that notifications are being dropped.

- Rate Limit—(Pertains to northbound notifications only.) This is the rate in milliseconds at which the MSE generates northbound notifications. A value of 0 (default) means that the Mobility Services Engine generates event notifications as fast as possible. If you are using the northbound notifications system to communicate to a third-party application (such as AeroScout MobileView, for example) in the Schools SRA, it is recommended that you consider how often notifications are expected to be generated and how many total notifications will be requested of the MSE per minute. For example, an exception based notification (such as an emergency notification) is not a normal event and thus it would be extremely unusual to see a great deal of emergency events generated from many schools at the same time. However, a more routine event, such as the chokepoint entry event that would be used in a parent curbside pickup application, could be expected to generate much more traffic during, for example, the hours of 2:00-2:30 PM, when a large number of parents might be expected to pick up children from a suburban school district. In cases such as this where a large number of notifications might be a normal and routine event, it is recommended to increase the rate limit so as to allow the MSE to pace the transmission of notifications (for example, a rate limit value of 200 would slow the rate of notification transmission down to one every 200 msec). The correct notification delay will vary from deployment to deployment depending on the amount of traffic generated.
- Queue Limit—Specifies the size of the output notification queue of the MSE. Default queue limit value for the MSE-3350 is 18000 and for the MSE-3310 it is 5,000. The MSE drops any outbound notifications above this limit if the output notification queue size is exceeded. In the School SRA design, if you are using context-aware notifications, it is recommended that you use the Queue Limit parameter in conjunction with the Notifications Dropped counter to avoid any notifications from being dropped. If you notice that the Notifications Dropped counter is greater than zero, you should consider increasing the Queue Limit parameter to avoid any future increases. Given the relatively large default sizes for this parameter however, it is unlikely that adjustment will be required except in rare cases where very many notifications are generated.
- Retry Count—For each matching condition, the retry count specifies the number of times to generate an event notification before the refresh timer expires. The default value is 1. The total number of event notifications transmitted between Refresh Time periods is equal to one plus the value specified for Retry Count. After the value of one plus the Retry Count has been reached, the location appliance skips firing any further northbound notifications for this condition and device for the time period specified by the Refresh Time. Once the Refresh Time has expired, this cycle repeats unless the event has been cleared. Retry count is intended to help ensure (to a limited extent)

that notifications reach their intended destination. If notifications are not indicated as being dropped by the Notifications Dropped counter, but are not reliably reaching their destination application, you may wish to increase the number of notifications sent between Refresh Time periods by raising the Retry Count judiciously.

- The Mobility Service Engine transmits notifications using a “Fire and Forget” technique. Notifications are not retained in any database within the MSE after they are transmitted.
- Refresh Time—The wait time in minutes that must pass before an event notification is resent. The default is 60 minutes. Refresh Time and Retry Count are used cooperatively to help limit the number of notifications repeatedly generated for events that have not been cleared. Retry Count limits the number of notifications that are sent by the MSE, while Refresh Time imposes a “waiting period” during which time no further notifications are sent for this event condition and device. If you are noticing that repeated notifications are being generated for the same event, it may be due to the condition not clearing within the refresh time interval. In this case, you may wish to investigate why the triggered condition does not clear and possibly extend the refresh time.
- Notifications Dropped—The number of event notifications dropped from the queue since startup. The Notifications Dropped counter should be used in conjunction with the Queue Limit parameter to reduce the number of total dropped notifications.

WLAN Controller and Ethernet Switch Definition and Synchronization

To allow for proper tracking of the devices that may be registered or attached to them, WLAN controllers and context-aware Ethernet switches must be defined to WCS and then synchronized with the Mobility Services Engine.

Detailed information regarding how to add WLAN controller definitions to WCS using the WCS Configure > Controllers menu panel can be found in the section entitled Adding Controllers in the WCS Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0ctrlcfg.html#wp1041451).

Detailed information regarding how to add Ethernet switch definitions to WCS using the WCS Configure > Add Ethernet Switches menu panel can be found in the WCS Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0ctrlcfg.html#wp1089752).

Detailed information regarding how to synchronize the MSE with WLAN controllers and context-aware Ethernet switches using the WCS Services >Mobility Services > Synchronize WCS and MSE(s) menu panel can be found in the Synchronizing Mobility Services Engines chapter of the Context-Aware Service Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch3_CAS.html#wp998995).

Note Always ensure that the MSE is synchronized with the primary WLAN controllers it is providing Context-Aware Services for, as well as any backup WLAN controllers in the Schools SRA design. If the MSE is not kept in synchronization with your backup WLAN controllers, Context-Aware Services may not function properly or may not be available at all for WLAN clients and RFID tags in the event of a primary WLAN controller failure.

Wireless Client Context-Aware Considerations

The ability to track WLAN client location using Cisco Context-Aware Services can be useful in a school to locate WLAN clients that are part of our school network (such as authorized 7921G and 7925 VoWLAN phones, laptops, wireless desktops, etc.). Generally speaking, provided that a 802.11 wireless client device has its 802.11 wireless network interface adapter powered on and is sending periodic transmissions (probe requests), these WLAN client devices can be located by Context-Aware Services. Since devices such as portable VoWLAN phones are very often powered on for the entire day and carried on the belt, purse, or pocket of the user, these devices become useful in helping locate not only the device itself but the user to which the device is assigned. As the device becomes larger in size and heavier in weight, we find that the chances of the device being with the assigned user all the time diminishes and thus its usefulness as a way to determine the location of the user diminishes as well.

Tracking WLAN client devices by their wireless network interface adapter works well if the goal is to track the location of the device when it is in operation and use this information to enhance the operation of the device on the network, or its interaction with an application. For example, using WLAN client tracking in the school environment to perform one or more of the following represents a prime example of how this functionality can be put to use in the school environment:

- Determining where wireless users and their portable devices may congregate, allowing for the placement of access points to be further optimized to enhance overall coverage and performance.
- Investigate where a missing device is currently located within the school or district campus. A good example might be when equipment is “borrowed” from one classroom to another (or even from one school to another) without permission.
- Determining the location of users that are known to be visiting guests, and helping ensure that they do not stray into areas that have been explained to be off-limits to them.
- Using the location history of a wireless device to establish a pattern of usage and location in order to clarify past actions, such as any past actions that might relate to safety and security concerns.
- Use the location of wireless LAN clients as a parameter for network troubleshooting and security audits.
- Use the location of wireless printers (or other output devices) as input to an application designed to determine which device is available and most convenient for a particular wireless user depending on the user's location.

Figure 22 illustrates how Cisco Context-Aware Services can be used with Cisco WCS to display the current location of school faculty members equipped with Cisco 7925G IP phones, laptops, and PDAs in a sample lab school environment. Note that we have chosen to assign and display the user name associated with each device, rather than the device MAC address. Clicking on any of the blue WLAN client icons shown in Figure 22 displays a plethora of information about the client device, including its client properties, association history, connection troubleshooting information, as well as its event history.

Figure 22 WLAN Client Tracking

If the intention is to try and track a wireless device for inventory or loss prevention purposes, it is important to ascertain whether the embedded network interface remains active for any devices that may be in a powered-down or standby state. Even so, if the device remains active but accesses the network only very infrequently in order to conserve power, the degree of location fidelity obtained will likely be less than optimal, especially if the device can be expected to move frequently while in this state. A higher accuracy solution for this type of full-time location tracking application would be to attach or embed a RFID asset tag (see RFID Asset Tag Context-Aware Considerations) to the device. RFID tags are independently powered and operate without concern for the power state of the WLAN client device, and can be stimulated to transmit immediately when passing in proximity of properly equipped doorways and exits.

In general, best results are obtained in context-aware designs when all WLAN clients are compliant with the Cisco Compatible Extensions for WLAN Clients specification v2 at minimum, and preferably with the Cisco Compatible Extensions for WLAN Clients specification v4 or v5[1].

Additional information on the Cisco Compatible Extensions program for Wi-Fi Client Devices is available at http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html.

1. Readers interested in the technical details concerning compatibility with the Cisco Compatible Extensions for WLAN Clients specification v2 are referred to the section entitled Tracking Clients, Assets and Rogue Devices in Wi-Fi Location Based Services Design Guide 4.1, http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/wifich3.html#wp1049277

Note that this document does not detail the steps involved with important procedures such as calibration of the Context-Aware Engine for WLAN Clients, or the definition of location inclusion and exclusion regions and other deployment procedures. For information on these and other procedures that should be understood prior to deployment, refer to the *MSE Context Aware Service Deployment Guide* (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml).

Intel® Wi-Fi Clients and ProSet Client Supplicant Context-Aware Considerations

When using clients equipped with the Intel® Wireless WiFi Link 4965AGN, Intel® PRO/Wireless 3945ABG Network Connection, or the Intel® PRO/Wireless 2915ABG Network Connection adapter, it is important to note that the default "Personal Security" settings of the Intel® ProSet Configuration Utility does not include compatibility with the Cisco Compatible Extensions specification. In order to enable compatibility with the Cisco Compatible Extensions specification, the Intel ProSet client supplicant must be used to reconfigure the client for "Enterprise Security" and to enable Cisco Compatible Extensions using the "Cisco Options" (Figure 23 and Figure 24).

Figure 23 Enabling Cisco Compatible Extensions on Intel® ProSet Clients

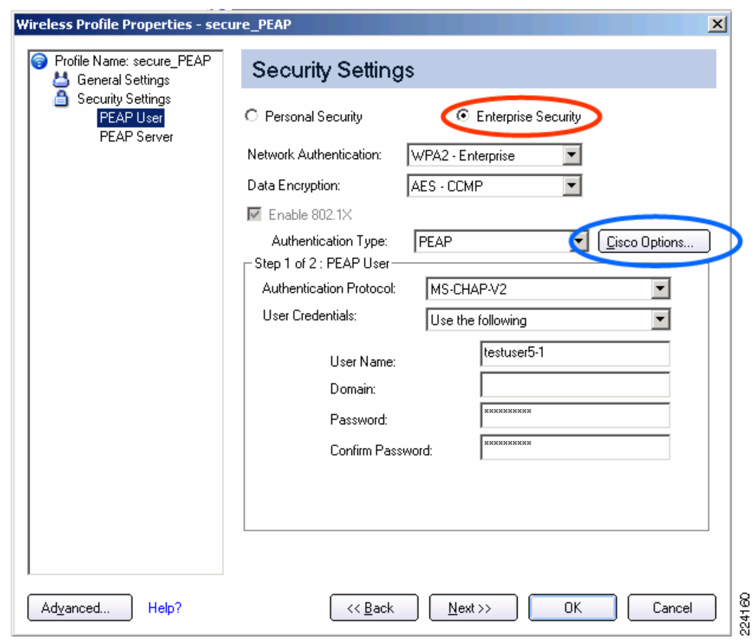
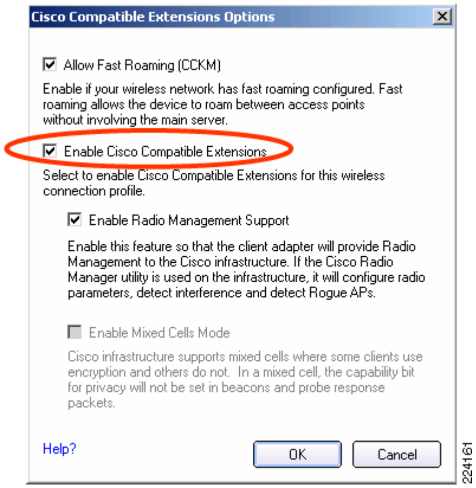


Figure 24 Enabling Cisco Compatible Extensions on Intel® ProSet Clients (2)

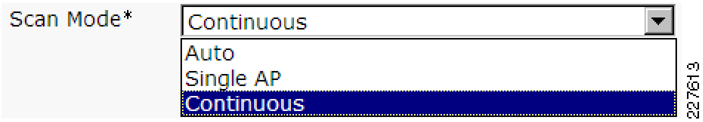


Cisco 7921 and 7925G Context-Aware Considerations

7921G and 7925G Unified IP Wireless Phone users should note that phones that are idle and not currently participating in an active call may not transmit 802.11 Probe Requests with sufficient frequency to ensure that changes in the actual location of the phone user are promptly reflected in the calculated location coordinates provided to the contest-aware services software in the MSE. In some cases this can be of concern, especially if the 7921G or 7925G user remains within the primary coverage area of the same access point for long periods of time. In cases where an access point might have a large coverage footprint, a roaming event may not occur very often despite a significant change in user location.

If you experience situations where the location fidelity of a 7921G or 7925G Unified IP Wireless Phone appears to be much better for those users actively participating on a call versus those that are on hook and idle, you may wish to consider changing the scan mode parameter associated with the 7921G or 7925G device in the Cisco Unified Communications Manager. In some cases, improved location fidelity can be achieved by enabling the "continuous" scan mode on the Device=>Phone configuration page of Cisco Unified Communications Manager Administration (shown in Figure 25). Note that scan mode options listed are "auto", "continuous", and "single AP", where auto is the default. "Continuous" scan mode causes the wireless IP phone to issue a probe request approximately every two seconds, whereas "auto" scan mode causes the device to issue probe requests primarily only when the device is engaged on an active call, when roaming, or when preparing to roam. "Single AP" is used in installations where the wireless IP phone is only used in the vicinity of a single access point at all times, as probe requests are issued only when the wireless IP phone is first powered on. "Single AP" mode is not applicable and should not be used in the Schools SRA design.

Figure 25 Scan Mode Option in Cisco Unified Communications Manager

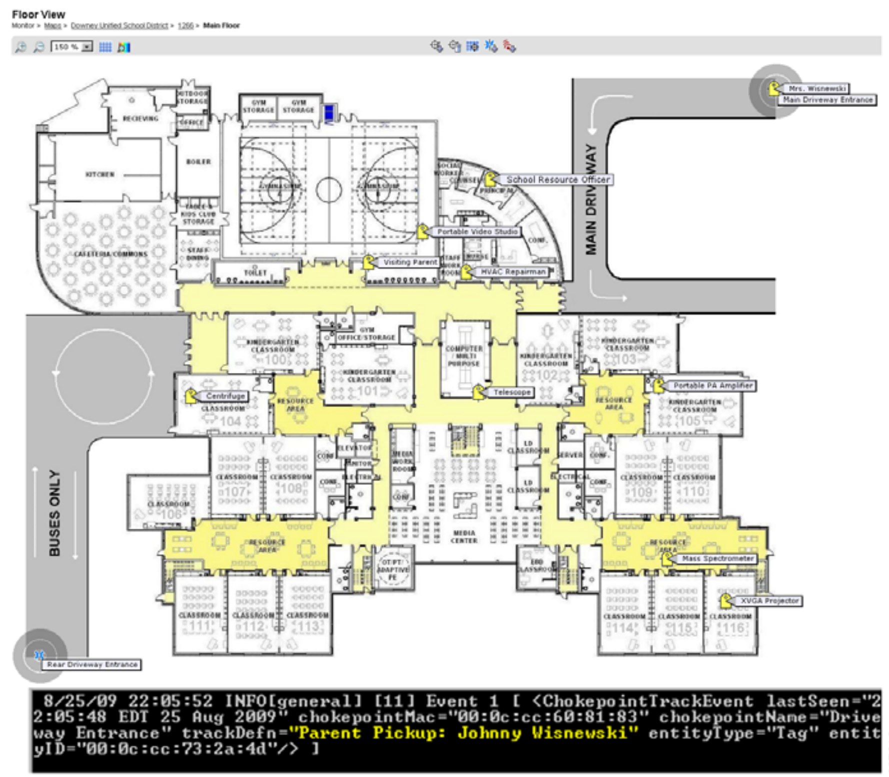


Note It is recommended that continuous scan mode be used only in situations where the anomaly described here is actually witnessed. This is because a trade-off associated with any increase in the frequency of probe requests transmitted is the potential for reduced 7921G or 7925G battery life. If you do not notice the anomaly described in this section, it is recommended that you leave the CUCM scan mode setting at the "auto" default.

RFID Asset Tag Context-Aware Considerations

Radio Frequency Identification (RFID) has many potential safety and security applications in the education arena. Already used in various enterprise sectors, from the logistics depot that tracks pallets of goods throughout the warehouse, to the motorist with the "EZ-Pass" or "CruiseCard" that no longer needs to search for change at the toll booth, schools can now embrace RFID technology to address a wide realm of challenges.

Figure 26 Floor Map Showing Various Uses of RFID Tags and Cisco Context-Aware Services



The illustration in Figure 26 provides us with a visual representation of just some of the ways RFID can be used in the Schools SRA in conjunction with Context-Aware Services:

- High value assets (such as projectors, microscopes, telescopes, audio/video equipment, etc.) can be kept safe and secure, since the application of RFID tags to these assets provides school administrators and school resource officers with the ability to locate the assets quickly and efficiently. Figure 26 illustrates how the present location of assets equipped in this fashion can be quickly ascertained by a quick check of the school floor map. Here we can see the last known location of a lab centrifuge, microscope, telescope, portable PA system, XVGA projector, and even a mass spectrometer. For buildings containing more than a single floor, database search techniques can be used to search for the desired asset by name or attached RFID tag MAC address.

Figure 27 ID Badge with Embedded Active RFID

- Faculty and administrators can wear specially manufactured badges (see Figure 27) that combine a traditional identification card with active RFID technology, allowing them to be located quickly in the event of an emergency. These same devices can also transmit special notifications using a push button sequence, which can be interpreted in various ways by Context-Aware Services, including as a signal that an emergency event is in progress. Figure 26 illustrates how a person can be located if they are carrying an RFID-enabled ID card, as seen in the displayed location of the school's resource officer (a law enforcement official), whose location is currently indicated as being inside of the school principal's office. Being able to physically locate the school resource officer using a tool such as this could help in saving precious seconds in the event of a school emergency.
- The whereabouts of school visitors (such as maintenance or repair contractors) can be monitored and alerts triggered to school resource officers and others if these visitors stray into areas that they have no authorization to be in. For example, in Figure 26, we see that in our school we have an HVAC repair contractor as well as a visiting parent. In addition to making us aware as to the presence of these visitors, our system can alert us if these personnel access areas that we do not want them to by comparing their current locations to location boundaries we have defined as notification rules. Third-party applications that can access context-aware information from the MSE may perform more advanced tasks as well.
- RFID tag technology can be combined with chokepoint triggers (Exciters) to enable the use of proximity applications. In this fashion, chokepoint triggers can serve many purposes, including stimulating asset tags affixed to assets that might be in the process of being removed from the school building without authorization. This makes it possible to notify school officials or resource officers of such action, so as to act quickly and determine whether such movement is legitimate.

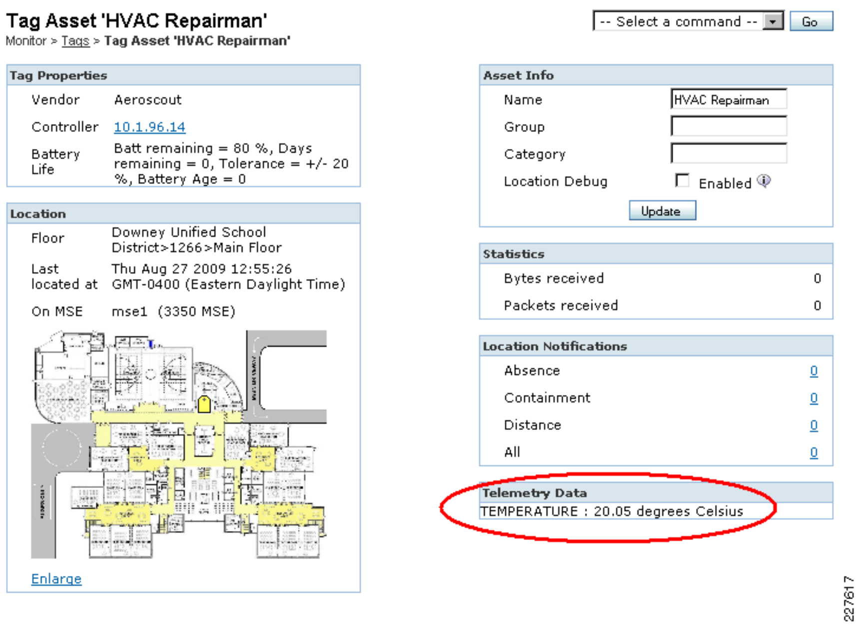
Figure 28 Curbside Congestion at an Urban K-12 School

- The concept of a curbside student receiving application in a suburban school system that notifies student hallway monitors and school faculty assistants when a parent has entered school property, ready to pickup their child at the end of the school day. By issuing the parent an RFID tag that is serialized and known to the context-aware system, safety, security, and efficiency is increased. School personnel are aware that the parent's vehicle has entered school property and is waiting in the queue for their child. Children can be retrieved from waiting areas and classrooms in an efficient manner, and presented to parents that are in queue at the school front entrance. This reduces school curbside congestion (see Figure 28), gets parents and students in and out of the school area quickly, and reduces the amount of pollutants emitted by idling vehicles waiting in line for curbside pickup and drop off.

  An RFID tag whose MAC address has been recorded and registered with Context-Aware Services as to being issued to a particular parent and vehicle is shown in Figure 26. In Figure 26, we see that the arrival of a young student's mother ("Mrs. Wisnewski") is signified by the appearance of an RFID tag assigned this label at the location of the chokepoint trigger installed at the school driveway entrance. Even more importantly, the lower portion of Figure 26 provides a conceptual illustration of how Cisco Context-Aware Services can generate a SOAP/XML notification to a receiving application ("Parent Pickup: Johnny Wisnewski"). The receiving application then could be used to trigger visual and audible notification in the school that this child's parent has arrived and that the child should be brought forward and queued for release. As each parent vehicle in a long stream of cars enters the school driveway and takes its place in the queue, school personnel are made aware that the parent is only a few hundred yards away and will soon be at the curbside front door pickup area to pickup their child. This system can help manage this process and drastically increase the ability of limited school resources to dispatch those children to those parents that prefer to drop off and pick up their children each day.

  In addition to simply displaying the location of assets, Cisco Context-Aware Services makes other contextual characteristics of the asset and its environment available to applications accessing the MSE via its SOAP/XML API. For instance, if the asset tags used contain on-board temperature sensors, we can also read the current temperature surrounding the asset tag via the MSE. This can be seen in Figure 29, where we see from WCS that the ambient temperature surrounding our HVAC repairman is 20 degrees Celsius or a comfortable 68 degree Fahrenheit. Looks like our school air conditioning system is doing its job from what this tag sensor tells us. It is important to note that while WCS is used to view this information in Figure 29, any authorized context-aware application that is written to use the MSE SOAP/XML API could have accessed this data as well.

Figure 29 Temperature Telemetry Information



Simply put, RFID technology and Cisco Context Aware Services can help schools improve their overall safety, security, and efficiency.

Cisco Context-Aware Software is designed to function with active RFID asset tags from vendors compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification. A list of current Cisco Compatible Extensions for Wi-Fi Tags compliant vendors can be found at http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html. Although all vendor RFID tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification share a great deal of functionality in common, the parameter names and means used to configure each brand of tags can differ from vendor to vendor, therefore no set prescribed configuration parameter list would apply to all. That being said, there are several general configuration functions that tag vendors share and although the exact parameter names may differ, it is important that you understand them and use this knowledge accordingly when configuring the particular tags of choice for your installation. More information regarding the configuration procedure for AeroScout tags can be found in the section entitled RFID Tag and WLC Configuration/Tuning in the Cisco MSE Context-Aware Deployment Guide (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#rfid-wlc)[1].

1. Additional information can also be found in the *Wi-Fi Location-Based Services Design Guide 4.1* section entitled Configuring Asset Tags, located at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/wifich6.html#wp1077248.

- RF Channel Configuration—It is recommended that tags be configured for the standard set of 2.4 Ghz non-overlapping channels, which is typically channels 1, 6, and 11 (this may vary depending on your international regulatory domain).
- Stationary Transmission Interval—This is the time between periodic tag transmissions that are normally generated when the tag is stationary and not in motion. It is recommended that this be configured for values between 3 and 5 minutes.
- Motion Transmission Interval—(Applies only to tags with motion sensors.) This is the time between periodic tag transmissions generated when the tag and asset is in motion. A recommended initial value is 15 seconds.
- Number of Tag Message Repetitions—Some popular RFID tags default to transmitting a single transmission on all defined channels. Tag parameters that control the number of tag message repetitions specify the number of times each transmitted message is repeated, per channel. It is generally recommended that this parameter be set to a value of three. Doing this helps protect against lost tag transmissions due to congestion or interference, which is a primary cause of poor tag location accuracy.

Message Repetitions Interval—The delay between subsequent message repetitions on the same channel. This is often defaulted to 512msec, although in lab testing we have seen some evidence of improved location accuracy when a message repetition interval of 256 msec is used with the default controller value of 2 seconds for NMSP notification interval. This parameter is discussed in more detail the section entitled RFID Tag and WLC Configuration/Tuning of the *Cisco MSE Context-Aware Deployment Guide* (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml#rfid-wlc).

This chapter does not detail the steps involved with procedures such as calibration of the Context-Aware Engine for Tags and other deployment procedures. For information on these and other procedures that should be understood prior to deployment, refer to the *MSE Context Aware Service Deployment Guide* (http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml). In addition, the AeroScout Context-Aware Engine for Tags for the Cisco MSE Users Guide, version 3.2, available from your AeroScout representative or https://support.aeroscout.com, is highly recommended.

RFID Tag Chokepoint Trigger Considerations

Chokepoint triggers are proximity communication devices that trigger RFID asset tags to alter their behavior when the tag enters into close range (otherwise known as the stimulation zone) of the chokepoint trigger. This behavioral modification may, for example, cause the RFID tag to immediately transmit its unique identifier (MAC address) or cause the tag to change its internal configuration, depending on how the tag is programmed. A very popular use of the chokepoint trigger is to stimulate the asset tag such that it provides indication to the MSE that the tag has entered or exited a given area, known as a chokepoint. Chokepoints are entry or exit points that provide passage between connected regions. Common chokepoints are entrances and exits such as doorways, hallways, and stairwells.

Note An Exciter is a registered trademark of AeroScout Ltd., and represent a popular example of a chokepoint trigger.

In schools, chokepoint triggers are useful in causing RFID tags to react quickly when assets are moved past certain points in the school. This could be a microscope with an affixed RFID tag moving past a chokepoint trigger located near a school exit, a faculty member with an RFID badge walking into the school through the front entrance at 7:00 AM, or it could be a parent in the family automobile that has a RFID tag on the front visor coming past a chokepoint trigger located at the entrance of the school property. In all these cases, the chokepoint trigger causes the tag to change its behavior, most likely to immediately transmit its MAC address (as well as the MAC address of the chokepoint trigger that stimulated it) to the MSE via one or more access points that can receive the tag's transmissions. The net result is to cause the MSE to indicate that the current location of the asset and its asset tag is within a known, pre-determined proximity of the chokepoint trigger.

In order to use chokepoint triggers with Cisco Context-Aware Services, they must be properly configured using the appropriate vendor-supplied software utility, defined to WCS, placed on floor maps, and synchronized as part of an updated network design to the MSE. After all of this is complete, the MSE is able to recognize the transmissions generated by asset tags that have been stimulated by specific chokepoint trigger MAC addresses. Based on this information, the MSE can attempt to localize the tag to the proximity of the chokepoint trigger. Applications such as WCS (or third party context-aware applications) may then display the asset tag's location at the chokepoint icon associated with the chokepoint trigger's MAC address.

Various chokepoint trigger specific parameters such as transmission range, IP address, transmission interval, transmission repetitions, and so on are set using vendor-specific utilities. Note that each vendor maintains their set of software tools necessary for configuration of their chokepoint triggers. These software configuration tools are not interoperable between vendors (for example, AeroScout software configuration tools cannot be used to configure WhereNet chokepoint triggers or vice-versa).

The individual configuration of each vendor's chokepoint trigger is beyond the scope of this document. Complete and detailed configuration information relating to the specific configuration of each vendor's chokepoint trigger can be found in the appropriate vendor's documentation, which can be obtained from your tag vendor representative.

- AeroScout EX-3200 User Guide https://support.aeroscout.com
- AeroScout Exciter EX-2000 User Guide https://support.aeroscout.com
- AeroScout Context-Aware Engine for Tags for the Cisco MSE Users Guide, version 3.2 https://support.aeroscout.com

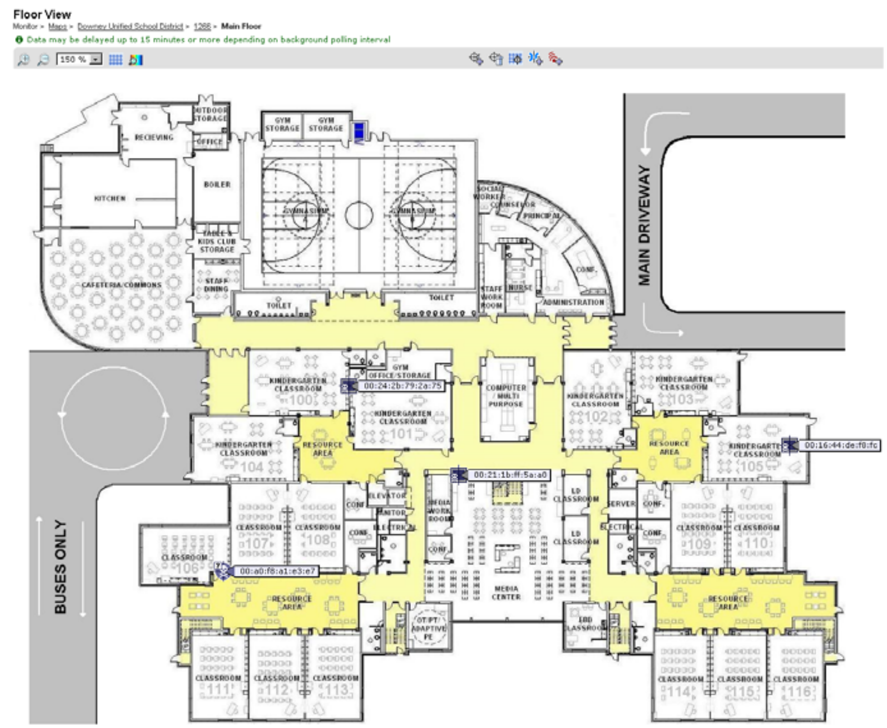
Technical documentation for WhereNet WherePort chokepoint triggers and the necessary software and hardware for configuration of WherePorts is available from WhereNet Corporation (http://www.wherenet.com) or via your WhereNet account representative.

Rogue Device Context-Aware Considerations

The use of context-aware services for locating clients and RFID tags that we have defined and authorized in the school environment is often what first comes to mind for many of us when we consider this solution. However, another equally important and useful function of context aware services is the ability to detect the location associated with those wireless clients and access points that we have not authorized to operate within our domain. In other words, context-aware services in our schools can help us in locating rogue access points or rogue clients that may have been installed within our school by students, contractors, visitors, vendors, or even faculty or administration members without authorization. Even if an unauthorized access point is innocently installed by a school user that is otherwise authorized to use the school network, the unauthorized and potentially insecure portal provided by such an access point can unnecessarily expose our secure school network to outside intruders.

The Cisco Wireless Control System can use the location capabilities provided by the Cisco Mobility Services Engine and the Cisco Context-Aware Engine for Clients to define the location of unauthorized access points and the wireless clients that may be using these access points, as shown in Figure 30. In the figure, we can see icons for both rogue access points as well as rogue clients displayed over their predicted positions on a floor map of an elementary school located within our school district. This capability is very useful both to the local school administrator, as well as the district network administrator and their technical teams. It allows them to determine the location of wireless equipment that may have been brought into the school and used in an attempt to gain unauthorized access to school or district computing resources. In Figure 30, the round icon with the "skull and crossbones" logo represents the rogue access point and the rectangular icon with the same logo represents a rogue client that is associated to this rogue access point.

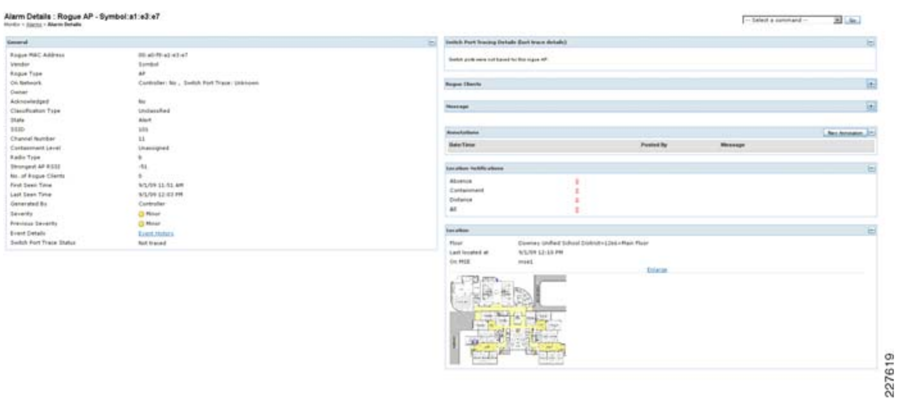
Figure 30 Using Context-Aware Services to Perform Location of Rogue Access Points and Clients



Note In comparison to WLAN clients and RFID tags, it is normal to experience a reduced accuracy when localizing rogue access points and rogue clients. The very nature of "rogue" devices establishes that these devices are not under the control of school administration. Therefore, the configuration of such these rogue devices may not facilitate optimal context-aware location accuracy (for example, they may not be Cisco Compatible Extensions devices, etc.).

As shown in Figure 31, clicking on either the rogue access point icon or the rogue client icon reveals additional information and capabilities that can help in further identifying (and even isolating) these devices. This includes the ability to perform switch port tracing with the latest versions of WCS, which allows tracing of rogue access points that have been connected to the switch infrastructure (for more information on switch port tracing, refer to the WCS Configuration Guide 6.0, (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0ctrlcfg.html#wp1089752).

Figure 31 Rogue AP Details

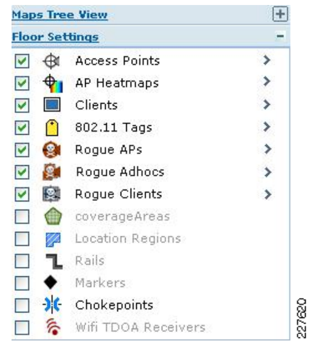


The collection of rogue AP and rogue client information is enabled by default on WLAN controllers. In order to enable the tracking of rogue access points and rogue clients by the context-aware service, it is important to ensure that the collection of rogue information has also been enabled for context-aware services on the MSE. Refer back to Figure 18 in this document and ensure that the "Rogue Client and Access Points" tracking parameter check box has been enabled under Mobility Services > Context-Aware Services > Administration >Tracking Parameters.

Note Be advised that depending on the environment in which your school is located, as well as the number of rogue devices present, the number of rogue devices detected can rise very quickly. Since the size of the rogue device population is typically not under the direct control of school IT staff or local school administration, it is highly advisable that you enable limiting for rogue clients and access points and set a limiting value. This is so that any unforeseen increase in the number of rogue devices detected does not consume all the remaining tracked device capacity on the MSE, thereby depriving the MSE of capacity that might be of more significance to school administration and faculty. This is especially important if the MSE is used to service more than just one school in your district.

In addition to enabling the collection of rogue access point and rogue client information by the context-aware services on the MSE, you must also enable the display rogue device location when displaying floor maps using WCS. This is accomplished via the WCS "Floor Settings" submenu that is displayed on every WCS floor map, as shown in Figure 32. Information on how to use the Floor Settings sub-menu for all the categories of device shown here can be found in Chapter Five of the WCS Configuration Guide 6.0, http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0maps.html#wp1210969.

Figure 32 WCS Floor Settings Sub-Menu



For further information regarding rogue access points and clients, refer to the following documents:

- Context Aware Service Configuration Guide 6.0 http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/CAS_60.html
- Cisco Wireless Control System Configuration Guide, Release 6.0 http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html
- Cisco MSE Context Aware Deployment Guide http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml

Context-Aware Considerations for Wired Device Tracking

As described previously in this document, beginning with release 6.0 Cisco Context-Aware Services provides the capability to determine the civic location and emergency line identifiers of devices connected to Cisco Catalyst switches, such as the 2960G, 3560E, 3750E, 3750G, 4500, and 4900 series. As participants in context-aware services, switches are configured with and provide the relevant contextual information for all the IP endpoints attached to them. These endpoints may include IP phones, PCs, host servers, access points, etc. The NMSP protocol is used between the switches and MSE to deliver this contextual information to the MSE. Location information may include the physical location address (also known as the civic address) as well as other information about endpoints such as the IP address, MAC address, port, VLAN, and username. If the end device makes use of the Cisco Discovery Protocol or Link Layer Discovery Protocol (LLDP), additional information, such as the version number and serial number, can also be sent to the MSE.

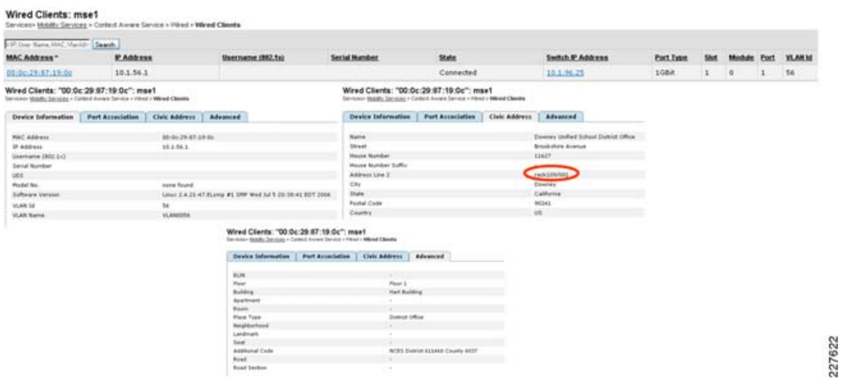
Note The use of Context-Aware Services for wired device location is entirely optional. In the School SRA, Context-Aware Services may be deployed for wireless devices, wired devices, or for both.

The district office, large school, and small school design of the Schools SRA provides that in the event of a failure of a switch line card in a 4500 series context-aware Catalyst switch, or a stack member in the 3750 switch stack, NMSP sessions recover from the failure without intervention from the user. For the Schools SRA design, NMSP session recovery time from isolated switch stack member or line card failure was seen to occur in the lab very quickly, and in most cases the recovery time was almost unnoticeable from the perspective of the Mobility Services Engine. Careful examination of the NMSP session status during simulated failures indicated that sessions remained up, intact, and passing NMSP data while stack member or line card hand-off occurred.

While still a relatively new context-aware capability, the inclusion of wired device tracking provides new visibility into the location of wired IP endpoints in your school network. For example, some of the ways that this new exciting capability can be used in the Schools SRA design include:

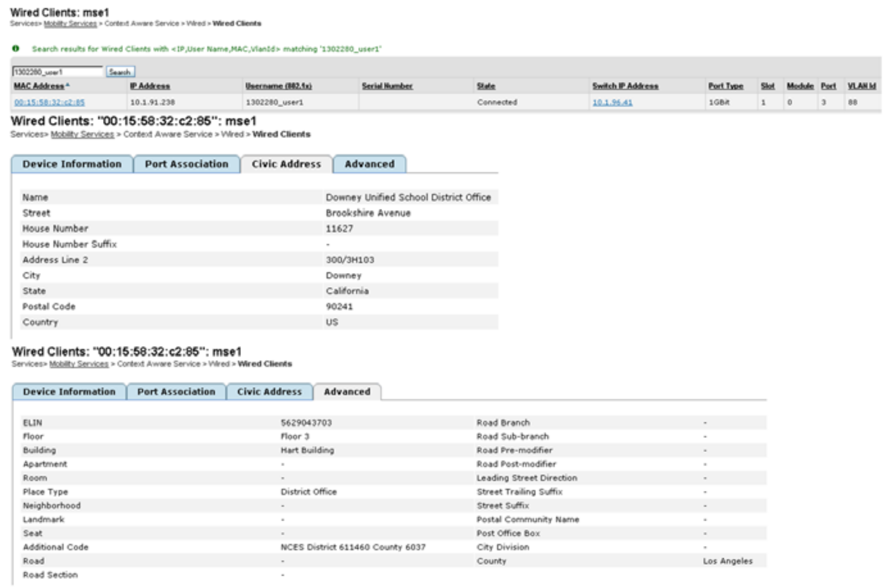
- Determining the whereabouts of missing IP phones, PCs, and peripheral devices such as printers and network scanners that have disconnected and moved from their originally installed locations to other locations within a school (or moved to another school). Once reconnected to the network, the MSE would be updated with the wired device's new attachment information and any location and/or ELIN information defined for that switch port.
- Keeping track of the location of host computers located in the district data center or in any school. The wired location capabilities contained in release 6.0 of Context-Aware Services make it possible to specify the location of a device down to the room, cubicle, seat, or even rack/slot location (see Figure 33). This can be important in verifying that equipment to be de-commissioned is actually removed from service and sanitized of all student information.

Figure 33 Displaying the Location of a Wired Host



- Determining the civic location of users based on their IP address or the user name that was specified during 802.1x / EAP login (refer to Figure 34). Context-Aware Services for wired devices makes it possible to quickly determine the civic or emergency line identifier information associated with the switch port. Figure 34 illustrates how we can search for the wired device by the known username.

Figure 34 Searching for Wired Device by Username



- For devices that support it, impromptu inventory checks of devices across the school district by examining wired device listings by serial number (see Figure 35) and comparing this information to deployment records. This can help school and district administrators better determine whether assets have been moved between schools without authorization.

Figure 35 Examining Device Serial Numbers Via Wired Device Tracking

In contrast to the manner in which searches for wireless clients and tags is handled via the WCS Monitor > Maps, in Release 6.0 of Context-Aware Services, all wired client searches are handled via the Services > Mobility Services >Context Aware Services > Wired > Wired Clients menu panel. Searches using the wired client WCS menu panel are specific to the particular MSE that you have selected.

Hardware and Software Requirements for Wired Device Tracking

As mentioned previously, at the current time wired device tracking is only performed on Catalyst switch hardware such as the 2960G, 3560E, 3750E, 3750G, 4500, and 4900 series. The images used for testing of wired device tracking during the production of this document included:

- cat4500e-entservicesk9-mz.122-53.SG.bin
- c3750-ipservicesk9-tar.122-50.SE3.tar

- c3750e-universalk9-tar.122-50.SE3.tar
- c2960-lanbasek9-tar.122-50.SE3.tar

Note Readers should note that cryptography-enabled (k9) switch images are required in order to enable wired device tracking in Catalyst switches.

- You should be aware that including wired device tracking in your design will require additional tracked device licenses on the MSE over and above that required for wireless device tracking alone. This is because wired tracked devices are included in the maximum number of simultaneous devices that can are licensed for tracking by an MSE. For example, a school that would otherwise possess a maximum licensed tracked device requirement of 500 for wireless LAN clients, RFID tags, and rogues might require 750 or more when wired device tracking is considered, depending on the number of switches deployed and whether wired device tracking is enabled for all of them. Be sure to plan appropriately for the number of wired devices that you intend to track when purchasing MSE client tracking licenses for the Cisco Context-Aware Engine for Clients.

In addition to planning appropriately for an increase in MSE tracked device licensing due to the use of wired device tracking, keep in mind that although a single MSE can technically support up to 500 NMSP sessions, scalability testing limits have only allowed Cisco to test up to 100 simulated NMSP connections to a single MSE at this time. Each context-aware switch that is enabled for wired device tracking in your network establishes one NMSP session to the MSE and counts against this limit. Therefore, when enabling many switches for context-aware wired device tracking, it is recommended that you plan for the total number of MSEs that may be required to support the total number of NMSP sessions in your network.

Enabling Context-Aware Wired Device Tracking

In order to track wired devices on Catalyst switch ports, each switch whose devices we wish to track must be configured to enable NMSP and other important parameters, and to contain the appropriate civic address and ELIN location information. In addition, WCS must be configured to be aware of the context-aware switches in the network and to be able to communicate with them. WCS is also used to transmit information about the switches to the Mobility Services Engine via the synchronization process.

A complete, step by step guide to configuring Catalyst switches and WCS for wired device tracking can be found in the Context Aware Service Configuration Guide 6.0 http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html#wp1224011.

In addition, the following chapters and documents provide valuable and detailed background information concerning the wired device tracking capability of Catalyst switches:

- Configuring LLDP, LLDP-MED, and Wired Location Service in the Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/swlldp.html
- Configuring LLDP, LLDP-MED, and Wired Location Service in the Catalyst 2960 Switch Software Configuration Guide, 12.2(50)SE http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/swlldp.html
- Configuring LLDP and LLDP-MED in the Catalyst 4500 Series Switch Software Configuration Guide, 12.2(53)SG http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/53SG/configuration/swlldp.html#wp1097119

Readers are reminded that:

- NMSP is disabled on switches by default. It must be explicitly enabled via the **nmsp enable** global configuration command.
- IP device tracking must be enabled on the switch in order for Context-Aware wired device tracking to function properly. It can be enabled by issuing the ip device tracking in global configuration mode on the context-aware switch.
- The civic location identifier in the LLDP-MED TLV is limited to 250 bytes or less. To avoid receiving error messages regarding available buffer space during switch configuration, the total length of all civic location information specified for each civic-location identifier must not exceed 250 bytes.
- In Release 6.0, all wired device client and switch tracking is available only to the root WCS virtual domain user. Because of this, you may wish to limit the use of context-aware wired device tracking to only those users with whom you are comfortable assigning WCS root virtual domain privileges.

NMSP Attachment Notification Interval

After an NMSP session is established between the MSE and a context-aware Catalyst switch, the MSE transmits an Echo Response packet to the switch every echo interval period, which is specified on the MSE (for all NMSP session partners) using the WCS menu entitled Services > Mobility Services > System > NMSP Parameters. In addition to Echo Responses, the switch will periodically send attachment notifications to the MSE via the NMSP session. Any link-up or link-down events that are detected by the switch are aggregated during a configurable time interval and sent to the MSE via an attachment notification at the conclusion of that time interval.

This interval is known as the nmsp attachment notification interval and is configurable on the switch via the **nmsp notification interval attachment** *interval-seconds* command. The range of values for interval-seconds is from 1 to 30 seconds, with 30 seconds being the default. In large networks where there are many NMSP sessions active across the MAN to an MSE and the number of users connecting and disconnecting from the switch is high, configuring **nmsp attachment notification** *interval* to a very short interval can increase the amount of NMSP traffic between switches and the MSE and is not recommended[1] without carefully understanding the nature of the traffic present in your network.

Civic Address Configuration

The information contained in the Context Aware Service Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html#wp1224011) provides the information necessary to configure context-aware switches and the WCS for wired device tracking.

As can be seen in the Context Aware Service Configuration Guide, in release 6.0 of Context-Aware Services all configuration of civic and ELIN location information is performed on each context-aware switch using the switch CLI. Once a switch is

1. Except for switches that are local to the Mobility Services Engine and need not traverse the MAN.

configured with the desired civic and ELIN location information, the switch will share all of the configured port information with the MSE when the NMSP session is initially established and will periodically update the MSE if any location updates are performed.

Note Readers should find the following IETF RFC documents helpful in better understanding the types of values that should be specified for the various civic location fields: RFC 4776 (http://www.ietf.org/rfc/rfc4776.txt), RFC 4589 (http://www.ietf.org/rfc/rfc4589.txt), and RFC 5139 (http://www.ietf.org/rfc/rfc5139.txt).

During the course of our lab testing, we discovered other useful facets of information regarding civic location and ELIN configuration in Catalyst switch IOS releases 12.2-52(SE) and 12.2-53(SG):

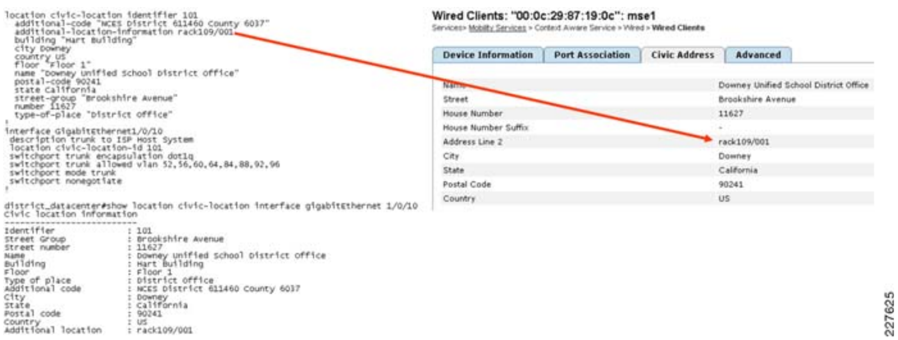
- Global Scope of Civic and ELIN location—Civic address or ELIN information must be configured at a global level and then assigned to each switch interface using the appropriate civic or ELIN location identifier. Globally defined civic address parameters (such as the building, county, postal code, floor, and so on) cannot be individually over-ridden at the interface level in release 6.0. If more than one switch port shares the same civic location or ELIN, then the same globally specified civic and ELIN location identifiers can be used on each switch port interface. However, if all ports possess unique civic address characteristics, then uniquely specified global civic address parameters for each port must be used. This can be seen in the following example where three unique civic location identifiers are applied to three different ports (Gi1/0/3 - 1/0/5). The test application server that is being tested on port Gi 1/0/6 is in the same physical location as the device connected to port Gi1/0/5, hence they share civic-location identifier 3.

```
location civic-location identifier 1
additional-code “NCES District 611460 County 6037"
building “Hart Building”
city Downey
country US
county “Los Angeles”
floor “Floor 3"
name “Downey Unified School District Office”
postal-code 90241
state California
street-group “Brookshire Avenue”
number 11627
room 300
seat 3H103
type-of-place “District Office”
!
location civic-location identifier 2
additional-code “NCES District 611460 County 6037"
building “Hart Building”
city Downey
country US
county “Los Angeles”
floor “Floor 3"
name “Downey Unified School District Office”
postal-code 90241
state California
street-group “Brookshire Avenue”
number 11627
room 300
seat 3H104
type-of-place “District Office”
!
location civic-location identifier 3
additional-code “NCES District 611460 County 6037"
building “Hart Building”
city Downey
country US
county “Los Angeles”
floor “Floor 3"
name “Downey Unified School District Office”
postal-code 90241
state California
street-group “Brookshire Avenue”
number 11627
room 300
seat 3H105
type-of-place “District Office”
!
interface GigabitEthernet0/3
description 802.1x data access only
location civic-location-id 1
switchport access vlan 88
switchport mode access
authentication port-control auto
dot1x pae authenticator
!
interface GigabitEthernet0/4
description 802.1x data access only
location civic-location-id 2
switchport access vlan 88
switchport mode access
authentication port-control auto
dot1x pae authenticator
!
interface GigabitEthernet0/5
description 802.1x data access only
location civic-location-id 3
switchport access vlan 88
switchport mode access
```

```
authentication port-control auto
dot1x pae authenticator
!
interface GigabitEthernet0/6
description test school local RFID gate application server
location civic-location-id 3
switchport access vlan 56
switchport mode access
!
```

- Civic location **additional-location-information** subcommand—During the course of our testing we found the **additional-location-information** subcommand useful in adding miscellaneous information about devices that can be displayed on the civic address tab of the WCS wired clients display under "Address Line 2". In our testing, we made use of this facility to label the rack and position location of various servers and other devices that are deployed in a common location. Figure 36 illustrates how the information entered using **additional-location-information** is then displayed on the civic address tab of the WCS wired clients display for the device (indicated by the red arrow). Below the configuration for the switch port, we can see the results of displaying the civic location for the switch interface using the **location civic-location interface** *interface* command.

Figure 36 Additional-Location-Information



- Civic Location **street-group** subcommand—In order to display a value under the street name component on the civic address tab of the WCS wired clients display, we found it was necessary to use the civic location **street-group** subcommand in the switch configuration. If we look again at the left hand portion of Figure 36, we can see the street-group is specified as "Brookshire Avenue". On the right hand of Figure 36, we see that this value appears under the civic address tab of the WCS wired clients display under the label "Street".

Excluding Device Tracking on Select Switch Ports

In the majority of cases, when using context-aware wired device tracking, it is usually acceptable to simply enable NMSP on the switch and allow the attachment status of all ports to be reported to the MSE. In this way, the attachment status and any location or ELIN information specified for each port in the switch is reported and can be accessed from the MSE. However, in some cases, it might be desirable to enable wired device tracking on a switch, but exclude selected switch ports from reporting device attachments to the MSE. A reason for doing this might be to help reduce the number of MSE tracked device licenses required by eliminating the NMSP reporting of device attachments on select ports where not much chance of device migration is expected. Recall that in release 6.0, while it is possible to enable or disable wired device tracking entirely on a per MSE basis, it is not possible to limit the number of wired devices that are tracked in each MSE at this time (i.e., wired device tracking is either on or off). Therefore, any such limiting must be done manually by either disabling NMSP sessions with selected switches entirely (**no nmsp enable**) or disabling only the tracking of select switch ports on a context-aware switch that is otherwise reported device attachments normally.

To disable device tracking for select switch ports on a switch where NMSP has been enabled, the switch interface configuration **nmsp attachment suppress** command should be specified on each switch interface where device tracking is not desired. The nmsp attachment suppress interface command is used to configure the interface to not send any attachment notifications to a Cisco Mobility Services Engine (MSE).

If you are using Location MAC Filtering (**Services > Mobility Services > Context Aware Service > Administration> Filtering Parameters**) to specifically limit or block (by MAC address) tracked wireless clients and tags, be advised that these address filters also apply to wired device clients as well. Make sure that any filtering specifications that you set using Location MAC Filtering are flexible enough to allow tracking of not only your wireless clients and tags, but wired devices as well. Any devices that have been blocked from location tracking as a result of a defined filter will be viewable under the "Blocked MACs" listing on the Filtering Parameters page. Detailed information regarding how to configure Location MAC filtering can be found in Modifying Filtering Parameters section of the Cisco Context-Aware Service Configuration Guide 6.0 (http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html#wp1100062).

Classification and Marking of NMSP Sessions

A vital component in assuring NMSP session stability and acceptable CAS performance during periods of network congestion is the application of QoS to NMSP data flows between the MSE and any WLAN controllers or context-aware Ethernet switches in the Schools SRA design. Classification, marking and QoS should be applied ideally in both cases of locally deployed as well as centralized MSE implementations, however, it is especially important when using a centralized MSE at the district site and remote WLAN controllers and context-aware Ethernet switches in the schools.

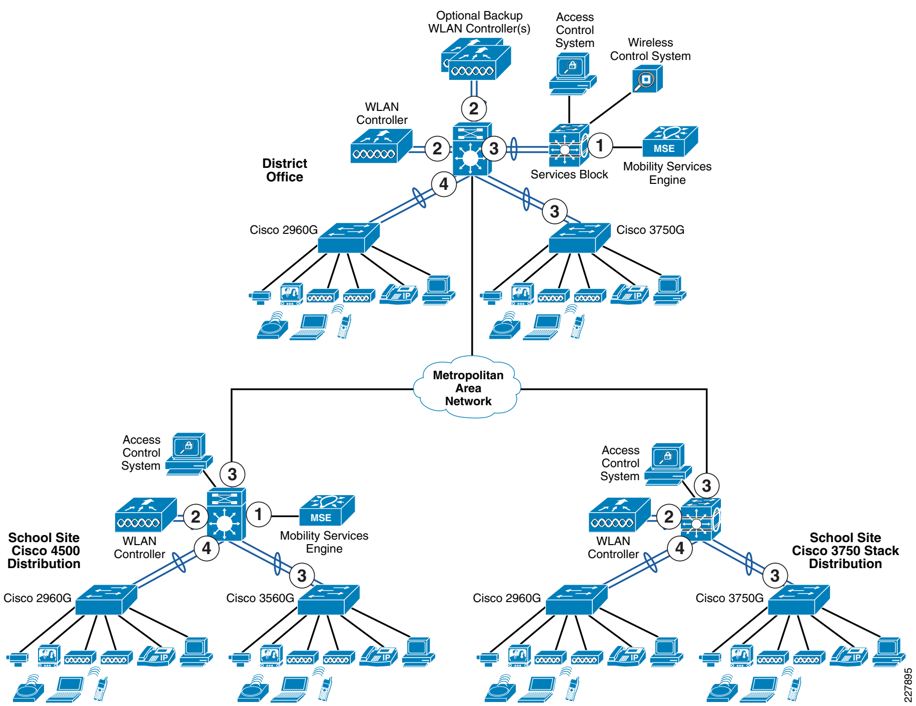
In order to ensure that QoS prioritization can occur properly for NMSP sessions the NMSP data flows must be properly identified, classified and marked as close as possible to their points of origin. This section explains where such marking of NMSP data flows should occur in the network, and how it should be performed.

Figure 37 provides an example of where identification, classification and marking of NMSP data flows should occur in the case of the school district design containing:

- A district office with adjoining data center
- A school site that is based on the Catalyst 4500 for distribution, with an MSE located at the school
- A school site that is based on the Catalyst 3750 switch stack for distribution.

In Figure 37, we have identified several points where classification and remarking needs to occur in order to properly mark NMSP traffic inbound from WLAN controllers and context aware switches, and outbound from Mobility Services Engines. These points are indicated by the yellow and red numbered circles.

Figure 37 Points of NMSP Classification and Marking



NMSP Traffic Flows Originating At The MSE

NMSP sessions between the MSE, WLAN controllers and context-aware switches are bi-directional in nature. Here, we are referring simply to that portion of any flow whose source address is that belonging to the Mobility Services Engine. Since the Mobility Services Engine does not mark the DSCP for the NMSP traffic it transmits into the network, all such traffic originating at the MSE will contain the default DSCP marking of 0x00. Left unchanged, when congestion is encountered in the Schools SRA design all NMSP traffic marked in this fashion will be treated with the lowest priority. This increases the probability that NMSP session data will be dropped in the network during periods of congestion. Left unchecked, this can result in NMSP session stability issues, and poor context-aware performance. Clearly, this is not desirable. We can avoid this by classifying and remarking NMSP data appropriately, as described in this section.

Since the MSE currently does not support classification and marking the DSCP value assigned to its traffic, we must make use of the classification and marking capabilities available to us in the Ethernet switch to which the MSE is attached. Thus, where **1** appears in Figure 37, we will:

- Define the criteria to select our NMSP traffic
- Define a class-map that will filter NMSP traffic using this criteria
- Define a service-policy to assign our desired DSCP value to the filtered traffic using the class-map
- Apply the service-policy to the port to which the MSE is attached.

Since we know that NMSP traffic will involve TCP port 16113, we can make use of this to identify NMSP traffic and proceed to mark it appropriately.

The following example defines a policy map that will mark NMSP traffic inbound to the network from the MSE as DSCP 0x12 (also referred to as DSCP 18, Assured Forwarding 21), police down to 10 Mbps per 8k burst, and mark down any NMSP traffic exceeding this accordingly using the QoS map.

```
mls qos
!
class-map match-all CAS
 match access-group name NMSP
!
policy-map MSE-Policy
 class CAS
 set dscp af21
 police 10000000 8000 exceed-action policed-dscp-transmit
!
ip access-list extended NMSP
 remark Identify NMSP traffic
 permit tcp any any eq 16113
 permit tcp any eq 16113 any


On the switch interface where the MSE is attached, it is imperative that
service-policy statement appears to assign the policy map to the
interface. For example:
interface GigabitEthernet1/0/2
description Mobility Services Engine MSE1
    .
      .
service-policy input MSE-Policy
```

NMSP Traffic Generated By WLAN Controllers

As was the case with the MSE, NMSP traffic entering the network originating at the WLC is also marked with the default DSCP value of 0x00. Left unchanged, when congestion is encountered in the Schools SRA design all NMSP traffic marked in this fashion will be treated with the lowest priority. Once again, this is not desirable and we shall address it in this section.

Like the MSE, the WLAN controller does not provide us with the ability to mark the NMSP traffic as we see fit, thus we must instead classify and mark this traffic inside the network. In accordance with general best practices, this operation is performed as close in the network as possible to the WLAN controller. Therefore, in Figure 37, the points at which this should occur are shown by **2**. Note that traffic coming from both normally active as well as any optional backup WLAN controllers must be classified and marked.

The method used to accomplish this classification and marking for WLAN controllers is very similar to that presented in the previous section for the MSE. However, since the WLAN controller is attached to the Ethernet switch using an Etherchannel port-channel group, there will be some relevant differences relating to whether the port-channel attachment is to a Catalyst 3750 switch stack or Catalyst 4500 distribution switch.

For example, when using the Catalyst 3750 switch stack in distribution, the following configuration would apply:

```
mls qos
!
class-map match-all CAS
 match access-group name NMSP
!
policy-map CAS-Policy
 class CAS
 set dscp af21
 police 10000000 8000 exceed-action policed-dscp-transmit
!
ip access-list extended NMSP
 remark Identify NMSP traffic
 permit tcp any any eq 16113
 permit tcp any eq 16113 any
```

The 3750 switch stack would also have a port-channel definition that would refer to the two physical Ethernet interfaces comprising the port-channel group.

```
interface Port-channel4
 description EC trunk to school 1266, WLC, interfaces gig1/0/28, 2/0/28
```

It is important to note that the 3750 switch stack does not support the use of a policy-map statement on a port-channel definition. In order to assure that NMSP traffic originating at the WLAN Controller in-bound to the network is properly classified and marked, ensure that a service-policy statement appears on each of the two physical interfaces that comprise the WLAN controller port-channel group in the 3750 switch stack. For example:

```
interface GigabitEthernet1/0/28
 description trunk to school 1266 WLC, port-channel4
    .
    .
 mls qos trust dscp
 channel-group 4 mode on
 service-policy input CAS-Policy
!
interface GigabitEthernet2/0/28
 description trunk to school 1266 WLC, port-channel4
    .
    .
 mls qos trust dscp
 channel-group 4 mode on
 service-policy input CAS-Policy
```

When using the Catalyst 4500 as the distribution switch, the scenario is a bit different. The Catalyst 4500 requires the service-policy to be assigned to the port-channel group used for the WLAN controller, and not the physical interfaces. Thus, our recommended configuration when using a Catalyst 4500 in distribution would be as follows:

```
!
class-map match-all CAS
 match access-group name NMSP
!
policy-map CAS-Policy
 class CAS
  set dscp af21
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit default
!
ip access-list extended NMSP
 remark Identify NMSP traffic
 permit tcp any any eq 16113
 permit tcp any eq 16113 any
!
interface Port-channel6
 description trunk to district WLC, interfaces gig2/11, gig3/11
    .
    .
 service-policy input CAS-Policy
!
!
interface GigabitEthernet2/11
 description trunk to district WLC, port-channel6
    .
    .
 channel-group 6 mode on
!
interface GigabitEthernet3/11
 description trunk to district WLC, port-channel6
    .
    .
 channel-group 6 mode on
!
```

NMSP Traffic Generated By Context-Aware Switches

As you will recall, specific models of Catalyst switches described earlier in this document (such as the 2960G, 3560, 3750, 4500, 4900 and others) can provide context-aware information to the MSE relating to IP-based attached devices. When this capability is enabled in a context-aware switch, the switch itself participates in an NMSP session with the MSE. This NMSP session is separate and independent of any NMSP sessions that may pass through the switch to or from attached devices (such as the WLAN controllers described earlier, or other downstream context-aware switches).

In order to ensure that the NMSP traffic originating at these switches is treated appropriately in the network during times of congestion, it is important that we properly classify the NMSP data originating at the context-aware switch and destined in-bound to the network for the MSE. Depending on the type of switch used, the exact method we shall use to apply this classification and marking will vary.

Layer-Three Context-Aware Switches

In the case of context-aware Layer-3 switches such as the 3750, 3560 and 4500, we can make use of local policy routing to assign an IP precedence 2 (DSCP 0x10) to NMSP traffic originating from the switch itself. Local policy routing in this fashion is performed internal to the context-aware L3 switch originating the NMSP traffic, and the traffic is marked prior to being introduced into the network. At the locations in Figure 37 marked with **3**, we can perform the required classification using a local policy route-map as follows:

```
ip local policy route-map switch-NMSP
!
route-map switch-NMSP permit 10
 match ip address NMSP
 set ip precedence 2
 set ip tos max-throughput
!
ip access-list extended NMSP
 permit tcp any any eq 16113
 permit tcp any eq 16113 any
!
```

Layer Two Context-Aware Switches

However, the use of the Cisco 2960G context-aware Layer-2 switch in the access layer presents a challenge. Local policy routing is not supported by the L2-only 2960G. Therefore, as a workaround, we must classify and mark the NMSP traffic originating from the 2960G at the next switch upstream to it in the network. In the Schools SRA design, this upstream switch would be the 3750 switch stack or 4500 distribution switch. In Figure 37, the points at where this must be performed are indicated by **4**.

Note that in the Schools SRA design, the 2960G access layer switches are attached to the distribution switches using an Etherchannel port-group, in a fashion very similar to that of the WLAN controllers. Therefore, similar techniques can be used to classify and mark the NMSP traffic originating at the 2960G and coming across the Etherchannel link.

Thus, for a 3750 switch stack used in distribution, a **class-map** and **policy-map** can be applied as described previously, and the **service-policy input CAS-Policy** statement applied to the physical interfaces in the 3750 switch stack that comprise the port-channel group to the 2960G switch. Just as for an Etherchannel-attached WLAN controller, a service-policy cannot be applied to the port-channel group definition used for the 2960G.

When using a Catalyst 4500 as the distribution switch with a context-aware 2960G at the access layer, apply the **service-policy input CAS-Policy** statement to the port-channel group definition for the 2960G. This would be done in a similar fashion to that described earlier for a Etherchannel-attached WLAN controller.

Hardware/Software Releases

Table 3 Hardware/Software Releases

Component	Version	Comments
Wireless Control System	6.0.132.0	For licensing and part number information, see http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html
Mobility Services Engine 3350	6.0.85.0	For client and tag licensing information, see http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html
Mobility Services Engine 3310	6.0.85.0	For client and tag licensing information, see http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html
WLAN Controller 4404	6.0.182.0	Standalone Cisco Wireless LAN Controller
WLAN Controller 4402	6.0.182.0	Standalone Cisco Wireless LAN Controller
Catalyst 4500	12.2.53-SG	Large school distribution switch; must use crypto (K9) image if CAS for wired devices is desired
Catalyst 3750E Switch Stack	12.2(52)SE	Small school distribution switch; must use crypto (K9) image if CAS for wired devices is desired
Catalyst 2960G	12.2(52)SE	Access switch; must use crypto (K9) image if CAS for wired devices is desired
Catalyst 3750E	12.2(52)SE	Access switch; must use crypto (K9) image if CAS for wired devices is desired
LAP1252 Access Point	6.0.182.0	Cisco Aironet 1250 Series Wireless Access Point
LAP1142 Access Point	6.0.182.0	Cisco Aironet 1140 Series Wireless Access Point
WCS Navigator	1.5.132.0	Optional component; for licensing information, see http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps7305/product_data_sheet0900aecd8065bd19.html
AeroScout T2 RFID Asset Tag	4.33	Available from http://www.aeroscout.com/; RFID tags are required only if RFID tracking is desired
AeroScout T3 RFID Asset Tag	6.05	Available from http://www.aeroscout.com/; RFID tags are required only if RFID tracking is desired
AeroScout EX-3200 Exciter	33007/60007	Chokepoint trigger, optional RFID enhancement; EX-2000 model recommended if outdoor placement is necessary

Context-Aware Services—General Best Practice References

The following are recommended references with regard to general best practice deployment recommendations for Cisco Unified Networks making use of Context-Aware Services release 6.0:

- A cornerstone of a successful design is knowledge of established best practices. Thus, it is highly recommended that you become familiar with the material presented in the following documents:
  - Context-Aware Solution Deployment Guide http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml
  - VoWLAN Design Guide 4.1 http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html
  - Context-Aware Services Configuration Guide, Release 6.0 http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/CAS_60.html
  - Wireless LAN Controller Configuration Guide, Release 6.0 http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html
  - Wireless Control System Configuration Guide, Release 6.0 http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html
- If you intend to make use of RFID tags in your Context-Aware solution, it is also recommended that you become familiar with the following document which explains the operation of the Cisco Context-Aware Engine for Tags:
  - AeroScout Context-Aware Engine for Tags for Cisco MSE User Guide, version 3.2 http://support.aeroscout.com
- If you intend to track the location and status of wired devices attached to Catalyst Ethernet switches, it is recommended that you familiarize yourself with the appropriate configuration guide for this feature in the switches you will be using. For example:
  - Catalyst 2960 Switch Software Configuration Guide, 12.2(50)SE http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/scg.html
  - Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/scg.html
  - Catalyst 4500 Series Switch Software Configuration Guide, 12.2(53)SG http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/53SG/configuration/config.html

During any deployment of Context-Aware Services and Cisco Unified Wireless Networks, detailed site surveys should be performed by a Cisco Wireless LAN Specialized Partner with expertise in voice, high speed data, and Context-Aware wireless network deployment. Cisco Systems also offers a complete package of bundled design and deployment services via the Cisco Advanced Services team. Cisco and our Wireless LAN Specialized Partners offer Context-Aware Design and Implementation Services to help you successfully deploy enterprise-class wireless connectivity. These services include the installation and configuration of crucial components such as the Mobility Services Engine (MSE), helping you to take full advantage of the strong security, management, and investment protection features that are built into Cisco Context-Aware components. In addition to planning, design, and implementation, we also offer services based on proven methodologies for operating and optimizing the performance of a Context-Aware Mobility solution, along with its associated technologies and strategies.

Note The importance of a properly performed wireless site survey of your facility cannot be over-emphasized. For more information on Cisco bundled planning, design, and deployment services, refer to http://www.cisco.com/en/US/services/ps2961/ps6899/ps8306/services_overview_context_aware.pdf. To locate a Cisco Wireless LAN Specialized Partner, refer to http://tools.cisco.com/WWChannels/LOCATR/openAdvanceSearch.do.